OOPS H1-2025

Der „hätte ich das mal früher gewusst“ Report

SECURITY INCIDENTS GERMANY

WHAT A TIME TO BE A...

CEO **CTO**

CFO

CIO

COO

....or who ever ends up footing the bill.

RIEDEL

Disclaimer

Die in diesem Whitepaper enthaltenen Informationen wurden nach bestem Wissen und Gewissen zusammengestellt und stellen die zum Zeitpunkt der Veröffentlichung verfügbaren Kenntnisse und Ressourcen dar. Der Herausgeber übernimmt jedoch keine Garantie für die Korrektheit, Vollständigkeit oder Aktualität der bereitgestellten Informationen. Es wird darauf hingewiesen, dass dieses Whitepaper keine vollumfängliche Sicherheitsberatung darstellt und nicht als Ersatz für eine professionelle, individuelle Beratung durch qualifizierte IT-Sicherheitsexperten betrachtet werden sollte.

Der Herausgeber übernimmt keine Haftung für etwaige Schäden oder Verluste, die direkt oder indirekt aus der Anwendung der in diesem Whitepaper beschriebenen Informationen oder Strategien resultieren.

RIEDEL

Die Welt hat sich verändert

Cyber-Resilienz ist einer der größten Wettbewerbsvorteile der Neuzeit

Einleitung

Die Anforderungen an die Cyber-Resilienz von Unternehmen waren noch nie so hoch wie heute. Viele Unternehmen sind in ihren oft komplexen Technologieumgebungen täglich mit Cyber-Bedrohungen konfrontiert und haben noch immer keine probaten Security-Lösungen für Unternehmensnetzwerke parat.

Im Ergebnis werden Unternehmen zunehmend gehackt und öffentlich an den Pranger gestellt. Kaum ein Tag vergeht, an dem es keine mediale Berichterstattung zu neuen Cybercrime-Vorfällen gibt. Für Unternehmen bedeutet das, sich mit einer Vielzahl von zusätzlichen Schadensfeldern auseinandersetzen zu müssen. Privatpersonen werden von Online-Anwälten zur Beteiligung an Sammelklagen aufgefordert, Börsenkurse großer Security-Unternehmen brechen um zahlreiche Prozentpunkte ein, was zu Gerichtsklagen von Aktionären führt, Mitarbeiter verlassen Unternehmen wegen bekannter Sicherheitslücken: Die Welt für Unternehmer hat sich nachweislich verändert.

Im vorliegenden Whitepaper haben wir einen Auszug der medial aufgegriffenen Sicherheitsvorfälle des ersten Halbjahres 2025 aufgelistet und eingeordnet. Wir haben uns explizit dazu entschieden, die betroffenen Unternehmen nicht direkt namentlich zu nennen. Denn das Ziel des Whitepapers ist nicht, geschädigte Unternehmen zu tadeln. Vielmehr soll das Whitepaper dabei helfen, aus Vorfällen zu lernen und Rückschlüsse für die eigene IT-Sicherheitsstrategie zu ziehen.

RIEDEL

Schadensfelder durch Sicherheitsvorfälle

Legende und Erklärung

Finanzielle Schäden (z.B. durch Lösegeldzahlungen, externe Aufwände, etc.)

Schaden durch zeitlichen Zusatzaufwand und Bindung von Ressourcen (z.B. für die interne IT-Abteilung, die Geschäftsführung etc.)

Reputationsschaden durch öffentliche Bekanntmachung oder Wahrnehmung des Angriffs bei Kunden, Partnern und anderen

Produktionsausfall durch Stilllegung von Infrastruktur (z.B. zum Schutz der Systeme gegen weitere Verbreitung von Schadsoftware)

Verlust von geistigem Eigentum: z.B. Geschäftsgeheimnisse, Patente, Produktpläne oder Forschungsergebnisse

Verlust von Kunden- und Geschäftsdaten mit rechtlichen Konsequenzen und/oder Vertrauensverlust von Kunden

Rechts- und Regulierungskosten: Rechtsstreitigkeiten, Bußgelder oder Strafen wegen Datenschutzverletzungen oder Nichteinhaltung gesetzlicher Vorschriften

Kosten für Wiederherstellung und Nachbesserung betroffener Systeme und Aufrüstung

Verlust von Marktanteilen durch Vertrauensverlust bei Kunden, die das zum Anlass nehmen, zur Konkurrenz zu wechseln

Anstieg von Versicherungsprämien und Kosten oder der Verlust von Versicherungsschutz nach einem großen Vorfall

Psychologische Belastungen und negatives Arbeitsklima, insbesondere für Mitarbeiter, die mit der Bewältigung des Vorfalls befasst sind

Rückgang des Aktienwerts, wenn der Vorfall öffentlich wird und das Vertrauen der Investoren sinkt

Strategische Unternehmensrisiken wie die Beeinträchtigung von Unternehmensfusionen, Übernahmen oder Partnerschaften

Verletzung von vertraglichen Verpflichtungen gegenüber Kunden, Lieferanten oder Partnern mit rechtlichen Konsequenzen

RIEDEL

JUNI 2025

SECURITY INCIDENTS GERMANY

RIEDEL

Hacker-Schock bei deutschem Sportmedium: Instagram-Account missbraucht!

27. Juni 2025, in Nürnberg/Bayern

BETRUG

KRYPTOWÄHRUNG

EINBRUCH

Was ist passiert?
Am 27. Juni 2025 wurde der Instagram-Account bekannten deutschen Sportmediums kurzzeitig von Cyberkriminellen übernommen. Die Angreifer veröffentlichten daraufhin arabischsprachige Beiträge, die weder auf eine deutsche Zielgruppe zugeschnitten waren noch thematisch zum Medium passten. Darunter befanden sich auch Inhalte mit betrügerischem Bezug zu Kryptowährungen.

Was hätte man besser machen können?
Der Vorfall hätte durch grundlegende Sicherheitsmaßnahmen wie eine konsequente Zwei-Faktor-Authentifizierung, regelmäßige Passwortänderungen und ein geschultes Social-Media-Team besser verhindert oder schneller eingedämmt werden können. Auch ein klarer Notfallplan zur schnellen Wiederherstellung des Accounts und zur Kommunikation mit der Community wäre hilfreich gewesen.

Anzunehmende Schadensfelder:

Quellen:
https://www.bild.de/sport/fussball/hacker-angriff-auf-kicker-sex-videos-auf-instagram-685e2dd854352c1fc4b2e495

Was lernen wir daraus:
In diesem Fall war der Betrug offensichtlich und sprachlich nicht auf die Zielgruppe abgestimmt. Doch wäre der Angriff subtiler gewesen – etwa mit täuschend echten Gewinnspielen, gefälschten News oder politischen Inhalten – hätte er erheblichen Schaden anrichten können. Gerade bei etablierten Accounts mit hoher Glaubwürdigkeit ist das Risiko besonders groß: Nicht die Reichweite allein, sondern das Vertrauen der Community macht sie zu einem lohnenden Ziel.

RIEDEL

Monitor-Hack in Bäckerei: Politische Botschaften statt Werbung

27. Juni 2025, in Wahrenholz/Niedersachsen

DEFACEMENT

SABOTAGE

EINBRUCH

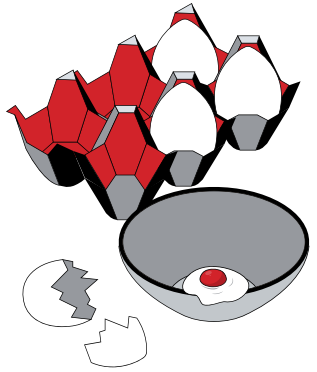
Was ist passiert?
Ende Juni 2025 kam es bei einem regionalen Bäckereiunternehmen zu einem Vorfall, bei dem unbekannte Täter politische Inhalte auf den Kundenmonitoren abspielten. Das Unternehmen entschuldigte sich öffentlich für den Vorfall und kündigte eine umfassende Untersuchung an, um die Ursache und mögliche Sicherheitslücken zu klären.

Was hätte man besser machen können?
Eine zentrale Maßnahme wäre die Härtung der Anzeigesysteme, etwa durch eingeschränkte Netzwerkzugriffe, regelmäßige Software-Updates und die Deaktivierung externer Steuerungsmöglichkeiten. Zusätzlich hätte eine Netzwerksegmentierung verhindert, dass Angreifer über andere Systeme Zugriff auf die Monitore erhalten.

Anzunehmende Schadensfelder:

Quellen:
https://www.waz-online.de/lokales/gifhorn-lk/wahrenholz-hackerangriff-auf-baeckerei-meyer-polit-botschaften-auf-monitoren-SHLLOHY4CZHPBCGH3OSDHCQ-D3A.html

Was lernen wir daraus:
Der Begriff Defacement bezeichnet in der IT-Sicherheit das Verunstalten oder Manipulieren von Webseiten oder digitalen Anzeigen, meist durch unbefugten Zugriff. Dabei ersetzen Angreifer den ursprünglichen Inhalt – etwa Texte, Bilder oder Anzeigen – durch eigene Botschaften, oft politischer, ideologischer oder provokativer Natur. Typische Ziele sind Websites, digitale Anzeigesysteme und Social-Media-Accounts.



RIEDEL

Offen wie nie: Persönliche Daten per URL abrufbar

26. Juni 2025, in Hamburg/Hamburg

SICHERHEITSLÜCKE

DATENPANNE

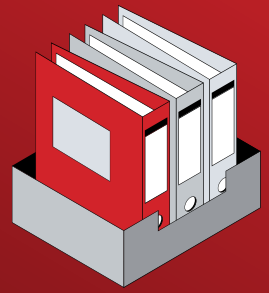
Was ist passiert?
Bei einem Anbieter von Restaurant-Websites wurden auf über 500 Seiten gravierende Sicherheitslücken entdeckt. Trotz gegenteiliger Aussagen waren persönliche Daten weiterhin über einfache URL-Manipulationen abrufbar. Das Unternehmen spricht von behobenen Schwachstellen und gelöschten Daten, während ein Mitbewerber der gezielten API-Sabotage verdächtigt wird.

Was hätte man besser machen können?
Eine abgesicherte API mit Authentifizierung, Zugriffsbeschränkungen und serverseitiger Validierung hätte unbefugte Zugriffe verhindert. Selbst manipulierte Anfragen hätten so keinen Zugang zu fremden Daten ermöglicht. Solche Maßnahmen gehören zur Basis sicherer Webentwicklung und hätten das Datenleck effektiv verhindern können.

Anzunehmende Schadensfelder:

Quellen:
https://www.heise.de//news/Nach-Datenleck-bei-Hunderten-Restaurant-Websites-Datenschuetzer-pruefen-Panne-10419767.htmlhttps://www.heise.de//news/Nach-Datenleck-bei-Hunderten-Restaurant-Websites-Datenschuetzer-pruefen-Panne-10419767.html

Was lernen wir daraus:
Der Vorfall zeigt, wie gefährlich es ist, wenn Webanwendungen keine serverseitige Zugriffskontrolle implementieren. Schon einfache URL-Manipulationen können ausreichen, um auf fremde Daten zuzugreifen – ein klassischer Fall von **IDOR (Insecure Direct Object Reference)**. Daraus lernen wir: Jeder Datenzugriff muss auf Serverseite geprüft werden, unabhängig davon, was im Browser passiert. Sicherheit darf niemals auf der Annahme beruhen, dass sich Nutzer „korrekt" verhalten – sondern muss technisch durchgesetzt werden.



RIEDEL

IT-Sicherheitsvorfall bei Elektronikunternehmen durch Ransomware-Gruppe

25. Juni 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

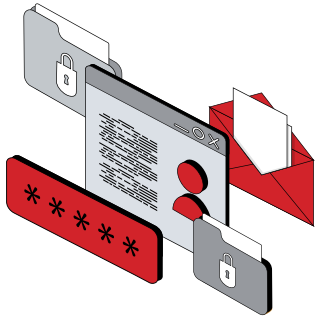
Was ist passiert?
Ein Anbieter von Elektronikbauteilen wurde von der Ransomware-Gruppe „Qilin“ als Opfer aufgelistet. Obwohl keine genauen Angaben zur erbeuteten Datenmenge gemacht wurden, veröffentlichte die Gruppe 14 Screenshots mit sensiblen Informationen als Beweis für den Angriff.

Was hätte man besser machen können?
Der Einsatz von **Multi-Faktor-Authentifizierung (MFA)** hätte den unbefugten Zugriff auf interne Systeme deutlich erschwert, selbst wenn Zugangsdaten kompromittiert wurden. Zusätzlich hätte eine konsequente **Netzwerksegmentierung** verhindert, dass sich Angreifer nach dem Eindringen ungehindert im gesamten Unternehmensnetzwerk ausbreiten können. Beide Maßnahmen zusammen hätten die Auswirkungen des Angriffs deutlich begrenzen oder sogar verhindern können.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9791-qilin.png
https://www.security-incidents.de/assets/img/incidents/9791-qilin-02.png

Was lernen wir daraus:
Die Veröffentlichung einzelner Beweise ist Teil einer psychologischen Eskalationsstrategie. Die Angreifer zeigen, dass sie Zugriff hatten, ohne gleich alles preiszugeben – das erhöht den Druck zur Zahlung. Durch vage Angaben zur Datenmenge bleibt unklar, was genau kompromittiert wurde – das erschwert dem betroffenen Unternehmen die Einschätzung des Schadens und die gezielte Reaktion – wodurch viele dazu geneigt sind, der Lösegeldforderung aus Panik nachzukommen.



RIEDEL

Ransomware-Angriff auf Oberflächentechniker: 11 GB Unternehmensdaten veröffentlicht

DATENDIEBSTAHL

RANSOMWARE

24. Juni 2025, in Nordrhein-Westfalen

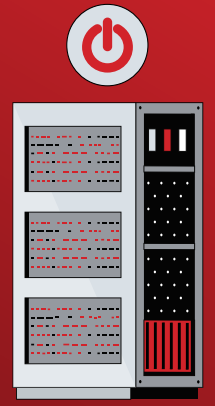
Was ist passiert?
Ein industrieller Oberflächentechniker wurde von der Ransomware-Gruppe „Akira“ auf ihrer Darknet-Leakseite gelistet. Die Angreifer entwendeten rund 11 GB an sensiblen Unternehmensdaten, darunter persönliche Informationen von Mitarbeitenden, Finanz- und Zahlungsdaten sowie projektbezogene Unterlagen.

Was hätte man besser machen können?
Ein Security Operations Center (SOC) spielt eine zentrale Rolle beim Schutz der IT-Systeme, da es die gesamte Infrastruktur rund um die Uhr überwacht, verdächtige Aktivitäten frühzeitig erkennt und schnell darauf reagiert. In diesem Fall hätte ein SOC die Datenexfiltration durch Akira frühzeitig bemerkt und reagieren können, bevor 11 GB sensibler Informationen im Darknet landen.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9772-Akira.png

Was lernen wir daraus:
Digitaler Schutz wird oft nicht ernst genug genommen, weil seine Erfolge unsichtbar sind – solange nichts passiert, wirkt es, als wäre der Aufwand übertrieben. Doch genau das ist trügerisch: Gute IT-Sicherheit verhindert Schäden, bevor sie sichtbar werden. Das macht sie schwer greifbar – bis es zu spät ist. Erst wenn ein Angriff den Betrieb lahmlegt oder Daten öffentlich auftauchen, wird klar, wie viel auf dem Spiel stand.



RIEDEL

Zurück auf Funk: Cyberangriff legt Polizei-Diensthandys lahm

23. Juni 2025, in Mecklenburg-Vorpommern

EINBRUCH
DATENDIEBSTAHL
AUSFALL
SABOTAGE

Was ist passiert?
Ein Cyberangriff auf die Landespolizei in Mecklenburg-Vorpommern legte im Juni 2025 den zentralen Server für über 3.500 Diensthandys lahm. Die Geräte wurden abgeschaltet, die Polizei musste auf Funktechnik umstellen. Laut Innenministerium sind Ermittlungsakten nicht betroffen. Die Opposition kritisiert, BSI-Warnungen seien ignoriert worden. Der Schaden wird auf 3,5 Mio. Euro geschätzt.

Was hätte man besser machen können?
Eine konsequente Umsetzung der BSI-Warnungen und frühzeitiges Patch-Management hätten bekannte Schwachstellen schließen und den Angriff womöglich verhindern können. Eine redundante Infrastruktur für kritische Systeme sowie kontinuierliches Monitoring durch ein SOC hätten zusätzlich zur Früherkennung und Aufrechterhaltung der Handlungsfähigkeit beigetragen.

Anzunehmende Schadensfelder:

Quellen:
https://www.zeit.de/news/2025-06/23/polizei-handys-seit-hackerangriff-nicht-nutzbar
https://www.ndr.de/nachrichten/mecklenburg-vorpommern/polizei-in-mv-schaltet-nach-hackerangriff-alle-diensthandys-ab,polizeifunk-102.html

Was lernen wir daraus:
Der Vorfall zeigt eindrücklich, wie angreifbar selbst sicherheitsrelevante Behörden sind, wenn bekannte Schwachstellen nicht rechtzeitig behoben werden. IT-Sicherheit scheitert oft nicht an fehlender Technik, sondern an unterlassener Umsetzung – Warnungen ernst zu nehmen und Sicherheitsupdates zeitnah einzuspielen, ist keine Kür, sondern Pflicht. Gerade im behördlichen Umfeld kann Nachlässigkeit schnell zur operativen Lähmung führen.

RIEDEL

IT-Angriff zwingt Unternehmen zur Abschaltung aller Systeme

19. Juni 2025, in Sulingen/Niedersachsen

AUSFALL

RANSOMWARE

Was ist passiert?
Ein mittelständisches Baustoffunternehmen in Norddeutschland wurde Opfer eines gezielten Ransomware-Angriffs. Die IT-Systeme wurden verschlüsselt, woraufhin alle Internetverbindungen sofort getrennt und ein Krisenstab eingerichtet wurde. Die Filialen blieben mehrere Tage geschlossen. Notlösungen sicherten den eingeschränkten Betrieb, Zahlungen waren zeitweise nur bar oder auf Rechnung möglich.

Was hätte man besser machen können?
Eine solide Vorbereitung auf Cyberangriffe hilft, Schäden zu minimieren. Ein erprobtes Notfallkonzept mit Backup-Strategien beschleunigt die Wiederherstellung. Ergänzend ermöglicht vorausschauendes Monitoring durch ein SOC mit SIEM die frühzeitige Erkennung und Eindämmung von Angriffen – idealerweise noch vor Aktivierung von Verschlüsselungsmechanismen.

Anzunehmende Schadensfelder:

Quellen:
https://www.leymann-baustoffe.de/news/
https://www.kreiszeitung.de/lokales/diepholz/sulingen-ort50128/cyberattacke-auf-sulinger-baustoffunternehmen-leymann-14-standorte-geschlossen-93792919.html

Was lernen wir daraus:
Ein Krisenstab ist ein zentrales Steuerungsteam, das bei schweren Vorfällen wie Cyberangriffen schnell zusammenkommt, um koordiniert zu handeln. Er bewertet die Lage, trifft Entscheidungen über Sofortmaßnahmen, steuert die interne und externe Kommunikation und koordiniert die Wiederherstellung des Betriebs. Nicht nur Technik, sondern auch klare Abläufe und Rollen im Krisenfall entscheiden darüber, wie gut ein Unternehmen auf einen Cybervorfall reagieren kann.

RIEDEL

IT-Störung an mehreren Bildungseinrichtungen nach Cybervorfall

AUSFALL

18. Juni 2025, in Demmin/Neustrelitz, Mecklenburg-Vorpommern

Was ist passiert?
Mehrere Schulen waren infolge eines Cyberangriffs von erheblichen technischen Ausfällen betroffen. Ursache war ein unbefugter Zugriffsversuch über das WLAN einer Schule auf das Datennetz einer Landesbehörde. Aus Sicherheitsgründen wurde der zentrale Verwaltungsserver vom Netz genommen. In der Folge fielen Geräte wie PCs, Tablets, Drucker und Telefone aus. Nach bisherigen Erkenntnissen sind keine Daten abgeflossen.

Was hätte man besser machen können?
Um solche Ausfälle zu verhindern, wäre eine strikte Netzwerksegmentierung entscheidend gewesen: Das Schul-WLAN und das Netz der Landesbehörde sollten klar getrennt und isoliert sein. Zusätzlich hätten moderne Zugriffskontrollen und starke Authentifizierung unbefugte Zugriffe blockieren können. Ein zentrales **Security-Information-and-Event-Management (SIEM)** hätte zudem ungewöhnliche Aktivitäten schneller erkannt und eine proaktive Reaktion ermöglicht.

Anzunehmende Schadensfelder:

Quellen:
https://www.ndr.de/nachrichten/mecklenburg-vorpommern/haff-mueritz/vermutlich-hackerangriff-auf-schulen-in-demmin-und-neustrelitz,mvregioneubrandenburg-112.html

Was lernen wir daraus:
Selbst ein scheinbar harmloser Zugangspunkt wie ein Schul-WLAN kann zur Schwachstelle für größere IT-Infrastrukturen werden. Gerade in vernetzten Bildungs- und Verwaltungsstrukturen braucht es klare Netzwerktrennung, durchdachte Zugriffskontrollen und ein gemeinsames Sicherheitsverständnis aller Beteiligten.

RIEDEL

52 GB sensible Daten durch Ransomware-Gruppe offengelegt

17. Juni 2025, in Bayern

DATENLECK

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Eine Projektberatungsfirma ist ins Visier der Ransomware-Gruppe „Sarcoma“ geraten. Die Angreifer gaben an, 52 GB an internen Firmendaten entwendet und veröffentlicht zu haben. Als Beleg präsentierten sie Screenshots aus den Systemen des Unternehmens auf ihrer Leaksite im Darknet.

Was hätte man besser machen können?
Das Unternehmen hätte durch eine konsequente Datenklassifizierung und den Einsatz von Verschlüsselung besonders sensibler Informationen das Risiko eines Datenlecks deutlich reduzieren können. Zudem wäre ein Security-Operations-Center (SOC) mit Echtzeit-Überwachung und SIEM-Technologie hilfreich gewesen, um ungewöhnliche Aktivitäten frühzeitig zu erkennen und den Angriff abzuwehren.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9725-sarcoma.png OOPS_H1-2025_Report ttps://www.security-incidents.de/assets/img/incidents/9725-sarcoma-02.png

Was lernen wir daraus:
Die Hackergruppe Sarcoma trat im Oktober 2024 erstmals auf und fiel durch gezielte Ransomware-Angriffe auf Unternehmen weltweit auf. Sie setzt auf doppelte Erpressung: Datenverschlüsselung und Veröffentlichung sensibler Infos. Über ihre Herkunft ist wenig bekannt, vermutet werden Verbindungen zu osteuropäischen Cybercrime-Strukturen.

RIEDEL

Vertrauliche Unternehmensdaten im Visiervon Cyberkriminellen

16. Juni 2025, in Niedersachsen

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Ein auf Roggenzucht spezialisiertes Pflanzenzuchtunternehmen wurde Opfer eines Cyberangriffs. Die Ransomware-Gruppe „Akira“ behauptet, 3GB interne Daten entwendet zu haben darunter Verträge, Finanzdokumente und Kundendaten.

Was hätte man besser machen können?
Das Unternehmen hätte durch den Einsatz von Datenverschlüsselung und strengen Zugriffskontrollen den Schutz sensibler Informationen deutlich erhöhen können. Ergänzend wäre eine kontinuierliche Überwachung der IT-Systeme mittels **Security-Information-and-Event-Management (SIEM)** sinnvoll gewesen, um ungewöhnliche Aktivitäten frühzeitig zu erkennen und zu verhindern, dass Daten unbemerkt entwendet werden.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9734-Akira-Pflanzenzucht.png

Was lernen wir daraus:
Dieser Fall verdeutlicht, dass Cyberangriffe heute nicht mehr nur große Konzerne treffen, sondern auch spezialisierte Mittelständler und Nischenunternehmen. Kein Unternehmen ist zu klein oder zu speziell, um Ziel von Ransomware und Datendiebstahl zu werden – Cyberkriminelle suchen gezielt nach jeder verwundbaren Stelle. Deshalb ist IT-Sicherheit eine Grundvoraussetzung für den langfristigen Unternehmenserfolg.

RIEDEL

E-Mail-Dienst gehackt: Millionen Nutzerdaten im Darknet

16. Juni 2025, in Deutschland

DATENLECK

SICHERHEITSLÜCKE

DATENDIEBSTAHL

Was ist passiert?
Ein datenschutzorientierter E-Mail-Dienst wurde gehackt. Eine veraltete Roundcube-Version ermöglichte den Diebstahl von über 1 Mio. Nutzerkonten inkl. E-Mail-Adressen, Login-Zeitstempeln und Systemeinstellungen. 93.000 Kontakte aus 10.400 Accounts wurden ebenfalls entwendet. Der Angreifer „Satoshi" bot die Daten für 1 Bitcoin an. Passwörter und Inhalte blieben laut Anbieter unangetastet.

Was hätte man besser machen können?
Der Angriff hätte durch konsequentes Patch-Management verhindert werden können – also durch zeitnahe Updates sicherheitsrelevanter Software wie Webmail-Clients. Auch regelmäßige Sicherheitsprüfungen (z. B. Penetrationstests) und ein Intrusion Detection System (IDS) hätten Schwachstellen erkennen und verdächtige Zugriffe frühzeitig melden können.

Anzunehmende Schadensfelder:

Quellen:
https://risky.biz/risky-bulletin-cock-li-gets-hacked-allegedly/
https://www.bleepingcomputer.com/news/security/hacker-steals-1-million-cockli-user-records-in-webmail-data-breach/

Was lernen wir daraus:
Dieser Vorfall zeigt, wie wichtig kontinuierliche Wartung und Aktualisierung von IT-Systemen sind, besonders bei Anwendungen, die direkten Nutzerzugang bieten. Selbst kleine Sicherheitslücken in oft genutzter Software können zu massiven Datenlecks führen. IT-Sicherheit endet nicht mit der Installation, sondern erfordert ständige Pflege und Kontrolle.

RIEDEL

Ransomware trifft Bildungssektor: Hackergruppe „Safepay“ listet zwei deutsche Einrichtungen

14. Juni 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

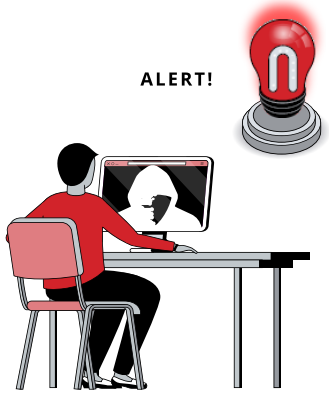
Was ist passiert?
Zwei Bildungseinrichtungen in Deutschland sind offenbar ins Visier der Ransomware-Gruppe „Safepay“ geraten. Sowohl ein gemeinnütziges Weiterbildungsinstitut als auch eine Realschule in Bayern wurden auf dem Opferblog der Gruppe im Darknet gelistet. Im Fall des Instituts behaupten die Hacker, rund 90 GB vertraulicher Daten aus Bereichen wie Geschäftsführung, IT und Buchhaltung entwendet zu haben. Bei der bayerischen Schule sind 17,3 GB sensibler Daten betroffen.

Was hätte man besser machen können?
Strikte Zugriffskontrollen mit rollenbasierten Berechtigungen und die Verschlüsselung ruhender Daten hätten das Risiko deutlich reduziert. Ein zentrales **SIEM-System** hätte verdächtige Zugriffe frühzeitig erkennen können. Auch regelmäßige Schwachstellenscans, etwa mit **REDSkull**, helfen, Sicherheitslücken rechtzeitig zu identifizieren und Angriffe zu verhindern.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9714-Safepay.png
https://www.security-incidents.de/assets/img/incidents/9713-Safepay-JohannRudolphGlauberSchule.png

Was lernen wir daraus:
Auch Bildungseinrichtungen sind längst keine Randziele mehr für Cyberkriminelle. Sie speichern große Mengen sensibler Daten – von Finanzunterlagen bis zu personenbezogenen Informationen – und verfügen oft nicht über die gleiche IT-Sicherheitsinfrastruktur wie Unternehmen. Genau das macht sie zu besonders verwundbaren Zielen. Bildung braucht deshalb nicht nur digitalen Zugang, sondern auch digitale Resilienz.



RIEDEL

Millionenschaden nach Ransomware-Attacke Produktionsbetrieb in der Insolvenz

12. Juni 2025, in Euskirchen/Nordrhein-Westfalen

EINBRUCH

AUSFALL

Was ist passiert?
Ein mittelständisches Produktionsunternehmen wurde durch einen Cyberangriff lahmgelegt. Über 200 Rechner wurden verschlüsselt, zentrale Bereiche wie Produktion und Buchhaltung waren betroffen. Die Täter forderten über ein automatisch über die Firmendrucker ausgegebenes Erpresserschreiben zur Kontaktaufnahme im Darknet auf. Der Schaden ging in die Millionen, das Unternehmen meldete Insolvenz an.

Was hätte man besser machen können?
Ein IT-Sicherheitskonzept mit Netzwerksegmentierung hätte die Ausbreitung der Schadsoftware auf über 200 Systeme verhindern können. Ein aktives Security Information and Event Management-System (SIEM) hätte verdächtige Vorgänge frühzeitig erkannt. Ergänzend hilft ein ganzheitliches Security-Assessment wie die IT-Musterung, den Sicherheitsstatus umfassend zu bewerten.

Anzunehmende Schadensfelder:

Was lernen wir daraus:
Dieser Vorfall macht deutlich, wie verheerend die Folgen eines Cyberangriffs für mittelständische Unternehmen sein können. Innerhalb kürzester Zeit wurde der gesamte Geschäftsbetrieb lahmgelegt mit massiven wirtschaftlichen Schäden bis hin zur Insolvenz.
IT-Sicherheit darf nicht als technisches Nebenprojekt verstanden werden. Sie ist ein unternehmenskritischer Bestandteil der Risikovorsorge. Wer nicht in Schutzmaßnahmen, Reaktionspläne und Wiederherstellungsstrategien investiert, riskiert im Ernstfall nicht nur Daten, sondern das gesamte Unternehmen.

RIEDEL

Quellen:
https://www1.wdr.de/nachrichten/rheinland/insolvenz-nach-cyberangriff-bonn-100.amp
https://www.ksta.de/region/euskirchen-eifel/stadt-euskirchen/euskirchen-stotzheim-fasana-stellt-nach-cyberangriff-insolvenzantrag-1042377

Stiller Alarm bei der Feuerwehr ausgelöst: Unbekannter dringt in Serverraum ein

8. Juni 2025, in Berlin/Berlin

EINBRUCH

EINBRUCHSVERSUCH

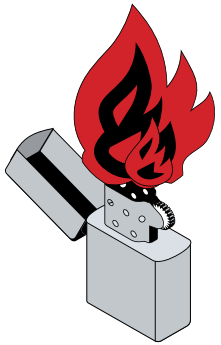
Was ist passiert?
Im Rahmen eines Vorfalls erhielt eine bislang unbekannte Person unautorisierten Zugang zum Serverraum der Berliner Feuerwehr. Dabei wurde versucht, interne Systeme zu kompromittieren und sensible Daten zu entwenden. Der digitale Einbruch löste einen stillen Alarm aus. Die Identität der verantwortlichen Person ist weiterhin ungeklärt, das Landeskriminalamt wurde eingeschaltet.

Was hätte man besser machen können?
Physische Zugangskontrollen mit biometrischen Systemen und Überwachungskameras hätten den Zutritt zum Serverraum besser abgesichert. Intelligente Alarmsysteme mit Anbindung an ein **Security Operations Center (SOC)** hätten eine schnelle Reaktion ermöglicht. Ein ganzheitliches IT-Security Assessment wie die **IT-Musterung** hilft, den eigenen Sicherheitsstatus realistisch einzuschätzen.

Anzunehmende Schadensfelder:

Quellen:
https://www.maz-online.de/berlin/it-angriff-auf-die-berliner-feuerwehr-landeskriminalamt-ermittelt-zu-moeglichem-cyberangriff-NCIZ5FNUC5GDRGWPC6UM5YARPA.html
https://www.bz-berlin.de/polizei/cyber-angriff-auf-berliner-feuerwehr

Was lernen wir daraus:
Ein oft unterschätzter Aspekt der Cybersicherheit zeigt sich in diesem Vorfall besonders deutlich: Nicht jeder Angriff beginnt online. Wer physischen Zugang zu Serverräumen erhält, kann selbst die besten digitalen Schutzmaßnahmen umgehen. Der Aha-Moment: IT-Sicherheit muss ganzheitlich gedacht werden, sie beginnt nicht erst im Netzwerk, sondern an der Tür.



RIEDEL

Gezielter Datendiebstahl bei Telefonhersteller

4. Juni 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Ein deutscher Hersteller aus dem Telekommunikationssektor ist ins Visier der Ransomware-Gruppe „INC Ransom“ geraten. Die Angreifer behaupten, 3,5 GB sensibler Daten aus internen Systemen entwendet zu haben. Die Gruppe drohte mit einer Veröffentlichung der Daten.

Was hätte man besser machen können?
Das Unternehmen hätte durch den Einsatz von Data Loss Prevention (DLP)-Systemen und einer strikten Zugriffskontrolle den unautorisierten Zugriff auf sensible Daten besser verhindern können. Ergänzend hätte ein Security-Operations-Center (SOC) mit Echtzeit-Überwachung und SIEM-Technologie dabei geholfen, verdächtige Aktivitäten frühzeitig zu erkennen und zu stoppen, bevor Daten entwendet werden konnten.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9625-inc-ransom.png

Was lernen wir daraus:
In den letzten Jahren hat sich die Cyberkriminalität stark verändert: Angriffe sind heute deutlich gezielter und professioneller. Im Fokus stehen vor allem Ransomware, Datenklau und sogenannte Doppel-Erpressungen. Kriminelle setzen zunehmend auf ausgefeilte Phishing-Methoden und nutzen auch bislang unbekannte Sicherheitslücken (Zero-Day-Exploits). Zudem wird Cybercrime immer mehr als Dienstleistung angeboten, was die Bedrohung weiter verschärft.

RIEDEL

Erpressung nach Account-Übernahme: Hacker fordert Lösegeld

4. Juni 2025, in Duisburg/Nordrhein-Westfalen

EINBRUCH

ERPRESSUNG

Was ist passiert?
Ein großer Tierschutzverein wurde Opfer eines Hackerangriffs: Der Instagram-Account mit 132.000 Followern wurde übernommen und zur Lösegeldforderung genutzt. Trotz aktivierter Zwei-Faktor-Authentifizierung und regelmäßiger Passwortwechsel vermutet die Organisation, dass ein Phishing-Angriff über ehrenamtliche Mitarbeitende erfolgt sein könnte. Spenden blieben aus, Tierrettungen wurden beeinträchtigt.

