OOPS H2-2024

Der “hätte ich das mal früher gewusst” Report

SECURITY INCIDENTS GERMANY

CYBERCRIME PAYS OFF?

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

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

DEZEMBER 2024

SECURITY INCIDENTS GERMANY

RIEDEL

Ransomware-Überraschung zum Jahresende bei Stuttgarter Bauunternehmen

28. Dezember 2024, in Stuttgart/Baden-Württemberg

RANSOMWARE

EINBRUCH

DATENDIEBSTAHL

Was ist passiert?
Seit dem 28. Dezember 2024 führt die Ransomwaregruppe „RA World“ ein Stuttgarter Bauunternehmen als Opfer auf ihrer Darknet-Leakseite. Die Angreifer behaupten, 600 GB sensibler Daten gestohlen zu haben. Sollte das Unternehmen das geforderte Lösegeld nicht zahlen, droht die Veröffentlichung der Informationen. Ob Verhandlungen laufen oder welche Daten genau betroffen sind, blieb unklar.

Was hätte man besser machen können?
Eine rund um die Uhr aktive Überwachung des Firmennetzwerks durch ein Security Operations Center (SOC) hätte ungewöhnliche Aktivitäten frühzeitig identifizieren und stoppen können. Durch eine fortlaufende Analyse und vorausschauende Erkennung von Bedrohungen wäre es möglich gewesen, den Angriff abzuwehren, bevor vertrauliche Daten in Gefahr gerieten.

Was lernen wir daraus:

Dedicated Leak Sites (DLS) sind spezielle Webseiten im Darknet, die von Ransomwaregruppen betrieben werden. Dort veröffentlichen Cyberkriminelle gestohlene Daten von Unternehmen und Organisationen. Diese Seiten dienen als Druckmittel, um die Opfer zur Zahlung zu bewegen und als Marktplatz für gestohlene Informationen, die an Dritte verkauft werden können. Durch das Beobachten von Dedicated Leak Sites können Unternehmen frühzeitig erkennen, ob sie ins Visier geraten sind, bevor sensible Daten vollständig veröffentlicht werden.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7825-die-STEG-Stadtentwicklung.RA-World-ransomware.png

RIEDEL

Vermögensverwaltungsgesellschaft startet 176 GB leichter ins neue Jahr

28. Dezember 2024, in Hamburg/Hamburg

DATENLECK

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

Was ist passiert?
Am 28. Dezember 2024 tauchte eine internationale Vermögensverwaltungsgesellschaft auf der Darknet-Leakseite der Ransomwaregruppe „Dragonforce“ auf. Die Angreifer behaupten, 176,85 GB vertraulicher Unternehmensdaten erbeutet zu haben, darunter auch Mitarbeiterinformationen. Laut den Hackern sind die gestohlenen Daten bereits auf ihrer Leak-Plattform einsehbar. Ob das Unternehmen Lösegeld zahlen will oder Verhandlungen laufen ist unklar.

Was hätte man besser machen können?
Eine Ende-zu-Ende-Verschlüsselung hätte womöglich dazu beigetragen, dass sensible Daten während der gesamten Übertragungs- und Speicherkette geschützt werden.

Bei der Übertragung von Daten sollten diese so verschlüsselt werden, dass sie nur vom vorgesehenen Empfänger entschlüsselt werden können, selbst wenn sie abgefangen werden. Im Ruhezustand sind die Daten mit Verschlüsselungen vor unbefugtem Zugriff zu schützen, sodass sie im Falle eines Angriffs oder Datenlecks unbrauchbar bleiben.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/8151-Dragonforce-IKAV.png

Was lernen wir daraus:
Unzureichender Schutz von sensiblen Daten kann zu schwerwiegenden Folgen für die betroffenen Personen führen, einschließlich Identitätsdiebstahl oder finanziellen Schäden und kann zudem rechtliche und finanzielle Strafen für die verantwortlichen Unternehmen nach sich ziehen. Ein effektives Sicherheitskonzept ist daher unerlässlich, um sowohl die Privatsphäre der Nutzer als auch die Integrität der Organisation zu wahren.

RIEDEL

Wir wissen wo dein Auto steht

27. Dezember 2024, in Wolfsburg/Niedersachsen

DATENLECK

SICHERHEITSLÜCKE

KONFIGURATIONSFEHLER

Was ist passiert?
Am 27. Dezember 2024 wurde auf dem 38. Chaos Computer Congress eine schwerwiegende Sicherheitslücke bei einem Tochterunternehmen eines führenden deutschen Automobilherstellers aufgedeckt. Ein ungeschützter Memory-Dump auf einem Webserver enthielt Zugangsdaten zu einem Amazon AWS-Cloudspeicher, in dem detaillierte Daten von 800.000 E-Fahrzeugen gespeichert waren. Diese beinhalteten präzise Geodaten und persönliche Informationen, darunter E-Mail-Adressen und Telefonnummern, von Privatpersonen sowie hochrangigen Politikern, DAX-Vorständen und sogar Bundesnachrichtendienst-Mitarbeitern.

