Universität Siegen

Wirtschaftswissenschaften
Wirtschaftsinformatik
Wirtschaftsrecht

Masterarbeit

zur Erlangung des Grades Master of Science Wirtschaftsinformatik

Evaluierung der Rolle der Kryptografie bei größeren IT-Sicherheitsvorfällen in den letzten fünf Jahren

Betreuer	Prof. Bernhard Esslinger
	Prof. Dr. Nils Kopal
Erstprüfer	Prof. Bernhard Esslinger
Zweitprüfer	Prof. Dr. Roland Wismüller

vorgelegt von	Felix Wiebe
Matrikelnummer	1142367
Abgabedatum	07. Januar 2025
(Update	02. März 2025)

Kurzzusammenfassung

Das Ziel dieser Arbeit war es, die Rolle der Kryptografie in IT-Sicherheitsvorfällen der letzten fünf Jahre zu untersuchen. Hierzu wurde eine qualitative Inhaltsanalyse nach Mayring durchgeführt, bei der verschiedene Sicherheitsvorfälle systematisch ausgewertet und deren Zusammenhang mit kryptografischen Praktiken analysiert wurden. Die Ergebnisse zeigen, dass Kryptografie eine wichtige Schutzfunktion hat, indem sie sensible Daten effektiv verschlüsselt und so das Risiko von Kompromittierungen reduziert. Gleichzeitig wurde deutlich, dass schwache oder falsch implementierte kryptografische Verfahren häufig zu erheblichen Sicherheitslücken führen können. Angreifer nutzen Kryptografie außerdem nicht nur als Ziel, sondern auch als Werkzeug, um Schadsoftware zu verschleiern und unerlaubten Zugriff auf Systeme zu erlangen. Neben den technischen Aspekten identifiziert die Arbeit auch organisatorische und menschliche Faktoren als entscheidend für die Wirksamkeit kryptografischer Maßnahmen.

Abstract

This thesis aimed to investigate the role of cryptography in IT-Security incidents over the last five years. For this purpose, a qualitative content analysis according to Mayring was conducted, in which various security incidents were systematically evaluated and their connection with cryptographic practices was analyzed. The results show that cryptography has an important protective function by effectively encrypting sensitive data and thus reducing the risk of compromise. At the same time, it became clear that weak or incorrectly implemented cryptographic procedures can often lead to significant security vulnerabilities. Attackers furthermore use cryptography not only as a target, but also as a tool to disguise malware and gain unauthorized access to systems. In addition to the technical aspects, this work also identifies organizational and human factors as decisive for the effectiveness of cryptographic measures.

Gender-Hinweis

Die in dieser Masterarbeit verwendeten Personenbezeichnungen beziehen sich immer gleichermaßen auf weibliche und männliche Personen. Auf eine Doppelnennung und gegenderte Bezeichnungen wird zugunsten einer besseren Lesbarkeit verzichtet.

Danksagung

An dieser Stelle möchte ich mich bei all denjenigen bedanken, die mich während der Anfertigung dieser Masterarbeit unterstützt und motiviert haben.

Zuerst gebührt mein Dank Herrn Prof. Bernhard Esslinger, der meine Masterarbeit betreut und begutachtet hat. Unser zweiwöchentlicher Austausch hat mir sehr dabei geholfen, immer am Ball zu bleiben. Für die hilfreichen Anregungen und die umfassenden Antworten auf meine Fragen möchte ich mich herzlich bei Ihnen bedanken.

Ich möchte mich auch bei Herrn Prof. Dr. Roland Wismüller bedanken, der sich als Zweitgutachter viel Zeit für meine Fragen und Feedback genommen hat. Unser Termin hat meine Masterarbeit nachhaltig geprägt, denn tatsächlich waren Sie es, der mich auf die Methodik der qualitativen Inhaltsanalyse aufmerksam gemacht hat.

Danke auch an Herrn Prof. Nils Kopal, der mir als Zweitbetreuer ebenfalls einige gute Hinweise und Ideen gegeben hat.

Ein besonderer Dank gilt meiner Freundin Isabel Roos und Yannick Benedickt, ohne die ich diese Arbeit nicht geschafft hätte. Ihr wart beide immer für mich da und hattet ein offenes Ohr für mich. Ihr habt mich aufgebaut, wenn ich eine Phase der Demotivation hatte und es immer wieder geschafft, dass ich nicht aufgebe. Danke.

Ebenfalls möchte ich mich bei meinem Bruder Andreas bedanken. Während meines Studiums hast du dir immer wieder Zeit für mich genommen und mir bei Fragen oder Problemen zur Seite gestanden.

Abschließend möchte ich mich bei meinen Eltern Valeria und Franz bedanken, die mir mein Studium durch ihre Unterstützung ermöglicht haben und stets ein offenes Ohr für mich hatten.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AES Advanced Encryption Standard
AD Active Directory
API Application Programming Interface
ASA Cisco Adaptive Security Appliance
AWS Amazon Web Services
BSI Bundesamt für Sicherheit in der Informationstechnik
CISO Chief Information Security Officer
CSIS Center for Strategic and International Studies
CSIDB Cyber Security Incident Database
CSV Comma-separated values
CVE Common Vulnerabilities and Exposures
CWE Common Weakness Enumeration
ECB Electronic Code Book Mode
FTC Federal Trade Commission
HIBP Have I Been Pwned?
HTTPS Hypertext Transfer Protocol Secure
MFA Multi-Faktor-Authentifizierung
MSA Microsoft Account
MITM Man-in-the-Middle-Angriff
NIS-2 2. EU-Richtlinie für Netzwerk- und Informationssicherheit
OAuth Open Authorization
OWA Outlook Web Access
RaaS Ransomware-as-a-Service
RDP Remote Desktop Protocol
RSA Rivest-Shamir-Adleman
SHA-1 Secure Hash Algorithm 1
SIT Südwestfalen-IT
SSH Secure Shell
SSL Secure Sockets Layer
SSRF Server-Side Request Forgery
TOR The Onion Router
VPN Virtual Private Network

WAF Web Application Firewall

1. Einleitung

Die digitale Transformation und der zunehmende Einsatz vernetzter Technologien haben die Abhängigkeit unserer Gesellschaft von Informations- und Kommunikationssystemen erheblich verstärkt. [1, 2] Gleichzeitig wächst die Bedrohung durch Cyberangriffe stetig, wie aktuelle Berichte belegen. Unternehmen, Behörden und Privatpersonen sehen sich immer ausgeklügelteren Angriffsmethoden gegenüber, die enorme wirtschaftliche und gesellschaftliche Schäden verursachen können. Allein im Jahr 2021 belief sich der Schaden auf die deutsche Wirtschaft durch Cyberangriffe auf über 204 Milliarden Euro. [3]

Zur Eindämmung dieser Risiken wurden in den vergangenen Jahren neue gesetzliche Richtlinien und Normen, wie die NIS-2-Richtlinie der Europäischen Union, beschlossen. Unternehmen werden damit aufgefordert, robuste Sicherheitsmaßnahmen für ein hohes Schutzniveau zu implementieren, um Angriffe abzuwehren und kritische Infrastrukturen zu schützen. NIS-2 legt dabei nicht nur den technischen Rahmen fest, sondern verweist auch auf die direkte Verantwortung und Haftung der Geschäftsführung für die Einhaltung der Sicherheitsstandards. Verstöße können zu hohen Strafen und existenziellen Bedrohungen für Organisationen führen, was das Interesse an einer korrekten Implementierung unterstreicht. [4]

Im Kontext dieser Entwicklungen spielt die Kryptografie eine zentrale Rolle. Sie bildet das Fundament der Informations- und IT-Sicherheit und stellt aber gleichzeitig ein gewisses Risiko bei falscher oder fehlender Implementierung dar. [5] Die Untersuchung von IT-Sicherheitsvorfällen bietet eine einzigartige Gelegenheit, ein besseres Verständnis für die Schwachstellen und Mechanismen hinter den Angriffen zu entwickeln.

Die Motivation dieser Arbeit ist es daher, eine Evaluation bedeutender IT-Sicherheitsvorfälle vorzunehmen, um ein besseres Verständnis für die Rolle der Kryptografie sowie für Schwachstellen und Angriffsvektoren zu erlangen. Langfristig sollen die Ergebnisse dazu beitragen, effektivere Präventions- und Abwehrmaßnahmen zu entwickeln und die Resilienz gegen Cyberangriffe zu stärken. Dieses Thema ist nicht nur wissenschaftlich relevant, sondern hat auch praktische Implikationen für Unternehmen, Behörden und die Gesellschaft als Ganzes.

1.1. Zielsetzung

Das Ziel dieser Masterarbeit ist die Untersuchung, welche Rolle die Kryptografie in größeren IT-Sicherheitsvorfällen der letzten fünf Jahre einnahm und welchen über- oder untergeordneten Einfluss sie auf den Verlauf dieser Vorfälle hatte. Der Fokus liegt insbesondere auf der Analyse kryptografischer Schwächen, fehlerhafter Implementierungen und falscher Anwendungen kryptografischer Verfahren, die zu IT-Sicherheitsvorfällen geführt haben. Die Arbeit strebt an, ein tieferes Verständnis für häufige Ursachen im Umgang mit Kryptografie zu gewinnen und deren Auswirkungen zu bewerten.

Im Rahmen dieser Zielsetzung werden folgende drei Forschungsfragen betrachtet:

- **F1**: Welche Gemeinsamkeiten und Muster lassen sich in den betrachteten Sicherheitsvorfällen erkennen?
- **F2**: Inwieweit tragen menschliche oder organisatorische Faktoren zu Sicherheitsvorfällen bei?
- **F3**: Welchen Einfluss hat Kryptografie in Sicherheitsvorfällen?

F1 und F2 werden in Abschnitt 5.2, F3 in Abschnitt 5.3 behandelt. Durch die Beantwortung dieser Forschungsfragen soll nicht nur ein Beitrag zur wissenschaftlichen Diskussion über die Bedeutung der Kryptografie in IT-Sicherheitsvorfällen geleistet werden, sondern auch praxisnahe Empfehlungen abgeleitet werden, die langfristig zur Erhöhung der IT-Sicherheit beitragen.

1.2. Aufbau der Arbeit

Diese Arbeit wurde wie folgt gegliedert. Sie beginnt mit der Einleitung in Abschnitt 1. Es folgt eine Einführung in die grundlegenden Begriffe und Konzepte in Abschnitt 2. Abschnitt 3 dient zur Vorstellung verwandter Literatur. In Abschnitt 4 wird eine Definition von größeren IT-Sicherheitsvorfällen vorgenommen, sowie der Suchprozess und die Vorstellung passender IT-Sicherheitsvorfälle beschrieben. Darauf folgt die Evaluation der IT-Sicherheitsvorfälle hinsichtlich der Rolle der Kryptografie in Abschnitt 5. Die Ergebnisse der Evaluation werden anschließend in Abschnitt 6 diskutiert, Limitationen der Arbeit dargelegt sowie ein Ausblick. Abschnitt 7 beendet die Arbeit mit der Zusammenfassung und dem Ausblick auf zukünftige mögliche Arbeiten.

2. Grundlagen

Dieser Abschnitt führt die zentralen Fachbegriffe und Konzepte ein, die für das Verständnis der nachfolgenden Untersuchung von Bedeutung sind. Hierzu werden grundlegende technische und theoretische Themen verständlich und prägnant erläutert.

2.1. Grundlegende Begriffe

Im Kontext von IT-Sicherheitsvorfällen werden viele verschiedene Termini verwendet, die ähnlich klingen oder nicht auf Anhieb deutlich werden. Dieses Kapitel stellt nachfolgend die zentralsten Begriffe vor.

2.1.1. Sicherheit

Es gibt drei übergeordnete Sicherheitsbegriffe: *Informationssicherheit*, *IT-Sicherheit* und *Cybersicherheit*. [6] Da die Begriffe in der Literatur nicht einheitlich beschrieben sind, werden zunächst Definitionen vorgenommen, die für die weitere Ausarbeitung verwendet wurden.

2.1.1.1 Informationssicherheit

Informationssicherheit bezeichnet den Schutz von Informationen und ihrer Verarbeitung vor unbefugtem Zugriff, Manipulation und Offenlegung. [6] Sie bildet eine unverzichtbare Grundlage für die Funktionsfähigkeit moderner Unternehmen und Behörden, da Informationen einen zentralen Wert darstellen. Nahezu alle Geschäftsprozesse und Fachaufgaben in Wirtschaft und Verwaltung sind heute ohne IT-Unterstützung nicht mehr denkbar. Eine verlässliche Informationsverarbeitung sowie die dazugehörige Technik sind daher unerlässlich für die Aufrechterhaltung des Betriebs. [7, S. 17]

Im Zentrum der Informationssicherheit stehen die drei Schutzziele **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** von Informationen, die im Englischen auch als *CIA-Triade* (**c**onfidentiality, **i**ntegrity, **a**vailability) bekannt sind. Sie beschreiben essenzielle

Anforderungen, die an den Schutz von Informationen gestellt werden müssen, und werden im Folgenden näher erläutert. [7, S. 17], [6]

Vertraulichkeit
Vertraulichkeit gewährleistet, dass Informationen nur von autorisierten Personen oder Systemen eingesehen werden können. Sie schützt sensible Daten wie personenbezogene Informationen oder unternehmensinterne Informationen vor unbefugtem Zugriff. Ein Verstoß gegen die Vertraulichkeit, etwa durch ungewollte Offenlegung, kann sowohl juristische als auch wirtschaftliche Schäden verursachen. [7, S. 17, 42]

Integrität
Integrität bezeichnet die Sicherstellung der Unversehrtheit und Korrektheit von Daten sowie der Funktionsweise von Systemen. Im Bezug auf Daten bedeutet das, dass diese vollständig und unverändert sind. In der Informationstechnik ist eine Erweiterung auf den Begriff Informationen geläufig, also Daten, die mit Attributen wie Autorenschaft oder Erstellungszeitpunkt verknüpft sind. Der Verlust von Integrität kann sich durch unautorisierte Änderungen von Attributen äußern, wie z. B. verfälschte Angaben zur Urheberschaft oder manipulierte Zeitangaben. [7, S. 38] Ein wesentlicher Bestandteil von Integrität ist die *Authentizität*, also die Überprüfbarkeit und Zuordnung von Daten zur richtigen Quelle. Würden einer Person falsche Daten zugeordnet werden, könnte sich dies in dem Missbrauch der digitalen Identität niederschlagen oder Bestellungen und Zahlungsanweisungen unberechtigten Dritten zugeordnet werden. [7, S. 17]

Verfügbarkeit
Verfügbarkeit bedeutet, dass Informationen und Systeme bei Bedarf zugänglich und funktionsfähig sind. Ein Verlust der Verfügbarkeit kann dazu führen, dass wesentliche Geschäftsprozesse zum Stillstand kommen. Beispiele hierfür sind Produktionsausfälle, unterbrochene Geldtransaktionen oder blockierte Online-Dienste. Selbst wenn die Verfügbarkeit nur eingeschränkt ist, kann dies den Betrieb erheblich beeinträchtigen. [7, S. 17]

Ein weiteres wichtiges Konzept der Informationssicherheit ist **Verbindlichkeit** (engl. nonrepudiation). Die Verbindlichkeit eines Systems stellt sicher, dass ein Subjekt die Durchführung bestimmter Aktionen im Nachhinein nicht abstreiten kann. [8, S. 13] Es sollen nur autorisierte Benutzer mit Daten arbeiten und diese nur auf autorisierte Weise

verwenden oder ändern können. [6] Diese Eigenschaft ist insbesondere im elektronischen Handel und Geschäftsverkehr von zentraler Bedeutung, da sie die Rechtsverbindlichkeit von Transaktionen wie Käufen oder Verträgen garantiert. Digitale Signaturen sind ein häufig genutztes Mittel zur Erfüllung dieser Anforderung. Verbindlichkeit ist eng mit der **Abrechenbarkeit** (engl. accountability) verknüpft, die Überwachungs- und Protokollierungsmaßnahmen erfordert, um Benutzeraktivitäten nachzuverfolgen. [8, S. 13]

2.1.1.2 IT-Sicherheit

IT-Sicherheit umfasst ein breites Spektrum an Technologien und Sicherheitslösungen, die sich nicht nur auf Dinge wie Computer, Server, Netzwerke und Anwendungen beschränkt, sondern auch physische Sicherheitsmaßnahmen wie Schlösser, Überwachungskameras oder Chipkarten einschließt. Aufgrund dieser Bandbreite gibt es innerhalb der IT-Sicherheit noch zahlreiche Unterarten, wie beispielsweise die Cloud-, Netzwerk oder Anwendungssicherheit. [9]

2.1.1.3 Cybersicherheit

Cybersicherheit umfasst alle Technologien, Verfahren und Richtlinien, die darauf abzielen, Computersysteme, Anwendungen, Geräte und Daten vor Cyberangriffen zu schützen oder deren Auswirkungen zu minimieren. Sie ist ein zentraler Bestandteil des Risikomanagements von Unternehmen und Behörden, da erfolgreiche Cyberangriffe zu Identitätsdiebstahl, Erpressung, Verlust sensibler Informationen und erheblichen finanziellen Schäden führen können. Wichtige Werkzeuge und Praktiken unfassen beispielsweise die Schulungen zur Stärkung des Sicherheitsbewusstsein (engl. Security-Awareness), die Erkennung und Reaktion auf Bedrohungen oder die Wiederherstellung im Katastrophenfall (engl. Disaster Recovery). [10]

2.1.2. IT-Sicherheitsvorfall

IT-Sicherheitsvorfälle (engl. IT-Security Incidents) entstehen durch einzelne Ereignisse oder eine Kette (unglücklicher) Umstände und können die Vertraulichkeit, Integrität oder Verfügbarkeit (siehe Abschnitt 2.1.1.1) von Informationen und IT-Systemen gefährden. Dies beeinträchtigt häufig zentrale Geschäftsprozesse und Fachaufgaben der betroffenen Institution. Auch ohne öffentliche Bekanntmachung können solche Vorfälle

das Vertrauen von Geschäftspartnern und Kunden schädigen oder rechtliche Vorgaben verletzen. Dabei ist zu erwähnen, dass es oft nicht die größten Schwachstellen sind, die erhebliche Schäden verursachen, sondern die Kombination kleinerer Ursachen. [7, S. 99]

Unzureichend geschützte Informationen stellen einen oft unterschätzten Risikofaktor dar, der für Institutionen existenzbedrohende Konsequenzen haben kann. Neben finanziellen Einbußen drohen auch Imageschäden, wenn Sicherheitsvorfälle öffentlich bekannt werden. Ein angemessener Schutz ist jedoch mit vergleichsweise geringen Mitteln zu erreichen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet in seinem IT-Grundschutz[1] praxistaugliche Methoden an, um Informationen effizient und angemessen zu schützen. [7, S. 17]

Bei einem kryptografischen IT-Security Incident werden häufig sensible Informationen wie Passwörter, Kreditkartennummern oder andere persönliche Daten aufgrund von mangelnder Sicherheit kompromittiert. [11] Angreifer machen sich dabei verschiedene Schwachstellen zunutze, um sich Zugang zu fremden Systemen oder Netzwerken zu verschaffen. Oft mit dem Ziel, Daten zu exfiltrieren oder zu verschlüsseln. Folgend werden einige Schwachstellen aufgelistet:

- Übertragung von Daten im Klartext (Passwörter, persönliche Daten, Kreditkartennummern, Gesundheitsdaten) durch unverschlüsselte Protokolle wie HTTP, SMTP oder FTP [11, 12],
- Speicherung von Daten im Klartext (Passwörter, Keys etc.) [11],
- Nutzung von veralteten Kryptografiealgorithmen und -verfahren [11] (z. B. Electronic Code Book Mode (ECB) [13, S. 149]),
- Nutzung von schwachen oder standardmäßigen Verschlüsselungsschlüsseln (engl. encryption keys) sowie die Wieder- oder Weiterverwendung kompromittierter Schlüsseln [11] oder
- Ausnutzen von kryptografischen Fehlermeldungen [12] (z. B. adaptive chosen-ciphertext attack [14, S. 43]).

[1] Weitere Informationen: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

2.1.3. Datenlecks und Datenexfiltration

Ein **Datenleck** (eng. data breach) bezeichnet die unbeabsichtigte Offenlegung vertraulicher Informationen, oft bedingt durch technische oder organisatorische Schwachstellen [15]. Auch wenn dabei nicht direkt ein Cyberangriff vorliegt, so stellt ein Datenleck einen Sicherheitsvorfall und damit eine erhebliche Bedrohung für Unternehmen und staatliche Organisationen dar. Sie beinhalten oft sensible Informationen wie Mitarbeiter- oder Kundendaten, geistiges Eigentum oder medizinische Unterlagen und können schwerwiegende Reputationsschäden, finanzielle Verluste und in manchen Fällen die langfristige Instabilität der betroffenen Organisation umfassen. [16, S. 1]

Bei der Klassifikation von Datenlecks unterscheidet man zwischen einer **bewussten** und einer **unbewussten Offenlegung** von Informationen: Bei der unbewussten wurde weiter zwischen inneren und äußeren Bedrohungen unterschieden. „Bewusst“ bedeutet, dass Informationen durch Eindringlinge oder durch Sabotageakte von Innentätern offengelegt werden. Letzteren stehen oft Motive wie Unternehmensspionage, Unzufriedenheit mit dem Arbeitgeber oder finanzielle Belohnungen entgegen. [16, S. 2]

Unbewusste Datenlecks entstehen in erster Linie durch unvorhergesehene Handlungen, die auf schlechte Geschäftsprozesse zurückzuführen sind. Darunter fallen interne Bedrohungen wie die Nachlässigkeit der Mitarbeiter oder etwa das Versäumnis, angemessene Präventivtechnologien und Sicherheitsrichtlinien im Unternehmen zu etablieren. Externe Bedrohungen entstehen durch Hackerangriffe, Social-Engineering-Techniken wie Phishing, Malware oder schlecht konfigurierte Zugriffskontrollen. [16, S. 2]

Datenexfiltration ist die diskrete Handlung von Datendiebstahl. Jede Datenexfiltration erfordert ein Datenleck oder eine Datenschutzverletzung, aber nicht alle Datenlecks oder Datenschutzverletzungen führen zu einer Datenexfiltration. Beispielsweise kann sich ein Bedrohungsakteur stattdessen dafür entscheiden, die Daten im Rahmen eines Ransomware-Angriffs zu verschlüsseln oder sie zu verwenden, um das E-Mail-Konto einer Führungskraft zu kapern. Dies ist dann solange keine Datenexfiltration, bis die Daten unter der Kontrolle des Angreifers kopiert oder auf ein anderes Speichergerät verschoben werden. [17]

2.1.4. Common Weakness Enumeration

Die Common Weakness Enumeration (CWE) ist eine von der MITRE Corporation entwickelte und von der Gemeinschaft gepflegte Liste von bekannten Schwachstellen und Sicherheitslücken in Software und Hardware. Sie dient als standardisierte und einheitliche Sprache zur Beschreibung von Schwachstellen, um Entwicklern, Sicherheitsforschern und Organisationen ein gemeinsames Verständnis und eine eindeutige Kommunikationsbasis zu bieten. Ziel der CWE ist es, Sicherheitsprobleme in Architektur, Design und Code zu identifizieren, zu kategorisieren und dadurch das Risiko von Sicherheitsverletzungen zu reduzieren. [18]

In dieser Arbeit aufgetretene oder erkannte CWE sind in Anhang A.1 auf S. 82 zu finden.

2.1.5. Common Vulnerabilites and Exposures

Common Vulnerabilities and Exposures (CVE) ist ein von der MITRE Corporation entwickeltes System zur standardisierten Identifikation und Benennung von öffentlich bekannten Sicherheitslücken und Schwachstellen in Software und Hardware. Im Gegensatz zu der CWE beziehen sich CVE auf Sicherheitslücken in konkreter Soft- oder Hardware, während in der CWE allgemeingültige Schwachstellen kategorisiert werden. In den CVE erhält jede Sicherheitslücke eine eindeutige CVE-Identifikationsnummer, um eine konsistente Referenzierung zu ermöglichen und die Zusammenarbeit zwischen verschiedenen Sicherheits- und Softwareanbietern zu erleichtern. Dadurch soll Transparenz und Effizienz in der Sicherheitsbranche gefördert werden, indem eine zentrale, öffentlich zugängliche Liste für Schwachstellen bereitgestellt wird. [19]

In dieser Arbeit aufgetretene CVE sind in Anhang A.2 auf S.83 zu finden.

2.2. Kryptografie

Kryptografie bezeichnet die Wissenschaft und Kunst der Sicherung von Informationen und Kommunikation gegen unbefugten Zugriff durch Dritte. [13, S. 3] Möglich gemacht wird dies durch Verschlüsselung. Das bedeutet, dass die eingegebenen Informationen mithilfe von speziellen mathematischen Algorithmen so verändert werden, dass diese ohne Kenntnis des richtigen „Schlüssels“ nicht wieder lesbar gemacht werden können und für Dritte somit unbrauchbar werden. [20]

Die Historie von Kryptografie reicht weit zurück. Erste Anwendungen lassen sich bereits in die Antike zurückverfolgen. Dort wurden in Ägypten bestimmte geheime, nicht allgemein bekannte Hieroglyphen verwendet, um den Empfängerkreis einer Nachricht einzuschränken. Spätere Anwendungen fanden sich unter anderem bei den Griechen und Spartanern. Diese verwendeten für die Übermittlung von Nachrichten eine Skytale. [21, S. 344] Dabei handelte es sich um einen Zylinder oder Stab einer bestimmten Größe und Länge, um den ein Lederband gewickelt wurde, auf dem die Buchstaben einer Nachricht aufgebracht wurden. Für die Entschlüsselung der richtigen Reihenfolge der Buchstaben benötigte der Empfänger einen Zylinder der gleichen Größe, wie ihn der Absender verwendet hatte. [13, S. 3] Auch im antiken Rom wurden ähnlich einfache kryptografische Verfahren verwendet. Der Feldherr Gaius Iulius Caesar verwendete eine Chiffre, die durch simple Verschiebung der Buchstaben des Alphabets funktionierte. [13, S. 15] Bei der sogenannten „Caesar-Chiffre“ wurden zwei Alphabete untereinander geschrieben:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Das untere Alphabet wurde um einen bestimmten numerischen Wert verschoben, z. B. um vier:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Die Buchstaben der Nachricht wurden anschließend mithilfe des verschobenen Alphabets umgewandelt und konnten damit auch wieder in die Ursprungsform überführt werden. Als Beispiel würde das Wort VERSCHLUESSELUNG bei einer Verschiebung um vier Stellen zu ZIVWGLPYIWWIPYRK werden.

Die Verschlüsselungstechniken entwickelten sich im Laufe der Jahrhunderte immer weiter und wurden irgendwann zu den hochkomplexen Algorithmen der modernen Kryptografie, die heute in digitaler Kommunikation allgegenwärtig sind. [13, S. 2] Heute ist die Kryptografie ein Kernelement der Cybersicherheit und hilft dabei, Informationstechnik vor dem unerwünschten Zugriff Dritter zu schützen. [13, S. 23] Anwendungen finden sich beispielsweise in der verschlüsselten Internetkommunikation, EC-Karten, digitalen Signaturen oder Wahl-Computern. [22]

Für alle genannten Verfahren ist in Esslinger [14, 37 f.] der Schlüsselraum tabellarisch aufbereitet und es wird dort auf kostenlose Software[2] verwiesen, um die Verfahren online auszuprobieren.

Für die kryptografische Verschlüsselung von Informationen gibt es grundsätzlich zwei Arten, die durch Kombination auch in Hybridverfahren angewendet werden können.

2.2.1. Symmetrische Verschlüsselung

Die **symmetrische Verschlüsselung** basiert auf der Verwendung eines gemeinsam bekannten Geheimschlüssels (engl. Secret Key), für die Kommunikation. In Folgendem werden beispielhaft zwei Personen betrachtet, Alice und Bob. Alice (Sender) und Bob (Empfänger) tauschen den Geheimschlüssel auf einem möglichst sicheren Kanal vor Beginn der eigentlichen Kommunikation aus. Anschließend kann der Schlüssel von beiden dazu verwendet werden, Nachrichten zu verschlüsseln und gleichermaßen wieder zu entschlüsseln. Die in Abschnitt 2.2 genannten Chiffren funktionieren alle nach diesem Prinzip. [14, 24 ff.]

Symmetrische Verschlüsselungsalgorithmen bieten hohe Geschwindigkeiten für die Ver- und Entschlüsselungsprozesse [14, S. 25] und werden häufig für das Hashen von Dateien und die Integritätsprüfung (siehe Abschnitt 2.2.3) von Nachrichten verwendet. [13, S. 4] Das bekannteste moderne Verfahren für symmetrische Verschlüsselung stellt der Advanced Encryption Standard (AES) dar. [14, S. 26]

[2] Siehe CrypTool: https://www.cryptool.org/de/

Durch die Notwendigkeit des vorherigen Austauschs des Geheimschlüssels scheint eine sichere Kommunikation für zwei sich unbekannte Parteien auf diese Weise fast unmöglich. [14, S. 25] Dieses Problem lässt sich jedoch mithilfe der asymmetrischen Verschlüsselung umgehen, die im nachfolgenden Teil erläutert wird.

2.2.2. Asymmetrische Verschlüsselung

Die **asymmetrische Verschlüsselung** benötigt für zwei Teilnehmer insgesamt vier schlüssel. Alice und Bob besitzen jeweils ein Schlüsselpaar, das aus einem öffentlichen (engl. Public Key) und einem geheimen Schlüssel (engl. Private Key) besteht. Alice und Bob tauschen ihre öffentlichen Schlüssel vor der Kommunikation aus, entweder durch das Mitsenden in der ersten Nachricht oder beispielsweise durch die Veröffentlichung im Internet [14, S. 28].

Um den sicheren Nachrichtenaustausch zu beginnen, verschlüsselt Alice ihre Nachricht mit dem öffentlichen Schlüssel von Bob. Dieser kann die eingehende Nachricht nur durch seinen eigenen geheimen Schlüssel wieder entschlüsseln. Umgekehrt würde Bob seine Antwort mit dem öffentlichen Schlüssel von Alice verschlüsseln, damit diese die Nachricht mithilfe ihres Geheimschlüssels wieder lesbar machen kann. [14, 28 f.]

Der Vorteil von asymmetrischen Verfahren ist, dass kein sicherer Kanal für den Schlüsseltausch erforderlich ist. Es ist nur wichtig darauf zu achten, dass der zu verwendende öffentliche Schlüssel auch wirklich von dem angestrebten Kommunikationspartner stammt und nicht manipuliert wurde. Ein Nachteil von asymmetrischen Verfahren ist, dass diese erheblich langsamer sind, als symmetrische. Das bekannteste Verfahren für die asymmetrische Verschlüsselung ist der RSA-Algorithmus. [14, S. 29]

2.2.3. Hashfunktionen

Unter Hashfunktionen verstehen wir hier eine kryptografische Einwegfunktion. Die Besonderheit von Einwegfunktionen ist, dass es sehr einfach ist, aus einem Ausgangswert einen Funktionswert zu berechnen, es aber erheblich mehr Aufwand erfordert, aus einem Funktionswert den dazu gehörigen Ausgangswert zu ermitteln. Ein Hashwert lässt sich

also immer zweifelsfrei zu seiner Ausgangsnachricht zuordnen, jedoch lassen sich über den Hashwert allein keine Rückschlüsse über die ursprüngliche Nachricht ziehen. [13, S. 369] Dadurch lassen sich Hashfunktionen in einer Vielzahl von Szenarien einsetzen. So ist es beispielsweise möglich, mittels Hashfunktion die Integrität eines langen Datenblocks zu prüfen. [13, 336 f.] Das Hashen der gleichen Nachricht führt immer zu einem gleichen Ausgangswert. Diese Eigenschaft macht man sich beispielsweise dann zu Nutzen, wenn man bei einer langen Nachricht lediglich den Hashwert der Nachricht signiert, statt die gesamte Nachricht. [13, 337 f.]

2.2.3.4 Salting

Eine gute Herangehensweise an den Umgang mit gespeicherten Nutzer-Accountdaten ist es, Passwörter niemals im Klartext auf den eigenen Systemen abzulegen, sondern nur den Hashwert der verwendeten Passwörter zu speichern oder zu übertragen. Da der Hashwert immer vom eingegebenen Passwort abhängt, muss man nicht die Passwörter selbst vergleichen, sondern kann lediglich die Hashwerte gegeneinander prüfen. [23] Dieser Umstand macht das Speichern von Passwörtern jedoch noch nicht sicher, da ein Angreifer mit ausreichend Zeit und Speicherplatz alle Hashwerte für Passwörter der Länge *1* bis n berechnen könnte. Die Ergebnisse dieser Berechnungen kursieren oftmals im Netz unter der Bezeichnung „Rainbow Table“ (siehe Tabelle 2.1), welche Hashwerte und die zugehörigen Klartext-Passwörter auflisten. [23] Um den Angriff mittels Rainbow Table abzuwehren, eignet sich die Verwendung von sogenannten Salt-Werten. Dies sind zufällige Zeichenfolgen fester Länge, die vor dem Hashen an das Passwort angehangen werden und anschließend mitsamt des Passworts in der Datenbank abgelegt werden. Dadurch ist eine naive Zuordnung von Passwort und Hashwert nicht mehr möglich. [23] Sollte ein Angreifer Kenntnis vom Passwort-Salt erlangen, beispielsweise durch (lesenden) Zugang zur Datenbank oder eines Datenbank-Dumps, kann diesem durch einen sog. „Pepper“ die Arbeit weiter erschweren. Ein Pepper funktioniert auf die gleiche Weise wie ein Salt, der Unterschied besteht hier jedoch, dass der Pepper für alle Passwörter identisch ist und nicht in der Datenbank gemeinsam mit den Hashwerten abgelegt wird. [23]

Moderne Hashverfahren wie bcrypt verwenden weitere Mechanismen, um sich gegen Angreifer zu schützen. Erklärt wird dies in Kapitel 7.1.4 von Esslinger [14, S. 447 ff.].

2.3. Arten von Cyberangriffen

Cyberangriffe zählen zu den größten Bedrohungen der modernen Informationslandschaft. Die Ausführung und Organisation erfolgt durch verschiedene Akteure, wie Staaten, kriminelle Gruppierungen, Aktivisten oder Einzelpersonen. Jede dieser Gruppen kann dabei unterschiedliche Methoden anwenden, um ihre Ziele zu erreichen. Sei es das Stehlen sensibler Daten, das Lahmlegen kritischer Infrastrukturen oder das Erpressen von finanziellen Lösegeldern durch „Geiselnahme“ von Clients und Servern. [24, S. 213] Angreifer finden die unterschiedlichsten Wege, um Schaden anzurichten. Die nachfolgenden Abschnitte sollen einen Überblick über die relevanten Angriffe und Vorgehensweisen bei IT-Sicherheitsvorfällen geben.

2.3.1. Angriffsvektoren mit kryptografischem Schwerpunkt

Während die Kryptografie Verschlüsselungsverfahren beschreibt und erzeugt, beschreibt die Kryptoanalyse Angriffe auf diese Verfahren. Die Kryptoanalyse umfasst viele verschiedene Angriffe, von denen nachfolgend vier in Tabelle 2.1 vorgestellt werden.

Unter dem Begriff „Angriffsvektoren“ werden in dieser Arbeit spezifische Wege oder Methoden verstanden, über die Cyberkriminelle unbefugten Zugriff auf die Systeme ihrer Zielobjekte erlangen können. Dies umfasst sowohl technische Schwachstellen als auch soziale Manipulationstechniken, die es den Angreifern ermöglichen, vertrauliche Daten zu stehlen, Systeme zu kompromittieren oder diese durch Verschlüsselung unbrauchbar zu machen.

Tab. 2.1: Ausgewählte Angriffsvektoren in der Kryptoanalyse

Angriff	**Beschreibung**
Brute-Force-Angriff	Der Angreifer probiert systematisch alle möglichen Schlüssel aus, um den richtigen zu finden. Die Anzahl der möglichen Schlüssel hängt dabei von der Schlüssellänge ab. Bei einem 8-Bit-Schlüssel gibt es beispielsweise 256 mögliche Schlüssel, die der Angreifer einzeln ausprobieren muss. Mit zunehmender Schlüssellänge steigt jedoch der Zeitaufwand für den Angriff exponentiell, was ihn bei ausreichend langen Schlüsseln unpraktikabel macht. [5]
Wörterbuchangriff	Der Angreifer erstellt ein „Wörterbuch“, das aus bekannten Geheimtexten und den dazugehörigen Klartexten besteht. In einer einfachen Variante sammelt der Angreifer über einen längeren Zeitraum solche Paare. Wenn er später einen neuen Geheimtext entdeckt, durchsucht er das Wörterbuch, um den entsprechenden Klartext zu finden. Dieser Angriff ist besonders effektiv, wenn sich Geheimtexte und Klartexte wiederholen oder wenn schwache Passwörter verwendet werden. [5]
Man-in-the-Middle-Angriff (MITM)	Ein Angreifer täuscht den Kommunikationspartnern, z. B. Alice und Bob, vor, direkt miteinander verbunden zu sein, während er in Wirklichkeit den Datenverkehr abfängt und manipuliert. Dabei geht der Angreifer wie folgt vor. Wenn Alice zu Beginn der Kommunikation Bobs öffentlichen Schlüssel anfordert, fängt er diese Anfrage ab und schickt stattdessen seinen eigenen öffentlichen Schlüssel an Alice. Alice verschlüsselt daraufhin ihre Nachricht mit diesem Schlüssel und sendet sie zurück an den Angreifer. Dieser kann nun die Nachricht entschlüsseln, lesen oder manipulieren. Dann verschlüsselt er die Nachricht erneut mit seinem öffentlichen Schlüssel und sendet diesen und die Nachricht an Bob. [5]
Rainbow Table	Hierbei werden vorab berechnete und optimierte Zuordnungen von Passwort-Hashes zu Klartext-Passwörtern in einer Tabelle gespeichert. Diese ermöglicht es einem Angreifer, Passwörter deutlich schneller zu finden, da lediglich eine schnelle Suche in der Tabelle erforderlich ist. Um solche Angriffe zu erschweren, sollten zusätzliche Sicherheitsmechanismen eingeführt werden. [20, S. 174]

2.3.1.5 Ransomware

Ransomware ist eine besonders tückische Art von Malware, die die Dateien eines Opfers verschlüsselt oder das System sperrt, bis ein Lösegeld gezahlt wird. Diese Form der digitalen Erpressung hat sich in den letzten Jahren zu einer der prominentesten Bedrohungen im Bereich der Cybersicherheit entwickelt. [25, S. 2] Ransomware-Angriffe zielen auf Einzelpersonen, aber auch auf Unternehmen, Krankenhäuser und kritische Infrastrukturen ab, was ihre Auswirkungen besonders verheerend machen kann. [25, S. 7] Man unterscheidet zwei Arten von Ransomware.

Kryptoransomware verschlüsselt bestimmte oder alle Dateien eines Opfers und macht sie unzugänglich, bis ein Lösegeld gezahlt wird. Dabei werden fortschrittliche Verschlüsselungstechniken verwendet, um sicherzustellen, dass die Daten ohne den entsprechenden Decryptor (Schlüssel zum Entschlüsseln) nicht wiederhergestellt werden können. [25, 26, S. 4] Eine bekannte Kryptoransomware ist *LockBit*, die seit ihrem Auftreten im Jahr 2019 bereits viele verschiedene Unternehmenssysteme befallen hat. Die Strategie der Kriminellen verfolgte dabei häufig eine Masche der doppelten Erpressung: Zuerst wurden die Opfer zu einer Zahlung für die Entschlüsselung ihrer Dateien gebracht, um anschließend weiteres Lösegeld für die Nicht-Veröffentlichung der gestohlenen Daten zu fordern. [27]

Lockerransomware sperrt hingegen das gesamte Gerät und macht es unbenutzbar. Der Zugriff durch Maus, Tastatur oder andere Eingabegeräte ist nicht mehr möglich. Lediglich ein Bildschirm mit Instruktionen zum Zahlen eines Lösegelds wird angezeigt. Der Angriff zielt darauf ab, das System so lange unbrauchbar zu machen, bis die Opfer zur Zahlung eines Lösegelds gebracht werden. [25, 26, S. 4] Im Jahre 2017 erregte die Lockerransomware *WannaCry* große Aufmerksamkeit und sperrte knapp 230.000 Systeme weltweit auf diese Weise. [26]

2.3.2. Angriffsvektoren ohne kryptografischen Schwerpunkt

In diesem Abschnitt werden typische Angriffsvektoren ohne kryptografischen Schwerpunkt, wie z. B. Social Engineering und Malware, vorgestellt.

2.3.2.6 Social Engineering und Phishing

Social Engineering gilt als eine der gefährlichsten Bedrohungen für die Cybersicherheit in der heutigen Zeit. Der Mensch gilt als schwächstes Glied in der Cybersicherheitskette, vor allem weil Menschen anderen Menschen mehr und eher Vertrauen entgegen bringen, als Computern. [28, S. 1] Daher ist Social Engineering eine beliebte Methode der Cyberkriminalität, die auf der Manipulation menschlicher Verhaltensweisen basiert, um sensible Informationen zu erlangen oder unerlaubte Handlungen durchzuführen. Die Angriffe nutzen Psychologie und soziale Interaktionen als Werkzeuge, um Sicherheitsmaßnahmen zu umgehen, ohne dabei technische Schwachstellen direkt auszunutzen. Kriminelle machen sich dies zunutze, indem sie sich von Beginn an ein hohes Maß an Vertrauen aufbauen, sodass das Opfer gar nicht merkt, dass es ausgenutzt wird. Dazu kommt, dass die Durchführung von Social-Engineering-Angriffen keine speziellen technischen Kenntnisse verlangt und es auch keine Möglichkeiten gibt, sich durch Hard- oder Software davor zu schützen. [29, S. 498]

Ein Social-Engineering-Angriff besteht nach Saini et. al. [29, S. 499] aus vier Phasen: **Informationsbeschaffung**, **Aufbau von Beziehungen**, **Ausbeutung** und **Ausführung**.

Eine gründliche **Informationsbeschaffung** bildet die Basis eines erfolgreichen Angriffs. In dieser Phase versuchen die Angreifer so viele Informationen wie möglich über das Ziel zu sammeln. Dafür werden Webseiten und öffentlich abrufbare Dokumente, aber auch analoge Informationsquellen wie beispielsweise Mülltonnen des Opfers durchsucht und soziale Kontakte überprüft. [29, S. 499] Konnten die Angreifer genug Informationen beschaffen beginnt die zweite Phase, der **Aufbau von Beziehungen**. Es wird eine persönliche Beziehung zum Opfer aufgebaut, etwa durch das Senden einer Nachricht oder über andere Wege, um sein Interesse zu wecken und eine Abhängigkeit zu etablieren. [29, S. 500] In der darauf folgenden **Ausbeutung** wird die Beziehung zum Opfer so weit vertieft, dass man die Informationen erhält, die für die Fertigstellung des Plans

und die Entwicklung einer neuen Spyware erforderlich sind. In der **Ausführung** wird schließlich der Plan umgesetzt und die Kommunikation mit dem Opfer eingestellt sowie keine Beweise hinterlassen. [29, S. 500]

Social Engineering umfasst insgesamt viele verschiedene Methoden, die sich oftmals in ihrer Durchführungsweise ähneln. Tabelle 2.2 bietet eine Übersicht über sieben dieser Methoden.

Tab. 2.2: Sieben verschiedene Arten des Social Engineering (Quelle: [30, 85110, Tab. 4])

Art	Beschreibung
Pretexting	Angreifer täuschen eine falsche Identität oder Geschichte vor, um an vertrauliche Informationen zu gelangen.
Baiting	Angreifer nutzen einen Köder (eng. bait), wie einen mit Malware versehenen USB-Stick, und platzieren ihn so, dass er gefunden wird. Die Neugier des Opfers führt im besten Falle dazu, dass der Datenträger in einen privaten oder geschäftlichen Computer gesteckt und das Gerät so kompromittiert wird.
Piggybacking	Kriminelle dringen auf physischem Wege in gesicherte Bereiche ein, indem sie sich als berechtigte Benutzer ausgeben. In Unternehmen mit großer Mitarbeiterzahl kann dies z. B. durch das Aufhalten von Türen durch „echte“ Mitarbeiter geschehen.
Phishing	Zielt darauf ab, Menschen dazu zu bringen, persönliche und finanzielle Informationen preiszugeben oder auf direktem Wege Geld an die Angreifer zu senden. Angreifer nutzen dafür häufig elektronische Kommunikationswege wie E-Mails, SMS, soziale Netzwerke oder Webseiten.
Vishing (Voice Phishing)	Telefonanrufe werden dazu benutzt, um Menschen durch soziale Manipulation und technologisch verstellte Stimmen zur Preisgabe sensibler Informationen zu bewegen.

Fortsetzung auf nächster Seite

Tab. 2.2 – Fortsetzung.

Art	Beschreibung
Spear-Phishing	Bezeichnet speziell auf eine Einzelperson oder eine ausgewählte Gruppe zugeschnittene Angriffe, die oft öffentlich zugängliche Informationen des Opfers nutzen, um betrügerische Nachrichten authentischer wirken zu lassen.
Whaling	Ist eine erweiterte Form von Spear-Phishing, die auf Personen von hohem finanziellem oder unternehmerischem Wert abzielt, wie Führungskräfte oder hochrangige Mitarbeiter.

2.3.2.7 Malware

Malware, kurz für *malicious software*, bezeichnet jedwede Art von Software, die speziell dazu entwickelt wurde, Computer und die darauf befindlichen Daten zu manipulieren, zu stehlen oder zu zerstören. [31, S. 20] Die Verbreitung von Malware erfolgt häufig über das Internet, etwa in Form von infizierten E-Mail-Anhängen, schädlichen Websites oder durch das Ausnutzen von Sicherheitslücken in Software. Dabei nimmt Social Engineering eine besondere Rolle ein, da Nutzer dazu verleitet werden, schädliche Dateien herunterzuladen oder auf verdächtige Links zu klicken. [32] Man unterscheidet verschiedene Arten von Malware (siehe Tabelle 2.3), die spezifische Ziele und Funktionsweisen besitzen. Die Abgrenzung ist dabei nicht immer eindeutig, da es viele Ähnlichkeiten untereinander gibt.

Malware wird ständig weiterentwickelt und deshalb ist ihre Bekämpfung schwer. Moderne Malware verwendet Verschlüsselungstechniken, um die Erkennung durch Virenscanner und andere Sicherheitsmechanismen zu umgehen. [32, S. 22] Nicht nur deshalb bleiben neue Malware-Varianten oft lange Zeit unentdeckt, was die Reaktionszeiten auf Sicherheitsvorfälle deutlich verlängert.

Tab. 2.3: Verschiedene Malwarearten (Quelle: [32, 21 f.])

Bezeichnung	Beschreibung
Viren	Selbst replizierende Programme, die für ihre Verbreitung einen Wirt (Datei oder Software) benötigen. Durch den infizierten Wirt können sie sich weiter auf Systemen und Netzwerken ausbreiten und diese bis hin zum Stillstand verlangsamen.
Würmer	Haben eine ähnliche Funktionsweise wie Viren, nur sind sie unabhängig von einem Wirt. Die Verbreitung erfolgt über Speichergeräte und E-Mails. Sie verlangsamen infizierte Systeme und führen zu einem hohen Ressourcenverbrauch.
Trojanisches Pferd	Wird auch Trojaner genannt und ist als harmlose Software getarnt. Wird die kompromittierte Software ausgeführt, beginnt der Trojaner im Hintergrund mit der Ausführung schädlicher Aktionen, wie dem Stehlen von sensiblen Daten oder der Überwachung des Nutzers.
Rootkit	Malware, die sich auf Betriebssystemebene installiert und Systemfunktionen manipuliert, um sich vor Entdeckung zu schützen.
Spyware	Spionagesoftware, die zur Überwachung und Ausspähung sensibler Informationen und Aktivitäten eines Nutzers dient.
Keylogger	Unterart von Spyware, die oft mit anderer Malware zusammen auftritt. Keylogger zeichnen Tastatureingaben auf und können dadurch Informationen wie Passwörter oder Kreditkartendaten erfassen und an Kriminelle senden.
Sniffer	Spähen die Netzwerkaktivitäten aus und überwachen diese für weitere mögliche zukünftige Malwareangriffe.

2.3.2.8 Zero-Day-Exploit

Ein Zero-Day-Exploit nutzt eine bislang unbekannte oder ungepatchte Sicherheitslücke in Software, Hardware oder Firmware, sodass der Anbieter „null Tage“ Zeit zur Abwehr hat und böswillige Akteure unmittelbar Zugriff erhalten. Man unterscheidet zwischen Zero-Day-Schwachstellen, also unentdeckten oder nicht behobenen Sicherheitslücken, und Zero-Day-Malware, das sind Schadprogramme ohne bekannte Signatur, die von Antivirenlösungen nicht erkannt werden. Obwohl laut dem X-Force Threat Intelligence Team von IBM nur etwa drei Prozent aller erfassten Sicherheitslücken Zero-Day-Schwachstellen sind, stellen sie aufgrund ihrer möglichen Verbreitung in populären Betriebssystemen und Geräten ein erhebliches Risiko dar. Ist eine Schwachstelle öffentlich bekannt, beginnt ein Wettlauf zwischen Sicherheitsteams, die an Patches arbeiten, und

Angreifern, die die Lücke versuchen auszunutzen. Da Exploits häufig innerhalb weniger Tage nach Bekanntwerden einer neuen Schwachstelle verfügbar sind, stehen Unternehmen und Entwickler unter Druck, rechtzeitig Sicherheitsupdates zu veröffentlichen, um das Gefahrenpotenzial einzugrenzen. [33]

2.3.2.9 Supply-Chain-Angriff

Das Cybersecurity-Unternehmen Fortinet [34] beschreibt das Vorliegen eines Supply-Chain-Angriffs, wenn ein externer Dienstleister oder Partner, der Zugriff auf die Daten und Systeme eines Zielunternehmens hat, genutzt wird, um unbefugt in dessen Infrastruktur einzudringen. Dabei reicht es oft, entweder die Abwehr des Drittanbieters zu überwinden oder in dessen Lösung eine Hintertür zu platzieren. Besonders attraktiv sind Produkte und Komponenten, die von vielen Organisationen verwendet werden. Denn sobald es Angreifern gelingt, in der Software eines häufig genutzten Herstellers oder einer Open-Source-Community Schadcode zu integrieren, eröffnet sich ihnen mit einem Schlag der Zugriff auf zahlreiche Ziele. Bei ausländischen Produkten kann zudem staatlicher Einfluss oder die unbemerkte Manipulation von Firmware zu einer Schwachstelle werden. [34]

Haben Angreifer eine Gelegenheit gefunden, binden sie den Schadcode meist in Software-Updates oder Hardware ein, die Kunden vertrauensvoll installieren. Auf diese Weise können sie Zertifikate missbrauchen, Entwicklungsprozesse manipulieren oder bereits vor Auslieferung Malware auf Geräten platzieren. All diese Varianten basieren darauf, dass man sich die über lange Zeit hinweg aufgebaute Vertrauenswürdigkeit externer Anbieter zunutze macht, um Sicherheitsbarrieren effektiv zu umgehen. [34]

Ein gut bekanntes Beispiel für einen Supply-Chain-Angriff ist der Sicherheitsvorfall bei *SolarWinds* (siehe Abschnitt 4.3.6, 35), bei dem die Angreifer die weit verbreitete Software *Orion* mit Schadcode infizierten und so zahlreiche Unternehmen und Regierungsbehörden angreifen konnten. Ein anderes Beispiel ist die *Stuxnet-Malware*[3], die 2010 verwendet wurde, um gezielt Nukleararanlagen des Irans zu infiltrieren. [34]

Die Methodik der qualitativen Inhaltsanalyse nach Mayring wird in Abschnitt 5 auf S. 48 beschrieben.

[3] https://de.wikipedia.org/wiki/Stuxnet

3. Verwandte Arbeiten

Die Analyse von Sicherheitsvorfällen ist ein wesentlicher Bestandteil der Forschung im Bereich der Informationssicherheit. Zahlreiche Studien haben sich darauf konzentriert, Ursachen, Angriffsvektoren und die Auswirkungen von Cyberangriffen zu untersuchen, um ein besseres Verständnis für die zugrunde liegenden Mechanismen zu entwickeln und präventive Maßnahmen zu fördern. Dabei lag der Fokus jedoch in den meisten Fällen nicht auf kryptografischen Verfahren oder Angriffen, sondern auf allgemeinen Schwachstellen, organisatorischen Mängeln oder technischen Aspekten. Die vorliegende Arbeit soll diese Forschungslücke adressieren, indem sie die Rolle der Kryptografie in Sicherheitsvorfällen systematisch untersucht.

Mehrere Studien widmen sich der Analyse und Kategorisierung von IT-Sicherheitsvorfällen in unterschiedlichen Branchen und liefern somit eine wertvolle Grundlage für weiterführende Forschung, wie sie in dieser Arbeit angestrebt wird. So geben beispielsweise sowohl [35] als auch [36] einen umfangreichen Überblick über eine Vielzahl verschiedener Vorfälle im maritimen oder Wassersektor. In beiden Publikationen werden die jeweiligen Angriffsvektoren, die betroffenen Systeme sowie organisatorische und technische Schwachstellen systematisch aufbereitet und dokumentiert. Damit stellen sie wertvolle Basisliteratur für Vorfallübersichten dar und liefern grundlegende Informationen über Vorgehensweisen und Methoden zur Analyse von IT-Sicherheitsvorfällen.

Obwohl die aufgeführten Arbeiten eine breite Palette von Schwachstellen und Angriffstypen abdecken, liegt in diesen Untersuchungen kein expliziter Fokus auf kryptografischen Aspekten. Insbesondere fehlen vertiefte Analysen dazu, ob und in welcher Form Verschlüsselungs- oder Authentifizierungsmechanismen eingesetzt wurden und wie sich diese auf den Verlauf der Sicherheitsvorfälle auswirkten. Gerade vor dem Hintergrund, dass Kryptografie eine zentrale Rolle in der IT-Sicherheit einnimmt, entsteht hier eine Forschungslücke, die in der vorliegenden Arbeit adressiert wird. Während etwa [37] bereits verschlüsselungsbasierte Angriffsszenarien wie Ransomware beleuchtet, bleibt auch dort in weiten Teilen unklar, inwieweit die Wirksamkeit kryptografischer Maßnahmen und Gegenmaßnahmen untersucht wurde.

4. IT-Sicherheitsvorfälle der letzten fünf Jahre

Dieser Abschnitt beschreibt den Prozess der Suche und das Zusammenfassen der gefundenen IT-Sicherheitsvorfälle der Jahre ab 2019 (die Arbeit entstand im Jahr 2024). Zu Beginn wird eine Klassifikation von größeren IT-Sicherheitsvorfällen vorgenommen. Auf Basis der Klassifikation wurde anschließend eine strukturierte Suche nach relevanten Vorfällen durchgeführt und dokumentiert. Die Ergebnisse werden abschließend im Einzelnen näher beschrieben.

4.1. Klassifikation von IT-Sicherheitsvorfällen

Die Klassifikation von IT-Sicherheitsvorfällen stellte eine die Grundlage für das weitere Vorgehen dar. Deshalb war eine klare Abgrenzung zwischen „normalen“ und „größeren“ Vorfällen erforderlich, um den Fokus der Analyse auf jene Vorfälle zu legen, die erhebliche Auswirkungen auf Organisationen, Branchen oder Nutzer hatten. Da es keine allgemeingültige Definition größerer IT-Sicherheitsvorfälle gibt, wurde eine eigene herausgearbeitet und für diese Arbeit verwendet. Hierfür wurde eine Liste von Kriterien entwickelt, die eine systematische Einordnung der Vorfälle ermöglichte (siehe Tabelle 4.1). Die Kriterien berücksichtigen sowohl qualitative als auch quantitative Aspekte.

Im Mittelpunkt stand der Bezug zur Kryptografie. Demnach musste jeder Sicherheitsvorfall dieses Kriterium erfüllen, was durch Schlüsselwörter wie „encryption“ oder „hashes“ abgelesen wurde. Daneben wurde festgelegt, dass mindestens ein weiteres Kriterium aus Tabelle 4.1 erfüllt sein musste, damit der Fall als relevant galt. Es sollte jedoch möglich sein, dass mehrere Kriterien gleichzeitig zutreffen konnten und somit die Schwere des Vorfalls unterstrichen. Aufgrund der unterschiedlichen Güte der dokumentierten Informationen einzelner Fälle bestand nicht der Anspruch, eine allgemeingültige Definition zu erfassen. Für die in dieser Arbeit betrachteten IT-Sicherheitsvorfälle wurde diese Vorgehensweise gewählt, um Nachvollziehbarkeit zu gewährleisten.

Tab. 4.1: Kriterien für größere IT-Sicherheitsvorfälle

Kriterium/Merkmal	**Beschreibung**
Bezug*	Der Fall muss einen Bezug zum Thema Kryptografie aufweisen. Dies kann etwa durch bestimmte Angriffsarten (z. B. Ransomware) oder andere Hinweise, die auf einen Kryptografiebezug hindeuten (z. B. kryptografiebezogene Begriffe, wie „Encryption“, „Hash“ oder „Key“), abgelesen werden.
Betroffene	Die Anzahl der von dem Angriff betroffenen Nutzer oder Dritten liegt bei über 10 Millionen.
Datenverlust	Es gibt einen schweren Verlust vertraulicher Daten. Für die Einordnung können die Größe (z. B. mehrere Giga- oder Terabyte) oder die Anzahl der kompromittierten Daten (z. B. über 10 Millionen) dienen.
Auswirkungen	Der Angriff hat erhebliche Auswirkungen auf betroffene Nutzer und Unternehmen. Darunter fallen Konsequenzen im Arbeitsalltag, wie etwa Produktionsstopps oder Ausfälle der Infrastruktur und Dienste.
Kritikalität der Ziele	Der Angriff richtet sich auf Ziele hoher Kritikalität, wie beispielsweise Regierungen, Behörden oder kritische Infrastruktur[4].
Schaden	Der finanzielle Schaden des Angriffs beläuft sich auf mehrere Millionen US-Dollar oder Euro.

*Das Kriterium muss immer zutreffen.

4.2. Suchprozess

Die Identifikation geeigneter IT-Sicherheitsvorfälle mit kryptografischem Bezug bildete eine wichtige Basis für die spätere Analyse in dieser Arbeit. Die Vorgehensweise orientierte sich grundsätzlich an den Methoden eines systematischen Literaturreviews, wich jedoch im Auswahlprozess von diesem ab, da aufgrund des Themas und auf unterschiedlichen Arten aufbereiteten Informationen keine einfache Zuordnung über Parameter wie *Titel* oder *Abstract* möglich war. Das Ziel war daher, relevante Vorfälle gezielt aufzunehmen, ohne dass ein strikter Ausschlussprozess notwendig war. Damit wurde der Fokus

[4] Siehe https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html

auf die effiziente Sammlung relevanter Informationen und deren themenspezifischer Auswertung gelegt.

4.2.1. Festlegung von Datenquellen

Zu Beginn wurden geeignete Datenquellen definiert, die die Grundlage für die Recherche bilden. Diese umfassen themenbezogene Datenbanken sowie öffentlich zugängliche Suchmaschinen und Listen. Die ausgewählten Datenquellen sind in Tabelle 4.2 aufgeführt. Die Suchmaschine DuckDuckGo wurde aufgrund der persönlichen Präferenz des Autors verwendet.

Tab. 4.2: Datenbanken und Suchmaschinen für die Recherche

Datenbank / Suchmaschine	**URL**
Have I Been Pwned? (HIBP)	`https://haveibeenpwned.com/PwnedWebsites`
Center for Strategic and International Studies (CSIS)	`https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents`
Cyber Security Incident Database (CSIDB)	`https://www.csidb.net`
DuckDuckGo	`https://duckduckgo.com`

4.2.2. Suchbegriffe und Suchzeitraum

Es wurden überwiegend englische Suchbegriffe verwendet. Für die Recherche wurde eine Trennung der Suchbegriffe vorgenommen, basierend auf der Art der genutzten Quelle. Dafür wurden die zwei Sammlungen *Allgemein* und *Spezifisch* erstellt, die in Tabelle 4.3 dargestellt sind. Für die Nutzung von Suchmaschinen wurden allgemeinere Suchbegriffe definiert, um auch Rankings, Übersichtslisten oder Berichte zu IT-Sicherheitsvorfällen einzuschließen. Der Fokus lag hierbei darauf, eine breite Basis potenziell relevanter Vorfälle zu generieren, die anschließend durch Detailanalyse weiter eingegrenzt wurden. Für Datenbanken wurden **spezifischere** Begriffe verwendet, da davon ausgegangen wurde, dass diese in der Regel detaillierte Informationen zu konkreten Sicherheitsvorfällen mit kryptografischem Bezug enthielten. Die Suchergebnisse der allgemeinen Suche wurden ebenfalls mit diesen Schlüsselwörtern durchsucht.

Tab. 4.3: Verwendete Suchbegriffe für die allgemeine und spezifische Suche nach IT-Sicherheitsvorfällen

Allgemein		**Spezifisch**
Englisch	Deutsch	Englisch
biggest cyber attacks	größte cyberangriffe	cryptography
biggest data breaches		encrypt
biggest data leaks	größte datenlecks	key
worst cyber attacks	schlimmste cyberangriffe	decrypt
worst data breaches		
worst data leaks	schlimmste datenlecks	

Der **Suchzeitraum** sollte die letzten fünf Jahre zum Zeitpunkt der Anfertigung dieser Arbeit abdecken. Dabei wurde das Jahr 2019 als untere Grenze festgelegt, jedoch keine scharfe Grenze im Dezember 2023 gemacht, sondern auch aktuellere Fälle aus dem Jahr 2024 berücksichtigt.

4.2.2.10 Recherche

Für die Suchmaschinensuche wurde ausschließlich DuckDuckGo verwendet. Die allgemeinen Suchbegriffe dienten dazu, gezielt nach Listen, Rankings oder Berichten zu suchen. Aus den gefundenen Übersichten wurden mithilfe der spezifischen Schlüsselwörter sowie durch das Lesen der Vorfallsbeschreibungen geeignete Fälle extrahiert.

Für die Recherche innerhalb der Datenbanken wurde zunächst eine geeignete Menge von Sicherheitsvorfällen extrahiert. Bei HIBP wurde der Quellcode der Seite in ein Textdokument kopiert. Dessen Inhalt wurde anschließend mit einem Python-Skript in ein CSV-Dateiformat überführt. Dabei wurden die Werte durch Kommata getrennt und konnten über Excel als Tabelle weiterverarbeitet werden.

Die Ergebnisse wurden, sofern die Plattform (Datenbank) dies ermöglichte, nach Kriterien wie der Anzahl kompromittierter Konten, der Angriffsart oder dem Angriffsziel sortiert. Anschließend wurden die Ergebnisse durch Anwendung der Schlüsselwörter analysiert, um Vorfälle mit kryptografischem Bezug zu identifizieren. Vorfälle von Interesse wurden direkt aufgenommen, ohne dabei einen aufwendigen Ausschlussprozess, wie er für einen systematischen Review vorgesehen ist, durchzuführen.