Was hätte man besser machen können?
Auch bei aktivierter Zwei-Faktor-Authentifizierung bleibt Phishing ein Risiko, besonders in Organisationen mit vielen Ehrenamtlichen. Regelmäßige Awareness-Schulungen und klare Richtlinien für den Umgang mit verdächtigen Nachrichten hätten helfen können, die Angriffsfläche zu reduzieren und den Zugriff auf den Account zu verhindern.

Was lernen wir daraus:
Technische Schutzmaßnahmen allein reichen nicht aus, wenn menschliche Faktoren unberücksichtigt bleiben. Der Vorfall zeigt, wie wichtig es ist, auch freiwillige Mitarbeitende in Sicherheitsprozesse einzubeziehen. Phishing bleibt eine der effektivsten Methoden für Angreifer, gerade bei öffentlich sichtbaren Organisationen mit großer Reichweite.

Anzunehmende Schadensfelder:

Quellen:
https://www.waz.de/lokales/duisburg/article409187135/hacker-erpresst-tierschuetzer-angst-um-hunde-in-toetungsstationen.html

RIEDEL

Digitale Infrastruktur nach Angriff lahmgelegt

3. Juni 2025, in Ostercappeln/Niedersachsen

RANSOMWARE

EINBRUCH

AUSFALL

Was ist passiert?
Am 30. Mai 2025 wurde eine Stadtverwaltung Opfer eines Ransomware-Angriffs. Der Angriff legte zentrale IT-Systeme still und brachte zahlreiche Bürgerdienste zum Erliegen. Die Kommune zahlte kein Lösegeld, sondern setzte auf Neuaufbau. Telefon und E-Mail wurden teilweise wiederhergestellt, doch viele Services blieben offline. Polizei und IT-Forensiker wurden hinzugezogen.

Was hätte man besser machen können?
Ein umfassendes Back-up- und Recovery-System mit isolierten Backups hätte die Stadtverwaltung schneller wieder einsatzfähig gemacht. Ein Security Operations Center (SOC) mit Security Information and Event Management-System (SIEM) hätte den Angriff frühzeitig erkennen können. Netzwerksegmentierung und regelmäßige Audits sind besonders im KRITIS-Bereich essenziell.

Anzunehmende Schadensfelder:

Quellen:
https://www.noz.de/lokales/ostercappeln/artikel/cyberangriff-auf-rathaus-ostercappeln-systeme-heruntergefahren-48804910
https://kommunaler-notbetrieb.de/tag/kgst-groessenklasse-7/

Was lernen wir daraus:
Stadtverwaltungen sind attraktive Ziele für Cyberangriffe, weil sie kritische Infrastrukturen und viele persönliche Daten verwalten von Bürgerdiensten bis zu sensiblen Verwaltungsinformationen. Ein erfolgreicher Angriff kann die öffentliche Versorgung lahmlegen und erheblichen Druck auf die Verantwortlichen ausüben.

RIEDEL

Verpackung mit böser Überraschung: IT-Angriff stoppt Produktion

2. Juni 2025, in Herford/Nordrhein-Westfalen

EINBRUCH

AUSFALL

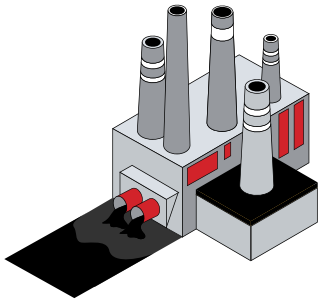
Was ist passiert?
Ein führender Verpackungsspezialist aus Herford wurde Ziel eines Cyberangriffs. Unbekannte drangen in interne Systeme ein, störten die Kommunikation und legten die Produktion zeitweise lahm. Trotz schneller Notfallmaßnahmen kam es zu erheblichen Ausfällen. Laut Unternehmen sind keine Daten abgeflossen. Die Kriminalpolizei wurde hinzugezogen.

Was hätte man besser machen können?
Das Unternehmen hätte von einem integrierten Security-Operations-Center (SOC) profitieren können, das mit einem SIEM-System ausgestattet ist, um Angriffe in Echtzeit zu erkennen und zu analysieren. So lassen sich Eindringlinge schneller identifizieren und Gegenmaßnahmen automatisieren, bevor kritische Produktionsprozesse beeinträchtigt werden. Im produzierende Gewerbe sollten regelmäßige Schwachstellentests etwaige Sicherheitslücken erkennen und beheben.

Anzunehmende Schadensfelder:

Quellen:
https://www.westfalen-blatt.de/owl/kreis-herford/herford/herforder-unternehmen-im-notbetrieb-3316980?pid=true&ueg=default
https://www1.wdr.de/nachrichten/westfalen-lippe/wellteam-cyberangriff-herford-100.html

Was lernen wir daraus:
Die Kriminalpolizei sichert bei Cyberangriffen digitale Spuren wie Logdateien und kompromittierte Systeme. Forensische Analysen helfen, Angriffsweg und Schäden zu ermitteln. Ermittler versuchen, Täter über IP-Adressen oder Darknet-Spuren zu identifizieren. Parallel arbeiten sie mit IT-Sicherheitsexperten zusammen, um den Angriff einzudämmen und weitere Schäden zu verhindern.



RIEDEL

GASTARTIKEL

Christopher Schwefel
Cyber Security Engineer

Peter Pillath
Geschäftbereichsleiter Cyber + Crime

hendricks

CYBERRISK-VERSICHERUNG: UMFASSENDER SCHUTZ VOR DEN FOLGEN VON CYBERANGRIFFEN

IT-Sicherheitsvorfälle sind längst keine Seltenheit mehr. Ob Ransomware-Angriffe, Datendiebstahl oder Systemausfälle, Unternehmen jeder Größe stehen vor der Herausforderung, sich wirksam gegen Cyberbedrohungen zu schützen. Eine Cyberversicherung bietet dabei weit mehr als finanzielle Absicherung. Sie verfolgt einen ganzheitlichen Ansatz, der Prävention, Krisenmanagement und Wiederherstellung kombiniert. Unternehmen, die sie strategisch in ihr Sicherheitskonzept integrieren, profitieren von gezielter Unterstützung bei der Risikobewertung, der Reaktion auf Vorfälle und der langfristigen Stärkung ihrer Sicherheitskultur.

Wir arbeiten bei hendricks und HOWDEN mit über 400 Partnermaklern und global mit mehr als 10.000 „Cyber-Kunden" zusammen. Durch unseren 360°-Beratungsansatz steht nicht der Versicherungsschutz, sondern die Cyber-Resilience unsere Kunden im Fokus. Risikotransfer ist immer nur ein Baustein einer Gesamtstrategie. Mit unseren Risikoingenieuren begleiten wir unsere Kunden und die Lösung Riedel Enterprise Defense [R.E.D.] ist ideal, um das Risiko eines erfolgreichen Cyberangriffs zu minimieren.

Eine wirksame Cyberstrategie beginnt mit der Identifikation und Bewertung unternehmenseigener Risiken. Häufig wird unterschätzt, welche digitalen Assets für den Geschäftsbetrieb essenziell sind. Unser Team unterstützt diesen Prozess durch Analysen wie die Business Impact Analysis (BIA), die kritische Unternehmenswerte identifiziert und entsprechende Schutzmaßnahmen priorisiert, um eine wichtige Grundlage für ein Business Continuity Management (BCM) zu schaffen.

Trotz umfassender Schutzmaßnahmen kann es zu Sicherheitsvorfällen kommen. In solchen Situationen zählt jede Minute und eine schnelle und koordinierte Incident Response ist essenziell. Kommt es zu einem Cyber-Angriff stellen wir über die Versicherung spezialisierte Forensik-Teams bereit, die unmittelbar nach einem Angriff eingreifen, Ursachen analysieren, Angriffe isolieren und weiteren Schaden verhindern. Auch beim Krisenmanagement erhalten Unternehmen Unterstützung, insbesondere bei der Kommunikation mit Behörden, Kunden und Medien, um Reputationsverluste zu minimieren. Ebenso entscheidend ist die schnelle Wiederherstellung betroffener Systeme. Der Versicherer und unsere Spezialisten koordinieren hierfür IT-Dienstleister, die Daten rekonstruieren und beschädigte Infrastrukturen reparieren.

Weiterhin können Cyberangriffe erhebliche finanzielle Schäden verursachen. Eine Cyberversicherung deckt typischerweise Kosten wie Umsatzausfälle durch Betriebsunterbrechungen sowie die Wiederherstellung von IT-Systemen ab. In bestimmten Fällen werden auch Lösegeldzahlungen bei Ransomware-Angriffen übernommen, oftmals begleitet von juristischer und strategischer Beratung, um das Risiko erneuter Angriffe zu minimieren. Neben finanziellen Folgen spielen rechtliche Konsequenzen eine große Rolle.

Ein weiterer wichtiger Bestandteil im Rahmen der Cyberrisikostrategie ist die Sensibilisierung der Belegschaft. Menschliches Fehlverhalten zählt zu den häufigsten Einfallstoren für Cyberangriffe. Zusammen mit Versicherern und Dienstleistern bieten wir daher Awareness-Trainings an, in denen Mitarbeitende lernen, Phishing-Angriffe zu erkennen und sicher mit IT-Systemen umzugehen. Ergänzend können Unternehmen simulierte Cyberangriffe durchführen lassen, um ihre Reaktionsfähigkeit zu testen und Schwachstellen in ihrer Sicherheitsstrategie zu identifizieren.

Zusammengefasst lässt sich sagen, dass eine Cyberversicherung weit mehr als eine finanzielle Absicherung ist, unser Team und der Versicherer sind strategische Partner für ein ganzheitliches IT-Risikomanagement. Unternehmen, die ihre Versicherung nicht nur als passive Deckung, sondern als integralen Bestandteil ihrer Cyber-Resilienz betrachten, profitieren langfristig von einem stabileren und widerstandsfähigeren Sicherheitskonzept. Die Kombination aus präventiven Maßnahmen, schneller Incident Response und rechtlicher Unterstützung hilft nicht nur, finanzielle Risiken zu minimieren, sondern stärkt auch nachhaltig die Sicherheitskultur eines Unternehmens.

„Unsere Erfahrung zeigt, dass viele Unternehmen noch immer auf der Suche nach dem richtigen Partner im Bereich Cyber-Security sind. Mit Riedel und R.E.D. können wir eine umfassende Lösung empfehlen, die das Risiko eines erfolgreichen Cyberangriffs mindert und die wichtigsten Tools aus einer Hand bietet. Um es deutlich zu sagen – Prävention ist günstiger, als Nachsorge. Insbesonders natürlich, wenn das Unternehmen noch keine Cyberversicherung abgeschlossen hat.", so Peter Pillath.

RIEDEL

MAI 2025

SECURITY INCIDENTS GERMANY

RIEDEL

Sensible Login- und Authentifizierungsdaten eines führenden Automobilkonzerns geleakt

31. Mai 2025, in Wolfsburg/Niedersachsen

DATENDIEBSTAHL

RANSOMWARE

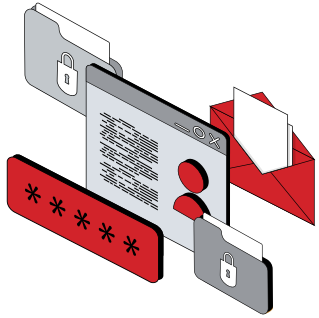
Was ist passiert?
Am 31. Mai 2025 listete die Ransomware-Gruppe „Stormous“ die Online-Umgebung eines deutschen Automobilkonzerns als Opfer. Unter den erbeuteten Daten befinden sich Account-Daten, Authentifizierungs-Tokens, Login-Links interner Systeme, Session-Cookies sowie weitere Informationen zur Authentifizierung und Identifizierung. Später stellten die Angreifer die gestohlenen Daten zum Download bereit.

Was hätte man besser machen können?
Die kontinuierliche Überwachung durch ein **Security Operations Center (SOC)** in Kombination mit einem Zero-Trust-Ansatz und einem **SIEM-System** zur Echtzeiterkennung verdächtiger Aktivitäten, hätte geholfen,, den Vorfall frühzeitig zu erkennen und den Datenabfluss zu verhindern.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9580-stormous-volkswagen-group-02.png
https://www.security-incidents.de/assets/img/incidents/9580-stormous-volkswagen-group.png

Was lernen wir daraus:
Der Vorfall zeigt, wie kritisch der Schutz von Authentifizierungsdaten ist. Unternehmen sollten ihre Sicherheitsarchitektur regelmäßig überprüfen, den Zugriff streng nach dem Need-to-Know-Prinzip regeln und verdächtige Aktivitäten kontinuierlich überwachen. Sicherheit muss als laufender Prozess verstanden werden – nicht als einmalige Maßnahme.



RIEDEL

140 GB Daten einer Fahrzeugteile-Fabrik im Darknet veröffentlicht

30. Mai 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

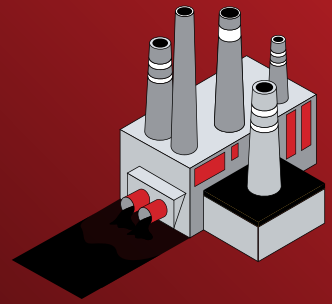
Was ist passiert?
Eine Fahrzeugteile-Fabrik wurden von Ransomware-Gruppe „Safepay“ auf ihrer Darknet-Leakseite aufgeführt. Die Hacker stellten 140 GB Daten aus den Firmensystemen zum Download bereit.

Was hätte man besser machen können?
Ein Security Operations Center (SOC) mit 24/7-Überwachung hätte erste Anzeichen wie ungewöhnliche Datenbewegungen oder verdächtige Zugriffe frühzeitig erkennen können. Als Managed Service ist es auch für kleine und mittlere Unternehmen mit hohem geistigem Eigentum eine effektive Schutzmaßnahme gegen IT-Gefahren. So wäre eine schnelle Reaktion möglich gewesen, um den Abfluss großer Datenmengen zu verhindern oder zumindest stark einzuschränken.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9581-safepay.png

Was lernen wir daraus:
Eine zuverlässige Erkennung von Angriffen setzt voraus, dass sicherheitsrelevante Vorgänge im Unternehmen rund um die Uhr überwacht werden. Ohne ein zentrales Monitoring-System bleiben kritische Aktivitäten oft unbemerkt – bis es zu spät ist. Der Einsatz eines SOC kann hier helfen, Risiken frühzeitig zu identifizieren und gezielt zu reagieren.



RIEDEL

Datenflut im Darknet: Glasfaserunternehmen im Visier

30. Mai 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Am 30. Mai 2025 listete die Ransomware-Gruppe „Safepay“ ein deutsches Unternehmen für die Messung und Einrichtung von Glasfaserleitungen als Opfer auf ihrer Darknet-Seite. Die Hacker veröffentlichten 408 GB Daten zum Download.

Was hätte man besser machen können?
Eine ausführliche Schwachstellenanalyse, bzw. ein vollumfänglicher IT-Security Audit, hätte mögliche Eintrittspforten in die Systeme möglicherweise erkannt und präventiv geschlossen. Zudem hätte ein frühzeitiges Erkennen durch ein Security Operations Center (SOC) die Veröffentlichung der Daten möglicherweise verhindern können.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9582-safepay.png

Was lernen wir daraus:
Cyberkriminelle setzen zunehmend auf großvolumige Datenleaks, um Druck auf Unternehmen auszuüben. Die Veröffentlichung ganzer Datenarchive zeigt, wie wichtig es ist, nicht nur den Zugriff zu schützen, sondern auch die Daten selbst – durch Verschlüsselung, Zugriffskontrollen und ein durchdachtes Berechtigungskonzept.

RIEDEL

Cyberangriff:
150 GB sensible Daten geleakt

29. Mai 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

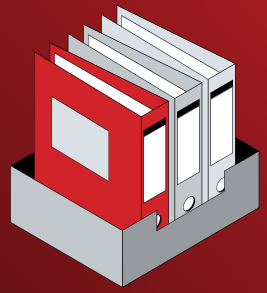
Was ist passiert?
Ein Betreiber von Zeiterfassungssoftware wurde von der Ransomware-Gruppe „Safepay“ als Opfer auf ihrer Darknet-Leakseite gelistet. Die Hacker veröffentlichten 150 GB an Daten aus den Firmensystemen als .zip-Datei.

Was hätte man besser machen können?
Ein strukturierter Incident-Response-Plan und eine kontinuierliche Überwachung der IT-Systeme hätten dazu beitragen können, den Angriff frühzeitig zu erkennen. Auch eine klare Trennung sensibler Datenbereiche im Netzwerk sowie regelmäßige Sicherheitsaudits wären hilfreich gewesen, um die Auswirkungen zu begrenzen.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9576-safepay.png

Was lernen wir daraus:
Cyberangriffe sind heute hochgradig professionell organisiert. Gruppen wie „Safepay“ agieren gezielt, nutzen moderne Angriffstechniken und setzen auf doppelte Erpressung. Unternehmen müssen sich darauf einstellen, dass Cybercrime längst ein Geschäftsmodell ist – mit spezialisierten Tools, Dienstleistungen und klarer Strategie.



RIEDEL

Cyberangriff auf Sanitätshaus in Würzburg – Daten veröffentlicht

29. Mai 2025, in Würzburg/Bayern

DATENDIEBSTAHL

RANSOMWARE

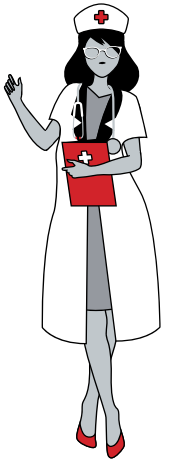
Was ist passiert?
Ein Sanitätshaus aus Würzburg wurde von der Ransomware-Gruppe „Safepay“ auf ihrer Darknet-Leakseite veröffentlicht. Kurz darauf standen die 30 GB Daten zum Download zur Verfügung.

Was hätte man besser machen können?
Eine kontinuierliche Netzwerküberwachung durch ein **Security Operations Center (SOC)** hätte verdächtige Aktivitäten frühzeitig erkannt. Ergänzend wären regelmäßige **Schwachstellenanalysen** und ein grundlegendes Sicherheitskonzept mit Zugriffskontrollen und Backups sinnvoll gewesen, um die Ausbreitung der Ransomware zu verhindern.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9578-safepay.png

Was lernen wir daraus:
Angreifer versuchen oft unbemerkt in Netzwerke einzudringen – etwa durch Phishing, gestohlene Zugangsdaten oder versteckte Malware. Ziel ist es, sensible Informationen zu sammeln und weiterzugeben. Der Vorfall zeigt, wie wichtig es ist, Sicherheitslücken frühzeitig zu erkennen und Mitarbeitende für solche Methoden zu sensibilisieren.



RIEDEL

Kundendaten bei deutschem Sportartikelhersteller kompromittiert

23. Mai 2025, in Herzogenaurach/Bayern

DATENDIEBSTAHL

SUPPLY CHAIN

Was ist passiert?
Ein großer deutscher Sportartikelhersteller meldete einen Cyberangriff auf einen seiner Dienstleister im Kundensupport. Dabei wurden Kundendaten abgegriffen, jedoch keine Passwörter oder Zahlungsinformationen. Das Unternehmen betonte, dass sensible Daten geschützt geblieben seien.

Was hätte man besser machen können?
Auch bei ausgelagerten Prozessen ist ein hohes Sicherheitsniveau entscheidend. Eine kontinuierliche Überwachung und Bewertung von Drittanbietern – etwa durch regelmäßige IT-Musterungen – hätte potenzielle Schwachstellen im Vorfeld aufdecken können. Zudem wäre eine Integration des Dienstleisters in ein zentrales SIEM-System sinnvoll gewesen, um sicherheitsrelevante Ereignisse frühzeitig zu erkennen.

Anzunehmende Schadensfelder:

Quellen:
https://www.adidas-group.com/en/data-security-information
https://www.heise.de//news/Datenleck-Kriminelle-erbeuten-Adidas-Kundendaten-10399077.html

Was lernen wir daraus:
Ein SIEM-System (Security Information and Event Management) sammelt und analysiert sicherheitsrelevante Daten aus verschiedenen IT-Systemen, um Bedrohungen frühzeitig zu erkennen. Es korreliert Ereignisse, erkennt Anomalien und löst bei verdächtigen Aktivitäten automatisch Alarme aus.

RIEDEL

IT-Angriff auf Hotelgruppe: Telefon- und Kassensysteme betroffen

23. Mai 2025, in Rostock/Mecklenburg-Vorpommern

EINBRUCH

AUSFALL

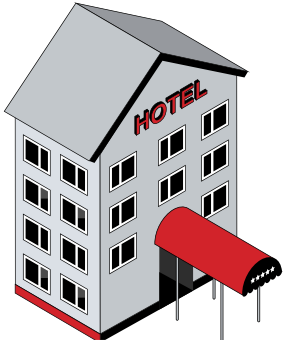
Was ist passiert?
Am 23. Mai 2025 wurden eine deutsche Hotelgruppe Ziel einer Cyberattacke, die an mehreren Standorten zu IT-Ausfällen führte. Die Hotels auf Rügen und in Weimar wurden dabei zwischenzeitlich von der zentralen IT getrennt. In der Zentrale in Rostock waren außerdem die Telefon- und Kassensysteme betroffen.

Was hätte man besser machen können?
Die IT-Ausfälle an mehreren Hotelstandorten zeigen, wie wichtig eine ganzheitliche Sicherheitsarchitektur ist. Eine Lösung wie **Extended Detection and Response (XDR)** hätte sicherheitsrelevante Ereignisse über verschiedene Systeme hinweg korreliert und frühzeitig Hinweise auf den Angriff geliefert. Ergänzend hätte eine strukturierte **IT-Musterung** helfen können, veraltete oder falsch konfigurierte Systeme zu identifizieren, bevor sie zum Einfallstor werden.

Anzunehmende Schadensfelder:

Quellen:
https://arcona.de/de/hinweis
https://www.ndr.de/nachrichten/mecklenburg-vorpommern/rostock/Cyberangriff-auf-Rostocker-Arcona-Hotels-Resorts-Gruppe-,mvregiorostock3536.html

Was lernen wir daraus:
Verteilte IT-Strukturen, wie sie in der Hotellerie üblich sind, erfordern besondere Aufmerksamkeit in der Sicherheitsarchitektur. Der Vorfall macht deutlich, dass zentrale Systeme wie Kassen oder Kommunikation besonders geschützt werden müssen – nicht nur technisch, sondern auch organisatorisch. Wer hier nicht vorbereitet ist, riskiert operative Ausfälle und langfristige Imageschäden.



RIEDEL

600 Diensthandys offline – IT-Angriff trifft Kreisverwaltung

22. Mai 2025, in Bodenseekreis/Baden-Württemberg

AUSFALL

RANSOMWARE

Was ist passiert?
Cyberkriminelle haben ein Programm zur Systemverwaltung von Systemhandys des Landratsamtes vom Bodenseekreis attackiert. Die Cyberkriminellen hatten gezielt die Systemverwaltungssoftware attackiert. Als Reaktion wurden umgehend Notfallmaßnahmen eingeleitet und sämtliche rund 600 Mobilgeräte der Kreisverwaltung vorsorglich vom Datennetz getrennt.

Was hätte man besser machen können?
Ein gezieltes Vulnerability Assessment hätte Schwachstellen in der eingesetzten Verwaltungssoftware frühzeitig aufdecken können. Auch eine sicher konfigurierte Verwaltung der Mobilgeräte mit klaren Zugriffsregeln und regelmäßigen Prüfungen hätte die Angriffsfläche deutlich reduziert und die Reaktionszeit im Ernstfall verkürzt.

Anzunehmende Schadensfelder:

Quellen:
https://www.bodenseekreis.de/aktuelles/artikel/2025/05/landratsamt-reagiert-mit-sofortmassnahmen-auf-it-uebergriff/

Was lernen wir daraus:
Auch mobile Infrastrukturen und deren Verwaltungslösungen müssen in die Sicherheitsstrategie eingebunden sein. Der Vorfall zeigt, dass technische Angriffsflächen nicht nur in klassischen IT-Systemen liegen, sondern auch in spezialisierten Anwendungen, die oft im Hintergrund laufen.

RIEDEL

Ransomware-Gruppe legt Daten deutscher Unternehmen offen

21. Mai 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

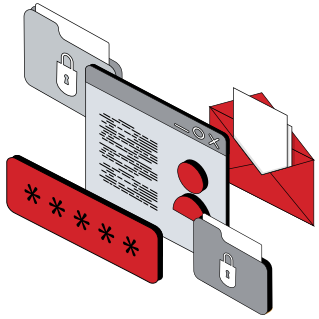
Was ist passiert?
Die Ransomware-Gruppe „Safepay“ veröffentlichte innerhalb kurzer Zeit vier deutsche Unternehmen auf ihrer Leak-Seite. Betroffen waren ein Beratungsunternehmen (123 GB), eine Wirtschaftsprüferei (452 GB), ein Container-Terminal (60 GB) und ein Notar (40,3 GB). Die Angriffe trafen unterschiedliche Branchen – die gestohlenen Daten wurden jeweils im Darknet veröffentlicht.

Was hätte man besser machen können?
Eine zentrale Sicherheitsüberwachung, etwa durch ein **Security Operations Center (SOC)**, hätte verdächtige Aktivitäten frühzeitig sichtbar machen können. Auch regelmäßige Sicherheitsaudits, klare Zugriffsrichtlinien und getestete Backups wären wichtige Bausteine gewesen, um die Angriffe zu erkennen, einzudämmen oder schneller darauf zu reagieren.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9522-safepay.png
https://www.security-incidents.de/assets/img/incidents/9521-safepay.png
https://www.security-incidents.de/assets/img/incidents/9523-safepay.png
https://www.security-incidents.de/assets/img/incidents/9524-safepay.png

Was lernen wir daraus:
Die Vorfälle zeigen, dass Ransomware-Angriffe nicht nur gezielt, sondern auch breit gestreut erfolgen können. Unternehmen jeder Größe und Branche müssen damit rechnen, ins Visier zu geraten. Wer keine zentrale Sicherheitsüberwachung etabliert und grundlegende Schutzmaßnahmen vernachlässigt, läuft Gefahr, Angriffe zu spät zu erkennen und empfindliche Daten zu verlieren.



RIEDEL

Dreifachschlag durch INC Ransom: Koordinierte Angriffe auf deutsche Unternehmen

16. Mai 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Am 16. Mai 2025 veröffentlichte die Ransomware-Gruppe „INC Ransom“ drei deutsche Unternehmen auf ihrer Leak-Seite: Ein Rollenhersteller verlor 450 GB Daten, eine Würzburger Steuerberatung 400 GB und eine Dresdner Immobilienagentur 20 GB. Die betroffenen Branchen waren unterschiedlich – ein Hinweis darauf, dass die Gruppe gezielt Schwachstellen ausnutzt, unabhängig von Größe oder Sektor.

Was hätte man besser machen können?
Eine 24/7-Überwachung durch ein Security Operations Center (SOC) hätte ungewöhnliche Aktivitäten frühzeitig erkennen und stoppen können. Durch kontinuierliche Analyse und vorausschauende Bedrohungserkennung wäre der Angriff womöglich abgewehrt worden, bevor vertrauliche Daten gefährdet waren. Ergänzend wären regelmäßige Sicherheitsaudits, Netzwerksegmentierung und ein getesteter Notfallplan zur Wiederherstellung essenziell gewesen.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9494-inc-ransom.png
https://www.security-incidents.de/assets/img/incidents/9493-inc-ransom.png
https://www.security-incidents.de/assets/img/incidents/9492-inc-ransom.png

Was lernen wir daraus:
Die koordinierte Veröffentlichung mehrerer Opfer an einem Tag deutet auf eine systematische Kampagne hin. Unternehmen müssen sich bewusst sein, dass Angreifer nicht nur gezielt, sondern auch breitflächig vorgehen. Wer keine vorausschauenden Sicherheitsmaßnahmen trifft, riskiert nicht nur Datenverlust, sondern auch massive Reputations- und Folgeschäden.

RIEDEL

Cyberangriff lässt nicht nur Milch sauer werden

16. Mai 2025, in Uphal/Mecklenburg-Vorpommern

EINBRUCH

AUSFALL

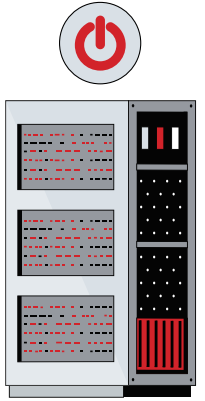
Was ist passiert?
Dänischer Lebensmittelriese bestätigte, dass sein deutscher Produktionsstandort zum Ziel eines Cyberangriffs wurde, wodurch die Produktionsabläufe beeinträchtigt wurden. Das Unternehmen rechnet nun damit, dass es durch den Angriff zu Verzögerungen oder sogar Stornierungen bei der Produktlieferung kommen werde.

Was hätte man besser machen können?
Um Angriffe auf Produktionsanlagen wirksam zu verhindern, empfiehlt sich für Unternehmen eine Orientierung an der Norm IEC 62443. Sie bietet einen ganzheitlichen und strukturierten Ansatz zur Absicherung industrieller Steuerungssysteme – unter anderem durch Netzwerksegmentierung, rollenbasierte Zugriffskontrollen und abgesicherte Fernzugriffe. Eine konsequente Umsetzung hätte potenzielle Schwachstellen in der OT-Infrastruktur reduzieren können.

Anzunehmende Schadensfelder:

Quellen:
https://www.just-food.com/news/arla-factory-in-germany-hit-by-cyber-incident/

Was lernen wir daraus:
IEC 62443 ist ein internationaler Sicherheitsstandard für industrielle Systeme, der klare Anforderungen an Technik, Prozesse und Verantwortlichkeiten stellt. Ziel ist es, Produktions- und Steuerungsanlagen vor Cyberbedrohungen zu schützen – durch abgestufte Sicherheitsmaßnahmen entlang der gesamten Liefer- und Betriebskette.



RIEDEL

Safepay leakt Daten von Abrissfirma, Malerbetrieb, Steuerberatung & Modehaus

11. Mai 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Die Ransomware-Gruppe ‚Safepay' listete vier deutsche Unternehmen auf ihrer Darknet-Seite. Von einer Abrissfirma und einem Malerbetrieb wurden je 15 GB Daten gestohlen, bei einer Steuerberatung 43 GB und bei einem bayerischen Bekleidungsgeschäft 30 GB. In allen Fällen stellten die Täter die Daten anschließend im Darknet zum Download bereit.

Was hätte man besser machen können?
Regelmäßige Sicherheitsaudits hätten den Angriff möglicherweise verhindert oder zumindest eingedämmt. Ergänzend wären verschlüsselte Backups und ein klar definierter Notfallplan zur schnellen Wiederherstellung der Systeme entscheidend gewesen, um Ausfallzeiten zu minimieren und die Datenveröffentlichung zu verhindern. Auch KMUs stehen im Visier von Cyberkriminellen und müssen an ihrer Cybersecurity-Awareness arbeiten.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9432-safepay.png
https://www.security-incidents.de/assets/img/incidents/9431-safepay.png
https://www.security-incidents.de/assets/img/incidents/9430-safepay.png
https://www.security-incidents.de/assets/img/incidents/9429-safepay.png

Was lernen wir daraus:
Cyberangriffe sind heute gezielter und professioneller – mit Fokus auf Ransomware, Datenexfiltration und Veröffentlichung im Darknet. Auch kleinere Unternehmen sind betroffen. Der Fall zeigt, wie wichtig es ist, Daten zu verschlüsseln, Zugriffe zu begrenzen und Sicherheitslücken frühzeitig zu erkennen, bevor Angreifer sie ausnutzen.

RIEDEL

Digitale Störung bei KiTa-Betreiber: Nur Telefonkontakt möglich

11. Mai 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

AUSFALL

Was ist passiert?
Seit dem 11. Mai 2025 listet die Ransomware-Gruppe „Safepay“ ein deutsches Kinderzentrum, das KiTas und Beratungsstellen betreibt, als Opfer. Das Zentrum ist aufgrund des Angriffs nur telefonisch erreichbar.

Was hätte man besser machen können?
Einrichtungen mit sensiblen Daten sollten auf ein mehrstufiges Sicherheitskonzept setzen. Dazu gehört unter anderem die Überwachung von Endgeräten, um verdächtige Aktivitäten frühzeitig zu erkennen. Lösungen wie **Endpoint Detection and Response (EDR)** helfen dabei, Angriffe direkt zu erkennen und zu intervenieren, bevor sie sich im Netzwerk ausbreiten können.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9433-safepay-02.png
https://www.security-incidents.de/assets/img/incidents/9433-safepay.png

Was lernen wir daraus:
Der Vorfall zeigt, warum die NIS-2-Richtlinie auch für soziale Einrichtungen relevant ist. Sie verpflichtet künftig zu stärkeren Sicherheitsmaßnahmen. Wären diese bereits umfassend umgesetzt worden, hätte der Angriff möglicherweise verhindert oder zumindest abgeschwächt werden können.

RIEDEL

Cyberangriff auf Apothekerverband: Angreifer verschlüsselten Daten

9. Mai 2025, in Offenbach/Hessen

EINBRUCH

SICHERHEITSLÜCKE

Was ist passiert?
Ein Apothekerverband wurde Opfer eines Cyberangriffs. Die Täter nutzten eine Netzwerkschwachstelle zur Verschlüsselung kritischer Systeme. Zwei Partnerorganisationen waren ebenfalls betroffen. IT-Spezialisten isolierten die Systeme und arbeiteten an der Wiederherstellung. Ein IT-Forensik-Team untersuchte den Vorfall, während der Verband gemeinsam mit dem LKA Anzeige erstattete.

Was hätte man besser machen können?
Die Ausnutzung einer Netzwerkschwachstelle hätte durch ein kontinuierliches Vulnerability Assessment frühzeitig erkannt und behoben werden können. Ergänzend hätte eine automatisierte Reaktion über Security Orchestration, Automation and Response (SOAR) dazu beigetragen, die Ausbreitung der Schadsoftware schneller einzudämmen.