Was hätte man besser machen können?
Eine vollumfängliche Sicherheitsstrategie, die u. a. regelmäßige Sicherheitsüberprüfungen und Penetrationstests umfasst wären notwendig gewesen. Sensible Daten hätten stets verschlüsselt und sicher gespeichert werden müssen, um unbefugten Zugriff zu verhindern. Zudem hätte der Memory-Dump durch eine strikte Zugriffskontrolle und ordnungsgemäße Datensicherung geschützt werden müssen.

Anzunehmende Schadensfelder:

Quellen
https://www.spiegel.de/netzwelt/web/volkswagen-konzern-datenleck-wir-wissen-wo-dein-auto-steht-a-e12d33d0-97bc-493c-96d1-aa5892861027
https://www.adac.de/news/vw-datenleck/
https://www.ccc.de/de/updates/2024/wir-wissen-wo-dein-auto-steht

Was lernen wir daraus:

Der Chaos Computer Congress (CCC) ist eine bedeutende Veranstaltung, die seit Jahren eine zentrale Plattform für den Austausch über IT-Sicherheit, Datenschutz und digitale Rechte bietet. Der Vortrag über diese Sicherheitslücke verdeutlicht die Rolle des CCC als „Weckruf“ für die IT-Community. Hier werden Schwachstellen aufgedeckt und Unternehmen auf ihre Sicherheitsdefizite hingewiesen, was zur Verbesserung der Cybersicherheit beiträgt.

RIEDEL

Digital in die Zukunft, aber sicher!

27. Dezember 2024, in Hamburg/Hamburg

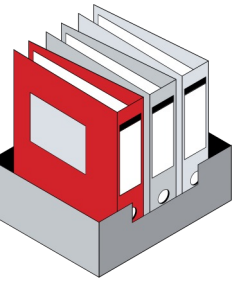
SICHERHEITSLÜCKE

Was ist passiert?
Ein schwerwiegender Sicherheitsvorfall erschüttert das Gesundheitssystem: Auf dem 38. Chaos Computer Congress demonstrierten IT-Experten, wie Angreifer weiterhin auf die elektronischen Patientenakten von 70 Millionen Versicherten zugreifen könnten. Mit einfachen Methoden lassen sich fremde Gesundheitskarten auslesen und Zugangsdaten erlangen. Zudem könnten Angreifer über unsichere Praxisverwaltungssysteme oder den Gebrauchtmarkt an kritische Zugangsdaten gelangen.

Was hätte man besser machen können?
Um Sicherheitslücken in der elektronischen Patientenakte (ePA) zu vermeiden, müssen Zugriffsmechanismen durch starke Authentifizierung und kryptografische Absicherung verbessert werden. Zudem sollten Praxisverwaltungssysteme besser gesichert und regelmäßigen Sicherheitsprüfungen unterzogen werden.

Was lernen wir daraus:

Die Verwundbarkeit medizinischer Daten betrifft nicht nur den Datenschutz, sondern kann auch weitreichende Folgen für Patienten haben – von Identitätsdiebstahl bis hin zur Manipulation sensibler Gesundheitsinformationen. Auch das Vertrauen in digitale Gesundheitslösungen kann durch solche Sicherheitslücken massiv beeinträchtigt werden.



Anzunehmende Schadensfelder:

Quellen
https://www.ccc.de/en/updates/2024/ende-der-epa-experimente
https://netzpolitik.org/2024/chaos-communication-congress-das-narrativ-der-sicheren-elektronischen-patientenakte-ist-nicht-mehr-zu-halten/

RIEDEL

Diebstahl: Kundendaten, Backups, Personal-dokumente etc. geraten in fremde Hände

20. Dezember 2024, in Gera/Thüringen

DATENDIEBSTAHL

DATENLECK

RANSOMWARE

Was ist passiert?
Die Ransomwaregruppe Morpheus hat im Dezember 2024 den Anbieter eines Zeiterfassungssystems, als Opfer gelistet. Seit dem 20. Dezember 2024 behaupten die Angreifer, sie hätten Kundendaten, Backups, Personaldokumente und technische Details gestohlen. Um ihre Behauptung zu untermauern, veröffentlichten sie Auszüge aus der Kundendatenbank sowie Bilder von Mitarbeitern und internen Dokumenten auf ihrer Leak-Seite.

Was hätte man besser machen können?
Ein Security Operations Center (SOC) hätte eine durchgehende Überwachung ermöglichen können. Ergänzend wäre ein Security Information and Event Management (SIEM)-System sinnvoll gewesen, um sicherheitsrelevante Ereignisse zentral zu analysieren.