Es wurde außerdem angenommen, dass im Darknet[4] weitere Informationen zu einzelnen Sicherheitsvorfällen vorliegen könnten. Hierzu wurde über den TOR-Browser[5] eine Verbindung zum Darknet hergestellt und einzelne, öffentlich bekannte Suchmaschinen mit den zuvor genannten Suchbegriffen (siehe Tabelle 4.3) sowie bereits gefundener Sicherheitsvorfälle durchsucht. Nachdem dies ergebnislos blieb, wurde dieser Schritt im weiteren Prozess nicht weiter berücksichtigt.

4.3. Ergebnisse

In diesem Abschnitt werden die Ergebnisse der Recherche vorgestellt. Insgesamt wurden siebzehn Sicherheitsvorfälle für eine nähere Betrachtung identifiziert. Tabelle 4.4 dient als Übersicht für die nachfolgend beschriebenen IT-Sicherheitsvorfälle. Jedem Sicherheitsvorfall wird eine Tabelle mit den wichtigsten Eckdaten vorangestellt. Die dort enthaltenen Einträge zur CWE werden, soweit aus den Quellen bestätigt werden konnte, entsprechend zitiert. Da allerdings nicht immer Informationen über die CWE vorlagen, steht an einigen Stellen eine Einschätzung des Autors, die durch einen Stern * gekennzeichnet ist. Eine Beschreibung aller verwendeten CWE-Einträge ist in Anhang A.1 zu finden. Details über genannte CVE sind ebenfalls im Anhang zu finden (siehe Anhang A.2).

Die Darstellung der einzelnen IT-Sicherheitsvorfälle folgt einer einheitlichen Struktur. Zu Beginn wird ein Sicherheitsvorfall zeitlich eingeordnet und die Folgen auf Organisationen und Nutzer beschrieben. Danach folgt eine Ausführung des Hergangs sowie der Methoden und Schwachstellen, die böswillige Akteure für den Angriff oder den Datendiebstahl genutzt haben. Abschließend wird die Reaktion der Betroffenen erläutert. Dazu gehören der Umgang mit dem Sicherheitsvorfall, die ergriffenen Maßnahmen zu Abwendung oder Minderung des Schadens sowie etwaige Entschädigungen, die direkt oder aus späteren Gerichtsverfahren folgten.

[4] https://de.wikipedia.org/wiki/Darknet
[5] https://www.torproject.org/de/

Tab. 4.4: Gefundene IT-Sicherheitsvorfälle im Überblick

Nr.	Jahr	Vorfall	Angriffsart	Besonderheit
SV01	2019	CafePress	Datenleck	Unsicherer Hash-Algorithmus verwendet
SV02	2020	Canva	Datenleck	Starker Hash-Algorithmus verwendet
SV03	2019	Capital One	Datenleck	Standardmäßiger Einsatz von Verschlüsselung schütze Großteil der kompromittierten Daten
SV04	2020	BigBasket	Datenleck	Unsicherer Hash-Algorithmus verwendet
SV05	2020	CAM4	Datenleck	Offengelegte Passwörter waren durch Hashing geschützt
SV06	2020	SolarWinds	Supply-Chain-Angriff, Trojaner	Überlistung des Signaturprozesses für Updates
SV07	2021	Brenntag	Ransomware	Lösegeld wurde für verschlüsselte Daten gezahlt
SV08	2021	Colonial Pipeline	Ransomware	Pipelineversorgung an der Ostküste der USA wurde durch Ransomware lahmgelegt
SV09	2021	Microsoft Exchange	Ransomware, Supply-Chain-Angriff, Zero-Day-Exploit	Vier Zero-Day-Schwachstellen ausgenutzt
SV10	2021	T-Mobile US	Datenleck	Etwa 100 Millionen Kundendaten betroffen
SV11	2022	LastPass	Datenleck, Social Engineering	Sensible Daten von Millionen Nutzern konnten kopiert werden, weil ein Mitarbeiter gehackt wurde.

Fortsetzung auf nächster Seite

Tab. 4.4 – Fortsetzung.

Nr.	Jahr	Vorfall	Angriffsart	Besonderheit
SV12	2022	Uber	Social Engineering	Angreifer verschafften sich Zugang über einen von MFA-Meldungen genervten Mitarbeiter
SV13	2023	MGM Resorts	Ransomware	Angreifer erlangten durch Vishing Zugang zu den Systemen von MGM
SV14	2023	Microsoft Exchange	Zero-Day-Exploit	Erbeuteter Signaturschlüssel erlaubte das Erstellen gefälschter Token für den Zugriff auf E-Mail-Konten
SV15	2023	Okta	Datenleck	Angreifer erbeuteten Session-Tokens und nutzen diese für Session-Hijacking
SV16	2023	Südwestfalen-IT	Ransomware, Zero-Day-Exploit	Über 150 Kommunen und Organisationen in Nordrhein-Westfalen und Niedersachsen betroffen
SV17	2024	Change Healthcare	Datenleck, Ransomware	Verschlüsselung von Daten eines großen US-Gesundheitsdienstleisters

4.3.1. SV01 – CafePress (2019)

Tab. 4.5: Eckdaten des CafePress Datenlecks (2019)

Merkmal	Beschreibung
Datum	Februar 2019
Art	Datenleck
Kryptografie	Schwache Hashfunktionen
CWE	*CWE-327

Im Februar 2019 wurde CafePress, ein US-Anbieter für personalisierte Merchandise-Artikel und T-Shirts, Opfer eines schwerwiegenden Datenlecks. Bei dem Sicherheitsvorfall wurden die Daten von über 23 Millionen Benutzerkonten kompromittiert: Darunter befanden sich E-Mail-Adressen, Namen, Wohnadressen, Telefonnummern und Passwörter. Später wurde bekannt, dass sich unter den gestohlenen Daten auch Antworten zu Sicherheitsfragen und etwa 180.000 besonders schützenswerte Sozialversicherungsnummern im Klartext befanden. [38, 39]

Wie genau es zu dem Angriff kommen konnte, ist nicht geklärt. Mit der Veröffentlichung der Passwörter wurde schnell deutlich, dass etwa die Hälfte lediglich mit dem veralteten und leicht zu umgehenden *SHA1-Algorithmus*[6] gehasht wurde. Eine von den Angreifern erstellte oder erbeutete Datenbank umfasste etwa 493.000 Einträge und wurde im Dark Web zum Verkauf angeboten. [38, 40]

CafePress hatte ein mangelhaftes Krisenmanagement im Umgang mit dem Datenleck. Das Unternehmen versuchte zunächst, den Sicherheitsvorfall zu vertuschen und informierte die betroffenen Personen offiziell erst im September 2019. Zu dem Zeitpunkt waren die ersten Berichte bereits einen Monat alt. Verschärfend kommt hinzu, dass CafePress bereits vor dem Vorfall Kenntnis über bestehende Sicherheitsprobleme hatte. BleepingComputer [41] berichtete, dass das Unternehmen laut einer Beschwerde der amerikanischen Finanzbehörde FTC bereits seit mindestens Januar 2018 von diversen kompromittierten Händlerkonten wusste. Anstatt die Betroffenen zu informieren, schloss CafePress diese Konten und verlangte sogar eine Gebühr von 25 US-Dollar für die Kontoschließung. Eine Maßnahme, die das Unternehmen ergriff, war die Erzwingung eines

[6] https://en.wikipedia.org/wiki/SHA-1

Passwortwechsels bei der Anmeldung – ohne dabei das Datenleck zu erwähnen. Drei Jahre später wurde CafePress von der FTC mit einer Strafe von 500.000 US-Dollar belegt. [38, 39, 40]

4.3.2. SV02 – Canva (2019)

Tab. 4.6: Eckdaten des Canva Datenlecks (2019)

Merkmal	Beschreibung
Datum	Mai 2019
Art	Datenleck
Kryptografie	Als sichere geltende Passworthashes konnten geknackt werden
CWE	Unbekannt

Im Mai 2019 wurde die australische Designplattform Canva Opfer eines großangelegten Datenlecks. Dabei wurden Daten von rund 139 Millionen Nutzern kompromittiert. Die gestohlenen Informationen umfassten vollständige Namen, Benutzernamen, E-Mail-Adressen und weitere persönliche Details. Obwohl die Passwörter der Nutzer mit dem als sicher geltenden bcrypt-Verfahren gehasht waren, konnten im Januar 2020 etwa 4 Millionen Passwörter entschlüsselt und online geteilt werden. Wie genau die Angreifer bcrypt knacken konnten, ist nicht bekannt. [42, 43]

Der Angreifer GnosticPlayers nutzte eine sogenannte Credential-Stuffing-Attacke, um Zugang zu den Datenbanken von Canva zu erhalten. Dabei wurden gestohlene Zugangsdaten aus früheren Sicherheitsvorfällen verwendet, um automatisiert Anmeldungen bei verschiedenen Diensten zu testen. Ein erfolgreicher Angriff auf die GitHub-Repositorys der Entwickler ermöglichte es den Angreifern, Zugriffsschlüssel zu erhalten und die Datenbank zu kompromittieren. [42]

Canva bemerkte den Angriff in Echtzeit und verhinderte, dass noch mehr Daten gestohlen wurden. Das Unternehmen informierte die betroffenen Nutzer und forderte sie auf, ihre Passwörter zu ändern. Es kam jedoch zu Kritik an der anfänglichen Kommunikation des Vorfalls, da die Benachrichtigungen zunächst als „Marketingsprech“ empfunden

wurden. Später wurde eine klarere Mitteilung versandt und Nutzer zur Änderung des Passworts aufgefordert. [42, 43]

4.3.3. SV03 – Capital One (2019)

Tab. 4.7: Eckdaten des Capital One Datenlecks (2019)

Merkmal	Beschreibung
Datum	Juli 2019
Art	Datenleck
Kryptografie	Trotz Verschlüsselung konnten Daten entschlüsselt werden
CWE	*CWE-918

Der amerikanische Finanzdienstleister Capital One war im Juli 2019 von einem schwerwiegenden Sicherheitsvorfall betroffen, bei dem die persönlichen Daten von etwa 100 Millionen US-Bürgern und 6 Millionen Kanadiern kompromittiert wurden. Unter den Daten befanden sich unter anderem Namen, Adressen, Telefonnummern, Geburtsdaten, Informationen zu Einkommen und einige sensible Kreditkartendaten. [44, 45]

Der Angriff wurde durch eine ehemalige Software-Ingenieurin namens Paige Thompson von Amazon Web Services (AWS) durchgeführt, die eine Fehlkonfiguration einer Web Application Firewall (WAF) ausnutzte, um unautorisierten Zugriff auf sensible Daten zu erlangen und diese zwischen dem 22. und 23. März 2019 von Servern von Capital One zu exfiltrieren. [44, 46] Capital One wurde am 17. Juli 2019 über die Sicherheitslücke informiert, als ein externer Sicherheitsforscher sich bei dem Unternehmen meldete. Mit der Kenntnisnahme der Meldung wurde sofort eine interne Untersuchung veranlasst und der Sicherheitsvorfall zwei Tage später entdeckt. Thompson konnte kurze Zeit später von den Behörden gefasst werden. Trotz standardmäßigen Hashings von Passwörtern konnten diese zurückgerechnet werden. Es gab keine verlässlichen Hinweise darauf, dass die gestohlenen Daten für betrügerische Aktivitäten genutzt oder verteilt wurden. [44, 45]

In Reaktion auf den Vorfall implementierte Capital One umgehend Maßnahmen zur Behebung der Sicherheitslücken und arbeitete eng mit den Strafverfolgungsbehörden

zusammen. Betroffene Kunden wurden per Post informiert, insbesondere die, deren Sozialversicherungsnummern oder Bankverbindungsdaten kompromittiert wurden. Darüber hinaus hat das Unternehmen bedeutende Investitionen in die Verbesserung seiner Sicherheitsarchitektur angekündigt und erklärte, dass fortschrittliche Betrugserkennungssysteme in Betrieb sind, um zukünftige Vorfälle zu verhindern. [44, 45]

4.3.4. SV04 – BigBasket (2020)

Tab. 4.8: Eckdaten des BigBasket Datenlecks (2020)

Merkmal	**Beschreibung**
Datum	Oktober 2020
Art	Datenleck
Kryptografie	Schwache Hashfunktionen für Passwörter
CWE	*CWE-328

Im Oktober 2020 wurde der indische Online-Lebensmittelhändler BigBasket Opfer eines massiven Datenlecks. Bei dem Vorfall wurden die persönlichen Daten von etwa 20 Millionen Nutzern gestohlen, darunter E-Mail-Adressen, Telefonnummern und physische Adressen. [47, 48]

Der Angriff wurde von der Cybersecurity-Firma Cyble entdeckt, die BigBasket Ende Oktober über das Datenleck informierte. Wie die Angreifer Zugriff auf die Datenbank erhielten, ist nicht geklärt. Die gestohlenen Daten umfassten 15 Gigabyte und wurden auf einem Cyber-Crime-Markplatz im Dark Web für über 40.000 US-Dollar zum Verkauf angeboten. [48] Ein halbes Jahr später, im April 2021, veröffentlichte ein Nutzer namens ShinyHunters die Datenbank mit freiem Zugang. Bereits kurze Zeit nach der Veröffentlichung tauchten Beiträge von anderen Usern im Forum auf, die eine erfolgreiche Entschlüsselung der gehashten Passwörter verkündeten und diese anschließend zum Verkauf anboten. [49]

BigBasket bestritt, dass es sich um einen neuen Sicherheitsvorfall handelte und verwies auf das ursprüngliche Datenleck von Oktober 2020. Das Unternehmen gab an, als Reaktion auf das Datenleck seine Sicherheitsrichtlinien verschärft und keine gehashten

Passwörter mehr in seiner Datenbank gespeichert zu haben. Stattdessen setzte man auf ein sichereres Zwei-Faktor-Authentisierungssystem. [49]

4.3.5. SV05 – CAM4 Data Breach (2020)

Tab. 4.9: Eckdaten des CAM4 Datenlecks (2020)

Merkmal	Beschreibung
Datum	März 2020
Art	Datenleck
Kryptografie	Unverschlüsselte Datenbanken
CWE	Unbekannt

CAM4, eine Plattform für Erwachsenenunterhaltung, sah sich im Jahr 2020 mit einem schwerwiegenden Datenleck konfrontiert. Dabei wurden fast 10,88 Milliarden Datensätze kompromittiert. Das Leck umfasste vollständige Namen, E-Mail-Adressen, IP-Adressen, Zahlungsinformationen, Chatprotokolle und Benutzerkommunikation von Nutzern aus der ganzen Welt, besonders viele davon aus den Brasilien, Italien und den Vereinigten Staaten von Amerika. [50, 51, 52, 53]

Das Datenleck wurde durch das SafetyDetectives CyberSecurity Team [52] entdeckt, als diese eine kritische Sicherheitslücke in einer Elasticsearch-Datenbank des Unternehmens fanden. Elasticsearch ist eine verteilte Such- und Analyse-Engine, die als skalierbarer Datenspeicher sowie als Vektordatenbank fungiert. Sie ermöglicht die Speicherung von Daten, schnelle Suchabfragen, präzise Relevanzbewertungen und umfangreiche Analysen, die flexibel skalierbar sind. [54] Aufgrund einer Fehlkonfiguration wurde das Speichern und Verarbeiten sensibler Benutzerdaten ohne ausreichenden Schutz möglich. Außerdem sei die Datenbank wegen fehlenden Passwortschutzes öffentlich zugänglich gewesen. [50]

Nach Bekanntwerden des Vorfalls handelte CAM4 schnell und nahm den betroffenen Server innerhalb einer halben Stunde offline. [51] Die fehlende Verschlüsselung und das Fehlen von Zwei-Faktor-Authentifizierungen waren kritische Versäumnisse, die zu dieser Sicherheitslücke führten. Es wurde angenommen, dass keine der exponierten Daten

von Dritten abgerufen wurden, deshalb gab es neben der Rufschädigung keine weiteren Folgen für CAM4. [50]

4.3.6. SV06 – SolarWinds (Sunburst) (2020)

Tab. 4.10: Eckdaten des SolarWinds-Angriffs (2020)

Merkmal	**Beschreibung**
Datum	September 2019 (Eindringen) / Dezember 2020 (Angriff)
Art	Supply-Chain-Angriff, Trojaner
Kryptografie	Umgehung der Softwaresignatur für Platzierung von Schadcode
CWE	*CWE-288, *CWE-506

Im Dezember 2020 wurde ein massiver Cyberangriff auf die Orion Plattform von SolarWinds bekannt, der als einer der größten Sicherheitsvorfälle in den USA gilt. Eine mutmaßlich staatlich gesponserte Hackergruppe nutzte eine Supply-Chain-Attacke, bei der Schadcode in Software-Updates des Orion-Systems eingeschleust wurde. Dieser Angriff kompromittierte rund 18.000 Netzwerke von Unternehmen, Regierungsbehörden und Institutionen weltweit. [55, 56]

Die Angreifer infiltrierten die Entwicklungs- und Lieferkette von SolarWinds, indem sie gestohlene Anmeldedaten nutzten und schädlichen Code in das Build-System der Software einfügten (CVE-2020-10148). Der kompromittierte Code wurde dann automatisch von Solar Winds Build-System mit offiziellen digitalen Signaturen versehen, was eine unentdeckte Verteilung des Updates ermöglichte. Nach der Installation konnten die Angreifer über sogenannte Command-and-Control-Server auf Kundennetzwerke zugreifen, Daten stehlen und weitere Malware verbreiten. [55]

Zu den betroffenen Organisationen gehörten das US-Finanzministerium, das Pentagon und führende Technologieunternehmen wie Microsoft und Intel. SolarWinds reagierte mit der Entfernung der schädlichen Updates, der Einführung eines Kill-Switches und der Veröffentlichung von Hotfixes, um Schwachstellen zu beheben. Dennoch verursachte der Angriff erhebliche Schäden, darunter ein Vertrauensverlust bei Kunden, finanzielle Einbußen und Klagen gegen das Unternehmen. [55] SolarWinds hatte einen Schaden

von mindestens 18 Millionen US-Dollar im ersten Quartal 2021, während betroffene Unternehmen und Behörden insgesamt bis zu 100 Milliarden US-Dollar für Schadensbegrenzung und Sicherheitsverbesserungen aufwenden mussten. Versicherungen deckten zwar rund 90 Millionen US-Dollar der Kosten, doch die langfristigen finanziellen Folgen umfassten regulatorische Verfahren, Rechtskosten und verstärkte Investitionen in Cybersicherheitsmaßnahmen. [57]

4.3.7. SV07 – Brenntag (2021)

Tab. 4.11: Eckdaten des Ransomwareangriffs auf Brenntag (2021)

Merkmal	**Beschreibung**
Datum	Mai 2021
Art	Ransomware
Kryptografie	Fehlende Verschlüsselung sensibler Informationen
CWE	unbekannt

Die nordamerikanische Einheit des deutschen Chemiedistributors Brenntag wurde Anfang Mai 2021 das Ziel eines Ransomwareangriffs der Gruppe DarkSide. Bei dem Angriff wurden sowohl Daten gestohlen als auch Geräte verschlüsselt. Insgesamt wurden etwa 150 GB an Daten, darunter Geburtsdaten, Führerscheinnummern, medizinische Aufzeichnungen und Sozialversicherungsnummern. Die Angreifer forderten zunächst ein Lösegeld von 7,5 Millionen US-Dollar. Brenntag konnte die Summe durch Verhandeln auf 4,4 Millionen Dollar reduzieren und zahlte dieses Lösegeld am Ende auch an die Angreifer. [58, 59]

Verantwortlich für den Angriff war die russische Ransomware-as-a-Service (RaaS)-Gruppe DarkSide. Die Gruppe nutzte gestohlene Anmeldedaten, um sich Zugriff auf das Brenntag-Netzwerk zu verschaffen. Im Anschluss veröffentlichten die Angreifer Beweise für den Datendiebstahl auf einer privaten Datenleaks-Seite, um ihre Forderungen zu untermauern. Nach der Entdeckung des Sicherheitsvorfalls trennte Brenntag die betroffenen Systeme sofort vom Netzwerk, um die Bedrohung einzudämmen. Das Unternehmen nahm die Dienste von Drittanbieterexperten für Cybersicherheit und Forensik in Anspruch und benachrichtigte die Strafverfolgungsbehörden. [58]

4.3.8. SV08 – Colonial Pipeline (2021)

Tab. 4.12: Eckdaten des Ransomwareangriffs auf Colonial Pipeline (2021)

Merkmal	Beschreibung
Datum	Mai 2021
Art	Ransomware
Kryptografie	Verschlüsselung durch Ransomware
CWE	Unbekannt

Im April 2021 wurde die US-Firma Colonial Pipeline Company von einem massiven Ransomware-Angriff der Gruppe DarkSide getroffen, der zur vorübergehenden Stilllegung des größten Kraftstoffpipelinesystems der USA führte. Der Angriff hatte erhebliche Auswirkungen auf die Treibstoffversorgung an der Ostküste der USA, da der Betrieb vorübergehend unterbrochen wurde, was zu einer angespannten Marktsituation führte. [60, 61]

Der Angriff erfolgte, nachdem die Angreifer Zugang zum Unternehmensnetzwerk erlangt hatten. Dies geschah durch gestohlene Zugangsdaten zu einem VPN-Account. Durch den Zugriff konnten die Hacker Geräte verschlüsseln und rund 150 GB unverschlüsselte Daten stehlen. Die Angreifer forderten ein Lösegeld von 4,4 Millionen USD, das schließlich von Colonial Pipeline bezahlt wurde. [60, 61]

Als Reaktion auf den Angriff schaltete Colonial Pipeline proaktiv bestimmte Systeme ab, um die Bedrohung einzudämmen und verhinderte so eine weitere Ausbreitung der Schadsoftware. Das Unternehmen arbeitete eng mit der US-Regierung, insbesondere mit dem Energieministerium, zusammen, um die Pipeline in einem schrittweisen Prozess wieder in Betrieb zu nehmen. Zudem engagierte Colonial Pipeline eine Sicherheitsfirma zur Unterstützung bei der Untersuchung und Aufklärung des Vorfalls. [61] Die Lehren aus dem Vorfall betonen die Notwendigkeit verstärkter Sicherheitsmaßnahmen, einschließlich der Implementierung von Multi-Faktor-Authentifizierung, um zukünftige Angriffe besser abwehren zu können. [60, 61]

4.3.9. SV09 – Microsoft Exchange Exploit (2021)

Tab. 4.13: Eckdaten des Microsoft Exchange Exploits (2021)

Merkmal	Beschreibung
Datum	Januar 2021
Art	Zero-Day-Exploit
Kryptografie	Server-Side Request Forgery (SSRF), CVE-2021-26855
CWE	*CWE-918[7]

Im Januar 2021 wurde ein schwerwiegender Cyberangriff auf Microsoft Exchange Server bekannt, bei dem die chinesische Hackergruppe HAFNIUM eine Kette von vier Zero-Day-Schwachstellen ausnutzte, um Tausende Organisationen weltweit zu kompromittieren. Dieser Vorfall betraf insbesondere Unternehmen, Forschungseinrichtungen und NGOs, die lokal gehostete Exchange-Server betrieben, und führte zu umfangreichem Datenverlust sowie einer erheblichen Erhöhung der Sicherheitsrisiken durch installierte Hintertüren für zukünftige Angriffe. [62, 63]

HAFNIUM nutzte eine Kombination aus Schwachstellen, darunter ein Server-Side Request Forgery (CVE-2021-26855), das Angreifern erlaubte, sich als Server zu authentifizieren, sowie eine unsichere Deserialisierung (CVE-2021-26857), um beliebigen Code als Systembenutzer auszuführen. Zusätzliche Schwachstellen ermöglichten das Schreiben von Dateien an beliebige Speicherorte (CVE-2021-26858 und CVE-2021-27065). Die Hacker setzten sogenannte Web-Shells ein, um Daten zu exfiltrieren und weitere Kompromittierungen zu ermöglichen. Ursprünglich zielte HAFNIUM auf spezifische Organisationen ab, weitete die Angriffe jedoch vor der Veröffentlichung von Sicherheitsupdates drastisch aus, um so viele Server wie möglich zu infizieren. [64, 63]

Microsoft reagierte am 2. März 2021 mit außerplanmäßigen Updates und veröffentlichte zusätzliche Tools zur Schadensbegrenzung. Dennoch blieben viele Systeme ungeschützt, da die Angriffe zu diesem Zeitpunkt bereits einen Großteil der verwundbaren Server kompromittiert hatten. Der Vorfall verdeutlicht die Bedeutung von schneller Patch-Verteilung und proaktivem Sicherheitsmanagement. Organisationen wurden dazu an-

[7] https://cwe.mitre.org/data/definitions/918.html

gehalten, ihre Systeme auf Indikatoren von Kompromittierungen zu überprüfen und Sicherheitsmaßnahmen zu verstärken, um zukünftige Angriffe zu verhindern. [62, 63]

4.3.10. SV10 – T-Mobile (US) Hack (2021)

Tab. 4.14: Eckdaten des T-Mobile Datenlecks (2021)

Merkmal	Beschreibung
Datum	August 2021
Art	Datenleck
Kryptografie	Fehlende Verschlüsselung persönlicher Daten
CWE	Unbekannt

Im August 2021 wurde ein schwerwiegender IT-Sicherheitsvorfall bei T-Mobile (US) bekannt, bei dem über 100 Millionen Kundendaten kompromittiert wurden. Betroffen waren die Daten von gegenwärtigen und ehemalige Kunden sowie potenzielle Neukunden, wie Namen, Adressen, Sozialversicherungsnummern, Geburtsdaten und Telefonnummern. Der Angriff führte zu erheblichen Bedenken hinsichtlich der Datensicherheit der betroffenen Personen und der Verpflichtungen von T-Mobile zum Schutz privater Daten. [65, 66]

Der Vorfall wurde bekannt, als Hacker in einem Cybercrime-Forum Daten zum Verkauf anboten. Die Daten stammten von T-Mobile-Servern und umfassten wichtige persönliche Informationen, die auf dem Schwarzmarkt einen hohen Wert darstellen. Die Angreifer nutzten wahrscheinlich Schwachstellen in den T-Mobile-Systemen aus, obwohl genaue Details über die Methoden entweder nicht veröffentlicht oder unklar geblieben sind. Der Zugang wurde vermutlich durch einen komplexen Angriff erlangt, der den Schutz der T-Mobile-Infrastruktur überwunden hatte. [65, 66]

Nach dem Angriff reagierte T-Mobile mit umfassenden Untersuchungen und nahm externe Cybersecurity-Experten zur Unterstützung hinzu. Der Zugangspunkt der Angreifer wurde identifiziert und geschlossen, und T-Mobile begann mit dem Prozess der technischen Prüfung ihrer Systeme, um das Ausmaß der Datenverletzung zu verstehen. [65, 66] Im Zuge der Nachwirkungen bot T-Mobile den betroffenen Kunden zwei Jahre kostenlosen Identitätsschutz an und ergriff Maßnahmen, um SIM-Swapping-Angriffe zu ver-

hindern, indem sie Kunden empfahlen, ihre PINs und Passwörter zu ändern. T-Mobile wurde auch von der FCC überwacht, die die Einhaltung ihrer regulatorischen Verpflichtungen sicherstellen wollte. [67]

4.3.11. SV11 – LastPass (2022)

Tab. 4.15: Eckdaten des LastPass-Hacks (2022)

Merkmal	Beschreibung
Datum	August 2022 (Erster Vorfall) / Oktober 2022 (Zweiter Vorfall)
Art	Datenleck, Social Engineering
Kryptografie	Mitarbeiter gehackt
CWE	Unbekannt

Im August und Oktober 2022 erlitt LastPass zwei schwere Datenlecks, die das Unternehmen und besonders seine Kunden stark betrafen. Erste Berichte über einen Sicherheitsvorfall kamen im August, als LastPass bekannt gab, dass ein unbefugter Dritter Zugriff auf den Quellcode und proprietäre technische Informationen der Firma erlangt hatte, was zu einer zweiten, schwerwiegenderen Verletzung im November führte. Letztlich wurden Teile der verschlüsselten Passworttresore sowie persönliche Informationen der Nutzer gestohlen, die ein hohes Risiko für Phishing-Angriffe darstellten. [68]

Der Angriff entwickelte sich in mehreren Phasen. Im ersten Vorfall im August 2022 wurden sensible Daten durch den Einsatz eines kompromittierten Entwicklerkontos erlangt, jedoch wurde zunächst fälschlicherweise davon ausgegangen, dass keine Kundendaten gefährdet seien. In der Folge wurde ein DevOps-Ingenieur gezielt anvisiert, dessen privater Computer über ein verwundbares drittes Mediensoftwarepaket gehackt wurde, was dem Angreifer ermöglichte, Keylogger-Malware zu installieren. Diese Malware erlaubte es dem Angreifer, das Master-Passwort des Ingenieurs zu erfassen, nachdem dieser sich mit Multi-Faktor-Authentifizierung eingeloggt hatte, und somit Zugriff auf den Unternehmensvault von LastPass zu erlangen. [69, 70]

Die Reaktion von LastPass auf die Vorfälle war zunächst von Intransparenz geprägt. Obwohl das Unternehmen die Sicherheitsvorfälle mit einem Cyber-Sicherheitsunternehmen

untersuchte, wurden wichtige Aspekte des Angriffs nicht ausreichend adressiert. Es wurde eine Erklärung veröffentlicht, dass die Kundendaten, insbesondere die Passwörter, sicher seien, da das Unternehmen keine Informationen zum Master-Passwort speichere. Diese Behauptung wurde jedoch von einer Klage in Frage gestellt, die vorbrachte, dass LastPass versuche, die Verantwortung für die negativen Folgen der Datenverletzung von sich zu schieben. [71] Nach den Vorfällen riet LastPass seinen Nutzern, alle gespeicherten Passwörter zu ändern, was trotz der Behauptung des Unternehmens nicht die bereits gestohlenen Daten schützen konnte. [70]

4.3.12. SV12 – Uber (2022)

Tab. 4.16: Eckdaten des Uber Hacks (2022)

Merkmal	**Beschreibung**
Datum	September 2022
Art	Social Engineering
Kryptografie	Faktor Mensch und fehlende Multi-Faktor-Authentifizierung (MFA)
CWE	Unbekannt

Am 15. September 2022 wurde Uber Ziel eines schwerwiegenden Cyberangriffs, der das Unternehmen und seine internen Systeme stark beeinträchtigte. Ein Hacker, der als 18-jähriger identifiziert wurde, gab an, Zugang zu vertraulichen Informationen erhalten zu haben, einschließlich interner Systeme und Sicherheitsberichte. Uber stellte fest, dass die Systeme, insbesondere der Zugriff auf kritische Dienste wie Slack und die AWS-Cloud, erheblich kompromittiert wurden. Während das Unternehmen zunächst versicherte, dass keine sensiblen Benutzerdaten, wie z.B. Fahrtenhistorien, betroffen seien, wurden durch das Datenleck dennoch Daten wie interne Slack-Nachrichten und Berichte zu Schwachstellen entwendet. [72, 73]

Der Angriff erfolgte in mehreren Phasen, beginnend mit dem ersten Zugang zu Ubers VPN, der wahrscheinlich durch den Kauf von Zugangsdaten eines Uber-Vertragspartners im Dark Web und der Infektion von dessen Gerät mit Malware ermöglicht wurde. Diese Zugangsdaten erlaubten dem Hacker, sich in das interne Netzwerk von Uber einzuloggen

und auf eine Vielzahl von Systemen zuzugreifen, darunter Sicherheitssoftware, Google Workspace, AWS-Konten und das VMware vSphere-System. [74, 73]

Uber hat sofort auf den Sicherheitsvorfall reagiert, indem es die betroffenen internen Dienste und Werkzeuge vorübergehend stilllegte. Das Unternehmen informierte die Strafverfolgungsbehörden und begann, kompromittierte Konten zu identifizieren und zu blockieren. In ihren Updates betonte die Unternehmensführung, dass alle wichtigen Dienste weiterhin funktionierten und dass zwischenzeitlich keine weiteren sicherheitsrelevanten Vorfälle festgestellt wurden. [72, 73]

4.3.13. SV13 – MGM Resorts (2023)

Tab. 4.17: Eckdaten des Ransomwareangriffs auf MGM Resorts (2023)

Merkmal	**Beschreibung**
Datum	September 2023
Art	Ransomware
Kryptografie	Mangelhafte Zugriffskontrollen
CWE	Unbekannt

Am 11. September 2023 wurde die Hotel- und Casino-Kette MGM Resorts Opfer eines gravierenden Cyberangriffs, der die Computer- und Buchungssysteme des Unternehmens lahmlegte. Mehrere Hotels und Casinos in Las Vegas waren von den Auswirkungen eines Ransomware-Angriffs betroffen, wodurch Gäste Schwierigkeiten hatten, ihre Zimmer zu betreten und andere Dienstleistungen in Anspruch zu nehmen. Der Systemausfall hielt mehrere Tage an, was zu langen Warteschlangen und improvisierten manuellen Abläufen führte, um den Betrieb irgendwie aufrechtzuerhalten. [75]

Der Angriff wurde möglicherweise durch Vishing ermöglicht, bei der sich ein Angreifer als Mitarbeiter ausgab und sensible Informationen erlangte, um Zugang zu den Systemen zu erhalten. Vishing ist besonders hinterhältig, da man sich dabei das Vertrauen von Menschen zunutze macht. Die Angreifer verschlüsselten die Systeme von MGM Resorts und verlangten ein Lösegeld von 30 Millionen US-Dollar. [75, 76, 77]

Als Reaktion auf den Vorfall fuhr MGM vorsorglich einige ihrer Systeme herunter, um die Auswirkungen zu begrenzen und um die Ursachen des Sicherheitsvorfalls zu untersuchen. Die betroffenen Hotels blieben für mehrere Tage offline, und erst am 20. September 2023 gab MGM bekannt, dass die Systeme „wieder normal funktionieren“, obwohl einige Probleme weiterhin bestehen blieben. [75, 76]

4.3.14. SV14 – Microsoft Exchange (2023)

Tab. 4.18: Eckdaten des Angriffs auf Microsoft Exchange (2023)

Merkmal	**Beschreibung**
Datum	Juli 2023
Art	Zero-Day-Exploit
Kryptografie	Zugang durch gestohlenen alten Signaturschlüssel
CWE	Unbekannt

Am 11. Juli 2023 gab Microsoft [78] bekannt, dass ein Cyberangriff der in China ansässigen Gruppe Storm-0558 auf seine Systeme entschärft werden konnte. Die Gruppe hatte seit dem 15. Mai 2023 mithilfe eines gestohlenen *Microsoft Account (MSA) consumer signing key* Zugang zu den E-Mailkonten von ungefähr 25 Regierungsbehörden und damit in Verbindung stehenden Einzelpersonen erhalten. Durch den Signaturschlüssel war es den Angreifern möglich, Authentifizierungstoken zu fälschen und so Zugriff auf die Postfächer in Exchange Online über *Outlook Web Access (OWA)* und *outlook.com* zu erlangen.

Der entwendete Schlüssel war nach Microsofts Angaben auf ein fehlerhaftes Absturzabbild (engl. crash dump) eines Anmeldesystems für Verbraucher (engl. consumer signing system) nach einem Absturz im April 2021 zurückzuführen. Der Signaturschlüssel war aufgrund einer Wettlaufsituation (engl. race condition) fälschlicherweise im Abbild gespeichert worden, welches nach einiger Zeit aus dem isolierten Produktionsnetzwerk in ein mit dem Internet verbundenes Debugging-Netzwerk überführt wurde. Die Systeme erkannten zu keinem Zeitpunkt, dass sich Schlüsselmaterial im Umlauf befand. Es wird vermutet, dass ein kompromittierter Unternehmensaccount eines Microsoft-Ingenieurs schließlich dazu führte, dass Storm-0558 Zugriff auf den Endkundenschlüssel erhalten konnte. [79]

Aufgrund einer nicht aktualisierten API zur kryptografischen Überprüfung von Signaturen wurde keine automatische Validierung des Schlüsselbereichs (engl. key scope) durchgeführt. Die Entwickler nahmen fälschlicherweise an, dass eine umfangreiche Validierung bereits über die API erfolgte und implementierten daher nicht die erforderliche Validierung des Ausstellers und des Gültigkeitsbereichs. Als Ergebnis akzeptierte das Mailsystem Anfragen für Unternehmens-E-Mails, die mit einem Sicherheitstoken signiert waren, das mit dem Endkundenschlüssel verknüpft war. [79]

4.3.15. SV15 – Okta (2023)

Tab. 4.19: Eckdaten des Okta Datenlecks (2023)

Merkmal	**Beschreibung**
Datum	Oktober 2023
Art	Datenleck
Kryptografie	Gestohlene Cookies aus Sitzungsdateien ermöglichten Zugriff auf das Support-Portal
CWE	Unbekannt

Zwischen dem 28. September und dem 17. Oktober 2023 erhielt ein Angreifer unautorisierten Zugriff auf das Kundensupport-System des US-Unternehmens Okta. Dies betraf Dateien von 134 Okta-Kunden, weniger als 1 % der gesamten Kundenbasis. Einige dieser Dateien waren HAR-Dateien (HTTP-Archive), die Session-Tokens enthielten. Diese wurden für Session-Hijacking-Angriffe genutzt, von denen fünf Kunden betroffen waren. [80]

Der Angreifer nutzte ein Service-Konto, das im Support-System gespeichert war und Berechtigungen zum Anzeigen und Aktualisieren von Support-Fällen hatte. Die Zugangsdaten dieses Kontos waren in einem persönlichen Google-Konto eines Okta-Mitarbeiters gespeichert, das über ein kompromittiertes Gerät oder Konto des Mitarbeiters offengelegt wurde. [80]

Am 13. Oktober 2023 übermittelte BeyondTrust Okta eine verdächtige IP-Adresse des Angreifers. Dadurch konnte Okta zusätzliche Datei-Zugriffsereignisse identifizieren, die mit dem kompromittierten Konto verknüpft waren. Der Vorfall führte dazu, dass der

Angreifer über 14 Tage hinweg Dateien aus dem Support-System abrufen konnte, bevor der Zugriff blockiert wurde. [80, 81]

4.3.16. SV16 – Südwestfalen-IT (2023)

Tab. 4.20: Eckdaten des Ransomwareangriffs auf Südwestfalen-IT (2023)

Merkmal	Beschreibung
Datum	Oktober 2023
Art	Ransomware
Kryptografie	Verschlüsselung von Systemen und Daten
CWE	*CWE-288

Der kommunale deutsche IT-Dienstleister Südwestfalen-IT (SIT) [82] wurde am 29. Oktober 2023 Opfer eines Ransomwareangriffs der Hackergruppe Akira. Der Angriff war auf die Domäne **intra.lan** gerichtet und führte zur Verschlüsselung der darüber zugreifbaren Dateien. Dies hatte einen Totalausfall der IT-Systeme von etwa 70 Kommunen im Sauer- und Siegerland zur Folge. Demnach waren alle Bürgerdienste in der Region offline. Mitarbeiter der Kommunalverwaltungen hatten keine Möglichkeit mehr, E-Mails zu versenden oder von zuhause aus zu arbeiten. [83]

Das von SIT beauftragte Cybersicherheitsunternehmen r-tec vermutet, dass durch einen vorangegangenen Brute-Force-Angriff Zugangsdaten von mindestens drei Benutzerkonten des verwendeten VPN-Dienstes erbeutet wurden. Der Angriff sei durch einen Zero-Day-Exploit (CVE-2023-20269) des von SIT verwendeten VPN-Dienstes Cisco Adaptive Security Appliance (ASA) und fehlender MFA möglich gewesen. Durch den Exploit könnten gültige Benutzernamen und Passwortkombinationen ermittelt worden sein, mit denen sich im zweiten Schritt eine clientlose SSL-VPN-Verbindung zum internen Netzwerk der Domäne intra.lan aufbauen ließ. [84]

In ihrer Analyse stellte r-tec außerdem fest, dass eine kritische Sicherheitslücke in der betroffenen Domäne intra.lan bestand. Das Passwort des Domänen-Administrators war seit 2014 zwar in verschlüsselter Form in einem Gruppenrichtlinienobjekt hinterlegt, konnte aber ohne weiteres mit einem von Microsoft bereitgestellten AES-Schlüssel entschlüsselt werden. Laut des Unternehmens wurden keine Anzeichen für Privilege Escalation und

Lateral Movement gefunden. Dabei handelt es sich um verschiedene Angriffstechniken, um tiefer in ein Netzwerk einzudringen und die Berechtigungen zu erweitern. Es lag nahe, dass die Angreifer sich über den Account intra.lan\Administrator die entsprechenden Berechtigungen gaben, ohne dabei aufzufallen. [84] Südwestfalen-IT konnte gegen Ende 2024, ein Jahr nach dem Vorfall, wieder in den Normalmodus wechseln und fast alle betroffenen Dienste wieder anbieten. [85]

4.3.17. SV17 – Change Healthcare (2024)

Tab. 4.21: Eckdaten des Ransomwareangriffs auf Change Healthcare (2024)

Merkmal	Beschreibung
Datum	Februar 2024
Art	Ransomware
Kryptografie	Verschlüsselung von Systemen und Daten
CWE	Unbekannt

Im Februar 2024 wurde Change Healthcare, ein großer US-Dienstleister für das Gesundheitswesen, Opfer eines Ransomware-Angriffs, der als eine der größten Datenschutzverletzungen in der Geschichte des US-Gesundheitswesens gilt. Dabei wurden die persönlichen und medizinischen Daten von mindestens 100 Millionen Menschen gestohlen. Zu den kompromittierten Daten gehörten medizinische Aufzeichnungen, Diagnosen, Versicherungs- und Finanzdaten sowie persönliche Details wie Namen und Adressen. [86, 87]

Der Angriff wurde von der russischsprachigen Ransomware-Gruppe ALPHV (auch bekannt als BlackCat) durchgeführt. Die Hacker drangen über ein gestohlenes Benutzerkonto ohne MFA in die Systeme ein. Anschließend nutzten sie Ransomware und drohten mit der Veröffentlichung der sensiblen Daten. Change Healthcare isolierte die Systeme, was zu weitreichenden Ausfällen im US-Gesundheitswesen führte, da viele Krankenhäuser und Praxen auf die Dienste des Unternehmens angewiesen sind. [86, 87]

Der Mutterkonzern, UnitedHealth, zahlte Anfang März ein Lösegeld von 22 Millionen Dollar, doch die Hackergruppe veröffentlichte später trotzdem Teile der Daten. Die gestohlenen Informationen führten zu massiven Störungen im Gesundheitswesen und lös-

ten eine Klagewelle aus, die auch zum Zeitpunkt der Veröffentlichung dieser Arbeit noch andauert. Es wurde festgestellt, dass grundlegende Sicherheitsmaßnahmen wie Multi-Faktor-Authentifizierung und die Segmentierung von IT-Systemen fehlten, was den Angriff erleichterte. Bis Oktober 2024 bestätigte UnitedHealth, dass der Datendiebstahl mehr als 100 Millionen Menschen betraf, wobei die endgültige Zahl der Betroffenen noch höher ausfallen könnte. [86, 87]

5. Evaluation

In diesem Kapitel werden die gefunden IT-Sicherheitsvorfälle systematisch analysiert und miteinander verglichen. Zunächst wird die verwendete Methodik beschrieben. Anschließend folgt die Analyse der Sicherheitsvorfälle. Hierfür werden zuerst Gemeinsamkeiten und Muster herausgestellt. Anschließend wird die Rolle der Kryptografie näher betrachtet.

5.1. Methodik

Für die Evaluation der IT-Sicherheitsvorfälle wurde die Methodik der **qualitativen Inhaltsanalyse** nach Mayring [88] angewendet. Bei einer qualitativen Inhaltsanalyse wird das vorliegende Material, welches z. B. Zeitungsartikel, Interviews oder Blogbeiträge umfasst, in einzelne Teile zerlegt und strukturiert aufgearbeitet, um die Forschungsfragen zu beantworten. Dabei steht die Bildung eines Kategorien- bzw. Codesystems im Mittelpunkt. [88, S. 60] Passende Textabschnitte oder Aussagen aus dem vorliegenden Material werden anschließend den Kategorien (engl. Codes) zugeordnet. In erster Linie stehen dabei **deduktive Kategorien** im Vordergrund. Deduktiv bedeutet, dass sich die Kategorien bereits im Vorfeld der Analyse als logische Schlussfolgerungen aus dem Material oder der Forschungsfrage ableiten lassen. Daneben verwendet man auch **induktive Kategorien**, die im Zuordnungsprozess aus dem Material heraus entstehen. Meist wird eine Mischform verwendet, wobei mit deduktiven Kategorien begonnen wird und induktive Kategorien im Laufe der Zuordnung ergänzt werden. [88]

Mayring [88] beschreibt drei verschiedene Analysetechniken, um das Material auszuwerten. Die **Zusammenfassung** hat zum Ziel, das Material so zu komprimieren, dass die Kerninhalte erhalten bleiben und nicht verfälscht werden. Für die **Explikation** wird zusätzliches Material hinzugezogen, um das Verständnis zu fördern und Lücken aufzufüllen. Schließlich kann die **Strukturierung** verwendet werden, welche darauf abzielt, bestimmte Aspekte des Materials herauszufiltern, einen Querschnitt durch das Material unter vorher festgelegten Ordnungskriterien zu erstellen oder das Material anhand bestimmter Kriterien zu bewerten. [88, S. 66]

An dieser Stelle ist anzumerken, dass die Menge der betrachteten Sicherheitsvorfälle eine bessere Eignung für eine quantitative Inhaltsanalyse suggerieren könnte. Eine quantitative Inhaltsanalyse legt den Fokus auf statistische Methoden zur Beantwortung der Forschungsfragen. [88, S. 17 f.] Da für diese Evaluation keine besonderen statistischen Werte erhoben werden sollten und die Stichprobengröße mit $n = 17$ ohnehin eher gering ausfällt, wurde eine quantitative Analyse nicht in Betracht gezogen. Außerdem lag der Fokus auf den qualitativen Aspekten der Fälle, die mit Mayrings Methoden im Folgenden herausgearbeitet werden.

5.1.1. Durchführung

Dieser Abschnitt widmet sich der Beschreibung der durchgeführten qualitativen Inhaltsanalyse. Das gewählte Material setzt sich zum Teil aus den Quellen zusammen, die für die Ausführungen der einzelnen Sicherheitsvorfälle verwendet wurden, und wurde an einigen Stellen durch weitere Literatur, bestehend aus wissenschaftliche Publikationen, vorhandenen Forensikberichten oder Internetquellen erweitert. Um den Rahmen des Materials zu beschränken, wurden maximal acht, aber mindestens drei Dokumente pro Fall betrachtet. Insgesamt wurden 88 Internet- und andere Informationsquellen analysiert, also durchschnittlich fünf pro Vorfall. Eine vollständige Quellenliste des betrachteten Materials ist in Anhang A.6 (siehe S. 145 ff.) zu finden.

Als technisches Hilfsmittel wurde MAXQDA 24[7] für die Analyse verwendet. Internetquellen wurden für die Verwendung im Programm mithilfe des Browser-Plugins *Web Collector for MAXQDA*[8] in ein einheitliches Textformat überführt, um die Codierung zu erleichtern. Anschließend wurden Aussagen der einzelnen Quellen den verschiedenen Kategorien zugeordnet (siehe Screenshot in Abb. 5.1).

Alle markierten Aussagen innerhalb einer Kategorie konnten im Programm als eigenständige Tabelle dargestellt werden, wodurch eine strukturierte Übersicht über die wesentlichen Inhalte entstand. Auf Basis dieser Tabellen wurden dann die Aussagen auf ihren Kerninhalt reduziert, sodass nur die wichtigsten Informationen erhalten blieben.

[7] https://www.maxqda.com/de/produkte/maxqda
[8] https://chromewebstore.google.com/detail/web-collector-for-maxqda/jhnochbooihpgjbgcjlpihaefoehlakd?pli=1

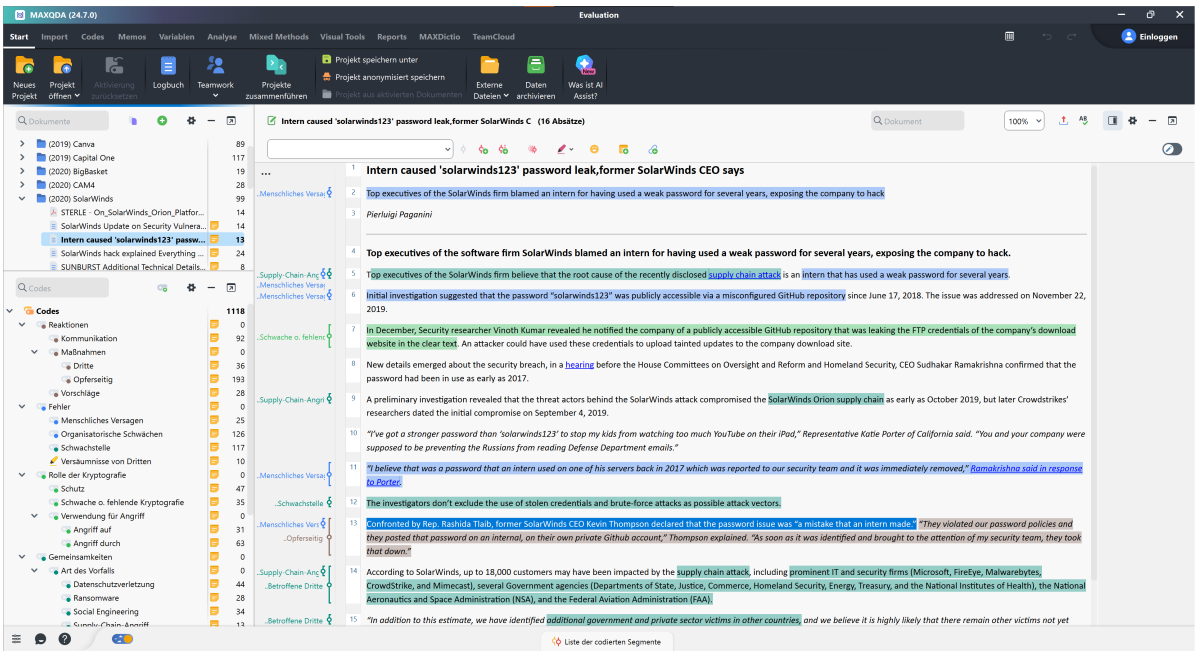


Abb. 5.1: Screenshot einer codierten Quelle in MAXQDA.

Basierend auf dieser komprimierten Darstellung wurden die einzelnen Fälle miteinander verglichen.

Das verwendete Codesystem ist in Anhang A.4 (siehe S. 87 ff.) zu finden. Die Kodierungen der einzelnen Aussagen und Textabschnitte befinden sich in Anhang A.5. Für eine verbesserte Lesbarkeit werden nachfolgend die in Tabelle 4.4 (siehe S. 28) dargestellten Kürzel für die Sicherheitsvorfälle verwendet.

5.2. Gemeinsamkeiten und Muster

In diesem Abschnitt werden Gemeinsamkeiten und Muster in den betrachteten IT-Sicherheitsvorfällen erörtert. Dabei sollen die folgenden Forschungsfragen beantwortet werden:

- **F1:** Welche Gemeinsamkeiten und Muster lassen sich in den betrachteten Sicherheitsvorfällen erkennen?
- **F2:** Inwieweit tragen menschliche oder organisatorische Faktoren zu Sicherheitsvorfällen bei?

5.2.1. Organisatorische und menschliche Faktoren

In diesem Abschnitt werden organisatorische und menschliche Faktoren vorgestellt. Tabelle 5.1 zeigt das Auftreten von Aussagen zur jeweiligen Kategorie (Spalte) an. Wenn in einer Zeile keine Kreuze zu sehen sind, dann gab es für diese Kategorie in einem Sicherheitsvorfall keine eindeutigen Aussagen für eine Zuordnung.

Tab. 5.1: Verteilung der Kategorien mit Informationen zu organisatorischen und menschlichen Faktoren

Kürzel	Menschliches Versagen	Organisatorische Schwächen
SV01		x
SV02		x
SV03	x	x
SV04		
SV05	x	x
SV06	x	x
SV07		x
SV08	x	x
SV09		x
SV10		x
SV11	x	x
SV12	x	x
SV13	x	x
SV14	x	x
SV15	x	x
SV16		x
SV17		x

5.2.1.11 Organisatorische Schwächen (Spalte 2)

Die analysierten Vorfälle machen deutlich, dass gravierende Schwächen in den organisatorischen Sicherheitsprozessen existieren. Dabei lassen sich mehrere Gemeinsamkeiten ausmachen, die in unterschiedlichen Ausprägungen bei den betroffenen Organisationen zu Kompromittierungen geführt haben. Für eine bessere Lesbarkeit werden diese in kleineren Textblöcken zusammengefasst.

Fehlende oder unzureichende Multi-Faktor-Authentifizierung
In vielen Fällen hätte eine aktivierte MFA den Angriff zumindest erschweren, wenn nicht gänzlich verhindern können. Mehrfach wird berichtet, dass Zugänge ausschließlich über die Kombination Benutzername und Passwort gesichert waren, sodass ein einziges kompromittiertes Passwort bereits zum Eindringen in das Netzwerk genügte (SV02, SV07, SV16, SV17). Die Einführung bzw. konsequente Nutzung von MFA galt deshalb in verschiedenen Fällen als zentrale, aber vernachlässigte Schutzmaßnahme.

Mangelhafte Patch- und Aktualisierungsprozesse
Ein weiterer Aspekt betrifft fehlende oder verspätete Sicherheitsupdates. In mindestens einem Fall blieben kritische Schwachstellen monatelang ungepatcht (SV09), während in einem anderen Umfeld eine bekannte VPN-Sicherheitslücke nicht rechtzeitig geschlossen wurde (SV16). Einmal erschwerten veraltete und nicht einheitliche Systemlandschaften die Umsetzung von Patch-Strategien, da zunächst Upgrades auf unterstützte Plattformen erforderlich waren (SV09).

Fehlendes oder unzureichendes Vorfalls- und Risikomanagement
Die Untersuchung zeigt, dass Unternehmen trotz wiederholter Sicherheitsvorfälle keine angemessenen Konsequenzen für die eigene IT-Sicherheitsstrategie zogen (SV01). Einmal fehlte ein detaillierter Notfallplan (SV02) oder es wurden nach einem ersten Angriff weiterhin kompromittierte Software-Updates verteilt (SV06).

Unzureichende Berechtigungsvergabe und -verwaltung
Mehrere Vorfälle verweisen auf übermäßige Zugriffsrechte einzelner Konten oder Systeme. So kam es etwa zu Fehlkonfigurationen, bei denen WAFs ungehinderten Zugriff auf AWS-Speicher ermöglichten, obwohl dies technisch nicht erforderlich gewesen wäre (SV03). Zudem blieb ein kompromittiertes VPN-Konto eines ausgeschiedenen Mitarbeiters aktiv (SV08), und in einem anderen Fall wurde ein lokaler Admin-Zugang mit Standard- oder viel zu schwachen Passwörtern geführt (SV10). Solche Versäumnisse begünstigen ein schnelles Lateral Movement im Netzwerk.

Schlechte interne Kommunikation und Personalmangel
Hohe Fluktuation und mangelnde Koordination zwischen IT-Abteilungen, CISOs und dem Vorstand (SV03) sowie fehlende Schulungen zum Schutz vor Vishing (SV13) unterstreichen generelle Defizite in der Sicherheitskultur. Hinzu kommt, dass Kompromittierungen zum Teil nicht oder nur unzureichend gemeldet wurden – selbst wenn einige technische Schutzlösungen die Vorfälle erkannt hatten (SV16).

Fehlende Netzwerksegmentierung und veraltete Systeme
Offen zugängliche SSH-Ports, ungesicherte Entwicklungsserver und unzureichend isolierte Netzwerke (SV10) erhöhen ebenso wie das Weiterbetreiben alter Exchange-Server (SV09) das Angriffsrisiko beträchtlich. Eine solide Netzwerksegmentierung und das kon-

sequente Austauschen oder Absichern veralteter Komponenten gelten allerdings als wesentliche Grundlage für ein effektives Sicherheitsmanagement.

Insgesamt zeigen die Sicherheitsvorfälle, dass organisatorische Defizite, beispielsweise in Form von fehlender MFA oder mangelhaften Sicherheitsprozessen, einen entscheidenden Beitrag zur erfolgreichen Kompromittierung von IT-Systemen leisten. Die Notwendigkeit, diese Schwachstellen gezielt zu adressieren, wird durch die wiederkehrenden Muster bei unterschiedlichen Vorfällen deutlich.

5.2.1.12 Menschliche Faktoren (Spalte 3)

In den untersuchten Fällen zeigt sich deutlich, dass nicht nur organisatorische und technische Defizite zu gravierenden Sicherheitslücken führen, sondern insbesondere menschliche Fehler und Unaufmerksamkeit. Dabei lassen sich verschiedene Muster erkennen, bei denen Fehlkonfigurationen, leichtsinniger Umgang mit Passwörtern sowie erfolgreiche Täuschungsmanöver durch Angreifer eine zentrale Rolle spielen.

Ein häufiger Aspekt ist die unsachgemäße Handhabung von Anmeldedaten oder sensiblen Informationen. So wurden beispielsweise Datensätze versehentlich in Protokolldateien geschrieben, weil ein Entwickler bei der Fehlersuche im Programmcode nicht auf die Speicherorte dieser Daten achtete (SV05). In einem anderen Fall (SV06) landete ein schwaches Passwort in einem öffentlich zugänglichen GitHub-Repository, das von einem Praktikanten betreut wurde, was zu einem ungehinderten Zugriff für die Angreifer führte. Ein weiterer Vorfall (SV08) zeigte, dass ein offengelegtes Passwort auf die Erpressung eines Ex-Mitarbeiters zurückzuführen sein könnte. Auch das unbedachte Verknüpfen eines Firmenlaptops mit einem privaten Google-Konto ermöglichte potenziell den Zugriff auf sensible Servicekonten, sobald das persönliche Konto oder Gerät kompromittiert wurde (SV15).

Social Engineering und zwischenmenschliche Manipulationen stellen eine weitere entscheidende Schwachstelle dar: Ein Supportmitarbeiter fiel beispielsweise auf die erfundene Geschichte eines Hackers rein und gab Zugangsinformationen preis, ohne dessen wahre Identität zu hinterfragen (SV13). Ebenso ist belegt, dass Angreifer wiederholt MFA-Anfragen an einen externen Mitarbeiter schickten, bis dieser die Anmeldung versehentlich oder aus Frust bestätigte und so ungewollt den Zugriff ermöglichte (SV12).

In einigen Fällen wurden zudem private oder geschäftliche Geräte zum Einfallstor. Ein Beispiel ist der kompromittierte Privatcomputer eines Software-Engineers, auf dem Keylogger-Software installiert wurde. Dadurch erhielten Angreifer das Master-Passwort zu einem Unternehmens-Passworttresor, obwohl der Mitarbeiter sich eigentlich per MFA geschützt hatte (SV11). Ein anderer Angreifer erlangte mutmaßlich einen Signaturschlüssel, indem er sich Zugang zum Laptop eines kürzlich eingestellten Mitarbeiters verschaffte (SV14). Insgesamt zeigen diese Fälle, dass der Mensch als Schwachstelle oder Angriffsziel weiterhin im Mittelpunkt steht – sei es durch versehentliches Offenlegen wichtiger Informationen oder durch bewusstes Ausnutzen vertrauensvoller Kommunikation. Eine entsprechende Sensibilisierung, Schulung und eine konsequente Durchsetzung von Sicherheitsrichtlinien sind daher essenzielle Bausteine einer ganzheitlichen IT-Sicherheitsstrategie.

5.3. Rolle und Wirksamkeit der Kryptografie

Im Folgenden soll untersucht werden, welche Rolle Kryptografie in den vorliegenden Sicherheitsvorfällen hatte. Dabei sollen sowohl die positiven Effekte kryptografischer Maßnahmen als auch deren Schwächen und Missbrauchspotenziale aufgezeigt werden. Als Forschungsfrage steht dabei im Vordergrund:

- **F3:** Welchen Einfluss hat Kryptografie in IT-Sicherheitsvorfällen?

Tabelle 5.2 zeigt die Verteilung der Kategorien in den Sicherheitsvorfällen in Bezug auf die Rolle der Kryptografie. Waren in der vorliegenden Literatur Aussagen zu den einzelnen Kategorien (Spalten) vorhanden, so wurde dies mit einem 'x' gekennzeichnet. Eine kurze Erklärung der einzelnen Kategorien ist in Anhang A.4. auf S. 89 zu finden.

Tab. 5.2: Verteilung der Kategorien zu der Rolle der Kryptografie in den Sicherheitsvorfällen

Kürzel	Schutz	Schwach/fehlt	Angriff auf	Angriff durch
SV01		x	x	
SV02	x		x	x
SV03	x	x	x	
SV04	x	x	x	
SV05	x			
SV06		x	x	x
SV07		x		x
SV08				x
SV09				x
SV10	x	x	x	x
SV11	x	x	x	
SV12	x	x		
SV13	x			x
SV14		x	x	x
SV15				x
SV16	x	x	x	x
SV17				x

5.3.1. Schutz durch Kryptografie (Spalte 2)

Innerhalb der untersuchten Sicherheitsvorfälle wird deutlich, dass Kryptografie in vielen Fällen eine schützende Rolle einnimmt und somit dazu beitragen kann, Schäden durch kompromittierte Systeme oder Daten zu reduzieren oder gänzlich abzuwenden. Im Folgenden werden verschiedene Beispiele zusammengeführt, die belegen, dass der Einsatz starker Verschlüsselungs- und Hash-Verfahren für Angreifer häufig eine deutliche Hürde darstellen konnte.

So wurden in einem Fall etwa 61 Millionen gestohlene Passwörter mithilfe des starken Algorithmus bcrypt gehasht, was bedeutet, dass potenzielle Angreifer beträchtlichen Zeitaufwand hätten investieren müssen, um diese Passwörter zu knacken (SV02). Zusätzlich waren OAuth-Token mit AES-128 verschlüsselt und die entsprechenden Schlüssel an einem separaten Ort hinterlegt, was einen direkten Zugriff weiter erschwerte (SV02). In einem anderen Fall stellte sich heraus, dass sowohl Daten-Verschlüsselung als auch Tokenisierung bereits standardmäßig genutzt wurden. Dank dieser Verfahren blieben sensible Sozialversicherungsnummern selbst nach der Kompromittierung geschützt (SV03). Auch die Tatsache, dass Passwörter zum Zeitpunkt des Angriffs in gehashter Form vorlagen, belegt grundsätzlich einen angemessenen Umgang mit sensiblen Daten (SV04, SV05).