Anzunehmende Schadensfelder:

Quellen:
https://www.pharmazeutische-zeitung.de/cyber-angriff-auf-hessischen-apothekerverband-155834/
https://www.apotheke-adhoc.de/nachrichten/detail/panorama/schwerer-cyber-angriff-auf-hessischen-apothekerverband/

Was lernen wir daraus:
Cyberangriffe auf zentrale Verbände können auch Partnerorganisationen in Mitleidenschaft ziehen. Das zeigt, wie wichtig es ist, Sicherheitsmaßnahmen nicht isoliert zu betrachten. Eine koordinierte IT-Sicherheitsstrategie mit regelmäßigen Schwachstellenanalysen, klaren Wiederanlaufplänen und abgestimmter Kommunikation ist entscheidend, um Schäden zu begrenzen und Vertrauen zu erhalten.

RIEDEL

17.000 Daten mit persönlichen Daten entwendet

8. Mai 2025, in Bremen

DATENDIEBSTAHL

RANSOMWARE

ERPRESSUNG

Was ist passiert?
Am 8. Mai 2025 listete die Ransomware-Gruppe „Everest“ einen in Bremen ansässigen Industriedienstleister als Opfer. Sie erbeuteten rund 17.000 Dateieinträge mit persönlichen Daten von Mitarbeitenden.

Was lernen wir daraus:
Personaldaten zählen zu den besonders schützenswerten Informationen. Der Vorfall zeigt, wie wichtig es ist, sensible Daten nicht nur technisch abzusichern, sondern auch organisatorisch zu schützen – etwa durch Zugriffsbeschränkungen, Verschlüsselung und klare Verantwortlichkeiten im Datenumgang.

Was hätte man besser machen können?
Ein gezieltes Berechtigungsmanagement, sowie die Verschlüsselung personenbezogener Daten, hätten das Risiko eines Datenabflusses deutlich reduziert. Ergänzend wären regelmäßige **Schwachstellenanalysen** und ein Frühwarnsystem zur Erkennung verdächtiger Aktivitäten sinnvoll gewesen, um den Angriff rechtzeitig zu stoppen.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9398-everest.png

RIEDEL

IT-Zwischenfall in Stadtverwaltung: Stadt reagiert schnell auf Sicherheitsvorfall

AUSFALL

4. Mai 2025, in Ellwangen/Baden-Württemberg

Was ist passiert?
Eine Stadtverwaltung stellte verdächtige IT-Aktivitäten fest. Ein Krisenteam aus BSI-zertifizierten Fachkräften und einer Cybersicherheitsagentur reagierte sofort und schaltete betroffene Systeme ab. Anzeige wurde erstattet und der Landesdatenschutzbeauftragte informiert. Die Kernverwaltung blieb erreichbar, digitale Schuldienstleistungen waren jedoch vorübergehend eingeschränkt.

Was hätte man besser machen können?
Auch bei schneller Reaktion ist ein strukturierter Incident-Response-Plan wichtig, um im Ernstfall koordiniert und effizient zu handeln. Zusätzlich hätte eine stärkere Segmentierung der IT-Infrastruktur dazu beitragen können, die Auswirkungen auf einzelne Bereiche wie die Schuldienste zu begrenzen.

Anzunehmende Schadensfelder:

Quellen:
https://www.ellwangen.de/buerger/stadt-ellwangen/stadt-ellwangen/ellwangen-aktuell/2880/cyberangriff-auf-die-stadtverwaltung
https://www.schwaebische-post.de/ostalb/ellwangen/stadt-ellwangen/hackerangriff-auf-ellwangen-stadtverwaltung-betroffen-93713478.html

Was lernen wir daraus:
Auch Kommunalverwaltungen sind zunehmend Ziel von Cyberangriffen. Der Fall zeigt, wie wichtig es ist, nicht nur auf den Ernstfall vorbereitet zu sein, sondern auch präventiv zu handeln – etwa durch kontinuierliche Überwachung, regelmäßige Schwachstellenanalysen und klare Kommunikationsstrukturen im Krisenfall.

RIEDEL

1,8 Terabyte Beute: Hackergruppe Lynx erpresst deutsches Unternehmen

2. Mai 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

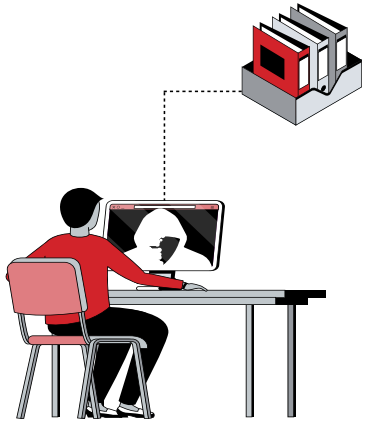
Was ist passiert?
Am 2. Mai 2025 gab die Ransomware-Gang „Lynx“ auf ihrem Darknet-Blog an, ein deutsches Fertigungsunternehmen gehackt zu haben. Die Angreifer haben dabei 1,8 Terabyte Daten entwendet.

Was hätte man besser machen können?
Der Angriff hätte durch den Einsatz eines **Managed-SIEM** und eines rund um die Uhr besetzten **Security Operations Centers (SOC)** früher erkannt und in seinem Ausmaß begrenzt werden können. Auch die Überwachung von Dedicated Leak Sites (DLS) hätte dem Unternehmen ermöglicht, schneller auf die Veröffentlichung der 1,8 Terabyte gestohlenen Daten zu reagieren und gezielte Gegenmaßnahmen einzuleiten.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9356-lynx.png

Was lernen wir daraus:
Dedicated Leak Sites (DLS) sind spezielle Webseiten im Darknet, auf denen Ransomware-Gruppen gestohlene Unternehmensdaten veröffentlichen. Sie dienen als Druckmittel zur Erpressung und als Marktplatz für sensible Informationen. Die frühzeitige Überwachung solcher Seiten kann helfen, Datenleaks schneller zu erkennen und gezielt zu reagieren, bevor vertrauliche Inhalte vollständig veröffentlicht werden.



RIEDEL

Cyberattacke auf Ärztekammer: Hacker nutzen Sicherheitslücke bei Hosting-Anbieter

2. Mai 2025, in Dresden/Sachsen

EINBRUCH

SICHERHEITSLÜCKE

RANSOMWARE

AUSFALL

Was ist passiert?
Am 2. Mai 2025 legte ein Ransomware-Angriff die Website einer Landesärztekammer lahm. Die Täter nutzten eine Schwachstelle beim externen Hosting-Dienst, sensible Daten waren jedoch nicht betroffen. Webserver und CMS wurden vorsorglich abgeschaltet, IT-Experten untersuchen den Vorfall. Mitarbeitende erhielten Hinweise zum sicheren Umgang mit E-Mail-Anhängen. Die Systeme werden schrittweise wieder hochgefahren.

Was hätte man besser machen können?
Ein Security Operations Center (SOC) überwacht die gesamte IT-Infrastruktur rund um die Uhr, erkennt verdächtige Aktivitäten frühzeitig und ermöglicht eine schnelle Reaktion auf Angriffe. Ergänzend helfen regelmäßige Schwachstellenanalysen dabei, Sicherheitslücken rechtzeitig zu identifizieren und zu schließen, bevor sie von Angreifern ausgenutzt werden können.

Anzunehmende Schadensfelder:

Quellen:
https://www.slaek.de/de/ueber-uns/presse/presse-mitteilungen/2025/cyberangriff.php

Was lernen wir daraus:
Organisationen im Gesundheitswesen tragen besondere Verantwortung für den Schutz sensibler Informationen. Der Vorfall zeigt, dass nicht nur interne Systeme, sondern auch externe Dienstleister Teil der Sicherheitsstrategie sein müssen. Ein SOC und regelmäßige Schwachstellenanalysen sind essenziell, um Angriffe frühzeitig zu erkennen und die Integrität medizinischer Daten zu wahren.

RIEDEL

Stadtverwaltung nach DDoS-Attacke lahmgelegt

1. Mai 2025, in Stuttgart/Baden-Württemberg

DDoS

AUSFALL

Was ist passiert?
Am 1.Mai wurde eine Stadtverwaltung in BaWü zum Ziel eines Cyberangriffs. Durch eine sogenannte DDoS-Attacke brachten die Angreifer die städtische Webseite vorübergehend zum Erliegen.

Was lernen wir daraus:
Der Vorfall zeigt deutlich, wie wichtig eine vorausschauende IT-Sicherheitsstrategie für öffentliche Einrichtungen ist. Insbesondere bei DDoS-Angriffen kommt es darauf an, nicht nur auf den Ernstfall zu reagieren, sondern sich proaktiv darauf vorzubereiten.

Was hätte man besser machen können?
Um die Widerstandsfähigkeit gegenüber DDoS-Angriffen zu erhöhen, hätten spezifische Schutzmaßnahmen wie die Filterung des Datenverkehrs, eine intelligente Lastverteilung sowie der Aufbau redundanter Systeme implementiert werden können. Zusätzlich wäre ein vordefinierter Notfallplan hilfreich gewesen, um im Ernstfall schneller reagieren und die öffentliche Verfügbarkeit der Website zügiger wiederherstellen zu können.

Anzunehmende Schadensfelder:

Quellen:
https://www.zvw.de/stuttgart-region/im-visier-von-kriminellen-cyber-angriff-auf-website-der-stadt-stuttgart_arid-950140

RIEDEL

APRIL 2025

SECURITY INCIDENTS GERMANY

RIEDEL

Logistikunternehmen im Visier von Datenerpressern

29. April 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

Was ist passiert?
Die Ransomware-Gruppe „PLAY“ hat ein deutsches Logistikunternehmen angegriffen und erklärt, umfangreiche sensible Daten gestohlen zu haben. Betroffen seien unter anderem Kundenunterlagen, Ausweiskopien und Finanzdokumente. Ab dem 02.05.2025 kündigten die Täter die Veröffentlichung der gestohlenen Daten auf ihrer Leak-Seite an.

Was hätte man besser machen können?
Durch ein Data-Loss-Prevention-(DLP)-System hätten ungewöhnliche Datenbewegungen erkannt und blockiert werden können. Auch die Implementierung von Multi-Faktor-Authentifizierung und regelmäßigen Sicherheitsüberprüfungen hätte den Schutz der sensiblen Daten deutlich erhöht.

Anzunehmende Schadensfelder:

Quellen:
http://mbrlkbtq5jonaqkurjwmxftytyn2ethqvbxfu4rgjbkkknndqwae6byd.onion/topic.php?id=SjXt9qsGv9YPZl
https://www.security-incidents.de/assets/img/incidents/9297-play.png

Was lernen wir daraus:
Ransomware-Gruppen veröffentlichen gestohlene Daten gezielt im Darknet, weil es ihnen Anonymität und Schutz vor Strafverfolgung bietet. Im Gegensatz zum regulären Internet sind Darknet-Seiten schwer auffindbar und kaum sperrbar – so bleibt der Druck auf die Opfer dauerhaft hoch, während die Täter ungestört agieren können.

RIEDEL

Cyberattacke auf städtische Dienste legte Webportal lahm

29. April 2025, in Dresden/Sachsen

DDoS

AUSFALL

Was ist passiert?
Zwischen dem 25. und 30.04.2025 beeinträchtigten DDoS-Angriffe den Onlineauftritt einer Stadtverwaltung. Wichtige Dienste wie Online-Terminvergabe waren nicht zuverlässig erreichbar. Die Verwaltung meldete am 29.04. eine erfolgreiche Abwehr. Eine prorussische Hackergruppe wird verdächtigt, auch andere Städte attackiert zu haben. Seit dem 28.04. lief der Betrieb wieder normal.

Was hätte man besser machen können?
DDoS-Angriffe hätten besser abgewehrt werden können, etwa durch spezialisierte Schutzsysteme, die schädlichen Datenverkehr automatisch erkennen und filtern. Eine skalierbare Cloud-Infrastruktur hätte Überlastungen durch dynamische Verteilung verhindert. Zusätzlich ermöglicht Echtzeit-Monitoring mit Anomalieerkennung eine frühzeitige Warnung, damit Gegenmaßnahmen schneller greifen.

Anzunehmende Schadensfelder:

Quellen:
https://www.radiodresden.de/beitrag/cyber-attacke-auf-dresden-was-bislang-bekannt-ist-864825/
https://www.dnn.de/lokales/dresden/dresden-cyberattacke-legt-stadtwebseite-lahm-KI-Y42U7Q4VCZ7IPTZMFQ25XHD4.html

Was lernen wir daraus:
Auch Bildungseinrichtungen sind längst keine Randziele mehr für Cyberkriminelle. Sie speichern große Mengen sensibler Daten – von Finanzunterlagen bis zu personenbezogenen Informationen – und verfügen oft nicht über die gleiche IT-Sicherheitsinfrastruktur wie Unternehmen. Genau das macht sie zu besonders verwundbaren Zielen. Bildung braucht deshalb nicht nur digitalen Zugang, sondern auch digitale Resilienz.

RIEDEL

Soziale Organisation von Hackerangriff betroffen

RANSOMWARE

ERPRESSUNG

29. April 2025, in Gießen/Hessen

Was ist passiert?
Am 27.04.2025 wurde eine soziale Einrichtung in Gießen Ziel eines Ransomware-Angriffs. Die Angreifer verschlüsselten Daten und forderten ein Lösegeld, das jedoch nicht gezahlt wurde. Dank Backups konnte ein IT-Notbetrieb starten. Der reguläre Betrieb lief analog weiter. Ob personenbezogene Daten betroffen waren, blieb unklar. Ermittlungen und IT-Analysen liefen an.

Was hätte man besser machen können?
Obwohl Backups den IT-Notbetrieb ermöglichten, zeigt der Vorfall, dass sie allein nicht ausreichen. Verhaltensbasierte Endpoint-Security hätte die Schadsoftware früher erkennen und stoppen können. Eine stärkere Netzwerksegmentierung hätte zudem die Ausbreitung begrenzt und den Schaden weiter reduziert.

Anzunehmende Schadensfelder:

Quellen:
https://www.it-daily.net/shortnews/awo-wird-mit-ransomware-erpresst
https://www.giessener-allgemeine.de/giessen/erpressen-die-awo-hacker-93712402.html
https://www.security-incidents.de/assets/img/incidents/9355-arbeiterwohlfahrt-giessen.png

Was lernen wir daraus:
Selbst wenn ein Lösegeld nicht gezahlt wird, kann ein Ransomware-Angriff den Betrieb massiv stören – vor allem, wenn unklar bleibt, ob sensible Daten kompromittiert wurden. Der Fall zeigt, wie wichtig es ist, nicht nur auf Prävention zu setzen, sondern auch gut vorbereitete Notfallpläne und schnelle Wiederherstellungsmechanismen zu haben. Besonders entscheidend ist, dass Backups regelmäßig geprüft und schnell verfügbar sind, um einen IT-Notbetrieb nahtlos zu ermöglichen und den regulären Betrieb aufrechtzuerhalten.

RIEDEL

Verwaltungsdienste nach Überlastungsangriff offline

28. April 2025, in Berlin/Berlin

DDoS

AUSFALL

SABOTAGE

Was ist passiert?
Die IT-Systeme einer Verwaltung wurden durch einen DDoS-Angriff gestört. Unbekannte überfluteten mehrere Verwaltungsportale mit Anfragen, sodass zentrale Dienste wie Terminbuchungen und Polizeimitteilungen waren bis zum 28. April nicht erreichbar. Laut Behörden wurden keine Daten entwendet. Es handelte sich um eine reine Überlastungsattacke.

Was hätte man besser machen können?
Um die Auswirkungen des DDoS-Angriffs zu minimieren, hätte man spezialisierte DDoS-Schutzlösungen einsetzen können, etwa vorgelagerte Filterdienste oder Cloud-basierte Traffic-Scrubbing-Systeme, die schädliche Anfragen automatisch aussortieren. Zusätzlich hätte eine skalierbare Infrastruktur mit Lastverteilung dafür gesorgt, dass zentrale Dienste wie Terminbuchungen trotz hoher Auslastung funktionsfähig bleiben.

Anzunehmende Schadensfelder:

Was lernen wir daraus:
DDoS-Attacken auf Verwaltungen werden oft durchgeführt, um öffentliche Strukturen gezielt zu stören oder zu diskreditieren – aus politischem Protest, ideologischer Motivation oder reiner Provokation. Für Cyberkriminelle ist es zudem ein einfacher Weg, Aufmerksamkeit zu erzeugen oder Handlungsdruck aufzubauen, ohne in Systeme eindringen zu müssen. In manchen Fällen sind DDoS-Angriffe auch Ablenkungsmanöver für schwerwiegendere Angriffe im Hintergrund.

RIEDEL

Quellen:
https://www.welt.de/regionales/berlin/article256027086/Cyberattacke-trifft-das-Hauptstadtportal-berlin-de.html
https://www.rbb24.de/politik/beitrag/2025/04/cyber-angriff-berlin-de-hauptstadt-portal-land-hacker.html

Ausfall nach Hackerangriff bei deutschem Logistiker

25. April 2025, in Solingen/Nordrhein-Westfalen

EINBRUCH

AUSFALL

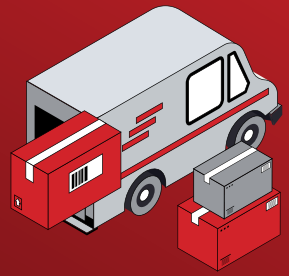
Was ist passiert?
Eine deutsche Spedition war infolge eines Cyberangriffs von IT-Störungen betroffen. Der Transportbetrieb lief weiter, doch E-Mail-Systeme und die Online-Auftragserfassung blieben außer Betrieb. Kundenanfragen wurden über Mobilnummern abgewickelt. Laut Unternehmen gingen keine E-Mails verloren. Der Angriff war durch verdächtige Netzwerkaktivitäten entdeckt worden.

Was hätte man besser machen können?
Der Vorfall hätte besser abgewehrt werden können, wenn verdächtige Netzwerkaktivitäten automatisiert durch ein Security Operations Center (SOC) erkannt und sofort eingegrenzt worden wären. Zusätzlich hätte eine isolierte, redundante Kommunikationsinfrastruktur – etwa ein abgesicherter Backup-Maildienst oder Ausweichplattformen – geholfen, die E-Mail-Ausfälle zu überbrücken und den Kundenkontakt ohne Umwege aufrechtzuerhalten.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9260-MitteilungIDCScreenshot.png

Was lernen wir daraus:
Wenn zentrale Kommunikationswege wie E-Mail plötzlich ausfallen, wirkt das nach außen schnell wie ein kompletter Stillstand – selbst wenn der Betrieb intern weiterläuft. Ohne erreichbaren Kundenservice steigt die Gefahr, dass Kunden abspringen und zur Konkurrenz wechseln. Der Vorfall macht deutlich: Ausfallsicherheit in der Kommunikation ist kein Nice-to-have, sondern geschäftskritisch.



RIEDEL

Betriebsstörung bei Logistikdienstleister durch Cyberangriff

25. April 2025, in Villingen-Schwenningen/Baden-Württemberg

DATENDIEBSTAHL

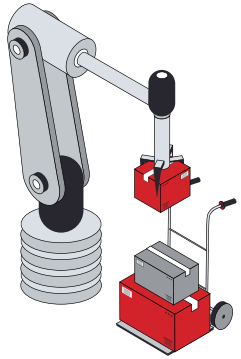
AUSFALL

EINBRUCH

Was ist passiert?
Ein Cyberangriff auf das deutsche Tochterunternehmen eines Schweizer Logistikdienstleisters störte den Betrieb erheblich. Rund 1.600 Geschäftskunden konnten Lager- und Transportdienste nur eingeschränkt nutzen. Die Angreifer erbeuteten Daten von 2020 bis 2025, möglicherweise auch sensible Personendaten. In Deutschland griffen Notfallpläne, die Systeme des Mutterkonzerns blieben unbeeinträchtigt.

Was hätte man besser machen können?
Durch eine **24/7-Überwachung** der IT-Systeme hätte die Bedrohung in Echtzeit erkannt und mit sofortigen Gegenmaßnahmen darauf reagiert werden können. Eine regelmäßige **Schwachstellenanalyse** und ein Cybersecurity-Audit helfen dabei, mögliche Angriffsvektoren zu erkennen und sich gezielt zu schützen.

Was lernen wir daraus:
Wenn IT-Systeme nicht frühzeitig Alarm schlagen und gezielt abschotten, wird aus einem gezielten Angriff schnell eine flächendeckende Betriebsstörung – mit teuren Folgen. Das unterstreicht die Bedeutung von aktiver Bedrohungserkennung und intelligenter Netzwerkarchitektur.



Anzunehmende Schadensfelder:

Quellen:
https://www.nau.ch/news/schweiz/post-kampft-gegen-cyberangriff-in-deutschland-66975755
https://www.post.ch/de/ueber-uns/medien/medienmitteilungen/2025/die-schweizerische-post-geht-gegen-cyberangriff-in-deutschland-vor

RIEDEL

DDoS-Attacke beeinträchtigt interaktive Webdienste

25. April 2025, in Nürnberg/Bayern

DDoS

AUSFALL

Was ist passiert?
Die Website einer Verwaltung war infolge eines DDoS-Angriffs zeitweise nicht erreichbar. Besonders interaktive Online-Dienste wie Suchfunktionen und Kontaktformulare waren betroffen. Die IT-Abteilung war nicht betroffen. Die Cybercrime-Einheit der Polizei wurde eingeschaltet und hat Ermittlungen zur Herkunft des Angriffs aufgenommen.

Was hätte man besser machen können?
Der DDoS-Angriff hätte besser abgewehrt werden können, etwa durch spezialisierte Schutzlösungen, die schädlichen Datenverkehr filtern und gezielte Überlastungen verhindern. Eine skalierbare Infrastruktur hätte bei hohem Traffic automatisch Ressourcen bereitgestellt. Kontinuierliche Überwachung und schnelle Alarmierung hätten eine proaktive Reaktion ermöglicht.

Anzunehmende Schadensfelder:

Quellen:
https://www.nuernberg.de/internet/stadtportal/aktuell_94259.html
https://www.br.de/nachrichten/bayern/massive-cyber-attacke-auf-webseite-der-stadt-nuernberg,UjO8PSX

Was lernen wir daraus:
Eine **DDoS-Attacke (Distributed Denial of Service)** ist ein Angriff, bei dem eine Website oder ein Online-Dienst mit einer extrem hohen Menge an Datenverkehr überflutet wird – oft von vielen verschiedenen Computern gleichzeitig. Dadurch wird die Website überlastet und für echte Nutzer nicht mehr erreichbar. DDoS-Attacken werden meist durchgeführt, um Dienste lahmzulegen, etwa aus politischen Gründen, zur Erpressung, um Wettbewerber zu stören oder einfach, um Schaden anzurichten und Aufmerksamkeit zu erregen. Ziel ist also nicht der Diebstahl von Daten, sondern die gezielte Störung der Verfügbarkeit.

RIEDEL

Vergleichsportal erleidet Datenverluste nach Cyberangriff

24. April 2025, in Hamburg/Hamburg

RANSOMWARE

AUSFALL

Was ist passiert?
Ein deutsches Vergleichsportal wurde Ziel eines Ransomware-Angriffs. Die Angreifer verschlüsselten und entwendeten mutmaßlich Daten, bevor das IT-Team die Systeme vom Netz trennte. Es kam zu Datenverlusten sowie spürbaren Einschränkungen bei Website-Inhalten und Kommunikation. Das Unternehmen arbeitete mit Hochdruck an der Störungsbeseitigung, das genaue Ausmaß blieb zunächst unklar.

Was hätte man besser machen können?
Durch eine kontinuierliche Überwachung und schnelle Alarmierung durch ein **SOC**, hätte der Angriff frühzeitiger gestoppt werden können. Eine schnelle Netzwerksegmentierung und automatisierte Isolierung betroffener Systeme hätte die Lage zusätzlich entschärft. Zudem wären regelmäßige, offline gespeicherte Backups essenziell gewesen, um Datenverluste zu minimieren und eine schnelle Wiederherstellung zu ermöglichen.

Anzunehmende Schadensfelder:

Quellen:
https://www.golem.de/news/preisvergleich-hacker-attackieren-guenstiger-de-mit-ransomware-2504-195611.html
https://www.heise.de//news/Ransomware-Angriff-bei-Preisvergleichsportal-guenstiger-de-10359486.html

Was lernen wir daraus:
Selbst gut vorbereitete IT-Teams stoßen bei plötzlichen Angriffen schnell an ihre Grenzen, wenn zentrale Prozesse nicht ausreichend abgesichert sind. Externe SOC-Lösungen unterstützen hier besonders effektiv, da sie rund um die Uhr überwachen, frühzeitig Warnungen geben und mit klarem, objektivem Blick reagieren – genau das, was in Stresssituationen oft fehlt. So helfen sie, Ausfallzeiten zu minimieren und die Reaktionsfähigkeit zu erhöhen.

RIEDEL

Traditionsunternehmen Ziel von Cyberkriminellen

24. April 2025, in Oettingen/Bayern

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

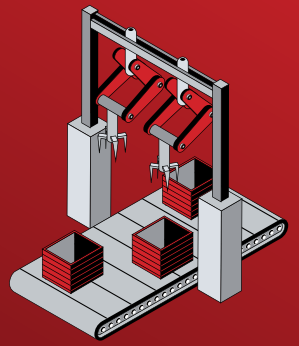
Was ist passiert?
Ein traditionsreicher Getränkehersteller wurde Opfer eines Cyberangriffs. Die Produktion lief an allen Standorten störungsfrei weiter, während IT-Spezialisten mögliche Datenlecks prüften. Die Gruppe „RansomHouse“ bekannte sich zur Tat und veröffentlichte Beweisdaten. Die Angreifer forderten das Unternehmen zur Kontaktaufnahme auf, um eine Datenveröffentlichung zu verhindern. Es wurden umgehend Sicherheitsmaßnahmen eingeleitet.

Was hätte man besser machen können?
Der Angriff hätte besser eingedämmt werden können, wenn eine strikte Netzwerksegmentierung implementiert gewesen wäre, die den Zugriff auf sensible Daten auf ein Minimum beschränkt. Zudem hätte eine kontinuierliche Überwachung der IT-Systeme durch ein SOC ungewöhnliche Aktivitäten frühzeitig erkennen und einen schnellen Eingriff ermöglichen können.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9269-Ransomhouse-Oettinger.png
https://www.tag24.de/nachrichten/wirtschaft/unternehmen/oettinger-im-visier-von-hackern-cyberangriff-auf-traditionsbrauerei-3380219

Was lernen wir daraus:
Dieser Fall zeigt, dass selbst wenn die Produktion technisch störungsfrei weiterläuft, ein Cyberangriff im Hintergrund unbemerkt sensible Daten gefährden kann. Das zeigt, wie wichtig es ist, nicht nur auf die Verfügbarkeit der Systeme zu achten, sondern auch auf umfassenden Datenschutz und kontinuierliche Überwachung. Nur so lassen sich versteckte Risiken frühzeitig erkennen und größerer Schaden verhindern.



RIEDEL

Cybervorfall legt Großhandelsbetrieb zeitweise lahm

21. April 2025, in Tettnang/Baden-Württemberg

EINBRUCH

AUSFALL

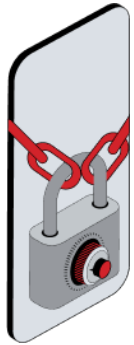
Was ist passiert?
Ein Großhändler wurde Opfer eines Cyberangriffs, bei dem interne IT-Systeme verschlüsselt wurden. Der Betrieb war stark eingeschränkt: Filialen schlossen, Auslieferungen pausierten, E-Mails fielen aus. Der Onlineshop lief weiter, jedoch mit eingeschränkter Preisanzeige. Seit dem 22. April laufen zentrale Prozesse wieder. Forensik und Datenschutzprüfungen dauern an.

Was hätte man besser machen können?
Der Vorfall hätte durch Netzwerksegmentierung, aktuelle Sicherheitspatches und einen Notfall-IT-Plan besser abgefedert werden können. Der Ausfall kritischer Prozesse zeigt die Bedeutung redundanter, getrennter Systeme. Regelmäßige, getestete Backups und eine klare Incident-Response-Strategie hätten die Ausfallzeit deutlich reduziert.

Anzunehmende Schadensfelder:

Quellen:
https://shop.layer-grosshandel.de/systemausfall2025.html
https://www.suedkurier.de/region/bodenseekreis/bodenseekreis/cyberangriff-auf-werkzeughaendler-layer-in-tettnang-worauf-kunden-jetzt-achten-sollen;art410936,12369153

Was lernen wir daraus:
Ein längerer IT-Ausfall durch einen Cyberangriff kann für Unternehmen schnell zum Existenzrisiko werden. Eingeschränkte Geschäftsabläufe führen zu Umsatzeinbußen und stockendem Cashflow, während Kosten weiterlaufen. Ohne schnelle Wiederherstellung und finanzielle Reserven steigt die Gefahr von Zahlungsschwierigkeiten bis hin zur Insolvenz. Deshalb ist eine solide IT-Sicherheit und Notfallplanung unerlässlich, um solche wirtschaftlichen Folgen zu verhindern.



RIEDEL

RALord schlägt zu: Kabelhersteller im Visier von Cyberkriminellen

19. April 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Ein deutscher Kabelhersteller wurde von der Ransomware-Gruppe „RALord“, auch bekannt als „Nova“, auf deren Darknet-Blog als Opfer aufgeführt. Die Angreifer gaben an, 30 GB vertraulicher Daten entwendet zu haben – darunter Dokumente, Datenbank-Backups, Kunden- und Bankinformationen. Als Beweis stellten sie mehrere Screenshots online.

Was hätte man besser machen können?
Der Vorfall hätte besser abgewehrt werden können, wenn verdächtige Netzwerkaktivitäten automatisiert durch ein Security Operations Center (SOC) erkannt und sofort eingegrenzt worden wären. Insbesondere als Managed Service, wie bei RIEDEL Enterprise Defense [R.E.D.], ist es möglich, direkte Maßnahmen zu ergreifen, um den Schaden zu begrenzen. Auch ein Schwachstellenscan hätte vorab mögliche Eintrittspforten detektieren können.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9229-ralord.png
https://www.security-incidents.de/assets/img/incidents/9229-ralord-02.png

Was lernen wir daraus:
Backups schützen nur dann, wenn sie selbst sicher gespeichert sind. Der Diebstahl von Datenbank-Backups zeigt, dass nicht nur Live-Systeme, sondern auch Sicherungskopien gezielt angegriffen werden – ein oft unterschätztes Einfallstor in der IT-Sicherheit.

RIEDEL

Ransomware-Schlag gegen Autohändler und Handwerksbetrieb

18. April 2025, in Deutschland

DATENDIEBSTAHL
RANSOMWARE
EINBRUCH

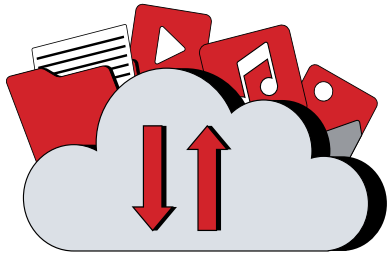
Was ist passiert?
Am 18. April 2025 wurden ein familiengeführter Autohändler und Werkstattbetrieb sowie ein Handwerksunternehmen von der Ransomware-Gruppe „Akira“ angegriffen. Die Täter behaupten, insgesamt 53 GB sensible Daten erbeutet zu haben, darunter Kundendaten, Mitarbeiterakten, Verträge, Finanzunterlagen sowie Rechnungen und Projektdaten.

Was hätte man besser machen können?
Auch für kleine und mittelständische Unternehmen ist eine klare IT-Sicherheitsstrategie essenziell. Auch wenn hier budgetär ggf. keine großen MSSPs möglich sind, kann über Angebote wie die IT-Musterung ein belastbarer Audit die Cybersicherheit (technisch und rechtlich) erfolgen, um ein individuelles Schutzkonzept zu entwickeln.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9196-Akira-Autowerkstatt.png
https://www.security-incidents.de/assets/img/incidents/9197-Akira-Handwerksunternehmen.png

Was lernen wir daraus:
Nicht die Datenmenge, sondern deren Sensibilität macht Unternehmen erpressbar. Trotz vergleichsweise geringer Datenvolumen (13–40 GB) richteten die Angriffe erheblichen Schaden an, da vertrauliche Informationen wie Kunden-, Mitarbeiter- und Finanzdaten betroffen waren. Das unterstreicht, wie wichtig der Schutz auch kleiner Datenbestände ist.



RIEDEL

Zehn deutsche Organisationen Opfer großflächiger Datenklau-Attacken

17. April 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

Was ist passiert?
Im April 2025 griff die Ransomware-Gruppe „Safepay“ mehrere deutsche Unternehmen und Kommunen an, darunter Maschinenhersteller, Bauunternehmen, Logistikfirmen sowie kommunale Verwaltungen. Insgesamt entwendeten sie dabei rund 831 GB an sensiblen Daten. In allen Fällen veröffentlichten die Täter Screenshots als Beweis und drohten mit der baldigen Veröffentlichung der gestohlenen Informationen.

Was hätte man besser machen können?
Durch regelmäßige Sicherheitsupdates, strikte Zugangsbeschränkungen und Netzwerksegmentierung hätte das Risiko der Angriffe verringert werden können. Wichtig sind zudem sichere, offline gespeicherte Backups und Mitarbeiterschulungen, um Phishing-Angriffe zu vermeiden. Ein effektives Monitoring und schnelle Reaktionspläne helfen, Schäden frühzeitig zu begrenzen.

Anzunehmende Schadensfelder:

Quellen:
https://www.dsgvo-portal.de/sicherheitsvorfall-datenbank/

Was lernen wir daraus:
Ransomware-Gruppen veröffentlichen oft alle Opfer an einem Tag, um mit einem großen Schlag Aufmerksamkeit zu erzeugen und den Druck auf die Betroffenen zu erhöhen. So wirken sie besonders bedrohlich, erschweren die Reaktion der Opfer und erhöhen die Wahrscheinlichkeit, dass Lösegeld gezahlt wird. Außerdem sparen sie Aufwand, indem sie die Veröffentlichung bündeln, statt sie einzeln zu streuen.

RIEDEL

Cyberangriff mit Beleg: Hacker legen Dateistruktur offen

15. April 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

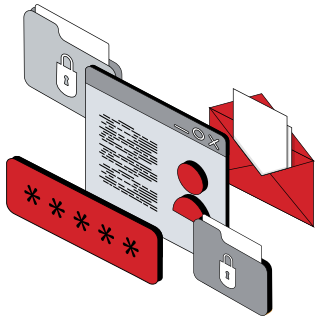
Was ist passiert?
Eine deutsche Maschinenbaufirma ist offenbar ins Visier der Hackergruppe „Lynx“ geraten. Auf ihrer Leak-Seite gab die Gruppe an, 45 GB Daten aus den Unternehmenssystemen gestohlen zu haben. Zur Untermauerung ihrer Forderung veröffentlichten die Täter Screenshots interner Dateien.