Was lernen wir daraus:

Die Folge eines solchen Sicherheitsvorfalls kann zu Social Engineering führen. Bei Social Engineering wird menschliches Vertrauen ausgenutzt, um an vertrauliche Informationen zu gelangen. Angreifer geben sich oft als vertrauenswürdige Personen aus und verleiten Opfer dazu, Zugangsdaten preiszugeben oder schädliche Aktionen auszuführen.

Ein typisches Beispiel für Social Engineering ist eine E-Mail, in der sich der Täter als Personalmitarbeiter eines Unternehmens ausgibt und dem Empfänger eine vermeintliche Gehaltsabrechnung zusendet. Der Anhang, der angeblich die Abrechnung enthält, ist jedoch ein schadhafter Link oder eine Datei, die Malware auf dem Computer des Opfers installiert

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7916-Morpheus-Pus.PNG

RIEDEL

Ransomware-Angriff trifft Medienunternehmen aus Thüringen

20. Dezember 2024, in Grammetal/Thüringen

EINBRUCH

DATENDIEBSTAHL

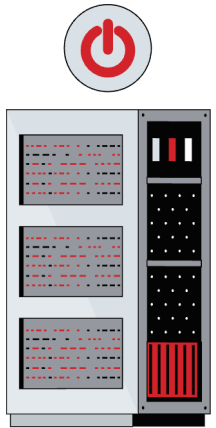
RANSOMWARE

Was ist passiert?
Kurz vor den Weihnachtsfeiertagen erklärte am 20. Dezember 2024 die „Fog"-Ransomwaregruppe, ein deutsches Medienunternehmen angegriffen zu haben. Auf ihrer Leakseite behaupten die Cyberkriminellen 6,8 GB hochsensibler Daten gestohlen zu haben, darunter Finanzdokumente, Mitarbeiter- und Kundenkontakte sowie Verschwiegenheitserklärungen.

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. Zudem wäre es ratsam gewesen, regelmäßig Schwachstellenanalysen durchzuführen. Diese helfen dabei, Sicherheitslücken frühzeitig zu identifizieren und zu schließen, bevor sie von Angreifern ausgenutzt werden können.

Was lernen wir daraus:

Durch die Veröffentlichung von Personaldokumenten und Mitarbeiterbildern könnten Cyberkriminelle diese Informationen nutzen, um gezielte Phishing-Angriffe oder Betrugsversuche durchzuführen. Zusätzlich kann die Veröffentlichung sensibler Unternehmensdaten dazu führen, dass Konkurrenten oder andere böswillige Akteure interne Strukturen, technische Details oder Geschäftsgeheimnisse ausnutzen, was langfristige wirtschaftliche Schäden nach sich ziehen kann.



Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7751-Fog-Schenkelberg.png

RIEDEL

Veröffentlichung von Reisepässen und technische Zeichnungen als Druckmittel

19. Dezember 2024, in Grünberg/Hessen

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Mitte Dezember 2024 tauchte ein Elektrotechnik-Unternehmen aus Hessen auf der Leak-Seite der Ransomwaregruppe BlackBasta auf. Die Hacker behaupten, 1,1 TB an sensiblen Daten erbeutet zu haben, darunter vertrauliche Unternehmensunterlagen und Personaldaten. Als Beweis veröffentlichten sie Dokumente wie Reisepässe und technische Zeichnungen. Sollte keine Einigung erzielt werden, droht die Veröffentlichung der Daten am pünktlich zu Weihnachten.

Was hätte man besser machen können?
Das Elektrotechnik-Unternehmen hätte mit einem Zero-Trust-Ansatz und strikten Zugriffskontrollen das Risiko minimieren können. Ein SOC mit SIEM-System hätte verdächtige Aktivitäten frühzeitig erkannt. Zudem hätten Mitarbeiterschulungen das Bewusstsein für Phishing-Angriffe gestärkt und so potenzielle Einfallstore geschlossen.

Was lernen wir daraus:

Ein absoluter Schutz vor Cyberangriffen ist zwar nicht realisierbar, doch durch kontinuierliche Sicherheitsmaßnahmen können Unternehmen das Risiko erheblich minimieren. Investitionen in präventive Maßnahmen wie Netzwerküberwachung, Zugriffskontrollen und Security Awareness zahlen sich langfristig aus. Die finanziellen Aufwendungen für eine robuste IT-Sicherheit stehen schließlich in keinem Verhältnis zu den potenziellen Schäden eines erfolgreichen Cyberangriffs.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7745-BlackBasta-Bender.PNG

RIEDEL

Mail-Flooding legt Kontaktformulare deutscher Behörden lahm

18. Dezember 2024, in Bremen/Bremen

AUSFALL

Was ist passiert?
In der Nacht zum 18. Dezember 2024 erlebten mehrere deutsche Behörden einen koordinierten Cyberangriff. Ein Botnetz überflutete die interaktiven Kontaktformulare mit Tausenden Spam-Mails, wodurch insbesondere das Gesundheits-, Sozial- und Bauressort sowie die Polizei betroffen waren. Innerhalb kurzer Zeit gingen allein im Gesundheitsressort 2.000 Mails ein. Um den Angriff einzudämmen, wurden die Formulare umgehend deaktiviert.