Eine besonders umfassende Verschlüsselungsstrategie zeigte sich bei der Aufbewahrung sensibler Kundendaten in Passworttresoren. Diese Daten waren nur mithilfe eines einzigartigen Schlüssels entschlüsselbar, der wiederum aus dem Master-Passwort abgeleitet wurde – wobei das Master-Passwort selbst nicht gespeichert wurde. Darüber hinaus war die MFA-Datenbank ebenfalls verschlüsselt (SV11). Zwar konnten Angreifer in einem zugehörigen Fall verschlüsselte Notizen exportieren, die Zugriffs- und Entschlüsselungsschlüssel enthielten; auf die zum Entschlüsseln notwendigen Schlüssel für Notizen oder Clouddaten hatten sie jedoch keinen Zugriff. Die im Einsatz befindliche Verschlüsselung erfolgte dabei mit einem 256-Bit-AES-Verfahren (SV11). In ähnlicher Weise gelang es Angreifern in einem anderen Szenario, Passwort-Hash-Dumps zu erbeuten, ohne diese entschlüsseln zu können (SV13).

Interessant ist auch die Perspektive, dass selbst die Angreifer kryptografische Methoden verwenden, um ihre eigenen Aktivitäten zu schützen. In einem Fall gelang es nicht, die Ransomware zu entfernen, sodass die verschlüsselten Daten des Opfers nicht wiederher-

gestellt werden konnten. Dies verdeutlicht, dass Kryptografie nicht nur Verteidigerinnen und Verteidigern, sondern ebenso kriminellen Akteuren als effektives Mittel dient, um digitale Inhalte zu sichern und Zugriff zu kontrollieren (SV16).

Zusammenfassend zeigt sich, dass starke Hashing- und Verschlüsselungsverfahren – beispielsweise bcrypt, AES-128 oder AES-256 – einen hohen Schutz bieten können. Durch die bewusste Trennung von Schlüsseln und Daten sowie den Einsatz von Master-Passwörtern und MFA-Systemen lässt sich die Widerstandsfähigkeit gegenüber Angriffen deutlich erhöhen. Die beobachteten Vorfälle verdeutlichen jedoch auch, dass Angreifer zunehmend raffiniertes Vorgehen an den Tag legen und sich ebenfalls kryptografischer Mittel bedienen, um ihre Schadsoftware oder erbeutete Daten zu verschleiern und so den Zugriff durch Dritte zu verhindern.

5.3.2. Schwache oder fehlende Kryptografie (Spalte 3)

In einigen der untersuchten Vorfälle traten deutlich erkennbare Defizite im Umgang mit kryptografischen Verfahren und Mechanismen zutage. Dies führte nicht nur dazu, dass personenbezogene und anderweitig sensible Informationen für Angreifer vergleichsweise leicht zugänglich waren, sondern eröffnete auch vielfältige Möglichkeiten für die Kompromittierung von Systemen oder die Ausweitung bereits bestehender Zugriffsrechte.

Passwörter wurden in zwei Fällen zwar gehasht gespeichert, allerdings mit dem als unsicher geltenden Hashing-Algorithmus SHA-1, wodurch ein effektiver Schutz von Zugangsdaten und persönlichen Daten nicht gewährleistet war (SV01, SV04). Noch gravierender ist die mehrfach erwähnte fehlende oder nur unzureichende Verschlüsselung: Persönliche Daten lagen teilweise völlig unverschlüsselt vor (SV01), was auch in einem anderen Fall bestätigt wurde (SV07). Ebenso wurde in einem Kontext eine nicht näher benannte Verschlüsselungsmethode angewendet, die in der Praxis als ineffizient und ungeeignet galt (SV03).

Neben der unzureichenden oder schwachen Verschlüsselung lassen sich auch Fälle von fahrlässigem Umgang mit Zugangsdaten nachweisen. So befanden sich Zugangsdaten in Klartextform in einem öffentlich zugänglichen GitHub-Repository (SV06), was einem potenziellen Angreifer den direkten Zugriff auf relevante Konten ermöglichte. In einem

ähnlichen Szenario lagen Zugangsdaten für ein privilegiertes Konto im Klartext in einem PowerShell-Skript vor, wodurch Angreifer auf Zugriffstoken verschiedener Dienste zugreifen konnten (SV12). Ebenso wurde vermutet, dass gestohlene Daten, darunter PINs von Mobilfunkkunden, in einigen Fällen im Klartext vorlagen und somit ohne Aufwand abgegriffen werden konnten (SV10). Auch bei einem anderen Vorfall war nur ein Teil der Daten tatsächlich gehasht, während der Rest im Klartext verfügbar blieb. Hier zeigte sich zusätzlich, dass das betroffene Unternehmen versäumt hatte, die Iterationszahl für Hashverfahren bei älteren Nutzerkonten zu erhöhen, wodurch diese besonders gefährdet waren (SV11).

Ein weiterer wesentlicher Aspekt der Sicherheitslücken betrifft die Verwaltung von Berechtigungen und Schlüsseln. Einmal war der Hostname der Angriffsinfrastruktur in den RDP-SSL-Zertifikaten hinterlegt, sodass bösartige IP-Adressen, die sich als legitime Organisation ausgaben, mittels internetweiter Scandaten identifiziert werden konnten (SV06). Darüber hinaus hätte die Implementierung von MSA-Keys eigentlich nur in den jeweiligen Systemen funktionieren sollen. Ein Validierungsfehler im Code erlaubte es Angreifern jedoch, Authentifizierungs-Tokens zu fälschen (SV14). Erschwerend kam hinzu, dass in demselben Fall das Passwort eines Administratorkontos mehrere Jahre in entschlüsselbarer Form in einem Gruppenrichtlinienobjekt vorlag (SV14).

Interessanterweise sind auch auf der Seite von Angreifern verschiedene Schwachstellen zu erkennen: In einem Vorfall war die Verschlüsselung der Logfiles von Ransomware so schwach umgesetzt, dass wichtige Informationen für die Verteidigungsteams noch lesbar waren (SV14). Darüber hinaus gestaltete sich die Ransomware in ihrer Funktionsweise als nur minimal verschleiernd und ohne weiterführende Anti-Tamper- oder Anti-Debugging-Mechanismen, weshalb Sicherheitsanalysten ihr Verhalten relativ leicht untersuchen konnten (SV14).

Die Ergebnisse verdeutlichen, dass nicht nur unzureichende Schutzmaßnahmen aufseiten der Verteidigung, sondern auch Schwächen in den Angriffs-Tools selbst eine Rolle spielen können.

5.3.3. Angriff mithilfe von Kryptografie (Spalten 4 und 5)

Während Kryptografie in vielen Fällen einen wirksamen Schutz gegen Cyberangriffe darstellt, zeigt sich in den untersuchten Vorfällen auch, dass Angreifer gezielt kryptografische Verfahren missbrauchen oder vorhandene Schutzmechanismen umgehen, um sich Zugang zu sensiblen Informationen zu verschaffen. Die Analyse verdeutlicht zugleich, dass Kryptografie nicht nur als Abwehrinstrument eingesetzt wird, sondern auch selbst zum Ziel oder Werkzeug eines Angriffs werden kann. Im Folgenden wird zwischen **Angriffen auf Kryptografie** und **Angriffen durch Kryptografie** unterschieden.

5.3.3.13 Angriffe auf Kryptografie (Spalte 4)

Unter Angriffen auf Kryptografie versteht man das Kompromittieren oder Brechen von Verschlüsselungs- und Hashverfahren sowie das Ausnutzen von Schwachstellen in Schlüssel- oder Zertifikatsverwaltung.

In mehreren Fällen gelang es Angreifern, Passworthashes zu entschlüsseln oder zumindest behauptete Erfolge in dieser Hinsicht zu erzielen. So konnten etwa bestimmte Passworthashes erfolgreich geknackt werden (SV01), wobei es in einem anderen Kontext lediglich als angeblich gelungen galt (SV04). Das Entschlüsseln von Passworthashes zog sich als Bedrohung durch verschiedene Szenarien: Insgesamt sollen 4 Millionen Passwörter publiziert worden sein, nachdem sie mithilfe von „credential cracking“, also einer Brute-Force-Attacke zum systematischen Durchprobieren von möglichen Kombinationen aus Nutzername und Passwort, geknackt werden konnten (SV02). In einem Fall wird zudem vermutet, dass unterschiedliche Methoden wie Wörterbuchangriffe, Rainbow-Table-Angriffe, Raten oder Spidering zum Einsatz kamen (SV10).

Auch gehashte Daten waren nicht immer sicher. So gelang es Angreifern, gehashte Daten zurückzurechnen (SV03), was auf eine unzureichende Implementierung oder Schlüsselexposition hindeutet. Im gleichen Fall konnte durch gestohlene AWS-Keys auf eine Datenbank zugegriffen werden (SV03). Daneben gab es Hinweise darauf, dass ein in einem Gruppenrichtlinienobjekt gespeichertes Passwort von den Angreifern entschlüsselt werden konnte (SV16). Darüber hinaus existieren Szenarien, in denen gestohlene Passwort-Tresore offline vorlagen und somit jegliche Sicherheitsmechanismen wie Sperren nach mehreren fehlgeschlagenen Anmeldeversuchen wirkungslos blieben. Dies ermöglich-

te potenziell ungehinderte Brute-Force-Attacken auf die verschlüsselten Tresore (SV11). Gleichermaßen wurde eine geteilte Wissenskomponente entwendet, mit der sich Kundendaten entschlüsseln ließen (SV11). Ebenso wurde in einem weiteren Fall berichtet, dass Angreifer Entschlüsselungsschlüssel stahlen, die Zugang zu Cloud-basierten Speicherressourcen ermöglichten (SV11). In einem anderen Szenario gab es Hinweise darauf, dass Azure AD Keys oder andere MSA-Keys verwendet worden sein könnten – ein Verdacht, der jedoch nicht zweifelsfrei belegt werden konnte (SV14).

Einen besonders interessanten Angriff auf Kryptografie stellt das Aushebeln der HTTPS-Zertifikatsverifikation dar, wie sie in einer untersuchten Malware beobachtet wurde. Indem die Funktion zur Zertifikatsprüfung gezielt deaktiviert wurde, war es möglich, den eigentlich verschlüsselten Datenverkehr zwischen einzelnen Computern mitzulesen und zu manipulieren (SV06). Dieses Vorgehen unterläuft das grundlegende Vertrauensmodell von HTTPS und öffnet Angriffsvektoren, die sonst nur schwer realisierbar wären.

Schließlich ist es nicht nur Angreifern gelungen, kryptografische Barrieren zu umgehen, denn in einem Fall konnten auch Sicherheitsforscher selbst die Hashes eines Trojaners mithilfe von Brute-Force-Angriffen zurückzurechnen (Siehe SW_GB_2 in Anhang A.6. auf S. 139) (SV06). Die Fähigkeit, solche Hashverfahren zu knacken, spielt eine wesentliche Rolle für die forensische Aufarbeitung, zeigt aber gleichzeitig auf, dass kryptografische Verfahren auf beiden Seiten – Angriff und Verteidigung – erfolgreich gebrochen oder ausgespielt werden können.

5.3.3.14 Angriffe durch Kryptografie (Spalte 5)

In anderen Fällen nutzen die Angreifer selbst kryptografische Methoden, um ihre eigenen Aktionen zu verschleiern, um an sensible Daten zu gelangen oder um ihren unerlaubten Zugriff zu festigen. Ein eindrückliches Beispiel ist der Missbrauch eines digital signierten Softwareupdates, um eine Hintertür auf den Systemen mehrerer tausend Unternehmen und Behörden zu verbreiten (SV06). Hierbei täuschen die Angreifern mitunter Legitimität vor, indem sie auf einen gültigen oder gekaperten Zertifikatsschlüssel zurückgreifen.

In mehreren Ransomware-Fällen wurde Kryptografie genutzt, um Dateien der Opfer zu verschlüsseln und so deren Verfügbarkeit zu unterbinden (SV07, SV08, SV13, SV16, SV17). Teilweise setzten die Angreifer die Ransomware erst ein, als der Angriff bereits öffentlich bekannt geworden war, um weitere Spuren zu verwischen oder den Schaden

noch zu erhöhen (SV09). Daneben nutzten die Täter verschlüsselte Kommunikationskanäle, etwa durch SSH-Tunneling, um auf Unternehmensdaten zuzugreifen. Diese Technik erschwerte die Erkennung des Angriffs und diente gleichzeitig dazu, eine Hintertür für weiteren Zugriff einzurichten sowie den Datenverkehr zu verschleiern (SV10).

Ein besonders gravierender Vorfall war der Diebstahl eines inaktiven MSA Consumer Signing Key, der missbraucht wurde, um Authentifizierungstokens zu fälschen und so Zugriff auf E-Mail-Konten zahlreicher Privatpersonen und Unternehmen zu erlangen (SV14). Auch das Kapern von legitimen Sitzungs-Token war in einem Fall möglich, nachdem die Angreifer Dateien mit entsprechenden Token auslesen konnten (SV15). Dieses Vorgehen erlaubte ihnen, bestehende Session-Verbindungen zu übernehmen und sich so nahtlos als autorisierte Benutzer auszuweisen.

Abseits dieser gezielten Nutzung verschlüsselnder Verfahren gegen die Opfer verschleierten Angreifer oft auch ihre Schadsoftware selbst. So wurde etwa der Name des schädlichen Prozesses mithilfe eines Hashingalgorithmus versteckt, um Virenscanner und andere Sicherheitsmechanismen zu umgehen (SV06). In direkter Verbindung hierzu zeigt sich jedoch die angesprochene Überschneidung zu Angriffen auf Kryptografie: Obwohl die Malware Hashing einsetzte, wurden offenbar schwache Hashverfahren verwendet, sodass es es Sicherheitsforschern gelang, die Hashes mittels Brute-Force-Attacken zurückzurechnen (SV06). Hinzu kommt, dass die Schadsoftware bestimmte Werte der infizierten Systeme hashte, um die Opfer über einen längeren Zeitraum zu verfolgen (SV06).

Darüber hinaus dokumentierten die Angreifer ihre Aktivitäten in eigenen Logfiles, die sie zumindest teilweise verschlüsselten. Dies sollte eine tiefergehende Analyse ihrer Vorgehensweise erschweren. Bei einem konkreten Fall löschte die Ransomware nach ihrer Ausführung zudem die Schattenkopien des Dateisystems via PowerShell-Befehl, um eine Wiederherstellung der kompromittierten Daten zusätzlich zu verhindern (SV16).

Es wird deutlich, dass Kryptografie nicht ausschließlich ein Verteidigungsinstrument darstellt. Vielmehr setzen auch Angreifer gezielt auf kryptografische Verfahren, um ihre Aktivitäten zu tarnen und nachhaltigen Schaden zu verursachen. Gleichzeitig zeigt sich, dass Angriffe auf und Angriffe durch Kryptografie vielfältig miteinander verknüpft sind. Einerseits brechen Angreifer kryptografische Maßnahmen und nutzen andererseits selbst

kryptografische Techniken, um Verteidigungsmechanismen auszuhebeln oder sich eine möglichst verdeckte Handlungsbasis zu schaffen.

6. Diskussion

In diesem Kapitel werden die Ergebnisse der Evaluation diskutiert. In der zweiten Hälfte des Kapitels findet eine kritische Reflexion der Forschungsarbeit statt, indem aufgezeigt wird, welche Limitationen bestanden und wie diese sich auf die Aussagekraft der Ergebnisse auswirken.

6.1. Ergebnisse

Die vorliegenden Ergebnisse zeigen deutlich, dass Kryptografie in aktuellen sowie vergangenen IT-Sicherheitsvorfällen eine bedeutende Rolle einnimmt, auch wenn sie dabei nicht immer die erhoffte Sicherheit gewährleistet. Die Untersuchung zeigt zum einen, dass die Verwendung von starken Verschlüsselungs- und Hashingverfahren wie AES oder bcrypt das Risiko für die Kompromittierung sensibler Daten nachweislich reduzieren können. Mehrere Beispiele haben gezeigt, dass Passwörter, die in starker gehashter Form vorlagen, nur mit erheblichem Aufwand oder gar nicht geknackt werden konnten. Ebenso blieben verschlüsselte Sozialversicherungsnummern und andere besonders schützenswerte Daten selbst nach einer Kompromittierung weitgehend sicher. Gerade die gezielte Trennung von Schlüssel und Daten, die Verwendung von Master-Passwörtern und Multi-Faktor-Authentifizierung sowie die konsequente Umsetzung sicherer Standardverfahren, wie z. B. AES-256, tragen dabei wesentlich zum Schutz bei.

Gleichzeitig wird aber deutlich, dass sich in der Praxis große Defizite zeigen, sobald Kryptografie nicht oder nur unzureichend implementiert wird. Mehrere Vorfälle veranschaulichen den Einsatz schwacher Hashfunktionen wie SHA-1 oder die Speicherung von Passwörtern im Klartext. Solche Fehlkonfigurationen und vernachlässigte Updates begünstigen erfolgreiche Angriffe, bei denen erhebliche Datenmengen kompromittiert werden können. Zudem können selbst stärkere Verfahren unwirksam sein, wenn sie falsch oder nur teilweise umgesetzt werden, etwa wenn Passwörter zwar gehasht, aber ohne ausreichende Iterationen verarbeitet werden oder wenn lediglich ein Teil der Informationen verschlüsselt vorliegt.

Ein weiterer Aspekt ist der jeweilige Anwendungsfall von Kryptografie. Auf der einen Seite verschlüsseln Angreifer wichtige Daten oder hebeln wichtige Kontrollen wie Zertifikatsverifikation bewusst aus. Auf der anderen Seite nutzen Angreifer selbst kryptografische Techniken, um ihre Schadsoftware zu verschleiern oder unerkannten Zugriff auf Systeme zu erlangen, etwa durch SSH-Tunneling oder digital signierte Softwareupdates. Damit wird Kryptografie nicht nur zum Mittel der Verteidigung, sondern gleichermaßen zum Angriffswerkzeug.

Allerdings sind viele Sicherheitsvorfälle nicht allein auf technische, sondern ebenso auf organisatorische und menschliche Faktoren zurückzuführen. Unzureichende MFA-Pflicht, fehlende oder verspätete Patches, mangelhafte Berechtigungsstrukturen und eine unklare Kommunikation zwischen IT-Teams und Management begünstigen Angriffe erheblich. Darüber hinaus stellen menschliche Fehler, wie das Offenlegen von Zugangs- oder Master-Passwörtern im Klartext, die unbedachte Bestätigung wiederkehrender MFA-Anfragen oder das Nachlässigwerden im Tagesgeschäft, ein hohes Sicherheitsrisiko dar. Social-Engineering-Methoden, sind nach wie vor ein beliebter Angriffsvektor, weil Mitarbeiter nicht ausreichend aufmerksam und geschult sind.

Insgesamt zeigen die Ergebnisse, dass Kryptografie zwar eine zentrale Komponente einer umfassenden Sicherheitsstrategie ist, aber nur dann ihre schützende Wirkung entfalten kann, wenn sie eng verzahnt mit organisatorischen Maßnahmen und einem hohen Bewusstsein für IT-Sicherheit eingesetzt wird. Ein effektives Sicherheitskonzept erfordert demnach neben der Umsetzung starker kryptografischer Verfahren sowohl kontinuierliche Audits und Schulungen als auch eine Sicherheitskultur, die Fehlkonfigurationen reduziert und menschliche Unachtsamkeiten vorbeugt. Wo Kryptografie vernachlässigt oder falsch eingesetzt wird, haben Angreifer ein leichtes Spiel; wo sie hingegen fachgerecht integriert ist und durch organisatorische Prozesse unterstützt wird, lassen sich gravierende Schäden in vielen Fällen erfolgreich abwenden oder zumindest stark abmildern.

6.2. Einschränkungen

Die Vorgehensweise dieser Arbeit weist einige Einschränkungen auf, die die Anwendbarkeit der Ergebnisse beeinflussen. Zunächst war es aufgrund formaler Anforderungen und der Anwendung der qualitativen Inhaltsanalyse nicht möglich, mehr als die siebzehn gewählten IT-Sicherheitsvorfälle zu beschreiben und zu analysieren. Es handelt sich daher nur um eine kleine Teilmenge, die möglicherweise nur bedingt repräsentativ ist, wenn sie auch ausreichend war, um einen guten Überblick über das Thema zu erlangen.

Zudem befand sich die Güte der Dokumentation zu den gefundenen Vorfällen nicht auf dem gleichen Niveau. Einige Fälle boten nur wenige Informationsquellen in Form von Nachrichtenartikeln, während andere umfassend durch Branchenexperten, Forensikberichte oder detaillierte Blogbeiträge aufgearbeitet worden sind. Im Allgemeinen war es schwierig, systematisch nach einem Kryptografiebezug zu suchen oder diesen festzustellen. Oft war es nicht die Beschreibung eines Vorfalls, die den Bezug verdeutlichte, sondern der Kontext, in dem der Fall passierte. Diese Tatsache sowie die massive Menge an erfassten Sicherheitsvorfällen erschwerten es, geeignete Fälle systematisch zu bestimmen. Aus Zeitgründen wurden deshalb Vorfälle, sobald eine Übereinstimmung mit einem oder mehrerer Auswahlkriterien vorlag, direkt für die weitere Betrachtung in diese Arbeit aufgenommen. Dadurch könnte die Auswahl zunächst willkürlich wirken, auch wenn sie an definierten Kriterien gemessen wurde. Es ist davon auszugehen, dass bei einer Wiederholung der Recherche eine andere Teilmenge von IT-Sicherheitsvorfällen bestimmt werden könnte.

Die Verwendung von MAXQDA 24 für die qualitative Inhaltsanalyse hat diese insgesamt erleichtert, war jedoch durch die Menge und die Qualität des Materials eingeschränkt. Für das Material wurde ein Teil der Dokumente bewusst gewählt, der für die Beschreibung der Vorfälle identifiziert wurde. Das weicht von der von Mayring beschriebenen Vorgehens der Stichprobenziehung ab. [88, S. 53 f.]

Die ungleichmäßige Qualität des Materials erschwerte auch die Zuordnung der Kategorien. Manche Kategorien konnten für einige Dokumente aufgrund fehlender Aussagen oder Schlüsselwörter gar nicht zugeordnet werden. Es wäre in einigen Fällen möglich gewesen, über den Kontext eine Kategoriezuordnung vorzunehmen, dies hätte aber nicht der Vorgehensweise der qualitativen Inhaltsanalyse entsprochen. Die Anwendung der

Analysetechnik Explikation (siehe Mayring [88, S. 89]) hätte dem entgegenwirken können, wurde in dieser Arbeit aber nicht verfolgt.

Ein weiterer limitierender Faktor war der begrenzte Suchzeitraum von 2019 bis 2024. Fünf Jahre sind ein kurzer Zeitraum, die zwar eine umfassende Menge an IT-Sicherheitsvorfällen insgesamt einschließen, aber auch viele besonders große und interessante Vorfälle aus der Zeit von 2010 bis 2019 nicht berücksichtigen, wie z. B. MySpace (2016)[9], Adult Friend Finder (2016)[10] und Marriott International (2018)[11]. Eine Ausdehnung des Suchzeitraums hätte dazu beigetragen, eine größere Menge von besonders gut dokumentierten Sicherheitsvorfällen zu untersuchen und so einen detaillierteren Blick auf die Rolle von Kryptografie zu erhalten.

[9] Siehe https://myspace.com/pages/blog

[10] Siehe https://www.zdnet.com/article/adultfriendfinder-network-hack-exposes-secrets-of-412-million-users/

[11] Siehe https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html

7. Zusammenfassung und Ausblick

Das Ziel dieser Masterarbeit war es, die Rolle von Kryptografie in IT-Sicherheitsvorfällen zu untersuchen. In der durchgeführten qualitativen Inhaltsanalyse nach Mayring zeigte sich, dass Kryptografie bei zahlreichen Vorfällen eine zentrale Rolle einnimmt: Einerseits kann sie durch angemessene Verschlüsselungs- und Hashverfahren sensible Daten zuverlässig schützen und viele Angriffsszenarien erschweren, andererseits werden kryptografische Maßnahmen häufig entweder zu schwach oder gar nicht eingesetzt. Dadurch entstehen vermeidbare Lücken, die Angreifer konsequent ausnutzen.

Die Fälle belegten, dass die Verwendung von starken Algorithmen den Schutz von Passwörtern und persönlichen Informationen deutlich verbessern und selbst im Fall eines erfolgreichen Angriffs den Schaden minimieren können. Gleichzeitig wurde deutlich, dass unzureichende Implementierungen, wie unsichere Hashverfahren, das Speichern von sensiblen Daten im Klartext oder die fehlende Trennung von Schlüsseln und Daten, fatale Folgen haben. Zudem nutzen Angreifer manchmal selbst kryptografische Werkzeuge, um Schadsoftware oder ihre Aktivitäten zu verschleiern. Dadurch nimmt Kryptografie eine Doppelrolle ein, denn sie dient sowohl der Abwehr als auch der Verstärkung von Angriffen.

Neben den rein technischen Aspekten stellten sich organisatorische und personelle Faktoren als kritische Punkte heraus. Die beste kryptografische Absicherung kann nicht vor einer Außerkraftsetzung durch menschliche Fehler oder schwache Sicherheitsprozesse schützen. Ein umfassendes Sicherheitskonzept erfordert deshalb nicht nur starke kryptografische Verfahren, sondern auch klare Vorgaben für den Einsatz, regelmäßige Schulungen des Personals und ein durchgängiges Risikobewusstsein auf allen Ebenen eines Unternehmens.

Um den Nutzen von Kryptografie weiter zu optimieren und Sicherheitslücken nachhaltig zu schließen, sind zukünftig mehrere Schritte erforderlich. Erstens sollten Unternehmen kontinuierliche Audits und Penetrationstests durchführen, um ihre kryptografischen Implementierungen zu evaluieren und weiterzuentwickeln. Zweitens gilt es, die Zusammenarbeit zwischen IT-Abteilungen, Sicherheitsverantwortlichen und dem Management zu verbessern, um klare Zuständigkeiten und effektive Entscheidungswege zu etablieren.

Drittens müssen Anwender für den sicheren Umgang mit kryptografischen Verfahren sensibilisiert und auf mögliche Bedrohungen, besonders durch Social Engineering, vorbereitet werden. Auf diese Weise kann Kryptografie ihr volles Potenzial entfalten und einen noch wirksameren Beitrag zur Abwehr von IT-Sicherheitsvorfällen leisten.

Literaturverzeichnis

[1] BSI (Bundesamt für Sicherheit in der Informationstechnik), *Die Lage der IT-Sicherheit in Deutschland 2024*, BSI [Online], 2024. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5 (besucht am 06. 01. 2025).

[2] CrowdStrike, *CrowdStrike 2024 Global Threat Report*, CrowdStrike [Online], 2024. Adresse: https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf (besucht am 06. 01. 2025).

[3] A. Streim und F. Kuhlenkamp, *203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen*, Bitkom [Online], 2022. Adresse: https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022 (besucht am 02. 03. 2025).

[4] P. Weissmann, *Das NIS2-Umsetzungsgesetz NIS2UmsuCG – OpenKRITIS*, OpenKRITIS [Online], 2024. Adresse: https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html (besucht am 06. 01. 2025).

[5] C. Prabha, N. Sharma, J. Singh, A. Sharma und A. Mittal, „A Review of Cyber Security in Cryptography: Services, Attacks, and Key Approach," in *2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, 2023, S. 1300–1306. DOI: 10.1109/ICAIS56108.2023.10073747.

[6] J. Holdsworth und M. Kosinski, *What Is Information Security?* IBM [Online], 2024. Adresse: https://www.ibm.com/topics/information-security (besucht am 06. 01. 2025).

[7] BSI (Bundesamt für Sicherheit in der Informationstechnik), *IT-Grundschutz-Kompendium*. Köln, de: Reguvis, Feb. 2023.

[8] C. Eckert, *IT-Sicherheit: Konzepte –- Verfahren –- Protokolle*. Berlin, Boston: De Gruyter Oldenbourg, 2023, ISBN: 9783110985115. DOI: doi:10.1515/9783110985115. Adresse: https://doi.org/10.1515/9783110985115.

[9] IBM, *What Is IT Security?* IBM [Online], 2024. Adresse: https://www.ibm.com/think/topics/it-security (besucht am 06. 01. 2025).

[10] G. Lindemulder und M. Kosinski, *Was ist Cybersicherheit?* IBM [Online], 2024. Adresse: https://www.ibm.com/de-de/topics/cybersecurity (besucht am 06. 01. 2025).

[11] A. Archondakis, *OWASP Top Ten: Cryptographic Failures*, PentestPeople [Online], 2024. Adresse: https://www.pentestpeople.com/blog-posts/owasp-top-ten-cryptographic-failures (besucht am 06. 01. 2025).

[12] OWASP, *A02 Cryptographic Failures - OWASP Top 10:2021*, OWASP [Online], 2021. Adresse: https://owasp.org/Top10/A02_2021-Cryptographic_Failures/ (besucht am 04. 10. 2024).

[13] C. Paar, J. Pelzl und T. Güneysu, *Understanding Cryptography: From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms*. Springer Berlin Heidelberg, 2024, ISBN: 9783662690079. DOI: 10.1007/978-3-662-69007-9.

[14] B. Esslinger, *Kryptografie lernen und anwenden mit CryptTool und Sagemath*. Lehmanns Media, Berlin, 2025, ISBN: 978-3-96543-517-9. Adresse: https://www.cryptool.org/de/ctbook.

[15] M. Kosinski, *Was ist ein Data Breach?* IBM [Online], 2024. Adresse: https://www.ibm.com/de-de/topics/data-breach (besucht am 06. 01. 2025).

[16] L. Cheng, F. Liu und D. Yao, „Enterprise data breach: causes, challenges, prevention, and future directions," *WIREs Data Mining and Knowledge Discovery*, Jg. 7, Nr. 5, Juni 2017, ISSN: 1942-4795. DOI: 10.1002/widm.1211.

[17] IBM, *Was ist Datenexfiltration?* IBM [Online], 2024. Adresse: https://www.ibm.com/de-de/topics/data-exfiltration (besucht am 06. 01. 2025).

[18] MITRE, *Common Weakness Enumeration — CWE™*, MITRE [Online], 2024. Adresse: https://makingsecuritymeasurable.mitre.org/docs/cwe-intro-handout.pdf (besucht am 06. 01. 2025).

[19] MITRE, *Common Vulnerabilities and Exposures — CVE®*, MITRE [Online], 2024. Adresse: https://makingsecuritymeasurable.mitre.org/docs/cve-intro-handout.pdf (besucht am 06. 01. 2025).

[20] N. Pohlmann, „Kryptografie," in *Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*. Wiesbaden: Springer Fachmedien Wiesbaden, 2019, S. 43–99, ISBN: 978-3-658-25398-1. DOI: 10.1007/978-3-658-25398-1_2. Adresse: https://doi.org/10.1007/978-3-658-25398-1_2.

[21] H. Li und Y. Wang, „The History of Cryptography and Its Aplications," in *International Journal of Social Science and Education Research*, 3, Bd. 25, Boya Century Publishing, 2022, S. 343–349. DOI: 10.6918/IJOSSER.202203_5(3).0056. Adresse: http://www.ijosser.org/download/IJOSSER-5-3-343-349.pdf.

[22] F. Badenschier, *Kryptologie: Alltag - Kryptologie - Forschung - Natur - Planet Wissen*, WDR [Online], 2021. Adresse: https://www.planet-wissen.de/natur/forschung/kryptologie_die_lehre_des_verborgenen/pwiekryptologieimalltag100.html (besucht am 06. 01. 2025).

[23] OWASP, *Password Storage - OWASP Cheat Sheet Series*, OWASP [Online], 2024. Adresse: https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html (besucht am 06. 01. 2025).

[24] J. F. Dooley, „Cyber Weapons and Cyber Warfare," in *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms*. Cham: Springer International Publishing, 2018, S. 213–239, ISBN: 978-3-319-90443-6. DOI: 10.1007/978-3-319-90443-6_13. Adresse: https://doi.org/10.1007/978-3-319-90443-6_13.

[25] H. Oz, A. Aris, A. Levi und A. S. Uluagac, „A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions," *ACM Comput. Surv.*, Jg. 54, Nr. 11s, Sep. 2022, ISSN: 0360-0300. DOI: 10.1145/3514229. Adresse: https://doi.org/10.1145/3514229.

[26] A. Trevino, *Locker- vs. Krypto-Ransomware: Was ist der Unterschied?* Keeper Security [Online], 2024. Adresse: https://www.keepersecurity.com/blog/de/2024/06/04/locker-vs-crypto-ransomware-whats-the-difference/ (besucht am 06. 01. 2025).

[27] Blackberry, *What Is LockBit Ransomware?* Blackberry [Online], 2024. Adresse: https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/lockbit (besucht am 06. 01. 2025).

[28] F. Salahdine und N. Kaabouch, „Social Engineering Attacks: A Survey," *Future Internet*, Jg. 11, Nr. 4, 2019, ISSN: 1999-5903. DOI: 10.3390/fi11040089. Adresse: https://www.mdpi.com/1999-5903/11/4/89.

[29] Y. S. Saini, L. Sharma, P. Chawla und S. Parashar, „Social Engineering Attacks," in *Emerging Technologies in Data Mining and Information Security*, P. Dutta, S. Chakrabarti, A. Bhattacharya, S. Dutta und V. Piuri, Hrsg., Singapore: Springer Nature Singapore, 2023, S. 497–509, ISBN: 978-981-19-4193-1.

[30] Z. Wang, L. Sun und H. Zhu, „Defining Social Engineering in Cybersecurity," *IEEE Access*, Jg. 8, S. 85 094–85 115, 2020. DOI: 10.1109/ACCESS.2020.2992807.

[31] R. Tahir, „A Study on Malware and Malware Detection Techniques," *International Journal of Education and Management Engineering (IJEME)*, Jg. 8, Nr. 2, S. 20–30, 2018. DOI: 10.5815/ijeme.2018.02.03.

[32] M. F. A. Razak, N. B. Anuar, R. Salleh und A. Firdaus, „The rise of "malware": Bibliometric analysis of malware study," *Journal of Network and Computer Applications*, Jg. 75, S. 58–76, 2016, ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2016.08.022. Adresse: https://www.sciencedirect.com/science/article/pii/S1084804516301904.

[33] IBM, *Was ist ein Zero-Day-Exploit?* IBM [Online], 2024. Adresse: https://www.ibm.com/de-de/topics/zero-day (besucht am 06. 01. 2025).

[34] Fortinet, *What are Supply Chain Attacks? Examples and Countermeasures*, Fortinet [Online], 2024. Adresse: https://www.fortinet.com/resources/cyberglossary/supply-chain-attacks (besucht am 06. 01. 2025).

[35] A. Hassanzadeh u. a., „A Review of Cybersecurity Incidents in the Water Sector," *Journal of Environmental Engineering*, Jg. 146, Nr. 5, S. 03 120 003, 2020. DOI: 10.1061/(ASCE)EE.1943-7870.0001686. eprint: https://ascelibrary.org/doi/pdf/10.1061/\%28ASCE\%29EE.1943-7870.0001686. Adresse: https://ascelibrary.org/doi/abs/10.1061/%5C%28ASCE%5C%29EE.1943-7870.0001686.

[36] P. H. Meland, K. Bernsmed, E. Wille, Ø. Rødseth und D. A. Nesheim, „A Retrospective Analysis of Maritime Cyber Security Incidents," *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, Jg. 15, S. 519–530, Jan. 2021. DOI: 10.12716/1001.15.03.04.

[37] S. Temara, „The Ransomware Epidemic: Recent Cybersecurity Incidents Demystified," *Asian Journal of Advanced Research and Reports*, Jg. 18, S. 1–16, Feb. 2024. DOI: 10.9734/AJARR/2024/v18i3610.

[38] L. Abrams, *CafePress Data Breach Exposes Personal Info of 23 Million Users*, Bleeping Computer [Online], 2019. Adresse: https://www.bleepingcomputer.com/news/security/cafepress-data-breach-exposes-personal-info-of-23-million-users/ (besucht am 06. 01. 2025).

[39] D. Winder, *CafePress Hacked: 23M Accounts Compromised. Is Yours One of Them?* Forbes [Online], 2019. Adresse: https://www.forbes.com/sites/daveywinder/2019/08/05/cafepress-hacked-23m-accounts-compromised-is-yours-one-of-them/ (besucht am 06. 01. 2025).

[40] S. Gatlan, *CafePress Fined $500,000 for Breach Affecting 23 Million Users*, Bleeping Computer [Online], 2022. Adresse: https://www.bleepingcomputer.com/news/security/cafepress-fined-500-000-for-breach-affecting-23-million-users/ (besucht am 06. 01. 2025).

[41] S. Gatlan, *FTC to Fine CafePress for Cover-Up of Massive Data Breach*, Bleeping Computer [Online], 2022. Adresse: https://www.bleepingcomputer.com/news/security/ftc-to-fine-cafepress-for-cover-up-of-massive-data-breach/ (besucht am 06. 01. 2025).

[42] M. H. Nguyen Ba, J. Bennett, M. Gallagher und S. Bhunia, „A Case Study of Credential Stuffing Attack: Canva Data Breach," in *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2021, S. 735–740. DOI: 10.1109/CSCI54926.2021.00187.

[43] C. Cimpanu, *Australian tech unicorn Canva suffers security breach*, ZDNet [Online], 2019. Adresse: https://www.zdnet.com/article/australian-tech-unicorn-canva-suffers-security-breach/ (besucht am 06. 01. 2025).

[44] Capital One, *2019 Capital One Cyber Incident*, Capital One [Online], 2022. Adresse: https://www.capitalone.com/digital/facts2019/ (besucht am 06. 01. 2025).

[45] S. Khan, I. Kabanov, Y. Hua und S. Madnick, „A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned," *ACM Transactions on Privacy and Security*, Jg. 26, Juli 2022. DOI: 10.1145/3546068.

[46] C. Duckett, *100 million Americans and 6 million Canadians caught up in Capital One breach*, ZDNet [Online], 2019. Adresse: https://www.zdnet.com/article/100-million-americans-and-6-million-canadians-caught-up-in-capital-one-breach/ (besucht am 06. 01. 2025).

[47] S. Rai, *Alibaba-Backed Bigbasket Suffers Major Data Loss in Cyberattack - Bloomberg*, Bloomberg [Online], 2020. Adresse: https://www.bloomberg.com/news/articles/2020-11-09/alibaba-backed-bigbasket-suffers-major-data-loss-in-cyberattack (besucht am 06. 01. 2025).

[48] P. Paganini, *20 million Bigbasket user records available on the dark web*, Security Affairs [Online], 2020. Adresse: https://securityaffairs.com/110543/data-breach/bigbasket-details-dark-web.html (besucht am 06. 01. 2025).

[49] M. Singh, *Alleged records of 20 million BigBasket users published online*, TechCrunch [Online], 2021. Adresse: https://techcrunch.com/2021/04/25/hacker-publishes-alleged-records-of-20-million-bigbasket-users/ (besucht am 06. 01. 2025).

[50] J. Sorn u. a., „Exploring the CAM4 Data Breach: Security Vulnerabilities and Response Strategies," in *2024 IEEE 24th International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, 2024, S. 174–179. DOI: 10.1109/CCGridW63211.2024.00028.

[51] B. Barrett, *Adult Cam Site CAM4 Exposed 10.88 Billion Records Online*, WIRED [Online], 2020. Adresse: https://www.wired.com/story/cam4-adult-cam-data-leak-7tb/ (besucht am 06. 01. 2025).

[52] SafetyDetectives Cybersecurity Team, *Live streaming adult site leaves 7 terabytes of private data exposed*, SafetyDetectives [Online], 2020. Adresse: https://www.safetydetectives.com/blog/cam-leak-report/ (besucht am 06. 01. 2025).

[53] TeamPassword, *What happened with the CAM4 Data Leak?* TeamPassword [Online], 2021. Adresse: https://teampassword.com/blog/what-happened-with-the-cam4-data-leak (besucht am 02. 03. 2025).

[54] Elastic, *Elasticsearch: Die offizielle Engine für verteilte Suche und Analytics*, Elastic [Online], 2024. Adresse: https://www.elastic.co/de/elasticsearch (besucht am 06. 01. 2025).

[55] L. Sterle und S. Bhunia, „On SolarWinds Orion Platform Security Breach," in *2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*, 2021, S. 636–641. DOI: 10.1109/SWC50871.2021.00094.

[56] S. Oladimeji und S. M. Kerner, *SolarWinds hack explained: Everything you need to know*, TechTarget [Online], 2023. Adresse: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (besucht am 06. 01. 2025).

[57] P. Barnum, *SolarWinds Hack (2020) – Technical, Financial, and Legal Analysis*, Inedo Security Labs [Online], 2025. Adresse: https://security.inedo.com/library/incidents/SolarWinds-2020 (besucht am 02. 03. 2025).

[58] L. Abrams, *Chemical distributor pays $4.4 million to DarkSide ransomware*, BleepingComputer [Online], 2021. Adresse: https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/ (besucht am 06. 01. 2025).

[59] A. Din, *Chemical Distributor Brenntag Says What Data Was Stolen During the Ransomware Attack*, Heimdal [Online], 2021. Adresse: https://heimdalsecurity.com/blog/chemical-distributor-brenntag-says-what-data-was-stolen-during-the-ransomware-attack/ (besucht am 06. 01. 2025).

[60] J. Beerman, D. Berent, Z. Falter und S. Bhunia, „A Review of Colonial Pipeline Ransomware Attack," in *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, 2023, S. 8–15. DOI: 10.1109/CCGridW59191.2023.00017.

[61] L. Abrams, *Largest U.S. pipeline shuts down operations after ransomware attack*, Bleeping Computer [Online], 2021. Adresse: https://www.bleepingcomputer.com/news/security/largest-us-pipeline-shuts-down-operations-after-ransomware-attack/ (besucht am 06. 01. 2025).

[62] B. Krebs, *Microsoft: Chinese Cyberspies Used 4 Exchange Server Flaws to Plunder Emails – Krebs on Security*, KrebsonSecurity [Online], 2021. Adresse: https://krebsonsecurity.com/2021/03/microsoft-chinese-cyberspies-used-4-exchange-server-flaws-to-plunder-emails/ (besucht am 06. 01. 2025).

[63] B. Schneier, *More on the Chinese Zero-Day Microsoft Exchange Hack - Schneier on Security*, Schneier on Security [Online], 2021. Adresse: https://www.schneier.com/blog/archives/2021/03/more-on-the-chinese-zero-day-microsoft-exchange-hack.html (besucht am 06. 01. 2025).

[64] Microsoft 365 Security und Microsoft Threat Intelligence, *HAFNIUM targeting Exchange Servers with 0-day exploits*, Microsoft [Online], 2021. Adresse: https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/ (besucht am 06. 01. 2025).

[65] B. Krebs, *T-Mobile Investigating Claims of Massive Data Breach – Krebs on Security*, KrebsonSecurity [Online], 2021. Adresse: https://krebsonsecurity.com/2021/08/t-mobile-investigating-claims-of-massive-data-breach/ (besucht am 06. 01. 2025).

[66] M. Hill, *The T-Mobile data breach: A timeline*, CSO online [Online], 2021. Adresse: https://www.csoonline.com/article/571199/the-t-mobile-data-breach-a-timeline.html (besucht am 06. 01. 2025).

[67] R. Lawler, *T-Mobile data breach exposed the personal info of more than 47 million people - The Verge*, The Verge [Online], 2021. Adresse: https://www.theverge.com/2021/8/18/22630446/t-mobile-47-million-data-breach-ssn-pin-pii (besucht am 06. 01. 2025).

[68] K. Toubba, *03-01-2023: Security Incident Update and Recommended Actions*, LastPass [Online], 2023. Adresse: https://blog.lastpass.com/posts/security-incident-update-recommended-actions (besucht am 06. 01. 2025).

[69] B. Krebs, *Experts Fear Crooks are Cracking Keys Stolen in LastPass Breach – Krebs on Security*, KrebsonSecurity [Online], 2023. Adresse: https://krebsonsecurity.com/2023/09/experts-fear-crooks-are-cracking-keys-stolen-in-lastpass-breach/ (besucht am 06. 01. 2025).

[70] J. Weatherbed, *Attackers stole LastPass data by hacking an employee's home computer*, The Verge [Online], 2023. Adresse: https://www.theverge.com/2023/2/28/23618353/lastpass-security-breach-disclosure-password-vault-encryption-update (besucht am 06. 01. 2025).

[71] BARR Advisory, *Reframing Password Management: The LastPass Breach*, Cloud Security Alliance [Online], 2023. Adresse: https://cloudsecurityalliance.org/blog/2023/02/02/reframing-password-management-what-we-learned-from-the-lastpass-breach (besucht am 06. 01. 2025).

[72] L. Abrams, *Uber hacked, internal systems breached and vulnerability reports stolen*, Bleeping Computer [Online], 2022. Adresse: https://www.bleepingcomputer.com/news/security/uber-hacked-internal-systems-breached-and-vulnerability-reports-stolen/ (besucht am 06. 01. 2025).

[73] L. H. Newman, *The Uber Hack's Devastation Is Just Starting to Reveal Itself*, WIRED [Online], 2022. Adresse: https://www.wired.com/story/uber-hack-mfa-phishing/ (besucht am 06. 01. 2025).

[74] InsiderSecurity, *The Uber Breach: Ways to Prevent Similar Attacks*, CloudSecurityAlliance [Online], 2023. Adresse: https://cloudsecurityalliance.org/blog/2023/03/23/insights-from-the-uber-breach-ways-to-prevent-similar-attacks (besucht am 06. 01. 2025).

[75] S. R. Kelleher, *Inside The Ransomware Attack That Shut Down MGM Resorts*, Forbes [Online], 2023. Adresse: https://www.forbes.com/sites/suzannerowankelleher/2023/09/13/ransomware-attack-mgm-resorts/ (besucht am 06. 01. 2025).

[76] S. Morrison, *MGM cyber attack: How a phone call may have led to the ongoing hack*, VOX [Online], 2023. Adresse: https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware (besucht am 06. 01. 2025).

[77] R. McMillan und K. Sayre, *The Audacious MGM Hack That Brought Chaos to Las Vegas*, The Wall Street Journal [Online], 2024. Adresse: https://www.wsj.com/tech/cybersecurity/mgm-hack-casino-hackers-group-0366c641 (besucht am 02. 03. 2025).

[78] Microsoft Security Response Center, *Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email*, Microsoft [Online], 2023. Adresse: https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/ (besucht am 04. 10. 2024).

[79] Microsoft Security Response Center, *Results of Major Technical Investigations for Storm-0558 Key Acquisition*, Microsoft [Online], 2023. Adresse: https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/ (besucht am 04. 10. 2024).

[80] D. Bradbury, *Unauthorized Access to Okta's Support Case Management System: Root Cause and Remediation*, Okta [Online], 2023. Adresse: https://sec.okta.com/articles/2023/11/unauthorized-access-oktas-support-case-management-system-root-cause (besucht am 06. 01. 2025).

[81] M. Maiffret, *BeyondTrust Discovers Breach of Okta Support Unit*, BeyondTrust [Online], 2023. Adresse: https://www.beyondtrust.com/blog/entry/okta-support-unit-breach (besucht am 06. 01. 2025).

[82] Südwestfalen-IT, *Südwestfalen-IT: Forensik-Bericht liefert Erkenntnisse zu Ransomware-Angriff – neuer Geschäftsführer der Südwestfalen IT arbeitet Vorfall auf*, Südwestfalen-IT [Online], 2024. Adresse: https://notfallseite.sit.nrw/ (besucht am 10. 04. 2024).

[83] D. Berg und J. Korte Martin andReinold, *Riesen-Cyberattacke: Rathäuser bleiben abgeschnitten*, Westfalenpost [Online], 2023. Adresse: https://www.wp.de/region/sauer-und-siegerland/article239913093/cyberattacke-auf-suedwestfalen-was-bislang-bekannt-ist.html (besucht am 06. 01. 2025).

[84] M. Fielenbach, *Abschlussbericht Security Incident*, Südwestfalen-IT [Online], 2024. Adresse: https://notfallseite.sit.nrw/fileadmin/user_upload/SIT_Incident_Response_v1.1.pdf (besucht am 10. 04. 2024).

[85] Südwestfalen-IT, *Ein Jahr nach dem Hackerangriff: Südwestfalen-IT zieht Bilanz: SIT.NRW*, Südwestfalen-IT [Online], 2024. Adresse: https://www.sit.nrw/detailansicht/ein-jahr-nach-dem-hackerangriff-suedwestfalen-it-zieht-bilanz (besucht am 06. 01. 2025).

[86] Z. Whittaker, *How the ransomware attack at Change Healthcare went down: A timeline*, TechCrunch [Online], 2024. Adresse: https://techcrunch.com/2024/12/18/how-the-ransomware-attack-at-change-healthcare-went-down-a-timeline/ (besucht am 06. 01. 2025).

[87] Z. Whittaker, *UnitedHealth says Change Healthcare hack affects over 100 million, the largest-ever US healthcare data breach*, TechCrunch [Online], 2024. Adresse: https://techcrunch.com/2024/10/24/unitedhealth-change-healthcare-hacked-millions-health-records-ransomware/ (besucht am 06. 01. 2025).

[88] P. Mayring, *Qualitative Inhaltsanalyse: Grundlagen und Techniken*, Neuausgabe. Weinheim: Beltz Verlagsgruppe, 2022, ISBN: 9783407258991.

Eidesstattliche Erklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe, insbesondere keine anderen als die angegebenen Informationen aus dem Internet. Diejenigen Paragraphen der für mich geltenden Prüfungsordnungen, die etwaige Betrugsversuche betreffen, habe ich zur Kenntnis genommen.

Der Speicherung meiner Masterarbeit zum Zweck der Plagiatsprüfung stimme ich zu. Ich versichere, dass die elektronische Version mit der gedruckten Version inhaltlich übereinstimmt.

Hereby I confirm that I have composed the present thesis independently. I only have used the sources and means specified in this thesis. Especially from the internet, I only have used the denoted references. I have taken note of the section in the examination regulations concerning attempts to cheat.

I confirm that the electronic version of the thesis which I deliver is identical to the printed version with respect to the content. I agree that an electronic version of the thesis will be stored for purposes of inspection of plagiarism.

_____ _____

(Datum/Date) (Unterschrift/Signature)

Inhalt der E-Mail

- Masterarbeit (PDF)
- Quellcode der Masterarbeit (ZIP, TEX)

A. Anhang

A.1. Inhaltsbeschreibungen CWE

CWE-288: Authentication Bypass Using an Alternate Path or Channel

The product requires authentication, but the product has an alternate path or channel that does not require authentication.
URL: https://cwe.mitre.org/data/definitions/288.html

CWE-327: Use of a Broken or Risky Cryptographic Algorithm

The product uses a broken or risky cryptographic algorithm or protocol.
URL: https://cwe.mitre.org/data/definitions/327.html

CWE-328: Use of Weak Hash

The product uses an algorithm that produces a digest (output value) that does not meet security expectations for a hash function that allows an adversary to reasonably determine the original input (preimage attack), find another input that can produce the same hash (2nd preimage attack), or find multiple inputs that evaluate to the same hash (birthday attack).
URL: https://cwe.mitre.org/data/definitions/328.html

CWE-506: Embedded Malicious Code

The product contains code that appears to be malicious in nature.
URL: https://cwe.mitre.org/data/definitions/506.html

CWE-918: Server-Side Request Forgery (SSRF)

The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.
URL: https://cwe.mitre.org/data/definitions/918.html

A.2. Inhaltsbeschreibungen CVE

CVE-2020-10148

The SolarWinds Orion API is vulnerable to an authentication bypass that could allow a remote attacker to execute API commands. This vulnerability could allow a remote attacker to bypass authentication and execute API commands which may result in a compromise of the SolarWinds instance. SolarWinds Orion Platform versions 2019.4 HF 5, 2020.2 with no hotfix installed, and 2020.2 HF 1 are affected.
URL: https://www.cve.org/CVERecord?id=CVE-2020-10148

CVE-2021-26855

Microsoft Exchange Server Remote Code Execution Vulnerability
URL: https://www.cve.org/CVERecord?id=CVE-2021-26855

CVE-2023-20269

A vulnerability in the remote access VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a brute force attack in an attempt to identify valid username and password combinations or an authenticated, remote attacker to establish a clientless SSL VPN session with an unauthorized user. This vulnerability is due to improper separation of authentication, authorization, and accounting (AAA) between the remote access VPN feature and the HTTPS management and site-to-site VPN features. An attacker could exploit this vulnerability by specifying a default connection profile/tunnel group while conducting a brute force attack or while establishing a clientless SSL VPN session using valid credentials. A successful exploit could allow the attacker to achieve one or both of the following: Identify valid credentials that could then be used to establish an unauthorized remote access VPN session. Establish a clientless SSL VPN session (only when running Cisco ASA Software Release 9.16 or earlier). Notes: Establishing a client-based remote access VPN tunnel is not possible as these default connection profiles/tunnel groups do not and cannot have an IP address pool configured. This vulnerability does not allow an attacker to bypass authentication. To successfully establish a remote access VPN session, valid credentials are required, including a valid second factor if multi-factor authentication (MFA) is configured. Cisco

will release software updates that address this vulnerability. There are workarounds that address this vulnerability.
URL: https://www.cve.org/CVERecord?id=CVE-2023-20269

A.3. Python-Skript

Folgendes Python-Skript wurde verwendet, um die Einträge von HaveIBeenPwned in ein Komma-separiertes Format zu konvertieren:

```
#csv_skript.py

import csv

# Funktion zum Lesen und Konvertieren der Textdatei in eine Liste von
                                        Einträgen
def read_and_parse_textfile(file_path):
    entries = []
    with open(file_path, 'r', encoding='utf-8') as file:
        while True:
            logotext = file.readline().strip()
            if not logotext:  # EOF erreicht
                break
            unternehmensname = file.readline().strip()
            beschreibung = file.readline().strip()
            file.readline()  # Leerzeile überspringen
            datum = file.readline().strip().split(": ", 1)[1]
            hinzugefügt_datum = file.readline().strip().split(": ", 1)[1]
            kompromittierte_accounts = file.readline().strip().split(": ",
                                                    1)[1]
            kompromittierte_daten = file.readline().strip().split(": ", 1)
                                                    [1]
            permalink = file.readline().strip()
            file.readline()  # Leerzeile überspringen

            # Eintrag als Liste hinzufügen
            entries.append([logotext, unternehmensname, beschreibung,
                                                    datum, hinzugefügt_datum,
                                                     kompromittierte_accounts
                                                    , kompromittierte_daten,
                                                    permalink])

    return entries

# Funktion zum Schreiben der Daten in eine CSV-Datei
def write_to_csv(entries, output_file):
```

```
    header = ['Logotext', 'Unternehmensname', 'Beschreibung', 'Datum', '
                                        Datum hinzugefügt', '
                                        Kompromittierte Accounts', '
                                        Kompromittierte Daten', '
                                        Permalink']

    with open(output_file, 'w', newline='', encoding='utf-8') as csvfile:
        writer = csv.writer(csvfile, delimiter=';')  # Semikolon als
                                            Trennzeichen
        writer.writerow(header)  # Kopfzeile schreiben
        writer.writerows(entries)

# Hauptfunktion
def convert_text_to_csv(input_file, output_file):
    entries = read_and_parse_textfile(input_file)
    write_to_csv(entries, output_file)

# Beispielaufruf der Funktion
input_file = 'hibp.txt'  # Pfad zur Textdatei (im selben Ordner wie csv-
                                    skript.py)
output_file = 'hibp_konvertiert.csv'  # Pfad zur fertig konvertierten CSV-
                                    Datei
convert_text_to_csv(input_file, output_file)
```

A.4. Codesystem (Kategorien) für MAXQDA 24

In diesem Anhang werden die für die Evaluation ab S. 48 verwendeten Kategorien erläutert. Da es sich um einen direkten Export aus dem Programm MAXQDA 24 handelt, liegen die vom Autor erstellten Beschreibungstexte stichpunktartig vor.

1 Reaktionen

Zu der Oberkategorie für Reaktionen auf den Sicherheitsvorfall gehören die Kommunikation und ergriffene Maßnahmen in Bezug auf den Sicherheitsvorfall sowie Vorschläge für Maßnahmen oder Handlungen, um Eskalationen oder weitere Sicherheitsvorfälle zu vermeiden.

1.1 Reaktionen » Vorschläge

Hierzu gehören Aussagen oder Hinweise auf Vorschläge, die von Betroffenen oder Dritten gemacht wurden, um den Schaden direkt oder zukünftig zu begrenzen. Damit ist beispielsweise gemeint, dass Hinweise für Änderungen von Passwörtern herausgegeben wurden oder welche Maßnahmen einen Fall verhindern könnten.

1.2 Reaktionen » Maßnahmen

Zu dieser Oberkategorie gehören Maßnahmen und Handlungen, die von den Opfern oder Dritten in Bezug auf den Sicherheitsvorfall ergriffen wurden.

1.2.1 Reaktionen » Maßnahmen » Dritte

Hierzu gehören Aussagen, die die von Dritten ergriffenen oder umgesetzten Maßnahmen oder Handlungen in Bezug auf den Sicherheitsvorfall beschreiben.

1.2.2 Reaktionen » Maßnahmen » Opferseitig

Hierzu gehören Aussagen, die die von Seite der Opfer ergriffenen, umgesetzten Maßnahmen oder Handlungen in Bezug auf den Sicherheitsvorfall beschreiben.

1.3 Reaktionen » Kommunikation

Hierzu gehören Aussagen, die die Kommunikation der Betroffenen beschreiben. Damit ist beispielsweise der Umgang mit dem Sicherheitsvorfall gemeint.

2 Fehler

Zu der Oberkategorie für Fehler, die mit dem Sicherheitsvorfall zusammenhängen, gehören Aussagen oder Hinweise zu menschlichem Versagen, organisatorischen Schwächen, Schwachstellen und Versäumnissen von Dritten.

2.1 Fehler » Schwachstelle

Hierzu gehören Aussagen oder Hinweise darüber, welche Schwachstellen ausgenutzt wurden oder wie böswillige Akteure Zugang zu Systemen oder Daten erlangten.

2.2 Fehler » Organisatorische Schwächen

Hierzu gehören Aussagen, die auf organisatorische Schwächen der Betroffenen hindeuten. Das können strukturelle und systemische Probleme sein, die von der Organisation als Ganzes verursacht werden oder Fehlverhalten von Personen, welches auf mangelnde Organisation zurückzuführen ist. Damit sind beispielsweise das Fehlen von Richtlinien oder Prozessen im Umgang mit Sicherheitsvorfällen, schlecht geschultes Personal oder das Verzichten auf moderne kryptografische Lösungen aus Kostengründen gemeint.

2.3 Fehler » Versäumnisse von Dritten

Hierzu gehören Aussagen darüber, dass Versäumnisse von Dritten zum Sicherheitsvorfall beigetragen haben. Damit sind beispielsweise nicht ausreichend abgesicherte oder konfigurierte Produkte von Softwareanbietern gemeint, aber auch Dritte, die den Sicherheitsvorfall durch Fehlverhalten oder andere Faktoren begünstigt haben.

2.4 Fehler » Menschliches Versagen

Hierzu gehören Aussagen oder Hinweise darauf, dass Fehlhandlungen oder Versäumnisse einzelner Personen den Angriff begünstigt haben. Damit sind beispielsweise Dinge wie Unwissenheit, Fehlentscheidungen oder mangelnde Aufmerksamkeit gemeint.

3 Rolle der Kryptografie

Zu der Oberkategorie für Aussagen, die die Rolle der Kryptografie beschreiben, gehören schwache oder fehlende Kryptografie, Schutz durch Kryptografie sowie die Verwendung von Kryptografie für oder durch den Angriff.

3.1 Rolle der Kryptografie » Schwache o. fehlende Kryptografie

Hierzu gehören Aussagen oder Hinweise darauf, dass schwache oder gar keine kryptografischen Maßnahmen implementiert wurden. Damit sind beispielsweise die Verwendung veralteter oder als unsicher geltender Algorithmen für Hashing und Verschlüsselung gemeint.

3.2 Rolle der Kryptografie » Verwendung für Angriff

Zu der Oberkategorie für Aussagen, die auf eine Verwendung von Kryptografie als Angriffswerkzeug hindeuten, gehören Angriffe auf Kryptografie, bei denen z. B. Verschlüsselungen geknackt werden sowie Angriffe durch Kryptografie, bei denen z. B. durch Verschlüsselung Schaden entsteht.

3.2.1 Rolle der Kryptografie » Verwendung für Angriff » Angriff durch

Hierzu gehören Aussagen oder Hinweise darauf, dass der Angriff durch oder mithilfe von Kryptografie erfolgte. Damit ist beispielsweise die Verschlüsselung von Daten durch Ransomware oder die Verwendung von Kryptografie zur Verschleierung von böswilligen Aktivitäten gemeint.

3.2.2 Rolle der Kryptografie » Verwendung für Angriff » Angriff auf

Hierzu gehören Aussagen oder Hinweise darauf, dass der Angriff auf Kryptografie erfolgte. Damit ist beispielsweise die Entschlüsselung von verschlüsselten oder gehashten Daten durch verschiedene Angriffsmethoden oder gestohlene Schlüssel gemeint.

3.3 Rolle der Kryptografie » Schutz

Hierzu gehören Aussagen oder Hinweise darauf, dass Kryptografie eine schützende Rolle einnahm. Beispielsweise waren betroffene Daten verschlüsselt oder konnten Daten durch die verwendete Verschlüsselung nicht entschlüsselt oder kopiert werden.

4 Gemeinsamkeiten

Zu dieser Oberkategorie gehören Gemeinsamkeiten der Fälle, wie die Art des Vorfalls, die Branche und die Schwachstellen.

4.1 Gemeinsamkeiten » Art des Vorfalls

Diese Oberkategorie umfasst die verschiedenen Arten von Sicherheitsvorfällen die vorkommen, darunter Datenschutzverletzungen, Ransomware, Social Engineering und Supply-Chain-Angriffe.

4.1.1 Gemeinsamkeiten » Art des Vorfalls » Social Engineering

Hierzu gehören Aussagen, die auf Social Engineering allgemein oder verwendete Techniken hinweisen.

4.1.2 Gemeinsamkeiten » Art des Vorfalls » Datenschutzverletzung

Hierzu gehören Aussagen, die auf eine Datenschutzverletzung, ein Datenleck oder eine Datenpanne hinweisen.

4.1.3 Gemeinsamkeiten » Art des Vorfalls » Supply-Chain-Angriff

Hierzu gehören Aussagen, die auf einen Supply-Chain-Angriff (Angriff auf die Lieferkette) hinweisen.

4.1.4 Gemeinsamkeiten » Art des Vorfalls » Ransomware

Hierzu gehören Aussagen, die darauf hinweisen, dass es sich um Ransomware handelt.

4.2 Gemeinsamkeiten » Branche

Diese Oberkategorie beschreibt die Branchen, in der das Hauptopfer oder betroffene Dritte tätig sind.