Was hätte man besser machen können?
Auch für kleine und mittelständische Unternehmen ist eine klare IT-Sicherheitsstrategie essenziell. Auch wenn hier budgetär ggf. keine großen MSSPs möglich sind, kann über Angebote wie die **IT-Musterung** ein belastbarer Audit die Cybersicherheit (technisch und rechtlich) erfolgen, um ein individuelles Schutzkonzept zu entwickeln.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9146-Lynx-Maschinenunternehmen.PNG

Was lernen wir daraus:
Nicht die Datenmenge, sondern deren Sensibilität macht Unternehmen erpressbar. Trotz vergleichsweise geringer Datenvolumen (13–40 GB) richteten die Angriffe erheblichen Schaden an, da vertrauliche Informationen wie Kunden-, Mitarbeiter- und Finanzdaten betroffen waren. Das unterstreicht, wie wichtig der Schutz auch kleiner Datenbestände ist.



RIEDEL

Betrugs-Mails über interne Konten: IT-Sicherheitsvorfall bei Wohnungsunternehmen

15. April 2025, in Pforzheim/Baden-Württemberg

PHISHING

EINBRUCH

Was ist passiert?
Cyberkriminelle verschafften sich Zugang zu zwei E-Mail-Konten eines kommunalen Wohnungsunternehmens. Über das interne Mailsystem versendeten sie anschließend eine Vielzahl betrügerischer und potenziell schadhafter Nachrichten. Die möglichen Empfänger wurden zeitnah über den Vorfall informiert.

Was hätte man besser machen können?
Um den Vorfall zu verhindern, wären Schutzmaßnahmen wie Zwei-Faktor-Authentifizierung für alle E-Mail-Konten sowie moderne Sicherheitsstandards wie DMARC, SPF und DKIM sinnvoll gewesen. Ergänzend hätte ein Security Awareness Training geholfen, Phishing frühzeitig zu erkennen und zu melden.

Anzunehmende Schadensfelder:

Quellen:
https://www.pz-news.de/pforzheim_artikel,-Achtung-vor-Mails-von-der-Pforzheimer-Stadtbau-Cyberangriff-sorgt-fuer-Sicherheitsrisiko-_arid,2205929.html

Was lernen wir daraus:
E-Mail-Konten sind nach wie vor ein beliebter und effektiver Angriffsvektor – besonders in öffentlichen Einrichtungen. Schon der Zugriff auf nur zwei Accounts kann reichen, um großflächig Schaden anzurichten. Der Vorfall zeigt, wie wichtig es ist, Mailkonten technisch abzusichern (z. B. mit 2FA) und Mitarbeitende regelmäßig für Risiken wie Phishing oder verdächtige Zugriffe zu sensibilisieren. Sicherheit beginnt beim Login.

RIEDEL

Datenklau bei deutschem Sanitärunternehmen

14. April 2025, in Biberach/Baden-Württemberg

DATENDIEBSTAHL

RANSOMWARE

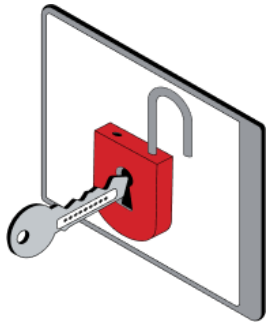
Was ist passiert?
Die Ransomware-Gruppierung „Akira“ listete ein deutsches Sanitär-Unternehmen auf ihrer Leak-Seite. Im Zuge eines vorausgegangenen Angriffs verschafften sich die Täter Zugang zu sensiblen Informationen, darunter Kontaktdaten von Mitarbeitenden und Kunden, E-Mail-Adressen, Geschäftslizenzen und Vertragsdokumente.

Was hätte man besser machen können?
Um den Angriff zu verhindern, hätte das Sanitär-Unternehmen eine mehrschichtige Sicherheitsstrategie benötigt: IAM für Zugriffskontrolle, Verschlüsselung sensibler Daten,**EDR** zur Erkennung verdächtiger Aktivitäten sowie regelmäßige Schulungen zu Phishing und Social Engineering zur Abwehr des initialen Angriffsvektors.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9121-akira-stumpf-und-mueller-biberach.png

Was lernen wir daraus:
Auch kleinere und mittelständische Unternehmen mit scheinbar niedrigem Risiko – wie ein Sanitärbetrieb – sind attraktive Ziele für Ransomware-Angriffe. Sensible Geschäftsdaten, Kundendetails und Vertragsinformationen haben für Angreifer hohen Erpressungswert. Wer glaubt, „zu klein“ für ein Ziel zu sein, unterschätzt die Lage. Grundlegende Sicherheitsmaßnahmen wie Zugriffsschutz, Datenverschlüsselung und Mitarbeiter-Sensibilisierung sind heute keine Kür mehr, sondern Pflicht.



RIEDEL

Doppelschlag durch INC Ransom: Mittelstand im Visier der Cyberkriminellen

9. April 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Zwei deutsche Unternehmen, ein Maschinenbauer aus Berlin und ein Ingenieurbüro – wurden Opfer der Ransomware-Gruppe „INC Ransom“. Beim Maschinenbauer wurden 137 GB, beim Ingenieurbüro 56 GB sensible Daten gestohlen. Letzteres wurde zudem auf der Leak-Seite der Gruppe gelistet, wo die Angreifer zunächst Screenshots als Beweis veröffentlichten und kurz darauf die vollständigen gestohlenen Daten online stellten.

Was hätte man besser machen können?
Um einen solchen Angriff zu verhindern, hätten die Unternehmen auf SIEM-Systeme zur zentralen Überwachung sicherheitsrelevanter Ereignisse und EDR-Lösungen zur frühzeitigen Erkennung und Abwehr von Bedrohungen setzen sollen. Ergänzend wären regelmäßige Schwachstellenanalysen sowie eine konsequente Verschlüsselung sensibler Daten sinnvoll gewesen, um potenzielle Einfallstore zu schließen und die Verwertbarkeit erbeuteter Informationen zu minimieren.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9052-inc-ransom-Maschinenhersteller.png
https://www.security-incidents.de/assets/img/incidents/9152-inc-ransom-ingenieurbuero-fuer-landentwicklung.png

Was lernen wir daraus:
Gezielte Ransomware-Angriffe treffen längst nicht mehr nur große Konzerne, sondern auch mittelständische Industrie- und Ingenieurbetriebe. Wer sensible Daten speichert, muss in moderne Sicherheitsmaßnahmen investieren, insbesondere in Frühwarnsysteme wie SIEM und EDR sowie in präventive Maßnahmen wie Schwachstellenmanagement und Datenverschlüsselung. Denn ein einzelner erfolgreicher Angriff kann nicht nur finanzielle, sondern auch langfristige Reputationsschäden verursachen.

RIEDEL

Metallbetrieb im Visier: Hacker stehlen sensible Daten

9. April 2025, in Keltern/Baden-Württemberg

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Die Ransomware-Gruppe „Akira“ bekannte sich zu einem Angriff auf ein deutsches Metallunternehmen. Dabei wurden 50 GB Daten gestohlen, darunter vertrauliche Dokumente wie Geheimhaltungsvereinbarungen, Kontaktinformationen von Mitarbeitenden und Kunden, Finanzdaten sowie Verträge.

Was hätte man besser machen können?
Ein **Security Operations Center (SOC)** hätte den Angriff frühzeitig erkennen und abwehren können, durch den Einsatz von **SOAR** und **XDR**, integriert in eine **SIEM-Plattform** zur Echtzeitüberwachung. Diese Kombination ermöglicht automatisierte Reaktionen, schnellere Angriffserkennung und effizientere Analyse von Sicherheitsvorfällen.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9040-akira-bauer-walser-ag.png

Was lernen wir daraus:
Der Einsatz moderner IT-Sicherheitslösungen wie
- ✓ SIEM & SOC
- ✓ XDR
- ✓ EDR
- ✓ SOAR
- ✓ SD-WAN
- ✓ SASE

ermöglicht Unternehmen, sowohl ihre sensiblen Geschäftsgeheimnisse als auch die persönlichen Daten ihrer Mitarbeiter effektiv zu schützen und unbefugten Zugriff zu verhindern.

RIEDEL

Russischer Spionageverdacht bei Forschungseinrichtung – E-Mailverkehr betroffen

9. April 2025, in Deutschland

EINBRUCH

SPIONAGE

Was ist passiert?
Eine deutsche Forschungseinrichtung wurde Ziel eines Cyberangriffs. Über längere Zeit hatten Angreifer Zugriff auf den E-Mail-Verkehr einer Arbeitsgruppe. Der Vorfall wurde durch eine verdächtige IP entdeckt. Sicherheitsbehörden ermitteln. Es besteht der Verdacht auf die russische APT-Gruppe „APT29“ („Midnight Blizzard“ / „Cozy Bear“).

Was hätte man besser machen können?
Durch den Einsatz von Zero Trust und Multi-Faktor-Authentifizierung hätte der unbefugte Zugriff auf E-Mail-Systeme deutlich erschwert werden können. Kontinuierliches Netzwerk-Monitoring sowie regelmäßige Systemaktualisierungen und Härtung hätten zusätzlich geholfen, verdächtige Zugriffe zu erkennen und die Angriffsfläche zu minimieren. Im Rahmen eines 24/7 SOC-Betriebs werden dann Unregelmäßigkeiten direkt erkannt und entsprechende Maßnahmen getroffen.

Anzunehmende Schadensfelder:

Quellen:
https://www.radiolippe.de/index.php?id=1783&L=0%252520%252520%252F%252F%253F_SERVER%25255BDOCUMENT_ROOT%25255D%25253D&tx_news_pi1%5Bnews%5D=508590&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&cHash=5fdb95aac85bbcd7113283b6f723183e

Was lernen wir daraus:
Spionageangriffe durch APT-Gruppen wie „APT29“ sind seltener als Ransomware, aber gezielter und langfristiger. Sie richten sich oft gegen Forschungsinstitute, Behörden oder kritische Infrastrukturen. Aufgrund ihrer Komplexität bleiben sie oft monatelang unentdeckt und stellen damit eine erhebliche Bedrohung für nationale Sicherheit und Wirtschaft dar.

RIEDEL

932.307 Dateien von Gabelstaplerhändler entwendet

7. April 2025, in Neckarsulm/Baden-Württemberg

DATENDIEBSTAHL

ERPRESSUNG

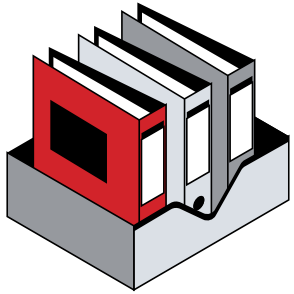
Was ist passiert?
Die Hacker-Gruppe „Hunters International“ listete auf ihrer Darknet-Seite einen deutschen Gabelstaplerhändler als Opfer. Die Gruppierung, die kürzlich von klassischen Ransomware-Angriffen auf reine Datenexfiltration und Erpressung umgestellt hatte, erbeutete rund 1,7 TB an Daten mit insgesamt 932.307 Dateien.

Was hätte man besser machen können?
Durch Data Loss Prevention (DLP) und kontinuierliches Monitoring hätte der Abfluss großer Datenmengen frühzeitig erkannt und gestoppt werden können. Eine Segmentierung der IT-Infrastruktur hätte die Ausbreitung des Angriffs erschwert. Managed Security Services wie **RIEDEL Enterprise Defense [R.E.D.]** bieten hier effektiven Schutz auch für den Mittelstand.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9024-hunters-international-hofmann-foerdertechnik-gmbh.png

Was lernen wir daraus:
Moderne Ransomware-Strategien gehen über reine Verschlüsselung hinaus: Angreifer setzen zunehmend auf Datenexfiltration, um zusätzlichen Druck auszuüben. Selbst bei Zahlungsverweigerung droht die Veröffentlichung sensibler Daten. Das führt zu Betriebsstillstand, Datenschutzverstößen, Reputationsschäden und rechtlichen Folgen.



RIEDEL

Cyberangriff führt zu Insolvenz bei deutschem Recycling-Unternehmen

7. April 2025, in Hermeskeil/Rheinland-Pfalz

DATENDIEBSTAHL
RANSOMWARE
EINBRUCH
DATENLECK

Was ist passiert?
Ein deutsches Recycling-Unternehmen wurde Opfer eines Cyberangriffs. Die Täter erbeuteten Daten von rund 200 Kunden, darunter Kontaktdaten und Bankverbindungen. Das Unternehmen informierte sofort die Behörden und änderte alle Passwörter. Wenige Wochen später folgte die Insolvenz. Später veröffentlichten die Täter ein 63-GB-Datenpaket.

Was hätte man besser machen können?
Um den Schaden zu begrenzen, hätte das Unternehmen auf eine starke Verschlüsselung sensibler Daten, rollenbasierte Zugriffskontrollen und regelmäßige Offline-Backups setzen sollen. Ergänzend hätte ein Security Operations Center (SOC) verdächtige Aktivitäten frühzeitig erkennen und Gegenmaßnahmen einleiten können, bevor es zum Datenabfluss kam.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9233-Safepay-EuRec.png
https://www.eu-rec.de/wp-content/uploads/2025/04/Schreiben-Datenschutzbehoerde-Website.pdf

Was lernen wir daraus:
Ein Cyberangriff kann nicht nur den unmittelbaren IT-Schaden verursachen, sondern durch den Verlust sensibler Kundendaten und den daraus resultierenden Vertrauensbruch eine Kettenreaktion auslösen, die letztlich zur Insolvenz führt. Die finanziellen Belastungen gehen weit über technische Wiederherstellungskosten hinaus und umfassen auch Umsatzeinbußen, rechtliche Folgen und langfristigen Imageschaden. Für Unternehmen zeigt sich hier klar, wie existenziell effektive Cyberabwehr und schnelle Reaktionsfähigkeit sind, um wirtschaftliche Katastrophen zu verhindern.

RIEDEL

Rüstungs-Gigant wird von Cyberkriminellen attackiert – 750 GB Daten gestohlen

4. April 2025, in Düsseldorf/Nordrhein-Westfalen

DATENDIEBSTAHL

RANSOMWARE

ERPRESSUNG

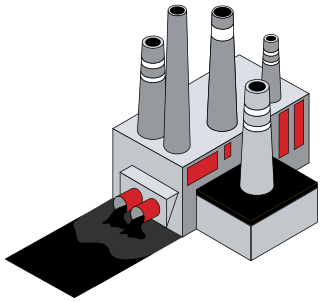
Was ist passiert?
Am 4. April 2025 listete die Ransomware-Gruppierung „Babuk“ einen deutschen Rüstungs-Giganten auf ihrer Leak-Website als Opfer. Dabei wurden rund 750 GB an Daten entwendet. Es wurden Datenproben veröffentlicht, um den Druck auf das Unternehmen zu erhöhen.

Was hätte man besser machen können?
In einem sicherheitssensiblen Umfeld wie der Rüstungsindustrie wäre ein stärkerer Fokus auf hardwarebasierte Verschlüsselung und Endpunkt-Härtung sinnvoll gewesen, um sensible Daten auch bei Zugriff durch Angreifer unlesbar zu machen. Zusätzlich hätte man durch eine **24/7 Überwachung** ungewöhnliche Datenbewegungen frühzeitig erkennen und ein Datenabfluss in diesem Maße verhindern können.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8996-babuk-rheinmetall.png
https://www.security-incidents.de/assets/img/incidents/8996-babuk-rheinmetall-02.png

Was lernen wir daraus:
Selbst hochgesicherte Unternehmen wie Rüstungskonzerne sind nicht unverwundbar. Ein erfolgreicher Angriff zeigt, dass selbst Air Gaps, Verschlüsselung und staatlich regulierte Sicherheitsvorgaben umgangen werden können – oft durch gezielte Social Engineering-Angriffe oder kompromittierte Schnittstellen. Das unterstreicht: Sicherheit endet nicht bei der Technik, sondern beginnt beim Menschen und erfordert kontinuierliche Wachsamkeit, Schulung und Anpassung an neue Angriffsvektoren.



RIEDEL

Daten von Großkunden veröffentlicht – Unternehmen bestätigt Attacke

2. April 2025, in Dresden/Sachsen

SUPPLY CHAIN

DATENDIEBSTAHL

EINBRUCH

Was ist passiert?
Der BreachForums-Nutzer „GHNA“ veröffentlichte mehrere Datensätze, die unter anderem Informationen von bekannten Unternehmen enthielten. Als Quelle der Daten nannte er einen Angriff auf ein deutsches Datenanalyseunternehmen. Die IT-Abteilung des Datenanalyseunternehmens leitete schließlich Untersuchungen ein.

Was hätte man besser machen können?
Durch eine konsequente Zugriffskontrolle, rollenbasierte Berechtigungen und die frühzeitige Erkennung verdächtiger Aktivitäten mittels Security Operations Center (SOC) hätte der Angriff deutlich eingedämmt oder sogar verhindert werden können. So wären sensible Daten besser geschützt und ein Abfluss rechtzeitig gestoppt worden.

Anzunehmende Schadensfelder:

Quellen:
https://www.bleepingcomputer.com/news/security/royal-mail-investigates-data-leak-claims-no-impact-on-operations/

Was lernen wir daraus:
Der Angriff auf das Datenanalyseunternehmen verdeutlicht, wie schnell Angreifer nicht nur firmeneigene Daten, sondern auch vertrauliche Informationen externer Kunden und Partner kompromittieren können. Das Vertrauen Dritter wird dadurch massiv gefährdet, da ihre sensiblen Daten in falsche Hände geraten und für Missbrauch oder Identitätsdiebstahl genutzt werden können.

RIEDEL

IT-Störung legt Kfz-Zulassungsstellen in Bayern lahm

AUSFALL

1. April 2025, in München/Bayern

Was ist passiert?
Bei einem bayerischen IT-Dienstleister für kommunale Verwaltungssysteme kam es zu einer technischen Störung, durch die zahlreiche Kfz-Zulassungsstellen stundenlang lahmgelegt wurden – betroffen waren u. a. die Landkreise Bamberg, Rosenheim und Passau. In bis zu 80 % der Stellen war keine An- oder Abmeldung möglich. Am 1. April 2025 war die Störung behoben, der Dienstleister leitete interne Untersuchungen ein.

Was hätte man besser machen können?
Um Ausfallzeiten bei kritischen Verwaltungsdiensten zu minimieren, hätte der IT-Dienstleister auf eine hochverfügbare Infrastruktur mit automatischem Failover und Echtzeit-Monitoring setzen können. Durch frühzeitige Erkennung technischer Störungen und gezielte Alarmierung ließen sich Probleme schneller beheben und die Betriebsfähigkeit aufrechterhalten.

Anzunehmende Schadensfelder:

Quellen:
https://www.br.de/nachrichten/bayern/bayernweit-it-probleme-bei-kommunalen-zulassungsstellen,Uh2SoQG

Was lernen wir daraus:
Der Ausfall ganzer Landkreise bei der Kfz-Zulassung zeigt klar: Fehlende **geografische Redundanz** und unzureichende **Netzwerksegmentierung** führen dazu, dass Störungen sich großflächig ausbreiten können. Um solche Ausfälle zu verhindern, müssen kritische Systeme so aufgebaut sein, dass sie bei Problemen automatisch auf alternative Standorte oder Verbindungen ausweichen können. Nur so bleibt die Verfügbarkeit wichtiger Dienste auch bei technischen Störungen gewährleistet.

RIEDEL

Marketinggesellschaft meldet Cybervorfall – Systeme nach zwei Tagen wiederhergestellt

RANSOMWARE

ERPRESSUNG

1. April 2025, in Heilbronn/Baden-Württemberg

Was ist passiert?
Eine städtische Marketinggesellschaft aus Süddeutschland wurde Opfer eines Ransomware-Angriffs. Die Angreifer verschlüsselten weite Teile der Systemumgebung und hinterließen ein Erpresserschreiben. Die technischen Teams konnten die Systeme innerhalb von zwei Tagen wiederherstellen.

Was hätte man besser machen können?
Durch regelmäßige Offline-Backups, ein getestetes Notfallwiederherstellungskonzept und den Einsatz von Endpoint Detection & Response (EDR) hätte die Marketinggesellschaft die Auswirkungen des Angriffs deutlich reduzieren können. So wären Systeme schneller wiederherstellbar gewesen und die Ausbreitung der Ransomware frühzeitig gestoppt worden.

Anzunehmende Schadensfelder:

Quellen:
https://www.swr.de/swraktuell/baden-wuerttemberg/heilbronn/cyberattacke-heilbronn-marketing-gmbh-100.html

Was lernen wir daraus:
Um Systeme nach einem Ransomware-Angriff wiederherzustellen, müssen technische Teams zuerst die Schadsoftware isolieren, alle betroffenen Systeme bereinigen und anschließend saubere Backups einspielen. Dabei prüfen sie die Integrität der Daten, setzen Zugangsdaten zurück und kontrollieren Netzwerkverbindungen. Zusätzlich wird die Infrastruktur auf Schwachstellen analysiert, um künftige Angriffe zu verhindern. Ein strukturierter Wiederherstellungsplan und gut vorbereitete Notfall-Backups sind dabei entscheidend.

RIEDEL

MÄRZ 2025

SECURITY INCIDENTS GERMANY

RIEDEL

Vertrauliche Daten in Gefahr: Ransomware-Angriff auf IT-Dienstleister

31. März 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

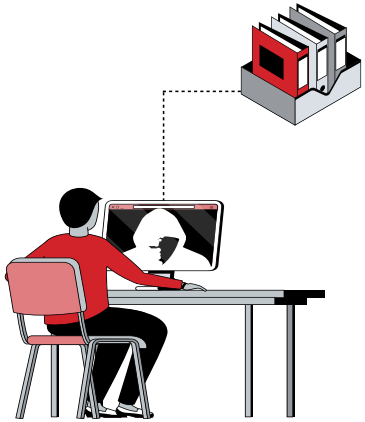
Was ist passiert?
Die Ransomware-Gruppe „Akira“ griff ein Unternehmen für Büro-Systemlösungen an und drohte mit der Veröffentlichung sensibler Daten, darunter Kunden- und Mitarbeiterkontakte, Finanzinformationen, Verträge, Sozialversicherungsnummern und weitere vertrauliche Unterlagen. Eine konkrete Zahlungsfrist nannten die Angreifer nicht.

Was hätte man besser machen können?
Um die Folgen des Angriffs zu minimieren, hätte das Unternehmen auf eine starke Verschlüsselung sensibler Daten, regelmäßige Sicherheits-Audits und ein erprobtes Incident-Response-Playbook setzen sollen. So hätten Schwachstellen frühzeitig erkannt und im Ernstfall schneller reagiert werden können, bevor es zur Veröffentlichung vertraulicher Daten kommt.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8971-akira-hartmann-stanyak-buero-systeme.png

Was lernen wir daraus:
Sozialversicherungsnummern sind für Ransomware-Gruppen besonders wertvoll: Sie sind dauerhaft gültig, schwer zurückzusetzen und oft mit weiteren personenbezogenen Daten verknüpft. Ihr Missbrauch ermöglicht Identitätsdiebstahl und Social Engineering. Für Unternehmen bedeutet ihr Verlust ein hohes Risiko, inklusive Reputationsschäden und Bußgeldern nach der DSGVO.



RIEDEL

Ransomware-Gruppe „Safepay“ entwendet Daten zahlreicher deutscher Unternehmen

30. März 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Die Ransomware-Gruppe „Safepay“ veröffentlichte erfolgreiche Angriffe auf mehrere deutsche Unternehmen verschiedenster Branchen. Betroffen waren u. a. eine Spedition (8,6 GB), ein Hygiene-Großhandel (132 GB), ein Schuheinzelhändler (74 GB) und weitere Firmen. In allen Fällen wurden sensible Daten entwendet und durch Screenshots auf dem Opferblog öffentlich belegt.

Was hätte man besser machen können?
Die betroffenen Unternehmen hätten durch regelmäßige Backups, aktuelle Software, starke Zugangskontrollen und gezielte Mitarbeiterschulungen ihre IT-Sicherheit deutlich stärken können. Netzwerksegmentierung sowie ein effektives Monitoring hätten zudem geholfen, Angriffe frühzeitig zu erkennen und einzudämmen. Ein ganzheitliches Sicherheitskonzept ist entscheidend, um Datenverluste durch Ransomware zu verhindern oder deren Folgen zu minimieren.

Anzunehmende Schadensfelder:

Quellen:
https://www.dsgvo-portal.de/sicherheitsvorfall-datenbank/

Was lernen wir daraus:
Gruppen wie „Safepay“ zielen oft gezielt auf deutsche Unternehmen, weil Deutschland eine starke Wirtschaft mit vielen international vernetzten Firmen hat, die meist wertvolle und sensible Daten speichern. Viele Unternehmen nutzen zwar digitale Systeme, aber oft fehlen moderne Sicherheitsmaßnahmen oder es finden sich Lücken in der IT-Infrastruktur. Die strengen Datenschutzvorgaben in Deutschland erhöhen außerdem im Ernstfall den Druck auf Unternehmen, auf Erpressungsversuche zu reagieren.

RIEDEL

Cyberangriff mit Alt-Zugangsdaten: Hunderttausende Kundendaten betroffen

30. März 2025, in Eschborn/Hessen

DATENDIEBSTAHL

DATENLECK

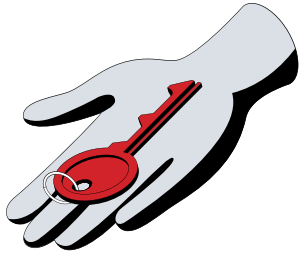
EINBRUCH

Was ist passiert?
Ein Angreifer namens „GHNA“ nutzte 2021 durch den Schadcode „Raccoon Infostealer“ gestohlene Zugangsdaten eines externen Dienstleisters, um interne Systeme eines großen Elektronikunternehmens in Deutschland zu kompromittieren. Rund 270.000 Personen waren vom Datenabfluss betroffen, darunter Namen, Adressen, E-Mails, Bestell- und Supportdaten.

Was hätte man besser machen können?
Der Zugriff über alte Zugangsdaten hätte durch MFA verhindert werden können. Zusätzlich hätte ein aktives **Security Operations Center (SOC)** verdächtige Aktivitäten frühzeitig erkannt und gestoppt. So wäre der Datenabfluss an über 270.000 Betroffene vermeidbar gewesen.

Anzunehmende Schadensfelder:

Was lernen wir daraus:
Alte, kompromittierte Zugangsdaten können Jahre später noch als Einfallstor für massive Datenschutzverletzungen dienen. Das zeigt: Zugangsdaten haben ein Verfallsdatum. Wer sie nicht regelmäßig ändert und absichert, riskiert, dass längst vergessene Sicherheitslücken zur tickenden Zeitbombe werden, mit Folgen für Hunderttausende Betroffene.



Quellen:
https://www.infostealers.com/article/samsung-tickets-data-leak-infostealers-strike-again-in-massive-free-dump/
https://www.securityweek.com/hacker-leaks-samsung-customer-data/

RIEDEL

Glas- und Polymerverarbeiter gerät ins Visier von Ransomware-Gruppe

27. März 2025, in Goslar/Niedersachsen

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Am 27. März 2025 war ein Hersteller aus der Glas- und Polymerverarbeitung von einem Cyberangriff betroffen, der mutmaßlich von der Ransomware-Gruppe „RansomHub“ ausging. Die Angreifer gaben an, etwa 10 GB an Daten aus den Unternehmenssystemen entwendet zu haben. Zur Untermauerung dieser Behauptung veröffentlichten sie mehrere Screenshots.

Was hätte man besser machen können?
Durch ein Security Operations Center (SOC) hätte der Angriff frühzeitig erkannt und damit besser abwehrt werden können. Es nutzt spezialisierte Sicherheitstools wie SIEM zur zentralen Überwachung, EDR zum Schutz von Endgeräten sowie Vulnerability Scan, um Schwachstellen im System zu identifizieren und zu beheben.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8970-ransomhub-europtec.png
https://www.security-incidents.de/assets/img/incidents/8970-ransomhub-europtec-01.png

Was lernen wir daraus:
Ransomware-Gruppen wie „RansomHub“ stehlen oft gezielt nur kleine Datenmengen, wie hier rund 10 GB, aber mit hohem Informationswert. Das zeigt: Es braucht keine riesigen Datenlecks, um massiven Druck aufzubauen. Schon wenige sensible Dateien können für ein Unternehmen enormen Schaden bedeuten.

RIEDEL

Angriff auf Kanzlei: Verträge und Ausweisdokumente veröffentlicht

20. März 2025, in Hamburg/Hamburg

DATENDIEBSTAHL
RANSOMWARE
EINBRUCH
DATENLECK

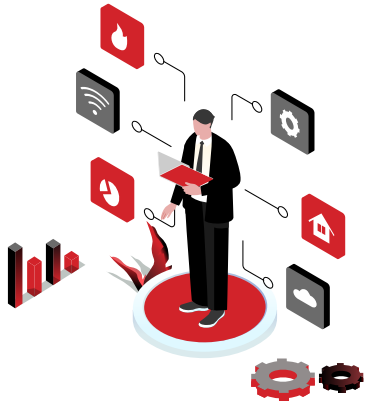
Was ist passiert?
Die Ransomware-Gruppe „Cloak“ veröffentlichte 231 GB Daten einer Kanzlei für Wirtschaftsrecht und Steuerberatung aus Norddeutschland. Darunter: Ausweiskopien, Verträge und Rechnungen. Bereits einen Monat zuvor war das Unternehmen anonymisiert auf der Leak-Seite der Angreifer genannt worden, jedoch ohne konkrete Namensnennung.

Was hätte man besser machen können?
Ein kontinuierlich aktives Security Operations Center (SOC) hätte verdächtige Aktivitäten wie ungewöhnliche Zugriffe oder große Datenabflüsse frühzeitig erkannt. Durch 24/7-Überwachung wäre eine schnelle Reaktion möglich gewesen. Ergänzend hätten gezielte Schulungen zu Phishing und Datenschutz das Risiko einer Kompromittierung reduziert.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8874-Cloak-WirtschaftsratRecht.png

Was lernen wir daraus:
Der Vorfall zeigt, dass Kanzleien und ähnliche Dienstleister mit hohem Datenwert besonders im Visier von Ransomware-Gruppen stehen. Sie verfügen über große Mengen sensibler Informationen – darunter Verträge, Ausweisdokumente und steuerrelevante Daten –, die für Angreifer äußerst attraktiv sind. Die Veröffentlichung solcher Daten gefährdet nicht nur den Datenschutz, sondern auch das Vertrauen der Mandanten sowie die Integrität der anwaltlichen Verschwiegenheitspflicht.



RIEDEL

Digitale Attacke auf Industrieunternehmen: Vertrauliche Daten veröffentlicht

19. März 2025, in Emmerich/Nordrhein-Westfalen

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

Was ist passiert?
Ein mittelständisches Industrieunternehmen mit Sitz in Nordrhein-Westfalen ist offenbar ins Visier der Ransomware-Gruppe „Play“ geraten. Am 19. März 2025 wurde das Unternehmen auf der Leakseite der Gruppe gelistet. Wenig später wurden sensible Geschäftsdaten wie Finanzunterlagen und Kundendaten auf der Darknet-Seite veröffentlicht.

Was hätte man besser machen können?
Ein Einsatz von Extended Detection and Response (XDR) hätte geholfen, den Angriff frühzeitig zu erkennen. XDR verknüpft sicherheitsrelevante Daten aus Endpoints, Netzwerken, Servern und E-Mail-Systemen und erkennt verdächtige Aktivitäten wie unübliche Datenbewegungen oder Zugriffe auf sensible Informationen, bevor Schaden entsteht.

Was lernen wir daraus:
Der Fall zeigt, dass Ransomware-Gruppen ihre Drohungen in der Regel wahr machen – insbesondere wenn keine wirksamen Gegenmaßnahmen getroffen oder Verhandlungen scheitern. Die Veröffentlichung sensibler Daten im Darknet kann schwerwiegende Folgen für betroffene Unternehmen haben, darunter Reputationsverluste, rechtliche Konsequenzen und Vertrauensbrüche bei Kunden und Partnern.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8850-PLAY-Q-Railing-02.png
https://www.security-incidents.de/assets/img/incidents/8850-PLAY-Q-Railing.jpg
https://www.security-incidents.de/assets/img/incidents/8850-PLAY-Q-Railing-03.png

RIEDEL

Cyberangriff auf Altenheimbetreiber: Notfallnummer eingerichtet

17. März 2025, in Mönchengladbach/Nordrhein-West-

RANSOMWARE

AUSFALL

Was ist passiert?
Ein kommunaler Dienstleistungsbetrieb in Nordrhein-Westfalen wurde Opfer eines Cyberangriffs. Die Angreifer verschlüsselten zentrale IT-Systeme, wodurch Telefon- und E-Mail-Dienste vorübergehend ausfielen. Der Pflegebetrieb blieb aufrechterhalten. Eine Notfall-Hotline wurde eingerichtet, um die Erreichbarkeit in dringenden Fällen sicherzustellen.

Was hätte man besser machen können?
Die Ursache des Angriffs lag vermutlich in einer ungesicherten Schnittstelle oder veralteter Software, die von den Angreifern ausgenutzt wurde. Ein gezielter **Schwachstellenscan** hätte diese Sicherheitslücke früher erkennen und beheben können. Zudem hätte der Einsatz eines **Endpoint Detection and Response (EDR)**-Systems verdächtige Aktivitäten auf den betroffenen Geräten schnell identifizieren und eine unmittelbare Reaktion auslösen können.

Anzunehmende Schadensfelder:

Quellen:
https://rp-online.de/nrw/staedte/moenchengladbach/cyberangriff-auf-sozial-holding-altenheime-in-moenchengladbach-betroffen_aid-125320881
https://www.faz.net/agenturmeldungen/dpa/cyberangriff-gegen-altenheim-verwaltung-in-moenchengladbach-110362676.html

Was lernen wir daraus:
Der Vorfall zeigt, welche Folgen ein erfolgreicher Ransomware-Angriff haben kann – insbesondere wenn die Systeme durch die Täter vollständig verschlüsselt werden. Solche Angriffe legen nicht nur Betriebsabläufe lahm, sondern bedrohen auch die Verfügbarkeit kritischer Informationen. Organisationen – insbesondere solche mit sensiblen Daten oder gesellschaftlicher Verantwortung – müssen sich der realen Gefahr bewusst sein und Sicherheitsrisiken strategisch ernst nehmen.