Was hätte man besser machen können?
Durch eine begrenzte Anzahl von Formularübermittlungen pro Minute pro IP-Adresse hätte der Angriff stark verlangsamt werden können. Eine weitere Option wäre gewesen, dass nach einer bestimmten Anzahl von Versuchen die IP temporär hätte gesperrt werden können.

Was lernen wir daraus:

Mail-Flooding wird gern als Ablenkungstaktik genutzt, um IT-Teams zu überlasten. Während diese mit der Abwehr tausender Spam-Mails beschäftigt sind, bleibt wenig Zeit, um andere Sicherheitsvorfälle zu erkennen – insbesondere wenn keine überwachenden Systeme wie SIEM oder ein SOC für präventiven Schutz sorgen.

Anzunehmende Schadensfelder:

Quellen
https://www.butenunbinnen.de/nachrichten/angriff-gesundheitsressort-bremen-100.html
https://www.weser-kurier.de/bremen/cyberangriff-auf-bremer-behoerden-und-die-polizei-doc7yj9vfu6wy917ah6eegi

RIEDEL

Russische Hackergruppe NoName057(16) attackiert mehrere deutsche Unternehmen

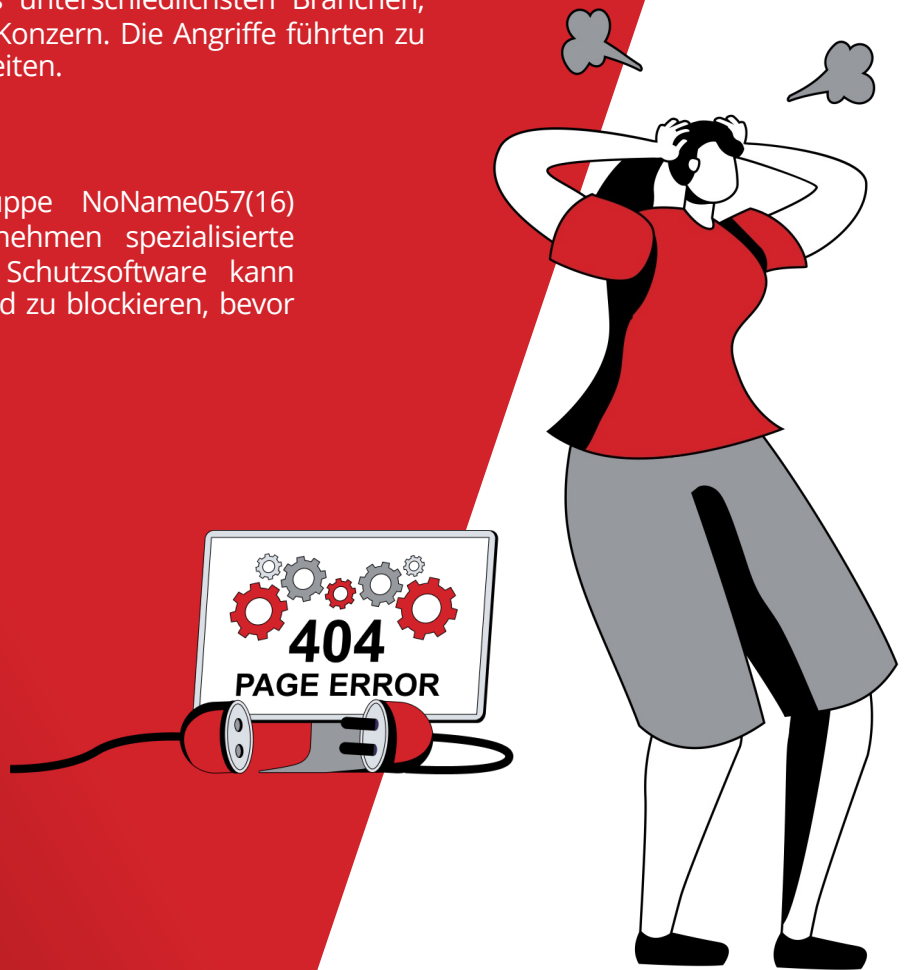
17. Dezember 2024, in Deutschland

AUSFALL

DDoS

Was ist passiert?
Am 17. Dezember 2024 wurden mehrere deutsche Unternehmen Opfer massiver DDoS-Angriffe durch die russische Gruppe NoName057(16). Ziel war es nicht, Lösegeld zu erpressen, sondern eine politische Botschaft zu senden. Unter den Opfern befanden sich Unternehmen aus unterschiedlichsten Branchen, darunter ein Waffenhersteller und ein Energie-Konzern. Die Angriffe führten zu stundenlangen Ausfällen der betroffenen Webseiten.