4.2.1 Gemeinsamkeiten » Branche » Betroffene Dritte

Hierzu gehören Aussagen, die die Branche oder Sektoren von Dritten beschreiben, die ebenfalls durch den Sicherheitsvorfall betroffen waren.

4.2.2 Gemeinsamkeiten » Branche » Opfer

Hierzu gehören Aussagen, die darauf hinweisen, in welcher Branche oder Sektor das Hauptopfer des Sicherheitsvorfalls tätig ist.

5 Angreifer

Zu dieser Oberkategorie gehören Aussagen, die darauf hinweisen, dass es sich um Unbekannte, staatliche Motivierte, unabhängige Gruppen oder Einzeltäter handelt.

5.1 Angreifer » Unbekannt

Hierzu gehören Aussagen, die beschreiben, dass der oder die Täter unbekannt sind.

5.2 Angreifer » Staatlich motiviert

Hierzu gehören Aussagen, die darauf hindeuten, dass es sich um staatlich motivierte Gruppierungen oder Akteure handelt.

5.3 Angreifer » Unabhängige Gruppierungen

Hierzu gehören Aussagen, die beschreiben, es sich um eine unabhängige Gruppe oder einen Zusammenschluss krimineller Akteure handelt.

5.4 Angreifer » Einzelne

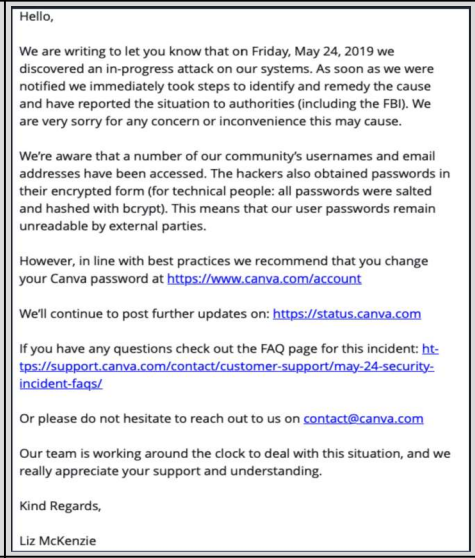
Hierzu gehören Aussagen, die beschreiben, dass es sich um einen Einzeltäter bzw. eine individuelle Person handelt.

A.5. Codierte Segmente der einzelnen Vorfälle

In diesem Anhang befinden sich alle mit MAXQDA 24 codierten Segmente. Ein codiertes Segment besteht aus einer oder mehreren Aussagen, die einer bestimmten Kategorie zugeordnet wurden. Für jeden Sicherheitsvorfall wurden verschiedene Quellen verarbeitet. Die nachfolgende Tabelle listet alle codierten Segmente, sortiert nach den Sicherheitsvorfällen, auf.

Dokumentgruppe	Dokumentname	Code	Segment
SV01 - CafePress	CP_BC_2	Angreifer > Unbekannt	After a February 2019 breach of CafePress' servers, unknown attackers
SV01 - CafePress	CP_BC_2	Fehler > Organisatorische Schwächen	As the consumer protection watchdog explained in a complaint from March 2022, Residual Pumpkin Entity stored its customers' Social Security numbers and password reset answers in plain text and longer than necessary.
SV01 - CafePress	CP_BC_2	Fehler > Organisatorische Schwächen	The company also failed to apply available protections and respond to security incidents. After its servers were breached multiple times, it tried to cover up the major data breach resulting from its sloppy security practices.
SV01 - CafePress	CP_BC_2	Fehler > Organisatorische Schwächen	CafePress knew that it had data security problems even before the 2019 breach since, according to FTC's complaint, the company found out that some of its shopkeepers' accounts had been compromised since at least January 2018.
SV01 - CafePress	CP_BC_2	Fehler > Organisatorische Schwächen	Several malware infections also impacted the company's network before the 2019 security breach, and CafePress, once again, failed to investigate the attacks.
SV01 - CafePress	CP_BC_1	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	data breach
SV01 - CafePress	CP_BC_1	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	CafePress data breach
SV01 - CafePress	CP_Forbes	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	CafePress breach
SV01 - CafePress	CP_Forbes	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	CafePress.com data breach
SV01 - CafePress	CP_BC_2	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	data breach
SV01 - CafePress	CP_BC_1	Gemeinsamkeiten > Branche > Direkt Betroffene	CafePress, a well-known custom T-Shirt and merchandise site
SV01 - CafePress	CP_Forbes	Gemeinsamkeiten > Branche > Direkt Betroffene	CafePress, the custom T-shirt and merchandise company
SV01 - CafePress	CP_BC_2	Gemeinsamkeiten > Branche > Direkt Betroffene	Residual Pumpkin Entity, the former owner of the CafePress t-shirt and merchandise site
SV01 - CafePress	CP_BC_1	Reaktionen > Kommunikation	Users became aware of the breach today, not through CafePress, but through notifications from Troy Hunt's Have I Been Pwned service.
SV01 - CafePress	CP_BC_1	Reaktionen > Kommunikation	At the time of this writing, CafePress has not responded to BleepingComputer's queries and has not issued a statement regarding the data breach. The only indication that something is wrong is that CafePress users are being forced to reset their password when they try to login to the site. In this password reset policy there is no mention of the breach as well.
SV01 - CafePress	CP_Forbes	Reaktionen > Kommunikation	Good question. An equally good one might be "why have I heard about this breach from HIBP and not CafePress itself?" of course. According to the Mozilla Firefox Monitor service, "It can sometimes take months or years for credentials exposed in a data breach to appear on the dark web. Breaches get added to our database as soon as they have been discovered and verified."
SV01 - CafePress	CP_Forbes	Reaktionen > Kommunikation	There have been no notification emails from CafePress as far as I can ascertain. I've positively not received one to either of the two addresses flagged by HIBP.
SV01 - CafePress	CP_Forbes	Reaktionen > Kommunikation	A CafePress spokesperson says that "CafePress Inc. learned of a potential security issue related to customer accounts. We have engaged third-party experts and are investigating the issue. Our commitment to maintaining the confidentiality of our customers' information is paramount to the employees and leadership of CafePress."
SV01 - CafePress	CP_BC_2	Reaktionen > Kommunikation	CafePress allegedly tried to cover up this massive data breach and didn't notify any affected individuals until September 2019, one month after BleepingComputer reported the breach. However, some users were made aware of the incident after receiving notifications from Troy Hunt's Have I Been Pwned service.
SV01 - CafePress	CP_BC_2	Reaktionen > Kommunikation	At the time, CafePress did not reply when BleepingComputer reached out for more information and did not issue a statement regarding the breach. The only sign that something was wrong was that its users were forced to reset their password when logging in (with no mention of the data breach).
SV01 - CafePress	CP_BC_2	Reaktionen > Kommunikation	Instead of informing them of the incidents, CafePress closed their accounts and charged each of them a $25 account closure fee.
SV01 - CafePress	CP_BC_2	Reaktionen > Maßnahmen > Dritte	The U.S. Federal Trade Commission (FTC) has ordered Residual Pumpkin Entity, the former owner of the CafePress t-shirt and merchandise site, to pay a $500,000 fine for covering up a data breach impacting more than 23 million customers and failing to protect their data.
SV01 - CafePress	CP_BC_2	Reaktionen > Maßnahmen > Dritte	According to the finalized order, on top of paying a $500,000 fine, Residual Pumpkin and PlanetArt (CAfePress' new owner) have to implement multi-factor authentication, minimize the amount of collected and retained data, and encrypt all stored Social Security numbers.

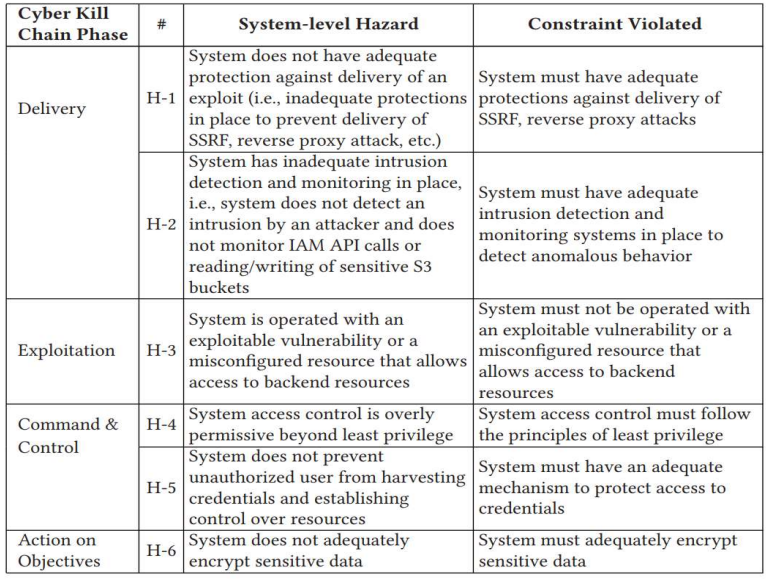
Dokumentgruppe	Dokumentname	Code	Segment
SV01 - CafePress	CP_BC_2	Reaktionen > Maßnahmen > Dritte	PlanetArt was also ordered to alert buyers and sellers whose personal info was accessed or stolen during the security breaches and provide them with information on how they can protect themselves.
SV01 - CafePress	CP_BC_1	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	Scott further told BleepingComputer that half of the compromised user's passwords were encoded in base64 SHA1, which is a very weak algorithm by today's standards. The other half of the users contained third-party tokens for logins through Facebook and Amazon.
SV01 - CafePress	CP_BC_1	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	"It came to my attention that Troy forgot to add that passwords were also affected in this security incident when first announcing this data breach, which has now been corrected. Out of the 23 million compromised users, roughly half of them had their passwords exposed encoded in base64 SHA1, which is a very weak encryption method to use especially in 2019 when better alternatives are available. The remaining users who used CafePress through third-party applications, such as FaceBook or Amazon, had no compromised passwords."
SV01 - CafePress	CP_Forbes	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	“It came to my attention that Troy forgot to add that passwords were also affected in this security incident,” Scotts says, continuing “out of the 23 million compromised users, roughly half of them had their passwords exposed encoded in base64 SHA1, which is a very weak encryption method to use especially in 2019 when better alternatives are available.” According to information supplied by Scott, the remaining users who used CafePress through third-party applications such as Facebook or Amazon did not have their passwords compromised.
SV01 - CafePress	CP_Forbes	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	Having spoken to Troy Hunt this afternoon, it would appear that the passwords in question are base64 encoded tokens, rather than user-chosen passwords, and there’s a lot of repetition.
SV01 - CafePress	CP_BC_2	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	millions of email addresses and passwords with weak encryption; millions of unencrypted names, physical addresses, and security questions and answers; more than 180,000 unencrypted Social Security numbers; and tens of thousands of partial payment card numbers and expiration dates.
SV01 - CafePress	CP_BC_1	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	Research by BleepingComputer shows that a dehashed CafePress database of approximately 493,000 accounts was being sold on hacker forums. It is not known if this is related to the same breach.
SV02 - Canva	CNV_Ba	Angreifer > Unabhängige Gruppierungen	GnosticPlayers
SV02 - Canva	CNV_Ba	Angreifer > Unabhängige Gruppierungen	GnosticPlayers claims responsibility for the hack to ZDNet.
SV02 - Canva	CNV_Ba	Angreifer > Unabhängige Gruppierungen	The hacker group behind the Canva data breach is Gnostic-Players
SV02 - Canva	CNV_Ba	Angreifer > Unabhängige Gruppierungen	GnosticPlayers is a group of hackers who have been using credential stuffing to breach many companies for a long time before Canva.
SV02 - Canva	CNV_ZDN	Angreifer > Unabhängige Gruppierungen	Responsible for the breach is a hacker going online as GnosticPlayers. The hacker is infamous. Since February this year, he/she/they has put up for sale on the dark web the data of 932 million users, which he stole from 44 companies from all over the world.
SV02 - Canva	CNV_CB	Angreifer > Unabhängige Gruppierungen	a hacker who goes by the name GnosticPlayers contacted ZDNet and claimed to have breached Canva earlier that morning.
SV02 - Canva	CNV_CB	Angreifer > Unabhängige Gruppierungen	GnosticPlayers is infamous as a hacker who has stolen data of over 900 million users from 45 companies worldwide and put them on sale on the dark web.
SV02 - Canva	CNV_Ba	Fehler > Organisatorische Schwächen	One of the top recommendations against credential stuffing is multi-factor authentication, which Canva does not require [8].
SV02 - Canva	CNV_Ba	Fehler > Organisatorische Schwächen	If Canva had a detailed plan in place for when a leak happened, as is inevitable, there would already be guidelines on how to inform users of the event.
SV02 - Canva	CNV_ZDN	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	Canva suffers security breach
SV02 - Canva	CNV_Canva	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	Datenangriffs vom 24. Mai
SV02 - Canva	CNV_Canva	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	Sie haben auf Informationen aus unserer Profil-Datenbank mit bis zu 139 Millionen Nutzern zugegriffen. Die Profil-Datenbank umfasst Benutzernamen, Namen, E-Mail-Adressen, Land und vom Nutzer optional bereitgestellte Daten wie Stadt und/oder Homepage-URL, die über ihr öffentliches Profil verfügbar waren.
SV02 - Canva	CNV_Canva	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	Sie haben sich kurz Dateien mit unvollständigen Kreditkarten- und Zahlungsdaten angesehen. Wir haben keine Beweise dafür gefunden, dass diese Dateien gestohlen wurden. Die Dateien enthielten unvollständige Kreditkartendaten von vor dem 28. September 2016 (Name, Ablaufdatum, letzte 4 Ziffern, Kartenmarke und Kartenland) und Zahlungsauflistungen von vor dem 16. September 2017, die Transaktionen in Dollarbeträgen, Daten und IDs für einige Zahlungen für Nutzer und Beitragende enthielten.Diese begrenzten Kartendaten können nicht für Zahlungen verwendet werden. Canva speichert nie vollständige Kreditkarteninformationen.
SV02 - Canva	CNV_Ba	Gemeinsamkeiten > Branche > Direkt Betroffene	Canva is a design and publishing platform currently competing with many other top-of-the-line platforms such as Adobe and PowerPoint
SV02 - Canva	CNV_ZDN	Gemeinsamkeiten > Branche > Direkt Betroffene	Canva, a Sydney-based startup that's behind the eponymous graphic design service

Dokumentgruppe	Dokumentname	Code	Segment
SV02 - Canva	CNV_ZDN	Gemeinsamkeiten > Branche > Direkt Betroffene	Canva is one of Australia's biggest tech companies. Founded in 2012, the Canva website has become a favorite among regular users and large companies who often use it to build quick websites, design logos, or put together eye-catching marketing materials.
SV02 - Canva	CNV_CB	Gemeinsamkeiten > Branche > Direkt Betroffene	background about Canva, it is one of the most popular graphic design startups that was founded in Australia in 2013
SV02 - Canva	CNV_Ba	Gemeinsamkeiten > Schwachstelle	GnosticPlayers methods for getting the database is using credential stuffing to get the developer's GitHub account, a simple but very effective method [3].
SV02 - Canva	CNV_Ba	Gemeinsamkeiten > Schwachstelle	While the exact vulnerability GnosticPlayers exploited has not been reported, Canva has claimed it was found and protected with help from Mandiant [4].
SV02 - Canva	CNV_Ba	Reaktionen > Kommunikation	May 25 2019 · · ·• Canva's email informing users of the breach is criticized.
SV02 - Canva	CNV_Ba	Reaktionen > Kommunikation	June 1 2019 · · ·• Canva describes in detail the event and their response on their website
SV02 - Canva	CNV_Ba	Reaktionen > Kommunikation	On the other hand, Canva's initial response reporting the breach to its users was heavily criticized. The first email sent out to users started off entirely unrelated to the attack, only mentioning it in later paragraphs [9].
SV02 - Canva	CNV_Ba	Reaktionen > Kommunikation	The "marketing fluff" made it less likely that users would notice the breach, only glancing at the first paragraph. This was eventually fixed with a separate email exclusively focused on the attack.
SV02 - Canva	CNV_Ba	Reaktionen > Kommunikation	Canva would have received much less backlash if they were upfront and honest about the incident [10].
SV02 - Canva	CNV_Ba	Reaktionen > Kommunikation	Canva also received heavy criticism due to its response in reporting the breach to its users. The initial email Canva sent out to users was full of unrelated information, only notifying people of the leak at the end of the email [9]. The so-called "marketing fluff" meant that people would only know of the breach if they read through the entire email. Anyone only reading the title or intro would be left completely unaware of the risk to their personal information.
SV02 - Canva	CNV_Ba	Reaktionen > Kommunikation	After some complaints on social media, another email was sent explicitly focused on the breach.
SV02 - Canva	CNV_Ba	Reaktionen > Kommunikation	In an attempt to hide the significance of the data breach, Canva only hurt their reputation more than it would have been otherwise.
SV02 - Canva	CNV_Ba	Reaktionen > Kommunikation	Canva's poor job in communicating the hack to users, their reputation was damaged much more than it would have been otherwise.
SV02 - Canva	CNV_CB	Reaktionen > Kommunikation	 Hello, We are writing to let you know that on Friday, May 24, 2019 we discovered an in-progress attack on our systems. As soon as we were notified we immediately took steps to identify and remedy the cause and have reported the situation to authorities (including the FBI). We are very sorry for any concern or inconvenience this may cause. We're aware that a number of our community's usernames and email addresses have been accessed. The hackers also obtained passwords in their encrypted form (for technical people: all passwords were salted and hashed with bcrypt). This means that our user passwords remain unreadable by external parties. However, in line with best practices we recommend that you change your Canva password at https://www.canva.com/account We'll continue to post further updates on: https://status.canva.com If you have any questions check out the FAQ page for this incident: https://support.canva.com/contact/customer-support/may-24-security-incident-faqs/ Or please do not hesitate to reach out to us on contact@canva.com Our team is working around the clock to deal with this situation, and we really appreciate your support and understanding. Kind Regards, Liz McKenzie
SV02 - Canva	CNV_CB	Reaktionen > Kommunikation	Canva promptly notified all its users of the attack and asked all those with unencrypted passwords to change their passwords immediately by sending out necessary emails containing a set of guidelines for setting the new password. On the 12th of January 2020, Canva forcibly reset the password of all those who hadn't changed their passwords yet and sent out emails about the same to its users.
SV02 - Canva	CNV_Canva	Reaktionen > Kommunikation	In den vergangenen 7 Monaten haben wir eine Vielzahl an Mitteilungen an die betroffenen Nutzer verschickt und sie darüber informiert, wie sie ihre Konten schützen können.
SV02 - Canva	CNV_Canva	Reaktionen > Kommunikation	Wir benachrichtigen ebenso alle Canva-Nutzer, deren Passwörter scheinbar entschlüsselt worden sind, damit sie andere Konten schützen können, bei denen sie evtl. dasselbe Passwort verwendet haben.
SV02 - Canva	CNV_Canva	Reaktionen > Kommunikation	Als Teil unserer Krisenbewältigung haben wir in einem ersten Schritt versucht, alle betroffenen Nutzer per E-Mail und über In-App-Alarme zu erreichen.

Dokumentgruppe	Dokumentname	Code	Segment
SV02 - Canva	CNV_Canva	Reaktionen > Kommunikation	Nach einer Untersuchung mit Experten für Cyber-Sicherheit können wir nun die Auswirkungen des Angriffs besser verstehen und möchten unserer Community so viele Informationen wie möglich weitergeben.
SV02 - Canva	CNV_Canva	Reaktionen > Kommunikation	Seitdem haben wir mit Experten für Cyber-Sicherheit und Behörden wie dem FBI zusammengearbeitet, um unsere Nutzer zu schützen. Die aktuellsten Informationen werden im Folgenden kommuniziert.
SV02 - Canva	CNV_Canva	Reaktionen > Kommunikation	Wir investieren weiterhin stark in die Sicherheit. Wir beabsichtigen, ein technisches Post-Mortem zu diesem Vorfall zu veröffentlichen, sobald unsere Untersuchungen abgeschlossen sind. Der Schutz unserer Nutzer hat für uns jedoch höchste Priorität.So gehen wir vor:
SV02 - Canva	CNV_Canva	Reaktionen > Kommunikation	Benachrichtigung unserer Nutzer: Wir möchten, dass unsere Nutzer wissen, dass sie betroffen sind. Wir haben Nutzer direkt per E-Mail kontaktiert. Einige Nutzer haben aber veraltete oder fehlerhafte E-Mail-Adressen, weshalb wir zudem In-App-Benachrichtigungen und die Presse genutzt haben, um Nutzer auf den Verstoß aufmerksam zu machen. Nach unserer ersten Benachrichtigung senden wir auch individuelle Folge-E-Mails an jeden Nutzer. Darin informieren wir, auf welche Daten zugegriffen wurde.
SV02 - Canva	CNV_Ba	Reaktionen > Maßnahmen > Dritte	The event was significant enough for Miami University to put out a warning to students. In it, IT services encourage students to change their passwords on Canva and any other sites using the same password [15].
SV02 - Canva	CNV_Ba	Reaktionen > Maßnahmen > Opferseitig	Canva noticed the attack as it was happening and they were able to stop it before the hacker was able to steal even more user data [2].
SV02 - Canva	CNV_Ba	Reaktionen > Maßnahmen > Opferseitig	Canva detects the breach and secures it.
SV02 - Canva	CNV_Ba	Reaktionen > Maßnahmen > Opferseitig	From a technical perspective, Canva had a solid response to the breach by Gnosticplayers. They were able to interrupt the attack mid-attempt and most of the data were still encrypted.
SV02 - Canva	CNV_Ba	Reaktionen > Maßnahmen > Opferseitig	Passwords and OAuth tokens that were potentially comprised were all reset. Users not reusing their passwords on different sites is a strong precaution that Canva encouraged after the breach.
SV02 - Canva	CNV_Ba	Reaktionen > Maßnahmen > Opferseitig	Canva also forcibly reset all passwords on their site that had not been changed yet, although users who reused the password on other sites could still be vulnerable
SV02 - Canva	CNV_ZDN	Reaktionen > Maßnahmen > Opferseitig	"They detected my breach and closed their database server."
SV02 - Canva	CNV_CB	Reaktionen > Maßnahmen > Opferseitig	Canva was very responsive throughout, be it in taking the necessary protective measures against the attack or informing the concerned cyber crime cell.
SV02 - Canva	CNV_CB	Reaktionen > Maßnahmen > Opferseitig	Here, the attack was discovered and stopped by Canva while it was still occurring. Canva had immediately shut its database servers on detecting the attack.
SV02 - Canva	CNV_Canva	Reaktionen > Maßnahmen > Opferseitig	Da unveränderte Passwörter genutzt werden könnten, um auf Canva-Konten zuzugreifen, haben wir sofort reagiert und den Zugriff auf Canva-Logins eingeschränkt. Gleichzeitig haben wir damit begonnen, sowohl unveränderte Passwörter ungültig zu machen als auch Nutzer, die mit entschlüsselten Passwörtern auf der Liste aufschienen, zu benachrichtigen.
SV02 - Canva	CNV_Canva	Reaktionen > Maßnahmen > Opferseitig	Am 12.01.2020 haben wir die Passwörter aller Nutzer, die ihr Passwort nach dem 24.05.2019 nicht selbst geändert haben, zurückgesetzt. Diese Nutzer werden bei ihrem nächsten Canva-Login aufgefordert, ihr Passwort zu ändern. Da wir die Passwörter zwangsweise zurücksetzen, benachrichtigen wir kürzlich Canva-Nutzer, die erst kürzlich aktiv waren und deren Passwörter zurückgesetzt wurden, auch direkt.
SV02 - Canva	CNV_Canva	Reaktionen > Maßnahmen > Opferseitig	Betroffene Nutzer müssen ein neues Passwort festlegen, um Canva weiterhin verwenden zu können. Bitte bedenke: Wenn dein Passwort zurückgesetzt wurde, bedeutet das nicht, dass unbefugte Personen auf dein Konto zugegriffen haben. Wir ergreifen diese Vorsichtsmaßnahme, um dein Canva-Konto zu schützen.
SV02 - Canva	CNV_Canva	Reaktionen > Maßnahmen > Opferseitig	Um also unsere Nutzer auf Canva und darüber hinaus zu schützen, haben wir alle unsere Nutzer aufgefordert, ihre Passwörter auf Canva und überall dort, wo sie dasselbe Passwort genutzt haben, zu ändern. Damit wir das Risiko für alle unsere Nutzer reduzieren, haben wir uns mit 1Password zusammengeschlossen. Einerseits bietet 1Password ein Jahr kostenlosen Zugriff auf sein Passwort-Manager-Service, andererseits wurden noch stärkere Passwort-Kontrollen in Canva implementiert.
SV02 - Canva	CNV_Canva	Reaktionen > Maßnahmen > Opferseitig	Seit dem Vorfall haben wir eine Reihe interner Änderungen zum Schutz deiner Daten vorgenommen. In enger Zusammenarbeit mit dem führenden Beratungsunternehmen Mandiant und anderen Partnern haben wir das Ausmaß und die Ursachen des Angriffs ermittelt und Änderungen an unseren Systemen vorgenommen, um eine zusätzliche Schutzbarriere für unsere Nutzer zu schaffen. Zu gegebener Zeit werden wir einen Abschlussbericht zu diesem Vorfall veröffentlichen. Wenn du Fragen hast oder mehr über die neuen Maßnahmen erfahren möchtest, die wir ergriffen haben, um die Sicherheit deiner Daten auf Canva zu gewährleisten, zögere nicht, uns zu kontaktieren.
SV02 - Canva	CNV_Canva	Reaktionen > Maßnahmen > Opferseitig	Am Freitag, den 24. Mai 2019, haben wir einen bösartigen Angriff auf unsere Systeme entdeckt. Diesen haben wir noch während dem Angriff gestoppt. Unsere erste Reaktion war es, Canva zu sperren und dann Behörden und Nutzer über den Vorfall in Kenntnis zu setzen.

Dokumentgruppe	Dokumentname	Code	Segment
SV02 - Canva	CNV_Canva	Reaktionen > Maßnahmen > Opferseitig	Aufforderung zum Ändern des Passworts: Wir haben alle Nutzer, die ihre Passwörter vor dem Angriff eingestellt haben, aufgefordert, sie zu ändern. Zudem führen wir Regeln ein, die unsere Nutzer bei der Wahl eines starken Passworts unterstützen. Zurücksetzen von OAuth-Token: Wir haben mit unseren Partnern zusammengearbeitet, um sicherzustellen, dass alle aktiven Login-Token, die vor dem Angriff bestanden, zurückgesetzt werden. Diese Nutzer werden aufgefordert, ihr Canva-Konto erneut zu verbinden. Koordination mit Partnern: Wir arbeiten mit Partneragenturen, um Informationen über den Angriff zu teilen, das Risiko für Nutzer zu identifizieren und die Reaktionen zu koordinieren. Zum Beispiel warnen wir die Teams für den E-Mail-Missbrauch von großen Anbietern, damit wir Angreifern das Phishing unserer Nutzer erschweren. Partnerschaft mit 1Password: Wir empfehlen unseren Nutzern, dass sie für jede von ihnen genutzte Seite ein anderes Passwort verwenden. Aber wir wissen natürlich, dass das schwer ist. Wir haben uns mit 1Password zusammengetan, um Canva-Nutzern, die ihren Service noch nicht nutzen, ein Jahr lang kostenlos anzubieten.
SV02 - Canva	CNV_Ba	Reaktionen > Vorschläge	Multi-Factor Authentication (MFA) is proven to be the best defense against most password-related attacks, which also includes credential stuffing. According to analysis from Microsoft, it would have stopped 99.9% of account compromises [17].
SV02 - Canva	CNV_Ba	Reaktionen > Vorschläge	Passwordless authentication (PA) verify the user by their ownership factors (something they have) like cellphone, OTP token, or hardware token; or their inherence factor (something they are) like fingerprint, face or voice recognition or retinal scan [18]. Since this method does not involve passwords, it will prevent credential stuffing completely.
SV02 - Canva	CNV_Ba	Reaktionen > Vorschläge	Breached password protection (BPP) makes sure the users' passwords are not in the database of breached credentials such as haveibeenpwned. It will notify the user in the case of breaching and block them from logging in without changing their password.
SV02 - Canva	CNV_Ba	Reaktionen > Vorschläge	1) Secondary Password (SP), PINs and Security Question (SQ): Besides requiring the user to input their password, the application can also prompt them to provide additional security details like a secondary password, answer some predefined security questions, or enter a PIN.
SV02 - Canva	CNV_Ba	Reaktionen > Vorschläge	2) CAPTCHA: CAPTCHA is an effective way to deal against login attempts made from automated tools as they prompt the user to solve a CAPTCHA every time they log in, which will slow the process of credential stuffing considerably. However, since tools for solving CAPTCHA exist, this may not be as effective anymore. One more thing to note is that CAPTCHA may somewhat lower users' experience, so it may be reasonable to use CAPTCHA in suspicious login attempts listed above.
SV02 - Canva	CNV_Ba	Reaktionen > Vorschläge	3) IP Block-listing (IP-BL): Block an IP address after a certain number of failed login attempts as some small attacks usually use a small range of IP addresses.
SV02 - Canva	CNV_Ba	Reaktionen > Vorschläge	4) Device Fingerprinting (DF): Create a fingerprint for a device using multiple factors aside from IP address such as operating system, browser, or language. Login attempts to the account will then be matched with the fingerprint created to see if they match. If not, the user will be prompt to take additional steps for authentication.
SV02 - Canva	CNV_Ba	Reaktionen > Vorschläge	Multi-factor authentication, passwordless authentication, and breached password protection are just some of the methods to defend against credential stuffing and leaked passwords.
SV02 - Canva	CNV_Canva	Reaktionen > Vorschläge	Ändere dein Passwort: Wenn du für Canva ein Passwort hast und dies noch nicht getan hast, empfehlen wir, dass jeder sein Passwort für Canva ändert. Wenn du für andere Websites dasselbe Passwort verwendet hast, solltest du diese ebenfalls ändern. Melde verdächtige E-Mails: Vorsichtshalber ermutigen wir alle, sich vor verdächtigen E-Mails zu hüten. Angreifer nutzen oft kreative Methoden, um dich dazu zu bringen, deine persönlichen Daten herauszugeben. Wenn du E-Mails erhältst, die du für verdächtig hältst, solltest du nicht auf sie klicken und nicht darauf reagieren. Wir empfehlen dir, diese bei deinem E-Mail-Provider zu kennzeichnen. Verwendung eines Passwort-Managers: Wir empfehlen dir, einen Passwort-Manager wie 1Password oder Google Chrome zu verwenden, um ein einzigartiges und sicheres Passwort für jede von dir genutzte Website zu generieren und es dir auch zu merken. Aktualisieren deines Google/Facebook-Logins, wenn wir die Verbindung getrennt haben: Wenn du dich mit Facebook oder Google anmeldest, haben wir möglicherweise deinen Login zurückgesetzt. Logge dich einfach erneut ein, um wieder in dein Canva-Konto einzusteigen. Aktualisiere deine Kontaktdaten: Sobald du dich bei Canva eingeloggt hast, füge bitte deine Kontaktdaten hinzu bzw. aktualisiere sie, damit wir dich bzgl. deines Kontos immer kontaktieren können.
SV02 - Canva	CNV_Ba	Rolle der Kryptografie > Schutz	However, the password data was all encrypted with Bcrypt, which is considered to be one of the most secure forms of encryption.
SV02 - Canva	CNV_Ba	Rolle der Kryptografie > Schutz	most of the data were still encrypted.

Dokumentgruppe	Dokumentname	Code	Segment
SV02 - Canva	CNV_Ba	Rolle der Kryptografie > Schutz	The passwords stolen by GnosticPlayers from Canva were all encrypted using Bcrypt. The Bcrypt algorithm hashes each password and adds random data to ensure the passwords are extra difficult to decrypt and hack. Therefore, to actually access the data, a significant amount of time would have to be spent to decrypt each of the passwords individually [16].
SV02 - Canva	CNV_Ba	Rolle der Kryptografie > Schutz	Resetting passwords before the encryptions are actually bypassed can protect all the users whose data was stolen.
SV02 - Canva	CNV_ZDN	Rolle der Kryptografie > Schutz	For 61 million users, password hashes were also present in the database. The passwords where hashed with the bcrypt algorithm, currently considered one of the most secure password-hashing algorithms around.
SV02 - Canva	CNV_ZDN	Rolle der Kryptografie > Schutz	"We securely store all of our passwords using the highest standards (individually salted and hashed with bcrypt) and have no evidence that any of our users' credentials have been compromised.
SV02 - Canva	CNV_CB	Rolle der Kryptografie > Schutz	Encrypted passwords using bcrypt hashing algorithm. bcrypt is still considered to be one of the most secure algorithms.
SV02 - Canva	CNV_CB	Rolle der Kryptografie > Schutz	Since the passwords had been first salted and then protected with a hashing function called bcrypt, it was considered then that even though the attackers had access to the hashed password they would never be able to decrypt them and recover the original password. bcrypt is one of the strongest hash algorithms there is since its iteration count can be dynamically increased with time to make it slower and thus resistant to brute force attacks.
SV02 - Canva	CNV_CB	Rolle der Kryptografie > Schutz	The OAuth tokens too were encrypted using an algorithm called AES128 and the keys for the same were stored in another separate secure location. There was no evidence that those keys from that location were accessed. And without the keys, the tokens alone wouldn’t prove to be of much use to the attacker.
SV02 - Canva	CNV_Canva	Rolle der Kryptografie > Schutz	verschlüsselten Passwortinformationen
SV02 - Canva	CNV_Canva	Rolle der Kryptografie > Schutz	Zugegriffen wurde auf einzelne salted- und bcrypt-hashed-Passwörter. Für technisch weniger versierte Nutzer: Das ist wie eine super-sichere Türe, die nur von einer Seite aus geöffnet werden kann, und die Passwörter in etwas verwandelt, das unheimlich schwer wieder zurück in das Originalpasswort konvertierbar ist – selbst für die leistungsfähigsten Computer.
SV02 - Canva	CNV_Canva	Rolle der Kryptografie > Schutz	Die Art und Weise, wie wir Passwörter speichern, erschwert das Erraten von Passwörtern erheblich, aber nichts ist unmöglich und es wird umso einfacher, die Passwörter zu erraten, wenn die Passwörter einfach gestrickt sind (wie z. B. password123456! oder Alex1997.
SV02 - Canva	CNV_Canva	Rolle der Kryptografie > Schutz	Sie haben auf kryptografisch geschützte Passwörter (diese waren einzelne salted- und bcrypt-hashed-Passwörter) von jedem dieser Nutzer mit Usernamen/Passwort-Logins zugegriffen.
SV02 - Canva	CNV_Canva	Rolle der Kryptografie > Schutz	Sie haben behauptet, dass sie OAuth-Login-Token von Nutzern hatten, die sich über Google angemeldet haben. Unsere OAuth-Token sind mit AES128 verschlüsselt. Die Verschlüsselungsdaten werden sicher an einem anderen Ort verwahrt. Wir haben keine Beweise dafür gefunden, dass sie die OAuth -Token heruntergeladen oder versucht haben, auf die Schlüssel zuzugreifen.
SV02 - Canva	CNV_Ba	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	Jan 11 2020 · · ·• 4 million decrypted passwords from the breach are shared online.
SV02 - Canva	CNV_Ba	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	Credential cracking, also known as brute force attack, is an attack using automated tools to test different values of usernames and passwords in order to find valid credential sets. This method usually utilizes common or simple password phrases, so it is pose to be useful against users with simple and easily guessable passwords.
SV02 - Canva	CNV_Ba	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	It was confirmed on January 11, 2020, by Canva that "a list of approximately 4 million Canva accounts containing user passwords stolen as part of the May 24 breach ... had been decrypted and recently shared online”
SV02 - Canva	CNV_Ba	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	Currently, only a small percentage of the data stolen by GnosticPlayers is known to be decrypted.
SV02 - Canva	CNV_CB	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	4 million accounts whose passwords had also been successfully decrypted by the hacker.
SV02 - Canva	CNV_CB	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	It was only on the 11th of January 2020, 7 months after the attack that the company became aware that the hacker had been able to decrypt the passwords of as many as 4 million Canva accounts out of the 139 million accounts that had been compromised by the breach
SV02 - Canva	CNV_Canva	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	Liste von rund 4 Millionen Canva-Konten, deren Passwörter im Rahmen der Datenangriffs vom 24. Mai gestohlen wurden (siehe untenstehende Anmerkungen vom 1. Juni 10:13 AEST). Die Passwörter wurden entschlüsselt und kürzlich online veröffentlicht.
SV02 - Canva	CNV_Canva	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	Es scheint, dass sie zu diesem Zeitpunkt mithilfe ihrer Ressourcen versucht haben, diese Passwörter zu knacken. Passwörter der rund 4 Millionen Canva-Konten, die vom Vorfall im Mai 2019 betroffen waren, wurden nun entschlüsselt.
SV02 - Canva	CNV_Ba	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Using code repositories from developers' Github account, Gnosticplayers were able to find AWS keys and similar credentials that allow them to access the database of Canva and get the information they want from the database server.

Dokumentgruppe	Dokumentname	Code	Segment
SV03 - Capital One	CO_Neto	Angreifer > Einzelne	Despite the strong investments on IT infrastructure, in July 2019 Capital One disclosed that the company had sensitive customer data assessed by an external individual.
SV03 - Capital One	CO_Neto	Angreifer > Einzelne	“Federal agents have arrested a Seattle woman named Paige A. Thompson for hacking into cloud computing servers rented by Capital One
SV03 - Capital One	CO_Khan	Angreifer > Einzelne	Further details revealed that the incident was caused by the unauthorized access to a Capital One data server by a former software engineer of Amazon Web Services (AWS), Paige A. Thompson—the primary suspect in the case [20].
SV03 - Capital One	CO_ZDN	Angreifer > Einzelne	In a separate announcement, the US Attorney's Office for the Western District of Washington said it had arrested a "former Seattle technology company software engineer" in relation to the breach. The accused suspect, Paige Thompson who uses the handle erratic, appeared in US District Court on Monday and is pending a hearing on August 1.
SV03 - Capital One	CO_KoS_2	Angreifer > Einzelne	On Monday, a former Amazon employee was arrested and charged with stealing more than 100 million consumer applications for credit from Capital One.
SV03 - Capital One	CO_KoS_1	Angreifer > Einzelne	On July 29, FBI agents arrested Paige A. Thompson on suspicion of downloading nearly 30 GB of Capital One credit application data from a rented cloud data server.
SV03 - Capital One	CO_CapOne	Angreifer > Einzelne	we determined that an outside individual gained unauthorized access and obtained certain types of personal information
SV03 - Capital One	CO_Neto	Fehler > Menschliches Versagen	The misconfiguration issues for some reason have not been detected and avoided by the security controls that Capital One claims to implement. A human error might be a cause.
SV03 - Capital One	CO_Neto	Fehler > Organisatorische Schwächen	AWS said its cloud unit that stored the data was not compromised in any way. Instead, it attributed the breach to a “misconfiguration” outside of the cloud. Capital One attributed the problem to an error in its own infrastructure (Henry, Capital One customer data breach rattles investors, 2019).
SV03 - Capital One	CO_Neto	Fehler > Organisatorische Schwächen	Even before the incident, some Capital One cyber staff raised concerns about employees morale: “employees raised concerns within the company about what they saw as high turnover in its cybersecurity unit and a failure to promptly install some software to help spot and defend against hacks (…)
SV03 - Capital One	CO_Neto	Fehler > Organisatorische Schwächen	Technology employees had at times been given free rein to write in many coding languages — so many that it made it harder for the cybersecurity unit to spot problems.” (
SV03 - Capital One	CO_Neto	Fehler > Organisatorische Schwächen	The study of the Capital One incident showed that the company failed to implement proper security controls. It also demonstrated that the NIST Framework would have been sufficient to mitigate the incident, if there were enough compliance controls in place to identify the unauthorized access and data exfiltration during the entire chain of events.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	Considered together, this means that this attack was successful, not because of its novelty, but because of a number of control failures at various levels of the organization, any one of which, if adequately enforced, would have been able to prevent the attack or at the very least would have been able to limit the scale of the breach.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	it is speculated that the role attached to the instance (ISRM-WAF-Role) also allowed decryption of data (since it most likely had kms:decrypt privilege as well).
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	

Cyber Kill Chain Phase	#	System-level Hazard	Constraint Violated
Delivery	H-1	System does not have adequate protection against delivery of an exploit (i.e., inadequate protections in place to prevent delivery of SSRF, reverse proxy attack, etc.)	System must have adequate protections against delivery of SSRF, reverse proxy attacks
	H-2	System has inadequate intrusion detection and monitoring in place, i.e., system does not detect an intrusion by an attacker and does not monitor IAM API calls or reading/writing of sensitive S3 buckets	System must have adequate intrusion detection and monitoring systems in place to detect anomalous behavior
Exploitation	H-3	System is operated with an exploitable vulnerability or a misconfigured resource that allows access to backend resources	System must not be operated with an exploitable vulnerability or a misconfigured resource that allows access to backend resources
Command & Control	H-4	System access control is overly permissive beyond least privilege	System access control must follow the principles of least privilege
	H-5	System does not prevent unauthorized user from harvesting credentials and establishing control over resources	System must have an adequate mechanism to protect access to credentials
Action on Objectives	H-6	System does not adequately encrypt sensitive data	System must adequately encrypt sensitive data

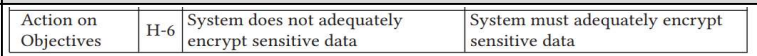
Dokumentgruppe	Dokumentname	Code	Segment
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	IAM team also failed in assigning the correct level of permissions to the “role” associated with the EC2 instance running the WAF
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	In addition, it did not effectively monitor IAM security policies and roles, leading to existence of overly permissive security groups.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	One plausible scenario that explains why a misconfiguration or vulnerable application made it to production is that the shift in focus into a tech-centric company coupled with a sudden increase in tech talent (that may not be steeped in security knowledge) may have led to an unintended “lowering of guard” on security, in preference for speed of development in the collective process model of the IT team.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	could explain why a vulnerable application was pushed into a production environment without undergoing sufficient application code reviews/testing by the DevOps team
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	Another plausible scenario is that, given the sheer size and complexity of the cloud infrastructure, the IT team just did not have full visibility of all its data; this limitation was known to upper management but the risk was considered acceptable.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	the IT team received tools, guidelines, and best practices from the cloud service provider (AWS). Under the shared-responsibility model (described in more detail in Section 4.2.2.3), Capital One’s IT team was expected to build its applications and ensure their security atop infrastructure and tools that it did not control (i.e., it was responsible for security in the cloud) while AWS was responsible for “security of the cloud,” i.e., the underlying infrastructure.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	Since the IT team did not control the underlying infrastructure, they would have believed that AWS best practices and guidelines were complete and following them would guarantee security. Evan Johnson (manager of product security team at Cloudflare) states [19], “There’s a lot of specialized knowledge that comes with operating a service within AWS, and to someone without specialized knowledge of AWS, [SSRF attacks are] not something that would show up on any critical configuration guide.” This indicates that following the AWS best practices and guidelines without specialized security knowledge could in fact have led to the vulnerability remaining unaddressed.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	Second, from a functional control structure point of view, the overreliance on AWS best practices by the IT/DevOps team points to an additional weakness within the control structure—insufficient coordination and communication between the information security team and the development team.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	This indicates that rather than following the “secure by design” principle and “baked-in security,” the IT/development team followed a “bolted-on security” approach, relying on multiple layers of defense, but not considering the interactions between those layers. The flawed belief here is that at least one of the layers would be able to stop the breach.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	Third, there may have been an incorrect belief in the principle of “security by obscurity,” i.e., that the environment was so complex that it was unlikely to be breached by an attacker without insider specialized knowledge. In the case of the Capital One breach, the attacker, having previously worked at AWS, indeed was knowledgeable about configuration vulnerabilities that organizations were routinely subject to, which she targeted.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	The InfoSec team failed on a number of counts in fulfilling its roles and responsibilities. For one, the InfoSec team failed to enforce periodic preventive vulnerability scanning that would have highlighted the vulnerability.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	Second, the InfoSec team had inadequate detection and monitoring in place; they did not know that an intruder lurked in their network for over 127 days and exfiltrated large amounts of data. Once the breach was reported by a white hat hacker, they were able to confirm the breach and network intrusion fairly quickly. This raises the question, “why the InfoSec team was not monitoring the network access logs in the first place?”
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	These inadequacies can be partly explained by examining the context in which the InfoSec team operated. As mentioned previously, Capital One had a strong tech-centric culture even before it unveiled its cloud strategy in [40]. The Wall Street Journal [40] reports that “Technology employees had at times been given free rein to write in many coding languages—so many that it made it harder for the cybersecurity unit to spot problems.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	According to the Wall Street Journal report [40], a third of the employees in the cybersecurity team left in 2018. Although Capital One reported significant investments in cybersecurity, there is evidence that lends credence to the existence of a high stress/workload, understaffed, and highturnover environment. For instance, in late 2017, the company bought a software called Endgame to improve its ability to detect a breach, but even after a year, the company had not finished installing the software—indicating high workload issues [40]. High turnover coupled with Capital One’s commitment to developing and using open-source technology [34] (which can at times be more difficult to configure and requires more in-depth knowledge of the underlying process) may have created an error-prone environment.

Dokumentgruppe	Dokumentname	Code	Segment
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	We can also speculate on one process model flaw that might have prevented the InfoSec team from enforcing the requisite constraints—there may have been a belief that the layered defense approach was resilient enough to prevent a large-scale breach. After all, Capital One was following AWS best practices—a WAF was deployed, IAM was used for authentication of users and instances, and the data was encrypted. The problem is that, as was demonstrated by the breach, due to the complexity of the environment, a checkbox approach was simply not sufficient. Individually, each of the components behaved exactly as they were designed to do, but as a system, failed miserably. Given this context and the process model flaws, it is easy to understand why the WAF was left misconfigured and why the network access logs were not being actively monitored.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	Although the Capital One breach was ultimately blamed on a “misconfigured firewall,” many of the policies and decisions taken by senior leadership, years before, created the conditions necessary for the breach. Insofar as cybersecurity is concerned, the primary responsibility of senior leadership was to provide a meaningful cybersecurity strategy and allocate sufficient resources to achieve their security goals in their transition to the cloud based on adequate risk assessment and management processes.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	Capital One’s [48, 49] annual reports provide evidence that the company continuously acknowledged its increased risk exposure due to the outsourcing of substantial amount of infrastructure to AWS. The company also realized that it may specifically face an increasing number of cyberattacks as it expands its used of cloud technologies (p.24 [48]). This validates the assumption that the management was in fact aware of the increased risks associated with migration to the cloud (p.23 [48], p.40 [49]).
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	However, the senior leadership failed to establish adequate risk management processes for its cloud strategy, “including appropriate design and implementation of network security controls, adequate data loss prevention controls, and effective intrusion detection and monitoring controls” [13].
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	One of the reasons for this inadequate action could be a flawed process model. Note that the functional control diagram (Figure 3) shows interactions between senior leadership and AWS. Given that the senior leadership understood the increased risks of migrating to the cloud, the flawed process model could be a result of a misunderstanding of the cloud shared responsibility model. This potentially led to a blind trust and pure reliance on the cloud provider’s security model. The assumption being that AWS was much better equipped to ensure security of the infrastructure as well as respond to security incidents than Capital One itself (in the cloud as well as on premise). Therefore, Capital One could focus on the rest of the stack instead, i.e., focus on developing applications to enhance user experience. In fact, one month before the breach, the company’s CEO, Richard Fairbank, said, “A lot of how we built our company is not by studying banking, but by forgetting about banking” [50]; indicating an inherent trust in the security of the underlying cloud infrastructure.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	This inherent trust in the cloud provider’s security model potentially also led to an elevated risk appetite stemming from use of new technologies. The fact that the company enhanced its cybersecurity governance after the incident lends credence to this hypothesis. The 2019 annual report [49] notes that the leadership established a senior management level committee mandated to support reporting of cybersecurity-related issues to the Board to fulfill OCC’s consent order.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	This strategy included reducing technology (data center) costs while taking advantage of the cloud’s rapid scalability and ever-increasing array of applications. The success of this strategy, however, was predicated on the bank’s ability to aggressively attract and acquire tech talent. For this, the company’s leadership committed to some bold decisions including open-source technology, agile development philosophy, and transition to the public cloud
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	Likewise, the commitment to public cloud (in direct contradiction to industry practice) in conjunction with acquisition of tech talent and blatant push by senior management to “not think like a bank” inadvertently increased the appetite for riskier approaches. The emergent consequence of this strategy (agile, open-source, and public cloud) was an unintended shift in priorities to speed and cost to develop new applications at the expense of security of those applications, which is clearly evident in the multiple control failures of the Capital One breach.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	one potential process model flaw is obvious; the board did not have a direct communication channel (feedback) with the CISO to receive information about potential risks from the company’s main security defender.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	the board probably missed to prioritize the importance of the cyber risk management related to the new technology-related risks, including cloud-related security risks, despite acknowledging their existence. We suppose that the weak feedback loop mentioned above was the major cause of it.

Dokumentgruppe	Dokumentname	Code	Segment
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	The second demand was to reassess the quality and transparency of cyber and technology risk reporting at the board level. Since the company included the CISO in the meetings with the board as a reaction to the cyber breach, we may conclude that prior to the breach, cyber risks were not comprehensively covered in the communications received by the board. They could have been potentially limited to providing formal reports to meet compliance requirements, but not revealing actual risks. These two facts have led us to believe that despite establishing cyber risk management practices, the maturity of these practices was insufficient to identify and address risks emerging from the adoption of new technologies. This was an unexpected finding, given that one of the board members was the former CISO of Amazon—a leader in cloud computing business.
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	These requirements have highlighted another deficiency in the company's risk management practice—internal audit. OCC identified that internal audit failed to identify numerous control weaknesses in the cloud operating environment and did not report on the identified weaknesses and gaps to the board audit committee. Moreover, some concerns raised by internal audit did not find an appropriate reaction from the board that failed to hold management accountable for the resolution of the issues [13].
SV03 - Capital One	CO_Khan	Fehler > Organisatorische Schwächen	In summary, we can conclude that the formal adherence to the principles of cyber risk management at the board level itself is not sufficient to effectively prevent a data breach.
SV03 - Capital One	CO_ZDN	Fehler > Organisatorische Schwächen	access was due to a misconfigured web application firewall.
SV03 - Capital One	CO_KoS_2	Fehler > Organisatorische Schwächen	the problem stemmed in part from a misconfigured open-source Web Application Firewall (WAF) that Capital One was using as part of its operations hosted in the cloud with Amazon Web Services (AWS).
SV03 - Capital One	CO_KoS_2	Fehler > Organisatorische Schwächen	In AWS, exactly what those credentials can be used for hinges on the permissions assigned to the resource that is requesting them. In Capital One's case, the misconfigured WAF for whatever reason was assigned too many permissions, i.e. it was allowed to list all of the files in any buckets of data, and to read the contents of each of those files.
SV03 - Capital One	CO_KoS_2	Fehler > Organisatorische Schwächen	"The intrusion was caused by a misconfiguration of a web application firewall and not the underlying infrastructure or the location of the infrastructure," the statement reads.
SV03 - Capital One	CO_SNK	Fehler > Organisatorische Schwächen	As Capital One outlined in their public announcement, the attack occurred due to a misconfiguration error at the application layer of a firewall installed by Capital One, exacerbated by permissions set by Capital One that were likely broader than intended.
SV03 - Capital One	CO_SNK	Fehler > Organisatorische Schwächen	Much has been made of the likely SSRF aspect of the breach, but as AWS makes clear, it was not the primary factor in the attack. Overly permissive configuration of cloud resources was.
SV03 - Capital One	CO_SNK	Fehler > Organisatorische Schwächen	misconfigured firewall in the Capital One AWS environment.
SV03 - Capital One	CO_SNK	Fehler > Organisatorische Schwächen	It's possible that an SSH port was opened for a maintenance window, or perhaps the server in question was left over from development efforts and no longer in use. Another possibility is that the server was running an application such as MongoDB or ElasticSearch that require an open port to function, but which should never have been exposed to the Internet via the firewall
SV03 - Capital One	CO_Khan	Fehler > Versäumnisse von Dritten	While it is true that in the Capital One breach the underlying infrastructure was not compromised, weaknesses within the design of the infrastructure were leveraged by the attacker. For instance, by design, the AWS metadata service (IMDSv1) does not verify the legitimacy of an APIrequest coming from an EC2 instance. The process model flaw here is that there is assumed trust in the security of the cloud—a call originating from a compromised instance is inherently trusted.
SV03 - Capital One	CO_Khan	Fehler > Versäumnisse von Dritten	AWS failed on two counts with respect to this weakness—both of which have been largely dismissed by the company [26]. First, AWS did not implement countermeasures in the metadata service against SSRF and open proxy attacks that leverage this weakness despite knowing about these vulnerabilities, since at least 2018 (and despite its competitors offering some level of security against these vulnerabilities) [43]. In fact, AWS updated its metadata access service four months after the Capital One breach, taking countermeasures against these vulnerabilities.
SV03 - Capital One	CO_Khan	Fehler > Versäumnisse von Dritten	Second, AWS did not provide sufficient guidance to protect against these vulnerabilities to its customers, disclaiming any responsibility under the shared-responsibility model. Evan Johnson [19] notes, "The impact of SSRF is being worsened by the offering of public clouds, and the major players like AWS are not doing anything to fix it. The problem is common and well-known, but hard to prevent and does not have any mitigations built into the AWS platform."
SV03 - Capital One	CO_Neto	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	Capital One data breach incident
SV03 - Capital One	CO_Neto	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	However, the company only identified the attack on July 19, resulting in a data breach that affected 106 million customers (100 million in the U.S. and 6 million in Canada) (Capital One, 2019).
SV03 - Capital One	CO_Khan	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	The 2019 Capital One data breach was one of the largest data breaches impacting the privacy and security of personal information of over a 100 million individuals
SV03 - Capital One	CO_Khan	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	one of the worst data breaches

Dokumentgruppe	Dokumentname	Code	Segment
SV03 - Capital One	CO_ZDN	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	data breach
SV03 - Capital One	CO_ZDN	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	data theft,
SV03 - Capital One	CO_KoS_2	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	Since then, many have speculated the breach was perhaps the result of a previously unknown “zero-day” flaw, or an “insider” attack in which the accused took advantage of access surreptitiously obtained from her former employer.
SV03 - Capital One	CO_KoS_1	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	Capital One incident contains the hallmarks of many other modern data breaches
SV03 - Capital One	CO_Neto	Gemeinsamkeiten > Branche > Direkt Betroffene	U.S. bank Capital One
SV03 - Capital One	CO_Neto	Gemeinsamkeiten > Branche > Direkt Betroffene	Capital One is the fifth largest consumer bank in the U.S. and eighth largest bank overall (Capital One, 2020), with approximately 50 thousand employees and 28 billion US dollars in revenue in 2018 (Capital One, 2019).
SV03 - Capital One	CO_Khan	Gemeinsamkeiten > Branche > Direkt Betroffene	the bank routinely collected for its credit card applications,
SV03 - Capital One	CO_Neto	Gemeinsamkeiten > Schwachstelle	Thompson created a scanning software tool that allowed her to identify servers hosted in a cloud computing company with misconfigured firewalls, allowing the execution of commands from outside to penetrate and to access the servers.
SV03 - Capital One	CO_Neto	Gemeinsamkeiten > Schwachstelle	“A firewall misconfiguration allowed commands to reach and to be executed at Capital One’s server, which enabled access to folders or buckets of data in a storage space at the Cloud Computing Company”
SV03 - Capital One	CO_Neto	Gemeinsamkeiten > Schwachstelle	After analyzing the records of the Seattle Court, cloud security company CloudSploit published an analysis of the incident in its corporate blog (CloudSploit, 2019), describing that the access to the vulnerable server was possible thanks to a Server-Side Request Forgery (SSRF) attack3 that was made possible due to a configuration failure in the Web Application Firewall (WAF) solution employed by Capital One
SV03 - Capital One	CO_Neto	Gemeinsamkeiten > Schwachstelle	The SSRF attack allowed the criminal to trick the server into executing commands as a remote user, which gave the attacker access to a private server;
SV03 - Capital One	CO_Neto	Gemeinsamkeiten > Schwachstelle	The WAF misconfiguration allowed the intruder to trick the firewall into relaying commands to a default back-end resource on the AWS platform, known as the metadata service (accessed through the URL http://169.254.169.254);
SV03 - Capital One	CO_Khan	Gemeinsamkeiten > Schwachstelle	a misconfigured web application firewall enabled exfiltration of sensitive private credit card application data.
SV03 - Capital One	CO_Khan	Gemeinsamkeiten > Schwachstelle	the attack did not include any significantly novel technique (i.e., a zero-day exploit), but rather exploited a number of well-understood vulnerabilities, including a Server-Side Request Forgery (SSRF) [5] and a weakness in the AWS EC2 service infrastructure [6]
SV03 - Capital One	CO_Khan	Gemeinsamkeiten > Schwachstelle	The initial entry point in the breach was the WAF
SV03 - Capital One	CO_ZDN	Gemeinsamkeiten > Schwachstelle	configuration vulnerability that this individual exploited
SV03 - Capital One	CO_ZDN	Gemeinsamkeiten > Schwachstelle	access was due to a misconfigured web application firewall.
SV03 - Capital One	CO_ZDN	Gemeinsamkeiten > Schwachstelle	firewall configuration allowed commands to be executed on a server that enabled access to "buckets of data".
SV03 - Capital One	CO_KoS_2	Gemeinsamkeiten > Schwachstelle	Known as “ModSecurity,” this WAF is deployed along with the open-source Apache Web server to provide protections against several classes of vulnerabilities that attackers most commonly use to compromise the security of Web-based applications.
SV03 - Capital One	CO_KoS_2	Gemeinsamkeiten > Schwachstelle	The misconfiguration of the WAF allowed the intruder to trick the firewall into relaying requests to a key back-end resource on the AWS platform. This resource, known as the “metadata” service, is responsible for handing out temporary information to a cloud server, including current credentials sent from a security service to access any resource in the cloud to which that server has access.
SV03 - Capital One	CO_KoS_2	Gemeinsamkeiten > Schwachstelle	The type of vulnerability exploited by the intruder in the Capital One hack is a well-known method called a “Server Side Request Forgery” (SSRF) attack, in which a server (in this case, CapOne’s WAF) can be tricked into running commands that it should never have been permitted to run, including those that allow it to talk to the metadata service.
SV03 - Capital One	CO_KoS_2	Gemeinsamkeiten > Schwachstelle	Evan Johnson, manager of the product security team at Cloudflare, recently penned an easily digestible column on the Capital One hack and the challenges of detecting and blocking SSRF attacks targeting cloud services. Johnson said it’s worth noting that SSRF attacks are not among the dozen or so attack methods for which detection rules are shipped by default in the WAF exploited as part of the Capital One intrusion.
SV03 - Capital One	CO_KoS_2	Gemeinsamkeiten > Schwachstelle	“SSRF has become the most serious vulnerability facing organizations that use public clouds,” Johnson wrote. “The impact of SSRF is being worsened by the offering of public clouds, and the major players like AWS are not doing anything to fix it. The problem is common and well-known, but hard to prevent and does not have any mitigations built into the AWS platform.”