RIEDEL

Cyberangriff bringt kommunale Verwaltung zum Stillstand

17. März 2025, in Kirkel/Saarland

EINBRUCH

AUSFALL

Was ist passiert?
Eine Kommunalverwaltung im Saarland wurde Ziel eines Cyberangriffs, der den Betrieb im Rathaus zeitweise lahmlegte. Rund 100 Geräte mussten neu aufgesetzt werden, was zur vorübergehenden Schließung führte. Polizei und IT-Sicherheitsexperten ermittelten, während benachbarte Gemeinden bei der schrittweisen Wiederherstellung der Systeme unterstützten.

Was hätte man besser machen können?
Der Vorfall hätte durch eine 24/7-Überwachung durch ein Security Operations Center (SOC) deutlich früher erkannt werden können. Dadurch wären rechtzeitige Gegenmaßnahmen möglich gewesen, um die Ausbreitung der Schadsoftware zu stoppen und negative Auswirkungen auf die IT-Infrastruktur zu minimieren. Ein solches Monitoring ermöglicht außerdem eine schnelle Erkennung von Anomalien und stärkt so die Sicherheit gegenüber zukünftigen Angriffen.

Anzunehmende Schadensfelder:

Quellen:
https://www.saarbruecker-zeitung.de/saarland/saar-pfalz-kreis/kirkel/nach-cyberangriff-auf-rathaus-kirkel-jetzt-spricht-der-buergermeister_aid-125320267
https://www.tagesschau.de/inland/regional/saarland/sr-gemeinde-kirkel-nach-cyberangriff-wieder-per-mail-erreichbar-100.html

Was lernen wir daraus:
Der Angriff auf das Rathaus unterstreicht die besondere Verantwortung öffentlicher Einrichtungen im Umgang mit sensiblen personenbezogenen Daten. Kommunale Verwaltungen sind gesetzlich verpflichtet, strenge Datenschutz- und IT-Sicherheitsstandards einzuhalten, um die Daten ihrer Bürgerinnen und Bürger zu schützen. Der Vorfall zeigt deutlich, wie kritisch es ist, diese gesetzlichen Vorgaben konsequent umzusetzen und kontinuierlich zu kontrollieren.

RIEDEL

Sicherheitslücke bei Glücksspielanbieter: Millionen Nutzerdaten gefährdet

15. März 2025, in Espelkamp/Nordrhein-Westfalen

DATENPANNE

AUSFALL

SICHERHEITSLÜCKE

Was ist passiert?
Ein Datenschutzvorfall bei einem großen deutschen Unternehmen der Unterhaltungs- und Glücksspielbranche offenbarte gravierende Sicherheitslücken. Über eine ungeschützte Schnittstelle wurden sensible Daten von fast einer Million Nutzern zugänglich. Die Regulierungsbehörde rügte das Unternehmen, mehrere Plattformen wurden vorübergehend offline genommen.

Was hätte man besser machen können?
Ein **Schwachstellenscan** hätte die ungesicherte GraphQL-Schnittstelle identifizieren können, bevor sie für einen Angriff ausgenutzt wurde. Solche Prüfungen tragen wesentlich dazu bei, technische Sicherheitslücken sichtbar zu machen und Risiken frühzeitig zu minimieren.
Darüber hinaus sollten Mitarbeitende gezielt zu gesetzlichen Sicherheitsvorgaben geschult werden.

Anzunehmende Schadensfelder:

Quellen:
https://lilithwittmann.medium.com/casinonutzer-der-merkur-gruppe-verlieren-nicht-nur-ihr-geld-sondern-auch-ihre-daten-ef6710184f7c
https://www.heise.de//hintergrund/Man-hat-sich-einen-Dreck-um-die-Sicherheit-der-Daten-der-Spieler-geschert-10321798.html

Was lernen wir daraus:
Der Vorfall verdeutlicht die kritische Bedeutung eines umfassenden Sicherheitsmanagements. Dass die Schwachstelle erst durch externe Sicherheitsforschung nach der Datenpanne entdeckt wurde, zeigt, dass interne Kontrollmechanismen unzureichend waren. Unternehmen sollten nicht erst auf öffentlich gewordene Vorfälle reagieren, sondern proaktiv Sicherheitslücken erkennen und schließen – bevor sie von Dritten gefunden und potenziell missbraucht werden.

RIEDEL

Ransomware-Gruppe entwendet sensible Unternehmensdaten

13. März 2025, in Tholey/Saarland

DATENDIEBSTAHL

RANSOMWARE

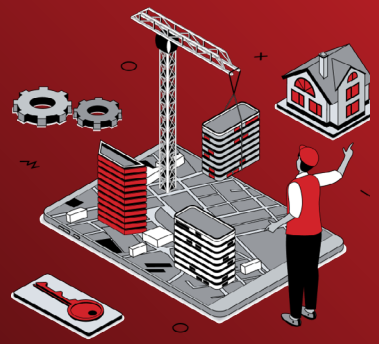
Was ist passiert?
Eine Ransomware-Gruppe gab auf ihrem Darknet-Blog Informationen über einen Angriff auf ein Unternehmen aus der Bauwirtschaft bekannt. Dabei soll eine nicht näher bezifferte Menge sensibler Daten entwendet worden sein, darunter personenbezogene Informationen, Kundendaten, Lohn- und Steuerunterlagen, Ausweiskopien sowie Finanz- und Budgetdaten.

Was hätte man besser machen können?
Ein Security Operations Center (SOC), das Sicherheitsereignisse kontinuierlich überwacht und auswertet, hätte in diesem Fall möglicherweise eine frühe Erkennung des Angriffs ermöglicht. Die strukturierte Analyse von Anomalien und ein zentral gesteuertes Incident-Response können entscheidend dazu beitragen, Angriffe rechtzeitig zu identifizieren und geeignete Gegenmaßnahmen einzuleiten – noch bevor es zu Datenabfluss oder weiteren Schäden kommt.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8748-play-backes-ag.png
https://www.security-incidents.de/assets/img/incidents/8748-play-backes-ag-02.png

Was lernen wir daraus:
Die gestohlene Daten betreffen nicht nur geschäftliche Informationen, sondern auch sensible personenbezogene Daten – mit potenziell weitreichenden Folgen für Betroffene. Immer häufiger nutzen Angreifer dabei die Veröffentlichung solcher Vorfälle als Druckmittel, um Unternehmen zur Zahlung zu bewegen. Der Fall macht deutlich: IT-Sicherheit ist längst kein rein technisches Thema mehr, sondern ein zentraler Bestandteil unternehmerischer Verantwortung.



RIEDEL

Cyberangriff auf Autohaus: 32 GB Firmendaten entwendet

13. März 2025, in Leipzig/Sachsen

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Eine bekannte Ransomware-Gruppe veröffentlichte auf ihrem Blog im Darknet Angaben über einen erfolgreichen Cyberangriff auf ein mitteldeutsches Unternehmen aus dem Automobilhandel. Die Angreifer behaupten, rund 32 Gigabyte an sensiblen Firmendaten entwendet zu haben und drohen nun mit deren Veröffentlichung. Als Beleg stellten sie eine strukturierte Übersicht in Form einer Textdatei bereit.

Was hätte man besser machen können?
Ein im Vorfeld durchgeführter **Schwachstellenscan** hätte die ausgenutzte Sicherheitslücke mit hoher Wahrscheinlichkeit frühzeitig erkannt und deren Behebung ermöglicht. Ergänzend dazu wäre eine **24/7-Überwachung** der IT-Systeme entscheidend gewesen, um Bedrohungen in Echtzeit zu identifizieren und unverzüglich angemessene Gegenmaßnahmen einzuleiten.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9361-J-Autohaus.png

Was lernen wir daraus:
Alle Unternehmen, unabhängig von Branche oder Größe, können Opfer von Cyberangriffen werden. Der Vorfall zeigt, wie schnell und gezielt Ransomware-Angriffe erfolgen und wie empfindlich Unternehmen durch den Diebstahl sensibler Daten getroffen werden können. Die Veröffentlichung von Beweismaterial im Darknet verdeutlicht zudem die zunehmende Professionalität und strategische Vorgehensweise der Täter, um zusätzlichen Druck auf das betroffene Unternehmen auszuüben.

RIEDEL

Hackerangriff auf ein weltweit führendes Etikettenunternehmen

11. März 2025, in Witzhave/Schleswig-Holstein

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Am 11. März 2025 nahm die Ransomware-Gruppe „Akira“ ein Verpackungsunternehmen ins Visier. Laut eigenen Angaben erlangten die Angreifer Zugriff auf über 192 GB interner Unternehmensdaten, darunter Finanzprüfungen, Zahlungsinformationen, Berichte sowie persönliche Kontaktdaten von Mitarbeitenden und Kunden.

Was hätte man besser machen können?
Eine umfassende Netzwerksegmentierung hätte verhindern können, dass sich Angreifer nach dem initialen Zugriff lateral durch das gesamte System bewegen. Durch das Aufteilen des Netzwerks in klar definierte Sicherheitszonen, etwa nach Abteilungen oder Datenklassen, lassen sich potenzielle Angriffsflächen verkleinern.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8725-akira-all4labels.png

Was lernen wir daraus:
Gerade moderne Angriffe setzen auf sogenannte „Laterale Bewegungen“, um sich nach einem erfolgreichen Einstieg tief ins Netzwerk zu graben. Organisationen sollten ihre interne Infrastruktur so gestalten, dass im Ernstfall nicht das gesamte Unternehmen kompromittiert werden kann – auch wenn ein Einfallstor genutzt wurde. Gute Netzwerkarchitektur wirkt hier wie ein Brandschutzsystem.

RIEDEL

Zentrales Buchungssystem von Flugticket-Händler nach Cyberattacke außer Betrieb

10. März 2025, in Berlin/Berlin

DATENVERLUST

AUSFALL

EINBRUCH

Was ist passiert?
Ein führender europäischer Flugticket-Händler wurde Ziel eines Cyberangriffs, der das zentrale Buchungssystem lahmlegte. Ein Krisenstab koordinierte die Wiederherstellung mit interner und externer Unterstützung. Laut Unternehmen gab es nur minimalen Datenverlust. Kunden wurden informiert, und ein Notfall-Buchungssystem hielt den Betrieb aufrecht.

Was hätte man besser machen können?
Eine segmentierte IT-Infrastruktur hätte den Schaden womöglich begrenzt. Durch die Trennung kritischer Systeme wie Buchungsserver, Kundendatenbanken und interner Kommunikation lassen sich Angriffsflächen verkleinern. Auch ein gezieltes Netzwerk-Zugriffsmanagement, etwa über Zero-Trust-Architekturen, hilft, Systeme besser zu isolieren und nur autorisierten Datenverkehr zuzulassen.

Anzunehmende Schadensfelder:

Quellen:
https://www.airliners.de/aerticket-ziel-cyberangriffs/79631
https://www.security-incidents.de/assets/img/incidents/8700-aerticket.png

Was lernen wir daraus:
IT-Sicherheit ist nicht nur Prävention, sondern auch Resilienz. Unternehmen sollten sich nicht nur auf Schutzmaßnahmen konzentrieren, sondern aktiv durchspielen, wie sie bei Ausfällen oder Angriffen handlungsfähig bleiben. Simulierte Stresstests, Kommunikationspläne und klare Entscheidungsstrukturen im Ernstfall sind entscheidend, um nicht unkoordiniert zu reagieren, sondern den Geschäftsbetrieb gezielt abzusichern.

RIEDEL

Ransomware-Gruppe listet Onlinehändler als Opfer – Screenshots veröffentlicht

10. März 2025, in Sindelfingen/Baden-Württemberg

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

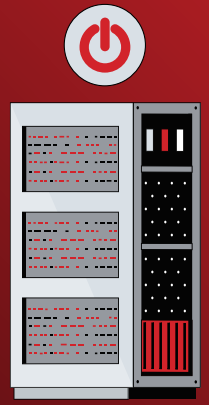
Was ist passiert?
Ein deutscher Online-Bekleidungshändler wurde Opfer einer Ransomware-Attacke. Die Tätergruppe „INC Ransom“ listet das Unternehmen seit dem 10. März 2025 auf ihrer Leakseite und behauptet, sensible Daten gestohlen zu haben. Zur Beweisführung veröffentlichten sie Screenshots.

Was hätte man besser machen können?
Ein effektives Zugriffsmanagement mit rollenbasierten Berechtigungen hätte den Schaden begrenzen können. Wären sensible Daten klar segmentiert und Zugriffe nach dem Prinzip der geringsten Rechte vergeben worden, wären nicht automatisch alle kritischen Informationen betroffen gewesen. Regelmäßige Rechteprüfungen helfen zusätzlich, Risiken zu minimieren.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8751-INCRansom-yeanshallede.png

Was lernen wir daraus:
Cyberangriffe verlaufen häufig in mehreren Phasen – vom ersten Eindringen über das Auskundschaften bis hin zur Verschlüsselung und Exfiltration von Daten. Wer in dieser Kette frühzeitig eingreifen kann, etwa durch Alarmierung bei ungewöhnlichem Datenabfluss oder verdächtigen Login-Versuchen, kann größeren Schaden verhindern. IT-Sicherheit beginnt daher nicht erst beim Vorfall, sondern bei der Fähigkeit, Muster zu erkennen und korrekt zu reagieren.



RIEDEL

Ransomware-Gruppe hackt Autohaus – Verträge und Kundendaten kompromittiert

10. März 2025, in Bottrop/Nordrhein-Westfalen

DATENDIEBSTAHL
RANSOMWARE
EINBRUCH

Was ist passiert?
Ein deutsches Autohaus wurde Ziel einer Ransomware-Attacke. Die Tätergruppe „INC“ Ransom listet das Unternehmen seit dem 10. März 2025 auf ihrem Darknet-Blog und gibt an, sensible Daten wie Verträge sowie Kunden- und Mitarbeiterinformationen erbeutet zu haben. Mehrere Screenshots der Daten wurden als Beweis veröffentlicht.

Was hätte man besser machen können?
Für Unternehmen wie Autohäuser, die täglich mit großen Mengen personenbezogener Daten arbeiten, ist ein mehrstufiges Sicherheitskonzept entscheidend. Neben technischer Grundhygiene wie Patch-Management und Backup-Strategien wären hier Lösungen wie ein **Security Operations Center (SOC)** in Kombination mit **Endpoint Detection & Response (EDR)** sinnvoll gewesen.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8890-INCransom-Bellendorf.png

Was lernen wir daraus:
Ein gezielter Blick auf die Reaktionszeit im Ernstfall lohnt sich. Wie lange dauert es im eigenen Unternehmen, bis ein Vorfall bemerkt wird? Wie viele Minuten oder Stunden vergehen, bis konkrete Maßnahmen eingeleitet werden? Die Differenz zwischen Angriff und Reaktion entscheidet oft über das Ausmaß des Schadens. Wer seine Erkennungs- und Reaktionszeiten realistisch kennt und regelmäßig testet, ist besser vorbereitet.

RIEDEL

Verwaltungsgesellschaft Opfer einer Ransomware-Attacke

9. März 2025, in Heringsdorf/Mecklenburg-Vorpommern

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

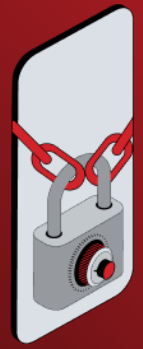
Was ist passiert?
Eine Verwaltungsgesellschaft aus Mecklenburg-Vorpommern wurde Opfer einer Ransomware-Attacke. Die Ransomware-Gruppe „INC Ransom“ gab an, 14,1 GB sensible Daten verschlüsselt und gestohlen zu haben. Als Beweis veröffentlichten sie einen Screenshot der Daten.

Was hätte man besser machen können?
Ein Security Operations Center (SOC) mit angebundener XDR-Lösung hätte den Angriff durch die Kombination aus Verhaltensanalyse, Netzwerk-Telemetrie und Echtzeit-Erkennung auffälliger Aktivitäten frühzeitig identifizieren können. Zusätzlich wäre eine regelmäßige Schwachstellenanalyse sinnvoll, um potenzielle Einfallstore – etwa durch veraltete Software – rechtzeitig zu schließen.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8689-INCRansom-Kaiserb%C3%A4der.png

Was lernen wir daraus:
Die ersten 72 Stunden nach einem Cyberangriff sind entscheidend. Wer in dieser Zeit vorbereitet und strukturiert handelt, kann Folgeschäden begrenzen. Dazu gehört u. a. ein klar definierter Notfallplan mit Zuständigkeiten, Kommunikationswegen und einem Krisenteam. Auch ein Meldesystem für Vorfälle und vorbereitete Kontaktlisten (z. B. Datenschutzbehörde, CERT, Dienstleister) sollten regelmäßig überprüft und griffbereit sein – idealerweise auch offline.



RIEDEL

Ransomware-Gruppe Lynx erpresst deutsches Industrieunternehmen

5. März 2025, in Plettenberg/Nordrhein-Westfalen

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

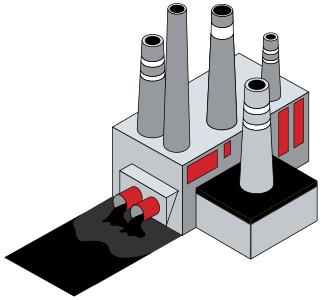
Was ist passiert?
Eine deutsche Firma aus dem Bereich Schmiedetechnik wurde Opfer einer Ransomware-Attacke. Die Täter, die sich Lynx-Gruppe nennen, behaupten, zahlreiche sensible Daten erbeutet zu haben. Zur Untermauerung ihrer Forderungen veröffentlichten sie bereits interne Dokumente und drohen mit der vollständigen Datenfreigabe, falls kein Lösegeld gezahlt wird.

Was hätte man besser machen können?
Ein Security Operations Center (SOC) mit durchgehender Überwachung hätte verdächtige Aktivitäten frühzeitig erkennen und Gegenmaßnahmen einleiten können. Durch definierte Reaktionsprozesse und abgestimmte Analysewerkzeuge lassen sich Angriffe wie dieser schneller eingrenzen.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8641-Lynx-Schmiedetechnik-Plettenberg.PNG

Was lernen wir daraus:
Cyberangriffe auf produzierende Unternehmen zeigen, wie sehr die Fertigung heute von digitalen Prozessen abhängt. Wer seine Produktion absichern will, sollte IT-Sicherheit als integralen Bestandteil der Unternehmensstrategie behandeln – nicht als nachgelagertes Thema. Zudem ist es hilfreich, sich regelmäßig mit aktuellen Bedrohungsszenarien zu beschäftigen, um interne Prozesse entsprechend anzupassen.



RIEDEL

Ransomware-Gruppe erpresst Fleischwarenhersteller mit 2 TB Daten

5. März 2025, in Ruppichteroth/Hessen

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

AUSFALL

Was ist passiert?
Ein mittelständischer deutscher Fleischwarenhersteller wurde Ziel einer Ransomware-Attacke. Die Angreifer behaupten, 2 Terabyte Unternehmensdaten erbeutet zu haben. Das Unternehmen erhielt eine Lösegeldfrist, ansonsten drohte die Veröffentlichung der Daten. Seit dem Angriff blieb die Firmenwebsite lange Zeit offline.

Was hätte man besser machen können?
Ein strukturierter Notfallplan inklusive vordefinierter Reaktionsmaßnahmen hätte die Auswirkungen der Attacke begrenzen können. Auch eine vorherige Überprüfung der Backup-Strategie – insbesondere auf Offline- und manipulationssichere Sicherungen – wäre entscheidend gewesen. Darüber hinaus sollten interne Zugriffsrechte regelmäßig überprüft und nur nach dem Prinzip der minimalen Berechtigung vergeben werden, um die Ausbreitung im Netzwerk einzuschränken.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8642-Safepay-Willms_1.png
https://www.security-incidents.de/assets/img/incidents/8642-Safepay-Willms_2.png

Was lernen wir daraus:
Produktionsbetriebe sind zunehmend von digitaler Infrastruktur abhängig – vom Einkauf bis zur Logistik. Fällt diese aus, gerät der Betrieb ins Stocken. Daher ist IT-Sicherheit nicht nur Schutzmaßnahme, sondern auch betriebswirtschaftliche Notwendigkeit. Unternehmen sollten Cybersicherheit als festen Bestandteil ihres Risikomanagements etablieren – mit klaren Zuständigkeiten, technischen Maßnahmen und regelmäßigen Notfallübungen.

RIEDEL

IT-Ausfall bei Stadtwerken sorgt für Beeinträchtigungen in der Stadtverwaltung

5. März 2025, in Schwerte/Nordrhein-Westfalen

RANSOMWARE

DATENLECK

EINBRUCH

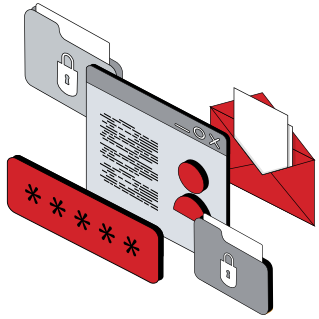
AUSFALL

Was ist passiert?
Anfang März 2025 legte ein Cyberangriff die IT-Systeme eines Stadtwerks lahm. Das interne Netzwerk und das Kundenportal waren zeitweise nicht erreichbar. Die Stadt kappte vorsorglich die digitale Verbindung zu den Stadtwerken und dem IT-Dienstleister. Online-Dienste wie Passwesen und Terminabmeldungen waren stark eingeschränkt. Externe IT-Experten wurden zur Behebung hinzugezogen.

Was hätte man besser machen können?
Kommunale IT-Infrastrukturen benötigen zugeschnittene Sicherheitskonzepte. Eine regelmäßige **Schwachstellenanalyse**, gepaart mit einer **SIEM-Plattform**, hätte potenziell Auffälligkeiten im Vorfeld identifizieren und zur Abwehr beitragen können. Zudem wäre ein Notfall- und Wiederanlaufplan wichtig gewesen, um die Auswirkungen auf städtische Dienste zu minimieren.

Anzunehmende Schadensfelder:

Was lernen wir daraus:
Cyberangriffe auf öffentliche Einrichtungen treffen nicht nur IT-Systeme, sondern direkt die Bürgerinnen und Bürger. Kommunen sollten daher Cybersicherheit als Teil der kritischen Daseinsvorsorge begreifen. Wer seine Verwaltungsprozesse digitalisiert, muss auch in Schutzmaßnahmen investieren – organisatorisch, technisch und personell.



Quellen:
https://www.ruhrnachrichten.de/schwerte/cyberangriff-cyberattacke-netzwerk-intern-kundenportal-versorgung-stadtwerke-schwerte-stoerung-w1005308-2001581632/
https://www.wa.de/nordrhein-westfalen/cyber-angriff-trifft-stadt-in-nrw-behoerden-wurden-in-kenntnis-gesetzt-93608511.html

RIEDEL

Cyberangriffe durch „FOG“: Vertrauliche Daten von vier deutschen Unternehmen geleakt

5. März 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

DATENLECK

Was ist passiert?
Die Ransomware-Gruppe „FOG“ veröffentlichte im März eine Liste mit 19 erbeuteten Gitlab-Datensätzen samt Download-Links. Betroffen waren u. a. eine internationale Organisation aus Darmstadt (291 GB), eine Medienfirma aus Karlsruhe (58 GB), eine Agentur für Browser-Spiele aus Bochum (500 GB) sowie ein IT-Dienstleister aus Frankfurt (39 GB).

Was hätte man besser machen können?
Ein grundlegendes Sicherheitskonzept hätte in mehreren Fällen helfen können: etwa durch regelmäßige Schwachstellenanalysen, klare Zugriffskontrollen und zentrale Monitoring-Systeme. So lassen sich verdächtige Aktivitäten frühzeitig erkennen und gezielt Gegenmaßnahmen einleiten – bevor sensible Daten in großem Umfang abfließen.

Anzunehmende Schadensfelder:

Quellen:
https://www.dsgvo-portal.de/sicherheitsvorfaelle/ransomware_angriff_neopoly-development-8648.php

Was lernen wir daraus:
Cyberangriffe wie die durch „FOG“ zeigen, wie wichtig grundlegende IT-Sicherheitsmaßnahmen sind. Regelmäßige Prüfungen, klare Zugriffsregeln und zentrale Überwachung helfen, Risiken frühzeitig zu erkennen. Prävention ist kein Luxus, sondern Voraussetzung für digitale Resilienz.

RIEDEL

Analysefirma nach Cyberattacke wochenlang offline

5. März 2025, in Berlin/Berlin

DATENDIEBSTAHL

RANSOMWARE

AUSFALL

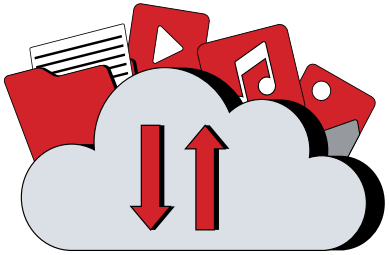
Was ist passiert?
Ein Datenanalyseunternehmen wurde Opfer eines Ransomware-Angriffs. Dabei wurden unter anderem zentralen Systeme verschlüsselt und Kundendaten kompromittiert. Der Betrieb kam deshalb zwischenzeitlich komplett zum Erliegen und Monitoring-Dienste konnten nicht mehr angeboten werden. Auch Wochen später war die Webseite des Unternehmens nicht vollständig erreichbar.

Was hätte man besser machen können?
Ein mehrstufiges Sicherheitskonzept mit regelmäßigen **Schwachstellenanalysen** sowie der Einsatz von **EDR**- und **XDR-Technologien** kann helfen, Angriffe frühzeitig zu erkennen und einzudämmen, bevor zentrale Systeme kompromittiert werden. Auch ein getesteter Notfall- und Wiederherstellungsplan ist entscheidend, um den Betrieb nach einem Vorfall schnellstmöglich wieder aufzunehmen.

Anzunehmende Schadensfelder:

Quellen:
https://medieninsider.com/hackerangriff-auf-pressespiegel-anbieter-argus/25216/
https://www.security-incidents.de/assets/img/incidents/8846-Safepay-ArgusDataInsights.jpg

Was lernen wir daraus:
Die Abhängigkeit von digitalen Kernsystemen macht datengetriebene Unternehmen besonders verwundbar. Neben Präventionsmaßnahmen ist es wichtig, Resilienz aufzubauen: etwa durch redundante Strukturen, regelmäßige Backups und die Schulung von Personal im Umgang mit IT-Notfällen. Wer vorbereitet ist, kann Ausfallzeiten verkürzen und Schäden begrenzen.



RIEDEL

Wenn die IT streikt: Handgeschriebene Rechnungen im digitalen Zeitalter

3. März 2025, in Deutschland

EINBRUCH

AUSFALL

Was ist passiert?
Ein internationales Hotelunternehmen wurde Opfer eines Cyberangriffs, der zentrale IT-Systeme lahmlegte. In einem Hotel mussten Rechnungen manuell erstellt werden. Einige Abläufe laufen weiterhin händisch, Telefonleitungen wurden umgeleitet. Externe Fachleute unterstützen bei der Analyse und vollständigen Wiederherstellung der Systeme.

Was hätte man besser machen können?
Ein regelmäßiger RED Skull Schwachstellenscan hätte dem Hotelunternehmen geholfen, Sicherheitslücken frühzeitig zu erkennen und zu schließen – bevor Angreifer sie ausnutzen konnten. Ergänzend hätte die R.E.D. Security-Suite mit aktiver Bedrohungserkennung und Netzwerksegmentierung die Ausbreitung des Angriffs wirksam eingedämmt.

Anzunehmende Schadensfelder:

Quellen:
https://www.hotelvor9.de/inside/systemausfall-bei-adina-wegen-cyber-angriffs
https://www.tageskarte.io/hotellerie/detail/cyber-vorfall-bei-adina-hotels.html
https://www.msn.com/de-de/reisen/nachrichten/cyber-vorfall-bei-adina-hotels/ar-AA1A7AbZ

Was lernen wir daraus:
Unternehmen zahlen im Schnitt deutlich mehr für die Aufarbeitung und Behebung eines Cyberangriffs durch externe Fachleute – inklusive IT-Forensik, Rechtsberatung und Ausfallkosten. Im Vergleich dazu kosten professionelle Sicherheitstools oft nur einen Bruchteil. Frühzeitige Investitionen in Schutzmaßnahmen sind daher nicht nur klüger, sondern auch wirtschaftlich sinnvoller, weil sie Schäden verhindern, bevor sie entstehen.

RIEDEL

Rechtsanwalt Dr. Arnt Glienke, LL.M.
Certified Compliance Professional (CCP), CGO, Bereichsleiter Compliance, Datenschutz & ESG

GASTARTIKEL

CLARIUS DATA & SECURITY

UMSETZUNG DER NIS-2-RICHTLINIE – HERAUSFORDERUNGEN UND CHANCEN FÜR UNTERNEHMEN

Die NIS-2-Richtlinie bezweckt die Stärkung der Cybersicherheit in Europa. Sie verschärft bestehende Vorgaben und verpflichtet Unternehmen in kritischen und wichtigen Sektoren, höhere Sicherheitsstandards einzuführen. Angesichts der bevorstehenden nationalen Umsetzung sollten Unternehmen frühzeitig Maßnahmen ergreifen, um Risiken zu minimieren und gesetzliche Vorgaben zu erfüllen.

Die Richtlinie fordert ein verbessertes Risikomanagement und die Implementierung von Schutzmaßnahmen zur Abwehr von Cyber-Bedrohungen. Sicherheitsvorfälle müssen binnen 24 bis 72 Stunden gemeldet werden. Zudem wird mehr Verantwortung auf die Geschäftsleitung übertragen, da diese für die Einhaltung der Maßnahmen haftet. Auch Lieferketten müssen gesichert werden, indem Dienstleister und Partner strenge Sicherheitsvorkehrungen nachweisen. Verstöße können mit erheblichen Geldstrafen geahndet werden.

Clarius Group ist ein auf IT-Sicherheit, Datenschutz und Compliance spezialisierter Legal Service Provider und unterstützt Unternehmen bei der Umsetzung der NIS-2-Anforderungen. Neben unserer rechtlichen Beratung, Compliance-Checks und praxisnahen Schulungen umfasst unser Leistungsportfolio auch Dokumentationen nach dem BSI-IT-Grundschutz, einem der wichtigsten Standards für Informationssicherheit in Deutschland. Insbesondere im Kontext der NIS-2-Richtlinie ist eine umfassende Dokumentation der Sicherheitsmaßnahmen unerlässlich.

Wir betreuen Unternehmen aus allen Branchen und Unternehmensgrößen – von mittelständischen Betrieben bis hin zu global agierenden Konzernen.

Für eine umfassende Lösung arbeitet die Clarius Group Data & Security GmbH mit der RIEDEL Networks GmbH & Co. KG zusammen. Während Clarius Group die rechtlichen und organisatorischen Aspekte abdeckt, gewährleistet Riedel Enterprise Defense [R.E.D.] die technische Umsetzung. Unsere Kooperation ermöglicht Unternehmen einen ganzheitlichen Ansatz zur Erfüllung der NIS-2-Vorgaben und sorgt für eine nachhaltige Erhöhung der Cybersicherheit.

Unsere Kunden profitieren von einer individuellen Beratung und praxisnahen Maßnahmen, die langfristigen Schutz bieten. Die Zusammenarbeit reduziert regulatorische Risiken und den Verwaltungsaufwand erheblich. Zwar sind die Anforderungen der NIS-2-Richtlinie herausfordernd; sie bieten aber auch die Möglichkeit, die IT-Sicherheitsstrategie grundlegend zu verbessern. Durch die enge Zusammenarbeit der Clarius Group Data & Security GmbH mit der RIEDEL Networks GmbH & Co. KG erhalten Unternehmen eine maßgeschneiderte Unterstützung, um sich frühzeitig auf die neuen Anforderungen vorzubereiten und Sicherheitsrisiken effektiv zu minimieren.

Clarius Group ist eine moderne Rechtsanwaltsgesellschaft mit Sitz in Hamburg, spezialisiert auf Legal Outsourcing, Legal Tech, Compliance und Datenschutz. Das Team aus erfahrenen Juristen bietet flexible Lösungen für Unternehmen. Ein besonderes Merkmal ist die Integration von Legal Tech, z. B. ein Dokumentengenerator für rechtssichere Verträge. 2022 gewann die Kanzlei den Best of Legal-Award in Compliance.
Geführt wird Clarius Group von Dr. Ernst Georg Berger und Nils Oberschelp. Mit über 180 Kunden zählt sie zu den Vorreitern innovativer Rechtsberatung.

RIEDEL

FEBRUAR 2025

SECURITY INCIDENTS GERMANY

RIEDEL

Technische Störung legt beliebten Messenger lahm

AUSFALL

28. Februar 2025, in Hamburg/Hamburg

Was ist passiert?
Am 28. Februar 2025 kam es beim sehr bekannten Messenger-Dienst zu einem etwa 30-minütigen Ausfall. Laut Mutterkonzern handelte es sich um eine technische Störung.

Was hätte man besser machen können?
Auch bei rein technischen Störungen lohnt sich ein genauer Blick auf die Ursachen. Hochverfügbarkeitskonzepte, regelmäßige Lasttests und automatisiertes Monitoring der Systemarchitektur könnten helfen, kritische Fehler frühzeitig zu erkennen und abzufangen, bevor sie zu einem spürbaren Ausfall führen.

Anzunehmende Schadensfelder:

Was lernen wir daraus:
Schon kurze Ausfälle bei zentralen Kommunikationsdiensten zeigen, wie stark unsere Abhängigkeit von digitalen Infrastrukturen ist. Unternehmen sollten regelmäßig Notfallpläne testen, alternative Kommunikationskanäle prüfen und die Resilienz ihrer IT-Systeme hinterfragen – ganz unabhängig davon, ob es sich um Angriffe oder interne Fehler handelt.

RIEDEL

Quellen:
https://www.rtl.de/news/stoerung-bei-whatsapp-id2116213.html
https://www.op-online.de/verbraucher/grosser-ausfall-bei-whatsapp-zehntausende-berichten-von-schwierigkeiten-zr-93600628.html

Cyberkriminelle erbeuten Kundendaten und Ausweise eines Autohauses

27. Februar 2025, in Zwickau/Sachsen

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Die Ransomware-Gruppe „Akira“ listete ein mittelständisches Autohaus aus Sachsen als Opfer auf ihrem Darknet-Blog. Den Tätern zufolge wurden sensible Kundendaten, Mitarbeiterkontakte, Finanzunterlagen sowie Ausweiskopien entwendet. Details zu Lösegeldforderungen sind nicht bekannt.