Was hätte man besser machen können?
Um die DDoS-Angriffe der russische Gruppe NoName057(16) abzuwehren, hätten die betroffenen Unternehmen spezialisierte DDoS-Schutzsoftware nutzen sollen. Solche Schutzsoftware kann helfen, den schädlichen Traffic zu erkennen und zu blockieren, bevor er das interne Netzwerk erreicht.



Was lernen wir daraus:

Dieser Vorfall verdeutlicht, dass Cyberangriffe nicht immer nur finanziellen Ertrag zum Ziel haben. In diesem Fall ging es den Angreifern darum, mit ihren DDoS-Attacken eine politische Botschaft zu verbreiten. Unternehmen sollten sich bewusst sein, dass solche Angriffe auch Teil größerer geopolitischer Konflikte sein können. Es ist wichtig, nicht nur auf finanzielle Bedrohungen vorbereitet zu sein, sondern auch auf Angriffe, die mit politischen oder ideologischen Zielen verbunden sind.

Anzunehmende Schadensfelder:

Quellen
https://www.heise.de//news/DDoS-Kampagne-Cyberkriminelle-legen-deutsche-Firmen-Websites-lahm-10202521.html

RIEDEL

DDoS-Attacke auf das Bundesinnenministerium

17. Dezember 2024, in Berlin/Berlin

DDoS

AUSFALL

Was ist passiert?
Ein Cyberangriff legte die Webseite des Bundesinnenministeriums (BMI) für über zwei Stunden lahm. Von 12:30 bis 14:30 Uhr war die Seite aufgrund einer DDoS-Attacke nicht erreichbar, bei der Server durch massenhafte Anfragen überlastet wurden. Das Informationstechnikzentrum Bund (ITZ Bund) bestätigte den Angriff, nannte jedoch keine weiteren Details zu den Hintergründen.

Was hätte man besser machen können?
Um einen DDoS-Angriff zu verhindern, hätte das Bundesinnenministerium verstärkt auf DDoS-Schutzmaßnahmen setzen können, wie etwa leistungsstarke Traffic-Filter, Rate-Limiting zur Begrenzung von Anfragen. Zudem könnten KI-gestützte Erkennungssysteme helfen, ungewöhnlichen Datenverkehr frühzeitig zu identifizieren und abzuwehren.

Was lernen wir daraus:

Der Vorteil einer DDoS-Attacke gegenüber anderen Cyberangriffen liegt für die Angreifer in ihrer einfachen Durchführung und schnellen Wirkung. Sie erfordert keinen direkten Zugriff auf das Zielsystem, sondern nutzt die schiere Masse an Anfragen, um Server lahmzulegen. Zudem ist sie schwer zurückzuverfolgen, da oft ein Botnetz aus weltweit verteilten Rechnern genutzt wird. Im Gegensatz zu gezielten Cyberangriffen, die Sicherheitslücken ausnutzen müssen, kann eine DDoS-Attacke ohne tiefgehendes Hacking-Wissen großen Schaden anrichten und öffentliche Aufmerksamkeit erzeugen.

Anzunehmende Schadensfelder:

Quellen
https://www.t-online.de/nachrichten/deutschland/militaer-verteidigung/id_100554736/cyber-angriff-faesers-innenministerium-stundenlang-lahmgelegt.html
https://www.oldenburger-onlinezeitung.de/nachrichten/cyberangriff-auf-bundesinnenministerium-143348.html

RIEDEL

Mitarbeiterin unter dem Visier der Staats-anwaltschaft – Datenklau in großen Mengen

11. Dezember 2024, in Broderstorf/Mecklenburg-Vorpommern

DATENDIEBSTAHL

INNENTÄTER

Was ist passiert?
Im Dezember 2024 wurde bekannt, dass eine ehemalige Mitarbeiterin des Einwohnermeldeamts der Stadt Rostock Daten von über 100 Stadtbeschäftigten, Richtern und deren Familienangehörigen gestohlen hatte. Der Vorfall kam ans Licht, nachdem die Stadt Ende Juli 2024 auf einen möglichen Datendiebstahl hingewiesen wurde und die Staatsanwaltschaft Ermittlungen aufnahm. Die Mitarbeiterin hatte sich unbefugt Zugang zu den Daten verschafft, indem sie das Passwort einer Kollegin verwendete. Betroffene wurden im Oktober und November 2024 informiert. Bei einer späteren Hausdurchsuchung wurden weitere gestohlene Daten sichergestellt

Was hätte man besser machen können?
Um den Missbrauch des Passworts zu verhindern, hätte das Einwohnermeldeamt individuelle Passwörter für jeden Mitarbeiter sowie eine Zwei-Faktor-Authentifizierung (2FA) einführen müssen. Zudem wären regelmäßige Passwortänderungen und eine strikte Überwachung von Zugriffsrechten sowie -protokollen sinnvoll gewesen, um unbefugten Zugriff frühzeitig zu erkennen und zu verhindern.