Dokumentgruppe	Dokumentname	Code	Segment
SV03 - Capital One	CO_KoS_1	Gemeinsamkeiten > Schwachstelle	“The attacker was a former employee of the web hosting company involved, which is what is often referred to as insider threats,” Watson said. “She allegedly used web application firewall credentials to obtain privilege escalation. Also the use of Tor and an offshore VPN for obfuscation are commonly seen in similar data breaches.”
SV03 - Capital One	CO_SNK	Gemeinsamkeiten > Schwachstelle	the attack occurred due to a misconfiguration error at the application layer of a firewall installed by Capital One, exacerbated by permissions set by Capital One that were likely broader than intended. After gaining access through the misconfigured firewall and having broader permission to access resources, we believe a SSRF attack was used (which is one of several ways an attacker could have potentially gotten access to data once they got in through the misconfigured firewall.
SV03 - Capital One	CO_SNK	Gemeinsamkeiten > Schwachstelle	"A firewall misconfiguration permitted commands to reach and be executed by that server, which enabled access to folders or buckets... (III.A.10)"
SV03 - Capital One	CO_SNK	Gemeinsamkeiten > Schwachstelle	It seems that a dangerous port was left open on whichever firewall type was in use, and this might have been the initial opening for the attack
SV03 - Capital One	CO_ZDN	Reaktionen > Kommunikation	It added the configuration vulnerability was disclosed to it by an external security researcher, which led to an internal investigation and discovery of the incident.
SV03 - Capital One	CO_CapOne	Reaktionen > Kommunikation	Like many companies, we have a Responsible Disclosure Program which provides an avenue for ethical security researchers to report vulnerabilities directly to us. The configuration vulnerability was reported to us by an external security researcher through our Responsible Disclosure Program on July 17, 2019. We then began our own internal investigation, leading to the July 19, 2019, discovery of the incident.
SV03 - Capital One	CO_CapOne	Reaktionen > Kommunikation	We have directly notified by mail the U.S. individuals whose Social Security numbers or linked bank account numbers were accessed. We also have notified all Canadian customers affected. Canadian customers can find more information at www.capitalone.ca/facts2019 or www.capitalone.ca/facts2019/fr.
SV03 - Capital One	CO_CapOne	Reaktionen > Kommunikation	Capital One is not proactively calling, texting or emailing customers to ask for account information or Social Security numbers related to this cyber incident.
SV03 - Capital One	CO_CapOne	Reaktionen > Kommunikation	We have notified by mail all individuals whose Social Security numbers or linked bank account numbers were accessed. The outside individual who took the data was captured by the FBI. The government has stated they believe the data has been recovered and that there is no evidence the data was used for fraud or shared by this individual.
SV03 - Capital One	CO_Neto	Reaktionen > Maßnahmen > Dritte	A class action lawsuit seeking unspecified damages was filed just days after the breach became public (Reeves, 2019).
SV03 - Capital One	CO_KoS_2	Reaktionen > Maßnahmen > Dritte	as the company is already facing a class action lawsuit over the breach and is likely to be targeted by more lawsuits going forward.
SV03 - Capital One	CO_Neto	Reaktionen > Maßnahmen > Opferseitig	In addition to the many negative consequences for the image and stock after the incident, Capital One also changed its chief information security officer out of the role.
SV03 - Capital One	CO_ZDN	Reaktionen > Maßnahmen > Opferseitig	Capital One said it became aware of the access on July 19, and that it "immediately fixed the configuration vulnerability that this individual exploited". It added that the individual that accessed the records is now arrested and in custody.
SV03 - Capital One	CO_KoS_1	Reaktionen > Maßnahmen > Opferseitig	“The good news, however, is that Capital One Incidence Response was able to move quickly once they were informed of a possible breach via their Responsible Disclosure program
SV03 - Capital One	CO_KoS_1	Reaktionen > Maßnahmen > Opferseitig	In Capital One’s statement about the breach, company chairman and CEO Richard D. Fairbank said the financial institution fixed the configuration vulnerability that led to the data theft and promptly began working with federal law enforcement.
SV03 - Capital One	CO_KoS_1	Reaktionen > Maßnahmen > Opferseitig	Capital One says it will notify affected individuals via a variety of channels, and make free credit monitoring and identity protection available to everyone affected.
SV03 - Capital One	CO_CapOne	Reaktionen > Vorschläge	Customers are encouraged to enroll in credit card account alerts to help them keep track of activity on their accounts. Customers can sign in to online banking and set up text or email alerts, based on their preferences. Additionally, we encourage customers to monitor their credit card accounts for unusual or suspicious activity and, if they notice any activity that they do not recognize, to call the number on the back of their Capital One card or on their statement as soon as possible.
SV03 - Capital One	CO_Neto	Rolle der Kryptografie > Schutz	Capital One reported via a press release (PRNewswire, 2019) that some of the stolen data was encrypted but the company did not provide any detail on how it was possible for the attacker to access the information: “We encrypt our data as a standard.
SV03 - Capital One	CO_Khan	Rolle der Kryptografie > Schutz	Capital One operated a state-of-the-art cloud infrastructure using encryption and tokenization.
SV03 - Capital One	CO_Khan	Rolle der Kryptografie > Schutz	Capital One announced “We encrypt our data as a standard.
SV03 - Capital One	CO_Khan	Rolle der Kryptografie > Schutz	Note that the official announcement by Capital One about the breach [12] stated that out of the 100 million affected customers in the US, Social Security numbers (SSN) for about 1% were exposed and out of the 6 million Canadian customers, 1 million (about 16%) social insurance numbers were exposed; the rest were protected due to application of a post-compromise protection measure7 [38] known as tokenization.8

Dokumentgruppe	Dokumentname	Code	Segment
SV03 - Capital One	CO_Khan	Rolle der Kryptografie > Schutz	The fact that Capital One employed post-compromise protections (in the form of tokenization) indicates that the company understood that it would not be able to watch every piece of data that resided on the cloud [37] and needed the additional layers of defense.
SV03 - Capital One	CO_Khan	Rolle der Kryptografie > Schutz	Post-compromise security refers to protection of user data after the encryption key has been compromised.
SV03 - Capital One	CO_Khan	Rolle der Kryptografie > Schutz	Tokenization refers to the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token, that has no extrinsic or exploitable meaning or value.
SV03 - Capital One	CO_ZDN	Rolle der Kryptografie > Schutz	"It is also our practice to tokenize select data fields, most notably Social Security numbers and account numbers," Capital One said. "Tokenization involves the substitution of the sensitive field with a cryptographically generated replacement. The method and keys to unlock the tokenized fields are different from those used to encrypt the data. Tokenized data remained protected."
SV03 - Capital One	CO_Khan	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	the ineffectiveness of the encryption method used
SV03 - Capital One	CO_Khan	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	
SV03 - Capital One	CO_Khan	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	Hazard H-6 refers to use of inadequate encryption techniques to store sensitive data.
SV03 - Capital One	CO_Khan	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	IAM team also failed in assigning the correct level of permissions to the “role” associated with the EC2 instance running the WAF and did not adequately encrypt the data (leading to leakage of sensitive personal identifiable information (PII)
SV03 - Capital One	CO_Neto	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	Due to the particular circumstances of this incident, the unauthorized access also enabled the decrypting of data.”
SV03 - Capital One	CO_Khan	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	the compromised data was stored on the public cloud and was supposedly encrypted; however, the particular circumstances surrounding this breach enabled the attacker to decrypt the data as well
SV03 - Capital One	CO_Khan	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	Although the data was encrypted, the intruder was able to decrypt the data as well.
SV03 - Capital One	CO_ZDN	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	Although Capital One said its data was encrypted, the attacker was able to decrypt it.
SV05 - BigBasket	BB_TC	Angreifer > Einzelne	A hacker who goes by the name ShinyHunters published the alleged BigBasket database
SV05 - BigBasket	BB_BC	Angreifer > Einzelne	well-known seller of data breaches known as ShinyHunters
SV05 - BigBasket	BB_BC	Fehler > Versäumnisse von Dritten	Another member claims that 700k of the customers used the password 'password' for their accounts.
SV05 - BigBasket	BB_SA	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	allegedly suffered a data breach
SV05 - BigBasket	BB_SA	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	Bigbasket has allegedly suffered a data breach
SV05 - BigBasket	BB_SA	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	became victim to a data breach.
SV05 - BigBasket	BB_TC	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	data breach.
SV05 - BigBasket	BB_SA	Gemeinsamkeiten > Branche > Direkt Betroffene	Bigbasket, a prominent online grocery store in India
SV05 - BigBasket	BB_SA	Gemeinsamkeiten > Branche > Direkt Betroffene	Grocery e-commerce website Bigbasket
SV05 - BigBasket	BB_SA	Gemeinsamkeiten > Branche > Direkt Betroffene	Big Basket, India’s leading online food and grocery store
SV05 - BigBasket	BB_BC	Gemeinsamkeiten > Branche > Direkt Betroffene	BigBasket is a popular Indian online grocery delivery service
SV05 - BigBasket	BB_BC	Reaktionen > Kommunikation	“There’s been a data breach and we’ve filed a case with the cybercrime police,” BigBasket CEO Hari Menon told Bloomberg News. “The investigators have asked us not to reveal any details as it might hamper the probe.”
SV05 - BigBasket	BB_SA	Rolle der Kryptografie > Schutz	password hashes (potentially hashed OTPs)
SV05 - BigBasket	BB_TC	Rolle der Kryptografie > Schutz	We had eliminated all hashed passwords from our system and moved to a secure OTP-based authentication mechanism quite some time back.
SV05 - BigBasket	BB_BC	Rolle der Kryptografie > Schutz	leaked approximately 20 million BigBasket user records containing personal information and hashed passwords
SV05 - BigBasket	BB_BC	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	The database includes BigBasket customer information, including email addresses, SHA1 hashed passwords
SV05 - BigBasket	BB_TC	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	In newer posts on the forum, at least two threat actors claimed that they had decoded the hashed passwords and had put them up for sale

Dokumentgruppe	Dokumentname	Code	Segment
SV05 - BigBasket	BB_BC	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	The passwords are hashed using the SHA1 algorithm, and forum members have claimed to crack 2 million of the listed passwords already.
SV05 - CAM4	CM4_Sorn	Angreifer > Unbekannt	It is worth mentioning that there is no evidence that suggests the website was maliciously broken by unauthorized users
SV05 - CAM4	CM4_Wired	Fehler > Menschliches Versagen	"The server in question was a log aggregation server from a bunch of different sources, but server was considered non-confidential," says Krieg. "The 93 records got into the logs due to a mistake by a developer who was looking to debug an issue, but accidentally logged those records when an error happened to that log file."
SV05 - CAM4	CM4_BC	Fehler > Organisatorische Schwächen	The sensitive data was leaked after one of the site's production databases was left open to Internet access on a misconfigured Elasticsearch cluster, with records dating back to March 16, 2020.
SV05 - CAM4	CM4_BC	Fehler > Organisatorische Schwächen	While ElasticSearch's dev team explained in December 2013 that Elastisearch servers should never be accessible from the Internet but instead configured for local access only, admins often forget this and expose highly sensitive data publicly, with no proper security controls.
SV05 - CAM4	CM4_Wired	Fehler > Organisatorische Schwächen	The mistake CAM4 made is also not unique. ElasticSearch server goofs have been the cause of countless high-profile data leaks. What typically happens: They're intended for internal use only, but someone makes a configuration error that leaves it online with no password protection.
SV05 - CAM4	CM4_BC	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	The sensitive data was leaked
SV05 - CAM4	CM4_SD	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	data leak
SV05 - CAM4	CM4_BC	Gemeinsamkeiten > Branche > Direkt Betroffene	Adult live streaming website CAM4
SV05 - CAM4	CM4_SD	Gemeinsamkeiten > Branche > Direkt Betroffene	CAM4 is a live streaming “cam model” website providing explicit content intended only for adults.
SV05 - CAM4	CM4_Wired	Gemeinsamkeiten > Branche > Direkt Betroffene	adult livestreaming service
SV05 - CAM4	CM4_Wired	Gemeinsamkeiten > Branche > Direkt Betroffene	adult platform
SV05 - CAM4	CM4_SD	Gemeinsamkeiten > Schwachstelle	The unsecured Elastic Search database included a significant amount of both user and company information with the vast majority of email data records referring to users in the US.
SV05 - CAM4	CM4_Wired	Gemeinsamkeiten > Schwachstelle	CAM4 had misconfigured an ElasticSearch production database so that it was easy to find and view heaps of personally identifiable information, as well as corporate details like fraud and spam detection logs.
SV05 - CAM4	CM4_Wired	Gemeinsamkeiten > Schwachstelle	“Leaving their production server publicly exposed without any password,”
SV05 - CAM4	CM4_BC	Reaktionen > Maßnahmen > Opferseitig	The CAM4 unsecured database was discovered by a Safety Detectives team lead by security researcher Anurag Sen and it was immediately taken down by Irish parent company Granity Entertainment after the leak was reported.
SV05 - CAM4	CM4_SD	Reaktionen > Maßnahmen > Opferseitig	The Ireland-based company was immediately contacted and the server was secured shortly afterwards.
SV05 - CAM4	CM4_Wired	Reaktionen > Maßnahmen > Opferseitig	CAM4 has taken the server offline, but not before it leaked 7TB of user data.
SV05 - CAM4	CM4_Wired	Reaktionen > Maßnahmen > Opferseitig	And Sen says that CAM4's parent company, Granity Entertainment, took the problematic server offline within a half hour of being contacted by the researchers. That doesn't excuse the initial error, but at least the response was swift.
SV05 - CAM4	CM4_Wired	Reaktionen > Maßnahmen > Opferseitig	Krieg says that the CAM4 has already taken steps to prevent a repeat of the data leak. "It's a server that should not have an outward facing IP in the first place," he says. "We're going to be moving it to our internal LAN to make it a lot harder for people to get access to this type of server, while making sure that nothing is on it that should not be on it, which includes any personally identifiable information."
SV05 - CAM4	CM4_BC	Rolle der Kryptografie > Schutz	Password hashes
SV05 - CAM4	CM4_BC	Rolle der Kryptografie > Schutz	"The security team also discovered 26,392,701 entries with passwords hashes with a proportion of hashes belonging to CAM4.com users and some from website system resources," the researchers said.
SV05 - CAM4	CM4_SD	Rolle der Kryptografie > Schutz	Password hashes
SV05 - CAM4	CM4_SD	Rolle der Kryptografie > Schutz	However, many pieces of private information were not available while password fields were masked in the instances seen by our investigators.
SV05 - CAM4	CM4_SD	Rolle der Kryptografie > Schutz	The security team also discovered 26,392,701 entries with passwords hashes with a proportion of hashes belonging to CAM4.com users and some from website system resources.
SV05 - CAM4	CM4_Wired	Rolle der Kryptografie > Schutz	26,392,701 had password hashes for both CAM4 users and website systems
SV05 - CAM4	CM4_Wired	Rolle der Kryptografie > Schutz	Moreover, despite the sensitive nature of the site and the data involved, it was actually fairly difficult to connect specific pieces of information to real names. “You really have to dig into the logs to find tokens or anything that would connect you to the real person or anything that would reveal his or her identity,” says Diachenko.
SV06 - SolarWinds	SW_Sterle	Angreifer > Staatlich motiviert	Speculation regarding those responsible for the attack points to a country sponsored espionage activity [4].

Dokumentgruppe	Dokumentname	Code	Segment
SV06 - SolarWinds	SW_Sterle	Angreifer > Staatlich motiviert	the evidence that has been obtained indicate patterns consistent with a foreign government's espionage behaviors and hacking techniques [6].
SV06 - SolarWinds	SW_TT	Angreifer > Staatlich motiviert	suspected nation-state hackers that have been identified as a group known as Nobelium by Microsoft
SV06 - SolarWinds	SW_TT	Angreifer > Staatlich motiviert	Federal investigators and cybersecurity agents believe a Russian espionage operation -- mostly likely Russia's Foreign Intelligence Service -- is behind the SolarWinds attack.
SV06 - SolarWinds	SW_TT	Angreifer > Staatlich motiviert	While it is suspected that the initial Sunburst code and the attack against SolarWinds and its users came from a threat actor based in Russia, other nation-state threat actors have also used SolarWinds in attacks
SV06 - SolarWinds	SW_TT	Angreifer > Staatlich motiviert	According to a Reuters report, suspected nation-state hackers based in China exploited SolarWinds during the same period of time the Sunburst attack occurred. The suspected China-based threat actors targeted the National Finance Center, which is a payroll agency within the U.S. Department of Agriculture.
SV06 - SolarWinds	SW_TT	Angreifer > Staatlich motiviert	It is suspected that the China-based attackers did not use Sunburst, but rather a different malware that SolarWinds identifies as Supernova.
SV06 - SolarWinds	SW_SoWi_2	Angreifer > Staatlich motiviert	The U.S. government and many private-sector experts have stated the belief that a foreign nation-state conducted this intrusive operation as part of a widespread attack against America's cyberinfrastructure
SV06 - SolarWinds	SW_SA	Fehler > Menschliches Versagen	Top executives of the SolarWinds firm blamed an intern for having used a weak password for several years, exposing the company to hack
SV06 - SolarWinds	SW_SA	Fehler > Menschliches Versagen	intern that has used a weak password for several years
SV06 - SolarWinds	SW_SA	Fehler > Menschliches Versagen	Initial investigation suggested that the password "solarwinds123" was publicly accessible via a misconfigured GitHub repository
SV06 - SolarWinds	SW_SA	Fehler > Menschliches Versagen	"I believe that was a password that an intern used on one of his servers back in 2017 which was reported to our security team and it was immediately removed," Ramakrishna said in response to Porter.
SV06 - SolarWinds	SW_SA	Fehler > Menschliches Versagen	Confronted by Rep. Rashida Tlaib, former SolarWinds CEO Kevin Thompson declared that the password issue was "a mistake that an intern made."
SV06 - SolarWinds	SW_TT	Fehler > Organisatorische Schwächen	For example, the company continued to distribute updates infected with the APT29 malware after the initial breach.
SV06 - SolarWinds	SW_Sterle	Gemeinsamkeiten > Art des Vorfalls > Supply-Chain-Angriff	Threat agents began their reconnaissance mission by implementing a very simple version of a Supply Chain Attack, a process accomplished by targeting a third-party client with access to SolarWinds' resources, rather than trying to hack SolarWinds' network directly [4].
SV06 - SolarWinds	SW_Sterle	Gemeinsamkeiten > Art des Vorfalls > Supply-Chain-Angriff	Now threat agents knew they had the ability to take the attack further and implement a large-scale Supply Chain Attack without being detected by the intrusion detection systems.
SV06 - SolarWinds	SW_SA	Gemeinsamkeiten > Art des Vorfalls > Supply-Chain-Angriff	op executives of the SolarWinds firm believe that the root cause of the recently disclosed supply chain attack
SV06 - SolarWinds	SW_SA	Gemeinsamkeiten > Art des Vorfalls > Supply-Chain-Angriff	SolarWinds Orion supply chain
SV06 - SolarWinds	SW_SA	Gemeinsamkeiten > Art des Vorfalls > Supply-Chain-Angriff	supply chain attack
SV06 - SolarWinds	SW_TT	Gemeinsamkeiten > Art des Vorfalls > Supply-Chain-Angriff	The SolarWinds hack was a major event not because a single company was breached, but because it triggered a much larger supply chain incident
SV06 - SolarWinds	SW_TT	Gemeinsamkeiten > Art des Vorfalls > Supply-Chain-Angriff	supply chain breach
SV06 - SolarWinds	SW_TT	Gemeinsamkeiten > Art des Vorfalls > Supply-Chain-Angriff	The hackers used a method known as a supply chain attack to insert malicious code into the Orion system. A supply chain attack works by targeting a third party with access to an organization's systems rather than trying to hack the networks directly.
SV06 - SolarWinds	SW_TT	Gemeinsamkeiten > Art des Vorfalls > Supply-Chain-Angriff	SolarWinds was a perfect target for this kind of supply chain attack
SV06 - SolarWinds	SW_TT	Gemeinsamkeiten > Art des Vorfalls > Supply-Chain-Angriff	The SolarWinds supply chain attack is a global hack,
SV06 - SolarWinds	SW_GB_2	Gemeinsamkeiten > Art des Vorfalls > Supply-Chain-Angriff	the SolarWinds supply chain compromise
SV06 - SolarWinds	SW_SoWi_3	Gemeinsamkeiten > Art des Vorfalls > Supply-Chain-Angriff	Orion Platform Supply-Chain Attack
SV06 - SolarWinds	SW_GB_1	Gemeinsamkeiten > Art des Vorfalls > Supply-Chain-Angriff	supply chain attack
SV06 - SolarWinds	SW_Sterle	Gemeinsamkeiten > Branche > Betroffene Dritte	The platform is used by major corporate entities such as Microsoft, Intel, Cisco, etc. as well as major governmental agencies such as the Infrastructure Security Agency, Department of Homeland Security, Department of the Treasury, Department of Justice, Pentagon, etc. [7].
SV06 - SolarWinds	SW_Sterle	Gemeinsamkeiten > Branche > Betroffene Dritte	One instance in particular proved threat agents had gained access into dozens of email accounts and networks in the Departmental Offices of the United States Treasury [3], leading to a breach of confidentiality in the United States government.

Dokumentgruppe	Dokumentname	Code	Segment
SV06 - SolarWinds	SW_Sterle	Gemeinsamkeiten > Branche > Betroffene Dritte	By maintaining this balance, the threat actors' presence remained unknown within client networks, including those of "Department of State, Department of Homeland Security, National Institutes of Health, Department of Energy, Department of the Treasury, Pentagon, Department of Commerce, Centers for Disease Control and Prevention, and even some state and local governments" [15].
SV06 - SolarWinds	SW_SA	Gemeinsamkeiten > Branche > Betroffene Dritte	prominent IT and security firms (Microsoft, FireEye, Malwarebytes, CrowdStrike, and Mimecast), several Government agencies (Departments of State, Justice, Commerce, Homeland Security, Energy, Treasury, and the National Institutes of Health), the National Aeronautics and Space Administration (NSA), and the Federal Aviation Administration (FAA).
SV06 - SolarWinds	SW_SA	Gemeinsamkeiten > Branche > Betroffene Dritte	additional government and private sector victims in other countries,
SV06 - SolarWinds	SW_TT	Gemeinsamkeiten > Branche > Betroffene Dritte	affected thousands of organizations, including the U.S. government.
SV06 - SolarWinds	SW_TT	Gemeinsamkeiten > Branche > Betroffene Dritte	More than 30,000 public and private organizations -- including local, state and federal agencies -- use the Orion network management system to manage their IT resources
SV06 - SolarWinds	SW_TT	Gemeinsamkeiten > Branche > Betroffene Dritte	government departments such as Homeland Security, State, Commerce and Treasury were affected, as there was evidence that emails were missing from their systems. Private companies such as FireEye, Microsoft, Intel, Cisco and Deloitte also suffered from this attack
SV06 - SolarWinds	SW_TT	Gemeinsamkeiten > Branche > Betroffene Dritte	There are speculations that many enterprises might be collateral damage, as the main focus of the attack was government agencies that make use of the SolarWinds IT management systems.
SV06 - SolarWinds	SW_GB_1	Gemeinsamkeiten > Branche > Betroffene Dritte	FireEye has detected this activity at multiple entities worldwide. The victims have included government, consulting, technology, telecom and extractive entities in North America, Europe, Asia and the Middle East. We anticipate there are additional victims in other countries and verticals.
SV06 - SolarWinds	SW_Sterle	Gemeinsamkeiten > Branche > Direkt Betroffene	SolarWinds offers software solutions for the main challenges in IT Management, more specifically, network management, systems management, IT security, database management, IT service management, application management and managed service providers.
SV06 - SolarWinds	SW_TT	Gemeinsamkeiten > Branche > Direkt Betroffene	SolarWinds is a major software company based in Tulsa, Okla., which provides system management tools for network and infrastructure monitoring, and other technical services to hundreds of thousands of organizations around the world. Among the company's products is an IT performance monitoring system called Orion.
SV06 - SolarWinds	SW_Sterle	Gemeinsamkeiten > Schwachstelle	Threat actors gained access to the SolarWinds Orion Platform by first performing reconnaissance and gaining information on SolarWinds and their clients, eventually stealing authorized credentials. Posing as an authorized entity using the stolen credentials, threat agents gained access to the SolarWinds network.
SV06 - SolarWinds	SW_Sterle	Gemeinsamkeiten > Schwachstelle	Threat agents began their reconnaissance mission by implementing a very simple version of a Supply Chain Attack, a process accomplished by targeting a third-party client with access to SolarWinds' resources, rather than trying to hack SolarWinds' network directly [4].
SV06 - SolarWinds	SW_SoWi_1	Gemeinsamkeiten > Schwachstelle	This was a highly sophisticated cyberattack on our systems that inserted a vulnerability within our Orion® Platform products
SV06 - SolarWinds	SW_SoWi_1	Gemeinsamkeiten > Schwachstelle	The vulnerability has only been identified in updates to the Orion Platform products delivered between March and June 2020, but our investigations are still ongoing.
SV06 - SolarWinds	SW_SoWi_1	Gemeinsamkeiten > Schwachstelle	The vulnerability was not evident in the Orion Platform products' source code but appears to have been inserted during the Orion software build process.
SV06 - SolarWinds	SW_SA	Gemeinsamkeiten > Schwachstelle	The investigators don't exclude the use of stolen credentials and brute-force attacks as possible attack vectors.
SV06 - SolarWinds	SW_SoWi_3	Gemeinsamkeiten > Schwachstelle	We narrowed it down to three most likely candidates for initial entry, but we don't limit the methods to these three. This excludes the possibility the initial access was through a known, unpatched vulnerability: Zero-day vulnerability in a third-party application or device; Brute-force attack, such as a password spray attack; or Social engineering, such as a targeted phishing attack.
SV06 - SolarWinds	SW_GB_1	Gemeinsamkeiten > Schwachstelle	They gained access to victims via trojanized updates to SolarWind's Orion IT monitoring and management software
SV06 - SolarWinds	SW_Sterle	Reaktionen > Kommunikation	To remedy the situation, SolarWinds issued public disclosure reports with federal authorities, sharing discoveries of the breach.
SV06 - SolarWinds	SW_Sterle	Reaktionen > Kommunikation	An action plan was published by SolarWinds to advise additional client responsibilities to secure their respective systems.
SV06 - SolarWinds	SW_SoWi_1	Reaktionen > Kommunikation	We have reached out and spoken to thousands of customers and partners in the past few days, and we will continue to be in constant communication with our customers and partners to provide timely information, answer questions and assist with upgrades.
SV06 - SolarWinds	SW_SoWi_1	Reaktionen > Kommunikation	e also have had numerous conversations with security professionals to further assist them in their research.

Dokumentgruppe	Dokumentname	Code	Segment
SV06 - SolarWinds	SW_SoWi_1	Reaktionen > Kommunikation	We are providing our customers, experts and others in the IT and security industries detailed information regarding the incident to aid with identifying indicators of compromise and steps they can take to further harden their systems against unauthorized incursion. These tools can be found on our Security Advisory page at www.solarwinds.com/securityadvisory which we are updating as we learn new information.
SV06 - SolarWinds	SW_SoWi_1	Reaktionen > Kommunikation	Our shared goal is to better understand and protect against these types of malicious attacks in the future. As we've noted, the attacks on our systems were incredibly complex, and it will take some time for our investigative work to be complete. We are committed to being deliberate as we take this on.
SV06 - SolarWinds	SW_SoWi_2	Reaktionen > Kommunikation	We encourage everyone to visit this blog post, authored by the CrowdStrike team, which provides additional details into these findings and other technical aspects of this attack, and contains valuable information intended to help the industry better understand attacks of this nature. As we discussed in our previous post, we hope that this event ushers in a new level of collaboration and information sharing within the technology industry to address and prevent similar attacks in the future. Our concern is that right now similar processes may exist in software development environments at other companies throughout the world. The severity and complexity of this attack has taught us that more effectively combatting similar attacks in the future will require an industry-wide approach as well as public-private partnerships that leverage the skills, insight, knowledge, and resources of all constituents. We want to be a part of that solution, which is why we are sharing this information with the broader community, and we will continue to share progress as we assimilate this information into our go-forward practices.
SV06 - SolarWinds	SW_SoWi_2	Reaktionen > Kommunikation	On December 12, 2020, we were informed of the cyberattack and moved swiftly to notify and protect our customers and to investigate the attack in collaboration law enforcement, intelligence and governments.
SV06 - SolarWinds	SW_SoWi_2	Reaktionen > Kommunikation	We are still investigating these incidents and are sharing information related to them with law enforcement to support investigation efforts. We will continue our investigations to help ensure our products and internal systems are secure and to provide information that we hope leads to the identification of the perpetrators and the prevention of these types of attacks in the future. We also plan to continue to share our broader findings with the industry at large in the hope that everyone is better able protect themselves and deliver more secure solutions to their customers.
SV06 - SolarWinds	SW_SoWi_3	Reaktionen > Kommunikation	We quickly published information about the attack and notified our customers.
SV06 - SolarWinds	SW_TT	Reaktionen > Maßnahmen > Dritte	Reports indicated Microsoft's own systems were being used to further the hacking attack, but Microsoft denied this claim to news agencies. Later, the company worked with FireEye and GoDaddy to block and isolate versions of Orion known to contain the malware to cut off hackers from customers' systems. They did so by turning the domain used by the backdoor malware used in Orion as part of the SolarWinds hack into a kill switch. The kill switch here served as a mechanism to prevent Sunburst from operating further.
SV06 - SolarWinds	SW_TT	Reaktionen > Maßnahmen > Dritte	In June 2023, the U.S. Securities and Exchange Commission (SEC) sent SolarWinds a Wells notice at the conclusion of their investigation. It informed former and current executives that the SEC intends to recommend civil enforcement action, alleging that SolarWinds broke federal security laws in public statements and internal controls related to the hack. For example, the company continued to distribute updates infected with the APT29 malware after the initial breach.
SV06 - SolarWinds	SW_TT	Reaktionen > Maßnahmen > Dritte	SolarWinds also settled a class action lawsuit October 2022, paying out $26 million to shareholders who maintained that SolarWinds neglected internal security preceding the breach and misled the public about its digital security.
SV06 - SolarWinds	SW_TT	Reaktionen > Maßnahmen > Dritte	In October 2023, the SEC sued SolarWinds and CISO Timothy Brown, stating the company concealed its cybersecurity vulnerabilities before it was attacked. This is the first time the SEC has sued the victim of a cyberattack. SolarWinds plans to fight the charges in court.
SV06 - SolarWinds	SW_SoWi_2	Reaktionen > Maßnahmen > Dritte	KPMG and CrowdStrike, working together with the SolarWinds team, have been able to locate the malicious code injection source. We have reverse-engineered the code responsible for the attack, enabling us to learn more about the tool that was developed and deployed into the build environment.
SV06 - SolarWinds	SW_SoWi_3	Reaktionen > Maßnahmen > Dritte	CrowdStrike performed a macro-level analysis of the SolarWinds environment and deployed their Falcon technology and other threat-hunting tools, providing ongoing monitoring for suspicious activity.
SV06 - SolarWinds	SW_SoWi_3	Reaktionen > Maßnahmen > Dritte	The KPMG forensics team performed micro-level analysis, conducting deep inspections of our build environments, as well as additional forensics and analysis. This analysis included inspection of various artifacts, including historical firewall logs, access control logs, and SIEM events.
SV06 - SolarWinds	SW_Sterle	Reaktionen > Maßnahmen > Opferseitig	The company removed the malicious code from the update and prevented the malware from operating further.
SV06 - SolarWinds	SW_Sterle	Reaktionen > Maßnahmen > Opferseitig	The company began working to improve the Orion Platform and deployed hotfixes that could be installed to remove vulnerabilities exploited by the breach.
SV06 - SolarWinds	SW_SoWi_1	Reaktionen > Maßnahmen > Opferseitig	Immediately after this call, we mobilized our incident response team and quickly shifted significant internal resources to investigate and remediate the vulnerability.
SV06 - SolarWinds	SW_SoWi_1	Reaktionen > Maßnahmen > Opferseitig	To accomplish that, we swiftly released hotfix updates to impacted customers that we believe will close the code vulnerability when implemented. These updates were made available to all customers we believe to have been impacted, regardless of their current maintenance status.

Dokumentgruppe	Dokumentname	Code	Segment
SV06 - SolarWinds	SW_SoWi_1	Reaktionen > Maßnahmen > Opferseitig	We shared all of our proprietary code libraries that we believed to have been affected by SUNBURST to give security professionals the information they needed to do their research.
SV06 - SolarWinds	SW_SoWi_1	Reaktionen > Maßnahmen > Opferseitig	We swiftly released hotfix updates to impacted customers, regardless of their maintenance status, that we believe will close the vulnerability when implemented.
SV06 - SolarWinds	SW_SoWi_1	Reaktionen > Maßnahmen > Opferseitig	After our release of Orion 2020.2.1 HF 2 on Tuesday night, December 15, we believe the Orion Platform now meets the US Federal and state agencies' requirements. We are providing direct support to these customers and will help them complete their upgrades quickly.
SV06 - SolarWinds	SW_SoWi_1	Reaktionen > Maßnahmen > Opferseitig	We are continuing to take measures to ensure our internal systems are secure, including deploying the Falcon Endpoint Protection Platform across the endpoints on our systems.
SV06 - SolarWinds	SW_SoWi_1	Reaktionen > Maßnahmen > Opferseitig	We have retained industry-leading third-party cybersecurity experts to assist us with this work and are actively collaborating with our partners, vendors, law enforcement and intelligence agencies around the world.
SV06 - SolarWinds	SW_SA	Reaktionen > Maßnahmen > Opferseitig	“They violated our password policies and they posted that password on an internal, on their own private Github account,” Thompson explained. “As soon as it was identified and brought to the attention of my security team, they took that down.”
SV06 - SolarWinds	SW_TT	Reaktionen > Maßnahmen > Opferseitig	The company has released patches for the malware and other potential vulnerabilities discovered since the initial Orion attack.
SV06 - SolarWinds	SW_SoWi_2	Reaktionen > Maßnahmen > Opferseitig	As we recently disclosed, we even shared all of our proprietary code libraries that we believed to have been affected by SUNBURST to give security professionals the information they needed in their research.
SV06 - SolarWinds	SW_SoWi_2	Reaktionen > Maßnahmen > Opferseitig	As part of our ongoing efforts to protect our customers and investigate the SUNBURST attack, we are reviewing historical and current customer inquiries that might contribute to a better understanding of the attack. To date, we have identified two previous customer support incidents during the timeline referenced above that, with the benefit of hindsight, we believe may be related to SUNBURST. We investigated the first in conjunction with our customer and two third-party security companies. At that time, we did not determine the root cause of the suspicious activity or identify the presence of the SUNBURST malicious code within our Orion Platform software.
SV06 - SolarWinds	SW_SoWi_3	Reaktionen > Maßnahmen > Opferseitig	We also released remediations to the affected versions of the Orion Platform software and engaged in extensive outreach and support to our customers. We also made available third-party support at our expense to help customers upgrade their Orion Platform software. Through our numerous blog posts, webinars, TechPod podcasts, interviews, and other public statements, we’ve provided to our customers, and to the industry more broadly, substantial information about the cyber incident and our learnings and adaptation from it to help them better understand the attack and protect themselves.
SV06 - SolarWinds	SW_SoWi_3	Reaktionen > Maßnahmen > Opferseitig	We’re working with industry experts to implement enhanced security practices designed to further strengthen and protect our products and environment against these and other types of attacks in the future.
SV06 - SolarWinds	SW_SoWi_3	Reaktionen > Maßnahmen > Opferseitig	To that end, we’re further securing our environment and systems by: Upgrading to stronger and deeper endpoint protections within our environment; Enhancing our Data Loss Prevention solution to better detect low and slow leaks; Expanding our Security Operations Center to improve visibility and threat hunting across our network; and Tightening our firewall policies to further limit east/west traffic.
SV06 - SolarWinds	SW_SoWi_3	Reaktionen > Maßnahmen > Opferseitig	Additionally, we’re adopting zero trust and least privilege access mechanisms by: Expanding and more consistently enforcing least privileges policies for ALL employees; Limiting external interfaces to our environments; and Increasing, expanding, and strictly enforcing requirements for multi-factor authentication throughout our environment, as well as expanding the use of a privilege access manager for all administrative accounts, with auditing.
SV06 - SolarWinds	SW_SoWi_3	Reaktionen > Maßnahmen > Opferseitig	Further, we’re addressing the possible risks associated with third-party applications access by: Increasing on-going monitoring and inspection of all SaaS tools within our environment; Ensuring that the configurations and implementation of all tools within our environment align with best practices; Reviewing all accounts, updating all passwords and turning up the level of conditional access; and Strengthening the level of pre-procurement security reviews for all vendors.
SV06 - SolarWinds	SW_SoWi_3	Reaktionen > Maßnahmen > Opferseitig	Additionally, we have made significant progress in redesigning our automated build process to help ensure the security and integrity of the code our products and that no insertions or alterations have occurred during the build process as occurred happened with SUNSPOT and SUNBURST.

Dokumentgruppe	Dokumentname	Code	Segment
SV06 - SolarWinds	SW_SoWi_3	Reaktionen > Maßnahmen > Opferseitig	In addition to these protective steps, we're conducting our software builds in three separate environments, using changing build systems, and with separate user credentials. We check the integrity of the builds across these environments to identify and address any compromises. In this way, we are changing and shifting the threat surface, thereby forcing a threat actor to replicate an attack across multiple heterogeneous environments with no overlapping privileges to be successful. We use a standard Secure Development lifecycle approach. That includes requirements analysis, secure development, security testing, release and respond. As part of the process, Checkmarx is utilized for static code analysis, Whitesource is utilized for Open-Source discovery/analysis, and internal PEN testing utilizing Burpsuite prior to a final security review. In addition to the build pipeline, business critical assets are identified, tracked, and reviewed on a regular basis. Security controls are defined for each asset.
SV06 - SolarWinds	SW_TT	Reaktionen > Vorschläge	Since the hack was discovered, SolarWinds has recommended customers update their existing Orion platform.
SV06 - SolarWinds	SW_TT	Reaktionen > Vorschläge	SolarWinds also recommended customers not able to update Orion isolate SolarWinds servers and/or change passwords for accounts that have access to those servers.
SV06 - SolarWinds	SW_SA	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	In December, Security researcher Vinoth Kumar revealed he notified the company of a publicly accessible GitHub repository that was leaking the FTP credentials of the company's download website in the clear text
SV06 - SolarWinds	SW_GB_1	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	The attacker infrastructure leaks its configured hostname in RDP SSL certificates, which is identifiable in internet-wide scan data. This presents a detection opportunity for defenders -- querying internet-wide scan data sources for an organization's hostnames can uncover malicious IP addresses that may be masquerading as the organization.
SV06 - SolarWinds	SW_GB_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	However, thanks to some hard work by members of the information security community, the hashes have been successfully brute-forced. The list of hashes and their corresponding strings can be viewed at this FireEye GitHub page.
SV06 - SolarWinds	SW_GB_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	After receiving a CNAME DNS response with a new host to communicate with, SUNBURST starts a new thread to execute the method HttpHelper.Initialize. This method is responsible for the C2 communications and dispatching. The HTTP thread begins by delaying for a configurable amount of time that is controlled by the SetTime command. The HTTP thread delays for a minimum of one minute between callouts. The malware uses HTTP GET or POST requests. The sample disables certificate verification so it is possible to decrypt HTTPS traffic if SSL man-in-the-middle is performed.
SV06 - SolarWinds	SW_TT	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Hackers compromised a digitally signed SolarWinds Orion network monitoring component, opening a backdoor into the networks of thousands of SolarWinds government and enterprise customers.
SV06 - SolarWinds	SW_GB_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	SUNBURST is a trojanized version of a digitally signed SolarWinds Orion plugin called SolarWinds.Orion.Core.BusinessLayer.dll. The plugin contains a backdoor that communicates via HTTP to third party servers. After an initial dormant period of up to two weeks, SUNBURST may retrieve and execute commands that instruct the backdoor to transfer files, execute files, profile the system, reboot the system, and disable system services. The malware's network traffic attempts to blend in with legitimate SolarWinds activity by imitating the Orion Improvement Program (OIP) protocol and persistent state data is stored within legitimate plugin configuration files. The backdoor uses multiple obfuscated blocklists to identify processes, services, and drivers associated with forensic and anti-virus tools.
SV06 - SolarWinds	SW_GB_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	First, the backdoor verifies that the lowercase name of the current process is solarwinds.businesslayerhost. UNC2452 avoided including this string directly in the source code by computing a hash of the string and comparing the result to the 64-bit number 17291806236368054941. The hash value is calculated as a standard FNV-1A 64-bit hash with an additional XOR by the 64-bit number 6605813339339102567. The additional XOR operation forces malware analysts to develop custom tools to brute force the hash preimage.
SV06 - SolarWinds	SW_GB_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	SUNBURST's behavior is affected by the presence of malware analysis and security software. To disguise the strings used to detect these security tools, UNC2452 calculated and embedded a hash value for each string. While it is trivial for the backdoor to check for the existence of a hashed process name, it is computationally expensive to determine what string a hash value corresponds to (the "preimage").
SV06 - SolarWinds	SW_GB_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	SUNBURST uses the aforementioned FNV-1A plus XOR algorithm to compute the hash of each process name, service name, and driver filename on the system.
SV06 - SolarWinds	SW_GB_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	A user ID is generated based on three values: MAC address of the first available, non-loopback network interface Domain name HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid value SUNBURST takes the MD5 hash of these combined values and encodes it using a custom XOR scheme. We believe this value is used by UNC2452 to track unique victims.
SV06 - SolarWinds	SW_GB_1	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	SolarWinds.Orion.Core.BusinessLayer.dll is a SolarWinds digitally-signed component of the Orion software framework that contains a backdoor that communicates via HTTP to third party servers. We are tracking the trojanized version of this SolarWinds Orion plug-in as SUNBURST.

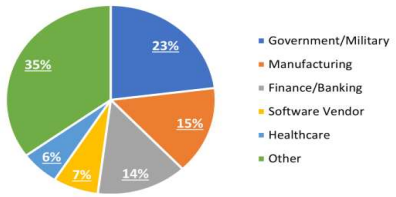
Dokumentgruppe	Dokumentname	Code	Segment
SV06 - SolarWinds	SW_GB_1	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	On execution of the malicious SolarWinds.Orion.Core.BusinessLayer.OrionImprovementBusinessLayer.Initialize method the sample verifies that its lower case process name hashes to the value 17291806236368054941. This hash value is calculated as the standard FNV-1A 64-bit hash with an additional XOR by 6605813339339102567 after computing the FNV-1A. This hash matches a process named "solarwinds.businesslayerhost".
SV06 - SolarWinds	SW_GB_1	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Process name, service name, and driver path listings are obtained, and each value is hashed via the FNV-1a + XOR algorithm as described previously and checked against hardcoded blocklists. Some of these hashes have been brute force reversed as part of this analysis, showing that these routines are scanning for analysis tools and antivirus engine components. If a blocklisted process is found the Update routine exits and the sample will continue to try executing the routine until the blocklist passes.
SV07 - Brenntag	BT_BC_1	Angreifer > Unabhängige Gruppierungen	data was stolen from its network by DarkSide ransomware operators
SV07 - Brenntag	BT_BC_1	Angreifer > Unabhängige Gruppierungen	the DarkSide attackers
SV07 - Brenntag	BT_BC_1	Angreifer > Unabhängige Gruppierungen	After the attack, the DarkSide ransomware group claimed to have exfiltrated150GB of data while they had access to Brenntag's systems.
SV07 - Brenntag	BT_HS	Angreifer > Unabhängige Gruppierungen	information was accessed and taken from its network by DarkSide ransomware operators
SV07 - Brenntag	BT_HS	Angreifer > Unabhängige Gruppierungen	The Darkside ransomware threat actors claimed to have stolen 150GB of data when the attack occurred.
SV07 - Brenntag	BT_BC_2	Angreifer > Unabhängige Gruppierungen	the DarkSide ransomware group claimed to have stolen 150GB of data during their attack.
SV07 - Brenntag	BT_BC_2	Fehler > Organisatorische Schwächen	While this was an expensive lesson, and unfortunately all-too-common, the attack illustrates the importance of enforcing multi-factor authentication for all logins on a network and putting all Remote Desktop servers behind a VPN. If MFA was enabled for account logins, it is unlikely that the DarkSide affiliate would have gained access to the network.
SV07 - Brenntag	BT_BC_1	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	data theft
SV07 - Brenntag	BT_BC_2	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	To prove their claims, the ransomware gang created a private data leak page containing a description of the types of data that were stolen and screenshots of some of the files.
SV07 - Brenntag	BT_BC_1	Gemeinsamkeiten > Art des Vorfalls > Ransomware	ransomware
SV07 - Brenntag	BT_BC_1	Gemeinsamkeiten > Art des Vorfalls > Ransomware	ransomware attack
SV07 - Brenntag	BT_HS	Gemeinsamkeiten > Art des Vorfalls > Ransomware	Ransomware Attack
SV07 - Brenntag	BT_BC_2	Gemeinsamkeiten > Art des Vorfalls > Ransomware	ransomware attack
SV07 - Brenntag	BT_BC_1	Gemeinsamkeiten > Branche > Direkt Betroffene	chemical distribution company Brenntag
SV07 - Brenntag	BT_HS	Gemeinsamkeiten > Branche > Direkt Betroffene	The global market leader in chemicals and ingredients distribution Brenntag
SV07 - Brenntag	BT_BC_2	Gemeinsamkeiten > Branche > Direkt Betroffene	Brenntag is a world-leading chemical distribution company headquartered in Germany
SV07 - Brenntag	BT_BC_1	Gemeinsamkeiten > Schwachstelle	The DarkSide affiliate who breached Brenntag's systems claimed to have gotten access to the network using stolen credentials bought from an unknown source.
SV07 - Brenntag	BT_HS	Gemeinsamkeiten > Schwachstelle	In Brenntag’s case, the DarkSide affiliate said they have obtained access to the network after purchasing stolen information, but didn’t know how the credentials were obtained, to begin with.
SV07 - Brenntag	BT_BC_2	Gemeinsamkeiten > Schwachstelle	In this particular case, the DarkSide affiliate claims to have gotten access to the network after purchasing stolen credentials. However, the DarkSide affiliate does not know how the credentials were originally obtained.
SV07 - Brenntag	BT_BC_1	Reaktionen > Kommunikation	The company also asked the impacted individuals (more than 6700 according to info provided to Maine's Attorney General) to review their account statements and keep an eye on their free credit reports to detect any attempts of identity theft and fraud. "If you find any transactions you do not recognize, contact the business or institution issuing the statement," Brenntag added.
SV07 - Brenntag	BT_BC_2	Reaktionen > Kommunikation	Today, Brenntag shared a statement with BleepingComputer confirming that they suffered a security incident but did not outright state it was a ransomware attack. "Brenntag North America is currently working to resolve a limited information security incident," Brenntag told BleepingComputer.
SV07 - Brenntag	BT_BC_1	Reaktionen > Maßnahmen > Opferseitig	Brenntag confirmed the ransomware attack in an email statement sent to BleepingComputer on May 13, saying that it disconnected all impacted systems from the network after the incident was discovered to contain the threat.

Dokumentgruppe	Dokumentname	Code	Segment
SV07 - Brenntag	BT_BC_1	Reaktionen > Maßnahmen > Opferseitig	As BleepingComputer reported in May, the chemical distributor company paid a $4.4 million ransom to DarkSide for a decryptor and to prevent the ransomware gang from leaking the stolen data.
SV07 - Brenntag	BT_HS	Reaktionen > Maßnahmen > Opferseitig	As soon as they learned about the attack, they disconnected affected systems from the network to limit the threat.
SV07 - Brenntag	BT_HS	Reaktionen > Maßnahmen > Opferseitig	In addition, third-party cybersecurity forensic specialists were immediately engaged to help with the investigation and law enforcement was notified.
SV07 - Brenntag	BT_HS	Reaktionen > Maßnahmen > Opferseitig	Bleeping Computer has confirmed that after negotiation the chemical distribution enterprise paid the requested ransom on May 11
SV07 - Brenntag	BT_BC_2	Reaktionen > Maßnahmen > Opferseitig	Chemical distribution company Brenntag paid a $4.4 million ransom in Bitcoin to the DarkSide ransomware gang to receive a decryptor for encrypted files and prevent the threat actors from publicly leaking stolen data.
SV07 - Brenntag	BT_BC_2	Reaktionen > Maßnahmen > Opferseitig	BleepingComputer was told that the ransom demand was decreased to $4.4 million, which was paid two days ago. From the bitcoin address shared with BleepingComputer, we confirmed that Brenntag sent the ransom to the attackers on May 11th.
SV07 - Brenntag	BT_BC_2	Reaktionen > Maßnahmen > Opferseitig	"As soon as we learned of this incident, we disconnected affected systems from the network to contain the threat." "In addition, third-party cybersecurity and forensic experts were immediately engaged to help investigate. We also informed law enforcement of this incident."
SV07 - Brenntag	BT_BC_2	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	stole unencrypted files.
SV07 - Brenntag	BT_HS	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	DarkSide Ransomware operates under the form of a Ransomware-as-a-Service (RaaS), in which the gains are shared between its holders and partners, or affiliates, who allow entry to companies and execute the ransomware. The DarkSide ransomware gang gets around 25% of a ransom payment, and the rest is taken by the affiliate who organized the assault.
SV07 - Brenntag	BT_BC_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	As part of this attack, the threat actors encrypted devices on the network and stole unencrypted files.
SV08 - Colonial Pipeline	ColP_Beerman	Angreifer > Unabhängige Gruppierungen	hacking group DarkSide
SV08 - Colonial Pipeline	ColP_Beerman	Angreifer > Unabhängige Gruppierungen	the hacker group Darkside
SV08 - Colonial Pipeline	ColP_Beerman	Angreifer > Unabhängige Gruppierungen	DarkSide is a relatively new hacker group that has been hacking U.S. and European companies since August of 2020.
SV08 - Colonial Pipeline	ColP_Beerman	Fehler > Menschliches Versagen	the password was either compromised through human blackmail (ex-employee)
SV08 - Colonial Pipeline	ColP_Beerman	Fehler > Organisatorische Schwächen	After the employee's retirement the group DarkSide simply acquired the password to the VPN account that was no longer in use by anyone, but still had access to the VPN network [12].
SV08 - Colonial Pipeline	ColP_Beerman	Gemeinsamkeiten > Art des Vorfalls > Ransomware	On April 29, 2021 the Colonial Pipeline Co. was hit by a ransomware attack.
SV08 - Colonial Pipeline	ColP_NYT	Gemeinsamkeiten > Art des Vorfalls > Ransomware	ransomware attack.
SV08 - Colonial Pipeline	ColP_NYT	Gemeinsamkeiten > Art des Vorfalls > Ransomware	Colonial Pipeline acknowledged that its corporate computer networks had been hit by a ransomware attack, in which criminal groups hold data hostage until the victim pays a ransom
SV08 - Colonial Pipeline	ColP_BC	Gemeinsamkeiten > Art des Vorfalls > Ransomware	ransomware attack
SV08 - Colonial Pipeline	ColP_Beerman	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	The hacker group most likely started with reconnaissance into how secure the systems were on the Colonial Pipeline network. Simply by monitoring the employee list of Colonial Pipeline on LinkedIn may have lead to them seeing that an employee was going to no longer be with the company.
SV08 - Colonial Pipeline	ColP_Beerman	Gemeinsamkeiten > Branche	The Colonial Pipeline fell under the category of "Critical Infrastructure vulnerable to attack"
SV08 - Colonial Pipeline	ColP_Beerman	Gemeinsamkeiten > Branche > Direkt Betroffene	The Colonial Pipeline Co. is the biggest oil pipeline company in the United States
SV08 - Colonial Pipeline	ColP_NYT	Gemeinsamkeiten > Branche > Direkt Betroffene	One of the nation's largest pipelines, which carries refined gasoline and jet fuel from Texas up the East Coast to New York,
SV08 - Colonial Pipeline	ColP_NYT	Gemeinsamkeiten > Branche > Direkt Betroffene	energy infrastructure
SV08 - Colonial Pipeline	ColP_Beerman	Gemeinsamkeiten > Schwachstelle	There was an old account that was no longer in use that was attached to the virtual private network (VPN)
SV08 - Colonial Pipeline	ColP_Beerman	Gemeinsamkeiten > Schwachstelle	t the VPN for which the account was connected to did not have multi-factor authentication, meaning that as soon as they got in there was no holding back.
SV08 - Colonial Pipeline	ColP_Beerman	Gemeinsamkeiten > Schwachstelle	Since there was no twofactor authentication, they were immediately able to access the Colonial Pipeline network.
SV08 - Colonial Pipeline	ColP_NYT	Reaktionen > Kommunikation	But on Saturday, Colonial, which is privately held, declined to say whether it planned to pay the ransom, which frequently suggests that a company is considering doing so, or has already paid. Nor did it say when normal operations would resume.

Dokumentgruppe	Dokumentname	Code	Segment
SV08 - Colonial Pipeline	ColP_NYT	Reaktionen > Kommunikation	The company initially said that it had learned on Friday that it “was the victim of a cybersecurity attack,” leading many in the industry and some investigators to believe that the attack might have directly affected the industrial control systems that regulate oil flow. Colonial issued an updated statement on Saturday saying that it had determined that the “incident involves ransomware”
SV08 - Colonial Pipeline	ColP_NYT	Reaktionen > Kommunikation	It said it had contacted the law enforcement authorities and other federal agencies. The F.B.I. confirmed that it was involved in the investigation, along with the Energy Department and the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency.
SV08 - Colonial Pipeline	ColP_NYT	Reaktionen > Kommunikation	People familiar with the investigation said that although Colonial insisted that it became aware of the attack on Friday, the events appeared to have unfolded over several days.
SV08 - Colonial Pipeline	ColP_BC	Reaktionen > Kommunikation	Today, Colonial Pipeline issued a statement confirming the attack
SV08 - Colonial Pipeline	ColP_BC	Reaktionen > Kommunikation	The Company will provide updates as restoration efforts progress.
SV08 - Colonial Pipeline	ColP_Beerman	Reaktionen > Maßnahmen > Dritte	The Justice Department was able to seize $2.3 million from the group DarkSide
SV08 - Colonial Pipeline	ColP_BC	Reaktionen > Maßnahmen > Dritte	Actions taken by the Federal Government to issue a temporary hours of service exemption for motor carriers and drivers transporting refined products across Colonial’s footprint should help alleviate local supply disruptions and we thank our government partners for their assistance in resolving this matter.
SV08 - Colonial Pipeline	ColP_Beerman	Reaktionen > Maßnahmen > Opferseitig	employee receiving a message at 5 a.m. telling him to pay $4.4 million in cryptocurrency to those responsible for the hack. Upon receiving the message the employee sent the message up to his supervisors, who then shut the plant down. The company opted to eventually pay the hackers
SV08 - Colonial Pipeline	ColP_Beerman	Reaktionen > Maßnahmen > Opferseitig	After paying the hackers the company started an extensive search to determine how the actual hack took place
SV08 - Colonial Pipeline	ColP_Beerman	Reaktionen > Maßnahmen > Opferseitig	The team who looked into the attack installed “alarms” so that if the hackers reached certain points in the network from now on without the correct permissions the company would be notified rather than allowing the hackers to have free reign over the network.
SV08 - Colonial Pipeline	ColP_Beerman	Reaktionen > Maßnahmen > Opferseitig	DarkSide left a ransom note on one of the computer screens, and was found by an employee [14]. In just one hour the whole pipeline and associated network were shut down.
SV08 - Colonial Pipeline	ColP_Beerman	Reaktionen > Maßnahmen > Opferseitig	Colonial Pipeline claims to have changed VPN services which should fix the first issue that the company had.
SV08 - Colonial Pipeline	ColP_Beerman	Reaktionen > Maßnahmen > Opferseitig	the Colonial Pipeline Hack caused the shut down of the Colonial Pipeline for the first time in fifty-seven years.The attack did not directly shutdown the pipeline, but the attack forced the operator of the system to initiate a complete shutdown.
SV08 - Colonial Pipeline	ColP_Beerman	Reaktionen > Maßnahmen > Opferseitig	In order to restart the pipeline, Joseph Blount, the CEO of Colonial Pipeline, decided to pay the Darkside hackers over 4.4 million dollars [25].
SV08 - Colonial Pipeline	ColP_NYT	Reaktionen > Maßnahmen > Opferseitig	The operator, Colonial Pipeline, said it had halted systems for its 5,500 miles of pipeline after being hit by a ransomware attack.
SV08 - Colonial Pipeline	ColP_NYT	Reaktionen > Maßnahmen > Opferseitig	was forced to shut down after being hit by ransomware in a vivid demonstration of the vulnerability of energy infrastructure to cyberattacks.
SV08 - Colonial Pipeline	ColP_NYT	Reaktionen > Maßnahmen > Opferseitig	it had shut down its 5,500 miles of pipeline, which it says carries 45 percent of the East Coast’s fuel supplies, in an effort to contain the breach.
SV08 - Colonial Pipeline	ColP_NYT	Reaktionen > Maßnahmen > Opferseitig	The company said it had shut the pipeline itself, a precautionary act, apparently for fear that the hackers might have obtained information that would enable them to attack susceptible parts of the pipeline.
SV08 - Colonial Pipeline	ColP_NYT	Reaktionen > Maßnahmen > Opferseitig	contended that it had taken down its systems as a preventive measure.
SV08 - Colonial Pipeline	ColP_NYT	Reaktionen > Maßnahmen > Opferseitig	It has hired the private cybersecurity company FireEye
SV08 - Colonial Pipeline	ColP_BC	Reaktionen > Maßnahmen > Opferseitig	Colonial Pipeline suffered a ransomware attack yesterday that forced them to shut down their entire network to prevent the spread of the malware.
SV08 - Colonial Pipeline	ColP_BC	Reaktionen > Maßnahmen > Opferseitig	stated that they temporarily shut down their pipeline operations while responding to the attack.
SV08 - Colonial Pipeline	ColP_BC	Reaktionen > Maßnahmen > Opferseitig	"On May 7, the Colonial Pipeline Company learned it was the victim of a cybersecurity attack. In response, we proactively took certain systems offline to contain the threat, which has temporarily halted all pipeline operations, and affected some of our IT systems."
SV08 - Colonial Pipeline	ColP_BC	Reaktionen > Maßnahmen > Opferseitig	"Upon learning of the issue, a leading, third-party cybersecurity firm was engaged, and they have already launched an investigation into the nature and scope of this incident, which is ongoing," Colonial Pipeline said in a statement.
SV08 - Colonial Pipeline	ColP_BC	Reaktionen > Maßnahmen > Opferseitig	In response to the cybersecurity attack on our system, we proactively took certain systems offline to contain the threat, which temporarily halted all pipeline operations, and affected some of our IT systems.

Dokumentgruppe	Dokumentname	Code	Segment
SV08 - Colonial Pipeline	ColP_Beerman	Reaktionen > Vorschläge	To help alleviate these problems, a Internal Review System can be utilized to mitigate the risk of an inactive VPN account being used by an unspecified user, as was the case in this attack. How the internal review system works is an automated review system audits the access permissions of users and then flags unauthorized access of those marked users. The IRS helps to ”provision or de-provision users who could be inactive, terminated from the organization or no longer in need of the system license.” If the VPN that was used by the hackers had been flagged and de-provisioned based on its inactivity, then the hackers would not have been able to gain access to the system.
SV08 - Colonial Pipeline	ColP_Beerman	Reaktionen > Vorschläge	Another solution that could have helped prevent the attack is the use of Multi-factor Authentication. Multi-factor authentication was listed in the previously mentioned executive order’s list of mandates, but its effectiveness is still overlooked. Multi-factor authentication operates through a series a steps the user must take to authenticate that they are the appropriate user trying to access the designated private, and/or sensitive information.
SV08 - Colonial Pipeline	ColP_Beerman	Reaktionen > Vorschläge	Internal Review System Automated Audit System that checks for unauthorized access privileges of user accounts and provisions/de-provisions accounts accordingly Multi-factor Authentication User must authenticate that they are the authorized user of the space/information they are trying to access by entering a passcode or opening a push notification tied to the authorized user’s email Zero-Trust network model Users are granted low-tier privileges with access to applications, hosts, and ports
SV08 - Colonial Pipeline	ColP_Beerman	Reaktionen > Vorschläge	In summary, to best protect against malicious activity as described in this paper is to: • Implement a Zero-trust network model • Perform a role based user access review • Utilize practical security measures, such as: Use strong passwords, mandate multi-factor authentication, etc
SV08 - Colonial Pipeline	ColP_Beerman	Reaktionen > Vorschläge	Other practical solutions involve backing up your data so that way a system can be restored if the information is compromised, such as the case with DarkSide. The Colonial Pipeline could have avoided paying the ransom if they had backed up their systems so that they could have restored their system [29].
SV08 - Colonial Pipeline	ColP_Beerman	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	DarkSide follows a ”ransomware-as-a-service” model, where DarkSide develops and sells the ransomware for other cyber actors to use [7]. Other analysts have compared DarkSide’s ransomware model to “franchising”, where those who buy and use the ransomware can use DarkSide’s name in association with their attack [8].
SV08 - Colonial Pipeline	ColP_Beerman	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	The hacker group, on the ransom note, demanded a payment of 4.4 million dollars to release the network from their grasp [15].
SV08 - Colonial Pipeline	ColP_NYT	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Colonial Pipeline acknowledged that its corporate computer networks had been hit by a ransomware attack, in which criminal groups hold data hostage until the victim pays a ransom
SV08 - Colonial Pipeline	ColP_BC	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Once they gain access to Windows domain credentials, they will deploy the ransomware throughout the network to encrypt devices.
SV09 - MS Exchange	MS21_Pitney	Angreifer > Einzelne	small scale hackers
SV09 - MS Exchange	MS21_Pitney	Angreifer > Staatlich motiviert	The hackers that were concluded to be responsible by several agencies, is an organization that goes by HAFNIUM [6]. HAFNIUM is a group that operates allegedly from a foreign nation [1]. Their goal is to find information from industries, disclose, and compromise the information. It has been noticed previously by Microsoft, as early as June of 2020. The group is known as a nation-state hacker, and is backed by an adversarial government.
SV09 - MS Exchange	MS21_Pitney	Angreifer > Staatlich motiviert	The group also had the resources needed for such an attack, as they are believed to be a nation-state hacker.
SV09 - MS Exchange	MS21_Pitney	Angreifer > Staatlich motiviert	nation-state
SV09 - MS Exchange	MS21_KoS_2	Angreifer > Staatlich motiviert	unusually aggressive Chinese cyber espionage unit that’s focused on stealing email from victim organizations
SV09 - MS Exchange	MS21_KoS_2	Angreifer > Staatlich motiviert	previously unidentified Chinese hacking crew it dubbed “Hafnium,”
SV09 - MS Exchange	MS21_KoS_2	Angreifer > Staatlich motiviert	Chinese cyber espionage group
SV09 - MS Exchange	MS21_KoS_2	Angreifer > Staatlich motiviert	the Chinese hacking group
SV09 - MS Exchange	MS21_KoS_2	Angreifer > Staatlich motiviert	The government cybersecurity expert said this most recent round of attacks is uncharacteristic of the kinds of nation-state level hacking typically attributed to China, which tends to be fairly focused on compromising specific strategic targets
SV09 - MS Exchange	MS21_KoS_2	Angreifer > Staatlich motiviert	“Its reckless,” the source said. “It seems out of character for Chinese state actors to be this indiscriminate.”
SV09 - MS Exchange	MS21_KoS_2	Angreifer > Staatlich motiviert	Microsoft has said the incursions by Hafnium on vulnerable Exchange servers are in no way connected to the separate SolarWinds-related attacks, in which a suspected Russian intelligence group installed backdoors in network management software used by more than 18,000 organizations.
SV09 - MS Exchange	MS21_KoS_1	Angreifer > Staatlich motiviert	Chinese Cyberspies
SV09 - MS Exchange	MS21_KoS_1	Angreifer > Staatlich motiviert	previously unidentified Chinese cyber espionage group

Dokumentgruppe	Dokumentname	Code	Segment
SV09 - MS Exchange	MS21_KoS_1	Angreifer > Staatlich motiviert	Microsoft says the flaws are being used by a previously unknown Chinese espionage group that's been dubbed "Hafnium,"
SV09 - MS Exchange	MS21_MS	Angreifer > Staatlich motiviert	Microsoft Threat Intelligence Center (MSTIC) attributes this campaign with high confidence to HAFNIUM, a group assessed to be state-sponsored and operating out of China, based on observed victimology, tactics and procedures.
SV09 - MS Exchange	MS21_Heise	Angreifer > Staatlich motiviert	mutmaßlich staatsnahe, aus China operierende Gruppe namens Hafnium
SV09 - MS Exchange	MS21_ITP	Angreifer > Staatlich motiviert	including Chinese state-backed cyber criminals, who had taken advantage of four zero-day vulnerabilities.
SV09 - MS Exchange	MS21_Pitney	Angreifer > Unabhängige Gruppierungen	foreign hacker group called HAFNIUM
SV09 - MS Exchange	MS21_Pitney	Angreifer > Unabhängige Gruppierungen	hacking groups.
SV09 - MS Exchange	MS21_KoS_3	Angreifer > Unabhängige Gruppierungen	Security firm ESET reports at least 10 "advanced persistent threat" (APT) cybercrime and espionage groups have been exploiting the newly-exposed Exchange flaws for their own purposes.
SV09 - MS Exchange	MS21_ITP	Angreifer > Unabhängige Gruppierungen	The popular email server had been hit by at least ten hacking groups
SV09 - MS Exchange	MS21_Pitney	Fehler > Organisatorische Schwächen	The biggest issue responders encountered when remediating this attack was that the Exchange servers were locally hosted. Due to this Microsoft could not push this patch through directly to all exposed machines [4].
SV09 - MS Exchange	MS21_Heise	Fehler > Organisatorische Schwächen	Zudem gab es beim Patchen eine Falle, die dazu führte, dass die Schwachstellen unter Umständen nicht geschlossen wurden. Erschwerend hinzu kommt Microsofts Patch-Policy, die zwingend zunächst das Upgrade auf ein noch unterstütztes kumulatives Update erforderte. Da diese vierteljährlich erscheinenden CUs nicht ganz einfach einzuspielen sind und es dabei in der Vergangenheit öfter zu Problemen und Fehlfunktionen kam, befinden sich viele Server auf einem älteren Stand.
SV09 - MS Exchange	MS21_Heise	Fehler > Organisatorische Schwächen	Die Folge: Die vom Hersteller veröffentlichten Patches konnten gar nicht eingespielt werden. Erst am 9. März ermöglichte Microsoft das Patchen mit älteren CU-Ständen.
SV09 - MS Exchange	MS21_Heise	Fehler > Organisatorische Schwächen	Eine verfehlte Produktpolitik (Exchange in jede Hundehütte), gepaart mit Produktmängeln (Exchange-Server zu patchen erfordert Know-how), in Kombination mit oft ungewarteten und damit über Sicherheitslücken angreifbaren Exchange-Servern.
SV09 - MS Exchange	MS21_Pitney	Fehler > Versäumnisse von Dritten	Since these companies were small, they had little need for extensive security. Due to this many of them had these servers connected to the internet, which allowed for Hafnium to gain access to these systems.
SV09 - MS Exchange	MS21_Pitney	Fehler > Versäumnisse von Dritten	As of March 9th Microsoft had confirmed that 100,000 servers were still not patched [28], and these systems were still being exploited at this time, and as of the most current report from Microsoft on March 12th there are still 82,000 servers not patched [29].
SV09 - MS Exchange	MS21_Pitney	Fehler > Versäumnisse von Dritten	Unlike a cloud where Microsoft has access to these machines the local machines had to be updated by whoever was managing them, such as a companies IT department, or in some cases people had to be brought in to install the patch to companies systems [32]. This led to a slow response time from server owners, and the only way to tell the owners how to fix this was to raise awareness.
SV09 - MS Exchange	MS21_KoS_3	Fehler > Versäumnisse von Dritten	Microsoft says there are still 82,000 unpatched Exchange servers exposed. "Groups trying to take advantage of this vulnerability are attempting to implant ransomware and other malware that could interrupt business continuity.
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	In January of 2021 there was a data breach in Microsoft Exchange Servers.
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	With all of these steps followed the hackers were able to take emails, company data, passwords, and usernames from the companies that they had infiltrated.
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Art des Vorfalls > Ransomware	Once the hack went public the hackers started to encrypt data, install ransomware and malware onto the systems.
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Art des Vorfalls > Ransomware	Many of the servers that have been compromised fell victim to ransomware attacks.
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Art des Vorfalls > Ransomware	The ransomware that was identified was DoejoCrypt/DearCry which was being deployed into systems that were still vulnerable
SV09 - MS Exchange	MS21_ITP	Gemeinsamkeiten > Art des Vorfalls > Ransomware	watch out for "human-operated ransomware attacks",
SV09 - MS Exchange	MS21_ITP	Gemeinsamkeiten > Art des Vorfalls > Ransomware	The ransomware, also known as DearCry, is typical in its approach, preventing users from being able to use their PCs or access their data until a payment is sent to hackers, according to information outlined by Microsoft.
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Branche > Betroffene Dritte	covering a wide range of companies rather than just a few. So much so that even the American government got involved as their information was also at risk.
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Branche > Betroffene Dritte	Many of these companies were relatively small, and had either a small IT department or no IT department at all

Dokumentgruppe	Dokumentname	Code	Segment
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Branche > Betroffene Dritte	 Fig. 5: Organization With Most Attacks
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Branche > Betroffene Dritte	As shown in the Fig. 4 The United States was hit the worst, but there were also countries like Germany, and the United Kingdoms who suffered from these attacks. In Fig. 5 The largest portion of servers to be attacked was Government, and Military which is what led to the United States government taking action in this large scale compromise of Exchange Servers [30].
SV09 - MS Exchange	MS21_KoS_2	Gemeinsamkeiten > Branche > Betroffene Dritte	small businesses, towns, cities and local governments
SV09 - MS Exchange	MS21_KoS_2	Gemeinsamkeiten > Branche > Betroffene Dritte	range of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs
SV09 - MS Exchange	MS21_KoS_2	Gemeinsamkeiten > Branche > Betroffene Dritte	The backdoor web shell is verifiably present on the networks of thousands of U.S. organizations, including banks, credit unions, non-profits, telecommunications providers, public utilities and police, fire and rescue units
SV09 - MS Exchange	MS21_KoS_2	Gemeinsamkeiten > Branche > Betroffene Dritte	It's police departments, hospitals, tons of city and state governments and credit unions
SV09 - MS Exchange	MS21_KoS_2	Gemeinsamkeiten > Branche > Betroffene Dritte	"On the call, many questions were from school districts or local governments that all need help,"
SV09 - MS Exchange	MS21_Heise	Gemeinsamkeiten > Branche > Betroffene Dritte	Alleine in Deutschland sind Zehntausende Exchange-Server betroffen, davon laut BSI einige in deutschen Bundesbehörden
SV09 - MS Exchange	MS21_ITP	Gemeinsamkeiten > Branche > Direkt Betroffene	Among the hundreds of thousands of victims are high-profile and political organisations such as the Norwegian government,
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Schwachstelle	discovered and exploited 4 different zero-day vulnerabilities
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Schwachstelle	The hackers exploited multiple errors within the code that created vulnerabilities [4]. The hackers had taken all of the vulnerabilities and in combination together used them to gain the initial access to Microsoft Exchange servers.
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Schwachstelle	The hackers would also set up back doors into the system [5], in the case that the they could not access after patches, and updates were deployed by Microsoft, fixing the vulnerabilities.
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Schwachstelle	The vulnerability that was in Microsoft Exchange came from multiple day one vulnerabilities, and the reason for the large scale coverage that came was due to the speed with which these vulnerabilities were discovered.
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Schwachstelle	When HAFNIUM scanned the servers for Microsoft Exchange, they were able to pin-point 4 zero-day vulnerabilities that they can exploit.
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Schwachstelle	These vulnerabilities allowed the hackers to access the servers that were only located on-site, in other words, the servers that were not connected to the cloud.
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Schwachstelle	The first of the four zero-day vulnerabilities is called CVE-2021-26855 [4]. This specific attack is a vulnerability that allows for server-side forgery (SSRF). Through this weakness, the hacker group was allowed to send arbitrary HTTPS requests to the server, and then say that the messages were real messages sent to the server. This weakness is especially concerning as anyone could access the server in this manner and it would not have to be a trusted source.
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Schwachstelle	The second vulnerability was called CVE-2021-26857 [15]. This particular vulnerability dealt with the Unified Messaging service within the Microsoft Exchange servers.
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Schwachstelle	Insecure deserialization makes a system vulnerable to Denial of Service attacks (DoS attacks), or bypass authentication [17].Standing by itself, this vulnerability does not appear to do much besides make the service unusable. Used with the other three vulnerabilities, this is a very good weapon for the hackers.In combination with the other weaknesses in the system, the hackers are able to pass data into the system that could harm the system as a whole.
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Schwachstelle	The third vulnerability was called CVE-2021-26858 [15]. This vulnerability dealt with an arbitrary file write. This means the hackers could have easily written random files within the server with information or even with programs to run [18]. The thing about this weakness is that the attacker would need to be able to authenticate who they were within the system. With the first vulnerability that was mentions, this is not a difficult task for the hackers.