Was hätte man besser machen können?
In diesem Fall hätte ein zentralisiertes **SIEM-System (Security Information and Event Management)** helfen können, sicherheitsrelevante Ereignisse wie unautorisierte Zugriffe oder Datenabflüsse frühzeitig zu erkennen und zu korrelieren. Auch regelmäßige Schulungen zum sicheren Umgang mit E-Mails und Anhängen könnten zur Prävention beitragen.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8565-akira-autohaus-kiessling.png

Was lernen wir daraus:
Eine ganzheitliche Cybersicherheitsstrategie vereint Prävention, Detektion und Reaktion: Firewalls, Updates und Schulungen schützen präventiv. SIEM-Systeme erkennen Bedrohungen in Echtzeit. Im Ernstfall helfen Notfallpläne und Experten, schnell zu reagieren und Schäden zu begrenzen.

RIEDEL

Ransomware-Angriff auf Startup: Über 10 GB sensible Daten gestohlen

27. Februar 2025, in Frankfurt a.M./Hessen

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

Was ist passiert?
Die Ransomware-Gruppe „Akira“ listete ein Frankfurter Health-Tech-Startup als Opfer auf ihrem Darknet-Portal. Die Täter geben an, mehr als 10 GB sensible Daten entwendet zu haben, darunter Mitarbeiter- und Kundendokumente, Finanzdaten sowie weitere vertrauliche Informationen.

Was hätte man besser machen können?
Gerade junge Unternehmen unterschätzen häufig die Notwendigkeit strukturierter IT-Sicherheitsmaßnahmen. Eine regelmäßige Schwachstellenanalyse hätte potenziell ausnutzbare Lücken frühzeitig identifizieren können. Zusätzlich wäre der Einsatz eines modernen EDR-Systems hilfreich gewesen, um verdächtige Aktivitäten wie das unautorisierte Auslesen sensibler Daten zu erkennen und zu blockieren.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8571-Akira-PraxisEins.png

Was lernen wir daraus:
Startups im digitalen Gesundheitsbereich verarbeiten besonders schützenswerte Informationen und müssen sich frühzeitig mit Sicherheitsstandards auseinandersetzen. Auch ohne große IT-Abteilungen lassen sich viele Grundpfeiler moderner Cybersicherheit mithilfe externer Partner oder spezialisierter Lösungen umsetzen. IT-Sicherheit sollte von Anfang an mitgedacht werden – nicht erst nach einem Vorfall.

RIEDEL

Hackattacke auf Elektrotechnik-Firma: Finanz- und Kundendaten kompromittiert

27. Februar 2025, Villingen-Schwenningen/Baden-Württemberg

DATENDIEBSTAHL

RANSOMWARE

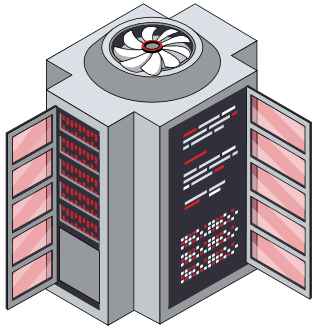
Was ist passiert?
Die Ransomware-Gruppe „Akira“ listete ein Elektrotechnik-Unternehmen als Opfer auf ihrem Darknet-Portal. Die Täter behaupten, mehr als 9 GB sensible Daten erbeutet zu haben, darunter Finanzinformationen sowie Kontaktinformationen von Mitarbeitern und Kunden.

Was hätte man besser machen können?
Die Einführung eines abgestuften Berechtigungskonzepts (Least Privilege) hätte den Zugriff auf sensible Dateien gezielter begrenzen können. In Kombination mit einer umfassenden Backup-Strategie, idealerweise offline und regelmäßig getestet, wäre auch die Wiederherstellung im Fall einer Verschlüsselung deutlich schneller und verlustärmer möglich gewesen.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8572-Akira-METAE2FOperations.png

Was lernen wir daraus:
Viele Angriffe starten mit dem Diebstahl von Zugangsdaten oder dem Ausnutzen veralteter Software. Wer regelmäßig prüft, welche Daten wirklich sensibel sind und wo sie liegen, kann effektiver priorisieren und schützen. Eine aktuelle Datenklassifizierung und ein Minimalprinzip beim Datenzugriff sind einfache, aber wirkungsvolle Maßnahmen für mehr Datensicherheit im Unternehmen.



RIEDEL

133 GB Firmendaten entwendet – Unternehmen nach Cyberattacke offline

27. Februar 2025, in Bad Salzuflen/Nordrhein-Westfalen

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Die Ransomware-Gruppe „Qilin“ listete ein mittelständisches Unternehmen aus Nordrhein-Westfalen als Opfer auf ihrer Darknet-Seite. Kurz darauf war die Webseite des Unternehmens nicht mehr erreichbar. Die Täter geben an, 133 GB sensible Daten erbeutet zu haben, darunter Personalinformationen, Lebensläufe, Rechnungen, Finanzdaten und Design-Dokumente.

Was hätte man besser machen können?
Ein umfassendes XDR-System hätte die vernetzten Sicherheitsdaten aus verschiedenen Quellen – etwa E-Mail, Endpunkten und Servern – korreliert und damit frühzeitig verdächtige Muster erkennen können. In Kombination mit einem SIEM-System und einer regelmäßigen Schwachstellenanalyse wäre es möglich gewesen, sowohl präventiv als auch reaktiv wirksam zu agieren.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8574-qilin-soco-system.png
https://www.security-incidents.de/assets/img/incidents/8574-qilin-soco-system-02.png

Was lernen wir daraus:
Viele Unternehmen unterschätzen den Schutzbedarf ihrer digitalen Assets. Dabei zeigt sich: Es lohnt sich, IT-Sicherheit als kontinuierlichen Prozess zu verstehen, nicht als einmalige Maßnahme. Regelmäßige Schulungen, Awareness-Kampagnen und die klare Definition von Verantwortlichkeiten im Notfallmanagement sind wichtige Bausteine, um die eigene Resilienz zu erhöhen.

RIEDEL

Cyberangriff auf Herz-Lungen-Praxis: 12.000 Patientendaten abgegriffen und verschlüsselt

26. Februar 2025, in Hamburg/Hamburg

DATENDIEBSTAHL

RANSOMWARE

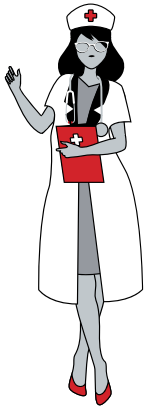
Was ist passiert?
Eine Herz-Lungen-Praxis aus Hamburg-Bergedorf, wurde Opfer eines mutmaßlichen Ransomware-Angriffs. Dabei wurden rund 12.000 Patientendaten entwendet und verschlüsselt. Die Wiederherstellung der IT-Systeme dauerte mehrere Wochen. Anschließend informierte das Zentrum die Betroffenen über den Vorfall.

Was hätte man besser machen können?
In medizinischen Einrichtungen sind sowohl Datenschutz als auch Ausfallsicherheit essenziell. Ein **EDR-System** hätte ungewöhnliches Verhalten auf Endgeräten, wie das Verschlüsseln von Dateien, frühzeitig erkennen und blockieren können. Ergänzend wären regelmäßige Offline-Backups und ein Notfallwiederherstellungsplan hilfreich gewesen, um die Ausfallzeit zu verkürzen.

Anzunehmende Schadensfelder:

Quellen:
https://www.shz.de/lokales/bargteheide-ahrensburg/artikel/hackerangriff-in-hamburg-12000-patientendaten-betroffen-48411581
https://www.abendblatt.de/schleswig-holstein/stormarn/article408420504/mvz-herz-lunge-opfer-eines-hackerangriffs.html

Was lernen wir daraus:
Mit der Umsetzung der NIS-2-Richtlinie rücken auch Einrichtungen mit kritischer Datenverarbeitung stärker in den Fokus der IT-Sicherheitsanforderungen. Die Richtlinie fordert unter anderem Risikomanagement, Incident Response, und Meldepflichten auch für den Gesundheitssektor. Wer frühzeitig mit strukturierten Sicherheitsmaßnahmen beginnt, ist nicht nur besser geschützt, sondern auch regulatorisch auf der sicheren Seite.



RIEDEL

Hacker verlangen 200.000 Dollar Lösegeld nach Cyberangriff auf Autobranche

25. Februar 2025, in Koblenz/Rheinland-Pfalz

DATENDIEBSTAHL

RANSOMWARE

ERPRESSUNG

SUPPLY CHAIN

Was ist passiert?
Die Ransomware-Gruppe „HellCat“ griff ein Marketing-Unternehmen aus der Autobranche an und veröffentlichte nach ausbleibender Zahlung von 200.000 US-Dollar rund 300.000 Datensätze (21 GB), darunter Infos bekannter Hersteller. Zudem sollen sie Zugriff auf weitere 18 GB eines anderen Autobauers erlangt haben. Die Daten wurden über ihre Darknet-Seite veröffentlicht.

Was hätte man besser machen können?
Unternehmen mit sensiblen Industriedaten sollten Zugriffsrechte und Datenflüsse kontinuierlich überwachen. Ein SIEM-System in Kombination mit einem Security Operations Center (SOC) hätte verdächtige Aktivitäten wie Datenabzug erkennen können. Präventive Schwachstellenanalysen helfen zudem, potenzielle Einfallstore frühzeitig zu identifizieren.

Anzunehmende Schadensfelder:

Was lernen wir daraus:
Datenlecks bei Dienstleistern wirken sich schnell auf ganze Branchen aus – in diesem Fall sogar auf bekannte Automobilhersteller. Wer mit vertraulichen Informationen Dritter arbeitet, trägt nicht nur eigene Verantwortung, sondern auch eine indirekte Haftung. Das zeigt, wie wichtig Sicherheitsanforderungen in Lieferverträgen und regelmäßige Audits entlang der gesamten Dienstleistungskette sind.

RIEDEL

Quellen:
https://www.security-incidents.de/assets/img/incidents/8573-hellcat-onedealer-03.png
https://www.security-incidents.de/assets/img/incidents/8573-hellcat-onedealer.png
https://www.security-incidents.de/assets/img/incidents/8573-hellcat-onedealer-02.png

Ransomware-Gruppe „CL0P“ attackiert Supply-Chain-Dienstleister

RANSOMWARE

24. Februar 2025, in Hallbergmoos/Bayern

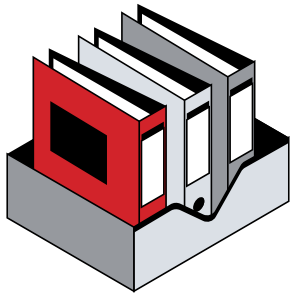
Was ist passiert?
Die Ransomware-Gang „CL0P“ listete einen deutschen Dienstleister für All-in-One-Supply-Chain-Lösungen als Opfer auf ihrer Darknet-Leakseite. Genaue Angaben zum Umfang oder zur Art der erbeuteten Daten machten die Täter allerdings nicht.

Was hätte man besser machen können?
Eine umfassende IT-Sicherheitsstrategie, die unter anderem ein **Extended Detection and Response (XDR)-System** sowie regelmäßige **Schwachstellenanalysen** umfasst, hätte helfen können, Angriffsversuche frühzeitig zu erkennen und abzuwehren. Auch die Segmentierung kritischer Systeme ist bei solchen Dienstleistern essenziell.

Anzunehmende Schadensfelder:

Quellen:
https://ransomfeed.it/index.php?page=post_details&id_post=21365
https://www.security-incidents.de/assets/img/incidents/8526-cl0p-supplyon.png

Was lernen wir daraus:
Angriffe ohne öffentlich bekannte Details zeigen, wie schwierig es ist, Risiken korrekt einzuschätzen, wenn Transparenz fehlt. Das unterstreicht die Bedeutung einer offenen Sicherheitskommunikation, intern wie extern. Unternehmen sollten klare Prozesse für Vorfallmanagement, Krisenkommunikation und Informationsweitergabe etablieren, um im Ernstfall schnell und glaubwürdig reagieren zu können.



RIEDEL

Hacker erbeuten sensible Daten bei IT-Firma aus Nordrhein-Westfalen

21. Februar 2025, in Velbert/Nordrhein-Westfalen

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

Was ist passiert?
Am 21. Februar 2025 meldete die Ransomware-Gruppe „Akira“ einen Angriff auf einen IT-Dienstleister aus Nordrhein-Westfalen. Die Täter geben an, vertrauliche Daten wie Geheimhaltungsvereinbarungen, Führerscheinkopien, Finanzinformationen sowie Mitarbeiter- und Kundendaten erbeutet zu haben.

Was hätte man besser machen können?
IT-Dienstleister sind besonders gefährdet, da sie Daten vieler Kunden verwalten. Tools wie Endpoint Detection and Response (EDR), regelmäßige Schwachstellenanalysen und zentrale Protokollauswertung via SIEM hätten verdächtige Aktivitäten frühzeitig erkennen und die Kompromittierung möglicherweise verhindern können.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8495-Akira-Insyst.png

Was lernen wir daraus:
Ein erfolgreicher Angriff auf einen IT-Dienstleister kann weitreichende Folgen für viele nachgelagerte Unternehmen haben. Deshalb ist nicht nur technischer Schutz entscheidend, sondern auch die vertragliche und organisatorische Absicherung: klare Regelungen zur Datenverarbeitung, Meldepflichten im Schadensfall und regelmäßige Sicherheitsüberprüfungen bei Drittanbietern sollten selbstverständlich sein.

RIEDEL

Cyberangriff: Unterricht an zwei Schulen massiv beeinträchtigt

21. Februar 2025, in Kehl/Baden-Württemberg

EINBRUCH

AUSFALL

Was ist passiert?
Eine Realschule in Kehl wurde Opfer eines Cyberangriffs. Aus Sicherheitsgründen wurde das IT-Netzwerk sofort abgeschaltet. Betroffen ist auch das benachbarte Gymnasium, dass das Netzwerk mitbenutzt. Beide Schulen sind aktuell digital eingeschränkt. Die Stadtverwaltung untersucht den Vorfall gemeinsam mit einer Cybersicherheitsagentur.

Was hätte man besser machen können?
Die gemeinsame IT-Infrastruktur zweier Schulen erhöht die Angriffsfläche und sollte vermieden werden. Zudem wäre ein **EDR-System** auf den Endgeräten hilfreich gewesen, um ungewöhnliches Verhalten zu erkennen und zu isolieren. Für Schulen und Schulträger, die keine eigene IT-Abteilung haben, sind Security-Lösungen als Managed Service grundsätzlich eine sinnvolle Option.

Anzunehmende Schadensfelder:

Quellen:
https://www.badische-zeitung.de/cyber-angriff-in-kehl

Was lernen wir daraus:
Cyberangriffe auf Bildungseinrichtungen zeigen, wie wichtig klare Zuständigkeiten und regelmäßige IT-Notfallübungen sind – gerade bei vernetzten Infrastrukturen wie gemeinsam genutzten Schulnetzwerken. Wer vorbereitet ist, kann im Ernstfall schneller reagieren, Ausfallzeiten minimieren und den Schulalltag zumindest teilweise aufrechterhalten. Auch eine Priorisierung der IT-Sicherheit in kommunalen Budgets ist essenziell.

RIEDEL

Daten einer deutschen Hochschule als Torrent-Link verfügbar

19. Februar 2025, in Trier/Rheinland-Pfalz

DATENDIEBSTAHL

RANSOMWARE

DATENLECK

Was ist passiert?
Am 19. Februar 2025 meldete die Ransomware-Gruppe „FOG“ eine Hochschule aus Trier als Opfer eines Cyberangriffs. Die Täter gaben an, rund 8 GB an sensiblen Daten erbeutet zu haben. Mittlerweile stehen die Daten im Darknet als Torrent-Datei zum Download zur Verfügung.

Was hätte man besser machen können?
In einem Hochschulumfeld mit vielen Einzelsystemen ist zentrale Sicherheitsüberwachung entscheidend. Ein SOC mit 24/7-Monitoring und ein automatisiertes SOAR-System können verdächtige Aktivitäten früh erkennen und Gegenmaßnahmen automatisch einleiten, für mehr Sicherheit und schnellere Reaktion.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8456-hochschule-trier-fog.png

Was lernen wir daraus:
Forschungs- und Bildungseinrichtungen müssen sich nicht nur gegen Sabotage, sondern auch gegen gezielte Datenexfiltration absichern, um die Integrität ihres Betriebs und die Vertraulichkeit akademischer Daten zu gewährleisten.

RIEDEL

Cyberkriminelle erbeuten sensible Daten bei deutschem Kabelproduzenten

19. Februar 2025, in Mannheim/ Baden-Württemberg

DATENDIEBSTAHL

RANSOMWARE

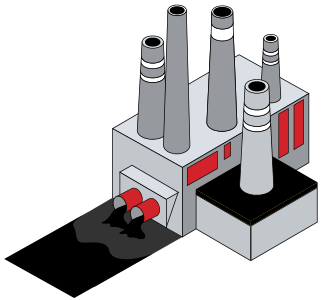
Was ist passiert?
Am 19. Februar 2025 meldete die Cyberkriminelle Gruppe „Akira“ einen Angriff auf einen deutschen Kabelproduzenten. Laut eigener Aussage erbeuteten die Täter rund 27 GB sensible Daten, darunter finanzielle Dokumente, Geheimhaltungsvereinbarungen, E-Mail-Adressen und weitere Kundendaten.

Was hätte man besser machen können?
Besonders produzierende Unternehmen sollten ihre Cybersecurity-Strategien regelmäßig durch Penetrationstests und Sicherheitsaudits überprüfen lassen. Insbesondere im industriellen Umfeld ist es wichtig, die Trennung zwischen OT (Operational Technology) und IT konsequent umzusetzen und zu überwachen.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8473-Akira-SuedKabel.PNG

Was lernen wir daraus:
Das erbeutete Datenpaket enthält nicht nur interne Unternehmensdaten, sondern auch Kundendaten, ein potenzieller Reputationsschaden mit rechtlichen Implikationen, etwa nach der DSGVO. Die Gruppe Akira ist seit 2023 aktiv und bekannt dafür, sowohl Windows- als auch Linux-Systeme zu kompromittieren. Auffällig ist ihre Strategie, gezielt mittelständische Unternehmen mit internationaler Geschäftstätigkeit ins Visier zu nehmen.



RIEDEL

Sensible Daten eines gemeinnützigen Vereins veröffentlicht

17. Februar 2025, in Köln/Nordrhein-Westfalen

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

Was ist passiert?
Seit dem 17. Februar 2025 führt die Ransomware-Gruppe „PLAY“ ein gemeinnütziges Unternehmen auf ihrer Darknet-Seite als Opfer. Die Angreifer behaupten, vertrauliche Daten wie Budget-, Lohn- und Steuerunterlagen, Ausweiskopien sowie Finanz- und Kundendaten erbeutet zu haben.

Was hätte man besser machen können?
Für Verbände, Vereine und andere zivilgesellschaftliche Organisationen gilt: Auch ohne große IT-Abteilungen ist ein Basisschutz essenziell. Dazu gehören regelmäßige Backups, die getrennt vom Hauptsystem gespeichert werden, sowie ein klar dokumentierter Notfallplan für Cybervorfälle.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8435-rheinischer-schuetzenbund-play.png
https://www.security-incidents.de/assets/img/incidents/8435-rheinischer-schuetzenbund-play-03.png

Was lernen wir daraus:
Eine wirksame Cybersicherheitsstrategie erfordert einen ganzheitlichen Ansatz. Regelmäßige Risikoanalysen decken Schwachstellen auf, klare Sicherheitsvorgaben regeln den Umgang mit sensiblen Daten, und strukturierte Notfallpläne sichern im Ernstfall eine schnelle Reaktion. So bleibt die IT-Infrastruktur widerstandsfähig gegenüber Angriffen.

RIEDEL

Quellcode falsch verladen: Ransomware trifft Logistikplattform

16. Februar 2025, in Leipzig/Sachsen

DATENDIEBSTAHL
RANSOMWARE
EINBRUCH
DATENLECK

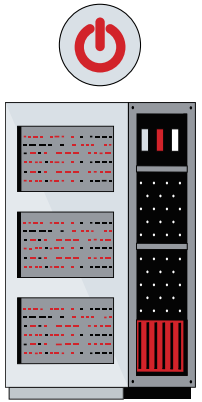
Was ist passiert?
Ein Leipziger Unternehmen für digitale Logistiklösungen wurde Opfer eines Ransomware-Angriffs. Seit dem 16. Februar listet die Gruppe „FOG“ es auf ihrer Darknet-Seite und veröffentlichte 7 GB Quellcode – vermutlich aus kompromittierten Gitlab-Repositories. Die Plattform vernetzt Speditionen und Verlader und bietet eine Vergleichs- und Buchungsfunktion für Transporte.

Was hätte man besser machen können?
Eine 24/7-Überwachung durch ein Security Operations Center (SOC) hätte ungewöhnliche Aktivitäten schnell feststellen und melden können. Automatisierte (SOAR) hätten zudem sofort Gegenmaßnahmen einleiten und so Schäden begrenzen können.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8417-FOG-PamyraDE.png

Was lernen wir daraus:
Ransomware-Angriffe gehören zu den gravierendsten Cyberbedrohungen und zielen darauf ab, Organisationen durch Verschlüsselung ihrer Daten zu erpressen. Die Täter drohen oft mit Veröffentlichung sensibler Informationen, falls das Lösegeld nicht gezahlt wird. Um sich zu schützen, sind regelmäßige Backups, Mitarbeiterschulungen und umfassende Sicherheitsstrategien essenziell.



RIEDEL

Cyberangriff auf Cloud- und KI-Spezialisten – FOG-Gruppe bekennt sich

16. Februar 2025, in München/Bayern

DATENDIEBSTAHL
SICHERHEITSLÜCKE
EINBRUCH
DATENLECK

Was ist passiert?
Ein Münchner Softwareunternehmen, spezialisiert auf Cloud, KI und Digitalisierung, wurde offenbar Opfer eines Ransomware-Angriffs. Die Gruppe „FOG“ listet das Unternehmen am 16. Februar 2025 auf ihrer Darknet-Seite und veröffentlichte 7 GB Quellcode per Torrent – vermutlich aus kompromittierten Gitlab-Repositories.

Was hätte man besser machen können?
Die Kompromittierung eines GitLab-Servers lässt sich oft auf unzureichende Zugriffskontrollen, veraltete Softwarestände oder mangelhafte Überwachung zurückführen. Ein zentraler Hebel zur Prävention sind regelmäßige Sicherheits-Audits, die Konfiguration, Zugriffsrechte und Schwachstellen in Repositorien und Entwicklungsumgebungen systematisch prüfen.

Anzunehmende Schadensfelder:

Was lernen wir daraus:
Bei einem Softwareunternehmen, das sich auf Cloud, KI und Digitalisierung spezialisiert, kann der Quellcode nicht nur Geschäftsgeheimnisse enthalten, sondern auch sicherheitskritische Algorithmen und kundenspezifische Lösungen. Der Verlust solcher Daten gefährdet nicht nur die Wettbewerbsfähigkeit, sondern kann auch die Sicherheit der Kundenlösungen beeinträchtigen – insbesondere wenn der veröffentlichte Code Sicherheitslücken offenbart.

RIEDEL

Quellen:
https://www.security-incidents.de/assets/img/incidents/8418-FOG-QBurst.png

Bayerische Ministerien nach DDoS-Angriff nicht erreichbar

14. Februar 2025, in München/Bayern

DDoS

AUSFALL

Was ist passiert?
Am 14. Februar 2025 waren mehrere Regierungswebseiten vorübergehend nicht erreichbar – verursacht durch einen koordinierten Distributed-Denial-of-Service (DDoS)-Angriff. Während die internen Systeme laut offiziellen Angaben unversehrt blieben, deuten erste Hinweise auf eine politisch motivierte Urheberschaft hin.

Was hätte man besser machen können?
Ein effektiver Schutz gegen Distributed Denial of Service-Angriffe (DDoS) erfordert spezialisierte Abwehrmechanismen wie vorgelagerte Filter, Lastverteilung und Traffic-Analyse in Echtzeit. Solche Schutzmaßnahmen lassen sich durch ein **SIEM-System** (Security Information and Event Management) sinnvoll ergänzen, das ungewöhnliche Zugriffsmuster frühzeitig meldet – besonders bei öffentlichen Webportalen.

Anzunehmende Schadensfelder:

Quellen:
https://www.br.de/nachrichten/bayern/prorussische-cyberattacke-auf-staatsregierung-und-polizei,UcnL8gT
https://www.faz.net/agenturmeldungen/dpa/websites-der-bayerischen-staatsregierung-gehackt-110301041.html

Was lernen wir daraus:
DDoS-Angriffe dienen oft weniger der Datenmanipulation als vielmehr der Störung und Symbolik – insbesondere bei staatlichen Stellen. Sie zeigen, wie schnell digitale Erreichbarkeit gezielt blockiert werden kann. Daher sollten auch Behörden mit hohem Publikumsverkehr in Ausfallsicherheit und Notfallkommunikation investieren – z. B. durch Alternativzugänge oder redundante Systeme.

RIEDEL

Webseite einer Stadtverwaltung nach DDoS-Attacke nicht erreichbar

DDoS

AUSFALL

14. Februar 2025, in Garching/Bayern

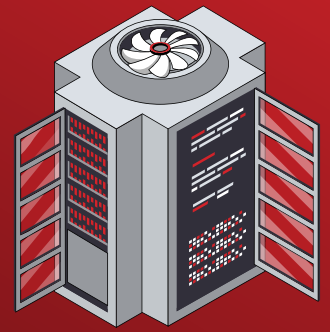
Was ist passiert?
Die Webseite einer bayerischen Stadtverwaltung wurde durch eine DDoS-Attacke massiv gestört. Die Überlastung führte dazu, dass die Seite bis in die Abendstunden nicht erreichbar war. Der zuständige IT-Dienstleister reagierte mit einer temporären Umleitung auf eine Ausweichseite, um zumindest grundlegende Informationen bereitzustellen.

Was hätte man besser machen können?
Ein strukturierter Incident Response-Plan inklusive vordefinierter Notfallseiten und Kommunikationskanäle hätte helfen können, schneller zu reagieren. In Kombination mit einem Security Operations Center (SOC), das rund um die Uhr arbeitet, lassen sich DDoS-Attacken rascher erkennen und analysieren. Frühzeitige Traffic-Filterung kann die Auswirkungen deutlich reduzieren.

Anzunehmende Schadensfelder:

Quellen:
https://www.merkur.de/lokales/muenchen-lk/garching-ort28709/webseite-stundenlang-nicht-erreichbar-cyberangriff-auf-homepage-der-stadt-garching-93570995.html
https://www.sueddeutsche.de/muenchen/landkreismuenchen/garching-landratsamt-muenchen-cyberangriff-li.3202254

Was lernen wir daraus:
Auch kleinere Kommunen geraten zunehmend ins Visier von DDoS-Attacken, sei es als politisches Signal oder Teil automatisierter Angriffsserien. Technische Maßnahmen allein reichen nicht aus: Es braucht klare Abläufe für Krisenkommunikation, abgestimmte Zuständigkeiten zwischen Verwaltung und IT-Dienstleistern sowie eine Sensibilisierung für digitale Störszenarien im öffentlichen Raum.



RIEDEL

Cyberangriff auf militärische Universität: Möglicher Datenabfluss sensibler Infos

13. Februar 2025, in München/Bayern

EINBRUCH

DATENPANNE

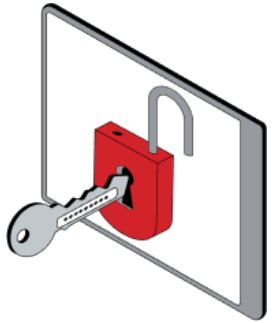
Was ist passiert?
Cyberkriminelle haben erfolgreich einen IT-Dienst des Rechenzentrums einer Universität der Bundeswehr kompromittiert. Zwar kam es laut Bundeswehr nicht zu Datenlöschung oder Verschlüsselung, jedoch könnten laut Medienberichten sensible personenbezogene Daten – etwa Handynummern und Bankverbindungen – von Studierenden und Dozierenden betroffen sein.

Was hätte man besser machen können?
Ein Extended Detection and Response-System (XDR) hätte potenziell verdächtige Aktivitäten über verschiedene IT-Komponenten hinweg frühzeitig korreliert und Alarm geschlagen – etwa bei untypischem Zugriff auf personenbezogene Daten. In sicherheitsrelevanten Umfeldern wie militärnahen Einrichtungen sollte zudem eine kontinuierliche 24/7-Überwachung durch ein Security Operations Center (SOC) Standard sein.

Anzunehmende Schadensfelder:

Quellen:
https://www.handelsblatt.com/politik/deutschland/cyberkriminalitaet-hackerangriff-auf-die-universitaet-der-bundeswehr/100107638.html
https://www.heise.de//news/Cyberattacke-auf-die-Universitaet-der-Bundeswehr-Muenchen-10281927.html

Was lernen wir daraus:
Nicht jeder Cyberangriff zielt auf Zerstörung oder Erpressung, oft steht der stille Zugriff auf personenbezogene Daten im Fokus. Gerade Universitäten mit sicherheitsrelevanten Aufgaben wie die Universität der Bundeswehr verwalten sensible Informationen, was sie zu attraktiven Zielen macht.



RIEDEL

DDoS-Attacke legt Polizei-Website und Behördenserver lahm

13. Februar 2025, in Bremen/Bremen

DDoS

AUSFALL

Was ist passiert?
Die Website der Polizei einer norddeutschen Stadt wurde Ziel eines DDoS-Angriffs mit bis zu 18.000 Anfragen pro Minute. Auch weitere Verwaltungsseiten wie Rathaus und Ressorts waren vorübergehend offline. Eine russische Hackergruppe bekannte sich zum Angriff. Zwar wurden keine Daten gestohlen, die Störungen dauerten bis in den Abend.

Was hätte man besser machen können?
Ein SIEM-System hätte die ungewöhnlich hohe Zugriffszahl früh erkannt und automatisiert eskaliert. Ein vorgelagerter DDoS-Schutz mit Load-Balancing hätte die Erreichbarkeit kritischer Verwaltungsportale sichern können. Besonders bei öffentlich sichtbarer Infrastruktur sollte die Belastbarkeit regelmäßig getestet werden.

Anzunehmende Schadensfelder:

Quellen:
https://www.behoerden-spiegel.de/2025/02/13/bremen-wehrt-russischen-dos-angriff-ab/
https://www.tagesschau.de/inland/regional/bremen/rb-cyberangriff-auf-webseiten-des-bremer-senats-abgewehrt-100.html

Was lernen wir daraus:
DDoS-Angriffe (Distributed Denial of Service) sind keine direkten Einbrüche in Systeme, sondern Überlastungsangriffe: Sie zielen darauf ab, Dienste durch massenhafte Anfragen lahmzulegen. Häufig werden dafür Botnetze genutzt – also gekaperte Geräte weltweit. Auch ohne Datenverlust können solche Angriffe erheblichen Reputations- und Vertrauensschaden verursachen, insbesondere bei öffentlichen Stellen mit Informationspflicht.

RIEDEL

Cyberangriff zwingt Firma zu Systemabschaltung und Notbetrieb

13. Februar 2025, in Berlin/Berlin

EINBRUCH

AUSFALL

Was ist passiert?
Am 13. Februar 2025 meldete ein international tätiges Unternehmen aus dem Bereich Medizintechnik und Strahlenanwendung einen Cyberangriff. Als Reaktion wurden Teile der Systeme vorsorglich abgeschaltet. Die Website zeigt seitdem Warnhinweise zu Störungen bei E-Mail- und Telefonkommunikation, alternative Kontaktwege wurden eingerichtet.

Was hätte man besser machen können?
Eine mehrstufige Verteidigung mit **EDR** hätte den Angriff frühzeitig eingrenzen können, bevor Systeme abgeschaltet werden mussten. Ergänzend kann ein rund um die Uhr betriebenes **SOC** ungewöhnliche Muster erkennen und sofortige Gegenmaßnahmen koordinieren für mehr Sicherheit bei kritischer Infrastruktur.

Anzunehmende Schadensfelder:

Quellen:
https://www.ezag.com/de/presse/detail/?newsid=2936843
https://www.security-incidents.de/assets/img/incidents/8429-eckert-ziegler-cyberangriff.png

Was lernen wir daraus:
Cyberangriffe auf Unternehmen im medizinischen Umfeld sind besonders kritisch, da Ausfälle nicht nur wirtschaftlich, sondern auch versorgungsrelevant sein können. Der Fall zeigt, wie wichtig funktionierende Notfallkommunikation ist, etwa durch alternative Kontaktkanäle. Zudem rückt das Thema Cyberresilienz in den Fokus: Unternehmen müssen nicht nur Angriffe abwehren, sondern auch im Krisenfall handlungsfähig bleiben.

RIEDEL

Kundendaten und Finanzdokumente bei Cyberangriff erbeutet

12. Februar 2025, in Burbach-Wahlbach/Nordrhein-Westfalen

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

Was ist passiert?
Am 12. Februar 2025 wurde ein deutscher Bürobedarf-Anbieter von der Ransomware-Gruppe „Fog“ als Opfer eines Cyberangriffs auf ihrer Leak-Seite aufgeführt. Die Angreifer behaupten, 6,5 GB an Daten entwendet zu haben, darunter interne Finanzunterlagen, E-Mail-Korrespondenz sowie Kunden- und Mitarbeiterdaten mit Adressinformationen.

Was hätte man besser machen können?
Ein durchdachtes Rechte- und Zugriffskonzept (Least Privilege) hätte helfen können, den Schaden zu begrenzen, indem sensible Finanz- und Personendaten nur gezielt zugänglich gewesen wären. Auch regelmäßige Backups – getrennt vom operativen Netz – und deren Wiederherstellungstests sind entscheidend, um im Angriffsfall nicht erpressbar zu sein.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8371-hess-gmbh-fog.png

Was lernen wir daraus:
Viele Unternehmen unterschätzen den wirtschaftlichen Wert ihrer internen Daten. Doch E-Mails, Adressdaten und Geschäftszahlen sind für Angreifer attraktiv – sei es zur Erpressung oder zum Weiterverkauf. Der Fall verdeutlicht, wie eng IT-Sicherheit mit Datenschutz und Compliance verknüpft ist. Unternehmen jeder Branche und Größe sollten sich regelmäßig fragen: Welche Daten habe ich – und wie schütze ich sie konkret?

RIEDEL

Kritische Störung: 112 und 110 vorübergehend nicht erreichbar

AUSFALL

12. Februar 2025, in Köln/Nordrhein-Westfalen

Was ist passiert?
Am 12. Februar 2025 fiel ein regionaler Telekommunikationsanbieter ganztägig aus. Zwischen 9:00 und 17:15 Uhr waren viele Dienste betroffen, darunter auch die Notrufnummern 110 und 112, die zeitweise nicht erreichbar waren und später umgeleitet wurden. Auch am Flughafen Köln-Bonn kam es zu Einschränkungen, der Betrieb lief jedoch weiter.