Was lernen wir daraus:

Bedrohungen kommen nicht nur von außen, sondern können auch innerhalb eines Unternehmens/einer Organisation entstehen. Nicht immer sind es externe Hacker die Schaden anrichten – oft reichen bereits kleine Fehler oder interne Sicherheitslücken aus. Deshalb ist es essenziell, umfassende Schutzmaßnahmen zu ergreifen, um sowohl externe Angriffe als auch interne Risiken effektiv zu minimieren.

Anzunehmende Schadensfelder:

Quellen
https://www.ndr.de/nachrichten/mecklenburg-vorpommern/Datenleck-im-Rostocker-Rathaus-beschaeftigt-Staatsanwaltschaft,rostock1766.html
https://www.nordkurier.de/regional/rostock/rathaus-mitarbeiterin-soll-in-rostock-persoenliche-daten-von-buergern-gesammelt-haben-3156212

RIEDEL

Krankenhaushacker werden rechtzeitig abgewehrt

10. Dezember 2024, in Ingolstadt/Bayern

EINBRUCH

Was ist passiert?
Ein Krankenhaus in Ingolstadt gab bekannt, dass es Ziel eines Cyberangriffs wurde. In einer Mitteilung wurde versichert, dass die Patientenversorgung weiterhin gewährleistet sei und ein IT-Dienstleister zur Lösung des Vorfalls eingeschaltet wurde. Details zum Angriff wurden aus ermittlungstaktischen Gründen nicht veröffentlicht. Später wurde mitgeteilt, dass der Angriff bereits einen Tag früher stattfand und in der "Ausspähphase" erkannt wurde. Das Krankenhaus bestätigte, dass die anfängliche Einschätzung, der Angriff habe wenig Auswirkungen auf die Betriebs- und Systemlandschaft, sich als korrekt erwies.

Was hätte man besser machen können?
Auch wenn der Angriff in der Ausspähungsphase erkannt wurde, hätten fortschrittliche Monitoring-Lösungen, die ungewöhnlichen Aktivitäten schneller identifizieren helfen können, noch früher auf verdächtige Vorgänge zu reagieren. Ein proaktives und sofortiges Einspielen von Sicherheits-Patches könnte dazu beitragen, Schwachstellen zu schließen, die möglicherweise den Angriff ermöglicht haben.

Anzunehmende Schadensfelder:

Quellen
https://www.br.de/nachrichten/bayern/hackerangriff-auf-klinikum-ingolstadt-lka-ermittelt,UWY2GmK
https://klinikum-ingolstadt.de/pressemitteilungen/it-sicherheitsvorfall-am-klinikum-ingolstadt/

Was lernen wir daraus:

Die Ausspähphase ist der erste Schritt eines Cyberangriffs, in dem die Angreifer versuchen, Informationen über das Zielsystem zu sammeln, ohne sofort aktiv in die IT-Infrastruktur einzugreifen. In dieser Phase scannen sie Netzwerke, identifizieren Schwachstellen und suchen nach potenziellen Einfalltoren, die für einen späteren Angriff ausgenutzt werden können. Ziel ist es, möglichst viele Informationen zu sammeln, um später gezielt und mit minimalem Risiko in das System einzudringen oder sensible Daten zu stehlen.

RIEDEL

Ärztezentrum: Behandlungsakten und Personalausweise von Patienten veröffentlicht

9. Dezember 2024, in Hof/Bayern

DATENLECK

RANSOMWARE

DATENDIEBSTAHL

AUSFALL

Was ist passiert?

Die Ransomware-Gruppe *Cloak* gab bekannt, die Website einer orthopädischen und neurochirurgischen Praxis angegriffen zu haben. Nach Ablauf einer Frist am 9. Dezember 2024 stellte die Gruppe 100 GB gestohlene Daten auf ihrem Blog zum Download bereit. Screenshots von sensiblen Daten wie Behandlungsakten und Personalausweisen wurden als Beweis veröffentlicht, deren Echtheit jedoch noch nicht bestätigt werden konnte. Auf der Webseite des Gesundheitsdienstleisters wird mitgeteilt, dass die Systeme bis zum 9. Dezember noch nicht vollständig wiederhergestellt waren.

Was hätte man besser machen können?

Das Zentrum hätte durch den Einsatz von Zero-Trust-Sicherheitsmodellen, regelmäßige Sicherheitsaudits und schnelle Incident-Response-Maßnahmen den Angriff möglicherweise verhindern oder eindämmen können. Zudem wären verschlüsselte Daten und Offsite-Backups entscheidend gewesen, um den Schaden zu minimieren und Erpressungen ins Leere laufen zu lassen.