Dokumentgruppe	Dokumentname	Code	Segment
SV09 - MS Exchange	MS21_Pitney	Gemeinsamkeiten > Schwachstelle	The final vulnerability that was a main part of the Microsoft Exchange breach was called CVE-2021-27065 [15]. This vulnerability is very similar to the third one mentioned in that it also deals with arbitrary file writing within the server after the hackers were authenticated. The hackers could and did use both of these to write files to any path within the server. The hackers used this also to create a web shell within the servers they exploited. Web shells are commonly used to escalate and maintain access within the system that was hacked [19]. This shell cannot perform any other actions except maintain access within the system after the hack is performed so it is always the next step to monitoring the system for hackers [19].
SV09 - MS Exchange	MS21_KoS_2	Gemeinsamkeiten > Schwachstelle	The espionage group is exploiting four newly-discovered flaws in Microsoft Exchange Server email software
SV09 - MS Exchange	MS21_KoS_1	Gemeinsamkeiten > Schwachstelle	According to Microsoft, Hafnium attackers have been observed combining all four zero-day flaws to target organizations running vulnerable Exchange Server products.
SV09 - MS Exchange	MS21_KoS_1	Gemeinsamkeiten > Schwachstelle	CVE-2021-26855 is a “server-side request forgery” (SSRF) flaw, in which a server (in this case, an on-premises Exchange Server) can be tricked into running commands that it should never have been permitted to run, such as authenticating as the Exchange server itself.
SV09 - MS Exchange	MS21_KoS_1	Gemeinsamkeiten > Schwachstelle	The attackers used CVE-2021-26857 to run code of their choice under the “system” account on a targeted Exchange server. The other two zero-day flaws — CVE-2021-26858 and CVE-2021-27065 — could allow an attacker to write a file to any part of the server.
SV09 - MS Exchange	MS21_MS	Gemeinsamkeiten > Schwachstelle	Microsoft has detected multiple 0-day exploits being used to attack on-premises versions of Microsoft Exchange Server in limited and targeted attacks.
SV09 - MS Exchange	MS21_MS	Gemeinsamkeiten > Schwachstelle	The vulnerabilities recently being exploited were CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065, all of which were addressed in today’s Microsoft Security Response Center (MSRC) release – Multiple Security Updates Released for Exchange Server.
SV09 - MS Exchange	MS21_MS	Gemeinsamkeiten > Schwachstelle	CVE-2021-26855 is a server-side request forgery (SSRF) vulnerability in Exchange which allowed the attacker to send arbitrary HTTP requests and authenticate as the Exchange server.
SV09 - MS Exchange	MS21_MS	Gemeinsamkeiten > Schwachstelle	CVE-2021-26857 is an insecure deserialization vulnerability in the Unified Messaging service. Insecure deserialization is where untrusted user-controllable data is deserialized by a program. Exploiting this vulnerability gave HAFNIUM the ability to run code as SYSTEM on the Exchange server. This requires administrator permission or another vulnerability to exploit.
SV09 - MS Exchange	MS21_MS	Gemeinsamkeiten > Schwachstelle	CVE-2021-26858 is a post-authentication arbitrary file write vulnerability in Exchange. If HAFNIUM could authenticate with the Exchange server then they could use this vulnerability to write a file to any path on the server. They could authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate admin’s credentials.
SV09 - MS Exchange	MS21_MS	Gemeinsamkeiten > Schwachstelle	CVE-2021-27065 is a post-authentication arbitrary file write vulnerability in Exchange. If HAFNIUM could authenticate with the Exchange server then they could use this vulnerability to write a file to any path on the server. They could authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate admin’s credentials.
SV09 - MS Exchange	MS21_Heise	Gemeinsamkeiten > Schwachstelle	Sicherheitsforscher des in Taiwan angesiedelten Unternehmens Devcore untersuchten die Sicherheit von Exchange-Systemen und stießen am 10. Dezember 2020 auf die erste, als ProxyLogon bezeichnete Schwachstelle CVE-2021-26855. Diese ermöglicht Angreifern, die reguläre Authentifizierung zu umgehen und sich als Administrator eines Exchange-Servers anzumelden. Im Rahmen der Untersuchungen fanden die Sicherheitsforscher eine weitere Schwachstelle, über die sie Dateien für eine Remote Code-Ausführung (RCE) in Exchange platzieren konnten.
SV09 - MS Exchange	MS21_Heise	Gemeinsamkeiten > Schwachstelle	Daraus bauten sie einen funktionsfähigen Proof of Concept Exploit. Mit dem ließ sich die Exchange-Authentifizierung umgehen und der Server kompromittieren.
SV09 - MS Exchange	MS21_Heise	Gemeinsamkeiten > Schwachstelle	Exchange-Server mit 0-Day-Exploits anzugreifen
SV09 - MS Exchange	MS21_Pitney	Reaktionen > Kommunikation	Immediately after data breach was discovered, Microsoft and other governmental security agencies alerted all the users
SV09 - MS Exchange	MS21_Pitney	Reaktionen > Kommunikation	Microsoft had now officially announced the vulnerabilities that were found.
SV09 - MS Exchange	MS21_KoS_2	Reaktionen > Kommunikation	“The best protection is to apply updates as soon as possible across all impacted systems,” a Microsoft spokesperson said in a written statement. “We continue to help customers by providing additional investigation and mitigation guidance. Impacted customers should contact our support teams for additional help and resources.”
SV09 - MS Exchange	MS21_MS	Reaktionen > Kommunikation	We are sharing this information with our customers and the security community to emphasize the critical nature of these vulnerabilities and the importance of patching all affected systems immediately to protect against these exploits and prevent future abuse across the ecosystem. This blog also continues our mission to shine a light on malicious actors and elevate awareness of the sophisticated tactics and techniques used to target our customers. The related IOCs, Azure Sentinel advanced hunting queries, and Microsoft Defender for Endpoint product detections and queries shared in this blog will help SOCs proactively hunt for related activity in their environments and elevate any alerts for remediation.

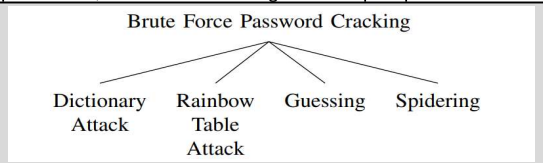
Dokumentgruppe	Dokumentname	Code	Segment
SV09 - MS Exchange	MS21_MS	Reaktionen > Kommunikation	The Microsoft Exchange Server team has published a blog post on these new Security Updates providing a script to get a quick inventory of the patch-level status of on-premises Exchange servers and answer some basic questions around installation of these patches.
SV09 - MS Exchange	MS21_MS	Reaktionen > Kommunikation	Microsoft is releasing a feed of observed indicators of compromise (IOCs) in related attacks. This feed is available in both CSV and JSON formats. This information is being shared as TLP:WHITE.
SV09 - MS Exchange	MS21_Heise	Reaktionen > Kommunikation	Am 5. Januar 2021 informierten sie das Microsoft Security Resource Center (MSRC), wie Devcore auf der Proxylogon-Seite dokumentiert.
SV09 - MS Exchange	MS21_Heise	Reaktionen > Kommunikation	Das MSRC bestätigte die Schwachstellen und den PoC im Zeitraum 6. bis 8. Januar 2021, stellte aber bis Anfang Februar 2021 kein Sicherheitsupdate bereit. Auf Nachfrage der Sicherheitsforscher hieß es, verschiedene Aspekte seien zur einzelnen Überprüfung aufgeteilt worden. Microsoft versprach, mindestens einen Fix freizugeben, bevor die Frist zur Veröffentlichung der Schwachstelle ablaufen werde.
SV09 - MS Exchange	MS21_Pitney	Reaktionen > Maßnahmen > Dritte	Microsoft was working on a patch to fix these vulnerabilities while it was still small scale, but then the hack went viral. Microsoft security reports have shown that before a patch could be deployed HAFNIUM had decided to ramp up the identification of vulnerable servers, which allowed for the number of compromised systems to spike.
SV09 - MS Exchange	MS21_Pitney	Reaktionen > Maßnahmen > Dritte	The announcement led to a large surge in attacks [25], as now it was public that there was something wrong. This with HAFNIUM releasing the hack that was implemented to the public created a chain reaction of more servers being compromised [14]. HAFNIUM, other groups, and amateur hackers now started to scan for more compromised Exchange Servers and started to install back doors on as many of them as possible.
SV09 - MS Exchange	MS21_Pitney	Reaktionen > Maßnahmen > Dritte	After Microsoft had released the news of the exploit the amount of systems being attacked increased, and more servers became compromised.
SV09 - MS Exchange	MS21_KoS_2	Reaktionen > Maßnahmen > Dritte	Meanwhile, CISA has issued an emergency directive ordering all federal civilian departments and agencies running vulnerable Microsoft Exchange servers to either update the software or disconnect the products from their networks.
SV09 - MS Exchange	MS21_KoS_2	Reaktionen > Maßnahmen > Dritte	Security researchers have published several tools for detecting vulnerable servers. One of those tools, a script from Microsoft's Kevin Beaumont, is available from Github.
SV09 - MS Exchange	MS21_ITP	Reaktionen > Maßnahmen > Dritte	Vietnam-based independent security researcher Nguyen Jang is believed to have shared the first functional public proof-of-concept exploit for a group of vulnerabilities in Microsoft Exchange servers known as ProxyLogon, according to reports by The Record.
SV09 - MS Exchange	MS21_Pitney	Reaktionen > Maßnahmen > Opferseitig	Microsoft has released an effective security patch to stop the exploitation of the vulnerabilities.
SV09 - MS Exchange	MS21_Pitney	Reaktionen > Maßnahmen > Opferseitig	Microsoft had set a date for "Patch Tuesday", but had to escalate the progress of development as the attacks had become a crisis. The patch was deployed on March 2nd
SV09 - MS Exchange	MS21_KoS_2	Reaktionen > Maßnahmen > Opferseitig	On March 2, Microsoft released emergency security updates to plug four security holes in Exchange Server versions 2013 through 2019 that hackers were actively using to siphon email communications from Internet-facing systems running Exchange.
SV09 - MS Exchange	MS21_MS	Reaktionen > Maßnahmen > Opferseitig	The Exchange Server team has created a script to run a check for HAFNIUM IOCs to address performance and memory concerns.
SV09 - MS Exchange	MS21_Heise	Reaktionen > Maßnahmen > Opferseitig	Im Verlauf der Korrespondenz kündigte Microsoft am 18. Februar den 9. März 2021 (Patchday) als Termin für die Freigabe der Exchange-Sicherheitsupdates an. Doch dann veröffentlichte Microsoft die Sicherheitsupdates außerplanmäßig bereits am 3. März 2021 mitsamt einer Sicherheitswarnung.
SV09 - MS Exchange	MS21_Heise	Reaktionen > Maßnahmen > Opferseitig	Zu dieser explosiven Gemengelage gesellt sich die Tatsache, dass sich Microsoft doch reichlich Zeit gelassen hat, die kritischen Sicherheits-Updates bereitzustellen.
SV09 - MS Exchange	MS21_KoS_3	Reaktionen > Maßnahmen > Opferseitig	On Mar. 2, Microsoft patched four flaws in Exchange Server 2013 through 2019. Exchange Server 2010 is no longer supported, but the software giant made a "defense in depth" exception and gave Server 2010 users a freebie patch, too. That means the vulnerabilities the attackers exploited have been in the Microsoft Exchange Server code base for more than ten years.
SV09 - MS Exchange	MS21_KoS_3	Reaktionen > Maßnahmen > Opferseitig	Mar. 2: A week earlier than previously planned, Microsoft releases updates to plug 4 zero-day flaws in Exchange.
SV09 - MS Exchange	MS21_KoS_3	Reaktionen > Maßnahmen > Opferseitig	Working exploit for Exchange flaw published on Github and then removed by Microsoft, which owns the platform.
SV09 - MS Exchange	MS21_ITP	Reaktionen > Maßnahmen > Opferseitig	"We have detected and are now blocking a new family of ransomware being used after an initial compromise of unpatched on-premises Exchange Servers," Microsoft's Security Intelligence team informed its Twitter followers.
SV09 - MS Exchange	MS21_ITP	Reaktionen > Maßnahmen > Opferseitig	"In accordance with our Acceptable Use Policies, we disabled the gist following reports that it contains proof of concept code for a recently disclosed vulnerability that is being actively exploited," they added.
SV09 - MS Exchange	MS21_Pitney	Reaktionen > Vorschläge	The main remedy that Microsoft highly recommended to its users is that they update their systems to at least the March 2021 version as all the previous versions had the vulnerabilities that HAFNIUM used to break into the servers [1].
SV09 - MS Exchange	MS21_Pitney	Reaktionen > Vorschläge	Another remedy that Microsoft suggested was to block off port 443,

Dokumentgruppe	Dokumentname	Code	Segment
SV09 - MS Exchange	MS21_Pitney	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	To solve the issue of the speed of exfiltration, they started to encrypt the data they were taking and using a 7- zip to compress the files and take them quicker.
SV09 - MS Exchange	MS21_Pitney	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Once the hack went public the hackers started to encrypt data, install ransomware and malware onto the systems. Through this the hackers were able to take a lot of information.
SV09 - MS Exchange	MS21_Pitney	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	This allowed for hackers to enter into vulnerable systems, and start to encrypt the data that was being stored within the systems.
SV09 - MS Exchange	MS21_Pitney	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	As this was seen as one of the most common forms of ransomware used in these attacks it could be inferred that many groups were put into situations where their data was encrypted until an amount of money was paid to the malicious agents.
SV10 - T-Mobile	TM_Faircloth	Angreifer > Einzelne	The person who took responsibility for the attack, John Erin Binns, is a 21 year old originally from the United States [5].
SV10 - T-Mobile	TM_CSO	Angreifer > Einzelne	In an interview with the Wall Street Journal, a 21-year-old American man living in Turkey claimed to be responsible for the attack on T-Mobile.
SV10 - T-Mobile	TM_CSO	Angreifer > Einzelne	It remains uncertain whether he acted alone, part of a group, or if any of the stolen data has been sold thus far.
SV10 - T-Mobile	TM_WSJ	Angreifer > Einzelne	John Binns, a 21-year-old American who moved to Turkey a few years ago, told The Wall Street Journal he was behind the security breach
SV10 - T-Mobile	TM_WSJ	Angreifer > Einzelne	It is unclear whether Mr. Binns worked alone.
SV10 - T-Mobile	TM_KoS_1	Angreifer > Einzelne	How do we know all this about IntelSecrets/IRDev/V0rtex? That identity has acknowledged as much in a series of bizarre lawsuits filed by a person who claims their real name is John Erin Binns. The same Binns identity operates the website intelsecrets[.]su.
SV10 - T-Mobile	TM_KoS_2	Angreifer > Einzelne	The intrusion first came to light on Twitter when the account @und0xxed started tweeting the details, and someone on a cybercrime forum began selling what they claimed were more than 100 million freshly hacked records from T-Mobile.
SV10 - T-Mobile	TM_KoS_1	Angreifer > Unabhängige Gruppierungen	The intrusion came to light on Twitter when the account @und0xxed started tweeting the details. Reached via direct message, Und0xxed said they were not involved in stealing the databases but was instead in charge of finding buyers for the stolen T-Mobile customer data.
SV10 - T-Mobile	TM_KoS_1	Angreifer > Unabhängige Gruppierungen	The Twitter profile for the account @Und0xxed includes a shout out to @IntelSecrets, the Twitter account of a fairly elusive hacker who also has gone by the handles IRDev and V0rtex. Asked if @IntelSecrets was involved in the T-Mobile intrusion, @und0xxed confirmed that it was.
SV10 - T-Mobile	TM_Faircloth	Fehler > Organisatorische Schwächen	T-Mobile itself requires extensive measures to prevent a similar data breach from occurring in the future. The number one reason for failure in system security is lack of employees following protocol. Routers typically come with an admin and password that can be found on hackers lists of common combinations. The router Binns located to initialize his attack was unprotected from outside access as were the testing and development servers. Ensuring protocol is followed for router security is paramount to preventing future breaches.
SV10 - T-Mobile	TM_Faircloth	Fehler > Organisatorische Schwächen	Brute Force: There are common ways of protecting against brute force attacks. These attacks require time and multiple attempts, therefore common defenses limit these two factors. Regular computer or smart phone users would be familiar with the limit of incorrect passwords that can be entered in a given time frame. A user may only input an incorrect password three times before having to wait several minutes until they are allowed to try again. Some versions impose growing wait times for subsequent failures or additional verification after a specified number of failed attempts.
SV10 - T-Mobile	TM_Faircloth	Fehler > Organisatorische Schwächen	The defense methods listed here are all relatively simple and are only a small subsection of the defenses that could be implemented to reliably stop brute force attacks. Had T-Mobile implemented better defenses and alerts using these or other methods, it is possible the August 2021 breach wouldn't have escalated to the scale that occurred.
SV10 - T-Mobile	TM_Faircloth	Fehler > Organisatorische Schwächen	One of the easiest and most popular ways to mitigate SSH tunneling misuse involves setting up a custom SSH port "Because by default, SSH comes listening on port 22, which is widely known among attackers and security tools/port scanners that launch brute force attacks against it" [18]
SV10 - T-Mobile	TM_Faircloth	Fehler > Organisatorische Schwächen	Another technique to mitigate attacks that use SSH tunneling is to disable root login to SSH servers. Even when the root password is relatively strong, it is still susceptible to brute force, and once the bad actor has access to the root user, they can perform a number of brute force attacks against the entire network.
SV10 - T-Mobile	TM_Faircloth	Fehler > Organisatorische Schwächen	System Architecture: System and network separation can provide a layer of security in and of itself. Compartmentalizing systems, such as using a demilitarized zone to proxy traffic in and out of a network also lends itself to a more a secure architecture. Requiring virtual private network gateways to access various parts of the network are additional measures that can be utilized. Most importantly having a production and testing environment produced on a separate network to the main customer database is a basic yet essential change [19].

Dokumentgruppe	Dokumentname	Code	Segment
SV10 - T-Mobile	TM_Faircloth	Fehler > Organisatorische Schwächen	Password security is a major factor in the success or failure of a bad actors attempt at SSH tunneling into sensitive machines. A large company such as T-Mobile will have to manage their access to servers at scale and compartmentalize their production servers from their databases and other systems that are on their network.
SV10 - T-Mobile	TM_Faircloth	Fehler > Organisatorische Schwächen	Secure passwords could have mitigated or outright prevented the breach at any point during the hack. The use of insecure passwords can be reduced through company education on what a secure password is, or through programmatic system enforcement of secure passwords. It may not be possible to achieve 100 percent enforcement of secure password use throughout a company as large as T-Mobile and additional security measures should also be in place.
SV10 - T-Mobile	TM_CSO	Fehler > Organisatorische Schwächen	The second, Durwalla v T-Mobile USA, stated that T-Mobile “failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect its customers’ personal information, yet again putting millions of customers at great risk of scams and identity theft.”
SV10 - T-Mobile	TM_WSJ	Fehler > Organisatorische Schwächen	Several cybersecurity experts said the public details of the hack and reports of previous T-Mobile breaches show the carrier’s defenses need improvement. Many of the records reported stolen were from prospective clients or former customers long gone. “That to me does not sound like good data management practices,” said Glenn Gerstell, a former general counsel for the National Security Agency.
SV10 - T-Mobile	TM_Faircloth	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	This is T-Mobiles largest data breach to-date
SV10 - T-Mobile	TM_CSO	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	exposed via a data breach
SV10 - T-Mobile	TM_KoS_1	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	T-Mobile acknowledged that a data breach
SV10 - T-Mobile	TM_KoS_2	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	T-Mobile is warning that a data breach
SV10 - T-Mobile	TM_KoS_2	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	breach of data on millions of customers
SV10 - T-Mobile	TM_TV	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	T-Mobile has released more information about its most recent data breach,
SV10 - T-Mobile	TM_TM	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	August 2021 cybersecurity data breach incident
SV10 - T-Mobile	TM_Faircloth	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	Spidering: Spidering, also known as web crawling, involves scraping company web-pages and other public sites for information that may be available about a target. For example job postings are a very useful source of information for a hacker. Job postings include a job description which often lists what types of technology the potential employee will have to use and thus what technology the hacker may potentially target.
SV10 - T-Mobile	TM_Faircloth	Gemeinsamkeiten > Branche > Direkt Betroffene	T-Mobile, the now third largest cellular network carrier in the United States
SV10 - T-Mobile	TM_Faircloth	Gemeinsamkeiten > Branche > Direkt Betroffene	T-Mobile was acquired and renamed in 2001 by the German telecommunications company Deutsche Telekom AG [10]. It has since been purchased or merged with multiple companies, the latest being Sprint, making it the third largest telecommunications company in the world.
SV10 - T-Mobile	TM_CSO	Gemeinsamkeiten > Branche > Direkt Betroffene	Telecommunications giant T-Mobile
SV10 - T-Mobile	TM_WSJ	Gemeinsamkeiten > Branche > Direkt Betroffene	The Bellevue, Wash., company is the second-largest U.S. mobile carrier with roughly 90 million cellphones connecting to its networks.
SV10 - T-Mobile	TM_KoS_1	Gemeinsamkeiten > Branche > Direkt Betroffene	Communications giant T-Mobile
SV10 - T-Mobile	TM_Faircloth	Gemeinsamkeiten > Schwachstelle	The attacker gained entry into T-Mobile’s systems through an unprotected router and used brute force techniques to access the sensitive information stored on the internal servers.
SV10 - T-Mobile	TM_Faircloth	Gemeinsamkeiten > Schwachstelle	T-Mobile’s data was accessed July 2021 through an unprotected router located in Washington
SV10 - T-Mobile	TM_Faircloth	Gemeinsamkeiten > Schwachstelle	Once having accessed the router, the hacker was able to access a testing environment. Afterwards, Binns used brute force login techniques to break into an internal computer with access to customer data.
SV10 - T-Mobile	TM_Faircloth	Gemeinsamkeiten > Schwachstelle	In July Binns found access to an unsecured T-Mobile router near East Wenatchee, Washington [5]. From this router he was able to SSH tunnel into a testing and production environment before he hit any preventative security measures. In order to proceed further, Binns employed brute force password cracking methods.
SV10 - T-Mobile	TM_Faircloth	Gemeinsamkeiten > Schwachstelle	Hardware companies often use default passwords for their products. Knowing this hackers are able to look up default passwords used for their target’s technology. If the default password is still in use, then the attacker will be able to easily guess and gain access.
SV10 - T-Mobile	TM_CSO	Gemeinsamkeiten > Schwachstelle	According to the report, John Binns told reporters that he originally gained access to T-Mobile’s network in July via an unprotected router.

Dokumentgruppe	Dokumentname	Code	Segment
SV10 - T-Mobile	TM_WSJ	Gemeinsamkeiten > Schwachstelle	In messages with the Journal, Mr. Binns said he managed to pierce T-Mobile's defenses after discovering in July an unprotected router exposed on the internet. He said he had been scanning T-Mobile's known internet addresses for weak spots using a simple tool available to the public.
SV10 - T-Mobile	TM_WSJ	Gemeinsamkeiten > Schwachstelle	Mr. Binns said he used that entry point to hack into the cellphone carrier's data center outside East Wenatchee, Wash., where stored credentials allowed him to access more than 100 servers.
SV10 - T-Mobile	TM_KoS_1	Gemeinsamkeiten > Schwachstelle	Und0xxed said the hackers found an opening in T-Mobile's wireless data network that allowed access to two of T-Mobile's customer data centers. From there, the intruders were able to dump a number of customer databases totaling more than 100 gigabytes.
SV10 - T-Mobile	TM_CSO	Reaktionen > Kommunikation	With news of the incident making headlines around the globe, T-Mobile issued a statement confirming that unauthorized access to some T-Mobile data had occurred, though investigations were yet to determine if any personal customer information was involved. "We have been working around the clock to investigate claims being made that T-Mobile data may have been illegally accessed. We take the protection of our customers very seriously and we are conducting an extensive analysis alongside digital forensic experts to understand the validity of these claims, and we are coordinating with law enforcement."
SV10 - T-Mobile	TM_WSJ	Reaktionen > Kommunikation	On Aug. 13, the security research firm Unit221B LLC reported to T-Mobile that an account was attempting to sell T-Mobile customer data, according to the security firm. Two days later, T-Mobile publicly acknowledged it was investigating a potential breach.
SV10 - T-Mobile	TM_WSJ	Reaktionen > Kommunikation	T-Mobile last week started notifying affected customers.
SV10 - T-Mobile	TM_Faircloth	Reaktionen > Maßnahmen > Dritte	As a result of the five data breaches in the last three years, and the fact that each one has put customer data at risk, various lawsuits have emerged against the company claiming negligence on the part of T-Mobile.
SV10 - T-Mobile	TM_CSO	Reaktionen > Maßnahmen > Dritte	T-Mobile was issued two lawsuits following the breach of its data. The first, Espanoza v. T-Mobile USA, claimed that the company put plaintiffs at risk over its failure to adequately protect customers as a result of negligent conduct. "As a result of the data breach, plaintiffs and class members are exposed to a heightened present and imminent risk of fraud and identity theft," the complaint read.
SV10 - T-Mobile	TM_CSO	Reaktionen > Maßnahmen > Dritte	Both suits seek various actions for violations of the Washington Consumer Protection Act and the California Consumer Privacy Act, including compensation and reimbursement of out-of-pocket costs for efforts to repair any damage caused by the data breach.
SV10 - T-Mobile	TM_NYT	Reaktionen > Maßnahmen > Dritte	T-Mobile has agreed to a settlement totaling $500 million in a class-action lawsuit filed by customers after the company disclosed in August that sensitive data had been breached in a cyberattack.
SV10 - T-Mobile	TM_NYT	Reaktionen > Maßnahmen > Dritte	In a court filing late Friday, the mobile phone giant said it would pay $350 million to settle the customers' claims and spend $150 million over the next few years bolstering its cybersecurity protection and technologies.
SV10 - T-Mobile	TM_Faircloth	Reaktionen > Maßnahmen > Opferseitig	T-Mobile "is offering two years of McAfee's ID Theft Protection Service" for free, to all those affected [3].
SV10 - T-Mobile	TM_CSO	Reaktionen > Maßnahmen > Opferseitig	The company said it was confident that the entry point used to gain access had been closed, and that it was continuing its deep technical review of the situation across systems to identify the nature of any data that was illegally accessed.
SV10 - T-Mobile	TM_CSO	Reaktionen > Maßnahmen > Opferseitig	We immediately began an exhaustive investigation into these claims and brought in world-leading cybersecurity experts to help with our assessment."
SV10 - T-Mobile	TM_CSO	Reaktionen > Maßnahmen > Opferseitig	T-Mobile said it located and immediately closed the access point it believed was used to illegally gain entry to its servers, and while its investigation was still underway, it confirmed that the data stolen included some personal information.
SV10 - T-Mobile	TM_CSO	Reaktionen > Maßnahmen > Opferseitig	T-Mobile said it would be issuing communications to advise customers on next steps and recommended action to avoid falling victim to follow-on attacks. This included the offer of two years of free identity protection services and advice that all T-Mobile postpaid customers should change their PIN. "This precaution is despite the fact that we have no knowledge that any postpaid account PINs were compromised," it added. T-Mobile also offered an extra step to protect mobile accounts with its Account Takeover Protection capabilities for postpaid customers and said it would be publishing a unique webpage for information and solutions to help customers take steps to further protect themselves.
SV10 - T-Mobile	TM_CSO	Reaktionen > Maßnahmen > Opferseitig	T-Mobile reiterated its confidence that it has closed off the access and egress points the bad actor used in the attack.
SV10 - T-Mobile	TM_WSJ	Reaktionen > Maßnahmen > Opferseitig	T-Mobile confirmed that more than 50 million customer records have been stolen. The wireless carrier said it had repaired the security hole that enabled the breach. "We are confident that we have closed off the access and egress points the bad actor used in the attack," it said in a statement.
SV10 - T-Mobile	TM_WSJ	Reaktionen > Maßnahmen > Opferseitig	The company offered two years of identity-protection services and reminded customers to regularly update passwords and PIN codes as a standard precaution.
SV10 - T-Mobile	TM_KoS_1	Reaktionen > Maßnahmen > Opferseitig	"We are confident that the entry point used to gain access has been closed, and we are continuing our deep technical review of the situation across our systems to identify the nature of any data that was illegally accessed," the statement continued.

Dokumentgruppe	Dokumentname	Code	Segment
SV10 - T-Mobile	TM_KoS_2	Reaktionen > Maßnahmen > Opferseitig	“We have already proactively reset ALL of the PINs on these accounts to help protect these customers, and we will be notifying accordingly right away.
SV10 - T-Mobile	TM_KoS_2	Reaktionen > Maßnahmen > Opferseitig	T-Mobile said it would pay for two years of identity theft protection services for any affected customers, and that it was offering “an extra step to protect your mobile account with our Account Takeover Protection capabilities for postpaid customers, which makes it harder for customer accounts to be fraudulently ported out and stolen.”
SV10 - T-Mobile	TM_TV	Reaktionen > Maßnahmen > Opferseitig	T-Mobile has added a page on its site where customers can go for information as well as shortcuts to change their PINs and passwords. It’s offering two years of free identity protection services from McAfee, recommends postpaid customers change their PIN, and mentions its Account Takeover Protection capabilities to prevent SIM-swapping attacks.
SV10 - T-Mobile	TM_TM	Reaktionen > Maßnahmen > Opferseitig	Our investigation is ongoing and will continue for some time, but at this point, we are confident that we have closed off the access and egress points the bad actor used in the attack.
SV10 - T-Mobile	TM_TM	Reaktionen > Maßnahmen > Opferseitig	As we previously reported, approximately 850,000 active T-Mobile prepaid customer names, phone numbers and account PINs were exposed. We have proactively reset ALL of the PINs on these accounts.
SV10 - T-Mobile	TM_TM	Reaktionen > Maßnahmen > Opferseitig	Offering two years of free identity protection services with McAfee’s ID Theft Protection Service to any person who believes they may be affected
SV10 - T-Mobile	TM_TM	Reaktionen > Maßnahmen > Opferseitig	Supporting customers with additional best practices and practical security steps like resetting PINs and passwords Publishing a customer support webpage that includes information and access to these tools at https://www.t-mobile.com/brand/data-breach-2021
SV10 - T-Mobile	TM_TM	Reaktionen > Maßnahmen > Opferseitig	We immediately began an exhaustive investigation into these claims and brought in world-leading cybersecurity experts to help with our assessment. We then located and immediately closed the access point that we believe was used to illegally gain entry to our servers. Yesterday, we were able to verify that a subset of T-Mobile data had been accessed by unauthorized individuals. We also began coordination with law enforcement as our forensic investigation continued.
SV10 - T-Mobile	TM_TM	Reaktionen > Maßnahmen > Opferseitig	As a result of this finding, we are taking immediate steps to help protect all of the individuals who may be at risk from this cyberattack. Communications will be issued shortly to customers outlining that T-Mobile is: Immediately offering 2 years of free identity protection services with McAfee’s ID Theft Protection Service.
SV10 - T-Mobile	TM_TM	Reaktionen > Maßnahmen > Opferseitig	Offering an extra step to protect your mobile account with our Account Takeover Protection capabilities for postpaid customers, which makes it harder for customer accounts to be fraudulently ported out and stolen. Publishing a unique web page later on Wednesday for one stop information and solutions to help customers take steps to further protect themselves.
SV10 - T-Mobile	TM_TM	Reaktionen > Maßnahmen > Opferseitig	At this time, we have also been able to confirm approximately 850,000 active T-Mobile prepaid customer names, phone numbers and account PINs were also exposed. We have already proactively reset ALL of the PINs on these accounts to help protect these customers, and we will be notifying accordingly right away.
SV10 - T-Mobile	TM_TM	Reaktionen > Vorschläge	Recommending that all eligible T-Mobile customers sign up for free scam-blocking protection through Scam Shield
SV10 - T-Mobile	TM_TM	Reaktionen > Vorschläge	Recommending all T-Mobile postpaid customers proactively change their PIN by going online into their T-Mobile account or calling our Customer Care team by dialing 611 on your phone. This precaution is despite the fact that we have no knowledge that any postpaid account PINs were compromised.
SV10 - T-Mobile	TM_Faircloth	Rolle der Kryptografie > Schutz	SSH tunneling is “a method of transporting arbitrary networking data over an encrypted SSH connection” [14]. The intended purpose of SSH tunneling is to protect important data from being exposed while in transit to/from a client and a server. For this reason, many companies, including T-Mobile, utilize SSH tunneling for multiple purposes, including better security for their applications. SSH tunneling encrypts the data in transit
SV10 - T-Mobile	TM_Faircloth	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	Stored Data Encryption: The encryption of sensitive data is an essential practice in computer security. We hypothesize that the data stolen from T-Mobile’s servers was not encrypted. Refer to the events around August 4th and on August 13th in Figure 2. Binns began exfiltration around August 4th and would have to post on the hacking forum before August 13th when Unit221B notified T-Mobile of the listing to sell the stolen data. This means either the stolen data took at most nine days to decrypt, or the data wasn’t encrypted in the database. Given the scale of the data breach that took place, it is most likely that the data would take longer than nine days to decrypted using the tools available to Binns. Data with a sensitive nature such as birth dates and names associated with Social Security Numbers should be stored hashed or encrypted within the database to preserve the security to the customers.
SV10 - T-Mobile	TM_Faircloth	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	It is strongly speculated by this paper that data was stored in plain text, giving Binns the opportunity to sell the data through a hacker forum without the need for decryption.
SV10 - T-Mobile	TM_KoS_1	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	They claim one of those databases holds the name, date of birth, SSN, drivers license information, plaintext security PIN, address and phone number of 36 million T-Mobile customers in the United States — all going back to the mid-1990s.

Dokumentgruppe	Dokumentname	Code	Segment
SV10 - T-Mobile	TM_Faircloth	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	Brute Force Password cracking.
SV10 - T-Mobile	TM_Faircloth	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	Rainbow Table Attack: Rainbow Table attacks attempt to find passwords by cycling through tables of hashed passwords, and are effective against complex passwords.
SV10 - T-Mobile	TM_Faircloth	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	
SV10 - T-Mobile	TM_Faircloth	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	Dictionary Attack: Dictionary attacks use a list of words and attempts each one as a possible password.
SV10 - T-Mobile	TM_Faircloth	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	benefit of a much faster attack speed, as it is very quick to check a hashed password against a precomputed table of hashes. If the hashed password matches an entry in the rainbow table, then the password has been cracked, effectively undoing the hash. As an example, a bad actor may take a brute force table of passwords and hash those passwords into a table. The hashed password that is set to be cracked is then compared against the precomputed table. If there is a match between the target hash and an entry on the table, then the original password is known and the attack is a success.
SV10 - T-Mobile	TM_Faircloth	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	he remotely accessed T-Mobile's data through SSH tunneling
SV10 - T-Mobile	TM_Faircloth	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	When SSH tunneling is active and not purposefully handled, the content being transmitted bypasses both Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), allowing intruders to "sneak past" the firewall into the internal systems of the corporation. Once the hacker has access to the internal servers, they can again use SSH tunneling "to leave a backdoor into the internal network.
SV10 - T-Mobile	TM_Faircloth	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	It can also be used for hiding an attacker's tracks by bouncing an attack through multiple devices that permit uncontrolled tunneling" [14]. With such access to the internal servers, hackers can collect, analyze, and steal any sensitive information stored there.
SV11 - LastPass	LP_LP_1	Angreifer > Unbekannt	To date, however, the identity of the threat actor and their motivation remains unknown.
SV11 - LastPass	LP_LP_1	Fehler > Menschliches Versagen	A software engineer's corporate laptop was compromised
SV11 - LastPass	LP_LP_2	Fehler > Menschliches Versagen	This was accomplished by targeting the DevOps engineer's home computer and exploiting a vulnerable third-party media software package
SV11 - LastPass	LP_LP_2	Fehler > Menschliches Versagen	The threat actor was able to capture the employee's master password as it was entered, after the employee authenticated with MFA, and gain access to the DevOps engineer's LastPass corporate vault.
SV11 - LastPass	LP_KoS	Fehler > Menschliches Versagen	The vulnerability exploited by the intruders was patched back in 2020, but the employee never updated his Plex software.
SV11 - LastPass	LP_KoS	Fehler > Menschliches Versagen	Connor said he's kicking himself because he recently started the process of migrating his cryptocurrency to a new wallet protected by a new seed phrase. But he never finished that migration process. And then he got hacked. "I'd set up a brand new wallet with new keys," he said. "I had that ready to go two months ago, but have been procrastinating moving things to the new wallet."
SV11 - LastPass	LP_TV	Fehler > Menschliches Versagen	One of the engineers was targeted by exploiting an (undisclosed) vulnerable third-party media software package on their home computer and installing keylogger malware.
SV11 - LastPass	LP_TV	Fehler > Menschliches Versagen	After installing the keylogger, LastPass says the threat actor "was able to capture the employee's master password as it was entered, after the employee authenticated with [multifactor authentication], and gain access to the DevOps engineer's LastPass corporate vault."
SV11 - LastPass	LP_Ars	Fehler > Menschliches Versagen	same attacker hacked an employee's home computer and obtained a decrypted vault available to only a handful of company developers.
SV11 - LastPass	LP_KoS	Fehler > Organisatorische Schwächen	LastPass says that since 2018 it has required a twelve-character minimum for master passwords, which the company said "greatly minimizes the ability for successful brute force password guessing." But Palant said while LastPass indeed improved its master password defaults in 2018, it did not force all existing customers who had master passwords of lesser lengths to pick new credentials that would satisfy the 12-character minimum.
SV11 - LastPass	LP_KoS	Fehler > Organisatorische Schwächen	"If you are a LastPass customer, chances are that you are completely unaware of this requirement," Palant wrote. "That's because LastPass didn't ask existing customers to change their master password. I had my test account since 2018, and even today I can log in with my eight-character password without any warnings or prompts to change it."

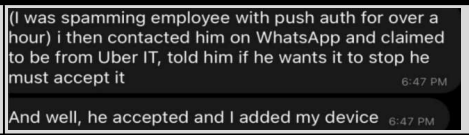
Dokumentgruppe	Dokumentname	Code	Segment
SV11 - LastPass	LP_KoS	Fehler > Organisatorische Schwächen	Palant believes LastPass also failed to upgrade many older, original customers to more secure encryption protections that were offered to newer customers over the years. One important setting in LastPass is the number of “iterations,” or how many times your master password is run through the company’s encryption routines. The more iterations, the longer it takes an offline attacker to crack your master password.
SV11 - LastPass	LP_KoS	Fehler > Organisatorische Schwächen	Palant noted last year that for many older LastPass users, the initial default setting for iterations was anywhere from “1” to “500.” By 2013, new LastPass customers were given 5,000 iterations by default. In February 2018, LastPass changed the default to 100,100 iterations. And very recently, it upped that again to 600,000.
SV11 - LastPass	LP_KoS	Fehler > Organisatorische Schwächen	“Worse yet, for reasons that are beyond me, LastPass didn’t complete this migration,” Palant wrote. “My test account is still at 5,000 iterations, as are the accounts of many other users who checked their LastPass settings. LastPass would know how many users are affected, but they aren’t telling that. In fact, it’s painfully obvious that LastPass never bothered updating users’ security settings. Not when they changed the default from 1 to 500 iterations. Not when they changed it from 500 to 5,000. Only my persistence made them consider it for their latest change. And they still failed implementing it consistently.”
SV11 - LastPass	LP_KoS	Fehler > Organisatorische Schwächen	A chart on Palant’s blog post offers an idea of how increasing password iterations dramatically increases the costs and time needed by the attackers to crack someone’s master password. Palant said it would take a single GPU about a year to crack a password of average complexity with 500 iterations, and about 10 years to crack the same password run through 5,000 iterations.
SV11 - LastPass	LP_KoS	Fehler > Organisatorische Schwächen	Weaver said LastPass deserves blame for not having upgraded iteration counts for all users a long time ago, and called the latest forced upgrades “a stunning indictment of the negligence on the part of LastPass.”
SV11 - LastPass	LP_KoS	Fehler > Organisatorische Schwächen	“That they never even notified all those with iteration counts of less than 100,000 — who are really vulnerable to brute force even with 8-character random passwords or ‘correct horse battery staple’ type passphrases — is outright negligence,” Weaver said. “I would personally advocate that nobody ever uses LastPass again: Not because they were hacked. Not because they had an architecture (unlike 1Password) that makes such hacking a problem. But because of their consistent refusal to address how they screwed up and take proactive efforts to protect their customers.”
SV11 - LastPass	LP_TV	Fehler > Organisatorische Schwächen	the attacker stole valid credentials from a senior DevOps engineer to gain access to shared cloud storage containing the encryption keys for customer vault backups stored in Amazon S3 buckets.
SV11 - LastPass	LP_TV	Fehler > Organisatorische Schwächen	Just four DevOps engineers had access to the decryption keys needed to access the cloud storage service.
SV11 - LastPass	LP_Ars	Fehler > Organisatorische Schwächen	Among other things, the vault gave access to a shared cloud-storage environment that contained the encryption keys for customer vault backups stored in Amazon S3 buckets.
SV11 - LastPass	LP_Ars	Fehler > Organisatorische Schwächen	The hacked DevOps engineer was one of only four LastPass employees with access to the corporate vault.
SV11 - LastPass	LP_CSA	Fehler > Organisatorische Schwächen	cloud backups – and to access a shocking amount of the most sensitive data imaginable
SV11 - LastPass	LP_CSA	Fehler > Organisatorische Schwächen	One of the most shocking aspects of these incidents is how long they took to uncover. The initial breach happened in August, and was reported by LastPass in December. The second incident ended on October 26, and was only uncovered at the end of February.
SV11 - LastPass	LP_CSA	Fehler > Organisatorische Schwächen	LastPass took months to detect the incidents, and additional months to understand the full scope of each breach and the extent to which customer data was compromised. This led the company to issue conflicting statements which only furthered the reputational damage to themselves, and potentially hindered their customers from applying the correct mitigation measures.
SV11 - LastPass	LP_CSA	Fehler > Organisatorische Schwächen	These incidents are a direct result of current gaps in cloud data security, starting with lack of visibility.
SV11 - LastPass	LP_CSA	Fehler > Organisatorische Schwächen	nd yet, most companies don't have an easy way to understand where their sensitive data is stored, how data flows between environments, and who has accessed it. This is the type of context that was missing in the LastPass incident; and consequently, the full scope of the incident went undetected for months.
SV11 - LastPass	LP_KoS	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	LastPass disclosed a breach
SV11 - LastPass	LP_CSA	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	data security scandal
SV11 - LastPass	LP_CSA	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	two data breach incidents
SV11 - LastPass	LP_LP_1	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	The threat actor targeted a senior DevOps engineer
SV11 - LastPass	LP_LP_2	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	This attack targeted LastPass infrastructure, resources, and an employee in a campaign of overlapping activity.
SV11 - LastPass	LP_LP_2	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	Specifically, the threat actor was able to leverage valid credentials stolen from a senior DevOps engineer to access a shared cloud-storage environment
SV11 - LastPass	LP_LP_2	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	the threat actor targeted one of the four DevOps engineers who had access to the decryption keys needed to access the cloud storage service

Dokumentgruppe	Dokumentname	Code	Segment
SV11 - LastPass	LP_LP_2	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	The threat actor was able to capture the employee's master password as it was entered, after the employee authenticated with MFA, and gain access to the DevOps engineer's LastPass corporate vault.
SV11 - LastPass	LP_KoS	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	In February 2023, LastPass disclosed that the intrusion involved a highly complex, targeted attack against a DevOps engineer who was one of only four LastPass employees with access to the corporate vault.
SV11 - LastPass	LP_Ars	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	In the process, the unknown threat actor was able to steal valid credentials from a senior DevOps engineer and access the contents of a LastPass data vault.
SV11 - LastPass	LP_Ars	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	"Specifically, the threat actor was able to leverage valid credentials stolen from a senior DevOps engineer to access a shared cloud-storage environment, which initially made it difficult for investigators to differentiate between threat actor activity and ongoing legitimate activity."
SV11 - LastPass	LP_CSA	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	A DevOps engineer was specifically targeted by the attacker
SV11 - LastPass	LP_LP_1	Gemeinsamkeiten > Schwachstelle	Rather, the threat actor exploited a vulnerability in third-party software, bypassed existing controls, and eventually accessed non-production development and backup storage environments.
SV11 - LastPass	LP_LP_1	Gemeinsamkeiten > Schwachstelle	A software engineer's corporate laptop was compromised, allowing the unauthorized threat actor to gain access to a cloud-based development environment and steal source code, technical information, and certain LastPass internal system secrets.
SV11 - LastPass	LP_LP_1	Gemeinsamkeiten > Schwachstelle	The threat actor targeted a senior DevOps engineer by exploiting vulnerable third-party software. The threat actor leveraged the vulnerability to deliver malware, bypass existing controls, and ultimately gain unauthorized access to cloud backups.
SV11 - LastPass	LP_LP_2	Gemeinsamkeiten > Schwachstelle	vulnerability in a third-party media software package to launch a coordinated second attack
SV11 - LastPass	LP_LP_2	Gemeinsamkeiten > Schwachstelle	exploiting a vulnerable third-party media software package, which enabled remote code execution capability and allowed the threat actor to implant keylogger malware.
SV11 - LastPass	LP_KoS	Gemeinsamkeiten > Schwachstelle	"This was accomplished by targeting the DevOps engineer's home computer and exploiting a vulnerable third-party media software package, which enabled remote code execution capability and allowed the threat actor to implant keylogger malware," LastPass officials wrote. "The threat actor was able to capture the employee's master password as it was entered, after the employee authenticated with MFA, and gain access to the DevOps engineer's LastPass corporate vault."
SV11 - LastPass	LP_KoS	Gemeinsamkeiten > Schwachstelle	Dan Goodin at Ars Technica reported and then confirmed that the attackers exploited a known vulnerability in a Plex media server that the employee was running on his home network, and succeeded in installing malicious software that stole passwords and other authentication credentials.
SV11 - LastPass	LP_TV	Gemeinsamkeiten > Schwachstelle	LastPass says that a threat actor was able to steal corporate and customer data by hacking an employee's personal computer and installing keylogger malware, which let them gain access to the company's cloud storage
SV11 - LastPass	LP_TV	Gemeinsamkeiten > Schwachstelle	exploiting an (undisclosed) vulnerable third-party media software package on their home computer and installing keylogger malware. Ars Technica reports that the computer was likely hacked through the Plex media platform, which similarly reported a data breach shortly after LastPass disclosed its first incident in August.
SV11 - LastPass	LP_Ars	Gemeinsamkeiten > Schwachstelle	"This was accomplished by targeting the DevOps engineer's home computer and exploiting a vulnerable third-party media software package, which enabled remote code execution capability and allowed the threat actor to implant keylogger malware," LastPass officials wrote. "The threat actor was able to capture the employee's master password as it was entered, after the employee authenticated with MFA, and gain access to the DevOps engineer's LastPass corporate vault."
SV11 - LastPass	LP_Ars	Gemeinsamkeiten > Schwachstelle	the media software package that was exploited on the employee's home computer was Plex
SV11 - LastPass	LP_CSA	Gemeinsamkeiten > Schwachstelle	who exploited a third-party software vulnerability on the employee's home computer
SV11 - LastPass	LP_CSA	Gemeinsamkeiten > Schwachstelle	The attacker used this vulnerability to gain access to cloud backups – and to access a shocking amount of the most sensitive data imaginable.
SV11 - LastPass	LP_LP_1	Reaktionen > Kommunikation	We have shared technical information, Indicators of Compromise (IOCs), and threat actor tactics, techniques, and procedures (TTPs) with law enforcement and our threat intelligence and forensic partners.
SV11 - LastPass	LP_KoS	Reaktionen > Kommunikation	LastPass declined to answer questions about the research highlighted in this story, citing an ongoing law enforcement investigation and pending litigation against the company in response to its 2022 data breach. "Last year's incident remains the subject of an ongoing investigation by law enforcement and is also the subject of pending litigation," LastPass said in a written statement provided to KrebsOnSecurity. "Since last year's attack on LastPass, we have remained in contact with law enforcement and continue to do so."
SV11 - LastPass	LP_KoS	Reaktionen > Kommunikation	"We have shared various technical information, Indicators of Compromise (IOCs), and threat actor tactics, techniques, and procedures (TTPs) with our law enforcement contacts as well as our internal and external threat intelligence and forensic partners in an effort to try and help identify the parties responsible.

Dokumentgruppe	Dokumentname	Code	Segment
SV11 - LastPass	LP_TV	Reaktionen > Kommunikation	Alongside the announcement, LastPass has published a complete list of the data that was compromised across both security breaches on a dedicated support page. BleepingComputer reports that LastPass has made efforts to conceal this information, however, noting that HTML tags had been added to the document to prevent the updates from being indexed by search engines. LastPass has additionally published a PDF containing further details regarding the incidents last year alongside two additional security bulletins — one for LastPass Free, Premium, and Families customers and another for business administrators — with recommended actions to secure your accounts.
SV11 - LastPass	LP_LP_1	Reaktionen > Maßnahmen > Opferseitig	Removed the development environment and rebuilt a new one to ensure full containment and eradication of the threat actor.
SV11 - LastPass	LP_LP_1	Reaktionen > Maßnahmen > Opferseitig	Deployed additional security technologies and controls to supplement existing controls.
SV11 - LastPass	LP_LP_1	Reaktionen > Maßnahmen > Opferseitig	Rotated all relevant cleartext secrets used by our teams and any exposed certificates.
SV11 - LastPass	LP_LP_1	Reaktionen > Maßnahmen > Opferseitig	Analyzed LastPass cloud-based storage resources and applied additional policies and controls.
SV11 - LastPass	LP_LP_1	Reaktionen > Maßnahmen > Opferseitig	Analyzed and changed existing privileged access controls.
SV11 - LastPass	LP_LP_1	Reaktionen > Maßnahmen > Opferseitig	Rotated relevant secrets and certificates that were accessed by the threat actor.
SV11 - LastPass	LP_LP_1	Reaktionen > Maßnahmen > Opferseitig	Since August, we have deployed several new security technologies across our infrastructure, data centers, and our cloud environments to further bolster our security posture. Much of this was already planned and was done in record time, as we had begun these efforts prior to the first incident.
SV11 - LastPass	LP_LP_1	Reaktionen > Maßnahmen > Opferseitig	We have also prioritized and initiated significant investments in security, privacy, and operational best practices. We have performed a comprehensive review of our security policies and incorporated changes to restrict access and privilege, where appropriate. We completed a comprehensive analysis of existing controls and configurations, and we've made the necessary changes to harden existing environments.
SV11 - LastPass	LP_LP_1	Reaktionen > Maßnahmen > Opferseitig	We have also begun the work to expand the use of encryption within our application and backup infrastructure.
SV11 - LastPass	LP_LP_2	Reaktionen > Maßnahmen > Opferseitig	With the assistance of Mandiant, we forensically imaged devices to investigate corporate and personal resources and gather evidence detailing potential threat actor activity.
SV11 - LastPass	LP_LP_2	Reaktionen > Maßnahmen > Opferseitig	We assisted the DevOps Engineer with hardening the security of their home network and personal resources.
SV11 - LastPass	LP_LP_2	Reaktionen > Maßnahmen > Opferseitig	We enabled Microsoft's conditional access PIN-matching multifactor authentication using an upgrade to the Microsoft Authenticator application which became generally available during the incident.
SV11 - LastPass	LP_LP_2	Reaktionen > Maßnahmen > Opferseitig	We rotated critical and high privilege credentials that were known to be available to the threat actor; we continue to rotate the remaining lower priority items that pose no risk to LastPass or our customers.
SV11 - LastPass	LP_LP_2	Reaktionen > Maßnahmen > Opferseitig	We began revoking and re-issuing certificates obtained by the threat actor.
SV11 - LastPass	LP_LP_2	Reaktionen > Maßnahmen > Opferseitig	We analyzed LastPass AWS S3 cloud-based storage resources and applied or started to apply additional S3 hardening measures: We put in place additional logging and alerting across the Cloud Storage environment with tighter IAM policies enforced. We deactivated prior development IAM users. We enabled a policy that prevents the creation and use of long-lived development IAM users in the new development environment. We rotated existing production service IAM user keys, applied tighter IP restrictions, and reconfigured policies to adhere to least privilege. We deleted obsolete service IAM users from the development and production environments. We are enabling IAM resource tagging enforcement on accounts for both users and roles with periodic reporting on non-compliant resources.
SV11 - LastPass	LP_LP_2	Reaktionen > Maßnahmen > Opferseitig	We rotated critical SAML certificates used for internal and external services.
SV11 - LastPass	LP_LP_2	Reaktionen > Maßnahmen > Opferseitig	We deleted obsolete/unused SAML certificates used for development, services, or third parties.
SV11 - LastPass	LP_LP_2	Reaktionen > Maßnahmen > Opferseitig	We revised our 24x7 threat detection and response coverage, with additional managed and automated services enabled to facilitate appropriate escalation.
SV11 - LastPass	LP_LP_2	Reaktionen > Maßnahmen > Opferseitig	We developed and enabled custom analytics that can detect ongoing abuse of AWS resources.
SV11 - LastPass	LP_TV	Reaktionen > Maßnahmen > Opferseitig	The company has since taken additional steps to secure its platform, including revoking certificates and rotating credentials known to the threat actor and implementing additional logging and alerting across its cloud storage.
SV11 - LastPass	LP_TV	Reaktionen > Vorschläge	LastPass then advised its users to change all of their stored passwords as "an extra safety measure," despite maintaining that the passwords were still secured by the account's master password.
SV11 - LastPass	LP_LP_1	Rolle der Kryptografie > Schutz	encrypted and unencrypted LastPass customer data
SV11 - LastPass	LP_LP_1	Rolle der Kryptografie > Schutz	All sensitive customer vault data, other than URLs, file paths to installed LastPass Windows or macOS software, and certain use cases involving email addresses, were encrypted using our Zero knowledge model and can only be decrypted with a unique encryption key derived from each user's master password.

Dokumentgruppe	Dokumentname	Code	Segment
SV11 - LastPass	LP_LP_1	Rolle der Kryptografie > Schutz	Backup of LastPass MFA/Federation Database – contained copies of LastPass Authenticator seeds, telephone numbers used for the MFA backup option (if enabled), as well as a split knowledge component (the K2 “key”) used for LastPass federation (if enabled). This database was encrypted
SV11 - LastPass	LP_LP_2	Rolle der Kryptografie > Schutz	To access the cloud-based storage resources – notably S3 buckets which are protected with either AWS S3-SSE encryption, AWS S3-KMS encryption, or AWS S3-SSE-C encryption – the threat actor needed to obtain AWS Access Keys and the LastPass-generated decryption keys. The encrypted cloud-based storage services house backups of LastPass customer and encrypted vault data.
SV11 - LastPass	LP_LP_2	Rolle der Kryptografie > Schutz	certain LastPass credentials stolen during the first attack were encrypted and the threat actor did not have access to the decryption keys
SV11 - LastPass	LP_LP_2	Rolle der Kryptografie > Schutz	The threat actor then exported the native corporate vault entries and content of shared folders, which contained encrypted secure notes with access and decryption keys needed to access the AWS S3 LastPass production backups, other cloud-based storage resources, and some related critical database backups.
SV11 - LastPass	LP_KoS	Rolle der Kryptografie > Schutz	hackers stole password vaults containing both encrypted
SV11 - LastPass	LP_KoS	Rolle der Kryptografie > Schutz	LastPass disclosed that criminal hackers had compromised encrypted copies of some password vaults, as well as other personal information.
SV11 - LastPass	LP_KoS	Rolle der Kryptografie > Schutz	LastPass has always emphasized that if you lose this master password, that’s too bad because they don’t store it and their encryption is so strong that even they can’t help you recover it.
SV11 - LastPass	LP_Ars	Rolle der Kryptografie > Schutz	as well as website usernames and passwords, secure notes, and form-filled data, which had an additional layer of encryption using 256-bit AES.
SV11 - LastPass	LP_CSA	Rolle der Kryptografie > Schutz	encrypted copies of LastPass customers' password vaults
SV11 - LastPass	LP_LP_1	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	unencrypted LastPass customer data
SV11 - LastPass	LP_KoS	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	plaintext data for more than 25 million users.
SV11 - LastPass	LP_KoS	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	Palant believes LastPass also failed to upgrade many older, original customers to more secure encryption protections that were offered to newer customers over the years. One important setting in LastPass is the number of “iterations,” or how many times your master password is run through the company’s encryption routines. The more iterations, the longer it takes an offline attacker to crack your master password.
SV11 - LastPass	LP_KoS	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	“With LastPass, the idea is the user’s password vault is encrypted with a cryptographic hash (H) of the user’s passphrase,” Weaver said. “The problem is a hash of the user’s passphrase is remarkably weak on older LastPass vaults with master passwords that do not have many iterations.
SV11 - LastPass	LP_TV	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	On December 22nd, LastPass revealed that the hackers had used information from the first breach in August to access its systems during the second incident in November and that the attacker was able to copy a backup of partially encrypted customer vault data containing website URLs, usernames, and passwords.
SV11 - LastPass	LP_Ars	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	Already smarting from a breach that put partially encrypted login data into a threat actor’s hands
SV11 - LastPass	LP_Ars	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	Monday’s update comes two months after LastPass issued a previous bombshell update that for the first time said that, contrary to previous assertions, the attackers had obtained customer vault data containing both encrypted and plaintext data.
SV11 - LastPass	LP_Ars	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	The backup data contained both unencrypted data, such as website URLs,
SV11 - LastPass	LP_CSA	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	Unencrypted customer data, including metadata and URLs
SV11 - LastPass	LP_LP_1	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	but the separately-stored decryption key was included in the secrets stolen by the threat actor during the second incident.
SV11 - LastPass	LP_KoS	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	some security experts to conclude that crooks likely have succeeded at cracking open some of the stolen LastPass vaults.
SV11 - LastPass	LP_KoS	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	Then on Aug. 28, Monahan said she’d concluded that the common thread among nearly every victim was that they’d previously used LastPass to store their “seed phrase,” the private key needed to unlock access to their cryptocurrency investments. Armed with your secret seed phrase, anyone can instantly access all of the cryptocurrency holdings tied to that cryptographic key, and move the funds to anywhere they like.
SV11 - LastPass	LP_KoS	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	But experts say all bets are off when cybercrooks can get their hands on the encrypted vault data itself — as opposed to having to interact with LastPass via its website. These so-called “offline” attacks allow the bad guys to conduct unlimited and unfettered “brute force” password cracking attempts against the encrypted data using powerful computers that can each try millions of password guesses per second.
SV11 - LastPass	LP_Ars	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	Once in possession of the decrypted vault, the threat actor exported the entries, including the “decryption keys needed to access the AWS S3 LastPass production backups, other cloud-based storage resources, and some related critical database backups.”