Was hätte man besser machen können?
Kritische Infrastrukturen wie die Notrufkommunikation benötigen redundante Systeme mit automatischer Umschaltung im Störungsfall (Failover). Eine regelmäßige Überprüfung solcher Notfallszenarien gehört zum Pflichtprogramm.

Anzunehmende Schadensfelder:

Quellen:
https://ga.de/news/panorama/stoerung-bei-netcologne-behoben-koeln-bonn_aid-124081227
https://rp-online.de/wirtschaft/unternehmen/netcologne-stoerung-bei-internet-telefon-und-notruf-behoben_aid-124080033

Was lernen wir daraus:
Der Ausfall zeigt, wie stark unsere Gesellschaft auf funktionierende Kommunikationsnetze angewiesen ist, besonders im Notfall. Ein einzelner Fehler kann weitreichende Folgen haben. In sicherheitskritischen Bereichen sollte daher nicht nur die technische, sondern auch die organisatorische Resilienz regelmäßig getestet werden, etwa durch Stresstests und Notfallübungen in Zusammenarbeit mit Behörden und Partnern.

RIEDEL

Cyberangriff auf Justiz-Dienstleister: Insassen ohne Telefon und TV

12. Februar 2025, in Hamburg/Hamburg

DATENDIEBSTAHL

RANSOMWARE

AUSFALL

SUPPLY CHAIN

Was ist passiert?
Ein Ransomware-Angriff auf den IT-Dienstleister der Brandenburger JVA führte Anfang Februar 2025 zum Ausfall von Telefonie und TV für Inhaftierte. Tablets und Mediaboxen wurden abgeschaltet. Übergangsweise verteilte man DVDs und Spiele. Später wurde bekannt, dass auch sensible Mitarbeiterdaten wie Gesundheits- und Finanzinfos betroffen waren. Ende Februar lief der TV-Empfang teilweise wieder.

Was hätte man besser machen können?
Hätte ein XDR-System im Einsatz gewesen, wären verdächtige Aktivitäten womöglich früh erkannt und isoliert worden. Mit Unterstützung eines SOCs, das rund um die Uhr überwacht, hätte der Angriff schneller eingedämmt werden können. Eine clevere Netzwerksegmentierung hätte zudem kritische Verwaltungsdaten besser geschützt und den Schaden begrenzt.

Anzunehmende Schadensfelder:

Was lernen wir daraus:
Digitale Dienste sind längst fester Bestandteil selbst in sicherheitsrelevanten Einrichtungen wie Gefängnissen. Der Vorfall zeigt, dass Ausfälle in diesen Systemen nicht nur funktionale, sondern auch soziale Auswirkungen haben können. Gleichzeitig unterstreicht der Abfluss von Mitarbeiterdaten, wie sensibel Justizinfrastrukturen sind – und dass Datenschutz auch im geschlossenen System höchste Priorität haben muss. Hier verschwimmen IT-Sicherheit, Menschenwürde und staatliche Verantwortung.

RIEDEL

Quellen:
https://tel.io/de/2025/02/12/informationsschreiben-gemaess-art-34-dsgvo-an-ehemalige-mitarbeiter/
https://www.maz-online.de/brandenburg/telio-unter-beschuss-hackerangriff-legt-telefone-und-tv-in-gefaengnissen-lahm-WCXTBSZXTNFANKKHRUISM7BQKA.html

Cyberangriff auf kirchliche Institution legt IT-Systeme lahm

11. Februar 2025, in Berlin/Berlin

EINBRUCH

AUSFALL

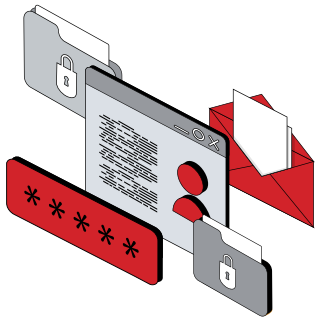
Was ist passiert?
Am 10. Februar 2025 wurde das Sekretariat einer zentralen kirchlichen Organisation Opfer eines Cyberangriffs. Die IT-Systeme wurden vorsorglich abgeschaltet, was auch die E-Mail-Kommunikation einschränkte. Eine professionelle Hackergruppe bekannte sich zur Tat. Technische Details wurden nicht veröffentlicht, eine Ransomware-Attacke gilt als wahrscheinlich.

Was hätte man besser machen können?
In komplexen IT-Umgebungen mit hohem Kommunikationsaufkommen zählt jede Minute. Eine **SOAR**-Plattform hätte automatisiert auf bekannte Bedrohungen reagieren und betroffene Systeme isolieren können. Zusammen mit einem rund um die Uhr aktiven **SOC** und **EDR**-Lösungen wäre die Reaktionszeit deutlich verkürzt worden und der Schaden womöglich geringer ausgefallen.

Anzunehmende Schadensfelder:

Quellen:
https://www.dbk.de/presse/aktuelles/meldung/cyberangriff-auf-die-it-systeme-des-sekretariats-der-deutschen-bischofskonferenz
https://www.domradio.de/artikel/cyberangriff-auf-deutsche-bischofskonferenz

Was lernen wir daraus:
Auch gesellschaftliche Institutionen wie Kirchen sind zunehmend Ziel professioneller Angreifer, oft wegen ihrer Netzwerke, Spendenverwaltung oder ihrer gesellschaftlichen Sichtbarkeit. Der Vorfall zeigt, dass Cybersicherheit längst keine rein technische Aufgabe mehr ist, sondern zum Selbstverständnis jeder Organisation gehören muss, unabhängig von Branche oder Größe.



RIEDEL

Verträge, SQL-Dateien und Angebote im Netz – Cyberangriff endet mit Datenleck

11. Februar 2025, in Kropp/Schleswig-Holstein

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

Was ist passiert?
Ein deutsches Ingenieurbüro für technische Gebäudeplanung wurde Ziel eines Ransomware-Angriffs. Die Täter, die sich der Gruppe „Sarcoma“ zuordnen, entwendeten rund 166 GB an sensiblen Daten – darunter Verträge, Angebote und SQL-Datenbanken. Sie setzten eine Frist und veröffentlichten nach ihrem Ablauf die Daten auf ihrer Leak-Seite im Darknet.

Was hätte man besser machen können?
Ein effektives Berechtigungsmanagement hätte den Zugriff auf sensible Daten wie SQL-Datenbanken oder Vertragsdokumente stärker einschränken können. Darüber hinaus wäre ein strukturierter Notfallplan mit regelmäßigen Wiederherstellungstests entscheidend gewesen, um auf den Fristablauf vorbereitet zu sein.

Was lernen wir daraus:
Technische Dienstleister unterschätzen oft die Attraktivität ihrer Daten für Angreifer, vor allem wenn Projekte öffentliche oder kritische Infrastruktur betreffen. Darüber hinaus zeigt der Fall die Notwendigkeit strukturierter Backup-Strategien und klar definierter Reaktionsprotokolle. Wer vertrauliche Projektinformationen digital verwaltet, sollte sich regelmäßig mit Fragen der Zugriffssicherung, Verschlüsselung und Risikobewertung auseinandersetzen.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8380-Sarcoma-WisperReimerIng_01.png
https://www.security-incidents.de/assets/img/incidents/8380-Sarcoma-WisperReimerIng_02.png

RIEDEL

Cyberangriff auf Ersatzteilspezialist – Gehalts- und Kundendaten veröffentlicht

11. Februar 2025, in Euskirchen/Nordrhein-Westfalen

DATENDIEBSTAHL
RANSOMWARE
EINBRUCH
AUSFALL

Was ist passiert?
Ein deutsches Ingenieurbüro wurde offenbar von der Ransomware-Gruppe „Sarcoma“ angegriffen. Am 11. Februar 2025 tauchte es auf deren Darknet-Portal auf. Die Angreifer behaupten, 166 GB vertraulicher Daten erbeutet zu haben, darunter Verträge und SQL-Dateien. Sie setzten eine Frist bis zum 19. Februar, andernfalls droht die Veröffentlichung.

Was hätte man besser machen können?
Für Unternehmen mit hohem Datenverkehr und sensiblen Informationen lohnt sich ein **SIEM-System**, das sicherheitsrelevante Logdaten bündelt und verdächtige Aktivitäten früh sichtbar macht. Ergänzend hätte ein Zero-Trust-Ansatz den Zugriff auf sensible Kunden- und Finanzdaten stärker reglementiert und so das Risiko deutlich reduziert.

Anzunehmende Schadensfelder:

Was lernen wir daraus:
Cyberkriminelle nutzen gezielt Druckmittel wie Leak-Seiten, um Unternehmen zur Zahlung zu bewegen. Das zeigt: Ein reines Reagieren reicht oft nicht – Prävention und Transparenz gegenüber Kunden sind entscheidend. Unternehmen sollten zudem regelmäßig prüfen, welche sensiblen Daten wie lange gespeichert und wie sie geschützt werden. Auch eine professionelle Krisenkommunikation sollte fester Bestandteil der IT-Sicherheitsstrategie sein.

RIEDEL

Quellen:
https://www.security-incidents.de/assets/img/incidents/8406-Play-ratioparts.png
https://www.security-incidents.de/assets/img/incidents/8406-Play-ratioparts_2.png
https://www.security-incidents.de/assets/img/incidents/8406-Play-ratioparts_02

Ransomware-Gruppe droht mit Veröffentlichung von fast einem Terabyte Firmendaten

10. Februar 2025, in Rabenau/Sachsen

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

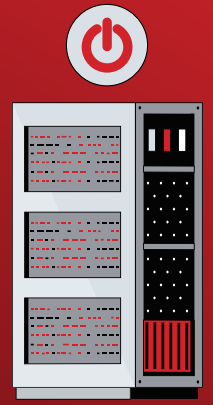
Was ist passiert?
Ein deutsches Unternehmen aus der Möbelbranche wurde auf der Leak-Seite der Ransomware-Gruppe „Sarcoma“ gelistet. Die Angreifer behaupten, fast ein Terabyte an sensiblen Unternehmensdaten erbeutet zu haben, darunter Dateien aus SQL-Datenbanken und E-Mail-Kommunikation. Um ihre Drohungen zu untermauern, veröffentlichten sie Screenshots und setzten eine Frist zur Zahlung.

Was hätte man besser machen können?
Ein strukturierter Schwachstellenmanagement-Prozess inklusive regelmäßiger Sicherheitsüberprüfungen hätte potenzielle Einfallstore identifizieren können – etwa durch veraltete SQL-Instanzen oder fehlerhafte Mailserver-Konfigurationen. Zusätzlich kann eine Endpoint Detection and Response-Lösung (EDR) verdächtige Aktivitäten direkt an den Endpunkten erkennen und isolieren, bevor größerer Schaden entsteht.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8347-Sarcoma-Oelsa_1.png
https://www.security-incidents.de/assets/img/incidents/8347-Sarcoma-Oelsa_2.png

Was lernen wir daraus:
Die Kombination aus entwendeten Daten und gezieltem Druckaufbau durch Veröffentlichung von Beweisen ist typisch für Ransomware-Gruppen. Für Unternehmen bedeutet das: Die Sicherheitsstrategie darf sich nicht nur auf den Schutz vor Angriffen beschränken, sondern muss auch Maßnahmen zur Abwehr von Erpressungsversuchen und zur Schadensbegrenzung nach einem Vorfall beinhalten. Dazu zählen auch Kommunikationspläne und rechtliche Bewertungen im Krisenfall.



RIEDEL

Ransomware trifft Gesundheitswesen – Angreifer fordern Millionenbetrag

10. Februar 2025, in Ludwigslust-Parchim/Mecklenburg-Vorpommern

RANSOMWARE
ERPRESSUNG
EINBRUCH
AUSFALL

Was ist passiert?
Ein Klinikverbund in Norddeutschland wurde Ziel eines Cyberangriffs durch die Gruppe „INC Ransom“. Zwei Standorte wurden vorsorglich vom Netz genommen, der Notbetrieb lief weiter. Die Angreifer forderten ein Millionen-Lösegeld, das nicht gezahlt wurde. Inzwischen wurden entwendete Daten veröffentlicht, laut Behörden ohne direkten Personenbezug.

Was hätte man besser machen können?
Gerade im Umfeld kritischer Infrastrukturen ist ein abgestuftes Sicherheitskonzept entscheidend. Dazu gehört unter anderem eine ständige **Überwachung** sensibler Systeme, gekoppelt mit automatisierten Alarmierungs- und Reaktionsmechanismen (z. B. durch **SOAR** – Security Orchestration, Automation and Response). Auch Segmentierung der Netzwerke kann helfen, die Ausbreitung eines Angriffs zu begrenzen und besonders sensible Systeme abzuschirmen.

Anzunehmende Schadensfelder:

Quellen:
https://www.heise.de//news/Lup-Kliniken-von-Cyberangriff-betroffen-10277022.html
https://www.security-incidents.de/assets/img/incidents/8353-inc-ransom-lup-kliniken-ludwigslust-pachim.png

Was lernen wir daraus:
Cyberangriffe auf das Gesundheitswesen nehmen weltweit zu – und oft geht es dabei nicht nur um Daten, sondern auch um Erpressung mit dem Risiko realer Versorgungsengpässe. Kliniken und Pflegeeinrichtungen sollten ihre Sicherheitsstrategie nicht als bloße IT-Aufgabe sehen, sondern als Teil des täglichen Risikomanagements.

RIEDEL

IT-Ausfall am Stichtag: Steuer-Software versagt bei Fristende

AUSFALL

10. Februar 2025, in Nürnberg/Bayern

Was ist passiert?
Bei einem großen IT-Dienstleisters im Steuerwesen, kam es zu weitreichenden Störungen bei den Anwendungen. Besonders brisant: Der Ausfall traf ausgerechnet am letzten Tag für die fristgerechte Abgabe der Umsatzsteuervoranmeldungen ein. Zahlreiche Steuerkanzleien und Mandanten konnten ihre Meldungen dadurch nicht rechtzeitig übermitteln. Die genaue Ursache der Störung ist nicht bekannt.

Was hätte man besser machen können?
Bei der Bereitstellung kritischer IT-Dienste ist eine resiliente Infrastruktur unerlässlich. Hochverfügbarkeitslösungen, wie Lastverteilung und geo-redundante Rechenzentren, hätten die Auswirkungen des Ausfalls mindern können. Zudem wäre ein gut vorbereitetes Notfallkommunikationssystem hilfreich gewesen, um betroffene Nutzer frühzeitig über Alternativen und Fristverlängerungen zu informieren.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8408-DATEV-Ausfall.png

Was lernen wir daraus:
Digitale Abhängigkeiten erfordern stabile und skalierbare Systeme, besonders bei gesetzlich gebundenen Fristen. Dieser Fall zeigt, wie schnell technische Probleme auch juristische oder wirtschaftliche Folgen nach sich ziehen können. Unternehmen sollten regelmäßig überprüfen, wie robust ihre Systeme bei Spitzenlasten sind und wie sie im Notfall reagieren und kommunizieren können.

RIEDEL

Erpressung ohne Erfolg: Hacker machen gestohlene Firmendaten öffentlich

8. Februar 2025, in Büren-Ahden/Nordrhein-Westfalen

DATENDIEBSTAHL
RANSOMWARE
EINBRUCH
DATENHEHLEREI

Was ist passiert?
Ein deutsches Unternehmen aus der Luftfahrtwartung wurde Ziel eines Ransomware-Angriffs durch die Gruppe „Medusa“. Die Erpresser forderten 100.000 US-Dollar oder täglich 10.000 für eine Fristverlängerung. Da keine Zahlung erfolgte, wurden die gestohlenen Daten nach Ablauf der Frist auf einer Leak-Seite veröffentlicht.

Was hätte man besser machen können?
Ein **EDR-System** hätte verdächtiges Verhalten auf betroffenen Endgeräten frühzeitig erkennen und eindämmen können. Ergänzend dazu hätte eine **SOAR-Plattform** automatisiert auf Ransomware-Indikatoren reagieren und Gegenmaßnahmen einleiten können – etwa das Trennen kompromittierter Systeme, um Datenabfluss zu verhindern.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8348-Medusa-Pad_1.png
https://www.security-incidents.de/assets/img/incidents/8348-Medusa-Pad_2.png

Was lernen wir daraus:
Ransomware-Angriffe richten sich zunehmend gegen Betriebe mit hohem Schutzbedarf, etwa aus Luftfahrt, Gesundheitswesen oder Infrastruktur. Neben technischen Schutzmaßnahmen sollten Unternehmen auch regelmäßig prüfen, ob ihr Umgang mit Lösegeldforderungen strategisch und juristisch durchdacht ist. Prävention, Wiederherstellbarkeit und rechtliche Bewertung gehören fest in jedes Sicherheitskonzept.

RIEDEL

Sicherheitsleck bei Fluggastrechte-Plattform – Datenbank kurzfristig einsehbar

7. Februar 2025, in Hamburg/Hamburg

DATENPANNE

EINBRUCH

SICHERHEITSLÜCKE

Was ist passiert?
Ein Sicherheitsforscher entdeckte bei einem juristischen Online-Dienstleister für Fluggastrechte eine ungeschützte Datenbank. Die Schwachstelle ermöglichte unbefugten Zugriff auf sensible Inhalte. Nach der Meldung durch den Forscher wurde die Lücke noch am selben Tag geschlossen.

Was hätte man besser machen können?
Eine sichere Konfiguration von Datenbanksystemen sollte von Beginn an Teil des Entwicklungsprozesses sein. Dazu gehören Zugangsbeschränkungen, Authentifizierungspflichten und regelmäßige Überprüfungen durch automatisierte Tools.

Anzunehmende Schadensfelder:

Quellen:
https://www.heise.de//news/Sicherheitsexperten-enthuellen-triviale-Datenlecks-bei-Legaltechs-10272273.html

Was lernen wir daraus:
Offen zugängliche Datenbanken gehören zu den häufigsten und vermeidbarsten Sicherheitsrisiken. Oft entstehen sie durch Fehlkonfigurationen. Das Beispiel zeigt, wie wichtig die Zusammenarbeit mit Sicherheitsforschenden ist: Responsible Disclosure schützt nicht nur betroffene Unternehmen, sondern auch die Daten unbeteiligter Nutzer. Transparente Prozesse und schnelle Reaktion sind dabei entscheidend.

RIEDEL

Datenpanne bei Legal-Tech-Anbieter – sensible Kundendaten offen im Netz

7. Februar 2025, in Hamburg Altona/Hamburg

DATENPANNE
SICHERHEITSLÜCKE
EINBRUCH
KONFIGURATIONSFEHLER

Was ist passiert?
Ein Sicherheitsforscher entdeckte eine fehlkonfigurierte, unzureichend geschützte Datenbank eines juristischen Online-Dienstleisters. Die Schwachstelle wurde der Datenschutzbehörde gemeldet. Nach Angaben des Forschers waren Daten von rund 25.000 Kunden betroffen, darunter sensible Dokumente wie Ausweise, Fahrzeugpapiere und Informationen zu gespielten Sportwetten.

Was hätte man besser machen können?
Die fehlerhafte Datenbankkonfiguration hätte durch automatisierte Schwachstellenscans oder eine strukturierte **Schwachstellenanalyse** frühzeitig erkannt werden können. Auch ein internes Sicherheitsmonitoring in Kombination mit rollenbasierten Zugriffskontrollen hätte helfen können, unautorisierten Zugriff zu unterbinden.

Anzunehmende Schadensfelder:

Quellen:
https://www.heise.de//news/Sicherheitsexperten-enthuellen-triviale-Datenlecks-bei-Legal-techs-10272273.html

Was lernen wir daraus:
Technische Fehlkonfigurationen können schnell zu Datenschutzverstößen, mit erheblichen Folgen führen. Wer sensible personenbezogene Daten verarbeitet, trägt eine hohe Verantwortung und sollte Datenschutz nicht als reine Formalität betrachten. Für Unternehmen lohnt es sich, Sicherheitsaspekte auch aus Sicht der Betroffenen zu betrachten.

RIEDEL

IT-Unternehmen wird Opfer eines Ransomware-Angriffs

7. Februar 2025, in Stuttgart/Baden-Württemberg

DATENDIEBSTAHL
RANSOMWARE
EINBRUCH
DATENLECK

Was ist passiert?
Ein IT-Unternehmen aus dem Raum Stuttgart, das auf Softwarelösungen für digitale Unterhaltungsplattformen spezialisiert ist, wurde offenbar Ziel eines Ransomware-Angriffs. Die Tätergruppe „FOG“ listete das Unternehmen auf ihrer Darknet-Seite und veröffentlichte 5 GB Quellcode als Torrent-Link. Die Daten sollen aus kompromittierten GitLab-Repositories stammen.

Was hätte man besser machen können?
Gerade bei Entwicklungsumgebungen wie GitLab ist eine Absicherung durch mehrstufige Authentifizierung (z. B. MFA), regelmäßige Rechteprüfungen und das Monitoring von Zugriffsaktivitäten essenziell. Eine Extended Detection and Response (XDR)-Lösung hätte Anomalien wie ungewöhnliche Repository-Zugriffe oder große Datenabflüsse automatisch erkannt und analysiert.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8344-FOG-3SS.png

Was lernen wir daraus:
Quellcode zählt zum intellektuellen Kapital vieler Digitalunternehmen und sollte als besonders schützenswert betrachtet werden. Der Schutz von Entwicklerplattformen erfordert daher nicht nur technische Maßnahmen, sondern auch klare Sicherheitsrichtlinien für alle Beteiligten. Unternehmen sollten zudem regelmäßig simulieren, wie sie auf einen Quellcode-Leak reagieren würden – nicht nur technisch, sondern auch kommunikativ.

RIEDEL

Datenleck in Rezeptplattform: Persönliche Infos von 3,3 Millionen Nutzern veröffentlicht

DATENDIEBSTAHL

DATENPANNE

6. Februar 2025, in Wuppertal/Nordrhein-Westfalen

Was ist passiert?
Auf einem Leak-Forum werden persönliche Daten von rund 3,3 Millionen Nutzenden einer beliebten Küchenmaschine zum Kauf angeboten – darunter E-Mail-Adressen, Anschriften und freiwillige Angaben wie Geburtsdaten. Die Daten stammen offenbar aus Rezeptforen mehrerer Länder, besonders betroffen ist Deutschland. Der Hersteller bestätigt ein Datenleck bei einem externen Dienstleister.

Was hätte man besser machen können?
Der Vorfall unterstreicht die Risiken, die aus der Zusammenarbeit mit Drittanbietern entstehen können. Ein regelmäßiges Sicherheitsmonitoring der externen Dienstleister sowie vertraglich klar geregelte Sicherheitsstandards hätten hier potenziell Risiken minimieren können.

Was lernen wir daraus:
Datenlecks bei Drittanbietern betreffen oft nicht nur deren eigene Kunden, sondern auch Unternehmen, die deren Dienste nutzen. Die Verantwortung für Datenschutz endet also nicht an der Unternehmensgrenze. Für Nutzer gilt: Auch scheinbar harmlose Angaben wie Gerätemodelle oder Telefonnummern können in Kombination ein Risiko darstellen – etwa durch Phishing oder gezielte Betrugsversuche.

Anzunehmende Schadensfelder:

Quellen:
https://www.spiegel.de/netzwelt/gadgets/thermomix-daten-von-millionen-kunden-geleakt-a-3fdde071-8f88-48cb-8487-a0573372f502
https://www.security-incidents.de/assets/img/incidents/8310-Thermomix-Kunden-Datenleck.png

RIEDEL

Gemeinnütziger Verein als Opfer einer Ransomware-Attacke gelistet

4. Februar 2025, in Berlin/Berlin

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

DATENLECK

Was ist passiert?
Ein gemeinnütziger Verein, der an einem Open-Source-Webmailprojekt arbeitet, wurde offenbar Opfer einer Ransomware-Attacke. Die Gruppe „FOG“ führte den Vorfall am 4. Februar 2025 auf ihrer Leakseite auf und veröffentlichte 5 GB Quellcode in Form einer Torrent-Datei. Die Daten sollen aus kompromittierten GitLab-Repositories der Organisation stammen.

Was hätte man besser machen können?
Bei Open-Source-Projekten ist eine gut abgesicherte Entwicklungsinfrastruktur entscheidend. GitLab-Instanzen sollten durch Zwei-Faktor-Authentifizierung, rollenbasierte Zugriffsrechte und regelmäßige Updates geschützt sein. Ergänzend kann eine SOAR-Plattform automatisiert auf verdächtige Zugriffe reagieren – etwa bei ungewöhnlichen Aktivitäten außerhalb üblicher Zeiten.

Anzunehmende Schadensfelder:

Quellen:
http://xbkv2qey6u3gd3qxcojynrt4h5sgrhkar6whuo74wo63hijnn677jnyd.onion/posts/67a2592c03e546ad96cc2ecc/
https://www.security-incidents.de/assets/img/incidents/8286-FOG-HEMI.png

Was lernen wir daraus:
Die Ransomware-Gruppe FOG ist seit einiger Zeit aktiv und bekannt dafür, gezielt Organisationen mit schwach abgesicherten IT-Strukturen anzugreifen auch im Non-Profit- oder Open-Source-Bereich. Ihre Taktik besteht oft darin, sensible Daten wie Quellcode oder interne Dokumente aus kompromittierten Systemen zu exfiltrieren und anschließend auf Leak-Seiten im Darknet zu veröffentlichen, wenn keine Zahlung erfolgt.

RIEDEL

473 GB vertrauliche Unternehmensdaten durch Ransomware entwendet

4. Februar 2025, in Aschheim/Bayern

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

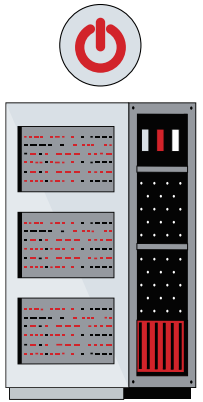
Was ist passiert?
Ein deutsches Modeunternehmen wurde offenbar Ziel eines Ransomware-Angriffs durch die Gruppe „RansomHub“. Die Angreifer gaben an, 473 GB an Unternehmensdaten entwendet zu haben, und setzten dem Unternehmen eine Frist zur Lösegeldzahlung.

Was hätte man besser machen können?
Neben klassischen Schutzmaßnahmen wäre eine Zero-Trust-Architektur sinnvoll gewesen, um kompromittierte Konten oder Systeme im Netzwerk zu begrenzen. Ergänzend hätte eine datenzentrierte Sicherheitsstrategie, etwa durch Verschlüsselung sensibler Dateien im Ruhezustand und bei der Übertragung geholfen, die Folgen eines Angriffs deutlich zu minimieren.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8294-Ransomhub-Escada.jpg

Was lernen wir daraus:
Ransomware-Gruppen wie RansomHub sind bekannt dafür, gestohlene Daten als Druckmittel zu verwenden – oft auch dann, wenn kein direktes Lösegeld gezahlt wird. Besonders bei großen Datenmengen wie den genannten 473 GB steigt das Risiko, dass auch vertrauliche Geschäftsunterlagen, Kunden- oder Mitarbeiterdaten kompromittiert wurden. Kommt es zur Veröffentlichung, drohen nicht nur Reputationsverluste, sondern auch aufsichtsrechtliche Konsequenzen, etwa bei Verstößen gegen die DSGVO.



RIEDEL

Daten einer Forschungseinrichtung via Torrent-Link verfügbar

1. Februar 2025, in Potsdam/Brandenburg

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

Was ist passiert?
Am 1. Februar 2025 veröffentlichte die Ransomware-Gruppe „FOG“ auf ihrer Darknet-Seite den angeblichen Diebstahl von 5 GB Quellcode. Die Daten sollen von einem GitLab-Server einer Forschungseinrichtung stammen. FOG ist dafür bekannt, gezielt GitLab-Instanzen anzugreifen und den erbeuteten Code über Torrent-Links im Netz zu verbreiten.

Was hätte man besser machen können?
Eine Maßnahme in diesem Fall wäre die Segmentierung von Entwicklungs- und Produktionsumgebungen gewesen. Quellcode-Repositories wie GitLab sollten grundsätzlich nur aus gesicherten Netzen erreichbar sein und durch Multi-Faktor-Authentifizierung (MFA) sowie rollenbasierte Zugriffskontrollen geschützt werden.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8262--FOG-Ransomware-GFZ-Helmholtz-Zentrum-Geoforschung.png

Was lernen wir daraus:
Forschungseinrichtungen speichern häufig sensible, teilweise vorveröffentlichte oder geistig geschützte Codes, die wirtschaftlich und wissenschaftlich wertvoll sind. Der Diebstahl solcher Daten durch Ransomware-Gruppen birgt die Gefahr, dass Erkenntnisse frühzeitig in die Hände Dritter gelangen – z. B. Mitbewerber oder staatlich gesteuerte Akteure.

RIEDEL

JANUAR 2025

SECURITY INCIDENTS GERMANY

RIEDEL

Sicherheitslücke in Rehaklinik-App führt zur Offenlegung von etlichen Patientenakten

30. Januar 2025, in Oberhausen/Nordrhein-Westfalen

DATENLECK

SICHERHEITSLÜCKE

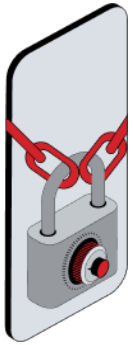
Was ist passiert?
In einer App zur Patientenkommunikation mehrerer Rehakliniken wurden sensible Gesundheitsdaten unverschlüsselt übertragen und waren über den Browser einsehbar. Ein Patient meldete die Sicherheitslücke dem BSI und seiner Klinik. Der Betreiber schloss die Lücke und führte nachträglich eine Transportverschlüsselung ein.

Was hätte man besser machen können?
Die Transportverschlüsselung hätte zwingend von Anfang an implementiert werden müssen, um sensible Gesundheits- und Termindaten bei der Übertragung zu schützen. Ohne diese Verschlüsselung waren die Daten leicht über einen Browser zugänglich.

Anzunehmende Schadensfelder:

Quellen:
https://www.heise.de//news/Datenleck-in-Reha-Kliniken-Hunderttausende-Patienten-potenziell-betroffen-10262109.html

Was lernen wir daraus:
Die Sicherheitslücke hätte bereits in der Planungs- und Entwicklungsphase vermieden werden können. In dieser frühen Phase wird die Architektur der App festgelegt, hier müssen grundlegende Sicherheitsmechanismen wie Transportverschlüsselung (HTTPS/TLS) eingeplant und technisch umgesetzt werden. IT-Sicherheit darf kein nachträglicher Zusatz sein – sie muss integraler Bestandteil der Softwareentwicklung von Anfang an sein.



RIEDEL

Daten eines Gebrauchtmaschinen-Händlers veröffentlicht

30. Januar 2025, in Köln/Nordrhein-Westfalen

DATENDIEBSTAHL

RANSOMWARE

DATENLECK

Was ist passiert?
Am 30. Januar 2025 fügte die Ransomware-Gruppierung „Monti“ einen Gebrauchtmaschinen-Händler ihrer Opferliste hinzu. Die Daten, deren Umfang und Art immer noch unklar ist, stehen seitdem zum Download bereit.

Was hätte man besser machen können?
Mit kontinuierlichen Sicherheitskontrollen hätte das Unternehmen mögliche Schwachstellen rechtzeitig aufdecken können. Ein einsatzbereites Security Operations Center (SOC) hätte außerdem im Ernstfall schneller reagieren können.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8238-nenok-monti.png
https://www.security-incidents.de/assets/img/incidents/8238-nenok-monti-02.png

Was lernen wir daraus:
Es ist wichtig, eine klare und schnelle Kommunikation nach außen zu pflegen im Ernstfall. Unklare Informationen über Umfang und Art der gestohlenen Daten verunsichern Kunden und Partner. Transparente, frühzeitige Kommunikation schafft Vertrauen, signalisiert Handlungsfähigkeit und hilft, den Imageschaden im Ernstfall zu begrenzen.

RIEDEL

DDoS-Attacke: Websites mehrerer Bahngesellschaften tagelang nicht erreichbar

AUSFALL

DDoS

30. Januar 2025, in Soltau/Niedersachsen

Was ist passiert?
Ein DDoS-Angriff legte vier Tage lang die Webseiten mehrerer norddeutscher Bahnunternehmen lahm. Wegen gemeinsamer Servernutzung waren Infos zu Zugausfällen und Verspätungen nicht abrufbar. Laut dpa handelte es sich um eine Botnetz-Attacke. Trotz Gegenmaßnahmen blieb die Lage laut Unternehmenssprecher „sehr dynamisch".

Was hätte man besser machen können?
Die Auswirkungen des DDoS-Angriffs hätten reduziert werden können, wenn ein zentrales **SIEM-System** im Einsatz gewesen wäre. So lassen sich Muster von Überlastungen schneller erkennen und gezielter einordnen. Ergänzend kann ein **Security Operations Center (SOC)** in Echtzeit reagieren und Abwehrmaßnahmen einleiten.

Anzunehmende Schadensfelder:

Quellen:
https://www.heise.de//news/Vermutlich-DDoS-Attacke-Websites-mehrerer-Bahngesellschaften-nicht-erreichbar-10263961.html
https://www.abendblatt.de/niedersachsen/landkreis-harburg/article408192806/hacker-angriff-auf-metronom-nach-drei-tagen-ist-der-spuk-vorbei.html

Was lernen wir daraus:
DDoS-Angriffe stören nicht nur IT-Systeme, sondern auch die Informationsversorgung der Öffentlichkeit. Unternehmen mit digitalem Kundenkontakt sollten Resilienzstrategien entwickeln – z. B. durch Lastverteilung, Backup-Systeme und klare Kommunikationswege im Störfall. Wer auf digitale Dienste setzt, muss Ausfallsicherheit als Teil der Gesamtstrategie begreifen.

RIEDEL

Angriff auf E-Commerce-Unternehmen – welche sensiblen Daten wurden erbeutet?

30. Januar 2025, in Bonn/Nordrhein-Westfalen

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

Was ist passiert?
Ein E-Commerce-Unternehmen wurde auf dem Opferblog der Ransomware-Gruppe „Akira“ im Darknet gelistet. Die Angreifer behaupten, sensible Daten wie NDAs, Kontakt- und E-Mail-Daten von Mitarbeitenden und Kunden, Finanzunterlagen, vertrauliche Verträge sowie interne Kommunikation erbeutet zu haben. Eine Veröffentlichung der gestohlenen Informationen wird angedroht.