Was lernen wir daraus:

Ein Offsite-Backup wäre entscheidend gewesen, um die Daten unabhängig vom gehackten System schnell wiederherstellen zu können. Dabei handelt es sich um eine Sicherung, die an einem externen Ort gespeichert wird – physisch oder in der Cloud. So bleibt ein Zugriff auch nach einem Cyberangriff möglich. Ohne ein solches Backup verzögert sich die Wiederherstellung erheblich, was zu langen Ausfällen und Datenverlust führt.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7634-Cloak-orthopaedie-hof-1.png
https://www.security-incidents.de/assets/img/incidents/7634-Cloak-orthopaedie-hof-2.png

RIEDEL

Daten aus Personalabteilung entwendet

5. Dezember 2024, in Thalmässing/Bayern

RANSOMWARE

EINBRUCH

DATENDIEBSTAHL

Was ist passiert?
Ein Handelsunternehmen für Eisenwaren und Maschinen wurde auf der Opferliste einer Ransomware-Gruppe gelistet. Die Gruppe behauptet, 1 GB an Daten aus der Personalabteilung erlangt zu haben, darunter Kontaktdaten und E-Mail-Adressen von Mitarbeitenden. Das Unternehmen hat bislang keine Stellungnahme zu den Vorwürfen abgegeben und die Webseite ist weiterhin uneingeschränkt erreichbar.

Was hätte man besser machen können?
Der Einsatz fortschrittlicher IT-Sicherheitslösungen hätte den Angriff möglicherweise verhindert. SIEM & SOC hätten Bedrohungen frühzeitig erkannt, XDR und EDR hätten umfassende Schutzmaßnahmen geboten, und SOAR hätte automatisierte Reaktionen ermöglicht.

Next-Generation Firewalls, (D)DoS Protection, SD-WAN und SASE hätten zusätzlichen Schutz und Netzwerksicherheit gewährleistet

Was lernen wir daraus:

Die Zusammenarbeit mit einem Anbieter von Managed IT-Security Lösungen kann entscheidend sein, um die Auswirkungen eines Cyberangriffs zu begrenzen. Neben finanziellen Schäden durch Betriebsunterbrechungen und Wiederherstellungsmaßnahmen können auch rechtliche Konsequenzen und Reputationsverluste entstehen. Durch präventive Sicherheitsmaßnahmen und eine schnelle Reaktion im Ernstfall lassen sich diese Risiken erheblich reduzieren.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7587-FOG-Dorner.png

RIEDEL

Universität in Frankfurt: Opfer einer Ransomware-Attacke

4. Dezember 2024, in Frankfurt am Main/Hessen

RANSOMWARE

EINBRUCH

DATENDIEBSTAHL

Was ist passiert?

Am 3. Dezember 2024 bekannte sich die Ransomware-Gruppe RansomHub zu einem Angriff auf die Goethe-Universität Frankfurt. Laut eigenen Angaben haben die Täter 180 GB sensibler Daten erlangt und als Beweis eine Budgeteinteilung von 2020 veröffentlicht. Unklar ist, ob auch andere Rhein-Main-Universitäten betroffen sind, da sie in der Mitteilung erwähnt werden. Die Gruppe droht mit der vollständigen Veröffentlichung der Daten, falls ihre Lösegeldforderung bis zum nicht erfüllt wird.

Was hätte man besser machen können?

Zum einen hätte die Implementierung von fortschrittlichen Verschlüsselungstechnologien geholfen, sensible Daten zu schützen und den Zugriff von unbefugten Dritten zu verhindern. Zum anderen hätte eine Proaktive Überwachung und kontinuierliche Netzwerküberprüfung, die Universität in die Lage versetzt, Anomalien frühzeitig zu erkennen und darauf zu reagieren.

Was lernen wir daraus:

Universitäten sind attraktive Ziele für Ransomware-Gruppen, weil sie oft über wertvolle, sensible Daten verfügen und oft keine ausreichend robusten Cybersicherheitsmaßnahmen verfolgen. Viele Hochschulen speichern Forschungsdaten, persönliche Informationen von Studierenden und Mitarbeitenden sowie finanzielle Informationen, die für Angreifer von hohem Wert sind. Zudem sind Universitäten häufig in großem Maßstab vernetzt, was Angreifern mehr potenzielle Einfallspunkte bietet.

Anzunehmende Schadensfelder:

Quellen

https://www.security-incidents.de/assets/img/incidents/7563-RansomHub-Goethe-Universit%C3%A4t-Frankfurt-2.png

https://www.security-incidents.de/assets/img/incidents/7563-RansomHub-Goethe-Universit%C3%A4t-Frankfurt-1.png

RIEDEL

Technologiehersteller auf Opferliste erfasst

4. Dezember 2024, in Neu-Isenburg/Hessen

RANSOMWARE

DATENDIEBSTAHL

ERPRESSUNG

Was ist passiert?
Ein Technologiehersteller wurde womöglich Opfer eines Angriffs der *Black Basta* Gruppe. Sie setzten dem Unternehmen eine Frist bis zum 11. Dezember, nach deren Ablauf sie planen 700 GB erbeuteter Daten zu veröffentlichen.