Dokumentgruppe	Dokumentname	Code	Segment
SV11 - LastPass	LP_Ars	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	LastPass said then that the threat actor had also obtained a cloud storage access key and dual storage container decryption keys, allowing for the copying of customer vault backup data from the encrypted storage container.
SV11 - LastPass	LP_CSA	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	The split knowledge component ("K2") Key which can be used to decrypt customer data
SV12 - Uber	UB_IS	Angreifer > Einzelne	an allegedly 17-year-old attacker hacked Uber's IT infrastructure and acquired sensitive data.
SV12 - Uber	UB_Wired	Angreifer > Einzelne	An entity that claims to be an individual 18-year-old hacker took responsibility for the attack, bragging to multiple security researchers about the steps they took to breach the company. The attacker reportedly posted, "Hi @here I announce I am a hacker and Uber has suffered a data breach," in a channel on Uber's Slack on Thursday night.
SV12 - Uber	UB_BC	Angreifer > Einzelne	Uber suffered a cyberattack Thursday afternoon with an allegedly 18-year-old hacker
SV12 - Uber	UB_UB	Angreifer > Unabhängige Gruppierungen	We believe that this attacker (or attackers) are affiliated with a hacking group called Lapsus$,
SV12 - Uber	UB_DR	Angreifer > Unabhängige Gruppierungen	notorious Lapsus$ hacking group
SV12 - Uber	UB_DR	Angreifer > Unabhängige Gruppierungen	We believe that this attacker (or attackers) are affiliated with a hacking group called Lapsus$,
SV12 - Uber	UB_UB	Fehler > Menschliches Versagen	The attacker then repeatedly tried to log in to the contractor's Uber account. Each time, the contractor received a two-factor login approval request, which initially blocked access. Eventually, however, the contractor accepted one, and the attacker successfully logged in.
SV12 - Uber	UB_IS	Fehler > Menschliches Versagen	the attacker successfully logged in after the contractor accepted one of the many attempted two-factor login approval requests
SV12 - Uber	UB_DR	Fehler > Organisatorische Schwächen	Researchers say the incident has highlighted the risks that can come from trusting too much in multifactor authentication (MFA), as well as unmanaged risk around cloud-service adoption.
SV12 - Uber	UB_DR	Fehler > Organisatorische Schwächen	Patrick Tiquet, vice president of security and architecture at Keeper Security, says the Uber attack highlights a fundamental misconception around MFA's strength as a method to secure access.
SV12 - Uber	UB_DR	Fehler > Organisatorische Schwächen	"Although MFA adds a critical second layer of security to your accounts, the biggest misconception about MFA is that all forms are equally secure," he says.
SV12 - Uber	UB_DR	Fehler > Organisatorische Schwächen	The move to a more distributed model has increased enterprise reliance on asynchronous communications tools such as Slack and WhatsApp in business-critical environments, he says. The rapid adoption of SaaS has created an unmanaged risk in the form of complex integrations between poorly managed services.
SV12 - Uber	UB_Wired	Fehler > Organisatorische Schwächen	The phrase "zero trust" has become a sometimes meaningless buzzword in the security industry, but the Uber breach seems to at least show an example of what zero trust is not. Once the attacker had initial access inside the company, they claim they were able to access resources shared on the network that included scripts for Microsoft's automation and management program PowerShell.
SV12 - Uber	UB_IS	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	data exfiltration
SV12 - Uber	UB_Wired	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	Uber has suffered a data breach
SV12 - Uber	UB_UB	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	An Uber EXT contractor had their account compromised by an attacker. It is likely that the attacker purchased the contractor's Uber corporate password on the dark web, after the contractor's personal device had been infected with malware, exposing those credentials.
SV12 - Uber	UB_IS	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	An Uber EXT contractor had their account compromised by an attacker,
SV12 - Uber	UB_IS	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	It is likely that the attacker purchased the contractor's Uber corporate password on the dark web after the contractor's device had been infected with malware, exposing those credentials.
SV12 - Uber	UB_DR	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	And indeed, Uber on Monday said the attacker who breached its network last week had first obtained the VPN credentials of an external contractor, likely by purchasing them on the Dark Web. The attacker then repeatedly tried to log in to the Uber account using the illegally obtained credentials, prompting a two-factor login approval request each time.
SV12 - Uber	UB_DR	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	After the contractor initially blocked those requests, the attacker contacted the target on WhatsApp posing as tech support, telling the person to accept the MFA prompt — thus allowing the attacker to log in.
SV12 - Uber	UB_Wired	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	they first gained access to company systems by targeting an individual employee and repeatedly sending them multifactor authentication login notifications
SV12 - Uber	UB_Wired	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	After more than an hour, the attacker claims, they contacted the same target on WhatsApp pretending to be an Uber IT person and saying that the MFA notifications would stop once the target approved the login.
SV12 - Uber	UB_BC	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	they breached Uber after performing a social engineering attack on an employee and stealing their password.
SV12 - Uber	UB_BC	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	the hacker said they were able to gain access to Uber's Intranet after conducting a social engineering attack on an employee.
SV12 - Uber	UB_BC	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	As the Uber account was protected with multi-factor authentication, the attacker allegedly used an MFA Fatigue attack and pretended to be Uber IT support to convince the employee to accept the MFA request.

Dokumentgruppe	Dokumentname	Code	Segment
SV12 - Uber	UB_BC	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	
SV12 - Uber	UB_Wired	Gemeinsamkeiten > Schwachstelle	Such attacks, sometimes known as “MFA fatigue” or “exhaustion” attacks, take advantage of authentication systems in which account owners simply have to approve a login through a push notification on their device rather than through other means, such as providing a randomly generated code.
SV12 - Uber	UB_UB	Reaktionen > Maßnahmen > Opferseitig	We identified any employee accounts that were compromised or potentially compromised and either blocked their access to Uber systems or required a password reset.
SV12 - Uber	UB_UB	Reaktionen > Maßnahmen > Opferseitig	We disabled many affected or potentially affected internal tools.
SV12 - Uber	UB_UB	Reaktionen > Maßnahmen > Opferseitig	We rotated keys (effectively resetting access) to many of our internal services.
SV12 - Uber	UB_UB	Reaktionen > Maßnahmen > Opferseitig	We locked down our codebase, preventing any new code changes.
SV12 - Uber	UB_UB	Reaktionen > Maßnahmen > Opferseitig	When restoring access to internal tools, we required employees to re-authenticate. We are also further strengthening our multi-factor authentication (MFA) policies.
SV12 - Uber	UB_UB	Reaktionen > Maßnahmen > Opferseitig	We added additional monitoring of our internal environment to keep an even closer eye on any further suspicious activity.
SV12 - Uber	UB_UB	Reaktionen > Maßnahmen > Opferseitig	We’re working with several leading digital forensics firms as part of the investigation. We will also take this opportunity to continue to strengthen our policies, practices, and technology to further protect Uber against future attacks.
SV12 - Uber	UB_UB	Reaktionen > Maßnahmen > Opferseitig	As we shared yesterday, we have notified law enforcement. Internal software tools that we took down as a precaution yesterday are coming back online this morning.
SV12 - Uber	UB_IS	Reaktionen > Maßnahmen > Opferseitig	Uber responded by identifying and blocking compromised accounts to ensure the attacker had no further access to systems. In some cases, the company required a password reset to restore accounts. Uber also disabled affected tools, rotated keys to reset access to internal servers, locked down the codebase, and required employees to re-authenticate to regain access.
SV12 - Uber	UB_Wired	Reaktionen > Maßnahmen > Opferseitig	The company temporarily took down access on Thursday evening to Slack and some other internal services, according to The New York Times, which first reported the breach. In a midday update on Friday, the company said that “internal software tools that we took down as a precaution yesterday are coming back online.”
SV12 - Uber	UB_BC	Reaktionen > Maßnahmen > Opferseitig	As we shared yesterday, we have notified law enforcement. Internal software tools that we took down as a precaution yesterday are coming back online this morning.
SV12 - Uber	UB_DR	Reaktionen > Vorschläge	He notes that best practices include using phishing- and MiTM-resistant forms of MFA rather than time-based one-time passwords (TOTP), not centralizing access keys, and rotating keys regularly. On the latter point, organizations also often do not limit access keys to the minimum privileges required for the key's intended purpose.
SV12 - Uber	UB_UB	Rolle der Kryptografie > Schutz	We also encrypt credit card information and personal health data, offering a further layer of protection.
SV12 - Uber	UB_IS	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	the cyber actor located a PowerShell script containing hard-corded privileged credentials for Thycotic, the target’s Privileged Access Management (PAM) solution. The PAM user credentials granted access to Uber’s secret services, such as DA, DUO, AWS, GSuite, and Onelogin.
SV12 - Uber	UB_Wired	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	The attacker said that one of the scripts contained hard-coded credentials for an administrator account of the access management system Thycotic. With control of this account, the attacker claimed, they were able to gain access tokens for Uber's cloud infrastructure, including Amazon Web Services, Google's GSuite, VMware's vSphere dashboard, the authentication manager Duo, and the critical identity and access management service OneLogin.
SV12 - Uber	UB_BC	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	the hacker says they found a PowerShell script containing admin credentials for the company's Thycotic privileged access management (PAM) platform, which was used to access the login secrets for the company's other internal services.
SV12 - Uber	UB_BC	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	"ok so basically uber had a network share \\[redacted]pts. the share contained some powershell scripts. one of the powershell scripts contained the username and password for a admin user in Thycotic (PAM) Using this i was able to extract secrets for all services, DA, DUO, Onelogin, AWS, Gsuite"
SV13 - MGM	MGM_Vox	Angreifer > Unabhängige Gruppierungen	A group known as Scattered Spider is believed to be responsible for the MGM breach
SV13 - MGM	MGM_Forbes	Angreifer > Unabhängige Gruppierungen	The ALPHV/BlackCat ransomware group
SV13 - MGM	MGM_Forbes	Angreifer > Unabhängige Gruppierungen	On Tuesday night, VX-Underground, a malware research group with nearly 229,000 followers on X, posted that ransomware-as-a-service group ALPHV, also known as BlackCat, claimed responsibility for executing the attack
SV13 - MGM	MGM_Forbes	Angreifer > Unabhängige Gruppierungen	ALPHV is an extremely well-known black-hat actor in the cybersecurity industry
SV13 - MGM	MGM_Forbes	Angreifer > Unabhängige Gruppierungen	While ALPHV’s responsibility for the attack has not been verified, cybersecurity experts say VX-Underground is a reliable source.

Dokumentgruppe	Dokumentname	Code	Segment
SV13 - MGM	MGM_WSJ	Angreifer > Unabhängige Gruppierungen	The gang behind the MGM hack call themselves Star Fraud, and investigators say they sprung out of a sprawling online community called the Com. Virtually unheard of five years ago, the Com has become one of the top cybersecurity problems facing the U.S.
SV13 - MGM	MGM_Heise_2	Angreifer > Unabhängige Gruppierungen	Die Drahtzieher der ALPHV-Gruppe sind offensichtlich mit der Berichterstattung über den Hack der US-Casino-Kette MGM und den fehlenden Reaktionen der Opfer unglücklich. Deswegen haben sie nun auf ihrer Website im Darknet eine Klarstellung veröffentlicht.
SV13 - MGM	MGM_WSJ	Fehler > Menschliches Versagen	What tech support didn't realize was that the caller was a hacker.
SV13 - MGM	MGM_Vox	Fehler > Organisatorische Schwächen	It doesn't help that companies often overlook vishing in their employee cybersecurity training, and they aren't asking people like Carruthers to test for vishing vulnerabilities, as they do for phishing.
SV13 - MGM	MGM_Heise_3	Fehler > Versäumnisse von Dritten	Die Zugangscodes erbeuteten die Cyberkriminellen beim Identitätsdienst Okta.
SV13 - MGM	MGM_Heise_2	Fehler > Versäumnisse von Dritten	haben sie sich auf den Okta-Servern zur zentralisierten Zugriffsverwaltung umgeschaut.
SV13 - MGM	MGM_Vox	Gemeinsamkeiten > Art des Vorfalls > Ransomware	it reportedly used ransomware made by ALPHV, or BlackCat, a ransomware-as-a-service operation
SV13 - MGM	MGM_Forbes	Gemeinsamkeiten > Art des Vorfalls > Ransomware	One clue that this was a ransomware attack was the high visibility of the disruption.
SV13 - MGM	MGM_Heise_1	Gemeinsamkeiten > Art des Vorfalls > Ransomware	Der Verdacht, dass es sich um einen Angriff mit Ransomware handelt, liegt nahe
SV13 - MGM	MGM_Vox	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	And it may have all started with a phone call, if reports citing the hackers themselves are to be believed.
SV13 - MGM	MGM_Vox	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	In this case, it appears that publicly available information and a persuasive phone manner were enough to give the hackers all they needed to get into MGM's systems and create what is likely to be some very expensive havoc that will hurt both the resort chain and many of its guests.
SV13 - MGM	MGM_Vox	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	Scattered Spider specializes in social engineering,
SV13 - MGM	MGM_Vox	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	The hackers are said to be especially good at "vishing," or gaining access to systems through a convincing phone call rather than phishing, which is done through an email.
SV13 - MGM	MGM_Vox	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	In this case, it appears that the hackers found an employee's information on LinkedIn and impersonated them in a call to MGM's IT help desk to obtain credentials to access and infect the systems.
SV13 - MGM	MGM_Vox	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	A subsequent Bloomberg report, citing an executive at cybersecurity company Okta, blamed a successful social engineering attack on the help desk as well
SV13 - MGM	MGM_Vox	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	A portmanteau of "voice" and "phishing," vishing, like all social engineering techniques, targets what's usually the weakest link in the cybersecurity chain: us. More than 90 percent of cyberattacks start with phishing, and it's one of the most common ways that organizations are penetrated as well. And vishing is a particularly effective avenue of attack: A 2022 IBM report found that targeted phishing attacks that included phone calls were three times more effective than those that didn't.
SV13 - MGM	MGM_Vox	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	"From the attacker point of view, vishing is easy," she told Vox. "With phishing, I have to set up infrastructure, I have to craft an email and do all these extra technical things. But with vishing ... it's picking up the phone and calling someone and asking for a password reset. It's pretty simple." One of the keys to a successful vishing attack is knowing enough about a system, company, or employee to pull off the impersonation. You can learn a lot about people and organizations just from what's publicly available — including who companies' high-value targets are. "It makes the job of an attacker so much easier," Carruthers said. "Things like LinkedIn and different types of people search engines, that is the first step into making a successful vish." From there, the attacker can use other social engineering techniques like adding a sense of authority or urgency to a request. Organizations with inadequate verification processes to prove that the caller is who they claim to be are especially vulnerable. "It's something we see happen all the time," Carruthers added.
SV13 - MGM	MGM_Forbes	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	executing the attack by using social engineering to identify on LinkedIn an MGM employee who worked in IT support
SV13 - MGM	MGM_WSJ	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	Step one was a phone call to MGM Resorts' tech support. The person on the line said they were an employee, but had forgotten their password and were locked out of their account.
SV13 - MGM	MGM_Vox	Gemeinsamkeiten > Branche > Direkt Betroffene	casino chain MGM Resorts
SV13 - MGM	MGM_Vox	Gemeinsamkeiten > Branche > Direkt Betroffene	MGM, which owns more than two dozen hotel and casino locations around the world as well as an online sports betting arm
SV13 - MGM	MGM_WSJ	Gemeinsamkeiten > Schwachstelle	Star Fraud had targeted a widely overlooked and hard-to-fix weakness in technology—the tech support systems that help people get into their online accounts when they're locked out.
SV13 - MGM	MGM_WSJ	Gemeinsamkeiten > Schwachstelle	The anonymous associate of the gang later told The Wall Street Journal the group had obtained information on the MGM employee they impersonated by mining the vast troves of stolen and illegally available data on the internet.

Dokumentgruppe	Dokumentname	Code	Segment
SV13 - MGM	MGM_Vox	Reaktionen > Kommunikation	The group posted a message on September 14 claiming responsibility for the attack but denying that it was perpetrated by teenagers in the US and Europe or that anyone tried to tamper with slot machines. It also criticized what it said was inaccurate reporting on the hack and said it hadn't officially spoken to anyone about the hack, and "most likely" wouldn't in the future. The message said that data was stolen from MGM, which has thus far refused to engage with the hackers or pay any kind of ransom.
SV13 - MGM	MGM_WSJ	Reaktionen > Kommunikation	MGM declined to release communications from the hackers.
SV13 - MGM	MGM_Heise_1	Reaktionen > Kommunikation	"MGM Resorts hat kürzlich einen Cybersicherheits-Vorfall entdeckt, der einige der Systeme des Unternehmens betrifft", teilte das Unternehmen am Montag auf X (ehemals Twitter) mit.
SV13 - MGM	MGM_Heise_3	Reaktionen > Kommunikation	Nach dem Cyberangriff auf die US-Casino-Kette MGM Resorts informiert das Unternehmen jetzt seine Kunden über den Vorfall. Der IT-Sicherheitsforscher Troy Hunt hat in einem Post auf X einen Screenshot eines solchen Anschreibens veröffentlicht.
SV13 - MGM	MGM_Vox	Reaktionen > Maßnahmen > Opferseitig	a "cybersecurity issue" was affecting some of its systems, which it shut down to "protect our systems and data."
SV13 - MGM	MGM_Vox	Reaktionen > Maßnahmen > Opferseitig	MGM says it is informing customers whose data was stolen and offering them free identity protection and credit monitoring
SV13 - MGM	MGM_Forbes	Reaktionen > Maßnahmen > Opferseitig	Once the MGM breach was discovered, Hamerstone says it was appropriate for the company shut down their systems.
SV13 - MGM	MGM_WSJ	Reaktionen > Maßnahmen > Opferseitig	Hornbuckle gave the order. It was time to start shutting down some of the company's systems. The shutdowns, including its email, would lock out the hackers, the company figured, and the tech team could clean up anything the gang had left behind. It would make communications between employees and online bookings more difficult, but it wouldn't cause a catastrophe.
SV13 - MGM	MGM_WSJ	Reaktionen > Maßnahmen > Opferseitig	Instead of simply cleaning up infected parts of the computer systems, now they'd have to rebuild the thousands of servers the company used from scratch, installing clean versions of the operating system and other software. The cost would far exceed the ransom request. MGM decided to do it anyway.
SV13 - MGM	MGM_Heise_1	Reaktionen > Maßnahmen > Opferseitig	Die US-Casino-Kette MGM Resorts hat nach einem Cyberangriff ihre IT-Systeme teilweise heruntergefahren, was offenbar zu weitreichenden Ausfällen in allen Hotels und Casinos der Kette in den USA geführt hat.
SV13 - MGM	MGM_Heise_1	Reaktionen > Maßnahmen > Opferseitig	Die Ermittlungsbehörden sowie externe Sicherheitsexperten seien hinzugezogen worden. Zum Schutz der Daten seien "einige Systeme" heruntergefahren worden. "Wir arbeiten gewissenhaft daran, Ursache und Ausmaß des Vorfalls festzustellen."
SV13 - MGM	MGM_Heise_3	Reaktionen > Maßnahmen > Opferseitig	Das Unternehmen habe zusätzliche Sicherheitsmaßnahmen eingeleitet, um die Systeme "noch besser" zu schützen. Zudem stellt MGM den Betroffenen zwei Jahre lang kostenlos ein Überwachungs-Tool zu Verfügung, um Kreditkarten-Daten und die Identitäten zu schützen.
SV13 - MGM	MGM_Heise_2	Reaktionen > Maßnahmen > Opferseitig	In diesem Moment haben die Verantwortlichen bei MGM ihre kompletten Okta-Systeme in einer "übereilten Entscheidung" heruntergefahren.
SV13 - MGM	MGM_Heise_3	Reaktionen > Vorschläge	Ebenso empfiehlt MGM seinen Kunden, wachsam gegenüber Phishing-Versuchen zu sein. Die Untersuchung des Vorfalls sei noch nicht abgeschlossen, geht aus der Mitteilung hervor.
SV13 - MGM	MGM_Heise_2	Rolle der Kryptografie > Schutz	Nachdem sie die vom Domain-Controller erbeuteten Passwörter in Form von Hash-Dumps nicht knacken konnten
SV13 - MGM	MGM_Vox	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Someone claiming to be a representative of Scattered Spider told the Financial Times that it stole and encrypted MGM's data
SV13 - MGM	MGM_WSJ	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	The hackers emailed Hornbuckle a standard ransomware note saying they'd installed devastating software that would freeze systems across MGM's network. They wanted more than $30 million for the cryptographic keys that would allow MGM to get things up and running again.
SV13 - MGM	MGM_WSJ	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Star Fraud planned to use Alphv's ransomware to encrypt thousands of MGM's computer systems, rendering them unusable until Hornbuckle and his team paid up.
SV13 - MGM	MGM_Heise_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Erst, nachdem sie bereits einen Tag im MGM-System waren, haben sie eigenen Angaben zufolge über 100 ESXi-Hypervisors mit Ransomware verschlüsselt.
SV14 - MS Exchange	MS23_THN_1	Angreifer > Staatlich motiviert	Chinese nation-state actor
SV14 - MS Exchange	MS23_THN_1	Angreifer > Staatlich motiviert	Storm-0558, describing it as a nation-state activity group based out of China
SV14 - MS Exchange	MS23_THN_2	Angreifer > Staatlich motiviert	Storm-0558 is suspected to be a China-based threat actor conducting malicious cyber activities that are consistent with espionage
SV14 - MS Exchange	MS23_BC	Angreifer > Staatlich motiviert	Storm-0558 is a cyberespionage actor affiliated with China
SV14 - MS Exchange	MS23_THN_3	Angreifer > Staatlich motiviert	China-based threat group Storm-0558
SV14 - MS Exchange	MS23_BC	Fehler > Menschliches Versagen	Microsoft believes that last May's Exchange Online hack is linked to a threat actor known as 'Storm-0558' stealing an Azure signing key from an engineer's laptop that was previously compromised by the hackers at an acquired company.

Dokumentgruppe	Dokumentname	Code	Segment
SV14 - MS Exchange	MS23_BC	Fehler > Menschliches Versagen	The theory that Microsoft shared with the CSRB is that the 2023 Exchange Online hack is connected to another incident in 2021 where the same threat actor compromised its corporate network through an engineer’s account that had been hacked more than a year earlier, and provided access to sensitive authentication and identity data.
SV14 - MS Exchange	MS23_THN_3	Fehler > Menschliches Versagen	Microsoft on Wednesday revealed that a China-based threat actor known as Storm-0558 acquired the inactive consumer signing key to forge tokens and access Outlook by compromising an engineer's corporate account.
SV14 - MS Exchange	MS23_BC	Fehler > Organisatorische Schwächen	The hackers accessed the email accounts using forged authentication tokens signed with a Microsoft Services Account (MSA) consumer key the company created in 2016 and which should have been revoked in March 2021.
SV14 - MS Exchange	MS23_BC	Fehler > Organisatorische Schwächen	The reason for the key being still valid in 2021 is that rotating the keys was done manually for the consumer system at the time, unlike the automated process for enterprise.
SV14 - MS Exchange	MS23_BC	Fehler > Organisatorische Schwächen	After a major cloud outage because of the manual rotation, Microsoft stopped the process completely in 2021, leaving no system in place to alert employees of old, active signing keys in the consumer MSA service that should be retired.
SV14 - MS Exchange	MS23_BC	Fehler > Organisatorische Schwächen	When the engineer’s device was compromised, they were working for Affirmed Networks, which Microsoft acquired in 2020 to consolidate its cloud platform with “fully virtualized, cloud-native mobile network solutions” for operators that wanted to deploy and maintain 5G networks more easily and with lower costs. After acquiring Affirmed Networks and without running a cybersecurity audit, Microsoft provided corporate credentials to the engineer whose device Storm-0558 had already compromised.
SV14 - MS Exchange	MS23_THN_3	Fehler > Organisatorische Schwächen	"The crash dumps, which redact sensitive information, should not include the signing key. In this case, a race condition allowed the key to be present in the crash dump. The key material's presence in the crash dump was not detected by our systems."
SV14 - MS Exchange	MS23_THN_3	Fehler > Organisatorische Schwächen	The Windows maker said the crash dump was moved to a debugging environment on the internet-connected corporate network, from where Storm-0558 is suspected to have acquired the key after infiltrating the engineer's corporate account.
SV14 - MS Exchange	MS23_THN_3	Fehler > Organisatorische Schwächen	It's not currently not known if this is the exact mechanism that was adopted by the threat actor since Microsoft noted it does not have logs that offer concrete proof of the exfiltration due to its log retention policies.
SV14 - MS Exchange	MS23_THN_1	Gemeinsamkeiten > Branche > Betroffene Dritte	targeting two dozen organizations, some of which include government agencies
SV14 - MS Exchange	MS23_THN_2	Gemeinsamkeiten > Branche > Betroffene Dritte	The attacks singled out approximately 25 organizations, including government entities and associated consumer accounts
SV14 - MS Exchange	MS23_BC	Gemeinsamkeiten > Branche > Betroffene Dritte	During the 2023 intrusion, the threat actor accessed emails from senior U.S. government representatives who were involved in national security matters: Commerce Secretary, Gina Raimondo U.S. Ambassador to the People’s Republic of China, R. Nicholas Burns Congressman Don Bacon Assistant Secretary of State for East Asian and Pacific Affairs, Daniel Kritenbrink
SV14 - MS Exchange	MS23_BC	Gemeinsamkeiten > Branche > Betroffene Dritte	For at least six weeks, the hackers stole around 60,000 unclassified emails just from the U.S. Department of State.
SV14 - MS Exchange	MS23_THN_1	Gemeinsamkeiten > Schwachstelle	"The actor exploited a token validation issue to impersonate Azure AD users and gain access to enterprise mail."
SV14 - MS Exchange	MS23_THN_2	Gemeinsamkeiten > Schwachstelle	Microsoft on Friday said a validation error in its source code allowed for Azure Active Directory (Azure AD) tokens to be forged by a malicious actor known as Storm-0558 using a Microsoft account (MSA) consumer signing key to breach two dozen organizations.
SV14 - MS Exchange	MS23_THN_2	Gemeinsamkeiten > Schwachstelle	"Though the key was intended only for MSA accounts, a validation issue allowed this key to be trusted for signing Azure AD tokens.
SV14 - MS Exchange	MS23_THN_2	Gemeinsamkeiten > Schwachstelle	It's not immediately clear if the token validation issue was exploited as a "zero-day vulnerability" or if Microsoft was already aware of the problem before it came under in-the-wild abuse.
SV14 - MS Exchange	MS23_BC	Gemeinsamkeiten > Schwachstelle	Although the 2016 MSA key was designed to sign access tokens only for consumer accounts, a previously unknown vulnerability allowed Storm-0558 to use it with enterprise emails, too.
SV14 - MS Exchange	MS23_BC	Gemeinsamkeiten > Schwachstelle	However, the software development kits (SDKs) were not properly updated to distinguish on the endpoint between MSA signing keys for consumers and enterprises. This allowed authentication for the email application through the Microsoft Entra identity and access management (IAM) system using either key type.
SV14 - MS Exchange	MS23_THN_3	Gemeinsamkeiten > Schwachstelle	This enabled the adversary to access a debugging environment that contained information pertaining to a crash of the consumer signing system and steal the key. The system crash took place in April 2021.

Dokumentgruppe	Dokumentname	Code	Segment
SV14 - MS Exchange	MS23_THN_3	Gemeinsamkeiten > Schwachstelle	"A consumer signing system crash in April of 2021 resulted in a snapshot of the crashed process ('crash dump')," the Microsoft Security Response Center (MSRC) said in a post-mortem report. "The crash dumps, which redact sensitive information, should not include the signing key. In this case, a race condition allowed the key to be present in the crash dump. The key material's presence in the crash dump was not detected by our systems."
SV14 - MS Exchange	MS23_THN_3	Gemeinsamkeiten > Schwachstelle	The zero-day issue was blamed on a validation error that allowed the key to be trusted for signing Azure AD tokens.
SV14 - MS Exchange	MS23_THN_1	Reaktionen > Kommunikation	Microsoft said it notified all targeted or compromised organizations directly via their tenant admins. It did not name the organizations and agencies affected and the number of accounts that may have been hacked.
SV14 - MS Exchange	MS23_THN_2	Reaktionen > Kommunikation	The disclosure comes as Microsoft has faced criticism for its handling of the hack and for gating forensic capabilities behind additional licensing barriers, thereby preventing customers from accessing detailed audit logs that could have otherwise helped analyze the incident.
SV14 - MS Exchange	MS23_BC	Reaktionen > Maßnahmen > Dritte	The U.S. Department of Homeland Security's Cyber Safety Review Board (CSRB) has released a scathing report on how Microsoft handled its 2023 Exchange Online attack, warning that the company needs to do better at securing data and be more truthful about how threat actors stole an Azure signing key.
SV14 - MS Exchange	MS23_THN_1	Reaktionen > Maßnahmen > Opferseitig	Microsoft has since blocked the usage of tokens signed with the acquired MSA key in OWA to mitigate the attack.
SV14 - MS Exchange	MS23_THN_2	Reaktionen > Maßnahmen > Opferseitig	"Though the key was intended only for MSA accounts, a validation issue allowed this key to be trusted for signing Azure AD tokens. This issue has been corrected."
SV14 - MS Exchange	MS23_THN_2	Reaktionen > Maßnahmen > Opferseitig	Microsoft said since the discovery of the campaign on June 16, 2023, it has "identified the root cause, established durable tracking of the campaign, disrupted malicious activities, hardened the environment, notified every impacted customer, and coordinated with multiple government entities." It also noted it mitigated the issue "on customers' behalf" effective June 26, 2023.
SV14 - MS Exchange	MS23_BC	Reaktionen > Maßnahmen > Opferseitig	Creating the “Big Yellow Taxi” rule was possible because the U.S. State Department purchased a Microsoft 365 Government G5 license that comes with enhanced logging through the premium tier of Microsoft’s Purview Audit service. However, other breached organizations were unable to detect that their accounts were breached as they had not purchased the premium logging features. This led to Microsoft working with CISA to offer critical logging features for free, so all customers could detect similar attacks.
SV14 - MS Exchange	MS23_THN_3	Reaktionen > Maßnahmen > Opferseitig	It has also expanded access to security logging following criticism that the feature was limited to customers with Purview Audit (Premium) licenses, thereby restricting forensics data to others.
SV14 - MS Exchange	MS23_THN_1	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	"MSA (consumer) keys and Azure AD (enterprise) keys are issued and managed from separate systems and should only be valid for their respective systems."
SV14 - MS Exchange	MS23_THN_2	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	Microsoft admits a validation issue in its code that enabled China-based hackers to forge authentication tokens, granting unauthorized access.
SV14 - MS Exchange	MS23_THN_1	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	There is no evidence that the threat actor used Azure AD keys or any other MSA keys to carry out the attacks.
SV14 - MS Exchange	MS23_THN_1	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	The access to customer email accounts, per Redmond, was facilitated through Outlook Web Access in Exchange Online (OWA) and Outlook.com by forging authentication tokens.
SV14 - MS Exchange	MS23_THN_1	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	The actor used an acquired MSA key to forge tokens to access OWA and Outlook.com
SV14 - MS Exchange	MS23_THN_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	enabled China-based hackers to forge authentication tokens, granting unauthorized access.
SV14 - MS Exchange	MS23_THN_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	"Storm-0558 acquired an inactive MSA consumer signing key and used it to forge authentication tokens for Azure AD enterprise and MSA consumer to access OWA and Outlook.com
SV14 - MS Exchange	MS23_BC	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	The hackers accessed the email accounts using forged authentication tokens signed with a Microsoft Services Account (MSA) consumer key the company created in 2016 and which should have been revoked in March 2021.
SV14 - MS Exchange	MS23_THN_3	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Storm-0558 acquired the inactive consumer signing key to forge tokens and access Outlook
SV15 - Okta	OKT_OKT_1	Angreifer > Unbekannt	a threat actor gained unauthorized access to files inside Okta’s customer support system
SV15 - Okta	OKT_BC_2	Angreifer > Unbekannt	a threat actor gained unauthorized access to files inside Okta's customer support system
SV15 - Okta	OKT_OKT_1	Fehler > Menschliches Versagen	During our investigation into suspicious use of this account, Okta Security identified that an employee had signed-in to their personal Google profile on the Chrome browser of their Okta-managed laptop. The username and password of the service account had been saved into the employee’s personal Google account. The most likely avenue for exposure of this credential is the compromise of the employee’s personal Google account or personal device.

Dokumentgruppe	Dokumentname	Code	Segment
SV15 - Okta	OKT_BC_2	Fehler > Menschliches Versagen	the threat actors used credentials for a support service account stolen from an employee's personal Google account after they logged into their personal Google profile while using an Okta-managed laptop.
SV15 - Okta	OKT_BC_2	Fehler > Menschliches Versagen	"the most likely avenue for exposure of this credential is the compromise of the employee's personal Google account or personal device."
SV15 - Okta	OKT_BC_1	Fehler > Organisatorische Schwächen	BeyondTrust says the attack was thwarted by "custom policy controls," but due to "limitations in Okta's security model," the malicious actor was able to perform "a few confined actions."
SV15 - Okta	OKT_BT	Fehler > Organisatorische Schwächen	Custom policy controls blocked the attacker's initial activity, but limitations in Okta's security model allowed them to perform a few confined actions.
SV15 - Okta	OKT_BT	Fehler > Organisatorische Schwächen	Okta admin privileges were granted to a user: Attackers often attempt to escalate privilege, or grant privilege to backdoor accounts. This information-level detection highlights all Okta admin assignments. These assignments are typically rare and usually occur within an established process.
SV15 - Okta	OKT_BC_2	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	To breach Okta's support system, the threat actors used credentials for a support service account stolen from an employee's personal Google account
SV15 - Okta	OKT_BC_2	Gemeinsamkeiten > Art des Vorfalls > Social Engineering	Over the last two years, Okta has experienced several other breaches due to credential theft and social engineering attacks.
SV15 - Okta	OKT_OKT_1	Gemeinsamkeiten > Schwachstelle	The unauthorized access to Okta's customer support system leveraged a service account stored in the system itself. This service account was granted permissions to view and update customer support cases.
SV15 - Okta	OKT_BC_2	Gemeinsamkeiten > Schwachstelle	To breach Okta's support system, the threat actors used credentials for a support service account stolen from an employee's personal Google account
SV15 - Okta	OKT_BT	Gemeinsamkeiten > Schwachstelle	Okta session hijacking: Attackers steal Okta session cookies and use them to access Okta from infrastructure they control, allowing them to bypass most MFA and security controls related to authentication. This detection looks for suspicious sessions appearing without an authentication event that are consistent with session hijacking.
SV15 - Okta	OKT_OKT_1	Reaktionen > Kommunikation	2023-10-19 Okta alerts all Okta customers with registered security contacts, confirming if they were or were not impacted by the security incident. 2023-10-20 Okta publishes public advisory at https://sec.okta.com/articles/2023/10/tracking-unauthorized-access-oktas-support-system 2023-10-20 to 2023-11-02 Okta is focused on helping all customers, answering their questions and rolling out remediation steps. 2023-11-02 Okta notifies all Okta customers with registered security contacts of the root cause and remediation steps. 2023-11-03 Okta publishes root cause and remediation steps at https://sec.okta.com/harfiles.
SV15 - Okta	OKT_BC_2	Reaktionen > Kommunikation	Despite being alerted about session hijacking attempts on September 29, Okta took over two weeks to officially confirm the breach in their support system after multiple meetings with the three affected customers.
SV15 - Okta	OKT_BC_2	Reaktionen > Kommunikation	"We have notified all customers of our findings and have completed remediations to protect all our customers.
SV15 - Okta	OKT_BC_1	Reaktionen > Kommunikation	While BeyondTrust contacted Okta and provided them with forensics data showing that their support organization was compromised, it took Okta over two weeks to confirm the breach.
SV15 - Okta	OKT_BC_1	Reaktionen > Kommunikation	"We raised our concerns of a breach to Okta on October 2nd. Having received no acknowledgement from Okta of a possible breach, we persisted with escalations within Okta until October 19th when Okta security leadership notified us that they had indeed experienced a breach and we were one of their affected customer," BeyondTrust said.
SV15 - Okta	OKT_BT	Reaktionen > Kommunikation	The initial incident response indicated a possible compromise at Okta of either someone on their support team or someone in position to access customer support-related data. We raised our concerns of a breach to Okta on October 2nd. Having received no acknowledgement from Okta of a possible breach, we persisted with escalations within Okta until October 19th when Okta security leadership notified us that they had indeed experienced a breach and we were one of their affected customers.
SV15 - Okta	OKT_BT	Reaktionen > Kommunikation	Okta have now issued this statement confirming the breach that we detected nearly three weeks ago.
SV15 - Okta	OKT_BT	Reaktionen > Kommunikation	Requested Okta support to escalate to their information security team given our concern that Okta was likely compromised, and other Okta customers might be exposed. No known compromise or ongoing security incident was communicated by Okta.
SV15 - Okta	OKT_BT	Reaktionen > Kommunikation	Okta committed to providing the requested logs and working with us. No known compromise or ongoing security incident was communicated by Okta.
SV15 - Okta	OKT_BT	Reaktionen > Kommunikation	Okta support logs were received but contained several discrepancies. We requested more detailed logs relating to the discrepancies and reiterated our concerns that there was a high likelihood of compromise within Okta support and that we were likely not the only customer impacted. No known compromise or ongoing security incident was communicated by Okta.
SV15 - Okta	OKT_BC_1	Reaktionen > Maßnahmen > Dritte	BeyondTrust's security team detected and blocked an attempt to log into an in-house Okta administrator account on October 2 using a cookie stolen from Okta's support system.

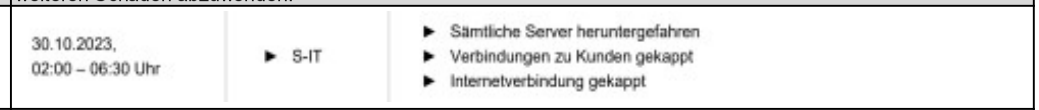
Dokumentgruppe	Dokumentname	Code	Segment
SV15 - Okta	OKT_BT	Reaktionen > Maßnahmen > Dritte	On October 2nd, 2023, the BeyondTrust security teams detected an identity-centric attack on an in-house Okta administrator account. We immediately detected and remediated the attack through our own Identity Security tools, resulting in no impact or exposure to BeyondTrust's infrastructure or to our customers.
SV15 - Okta	OKT_BT	Reaktionen > Maßnahmen > Dritte	We immediately disabled the backdoor user account and revoked the attacker's access before the account could be used and preventing any further actions.
SV15 - Okta	OKT_OKT_3	Reaktionen > Maßnahmen > Opferseitig	As part of our response, we engaged with law enforcement, notified regulators, published indicators of compromise (IOCs), and provided a customized impact report to affected customers.
SV15 - Okta	OKT_OKT_3	Reaktionen > Maßnahmen > Opferseitig	Additionally, Okta has taken a number of steps to review and enhance the security of the Okta Help Center. We are also changing how and when access is provisioned to customer administrators as well as that system's data retention policy.
SV15 - Okta	OKT_OKT_3	Reaktionen > Maßnahmen > Opferseitig	Zero Standing Privileges for Okta Admins: Ensure admin roles are requested, approved, and assigned to authorized users only for the duration that access is needed.
SV15 - Okta	OKT_OKT_3	Reaktionen > Maßnahmen > Opferseitig	MFA Required for Protected Actions in Admin Console: Provide an additional layer of protection for critical actions in Okta by requiring step-up authentication for admins to perform high-impact actions.
SV15 - Okta	OKT_OKT_3	Reaktionen > Maßnahmen > Opferseitig	In Dynamic Zones, Ability to Detect and Block Requests from Anonymizers to Okta Endpoints: Protect critical assets (e.g, Admin Console, App Dashboard, others) and allow request blocking from specified VPNs, anonymous proxies, and similar.
SV15 - Okta	OKT_OKT_3	Reaktionen > Maßnahmen > Opferseitig	Customers can now also apply IP binding to Okta products and Admin Console: Invalidate Okta sessions if the source IP changes during the session, which helps prevent session takeover. This is in addition to the initial remediation action for binding admin sessions.
SV15 - Okta	OKT_OKT_3	Reaktionen > Maßnahmen > Opferseitig	Enforce an Allowlisted Network Zone for APIs: Restrict attackers and malware from stealing SSWS tokens, and from replaying them outside of the specified IP range in order to gain unauthorized access.
SV15 - Okta	OKT_OKT_2	Reaktionen > Maßnahmen > Opferseitig	Admin Session Binding: As communicated in the Security Incident RCA, customers can now enable an Early Access feature in Okta that requires admins to reauthenticate if their session is reused from an IP address with a different ASN (Autonomous System Number). Okta strongly recommends customers enable this feature to further secure admin sessions.
SV15 - Okta	OKT_OKT_2	Reaktionen > Maßnahmen > Opferseitig	Admin Session Timeout: To align with NIST AAL3 guidelines and increase the security posture of every customer, Okta is introducing Admin Console timeouts that will be set to a default of 12-hour session duration and a 15-minute idle time. Customers will have the option to edit these settings. This will be available as an Early Access feature starting November 29th for preview orgs and December 4th for production orgs. The feature will be available for all production orgs by January 8th, 2024. An email was sent to all Super Admins regarding this change on November 27th, and a copy of that communication can be found in the Knowledge Base article: Admin Session Lifetime/Idle Timeout Security Enhancements.
SV15 - Okta	OKT_OKT_1	Reaktionen > Maßnahmen > Opferseitig	2023-10-17 Okta Security revokes the Okta session tokens embedded in the HAR files.
SV15 - Okta	OKT_OKT_1	Reaktionen > Maßnahmen > Opferseitig	2023-10-19 Okta Security revokes the Okta session tokens embedded in the newly discovered HAR files that had been downloaded by the threat actor.
SV15 - Okta	OKT_OKT_1	Reaktionen > Maßnahmen > Opferseitig	Disabled the compromised service account (Complete)Okta has disabled the service account in the customer support system.
SV15 - Okta	OKT_OKT_1	Reaktionen > Maßnahmen > Opferseitig	Blocking the use of personal Google profiles with Google Chrome (Complete)Okta has implemented a specific configuration option within Chrome Enterprise that prevents sign-in to Chrome on their Okta-managed laptop using a personal Google profile.
SV15 - Okta	OKT_OKT_1	Reaktionen > Maßnahmen > Opferseitig	Enhanced monitoring for the customer support system (Complete) Okta has deployed additional detection and monitoring rules for the customer support system.
SV15 - Okta	OKT_OKT_1	Reaktionen > Maßnahmen > Opferseitig	Binding Okta administrator session tokens based on network location (Complete) Okta has released session token binding based on network location as a product enhancement to combat the threat of session token theft against Okta administrators. Okta administrators are now forced to re-authenticate if we detect a network change. This feature can be enabled by customers in the early access section of the Okta admin portal.
SV15 - Okta	OKT_BC_2	Reaktionen > Maßnahmen > Opferseitig	In response to the breach, Okta took multiple measures to prevent similar incidents in the future, including disabling the compromised service account, blocking the use of personal Google profiles with Google Chrome on Okta-managed devices, deploying additional detection and monitoring rules for its customer support system, and binding Okta administrator session tokens based on network location.
SV15 - Okta	OKT_BC_1	Reaktionen > Maßnahmen > Opferseitig	The company worked with affected customers during the incident investigation and revoked session tokens embedded in shared HAR files.
SV15 - Okta	OKT_BC_1	Reaktionen > Maßnahmen > Opferseitig	Okta also shared a list of indicators of compromise observed during the investigation, including IP addresses and web browser User-Agent information linked to the attackers.
SV15 - Okta	OKT_BC_1	Reaktionen > Maßnahmen > Opferseitig	"While this was a troubling security incident, our Security Incident Response Team's (SIRT) real-time detection and prompt response enabled containment and minimized the impact to Cloudflare systems and data," the company said.

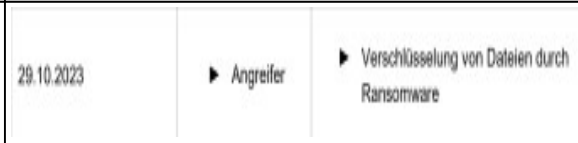
Dokumentgruppe	Dokumentname	Code	Segment
SV15 - Okta	OKT_OKT_2	Reaktionen > Vorschläge	Multi-Factor Authentication (MFA): We strongly recommend all Okta customers secure admin access using MFA at a minimum. We also strongly encourage customers to enroll administrative users in phishing resistant authenticators (such as Okta Verify FastPass, FIDO2 WebAuthn, or PIV/CAC Smart Cards) and to enforce phishing resistance for access to all administrative applications. Please refer to product documentation to enable MFA for the admin console (Classic or OIE).
SV15 - Okta	OKT_OKT_2	Reaktionen > Vorschläge	Phishing Awareness: In addition, Okta customers should be vigilant of phishing attempts that target their employees and especially wary of social engineering attempts that target their IT Help Desks and related service providers. We recommend Okta customers implement our industry-leading, phishing-resistant methods for enrollment, authentication, and recovery. Please see Okta Solutions for Phishing Resistance for more information on protecting your organization from phishing. We also strongly recommend that customers review their IT Help Desk verification processes and ensure that appropriate checks, such as visual verification, are performed before performing high risk actions such as password or factor resets on privileged accounts.
SV15 - Okta	OKT_BC_1	Reaktionen > Vorschläge	It now advises all customers to sanitize their HAR files before sharing to ensure they don't include credentials and cookies/session tokens.
SV15 - Okta	OKT_OKT_1	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Some of these files were HAR files that contained session tokens which could in turn be used for session hijacking attacks. The threat actor was able to use these session tokens to hijack the legitimate Okta sessions of 5 customers, 3 of whom have shared their own response to this event.
SV15 - Okta	OKT_BC_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	"Some of these files were HAR files that contained session tokens which could in turn be used for session hijacking attacks. The threat actor was able to use these session tokens to hijack the legitimate Okta sessions of 5 customers, 3 of whom have shared their own response to this event."
SV15 - Okta	OKT_BC_1	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	The attackers leveraged an authentication token stolen from Okta's support system to pivot into Cloudflare's Okta instance using an open session with Administrative privileges.
SV15 - Okta	OKT_BC_1	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	"It appears that in our case, the threat-actor was able to hijack a session token from a support ticket which was created by a Cloudflare employee. Using the token extracted from Okta, the threat-actor accessed Cloudflare systems on October 18," Cloudflare said.
SV15 - Okta	OKT_BT	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	The incident began when BeyondTrust security teams detected an attacker trying to access an in-house Okta administrator account using a valid session cookie stolen from Okta’s support system.
SV15 - Okta	OKT_BT	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Within 30 minutes of the administrator uploading the file to Okta’s support portal an attacker used the session cookie from this support ticket, attempting to perform actions in the BeyondTrust Okta environment.
SV15 - Okta	OKT_BT	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	BeyondTrust’s custom policies around admin console access initially blocked them, but they pivoted to using admin API actions authenticated with the stolen session cookie.
SV16 - Südwestfalen-IT	SIT_Golem	Angreifer > Unabhängige Gruppierungen	Allerdings gibt es keine konkreten Anzeichen einer Ausnutzung durch die Akira-Gruppe.
SV16 - Südwestfalen-IT	SIT_SIT_4	Angreifer > Unabhängige Gruppierungen	Genau ein Jahr ist es her, dass die Südwestfalen-IT (SIT) von kriminellen Hackern angegriffen wurde: In der Nacht auf den 30. Oktober 2023 verschlüsselte eine Ransomware-Gruppe die Systeme
SV16 - Südwestfalen-IT	SIT_SIT_3	Angreifer > Unabhängige Gruppierungen	Die Datei-Endung .akira weist auf die Ransomware-Gruppe „Akira“ hin.
SV16 - Südwestfalen-IT	SIT_Heise_1	Angreifer > Unabhängige Gruppierungen	Ransomware-Bande Akira
SV16 - Südwestfalen-IT	SIT_Heise_2	Angreifer > Unabhängige Gruppierungen	Ransomware-Gruppe Akira
SV16 - Südwestfalen-IT	SIT_SIT_2	Angreifer > Unabhängige Gruppierungen	Die spezifische Dateiendung der verschlüsselten Dateien .akira, die von den Angreifern hinterlassenen Erpressungsnachrichten sowie die Gesamtcharakteristik des Angriffs deuten darauf hin, dass die professionell agierende Ransomware-Gruppe „Akira“ für den Angriff verantwortlich ist.
SV16 - Südwestfalen-IT	SIT_SIT_2	Angreifer > Unabhängige Gruppierungen	Akira ist eine sich schnell entwickelnde, professionell agierende Ransomware-Gruppe.
SV16 - Südwestfalen-IT	SIT_Golem	Fehler > Organisatorische Schwächen	Entgegen der bisher öffentlich bekannten Information, dass der Cyberangriff in der Nacht vom 29. auf den 30. Oktober 2023 stattfand und unverzüglich durch Herunterfahren der Systeme gestoppt werden konnte, legt der Forensik-Bericht offen, dass die Angreifer die IT-Systeme des Kommunaldienstleisters über Tage auskundschaften konnten. Vorhandene Sicherheitssysteme griffen nicht ein, als die Angreifer das Netzwerk der SIT erkundeten, sondern protokollierten nur bestimmte Zugriffe.
SV16 - Südwestfalen-IT	SIT_Golem	Fehler > Organisatorische Schwächen	In der Kommunikation der SIT und auch im Forensik-Bericht wird CVE-2023-20269 zwar als Zero-Day-Schwachstelle bezeichnet, was im Kontext des obigen Cybervorfall so aber nicht stimmt. Anbieter Cisco veröffentlichte bereits am 6. September 2023 eine Sicherheitswarnung mit konkreten Maßnahmen zum Beseitigen der Schwachstelle mittels Hotfix und weiteren Hinweise zur Absicherung der Appliances.
SV16 - Südwestfalen-IT	SIT_Golem	Fehler > Organisatorische Schwächen	Bei der Analyse des Cybervorfalls stießen die Forensiker auf das Problem, dass die aufgezeichneten Event-Logs von Servern, Clients und IT-Infrastruktur nicht ausreichten, um das Verhalten der Angreifer nach dem initialen Eintritt ins Netzwerk über VPN-Verbindung vollständig zu rekonstruieren. Insbesondere fehlten laut Bericht wichtige Windows-Ereignisprotokolle oder Firewall-Logs innerhalb des Netzwerkes. Auch konnten einige Daten aufgrund der konfigurierten Dauer der Speicherung von Log-Dateien nicht rechtzeitig vor dem Löschen beziehungsweise Überschreiben bewahrt werden.

Dokumentgruppe	Dokumentname	Code	Segment
SV16 - Südwestfalen-IT	SIT_Golem	Fehler > Organisatorische Schwächen	Die Forensiker hielten im Bericht dazu fest, dass auf Grund dieser Konfiguration prinzipiell jeder Angreifer mit validen Domänen-Zugangsdaten das Kennwort des Domänen-Administrators auslesen und durch Verwendung des von Microsoft bereitgestellten AES-Schlüssels entschlüsseln kann. Das Kennwort ermöglicht eine Erhöhung der Zugriffsberechtigungen auf das Niveau des Domänen-Administrators, ohne dabei Spuren im System zu hinterlassen.
SV16 - Südwestfalen-IT	SIT_Golem	Fehler > Organisatorische Schwächen	Geht man den Bericht mit der Analyse des Vorfalls durch, wurden gravierende Fehler in der Absicherung der Systeme gemacht
SV16 - Südwestfalen-IT	SIT_Golem	Fehler > Organisatorische Schwächen	Die Systeme der SIT waren zwar durch den Windows-Defender mit einem Virenschutz versehen. Die Angreifer konnten aber über ihre Administratorberechtigungen eine Ausnahme für das Laufwerk C:\ definieren und es vom Scan auf Schadsoftware ausnehmen. Der Defender war ab diesem Zeitpunkt nutzlos, die Malware w.exe konnte so unerkannt auf verschiedenen Systemen platziert werden.
SV16 - Südwestfalen-IT	SIT_Golem	Fehler > Organisatorische Schwächen	Der Untersuchungsbericht weist für den 30. Oktober 2023 um 1:35 Uhr das Ende der "Symantec-Encryption-Meldungen" auf, vermutlich, weil die erreichbaren Dateien dann bereits verschlüsselt waren. Offenbar wurden zwar Sicherheitslösungen von Symantec eingesetzt, die den Angriff aber nicht abwehrten, sondern nur Operationen protokollierten.
SV16 - Südwestfalen-IT	SIT_Golem	Fehler > Organisatorische Schwächen	Die Aufarbeitung des Cybervorfalls offenbarte aber auch gravierende Schwachstellen in der Infrastruktur des kommunalen IT-Dienstleisters Südwestfalen IT, die diesen Angriff überhaupt erst ermöglichten.
SV16 - Südwestfalen-IT	SIT_Heise_1	Fehler > Organisatorische Schwächen	Die Angreifer begannen offenbar bereits am 18. Oktober, Zugangsdaten auszuprobieren und erbeuteten nach kurzer Zeit die VPN-Kennung eines SIT-Mitarbeiters. Mit diesem Zugang – der nicht per Mehr-Faktor-Authentifizierung (MFA) gegen derlei Ratespielchen geschützt war – hangelten die Kriminellen sich von niederländischen und US-amerikanischen IP-Adressen aus weiter
SV16 - Südwestfalen-IT	SIT_Heise_1	Fehler > Organisatorische Schwächen	Der Fehler mit der CVE-ID CVE-2023-20269 und einer CVSS-Punktzahl von immerhin 9,1 (Einstufung "kritisch") war bereits seit September vergangenen Jahres bekannt, blieb aber offenbar im SIT-Netzwerk ungepatcht.
SV16 - Südwestfalen-IT	SIT_Heise_1	Fehler > Organisatorische Schwächen	Es bleibt dennoch ein fahler Beigeschmack, denn bereits im August hatte der Hersteller vor Ransomware-Angriffen über schlecht geschützte ASA-Appliances gewarnt. Warum diese Warnung von den SIT-Netzwerkadministratoren nicht beachtet wurde, blieb auf Nachfrage durch heise security unklar.
SV16 - Südwestfalen-IT	SIT_Heise_1	Fehler > Organisatorische Schwächen	Einmal im Netz, durchforsteten die digitalen Eindringlinge die SIT-Infrastruktur weitgehend unbehelligt von den Verteidigungsmaßnahmen der Netzwerkadmins. So wurden Scan-Aktivitäten zwar durch eine Symantec-Software detektiert, jedoch offenbar nicht unterbunden oder an die Administratoren gemeldet.
SV16 - Südwestfalen-IT	SIT_Heise_1	Fehler > Organisatorische Schwächen	Nach dem Wiederaufbau der digitalen Infrastruktur in den Verbandskommunen steht für die SIT die kritische Auseinandersetzung mit den Ursachen des Angriffs an. Warum offenbar wichtige Updates nicht eingespielt wurden und wieso trotz anderslautender Warnungen des Herstellers keine Mehr-Faktor-Authentifizierung für das VPN der Südwestfalen-IT ausgerollt war, sind nur zwei Fragen für den künftigen Geschäftsführer Mirco Pinske.
SV16 - Südwestfalen-IT	SIT_Heise_2	Fehler > Organisatorische Schwächen	Die SIT wirkt mit dem Krisenmanagement überfordert, trotz der Hilfe anderer IT-Dienstleister. Ende November kündigt sie einen Notbetrieb mit „ersten wesentlichen Dienstleistungen“ wie dem Ausstellen von Ausweisen ab Mitte Dezember an. Anfang Dezember rudert sie zurück: Der versprochene Wiederanlauf verzögere sich wegen einer „Kombination aus erhöhten Sicherheitsanforderungen und der Komplexität der IT-Systeme“.
SV16 - Südwestfalen-IT	SIT_Heise_2	Fehler > Organisatorische Schwächen	Anfang Dezember machen in den Medien Gerüchte über angeblich niedrige Sicherheitsstandards bei der SIT die Runde. Ein Security-Experte, der nach eigenen Angaben Einblick in SIT-Systeme nehmen konnte, berichtet gegenüber der Siegener Zeitung von simplen Passwörtern wie „Admin123456“ und einem ausgebliebenen wichtigen Sicherheitsupdate für Cisco-Software. Die SIT erklärte dazu auf Anfrage, dass man sich an Spekulationen nicht beteilige.
SV16 - Südwestfalen-IT	SIT_SIT_2	Fehler > Organisatorische Schwächen	keine Multi-Faktor-Authentifizierung eingesetzt wurde.
SV16 - Südwestfalen-IT	SIT_SIT_2	Fehler > Organisatorische Schwächen	Einerseits könnte das teils fehlende Logging innerhalb der Organisation und insbesondere in der intra.lan Domäne dazu geführt haben, dass entscheidende Spuren des Angreifers nicht aufgezeichnet wurden. Dies würde bedeuten, dass mögliche laterale Bewegungen des Angreifers unentdeckt geblieben sind.
SV16 - Südwestfalen-IT	SIT_Golem	Gemeinsamkeiten > Art des Vorfalls > Ransomware	kommunalen IT-Dienstleister Südwestfalen-IT (SIT) zu einem Ransomwarebefall
SV16 - Südwestfalen-IT	SIT_SIT_4	Gemeinsamkeiten > Art des Vorfalls > Ransomware	Der Ransomware-Angriff auf die Südwestfalen-IT war bundesweit der bisher größte und komplexeste Vorfall dieser Art.
SV16 - Südwestfalen-IT	SIT_SIT_3	Gemeinsamkeiten > Art des Vorfalls > Ransomware	um die Ransomware auszuführen
SV16 - Südwestfalen-IT	SIT_SIT_3	Gemeinsamkeiten > Art des Vorfalls > Ransomware	„Die Südwestfalen-IT wurde Opfer eines kriminellen, professionell ausgeführten Ransomware-Angriffs
SV16 - Südwestfalen-IT	SIT_Heise_1	Gemeinsamkeiten > Art des Vorfalls > Ransomware	Der Ransomware-Angriff auf die Südwestfalen-IT (SIT)

Dokumentgruppe	Dokumentname	Code	Segment
SV16 - Südwestfalen-IT	SIT_Heise_2	Gemeinsamkeiten > Art des Vorfalls > Ransomware	Eine Ransomware-Attacke auf den Dienstleister Südwestfalen-IT
SV16 - Südwestfalen-IT	SIT_SIT_2	Gemeinsamkeiten > Art des Vorfalls > Ransomware	Ransomware-Sicherheitsvorfalls dargelegt, der am 29. Oktober 2023 bei der Südwestfalen-IT
SV16 - Südwestfalen-IT	SIT_SIT_2	Gemeinsamkeiten > Art des Vorfalls > Ransomware	Die Südwestfalen-IT wurde am 29. Oktober 2023 Opfer eines Ransomware-Angriffs.
SV16 - Südwestfalen-IT	SIT_SIT_1	Gemeinsamkeiten > Branche > Betroffene Dritte	Bei dem Cyberangriff auf die Südwestfalen-IT Ende Oktober 2023 handelte es sich um einen der größten Angriffe auf die öffentliche Verwaltung
SV16 - Südwestfalen-IT	SIT_SIT_1	Gemeinsamkeiten > Branche > Betroffene Dritte	Gemeinden, Städte und Kreise
SV16 - Südwestfalen-IT	SIT_SIT_1	Gemeinsamkeiten > Branche > Betroffene Dritte	Die freigegebenen Fachverfahren im Basisbetrieb umfassen die Bereiche Finanz-, Standesamts- und Sozialwesen sowie Melde- und Kraftfahrzeugwesen.
SV16 - Südwestfalen-IT	SIT_SIT_1	Gemeinsamkeiten > Branche > Betroffene Dritte	m Norden des Verbandsgebiets konnte bereits mit dem Basisbetrieb für das Meldeauskunftssystem für Sicherheitsbehörden und im Sozialwesen begonnen werden.
SV16 - Südwestfalen-IT	SIT_Heise_2	Gemeinsamkeiten > Branche > Betroffene Dritte	Seitdem ist die Verwaltung in 72 Städten und Gemeinden von Siegen bis Lippstadt mit insgesamt rund 1,7 Millionen Einwohnern weitgehend lahmgelegt
SV16 - Südwestfalen-IT	SIT_Heise_2	Gemeinsamkeiten > Branche > Betroffene Dritte	„bisher größten Cyberangriff auf die öffentliche Verwaltung in Deutschland“
SV16 - Südwestfalen-IT	SIT_Heise_2	Gemeinsamkeiten > Branche > Direkt Betroffene	Dienstleister Südwestfalen-IT
SV16 - Südwestfalen-IT	SIT_Heise_2	Gemeinsamkeiten > Branche > Direkt Betroffene	IT-Dienstleisters Südwestfalen-IT (SIT)
SV16 - Südwestfalen-IT	SIT_Golem	Gemeinsamkeiten > Schwachstelle	Unklar bleibt, wie die Angreifer an die Zugangsdaten für diese VPN-Zugänge gelangten. Ein Brute-Force-Angriff wurde auf Grund vieler fehlgeschlagener Logins vor dem initialen Zugriff vermutet. Belege, dass die Zugangsdaten per Phishing oder im Darknet erworben wurden, ließen sich allerdings nicht finden und dieser Verdacht konnte nicht erhärtet werden.
SV16 - Südwestfalen-IT	SIT_Golem	Gemeinsamkeiten > Schwachstelle	Bei der Analyse des Vorfalls wurde jedoch festgestellt, dass die verwendete Cisco ASA (Adaptive Security Appliances) eine Schwachstelle (CVE-2023-20269) aufwies, die sich für Brute-Force-Angriffe gegen Passwörter und Benutzernamen eignet. Die beauftragten Sicherheitsanalysten gehen davon aus, dass dies der wahrscheinlichste Eintrittsvektor für die Ermittlung der VPN-Zugangsdaten mit anschließender Kompromittierung des Systems darstellt.
SV16 - Südwestfalen-IT	SIT_Golem	Gemeinsamkeiten > Schwachstelle	Diese ungepatchte Schwachstelle in Verbindung mit einer fehlenden Zwei-Faktor-Authentifizierung (2FA) wird als wahrscheinliches Einfallstor für die Angreifer zum 18. Oktober 2023 angesehen.
SV16 - Südwestfalen-IT	SIT_SIT_3	Gemeinsamkeiten > Schwachstelle	Demnach konnten die Angreifer über eine VPN-Lösung eindringen
SV16 - Südwestfalen-IT	SIT_SIT_3	Gemeinsamkeiten > Schwachstelle	Den Zugang zum internen Netzwerk erlangten die Angreifer über eine softwarebasierte VPN-Lösung mit einer Zero-Day-Schwachstelle, die keine Multifaktor-Authentifizierung erforderte.
SV16 - Südwestfalen-IT	SIT_SIT_3	Gemeinsamkeiten > Schwachstelle	Sicherheitslücken in der intra.lan ermöglichten es den Angreifern, die Rechte bis zur Domain-Administrationsberechtigung zu erhöhen
SV16 - Südwestfalen-IT	SIT_Heise_1	Gemeinsamkeiten > Schwachstelle	Der Ransomware-Angriff auf die Südwestfalen-IT (SIT) gelang wohl aufgrund eines schwachen Passworts, fehlender Mehrfaktor-Authentifizierung und einer schlecht gepflegten VPN-Appliance
SV16 - Südwestfalen-IT	SIT_Heise_1	Gemeinsamkeiten > Schwachstelle	eine Sicherheitslücke in einer Cisco-ASA, einer "Adaptive Security Appliance", die als Firewall und VPN-Endpunkt dient. Der Fehler mit der CVE-ID CVE-2023-20269 und einer CVSS-Punktzahl von immerhin 9,1 (Einstufung "kritisch")
SV16 - Südwestfalen-IT	SIT_SIT_2	Gemeinsamkeiten > Schwachstelle	Die unautorisierten Zugriffe der Angreifer waren möglich, da die eingesetzte VPN-Lösung durch eine Schwachstelle verwundbar war und keine Multi-Faktor-Authentifizierung eingesetzt wurde.
SV16 - Südwestfalen-IT	SIT_SIT_2	Gemeinsamkeiten > Schwachstelle	Hierbei zeigten sich kurze Zeit vor dem initialen Zugriff durch die Angreifer vermehrt fehlgeschlagene VPN-Logins – ein Indiz für einen Brute-Force-Angriff
SV16 - Südwestfalen-IT	SIT_SIT_2	Gemeinsamkeiten > Schwachstelle	Die verwundbare Firmware der eingesetzten Firewall in Kombination mit dem Fehlen einer Zwei-Faktor-Authentifizierung erhöhten die Wahrscheinlichkeit, dass ein kompromittiertes VPN-Benutzerkonto als Eintrittspunkt für den Angriff gedient hatte. Dies deckt sich zudem mit dem typischen Vorgehen der Akira-Ransomgroup.
SV16 - Südwestfalen-IT	SIT_SIT_2	Gemeinsamkeiten > Schwachstelle	Eine alternative Möglichkeit, die dem Angreifer den Zugang zu gültigen Zugangsdaten ermöglicht haben könnte, ist die Ausnutzung einer Schwachstelle in der CISCO ASA (CVE-2023-202691,2), einer Zero-Day-Schwachstelle, die für Brute-Force-Angriffe gegen Passwörter als auch gegen Benutzernamen genutzt werden kann und in der Vergangenheit bereits von der Ransomgroup Akira ausgenutzt wurde3,4. Mit so erlangten Zugangsdaten ließe sich eine clientless SSL-VPN-Verbindung zum Zielnetzwerk aufbauen. r-tec betrachtet dieses Szenario als das wahrscheinlichste Einfallstor des Angreifers, insbesondere aufgrund der zum Zeitpunkt des Angriffs verwendeten CISCO ASA-Version 9.12(3)7, die anfällig für die zuvor erwähnte Schwachstelle ist1.