Was hätte man besser machen können?
Ein effektives EDR-System hätte verdächtige Aktivitäten auf den Endgeräten frühzeitig erkennen und isolieren können, bevor sich die Ransomware weiterverbreitet. Zusätzlich hätte eine regelmäßige Schwachstellenanalyse dabei helfen können, potenzielle Einfallstore zu identifizieren, insbesondere in einem sensiblen Umfeld wie dem E-Commerce mit vielen Kundendaten.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8248-Akira-Benuta.png

Was lernen wir daraus:
Ransomware zielt nicht nur auf IT-Systeme, sondern auch auf vertrauliche Unternehmensdaten, um Druck aufzubauen. Der Schutz sensibler Informationen erfordert mehr als Firewalls – auch Datenklassifizierung, Zugriffskontrollen und Verschlüsselung sind essenziell. Wer Daten verarbeitet, trägt Verantwortung – nicht nur technisch, sondern auch rechtlich und reputationsbezogen.

RIEDEL

Sensible Daten aus der Stadtverwaltung entwendet

28. Januar 2025, in Kaiserbach/Baden-Württemberg

DATENDIEBSTAHL

RANSOMWARE

DATENLECK

Was ist passiert?
Eine Gemeinde aus wurde offenbar Ziel eines Ransomware-Angriffs. Die Ransomware-Gruppe „Cloak“ veröffentlichte auf ihrer Darknet-Leakseite die einen Datensatz, den sie von der Webseite der Gemeinde Kaisersbach gestohlen hatte. Der Datensatz umfasst weniger als 100 GB, enthält jedoch laut Beweisproben sensible Informationen aus der Stadtverwaltung.

Was hätte man besser machen können?
Eine regelmäßige Sicherheitsüberprüfung der Systeme hätte helfen können, **Schwachstellen** in der IT der Gemeindeverwaltung frühzeitig zu erkennen. Besonders in öffentlichen Einrichtungen ist es wichtig, Systeme nicht nur zu betreiben, sondern auch aktiv zu schützen – u.a. durch aktuelle Patches, Zugangsbeschränkungen und Kontrolle sensibler Datenzugriffe.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8211-cloak-kaisersbach.png

Was lernen wir daraus:
Auch kleinere Verwaltungen sind attraktive Ziele für Angreifer – nicht trotz, sondern gerade wegen oft begrenzter IT-Ressourcen. IT-Sicherheit darf deshalb nicht als rein technisches Thema gesehen werden, sondern muss Teil der kommunalen Verantwortung sein. Schulungen, klare Zuständigkeiten und Sicherheitsbewusstsein sind essenziell für den Schutz öffentlicher Daten.

RIEDEL

Geschäftlicher Schriftverkehr von deutschem Kosmetikunternehmen offengelegt

28. Januar 2025, in Mauer/Baden-Württemberg

DATENDIEBSTAHL

RANSOMWARE

DATENLECK

Was ist passiert?
Die Ransomware-Gruppe „Cloak“ veröffentlichte einen 227 GB großen Datensatz, der von der Webseite eines deutschen Kosmetik-Unternehmens stammen soll. Wann genau es zu dem Angriff auf das Unternehmen kam, bleibt unklar. Bei den zum Download bereitstehenden Daten handele es sich wohl um geschäftliche Korrespondenzen des Unternehmens.

Was hätte man besser machen können?
Eine EDR-Lösung hätte verdächtige Aktivitäten wie unautorisierte Datenzugriffe oder ungewöhnliche Datenabflüsse frühzeitig erkennen können. Auch die Überwachung durch ein zentrales SIEM-System hätte dazu beigetragen, Auffälligkeiten in der Kommunikation oder im Netzwerkverkehr rechtzeitig zu erfassen – besonders bei großen Datenbewegungen wie hier.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8210-cloak-neovita.png

Was lernen wir daraus:
Wenn geschäftliche Kommunikation abfließt, kann das zu Vertrauensverlust, Wettbewerbsnachteilen und rechtlichen Problemen führen. Unternehmen sollten sich bewusst machen, wie sensibel alltägliche E-Mails oder Dokumente sein können. Ein strukturiertes Datenmanagement mit Zugriffskontrollen, Verschlüsselung und klarer Klassifizierung ist dafür ein wichtiger Baustein.

RIEDEL

Mehrere 100.000 € Schaden - Cyberangriff zwingt einen Hotelbetrieb in die Insolvenz

27. Januar 2025, in Aalen/Baden-Württemberg

BETRUG

EINBRUCH

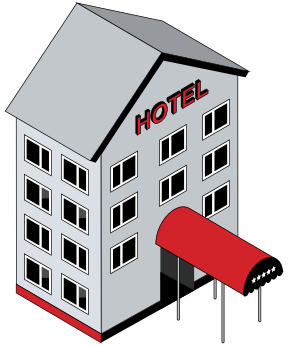
Was ist passiert?
Ein Hotelbetrieb musste Insolvenz anmelden. Ursache war ein Cyberangriff, der als Betrugsfall eingestuft wurde und finanzielle Schäden in Höhe mehrerer hunderttausend Euro verursachte. Ein Überbrückungskredit reichte nicht aus, um die Verluste auszugleichen. Das Hotel bleibt während des Verfahrens geöffnet, die Gehälter sind für drei Monate gesichert. Ziel ist die langfristige Stabilisierung.

Was hätte man besser machen können?
Bei Betrugsfällen im digitalen Raum etwa durch Business E-Mail Compromise oder manipulierte Zahlungsanweisungen, kann der Einsatz von XDR helfen, verdächtige Aktivitäten über mehrere Systeme hinweg zu erkennen. Ergänzend sind klare interne Kontrollmechanismen wichtig, etwa das Vier-Augen-Prinzip bei Zahlungen oder die technische Absicherung geschäftlicher Kommunikation.

Anzunehmende Schadensfelder:

Quellen:
https://www.pluta.net/en/press/press-release/pluta-attorney-florian-zistler-appointed-provisional-administrator-for-maxx-hotel-in-aalen.html
https://www.schwaebische.de/regional/ostalb/aalen/finanzieller-engpass-nach-cyberangriff-maxx-hotel-insolvent-3285465

Was lernen wir daraus:
Cyberangriffe gefährden nicht nur Daten, sondern auch wirtschaftliche Existenzen. Besonders im Mittelstand kann ein einzelner Vorfall weitreichende Folgen haben. Wer sich mit IT-Sicherheit beschäftigt, sollte auch finanzielle Risiken einbeziehen: Cyber-Versicherungen, Notfallpläne und Schulungen für Personal in sensiblen Bereichen sind wichtige Bausteine der Absicherung.



RIEDEL

100 GB eines Laborequipment-Herstellers veröffentlicht

27. Januar 2025, in Wiesbaden-Delkenheim/Hessen

DATENDIEBSTAHL

RANSOMWARE

DATENLECK

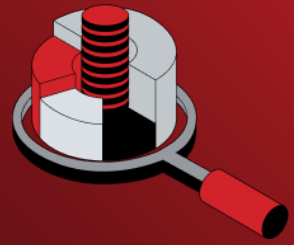
Was ist passiert?
Am 27. Januar 2025 fügte die Ransomware-Gruppe „Babuk“ einen weltweit aktiven deutschen Hersteller von Diagnostik- und Laborequipment zu ihrer Leakseite im Darknet hinzu. Sie erbeuteten 100 GB Daten, die noch am selben Tag veröffentlicht wurden.

Was hätte man besser machen können?
Bei einem gezielten Angriff auf ein Industrieunternehmen hätte ein SIEM-System in Verbindung mit einem aktiven SOC helfen können, ungewöhnliche Datenabflüsse frühzeitig zu erkennen und einzudämmen. Gerade bei forschungs- oder produktionsnahen Daten ist es entscheidend, systematische Überwachung mit klaren Reaktionsprozessen zu kombinieren, um Leaks zu verhindern.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8195-human-babuk.png
https://www.security-incidents.de/assets/img/incidents/8195-babuk-human-02.png

Was lernen wir daraus:
Industrieunternehmen sind attraktive Ziele – nicht nur wegen personenbezogener Daten, sondern auch wegen sensibler Geschäftsinformationen wie Produktentwicklungen oder Labordaten. Wer in kritischen Bereichen arbeitet, sollte Sicherheitsstrategien nicht isoliert betrachten, sondern ganzheitlich: Schutz von IT, Produktion, Kommunikation und Know-how gehören zusammen.



RIEDEL

Ransomware-Gruppe veröffentlicht 11 GB von Digitalisierungsunternehmen

27. Januar 2025, in Aalen/Baden-Württemberg

DATENDIEBSTAHL
RANSOMWARE
DATENLECK
ERPRESSUNG

Was ist passiert?
Am 27. Januar 2025 gab die Ransomware-Gruppe „Babuk“ bekannt, ein Digitalisierungsunternehmen angegriffen zu haben. Da das Unternehmen den Forderungen der Gruppe nicht nachkam, standen die 11 GB erbeuteten Daten wenig später zum Download bereit.

Was hätte man besser machen können?
Ein umfassender Schutz hätte durch den Einsatz von **EDR-Systemen** erfolgen können, die ungewöhnliche Aktivitäten auf Endpunkten erkennen, z. B. Verschlüsselungsvorgänge oder den Zugriff auf sensible Daten. In einem digital ausgerichteten Unternehmen ist zudem eine regelmäßige Überprüfung der Zugriffsrechte und Netzwerksegmentierung entscheidend, um Angriffe einzugrenzen.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8196-babuk-wuerttemberger-medien.png
https://www.security-incidents.de/assets/img/incidents/8196-wuerttemberger-medien-babuk-02.png

Was lernen wir daraus:
Wer digitale Lösungen anbietet, steht auch selbst in der Verantwortung, besonders hohe Sicherheitsstandards einzuhalten. Der Vorfall zeigt: Nicht nur die Menge der erbeuteten Daten ist relevant – auch kleinere Datenmengen können großen Schaden anrichten. IT-Sicherheit beginnt bei der Haltung: Wer Digitalisierung gestaltet, muss Sicherheit mitdenken.

RIEDEL

Deutsches Werkstoffunternehmen wurde Opfer eines Ransomware-Angriffs

24. Januar 2025, in Leverkusen/Nordrhein-Westfalen

DATENDIEBSTAHL

RANSOMWARE

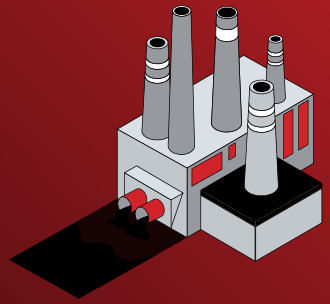
Was ist passiert?
Am 24. Januar haben Cyberkriminelle der „Cl0P-Gruppe“ ein deutsches Werkstoffunternehmen attackiert. Den Tätern ist es dabei laut eigenen Angaben gelungen, Daten zu stehlen.

Was hätte man besser machen können?
Der gezielte Diebstahl von Daten deutet auf eine sogenannte „Exfiltration“ hin, die oft unbemerkt bleibt. Ein XDR-System hätte helfen können, verdächtige Aktivitäten über verschiedene Ebenen hinweg zu korrelieren z. B. ungewöhnliche Zugriffe auf interne Datenbanken kombiniert mit ausgehendem Datenverkehr.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8188-Covestro-Cl0P.PNG

Was lernen wir daraus:
Datendiebstahl bleibt oft lange unbemerkt – gerade in technischen Branchen mit großen Datenbeständen. Unternehmen sollten sich nicht nur gegen Ransomware, sondern auch gegen leise, datenzentrierte Angriffe wappnen. Ein besseres Verständnis für typische Angriffswege und regelmäßige Schulungen helfen dabei, Bedrohungen schneller zu erkennen und richtig zu reagieren.



RIEDEL

Ransomware-Angriff trifft 45 Schulen in Rheinland-Pfalz – Datenverschlüsselung und IT-Ausfall

22. Januar 2025, in Speyer/Rheinland-Pfalz

DATENDIEBSTAHL

RANSOMWARE

AUSFALL

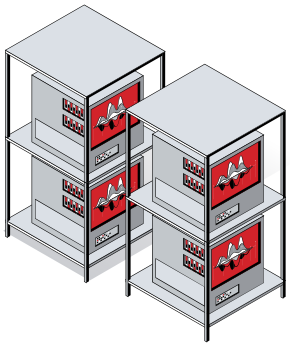
Was ist passiert?
Ein IT-Dienstleister aus Speyer wurde Opfer einer Ransomware-Attacke. Die Angreifer erbeuteten über 3 TB Daten und verschlüsselten Systeme. Auch 45 Schulen in Rheinland-Pfalz waren betroffen. Medien berichten von exfiltrierten Daten. Der Dienstleister empfahl allen Nutzenden des DNSX-Netzwerks, ihre Passwörter zu ändern, um weiteren Schaden zu vermeiden.

Was hätte man besser machen können?
Ein zentrales **SIEM-System** hätte dabei helfen können, Anomalien im Netzwerkverkehr wie große Datenabflüsse oder untypische Zugriffsmuster frühzeitig zu erkennen. Da viele Schulen betroffen waren, wäre eine segmentierte Netzwerkinfrastruktur essenziell gewesen, um die Ausbreitung der Attacke zu begrenzen. Zusätzlich hätten regelmäßige Backup-Tests die Wiederherstellung erleichtert.

Anzunehmende Schadensfelder:

Quellen:
https://www.csoonline.com/article/3807761/45-schulen-von-cyberangriff-betroffen.html
https://www.polizei.rlp.de/service/presse/detail/mehrere-schulen-in-rheinland-pfalz-von-cyberangriff-betroffen

Was lernen wir daraus:
Der Angriff verdeutlicht die Risiken zentralisierter IT-Dienstleistungen. Wenn viele Einrichtungen auf dieselbe Infrastruktur vertrauen, kann ein einzelner Vorfall weitreichende Folgen haben. Organisationen sollten ihre IT-Abhängigkeiten regelmäßig prüfen, Zuständigkeiten klar regeln und hinterfragen, ob ihre Sicherheitsinteressen ausreichend in Dienstleistungsverträgen verankert sind.



RIEDEL

100 GB Daten eines deutschen Sanitär- und Armaturenherstellers entwendet

17. Januar 2025, in Düsseldorf/Nordrhein-Westfalen

DATENDIEBSTAHL

RANSOMWARE

DATENLECK

Was ist passiert?
Einer der größten Hersteller von Sanitärarmaturen in Europa und führender Anbieter weltweit, wurde als Opfer einer Ransomware-Gruppe auf ihrer Erpressungswebseite gelistet. Die Angreifer behaupteten, 100 GB an Daten entwendet zu haben, machten jedoch keine Angaben zum konkreten Inhalt des Materials.

Was hätte man besser machen können?
Eine 24/7-Überwachung durch ein SOC hätte helfen können, verdächtige Aktivitäten frühzeitig zu erkennen – etwa ungewöhnliche Zugriffe auf interne Daten oder verdichtete Dateizugriffe vor der Exfiltration. Gerade bei international agierenden Industrieunternehmen ist kontinuierliche Überwachung entscheidend, da Angriffe oft außerhalb der regulären Geschäftszeiten beginnen.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8146-ransomhub-grohe.png
https://www.security-incidents.de/assets/img/incidents/8146-ransomhub-grohe-02.png

Was lernen wir daraus:
Auch wenn zunächst keine Details bekannt sind, ist der Datenabfluss allein schon ein Risiko – etwa für Geschäftsbeziehungen, geistiges Eigentum oder Lieferketten. Wer international tätig ist, sollte seine Sicherheitsstrategie global denken: Angreifer kennen keine Zeitzonen.

RIEDEL

Ungewissheit bei Software-Unternehmen: Wurden Daten entwendet?

16. Januar 2025, in Wiesbaden/Hessen

DATENDIEBSTAHL

RANSOMWARE

ERPRESSUNG

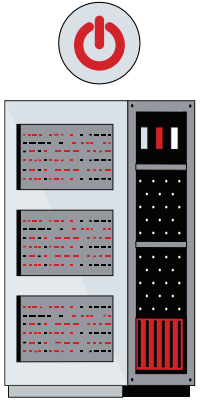
Was ist passiert?
Am 16. Januar 2025 gab die Ransomware-Gruppe „8Base“ bekannt, ein Wiesbadener Software-Unternehmen angegriffen und vertrauliche Daten gestohlen zu haben. Zu den angeblich erbeuteten Dokumenten zählen Steuerunterlagen, Rechnungen, Kontoauszüge und eine Mail-Datenbank.

Was hätte man besser machen können?
Die Auswirkungen des DDoS-Angriffs hätten reduziert werden können, wenn ein zentrales **SIEM-System** im Einsatz gewesen wäre. So lassen sich Muster von Überlastungen schneller erkennen und gezielter einordnen. Ergänzend kann ein **Security Operations Center (SOC)** in Echtzeit reagieren und Abwehrmaßnahmen einleiten.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8051-8base-netform-gmbh.png

Was lernen wir daraus:
Ransomware-Angriffe zielen längst nicht mehr nur auf die Verschlüsselung von Daten – die parallele Exfiltration sensibler Inhalte wie Steuerunterlagen oder Maildatenbanken ist Teil des sogenannten „Double Extortion“-Modells. Unternehmen sollten sich mit dieser Taktik vertraut machen: Auch wenn ein Backup existiert, kann der Druck durch drohende Datenveröffentlichung enorm sein. Prävention wird dadurch noch wichtiger als Reaktion.



RIEDEL

Offen für alle: API-Leck bei Anbieter von sicheren Identitäten

16. Januar 2025, in Berlin/Berlin

DATENDIEBSTAHL

EINBRUCH

Was ist passiert?
Ein Anbieter für elektronische Signaturkarten im Gesundheitswesen wurde Opfer eines Datenlecks. Eine offene API auf dem Antragsportal ermöglichte den Abruf personenbezogener Daten wie Name, E-Mail und Geburtsdatum. Ein anonymer Sicherheitsforscher entdeckte die Lücke und informierte nicht den Anbieter direkt, sondern wandte sich an den Chaos Computer Club (CCC).

Was hätte man besser machen können?
Das Unternehmen hätte die API durch wirksame Zugriffskontrollen absichern müssen – etwa durch Authentifizierung und Autorisierung. Eine regelmäßige Sicherheitsüberprüfung der Schnittstellen sowie automatisierte Scans auf offene Endpunkte hätten die Schwachstelle frühzeitig aufdecken können.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/8107-D-Trust.png
https://www.heise.de/news/Vertrauensdiensteanbieter-D-Trust-informiert-ueber-Datenschutzvorfall-10246338.html

Was lernen wir daraus:
Die betroffenen Signatur- und Siegelkarten sind für Ärzte wichtig, um sich in der Telematikinfrastruktur des Gesundheitswesens auszuweisen. Der Vorfall war also sicherheitstechnisch und politisch sensibel und zeigt, wie kritisch es ist, APIs sorgfältig abzusichern. Selbst ohne klassische Cyberangriffe können Daten abfließen, wenn Zugriffskontrollen fehlen.

RIEDEL

Für Marketingdienstleister gibt es mehr Reichweite als gewünscht

RANSOMWARE

13. Januar 2025, in Mainz/Rheinland-Pfalz

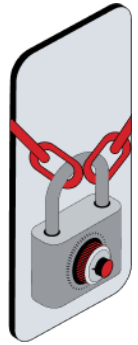
Was ist passiert?
Am 13. Januar 2025 wurde ein Marketingdienstleister aus Mainz von der Ransomware-Gruppe „LockBit 3.0“ auf deren Erpressungsplattform als Ziel eines Cyberangriffs genannt. Die Angreifer forderten das Unternehmen zur Zahlung eines Lösegelds auf und setzten eine Frist – andernfalls drohten sie damit, gestohlene Daten öffentlich zugänglich zu machen.

Was hätte man besser machen können?
Der Zugang hätte über VPN besser abgesichert werden können – etwa durch den Einsatz von Multi-Faktor-Authentifizierung, um den Zugriff für Unbefugte zu erschweren. Außerdem hätte eine Sicherheitslösung wie **XDR** dabei unterstützt, verdächtige Aktivitäten schneller zu entdecken und rechtzeitig Gegenmaßnahmen einzuleiten.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/7999-telering-marketing-lockbit.png

Was lernen wir daraus:
Ein häufiger Schwachpunkt in Unternehmen ist die unzureichende Protokollierung von Zugriffen. Ohne nachvollziehbare Logs bleiben verdächtige Aktivitäten oft unentdeckt. Eine saubere, manipulationssichere Protokollierung gehört zu den Grundlagen der IT-Sicherheit – nicht nur zur Aufklärung, sondern auch zur Prävention von Datenschutzverletzungen.



RIEDEL

Cyberkriminelle prangern den Umgang einer Hausarztpraxis mit deren Patienten an

9. Januar 2025, in Scheeßel/Niedersachsen

RANSOMWARE

EINBRUCH

DATENLECK

Was ist passiert?
Bei einem Ransomware-Angriff auf eine Hausarztpraxis, wurden laut Tätern 30 GB sensible Daten erbeutet und auf ihrer Webseite veröffentlicht. In ihrer Mitteilung kritisieren sie die Praxis und werfen ihr vor, sich angeblich nicht für Patienten zu interessieren, was auf nicht erfüllte Forderungen hinweist. Der Zeitpunkt des Angriffs ist unbekannt, doch die veröffentlichten Daten reichen bis Dezember 2024 zurück.

Was hätte man besser machen können?
Insbesondere kleinere Hausarztpraxen verfügen in der Regel nicht über eigenes Fachpersonal im Bereich IT-Sicherheit, da der Fokus auf der medizinischen Versorgung liegt und IT-Themen eine untergeordnete Rolle spielen. Eine Zusammenarbeit mit spezialisierten Dienstleistern, die über ein Security Operations Center (SOC) verfügen, bietet hier professionellen Schutz.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/7936-Hausarztpraxis_Schulstrasse-Three-Am.PNG

Was lernen wir daraus:
Ein Security Operations Center (SOC) ist eine spezialisierte Einheit, die IT-Systeme rund um die Uhr überwacht, analysiert und vor Cyberangriffen schützt. Es erkennt Sicherheitsvorfälle in Echtzeit, reagiert auf Bedrohungen und leitet Gegenmaßnahmen ein. So gelingt es, Angriffe frühzeitig zu erkennen und Schäden zu minimieren.

RIEDEL

Sensible Daten eines Metallverarbeiters aus Bayern womöglich bald öffentlich

7. Januar 2025, in Burgsinn/Bayern

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

Was ist passiert?
Die Ransomware-Gruppe „8Base“ listete einen bayerischen Metallverarbeiter als neues Opfer. Die Täter behaupten, intime Fotos, Rechnungen, Pläne, technische Zeichnungen, Reisepässe und zahlreiche weitere finanziell relevante Dokumente gestohlen zu haben, und drohen mit einer Veröffentlichung, insofern ihre Forderungen innerhalb einer Frist nicht erfüllt werden.

Was hätte man besser machen können?
Häufig fehlen den Unternehmen die nötigen Ressourcen oder Fachkenntnisse im Bereich IT-Sicherheit. Vor allem in solchen Fällen sollten die Unternehmen auf die Unterstützung von Spezialisten setzen. Experten entwickeln nämlich eine umfassende Sicherheitslösung, die präventive Schutzmaßnahmen gegen Cyberangriffe umfasst, um das Risiko eines Angriffs zu minimieren.

Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/7907-8Base-Weiniger_Metall.PNG

Was lernen wir daraus:
Ransomware-Angriffe nehmen weiter zu und viele Betroffene zahlen die geforderten Lösegelder, weil sie keine aktuellen Backups haben. Eine solide Backup-Strategie mit Offline-Kopien und regelmäßiger Wiederherstellungsprüfung ist ein entscheidendes Schutzmittel. Nur wer Daten wirklich wiederherstellen kann, bleibt auch im Angriffsfall handlungsfähig.

RIEDEL

Ausfall des Fahndungssystems „Inpol“ bringt die Bundespolizei in Ausnahmezustand

AUSFALL

3. Januar 2025, in Potsdam/Brandenburg

Was ist passiert?
Bei der Bundespolizei fiel das Fahndungssystem Inpol aus, wodurch die automatisierte Einreise aus Nicht-Schengen-Staaten nicht möglich war. Die Polizei kontrollierte manuell, was zu längeren Wartezeiten und Rückstaus führte. Am Abend gaben Flughäfen wie Frankfurt, Berlin und Düsseldorf Entwarnung. Die Ursache ist bislang unbekannt.

Was hätte man besser machen können?
Ein proaktives Überwachungssystem (Monitoring) hätte den Ausfall eventuell früher erkannt und automatisiert Warnungen generiert, bevor es zum vollständigen Systemversagen kam.

Anzunehmende Schadensfelder:

Quellen:
https://www.fr.de/panorama/it-ausfall-an-deutschen-flughaefen-entwarnung-nach-stunden-zr-93497106.html

Was lernen wir daraus:
Der Vorfall zeigt, wie wichtig klare und getestete Notfallpläne sind. Wenn im Ernstfall unklar ist, wer was tun muss, verstreicht wertvolle Zeit. Organisationen und Unternehmen sollten regelmäßig IT-Notfallübungen durchführen, Zuständigkeiten dokumentieren und ihre Reaktionspläne an neue Bedrohungen anpassen. Eine gute Vorbereitung ist entscheidend für die Schadensbegrenzung.

RIEDEL

Institut nach Ransomware-Angriff am ermitteln – wurden Daten entwendet?

3. Januar 2025, in Stuttgart/Baden-Württemberg

EINBRUCH

RANSOMWARE

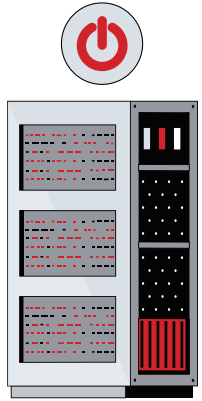
Was ist passiert?
Ein deutsches Institut für Arbeitswirtschaft und Organisation wurde Opfer eines Ransomware-Angriffs und es wird davon ausgegangen, dass personenbezogene Daten entwendet wurden. Das Institut reagierte rasch und arbeitete mit IT-Sicherheitsexperten sowie Ermittlungsbehörden zusammen, um den Angriff zu untersuchen und entsprechende Gegenmaßnahmen zu ergreifen.

Was hätte man besser machen können?
Mit einem **Schwachstellenscan** (auch Vulnerability Scan genannt) – bei dem IT-Systeme nach Sicherheitslücken durchsucht werden – hätte man dem Ransomware-Angriff womöglich vorbeugen können, indem Schwachstellen frühzeitig aufgedeckt und behoben worden wären.

Anzunehmende Schadensfelder:

Quellen:
https://www.heise.de//news/Ransomware-Angriff-am-Fraunhofer-fuer-Arbeitswirtschaft-und-Organisation-10225293.html

Was lernen wir daraus:
Veraltete Software zählt zu den größten Sicherheitsrisiken. Angreifer nutzen bekannte Schwachstellen gezielt aus, oft lange nachdem sie öffentlich dokumentiert und durch Updates behebbar gewesen wären. Wer IT-Sicherheit ernst nimmt, braucht ein konsequentes Patch-Management, das alle Systeme und Geräte regelmäßig auf dem aktuellen Stand hält.



RIEDEL

Erkenntnisse

OOPS REPORT H1-2025

RIEDEL

Summary

Welche Erkenntnisse stechen besonders hervor?

Im Vergleich zum letzten OOPS-Report H1-2024 zeigt sich die Branchenverteilung im ersten Halbjahr 2025 wie folgt:

- **Industrie & Produktion – 26 %**
- **IT & Telekommunikation – 18 %**
- **Öffentlicher Sektor / Verwaltung – 17 %**
- **Handel & Dienstleistungen – 14 %**
- **Finanzsektor – 10 %**
- **Gesundheitswesen – 8 %**
- **Sonstige – 7 %**

Auffällig ist, dass insbesondere **IT/Telekommunikation** und **Handel** zulegen, während **öffentliche Verwaltung und Industrie** leicht zurückgehen.

Im Vergleich zum letzten OOPS-Report zeigt sich die Verteilung der Angreifertypen im ersten Halbjahr 2025 wie folgt:

- **Cyberkriminelle (finanziell motiviert) – 71 %**
- **Hacktivisten (politisch motiviert) – 12 %**
- **Staatlich / Spionage – 9 %**
- **Insider / interne Täter – 5 %**
- **Unbekannt – 3 %**

Finanziell motivierte **Cyberkriminelle** und interne Täter legen leicht zu, **Hacktivisten** und **staatliche Angreifer** nehmen ab, unbekannt bleibt unverändert.

Im Vergleich zum letzten OOPS-Report zeigt sich die Verteilung der Angriffstypen im ersten Halbjahr 2025 wie folgt:

- **Ransomware – 38 %**
- **Datendiebstahl (ohne Verschlüsselung) – 22 %**
- **Einbruch / Netzwerkkompromittierung – 15 %**
- **Sicherheitslücken / Fehlkonfiguration – 11 %**
- **DDoS / Sabotage – 7 %**
- **Sonstige – 7 %**

Ransomware bleibt führend und steigt leicht, Sonstige Angriffsformen, wie **Phishing/Social Engineering** nehmen zu, andere Angriffsarten gehen zurück.

RIEDEL

Summary

Welche Erkenntnisse stechen besonders hervor?

1. **Ransomware dominiert weiterhin** – Sie betrifft zahlreiche Branchen von Industrie bis NGOs, wird oft mit Doppel-Erpressung kombiniert und kann im Extremfall, wie bei einem Produktionsbetrieb, direkt zur Insolvenz führen.

2. **Öffentlicher Sektor mehrfach Ziel** – Angriffe auf Polizei, Stadtverwaltungen, Bildungsnetzwerke und Feuerwehr zeigen, dass auch kritische Behörden durch ungepatchte Schwachstellen verwundbar bleiben.

3. **Sicherheitslücken verursachen Datenpannen** – Fälle wie bei einem Restaurant-Website-Anbieter oder einem veralteten E-Mail-Dienst belegen, dass fehlendes Patch-Management oder fehlende Zugriffskontrollen massive Folgen haben können.

4. **Social-Media-Übernahmen als Einfallstor** – Die Kompromittierung von Instagram-Accounts großer Organisationen zeigt, dass auch vermeintlich „banale“ Plattformen erheblichen Schaden anrichten können.

5. **Angriffe werden vielfältiger** – Der Einbruch in den Serverraum der Berliner Feuerwehr verdeutlicht, dass physische und digitale Angriffe zunehmend kombiniert werden.

6. **Auch kleine Unternehmen im Visier** – Angriffe auf Nischenbranchen wie Pflanzenzucht oder regionale Bäckereien belegen, dass Unternehmensgröße keinen Schutz mehr bietet.

RIEDEL

Vergleich

Welche Gemeinsamkeiten gibt es zwischen dem ersten Halbjahr 2024 und 2025?

Ransomware bleibt die dominierende Bedrohung

- In beiden Berichtszeiträumen war Ransomware der häufigste Angriffstyp.
- H1 2024: 45 % aller Angriffe waren Ransomware.
- H1 2025: Sinkt der Anteil leicht auf 38 %.

Cyberkriminelle übernehmen das Feld

- In beiden Berichtszeiträumen stellen Cyberkriminelle die größte Angreifergruppe dar.
- H1 2024: Erpresser machten 40 % aus.
- H1 2025: Cyberkriminelle dominieren mit 71 % aller Angriffe.

Industrie und IT besonders betroffen

- Cyberangriffe treffen zunehmend Industrie, IT und öffentliche Einrichtungen, während Finanzsektor und Gesundheitswesen deutlich an Bedeutung verlieren.

Staatliche Spionage bleibt relevant

- Obwohl der Anteil staatlich gesteuerter Angriffe sinkt, bleibt Spionage ein Risiko für daten-intensive Unternehmen und den öffentlichen Sektor.

RIEDEL

Vergleich

Welche Gemeinsamkeiten gibt es zwischen dem ersten Halbjahr 2024 und 2025?

	H1-2024	H1-2025	Veränderung
Angriffstypen	Ransomware (45%), Datendiebstahl (30%), Einbruch (15%), Erpressung (10%)	Ransomware (38%), Datendiebstahl (22%), Einbruch (15%), Sicherheitslücken (11%), DDoS (7%) , Sonstige (7%)	Ransomware und Datendiebstahl gehen zurück, während Sicherheitslücken, DDoS und neue Angriffsformen zunehmen.
Angreifertypen	Erpresser (40%), Staatliche Spionage (25%), Böse (20%), Whitehacker (15%)	Cyberkriminelle (71%), Hacktivisten (12%), Staatliche Spionage (9%), Insider (5%), Unbekannt (3%)	Cyberangriffe werden zunehmend von Cyberkriminellen ausgeführt, während Erpresser und staatliche Akteure deutlich an Einfluss verlieren.
Betroffene Branchen	Finanzsektor (28%), Gesundheitswesen (22%), Industrie (18%), Öffentlicher Sektor (15%), IT (10%), Bildung (7%)	Industrie (26%), IT (18%), Öffentlicher Sektor (17%), Handel (14%), Finanzsektor (10%), Gesundheitswesen (8%), Sonstige (7%)	Cyberangriffe verlagern sich von Finanz- und Gesundheitswesen zunehmend auf Industrie, IT und öffentliche Einrichtungen.
Neue Trends	Fokus auf klassische Angriffe (Ransomware, Einbruch)	Diversifizierung der Angriffsformen, Sicherheitslücken, DDoS und neue Angriffstypen gewinnen an Bedeutung	Der Trend geht weg von klassischen Angriffen hin zu vielfältigeren und technisch differenzierteren Methoden

RIEDEL

“

H1 2025 verdeutlicht, dass Cyberangriffe längst kein isoliertes IT-Problem mehr sind: Hochgradig organisierte, finanziell getriebene Gruppen agieren branchenübergreifend, kombinieren Ransomware, Datendiebstahl und Social Engineering mit gezielten physischen Zugriffen und finden ihre Chancen dort, wo Technik, Prozesse und Menschen nicht gleichermaßen auf Resilienz getrimmt sind.

”

RIEDEL

Get in Touch

Beim Thema IT-Security zählt vor allem eins: einfach anfangen!

RIEDEL Networks GmbH & Co. KG

RN-sales@riedel.net

+49 (0) 6033 9169 100

Noch nicht überzeugt?
Vielleicht hilft unser „Faule Ausreden-Quartett“ zum Thema Cyber Security
– und dann freuen wir uns auf einen weiteren Austausch mit Ihnen.

Aufsichtsbehörde: Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Tulpenfeld 4, 53113 Bonn, Reg-Nr. 12/158

RIEDEL