Dokumentgruppe	Dokumentname	Code	Segment
SV16 - Südwestfalen-IT	SIT_SIT_2	Gemeinsamkeiten > Schwachstelle	Während des explorativen Untersuchungsansatzes des Sicherheitsvorfalls stellte r-tec eine kritische Sicherheitslücke in der Windows-Domäne intra.lan fest. Es wurde festgestellt, dass das Kennwort des Domänen-Administrators intra.lan\Administrator seit 2014 in einem Gruppenrichtlinienobjekt in entschlüsselbarer Textform hinterlegt war. Durch diese Konfiguration kann prinzipiell jeder Angreifer mit validen Domänen-Zugangsdaten das Kennwort auslesen. Unter Verwendung des von Microsoft bereitgestellten AES-Schlüssels lässt sich das Kennwort entschlüsseln, was eine Erhöhung der Zugriffsberechtigungen auf das Niveau des Domänen-Administrators ermöglicht, ohne dabei Spuren zu hinterlassen.
SV16 - Südwestfalen-IT	SIT_SIT_2	Gemeinsamkeiten > Schwachstelle	Auf mehreren Systemen wurde zudem festgestellt, dass durch den Angreifer eine Ausnahme in Windows Defender angelegt wurde, um die gesamte C:\ Partition von Malware-Scans auszuschließen. Diese Maßnahme ermöglichte es dem Angreifer, die Ransomware auf verschiedenen Systemen unbemerkt zu platzieren und auszuführen, ohne entdeckt zu werden.
SV16 - Südwestfalen-IT	SIT_Golem	Reaktionen > Maßnahmen > Opferseitig	der Cyberangriff in der Nacht vom 29. auf den 30. Oktober 2023 stattfand und unverzüglich durch Herunterfahren der Systeme gestoppt werden konnte
SV16 - Südwestfalen-IT	SIT_Golem	Reaktionen > Maßnahmen > Opferseitig	Der Autor erfuhr von einer Quelle, die ungenannt bleiben wollte, dass die Ransomware-Infektion erst gegen 2:00 Uhr auffiel, als eine Polizeiabfrage scheiterte, weil bei dem entsprechenden IT-Dienst nichts mehr ging. Daraufhin wurden die Verantwortlichen der SIT informiert und sämtliche Server gegen 6:30 Uhr heruntergefahren sowie die Verbindungen ins Internet und zu den Kunden in den Kommunen gekappt. Ab diesem Zeitpunkt standen keine Dienste und Fachverfahren der SIT mehr für die Kunden zur Verfügung.
SV16 - Südwestfalen-IT	SIT_Golem	Reaktionen > Maßnahmen > Opferseitig	Seit dem 30. Oktober 2023 laufen Analyse und Neuaufbau der Systeme. Erste Fachverfahren stehen für die Kunden in den Kommunen wieder zur Verfügung. Die Südwestfalen-IT (SIT) ging nicht auf die Forderung der Erpresser zur Kontaktaufnahme und Aufnahme von Verhandlungen zu Lösegeldzahlungen ein. Grund war, neben dem entsprechenden Ratschlag der Polizei, wohl auch der Umstand, dass nicht-infizierte Backups vom Zeitraum vor dem 18. Oktober 2023 vorlagen und voraussichtlich keine Daten abgeflossen sind.
SV16 - Südwestfalen-IT	SIT_SIT_4	Reaktionen > Maßnahmen > Opferseitig	Der Krisenmodus der SIT dauerte insgesamt 11 Monate an – zum 30.09.2024 konnte die Organisation in den Normalmodus wechseln. Zum jetzigen Zeitpunkt stehen nahezu 100% des Produktportfolios von rund 160 Anwendungen wieder im vollen Funktionsumfang zur Verfügung. Für die von den Zweckverbandsmitgliedern als besonders prioritär eingestuften Anwendungen – darunter fallen Bürger-, Finanz- und Sozialdienste – wurde der Normalbetrieb bereits vor mehreren Monaten bzw. Wochen erreicht. Lediglich vereinzelt sind noch kleine Restarbeiten zu erledigen, teilweise steht noch Zuarbeit externer Partner aus. Zudem konnten zahlreiche weitere Dienste bereitgestellt und neu eingerichtete Zugriffe für eine dreistellige Anzahl externer Webanwendungen ermöglicht werden.
SV16 - Südwestfalen-IT	SIT_SIT_4	Reaktionen > Maßnahmen > Opferseitig	Gemeinsam mit externen IT- und Cyber-Security-Experten hat die SIT in den vergangenen Monaten bereits zahlreiche Sicherheitsvorkehrungen in allen aktuell eingesetzten Systemen implementiert. Zudem wurden die Erkenntnisse aus dem Vorfall genutzt, um die Sicherheit der IT-Systeme in allen Netzwerkbereichen weiter zu verstärken.
SV16 - Südwestfalen-IT	SIT_SIT_4	Reaktionen > Maßnahmen > Opferseitig	Um einen möglichen Schaden auf einzelne Bereiche zu limitieren, werden die Systeme bspw. noch stärker segmentiert.
SV16 - Südwestfalen-IT	SIT_SIT_4	Reaktionen > Maßnahmen > Opferseitig	Der VPN-Zugang wurde verbandsweit flächendeckend vereinheitlicht und nochmals extra gesichert (Multi-Faktor-Authentifizierung mit One-Time-Passwort und Zertifikat).
SV16 - Südwestfalen-IT	SIT_SIT_4	Reaktionen > Maßnahmen > Opferseitig	Mittels leistungsstarker Software wurde im Bereich Virenschutz sowie Angriffserkennung und -abwehr aufgerüstet.
SV16 - Südwestfalen-IT	SIT_SIT_3	Reaktionen > Maßnahmen > Opferseitig	Durch die unverzügliche Reaktion der Südwestfalen-IT wurde der Angriff erfolgreich gestoppt und das Schadensausmaß effektiv begrenzt. Es kam mit hoher Wahrscheinlichkeit zu keinem Abfluss von Daten, auch die Back-Ups waren nicht betroffen. Alle Sicherheitslücken sind beim Wiederanlaufen geschlossen worden.
SV16 - Südwestfalen-IT	SIT_SIT_3	Reaktionen > Maßnahmen > Opferseitig	Die Südwestfalen-IT dämmte den Angriff durch unverzügliches Herunterfahren und Isolieren der betroffenen Systeme ein. Direkt danach wurden externe, BSI-zertifizierte Cyber-Security-Experten mit der forensischen Untersuchung und dem Wiederaufbau der Infrastruktur beauftragt.
SV16 - Südwestfalen-IT	SIT_SIT_3	Reaktionen > Maßnahmen > Opferseitig	„Fakt ist, dass das Rechenzentrum nicht in der Lage war, den Angriff abzuwehren.“ so Theo Melcher. „Die Erkenntnisse aus dem forensischen Bericht werden nun genutzt, um die Sicherheit der IT-Systeme in allen Netzwerkbereichen und Domänen weiter zu verstärken. Zugleich kann der forensische Bericht anderen helfen, aus dem Vorfall bei der Südwestfalen-IT zu lernen. Die Transparenz, die wir durch die Veröffentlichung des Berichts herstellen, nutzt allen.“
SV16 - Südwestfalen-IT	SIT_SIT_3	Reaktionen > Maßnahmen > Opferseitig	Für den langfristigen Betrieb hat die Südwestfalen-IT wesentliche Änderungen in der System-Architektur geplant, um das System robuster zu gestalten und derartige Vorfälle künftig bestmöglich auszuschließen. Mit den Kreisen und Kommunen hat die Südwestfalen-IT einen Zeitplan abgestimmt. Danach werden die ersten wesentlichen Fachverfahren, die bislang im Basisbetrieb laufen, bis zum Ende des ersten Quartals 2024 in den Normalbetrieb überführt werden. Darüber hinaus werden im ersten Quartal 2024 weitere priorisierte Fachverfahren in den Basisbetrieb gehen.

Dokumentgruppe	Dokumentname	Code	Segment
SV16 - Südwestfalen-IT	SIT_Heise_1	Reaktionen > Maßnahmen > Opferseitig	Der Wiederanlauf geschehe in mehreren Phasen – aufgrund der Komplexität des SIT-Netzes sei eine genaue Prognose unmöglich. Zumindest wolle man die wichtigsten Fachverfahren – als solches bezeichnet die SIT etwa die KFZ-Zulassung oder Ausweis-Beantragung – bis Ende des ersten Quartals wieder in den Normalbetrieb überführen.
SV16 - Südwestfalen-IT	SIT_Heise_1	Reaktionen > Maßnahmen > Opferseitig	Unter Pinske wird die SIT die Erkenntnisse aus dem forensischen Bericht nutzen, um ihre Infrastruktur robuster zu gestalten und weitere Attacken bestmöglich auszuschließen. Zum Maßnahmenkatalog gehören unter anderem Einführung starker Passwortrichtlinien und MFA, aber auch ein ausgefeilteres Schwachstellenmanagement und ein umfassender Cyber-Sicherheitsplan. Eine Zertifizierung der SIT, etwa nach BSI-Grundschutz oder ISO27001, scheint hingegen nicht auf der Agenda zu stehen.
SV16 - Südwestfalen-IT	SIT_Heise_2	Reaktionen > Maßnahmen > Opferseitig	schalten die Mitarbeiter „sofort“ sämtliche Server in den SIT-Rechenzentren in Siegen und Hemer ab
SV16 - Südwestfalen-IT	SIT_SIT_2	Reaktionen > Maßnahmen > Opferseitig	Nach eigenständigen Analysen der S-IT sowie ersten Schritten zur Eindämmung der Anomalien wurden die betroffenen Systeme umgehend heruntergefahren und netzwerktechnisch isoliert. Am Vormittag des 30. Oktober 2023 wurde r-tec für die forensischen Untersuchungen und die Eindämmung des Vorfalls eingeschaltet.
SV16 - Südwestfalen-IT	SIT_SIT_2	Reaktionen > Maßnahmen > Opferseitig	Durch interne Fachleute der S-IT wurde gegen 0:30 Uhr mit eigenständigen Analysen sowie ersten Schritten zur Eindämmung der Anomalien reagiert. Noch in der Nacht entschied die S-IT, alle Systeme herunterzufahren, um weiteren Schaden abzuwenden.
SV16 - Südwestfalen-IT	SIT_SIT_2	Reaktionen > Maßnahmen > Opferseitig	
SV16 - Südwestfalen-IT	SIT_SIT_2	Reaktionen > Vorschläge	Da jedoch valide Sicherungskopien der verschlüsselten Daten vorhanden waren und keine Anzeichen für Datenabflüsse vorlagen, sah die S-IT keine Notwendigkeit, in Verhandlungen mit den Angreifern zu treten – laut eigener Aussage auch auf Empfehlung der Ermittlungsbehörden.
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Schutz	Ausgenommen hierbei ist lediglich der zur Verschlüsselung genutzte Key. Dieser konnte während der Untersuchung nicht identifiziert werden.
SV16 - Südwestfalen-IT	SIT_Golem	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	wurde festgestellt, dass das Kennwort des Domänen-Administrators intra.lan\Administrator seit 2014 in einem Gruppenrichtlinienobjekt in entschlüsselbarer Textform hinterlegt war.
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	das Kennwort des Domänen-Administrators intra.lan\Administrator seit 2014 in einem Gruppenrichtlinienobjekt in entschlüsselbarer Textform hinterlegt war
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	Die Verschlüsselung betraf häufig nicht den gesamten Inhalt der Dateien, sodass viele Informationen noch lesbar waren.
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Schwache o. fehlende Kryptografie	Die vorliegende Ransomware weist minimale Obfuskation sowie keine Anti-Tamper oder Anti-Debugging-Mechanismen auf. Auffallend sind die Aufrufe verdächtiger API-Funktionen sowie das Laden bestimmter DLLs, was typische Indikatoren für schädliche Aktivitäten darstellt. Die direkte Erkennbarkeit aller Strings innerhalb der Ransomware erleichterte die Analyse erheblich.
SV16 - Südwestfalen-IT	SIT_Golem	Rolle der Kryptografie > Verwendung für Angriff > Angriff auf	Als wahrscheinlichstes Szenario wird die Entschlüsselung des in einem Gruppenrichtlinienobjekt abgelegten Kennworts gesehen.
SV16 - Südwestfalen-IT	SIT_Golem	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	zu einem Ransomwarebefall gekommen, bei dem interne Systeme verschlüsselt wurden
SV16 - Südwestfalen-IT	SIT_Golem	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Am 29. Oktober 2023 leiteten die Angreifer dann eine rekursive Verschlüsselung der infizierten Systeme über die Malware w.exe ein. Dies umfasste Systeme, auf denen w.exe platziert worden war, und weitete sich auf Dateien aus, die über Freigaben von diesen Systemen erreichbar waren. Von den 770 Servern und 4.176 Clients der Domäne intra.lan wurden lediglich 961 Systeme mit einer Ransomware-Notiz akira_readme.txt gefunden. Diese Systeme dienten aber der Verwaltung und Bereitstellung der Dienste und Fachverfahren in den Kommunen der Kunden, so dass es zu Ausfällen kam.
SV16 - Südwestfalen-IT	SIT_SIT_4	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	In der Nacht auf den 30. Oktober 2023 verschlüsselte eine Ransomware-Gruppe die Systeme, was immense Auswirkungen auf die 72 Mitgliedskommunen aus dem Verbandsgebiet hatte
SV16 - Südwestfalen-IT	SIT_Heise_1	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Sie kundschafteten das SIT-Netz aus und begannen am 29. Oktober mit der Verschlüsselung der Systeme.
SV16 - Südwestfalen-IT	SIT_Heise_1	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Der eigentliche Verschlüsselungsangriff fand zwischen dem Vormittag des 29. Oktober und dem Folgetag statt: Insgesamt infizierten die vermutlich russischsprachigen Kriminellen über 960 Systeme.
SV16 - Südwestfalen-IT	SIT_Heise_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	steckt die Ransomware-Gruppe Akira hinter dem Angriff und hat Lösegeld für verschlüsselte Daten gefordert.
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Bei diesem Typ von Angriff werden Daten auf Geräten verschlüsselt und anschließend die Entschlüsselung gegen Zahlung eines Lösegeldes angeboten.
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Die ersten verschlüsselten Dateien mit der Dateiendung .akira wurden in der Nacht von Sonntag, 29. Oktober 2023, auf Montag, 30. Oktober 2023, bemerkt

Dokumentgruppe	Dokumentname	Code	Segment
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	koordinierten Verschlüsselung am 29. Oktober 2023
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Die Angreifer breiteten sich am 29. Oktober 2023 mit administrativen Berechtigungen auf mehrere zentrale Systeme der intra.lan Domäne aus, um von dort aus die Verschlüsselung der erreichbaren Systeme zu initiieren.
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Es wurden lediglich 961 Systeme identifiziert, auf denen die Ransomnote akira_readme.txt vorzufinden war, von denen durch die S-IT 346 als Clients klassifiziert wurden. Diese Tatsache impliziert, dass lediglich diese Systeme von der Verschlüsselung der Ransomware betroffen sind.
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Hierbei fiel auf, dass die Ransomware w.exe selbst Logfiles schreibt, in denen dokumentiert wird, welche Aktionen durch die Schadsoftware durchgeführt werden bzw. welche Fehler beim Verschlüsseln auftraten. Weil die Logfiles selbst teilweise von der Ransomware verschlüsselt wurden, sind nicht alle Daten für die Analyse verfügbar.
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Die Logdateien der w.exe machen deutlich, dass die Verschlüsselung der Zielsysteme ihren Ausgang von jenen Systemen nahm, auf denen die w.exe gezielt platziert wurde. Anschließend griff sie über Netzwerkfreigaben auf das Dateisystem der Zielsysteme zu und führte dort eine rekursive Verschlüsselung der Daten durch.
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Die Akira-Ransomgroup verwendete eine ausführbare Datei mit dem Namen w.exe zur Verschlüsselung des Dateisystems auf den Zielsystemen.
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Die Analyse offenbarte, dass die Ransomware bei ihrer Ausführung die Wiederherstellung von verschlüsselten Dateien verhindert, indem sie die Shadow Copies des Dateisystems mittels eines PowerShell-Befehls löscht.
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Bei der Verschlüsselung des Dateisystems durch die Ransomware wird ein rekursiver Ansatz verfolgt: Das Programm durchläuft das gesamte Dateisystem und verschlüsselt dabei jedes Verzeichnis einzeln, beginnend mit dem angegebenen Startpfad. Ein interessantes Detail dabei ist, dass w.exe eine Blacklist nutzt, um bestimmte Dateitypen, Dateiendungen und Verzeichnisse von der Verschlüsselung auszunehmen.
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Nachdem die Verschlüsselung in einem Verzeichnis abgeschlossen ist, platziert die Ransomware in jedem betroffenen Verzeichnis eine Erpressungsnachricht mit dem Namen akira_readme.txt (siehe Kapitel 8.2 Ransomnote akira_readme.txt). In dieser Nachricht befindet sich die Aufforderung zur Kontaktaufnahme mit den Angreifern.
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Die Ransomware bietet den Angreifern die Möglichkeit, über Command-Line-Argumente Einfluss auf ihre Funktionalität zu nehmen. Diese Optionen beinhalten unter anderem die Festlegung spezifischer Pfade, entlang derer eine rekursive Datenverschlüsselung durchgeführt werden soll. Weiterhin kann der Pfad zu einer Datei angegeben werden, die eine Liste mit weiteren Pfaden und Netzwerkfreigaben enthält, die für eine Verschlüsselung vorgesehen sind. Diese Anpassbarkeit der Ransomware ermöglicht es dem Angreifer, gezielt ausgewählte Daten und Bereiche im Netzwerk für die Verschlüsselung zu definieren.
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Ein weiterer Aspekt, der während der Analyse festgestellt wurde, ist die Fähigkeit der Ransomware, Logfiles zu erstellen. In diesen Protokollen werden die genutzten Threads zur Verschlüsselung sowie zum Dateizugriff, Anzahl der CPU-Kerne, der Fortschritt der Verschlüsselung sowie Fehlermeldungen dokumentiert.
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	Die Untersuchung zeigte, dass die Angreifer eine partielle Verschlüsselung der Dateien durchführten, indem sie mittels Command-Line-Argument nur einen geringen prozentualen Anteil der Dateien verschlüsselten. Beispielsweise waren die Logdateien zwar verschlüsselt, aber nur zu einem geschätzten Anteil von etwa 10 – 25 %. Dies führte dazu, dass Teile der betroffenen Daten noch lesbar blieben, während hauptsächlich der Anfang der Dateien durch die Verschlüsselung unlesbar wurde. Diese Methode der partiellen Verschlüsselung ermöglichte es den Angreifern, effizienter Schaden anzurichten, da bereits ein geringer verschlüsselter Anteil ausreicht, um viele Dateitypen funktional
SV16 - Südwestfalen-IT	SIT_SIT_2	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	unbrauchbar zu machen. Eine vollständige Verschlüsselung aller Daten hätte dagegen deutlich mehr Zeit in Anspruch genommen
SV17 - Change Healthcare	CH_Wired	Angreifer > Unabhängige Gruppierungen	Change Healthcare wrote that it paid a ransom to a cybercriminal group extorting the company, a hacker gang known as AlphV or BlackCat.
SV17 - Change Healthcare	CH_TC_2	Angreifer > Unabhängige Gruppierungen	the cyberattack was in fact the work of a ransomware gang
SV17 - Change Healthcare	CH_TC_2	Angreifer > Unabhängige Gruppierungen	UnitedHealth said the gang “represented itself to us as ALPHV/BlackCat,”
SV17 - Change Healthcare	CH_TC_2	Angreifer > Unabhängige Gruppierungen	A dark web leak site associated with the ALPHV/BlackCat gang also took credit for the attack

Dokumentgruppe	Dokumentname	Code	Segment
SV17 - Change Healthcare	CH_TC_2	Angreifer > Unabhängige Gruppierungen	ALPHV (aka BlackCat) is a known Russian-speaking ransomware-as-a-service gang. Its affiliates — contractors who work for the gang — break into victim networks and deploy malware developed by ALPHV/BlackCat's leaders, who take a cut of the profits collected from the ransoms collected from victims to get their files back.
SV17 - Change Healthcare	CH_Heise	Angreifer > Unabhängige Gruppierungen	Ransomware-Gang AlphV, auch bekannt als BlackCat
SV17 - Change Healthcare	CH_TC_1	Angreifer > Unabhängige Gruppierungen	UHG attributed the cyberattack to ALPHV/BlackCat, a Russian-speaking ransomware and extortion gang, which later took credit for the cyberattack.
SV17 - Change Healthcare	CH_TC_2	Fehler > Organisatorische Schwächen	That's what happened with UnitedHealth Group (UHG) chief executive Andrew Witty, who on Capitol Hill admitted that the hackers broke into Change Healthcare's systems using a single set password on a user account not protected with multi-factor authentication, a basic security feature that can prevent password reuse attacks by requiring a second code sent to that account holder's phone.
SV17 - Change Healthcare	CH_TC_2	Fehler > Organisatorische Schwächen	One of the biggest data breaches in U.S. history was entirely preventable, was the key message.
SV17 - Change Healthcare	CH_TC_1	Fehler > Organisatorische Schwächen	During a House hearing into the cyberattack in April, UnitedHealth's CEO Witty confirmed that the cybercriminals broke into one of its employee systems using stolen credentials that were not protected with multi-factor authentication (MFA), a security feature that can help to protect against the misuse of password theft.
SV17 - Change Healthcare	CH_TC_1	Fehler > Organisatorische Schwächen	It's unclear why the system was not protected with MFA, but this will likely remain a key part of the ongoing investigations by lawmakers and the government.
SV17 - Change Healthcare	CH_TC_1	Fehler > Organisatorische Schwächen	Lawmakers homed in on how UHG handles so much data and generates so much revenue and failed at basic cybersecurity.
SV17 - Change Healthcare	CH_TC_1	Fehler > Organisatorische Schwächen	While the lack of MFA was abused in this case, the sheer size and wealth of highly sensitive data that Change Healthcare collects and stores made it a target in itself, lawmakers said.
SV17 - Change Healthcare	CH_TC_2	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	one of the largest data breaches of U.S. health and medical data in history.
SV17 - Change Healthcare	CH_TC_2	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	Widespread disruption across U.S. healthcare amid fears of data breach
SV17 - Change Healthcare	CH_Heise	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	bestätigt die UnitedHealth Group einen Datenabflus
SV17 - Change Healthcare	CH_TC_1	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	data breach, after previously saying it anticipated the breach to include data on a "substantial proportion of people in America."
SV17 - Change Healthcare	CH_TC_1	Gemeinsamkeiten > Art des Vorfalls > Datenschutzverletzung	data breach at Change Healthcare stands as the largest known digital theft of U.S. medical records, and one of the biggest data breaches in living history.
SV17 - Change Healthcare	CH_Wired	Gemeinsamkeiten > Art des Vorfalls > Ransomware	ransomware debacle
SV17 - Change Healthcare	CH_TC_2	Gemeinsamkeiten > Art des Vorfalls > Ransomware	ransomware attack
SV17 - Change Healthcare	CH_Heise	Gemeinsamkeiten > Art des Vorfalls > Ransomware	Ransomware-Angriff
SV17 - Change Healthcare	CH_TC_1	Gemeinsamkeiten > Art des Vorfalls > Ransomware	ransomware attack on Change Healthcare
SV17 - Change Healthcare	CH_Wired	Gemeinsamkeiten > Branche > Betroffene Dritte	AlphV's digital paralysis of Change Healthcare snarled the insurance approval of prescriptions and medical procedures for hundreds of medical practices and hospitals across the country, making it by some measures the most widespread medical ransomware disruption ever.
SV17 - Change Healthcare	CH_TC_2	Gemeinsamkeiten > Branche > Betroffene Dritte	doctors offices and healthcare practices
SV17 - Change Healthcare	CH_TC_2	Gemeinsamkeiten > Branche > Betroffene Dritte	Meanwhile, weeks into the cyberattack, outages were still ongoing with many unable to get their prescriptions filled or having to pay cash out of pocket. Military health insurance provider TriCare said "all military pharmacies worldwide" were affected as well.
SV17 - Change Healthcare	CH_Heise	Gemeinsamkeiten > Branche > Betroffene Dritte	erhebliche Auswirkungen auf die Patientenversorgung, Ärzte und Apotheker, aber auch auf US-Militär-Krankenhäuser
SV17 - Change Healthcare	CH_TC_1	Gemeinsamkeiten > Branche > Betroffene Dritte	across the U.S. healthcare sector, including thousands of hospitals, pharmacies, and medical practices
SV17 - Change Healthcare	CH_Wired	Gemeinsamkeiten > Branche > Direkt Betroffene	medical firm Change Healthcare
SV17 - Change Healthcare	CH_TC_2	Gemeinsamkeiten > Branche > Direkt Betroffene	UnitedHealth-owned health tech company Change Healthcare
SV17 - Change Healthcare	CH_TC_2	Gemeinsamkeiten > Branche > Direkt Betroffene	Change Healthcare processes billing and insurance for hundreds of thousands of hospitals, pharmacies and medical practices across the U.S. healthcare sector.

Dokumentgruppe	Dokumentname	Code	Segment
SV17 - Change Healthcare	CH_Heise	Gemeinsamkeiten > Branche > Direkt Betroffene	UnitedHealth-Tochter Change Healthcare, dem größten Bezahldienstleister im US-Gesundheitswesen.
SV17 - Change Healthcare	CH_TC_1	Gemeinsamkeiten > Branche > Direkt Betroffene	Change Healthcare is one of the largest handlers of health, medical data, and patient records, as it processes patient insurance and billing across the U.S. healthcare sector
SV17 - Change Healthcare	CH_TC_2	Gemeinsamkeiten > Schwachstelle	the hackers broke into Change Healthcare’s systems using a single set password on a user account not protected with multi-factor authentication
SV17 - Change Healthcare	CH_Heise	Gemeinsamkeiten > Schwachstelle	Der Zugriff gelang den Angreifern über einen Server, der nicht über Multi-Faktor-Authentifizierung abgesichert war. So seien die Angreifer in der Lage gewesen, auf die Anwendung Citrix für den Remote-Zugang für die Systeme von Change Healthcare zuzugreifen
SV17 - Change Healthcare	CH_TC_1	Gemeinsamkeiten > Schwachstelle	By gaining access to a critical internal system using only a stolen password, the ransomware gang was able to reach other parts of Change Healthcare’s network and deploy ransomware.
SV17 - Change Healthcare	CH_Wired	Reaktionen > Kommunikation	Change Healthcare wrote that it paid a ransom to a cybercriminal group extorting the company
SV17 - Change Healthcare	CH_Wired	Reaktionen > Kommunikation	Compounding the situation, a conflict between hackers in the ransomware ecosystem has led to a second ransomware group claiming to possess Change Healthcare's stolen data and threatening to sell it to the highest bidder on the dark web. Earlier this month that second group, known as RansomHub, sent WIRED alleged samples of the stolen data that appeared to come from Change Healthcare's network, including patient records and a contract with another health care company.
SV17 - Change Healthcare	CH_TC_2	Reaktionen > Kommunikation	In a posting, the ALPHV affiliate who carried out the hack on Change Healthcare claimed that the ALPHV leadership stole $22 million paid as a ransom and included a link to a single bitcoin transaction on March 3 as proof of their claim.
SV17 - Change Healthcare	CH_TC_2	Reaktionen > Kommunikation	By March 13, Change Healthcare had received a “safe” copy of the stolen data that it had just days earlier paid $22 million for. This allowed Change to begin the process of poring through the dataset to determine whose information was stolen in the cyberattack, with the aim of notifying as many affected individuals as possible.
SV17 - Change Healthcare	CH_TC_2	Reaktionen > Kommunikation	For the first time, UnitedHealth confirmed on April 22 — more than two months after the ransomware attack began — that there was a data breach and that it likely affects a “substantial proportion of people in America,” without saying how many millions of people that entails.
SV17 - Change Healthcare	CH_TC_2	Reaktionen > Kommunikation	It took Change Healthcare until June 20 to begin formally notifying affected individuals that their information was stolen, as legally required under a law commonly known as HIPAA, likely delayed in part by the sheer size of the stolen dataset.
SV17 - Change Healthcare	CH_TC_2	Reaktionen > Kommunikation	The company published a notice disclosing the data breach and said that it would begin notifying individuals it had identified in the “safe” copy of the stolen data. But Change said it “cannot confirm exactly” what data was stolen about each individual and that the information may vary from person to person. Change says it was posting the notice on its website, as it “may not have sufficient addresses for all affected individuals.”
SV17 - Change Healthcare	CH_TC_2	Reaktionen > Kommunikation	The incident was so big and complex that the U.S. Department of Health and Human Services stepped in and said that affected healthcare providers, whose patients are ultimately affected by the breach, can ask UnitedHealth to notify affected patients on their behalf, an effort seen at lessening the burden on smaller providers whose finances were hit amid the ongoing outage.
SV17 - Change Healthcare	CH_TC_2	Reaktionen > Kommunikation	The health tech giant confirmed in late June that it would begin notifying those whose healthcare data was stolen in its ransomware attack on a rolling basis. That process began in late July. The letters going out to affected individuals will most likely come from Change Healthcare, if not the specific healthcare provider affected by the hack at Change. The letter confirms what kinds of data was stolen, including medical data and health insurance information, and claims and payment information, which Change said includes financial and banking information.
SV17 - Change Healthcare	CH_TC_2	Reaktionen > Kommunikation	It took the health insurance giant more than eight months to announce, but it has now confirmed that the data breach affects more than 100 million individuals. The number of those affected is expected to rise, given some have received data breach notifications as recently as October. The U.S. Department of Health and Human Services reported the updated number on its data breach portal on October 24.
SV17 - Change Healthcare	CH_TC_1	Reaktionen > Kommunikation	In paying the ransom, Change obtained a copy of the stolen dataset, allowing the company to identify and notify the affected individuals whose information was found in the data.
SV17 - Change Healthcare	CH_Wired	Reaktionen > Maßnahmen > Dritte	Compounding Change Healthcare's mess is an apparent double-cross within the ransomware underground: AlphV, by all appearances, faked its own law enforcement takedown after receiving Change Healthcare's payment in an attempt to avoid sharing it with its so-called affiliates, the hackers who partner with the group to penetrate victims on its behalf. The second ransomware group threatening Change Healthcare, RansomHub, now claims to WIRED that they obtained the stolen data from those affiliates, who still want to be paid for their work.

Dokumentgruppe	Dokumentname	Code	Segment
SV17 - Change Healthcare	CH_TC_2	Reaktionen > Maßnahmen > Dritte	In early March, the ALPHV ransomware gang vanished. The gang's leak site on the dark web, which weeks earlier took credit for the cyberattack, was replaced with a seizure notice claiming that U.K. and U.S. law enforcement took down the gang's site. But both the FBI and U.K. authorities denied taking down the ransomware gang as they had attempted months earlier. All signs pointed to ALPHV running off with the ransom and pulling an "exit scam."
SV17 - Change Healthcare	CH_TC_2	Reaktionen > Maßnahmen > Dritte	By late March, the U.S. government said it was upping its bounty for information on key leadership of ALPHV/BlackCat and its affiliates. By offering $10 million to anyone who can identify or locate the individuals behind the gang, the U.S. government seemed to hope that one of the gang's insiders would turn on their former leaders.
SV17 - Change Healthcare	CH_TC_2	Reaktionen > Maßnahmen > Dritte	And then there were two — ransoms, that is. By mid-April, the aggrieved affiliate set up a new extortion racket called RansomHub, and since it still had the data that it stole from Change Healthcare, it demanded a second ransom from UnitedHealth. In doing so, RansomHub published a portion of the stolen files containing what appeared to be private and sensitive patient records as proof of their threat.
SV17 - Change Healthcare	CH_TC_1	Reaktionen > Maßnahmen > Dritte	The ransomware gang's leaders later vanished after absconding with a $22 million ransom paid by the health insurance giant, stiffing the group's contractors who carried out the hacking of Change Healthcare out of their new financial windfall. The contractors took the data they stole from Change Healthcare and formed a new group, which extorted a second ransom from UHG, while publishing a portion of the stolen files online in the process to prove their threat.
SV17 - Change Healthcare	CH_TC_1	Reaktionen > Maßnahmen > Dritte	Months after the Change Healthcare breach, the U.S. State Department upped its reward for information on the whereabouts of the ALPHV/BlackCat cybercriminals to $10 million
SV17 - Change Healthcare	CH_Wired	Reaktionen > Maßnahmen > Opferseitig	it did indeed pay a $22 million ransom to the hackers who targeted the company in February.
SV17 - Change Healthcare	CH_Wired	Reaktionen > Maßnahmen > Opferseitig	"A ransom was paid as part of the company's commitment to do all it could to protect patient data from disclosure," the statement reads.
SV17 - Change Healthcare	CH_Wired	Reaktionen > Maßnahmen > Opferseitig	Change Healthcare's statement didn't state the size of the ransom payment. In a hearing held by the US Senate's Finance Committee on May 1, however, Andrew Witty, CEO of Change Healthcare parent company UnitedHealth Group, confirmed that the payment was $22 million.
SV17 - Change Healthcare	CH_Wired	Reaktionen > Maßnahmen > Opferseitig	Cybersecurity and cryptocurrency researchers told WIRED last month that Change Healthcare appeared to have paid that ransom on March 1
SV17 - Change Healthcare	CH_TC_2	Reaktionen > Maßnahmen > Opferseitig	It turns out that Change Healthcare invoked its security protocols and shut down its entire network to isolate intruders it found in its systems.
SV17 - Change Healthcare	CH_TC_2	Reaktionen > Maßnahmen > Opferseitig	UnitedHealth also confirmed it paid a ransom for the data but would not say how many ransoms it ultimately paid.
SV17 - Change Healthcare	CH_Heise	Reaktionen > Maßnahmen > Opferseitig	Change Healthcare bot den betroffenen Personen nach Bekanntwerden des Angriffs kostenlosen Identitätsschutz und Kreditüberwachung für zwei Jahre an. Zudem kooperiert das Unternehmen mit Cybersicherheitsexperten und Strafverfolgungsbehörden, um den Vorfall aufzuklären.
SV17 - Change Healthcare	CH_TC_1	Reaktionen > Maßnahmen > Opferseitig	The cyberattack became public on February 21 when Change Healthcare pulled much of its network offline to contain the intruders, causing immediate outages across the U.S. healthcare sector that relied on Change for handling patient insurance and billing.
SV17 - Change Healthcare	CH_TC_1	Reaktionen > Maßnahmen > Opferseitig	Witty told lawmakers that the organization has since rolled out and now enforces MFA following the cyberattack.
SV17 - Change Healthcare	CH_Wired	Rolle der Kryptografie > Verwendung für Angriff > Angriff durch	after it had already paid the hackers an exorbitant sum—a payment in exchange for a decryption key for the systems the hackers had encrypted and a promise not to leak the company's stolen data.

A.6. Materialquellen der Analyse

Dieser Anhang enthält eine Tabelle, in der alle verwendeten Materialquellen pro IT-Sicherheitsvorfall erfasst sind. Einige der URLS sind nicht anklickbar, da neben der Original-URL eine weitere Archiv-URL angegeben werden musste, weil nicht alle Artikel frei zugänglich waren.

Kürzel	Titel	Autor	Datum	URL	Abrufdatum
SV01	**CafePress**				
CP_BC_1	CP_BC_1	Lawrence Abrams	5. August 2019	https://www.bleepingcomputer.com/news/security/cafepress-data-breach-exposes-personal-info-of-23-million-users/	04. Jan 25
CP_Forbes	CafePress Hacked, 23M Accounts Compromised. Is Yours One Of Them?	Davey Winder	5. August 2019	https://www.forbes.com/sites/daveywinder/2019/08/05/cafepress-hacked-23m-accounts-compromised-is-yours-one-of-them/	04. Jan 25
CP_BC_2	CafePress fined $500,000 for breach affecting 23 million users	Sergiu Gatlan	24. Juni 2022	https://www.bleepingcomputer.com/news/security/cafepress-fined-500-	04. Jan 25
SV02	**Canva**				
CNV_Ba	A Case Study of Credential Stuffing Attack: Canva Data Breach	Minh Hieu Nguyen Ba; Jacob Bennett; Michael Gallagher; Suman Bhunia	Dezember 2021	https://doi.org/10.1109/CSCI54926.2021.00187	04. Jan 25
CNV_ZDN	Australian tech unicorn Canva suffers security breach	Catalin Cimpanu	24. Mai 2019	https://www.zdnet.com/article/australian-tech-unicorn-canva-suffers-	04. Jan 25
CNV_CB	Decrypting Canva's Security Breach That Affected 139 Million User Accounts | by Spreeha Dutta | codeburst	Spreeha Dutta	19. Juni 2020	https://codeburst.io/inside-canvas-security-breach-that-affected-139-million-user-accounts-78467e315681	04. Jan 25
CNV_Canva	Canva Security Incident – May 24 FAQs - Canva Help Center	Canva	17. Januar 2020	https://www.canva.com/help/incident-may24/	04. Jan 25
SV03	**Capital One**				
CO_Neto	A Case Study of the Capital One Data Breach	Novaes Neto, Nelson and Madnick, Stuart E. and Moraes G. de Paula, Anchises and Malara Borges, Natasha	Januar 2020	http://dx.doi.org/10.2139/ssrn.3542567	04. Jan 25
CO_Khan	A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned	Shaharyar Khan, Ilya Kabanov, Yunke Hua, and Stuart Madnick	7. November 2022	https://doi.org/10.1145/3546068	04. Jan 25
CO_ZDN	100 million Americans and 6 million Canadians caught up in Capital One breach	Chris Duckett	29. Juli 2019	https://www.zdnet.com/article/100-million-americans-and-6-million-canadians-caught-up-in-capital-one-breach/	04. Jan 25
CO_KoS_2	What We Can Learn from the Capital One Hack – Krebs on Security	Brian Krebs	2. August 2019	https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-	04. Jan 25
CO_KoS_1	Capital One Data Theft Impacts 106M People – Krebs on Security	Brian Krebs	30. Juli 2019	https://krebsonsecurity.com/2019/07/capital-one-data-theft-impacts-	04. Jan 25
CO_SNK	A Technical Analysis of the Capital One Cloud Misconfiguration Breach | Snyk	Josh Stella	26. August 2019	https://snyk.io/de/blog/a-technical-analysis-of-the-capital-one-cloud-misconfiguration-breach/	04. Jan 25
CO_CapOne	2019 Capital One Cyber Incident | What Happened | Capital One	Capital One	22. April 2022	https://www.capitalone.com/digital/facts2019/	04. Jan 25
SV04	**BigBasket**				
BB_SA	20 million Bigbasket user records available on the dark web	Pierluigi Paganini	07. Novmeber 2020	https://securityaffairs.com/110543/data-breach/bigbasket-details-dark-web.html	04. Jan 25
BB_TC	Alleged records of 20 million BigBasket users published online | TechCrunch	Manish Singh	25. April 2021	https://techcrunch.com/2021/04/25/hacker-publishes-alleged-records-of-20-million-bigbasket-users/	04. Jan 25
BB_BC	Hacker leaks 20 million alleged BigBasket user records for free	Lawrence Abrams	25. April 2021	https://www.bleepingcomputer.com/news/security/hacker-leaks-20-	04. Jan 25
					04. Jan 25
SV05	**CAM4**				
CM4_Sorn	Exploring the CAM4 Data Breach: Security Vulnerabilities and Response Strategies	Jacob Sorn; Patrick Carroll; Zachary Pang; Suman Bhunia; Mohammad Salman; Paulo A Regis	Mai 2024	https://doi.org/10.1109/CCGridW63211.2024.00028	
CM4_BC	CAM4 adult cam site exposes 11 million emails, private chats	Sergiu Gatlan	4. Mai 2020	https://www.bleepingcomputer.com/news/security/cam4-adult-cam-site-	04. Jan 25
CM4_SD	Live streaming adult site leaves 7 terabytes of private data exposed	SafetyDetectives Cybersecurity Team	4. Mai 2020	https://www.safetydetectives.com/blog/cam-leak-report/	04. Jan 25
CM4_Wired	Adult Cam Site CAM4 Exposed 10.88 Billion Records Online	Brian Barrett	5. Mai 2020	https://www.wired.com/story/cam4-adult-cam-data-leak-7tb/	04. Jan 25

SV06	**SolarWinds**				
SW_Sterle	On SolarWinds Orion Platform Security Breach	Lindsay Sterle; Suman Bhunia	Oktober 2021	https://doi.org/10.1109/SWC50871.2021.00094	04. Jan 25
SW_SoWi_1	SolarWinds Update on Security Vulnerability - Orange Matter	SolarWinds	17. Dezember 2020	https://orangematter.solarwinds.com/2020/12/17/solarwinds-update-on-	04. Jan 25
SW_SoWi_2	New Findings From Our Investigation of SUNBURST - Orange Matter	Sudhakar	11. Januar 2021	https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our	04. Jan 25
SW_SoWi_3	An Investigative Update of the Cyberattack - Orange Matter	Sudhakar	7. Mai 2021	https://orangematter.solarwinds.com/2021/05/07/an-investigative-	04. Jan 25
SW_SA	Intern caused 'solarwinds123' password leak,former SolarWinds CEO says	Pierluigi Paganini	1. März 2021	https://securityaffairs.com/115134/security/solarwinds-intern-solarwinds123-password-leak.html	04. Jan 25
SW_TT	SolarWinds hack explained: Everything you need to know	Saheed Oladimeji, Sean Michael Kerner	3. November 2023	https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know	04. Jan 25
SW_GB_1	SolarWinds Supply Chain Attack Uses SUNBURST Backdoor | Google Cloud Blog	FireEye	13. Dezember 2020	https://cloud.google.com/blog/topics/threat-intelligence/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-	04. Jan 25
SW_GB_2	SUNBURST Additional Technical Details | Mandiant | Google Cloud Blog	Stephen Eckels, Jay Smith, William	24. Dezember 2020	https://cloud.google.com/blog/topics/threat-intelligence/sunburst-additional-technical-details/?hl=en	04. Jan 25
SV07	**Brenntag**				
BT_BC_1	US chemical distributor shares info on DarkSide ransomware data theft	Sergiu Gatlan	3. Juli 2021	https://www.bleepingcomputer.com/news/security/us-chemical-distributor-shares-info-on-darkside-ransomware-data-theft/	04. Jan 25
BT_HS	Chemical Distributor Brenntag Says What Data Was Stolen During the Ransomware Attack	Antonia Din	5. Juli 2021	https://heimdalsecurity.com/blog/chemical-distributor-brenntag-says-what-data-was-stolen-during-the-ransomware-attack/	04. Jan 25
BT_BC_2	Chemical distributor pays $4.4 million to DarkSide ransomware	Lawrence Abrams	13. Mai 2021	https://www.bleepingcomputer.com/news/security/chemical-distributor-	04. Jan 25
SV08	**Colonial Pipeline**				
ColP_Beerman	A Review of Colonial Pipeline Ransomware Attack	Jack Beerman; David Berent; Zach Falter; Suman Bhunia	Mai 2023	https://doi.org/10.1109/CCGridW59191.2023.00017	04. Jan 25
ColP_NYT	Cyberattack Forces a Shutdown of a Top U.S. Pipeline	David E. SangerClifford	13. Mai 2021	https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html	04. Jan 25
ColP_BC	Largest U.S. pipeline shuts down operations after ransomware attack	Lawrence Abrams	8. Mai 2021	https://www.bleepingcomputer.com/news/security/largest-us-pipeline-shuts-down-operations-after-ransomware-attack/	04. Jan 25
SV09	**Microsoft Exchange 2021**				
MS21_Pitney	A Systematic Review of 2021 Microsoft Exchange Data Breach Exploiting Multiple Vulnerabilities	Alexis M Pitney; Spencer Penrod; Molly Foraker; Suman Bhunia	Juli 2022	https://doi.org/10.23919/SpliTech55088.2022.9854268	04. Jan 25
MS21_KoS_2	At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software – Krebs on Security	Brian Krebs	5. März 2021	https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/	04. Jan 25
MS21_Kos_1	Microsoft: Chinese Cyberspies Used 4 Exchange Server Flaws to Plunder Emails – Krebs on Security	Brian Krebs	2. März 2021	https://krebsonsecurity.com/2021/03/microsoft-chinese-cyberspies-used-4-exchange-server-flaws-to-plunder-emails/	04. Jan 25
MS21_MS	HAFNIUM targeting Exchange Servers with 0-day exploits	Microsoft 365 Security, Microsoft Threat	16. März 2021	https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/	04. Jan 25
MS21_Heise	Der Hafnium Exchange-Server-Hack: Anatomie einer Katastrophe	Günter Born	11. März 2021	https://www.heise.de/news/Der-Hafnium-Exchange-Server-Hack-	04. Jan 25
MS21_KoS_3	A Basic Timeline of the Exchange Mass-Hack – Krebs on Security	Brian Krebs	8. März 2021	https://krebsonsecurity.com/2021/03/a-basic-timeline-of-the-exchange-	04. Jan 25
MS21_ITP	Microsoft warns of ransomware attacks as Exchange hack escalates | ITPro	Sabina Weston	14. März 2021	https://www.itpro.com/security/ransomware/358876/microsoft-warns-of-ransomware-attacks-as-exchange-hack-escalates	04. Jan 25
SV10	**T-Mobile**				
TM_Faircloth	A Study on Brute Force Attack on T-Mobile Leading to SIM-Hijacking and Identity-Theft	Christopher Faircloth; Gavin Hartzell; Nathan Callahan; Suman Bhunia	Juni 2022	https://doi.org/10.1109/AIIoT54504.2022.9817175	04. Jan 25

TM_CSO	The T-Mobile data breach: A timeline | CSO Online	Michael Hill	27. August 2021	https://www.csoonline.com/article/571199/the-t-mobile-data-breach-a-	04. Jan 25
TM_WSJ	T-Mobile Hacker Who Stole Data on 50 Million Customers: 'Their Security Is Awful' - WSJ	Drew FitzGerald, Robert McMillan	27. August 2021	https://www.wsj.com/articles/t-mobile-hacker-who-stole-data-on-50-million-customers-their-security-is-awful-11629985105 (Archiv-Link: https://archive.ph/fClfV)	04. Jan 25
TM_KoS_1	T-Mobile Investigating Claims of Massive Data Breach – Krebs on Security	Brian Krebs	16. August	https://krebsonsecurity.com/2021/08/t-mobile-investigating-claims-of-massive-data-breach/	04. Jan 25
TM_NYT	T-Mobile Reaches $500 Million Settlement in Huge 2021 Data Breach	Michael Corkery	22. Juli 2022	https://www.nytimes.com/2022/07/22/business/t-mobile-hacking-	04. Jan 25
TM_KoS_2	T-Mobile: Breach Exposed SSN/DOB of 40M+ People – Krebs on Security	Brian Krebs	18. August 2021	https://krebsonsecurity.com/2021/08/t-mobile-breach-exposed-ssn-dob-of-40m-people/	04. Jan 25
TM_TV	T-Mobile data breach exposed the personal info of more than 47 million people - The Verge	Richard Lawler	18. August 2021	https://www.theverge.com/2021/8/18/22630446/t-mobile-47-million-data-breach-ssn-pin-pii	04. Jan 25
TM_TM	T-Mobile Shares Updated Information Regarding Ongoing Investigation into Cyberattack - T-Mobile Newsroom	T-Mobile	17. August 2021	https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation	04. Jan 25
SV11	**LastPass**				
LP_LP_1	03-01-2023: Security Incident Update and Recommended Actions	Karim Toubba	1. März 2023	https://blog.lastpass.com/posts/security-incident-update-recommended-actions	04. Jan 25
LP_LP_2	Incident 2 – Additional details of the attack	LastPass	1. März 2023	https://support.lastpass.com/s/document-item?language=en_US&bundleId=lastpass&topicId=LastPass/incident-2-	04. Jan 25
LP_KoS	Experts Fear Crooks are Cracking Keys Stolen in LastPass Breach – Krebs on Security	Brian Krebs	5. September	https://krebsonsecurity.com/2023/09/experts-fear-crooks-are-cracking-keys-stolen-in-lastpass-breach/	04. Jan 25
LP_TV	Attackers stole LastPass data by hacking an employee's home computer	Jess Weatherbed	28. Februar 2023	https://www.theverge.com/2023/2/28/23618353/lastpass-security-breach-disclosure-password-vault-encryption-update	04. Jan 25
LP_Ars	LastPass says employee's home computer was hacked and corporate vault taken	Dan Goodin	28. Februar 2023	https://arstechnica.com/information-technology/2023/02/lastpass-hackers-infected-employees-home-computer-and-stole-corporate-vault/	04. Jan 25
LP_CSA	The LastPass Breach is a Wake Up Call | CSA	Ofir Shaty and Ofir Balassiano	7. Juli 2023	https://cloudsecurityalliance.org/blog/2023/07/07/the-lastpass-breach-is-a-wake-up-call-for-cloud-data-security	04. Jan 25
SV12	**Uber**				
UB_UB	Security update | Uber Newsroom	Uber Team	19. September	https://www.uber.com/newsroom/security-update/	04. Jan 25
UB_IS	The Uber Breach: Ways to Prevent Similar Attacks | CSA	InsiderSecurity	23. März 2023	https://cloudsecurityalliance.org/blog/2023/03/23/insights-from-the-	04. Jan 25
UB_DR	Lapsus$ Targeted External Contractor With MFA Bombing Attack	Jai Vijayan	19. September 2022	https://www.darkreading.com/cyberattacks-data-breaches/uber-breach-	04. Jan 25
UB_Wired	The Uber Hack's Devastation Is Just Starting to Reveal Itself	Lily Hay Newman	16. September 2022	https://www.wired.com/story/uber-hack-mfa-phishing/	04. Jan 25
UB_BC	Uber hacked, internal systems breached and vulnerability reports stolen	Lawrence Abrams	16. September 2022	https://www.bleepingcomputer.com/news/security/uber-hacked-internal-systems-breached-and-vulnerability-reports-stolen/	04. Jan 25
SV13	**MGM Resorts**				
MGM_Vox	MGM cyber attack: How a phone call may have led to the ongoing hack | Vox	Sara Morrison	6. Oktober 2023	https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware	04. Jan 25
MGM_Forbes	Inside The Ransomware Attack That Shut Down MGM Resorts	Suzanne Rowan	13. September	https://www.forbes.com/sites/suzannerowankelleher/2023/09/13/ranso	04. Jan 25
MGM_WSJ	The Audacious MGM Hack That Brought Chaos to Las Vegas - WSJ	Robert McMillan and Katherine Sayre	29. März 2024	https://www.wsj.com/tech/cybersecurity/mgm-hack-casino-hackers-group-0366c641 (Archiv-Link: https://archive.ph/MuU4s)	04. Jan 25
MGM_Heise_1	Ransomware-Verdacht: Sicherheitsvorfall bei US-Hotelkette MGM Resorts	Volker Briegleb	12. September 2023	https://www.heise.de/news/Ransomware-Verdacht-Sicherheitsvorfall-bei-US-Hotelkette-MGM-Resorts-9301726.html	04. Jan 25
MGM_Heise_3	MGM: Nach Cyberangriff auf US-Casino-Kette informiert das Unternehmen Kunden | heise online	Marie-Claire Koch	9. November 2023	https://www.heise.de/news/Nach-Cyberangriff-auf-Casino-MGM-informiert-betroffene-Kunden-9210630.html	04. Jan 25
MGM_Heise_2	Statement der ALPHV-Gruppe: So lief der MGM-Hack ab – aus Sicht der Angreifer	Dennis Schirrmacher	15. September 2023	https://www.heise.de/news/Statement-der-ALPHV-Gruppe-So-lief-der-MGM-Hack-ab-aus-Sicht-der-Angreifer-9306135.html	04. Jan 25
SV14	**Microsoft Exchange**				
MS23_THN_1	Microsoft Thwarts Chinese Cyber Attack Targeting Western European Governments	Ravie Lakshmanan	12. Juli 2023	https://thehackernews.com/2023/07/microsoft-thwarts-chinese-cyber-attack.html	04. Jan 25
MS23_THN_2	Microsoft Bug Allowed Hackers to Breach Over Two Dozen Organizations via Forged Azure AD Tokens	Ravie Lakshmanan	15. Juli 2023	https://thehackernews.com/2023/07/microsoft-bug-allowed-hackers-to-breach.html	04. Jan 25

MS23_BC	Microsoft still unsure how hackers stole MSA key in 2023 Exchange attack	Ionut Ilascu	3. April 2024	https://www.bleepingcomputer.com/news/security/microsoft-still-unsure-how-hackers-stole-msa-key-in-2023-exchange-attack/	04. Jan 25
MS23_THN_3	Outlook Hack: Microsoft Reveals How a Crash Dump Led to a Major Security Breach	Ravie Lakshmanan	7. September	https://thehackernews.com/2023/09/outlook-breach-microsoft-reveals-how.html	04. Jan 25
SV15	**Okta**				
OKT_OKT_3	Okta October 2023 Security Incident Investigation Closure | Okta Security	David Bradbury	8. Februar 2024	https://sec.okta.com/harfiles	04. Jan 25
OKT_OKT_2	October Customer Support Security Incident - Update and Recommended Actions | Okta Security	David Bradbury	29. November 2023	https://sec.okta.com/october-security-incident-recommended-actions	04. Jan 25
OKT_OKT_1	Unauthorized Access to Okta's Support Case Management System: Root Cause and Remediation | Okta Security	David Bradbury	3. November 2023	https://sec.okta.com/articles/2023/11/unauthorized-access-oktas-support-case-management-system-root-cause/	04. Jan 25
OKT_BC_2	Okta breach: 134 customers exposed in October support system hack	Sergiu Gatlan	3. November 2023	https://www.bleepingcomputer.com/news/security/okta-breach-134-customers-exposed-in-october-support-system-hack/	04. Jan 25
OKT_BC_1	Okta says its support system was breached using stolen credentials	Sergiu Gatlan	20. Oktober 2023	https://www.bleepingcomputer.com/news/security/okta-says-its-support-system-was-breached-using-stolen-credentials/	04. Jan 25
OKT_BT	BeyondTrust Discovers Breach of Okta Support Unit | BeyondTrust	Marc Maiffret	20. Oktober 2023	https://www.beyondtrust.com/blog/entry/okta-support-unit-breach	04. Jan 25
SV16	**Südwestfalen-IT**				
SIT_Golem	Ransomwarebefall bei Südwestfalen-IT: Vertraulicher Forensik-Bericht offenbart viele Versäumnisse - Golem.de	Günter Born	29. Januar 2024	https://www.golem.de/news/ransomwarebefall-bei-suedwestfalen-it-vertraulicher-forensik-bericht-offenbart-viele-versaeumnisse-2401-181636.html	04. Jan 25
SIT_SIT_4	Ein Jahr nach dem Hackerangriff: Südwestfalen-IT zieht Bilanz: SIT.NRW	Südwestfalen-IT	30. Oktober 2024	https://www.sit.nrw/detailansicht/ein-jahr-nach-dem-hackerangriff-suedwestfalen-it-zieht-bilanz	04. Jan 25
SIT_SIT_1	Aktueller Stand und weiteres Vorgehen: SIT.NRW	Südwestfalen-IT	11. Januar 2024	https://www.sit.nrw/detailansicht/aktueller-stand	04. Jan 25
SIT_SIT_3	Südwestfalen-IT: Forensik-Bericht liefert Erkenntnisse zu Ransomware-Angriff – neuer Geschäftsführer der Südwestfalen IT arbeitet Vorfall auf: SIT.NRW	Südwestfalen-IT	25. Januar 2024	https://www.sit.nrw/detailansicht/suedwestfalen-it-forensik-bericht-liefert-erkenntnisse-zu-ransomware-angriff-neuer-geschaeftsfuehrer-der-suedwestfalen-it-arbeitet-vorfall-auf	04. Jan 25
SIT_Heise_1	Erpressung in Südwestfalen: Akira kam mit geratenem Passwort ins kommunale Netz | heise online	Dr. Christopher Kunz	27. Januar 2024	https://www.heise.de/news/Suedwestfalen-IT-Angreifer-errieten-Passwort-und-kamen-ueber-bekannte-Cisco-Luecke-9610102.html	04. Jan 25
SIT_Heise_2	Stillstand in Südwestfalen | c't | heise magazine	Christian Wölbert	Februar 2024	https://www.heise.de/select/ct/2024/2/2334207160432563233 (Archiv-Link: https://archive.ph/XwPNr)	04. Jan 25
SIT_SIT_2	Abschlussbericht Security Incident	Maurice Fielenbach	19. Januar 2024	https://www.sit.nrw/fileadmin/user_upload/SIT_Incident_Response_v1.1	04. Jan 25
SV17	**Change Healthcare**				
CH_Wired	Change Healthcare Finally Admits It Paid Ransomware Hackers—and Still Faces a Patient Data Leak	Andy Greenberg	22. April 2024	https://www.wired.com/story/change-healthcare-admits-it-paid-ransomware-hackers/	04. Jan 25
CH_TC_2	How the ransomware attack at Change Healthcare went down: A timeline | TechCrunch	Zack Whittaker	18. Dezember 2024	https://techcrunch.com/2024/12/18/how-the-ransomware-attack-at-change-healthcare-went-down-a-timeline/	04. Jan 25
CH_Heise	US-Zahlungsdienstleister: Krankendaten von 100 Millionen Menschen gestohlen | heise online	Marie-Claire Koch	19. Oktober 2024	https://www.heise.de/news/Change-Healthcare-Groesstes-Datenleck-im-US-Gesundheitswesen-9998090.html	04. Jan 25
CH_TC_1	UnitedHealth says Change Healthcare hack affects over 100 million, the largest-ever US healthcare data breach | TechCrunch	Zack Whittaker	24. Oktober 2024	https://techcrunch.com/2024/10/24/unitedhealth-change-healthcare-hacked-millions-health-records-ransomware/	04. Jan 25