Was hätte man besser machen können?
Das Unternehmen hätte regelmäßige Sicherheitsüberprüfungen, Schulungen für Mitarbeiter und starke Verschlüsselung einsetzen sollen. Darüber hinaus wären regelmäßige Backups und die Implementierung einer Zwei-Faktor-Authentifizierung wichtige Maßnahmen gewesen, um den Schutz sensibler Daten weiter zu erhöhen und die Auswirkungen eines möglichen Angriffs zu minimieren.

Was lernen wir daraus:

In den letzten Jahren hat sich Cybercrime erheblich gewandelt, weshalb Unternehmen dazu gezwungen sind, sich intensiver damit auseinanderzusetzen. Angriffe sind zunehmend zielgerichtet und professionell, mit Fokus auf Ransomware, Datenexfiltration und Doppel-Erpressung. Kriminelle nutzen ausgeklügelte Phishing-Techniken und Zero-Day-Exploits, während Cyberkriminalität als Service angeboten wird.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7576-beko-technologies-black-basta.png

RIEDEL

Netzwerkspeicher und Zugangsdaten des LKA Brandenburg zeitweise öffentlich zugänglich

3. Dezember 2024, in Eberswalde/Brandenburg

DATENLECK

SICHERHEITSLÜCKE

Was ist passiert?
Laut dem *Tagesspiegel* kam es beim LKA Brandenburg zu einem gravierenden Datenleck. Ein ungeschützter Netzwerkspeicher des Staatsschutzes, der unter anderem BKA-Server-Passwörter enthielt, war bis September 2024 öffentlich zugänglich. Ein Bürger entdeckte das Leck zufällig, als er ein Hinweisportal nutzen wollte. Am 20. September 2024 wurden das Innenministerium und die Datenschutzbeauftragte informiert. Das BKA unterbrach daraufhin zeitweise den Datenaustausch mit dem LKA. Untersuchungen ergaben, dass ein ranghoher Mitarbeiter, die Zugangsdaten ungeschützt speicherte. Zudem war der Speicher ohne Firewall erreichbar und auch das behördliche WLAN war nicht ausreichend gesichert.

Was hätte man besser machen können?
Grundlegende IT-Sicherheitsstandards hätten eingehalten werden müssen. Sensible Daten wie BKA-Zugangsdaten hätten verschlüsselt und nur auf gesicherten Systemen gespeichert werden dürfen, dafür wäre eine Schulung der Mitarbeiter unverzichtbar gewesen. Zudem hätte der Netzwerkspeicher durch Firewalls und Zugriffsbeschränkungen geschützt sein müssen.

Was lernen wir daraus:

Beim Staatsschutz ist die IT-Sicherheit besonders kritisch, da er mit hochsensiblen Informationen arbeitet – etwa zu Terrorismus, Spionage oder organisierter Kriminalität. Ein Datenleck kann nicht nur Ermittlungen gefährden, sondern auch die nationale Sicherheit bedrohen.

Anzunehmende Schadensfelder:

Quellen
https://www.tagesspiegel.de/potsdam/brandenburg/it-sicherheit-beim-lka-staatsschutz-akut-gefahrdet-bka-kappte-datenaustausch-mit-brandenburgs-polizei-12810017.html
https://www.rbb24.de/panorama/beitrag/2024/12/brandenburg-landeskriminalamt-datenleck-it-sicherheit-digitale-sicherheit-hacker.html

RIEDEL

Christopher Schwefel
Cyber Security Engineer

Peter Pillath
Geschäftsbereichsleiter Cyber + Crime

GASTARTIKEL

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

NOVEMBER 2024

SECURITY INCIDENTS GERMANY

RIEDEL

1 TB Daten von Sicherheitstechnik Unternehmen entwendet

19. November 2024, in Brilon/Nordrhein-Westfalen

RANSOMWARE

DATENDIEBSTAHL

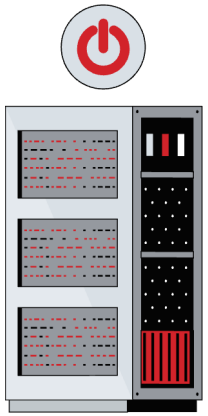
ERPRESSUNG

Was ist passiert?
Am 19. November 2024 wurde ein Unternehmen für Sicherheitstechnik von der Black Basta-Ransomwaregruppe als Opfer gelistet. Die Täter behaupten, 1 TB an Daten entwendet zu haben und drohen, diese nach Ablauf einer Frist zu veröffentlichen, insofern kein Lösegeld gezahlt wird. Die Firma bestätigte den Angriff auf seiner Webseite und gab an, an der Wiederherstellung der betroffenen Systeme zu arbeiten, wobei es zu Verzögerungen in der Kommunikation kommen könnte.

Was hätte man besser machen können?
Regelmäßige Sicherheitsaudits und Netzwerksegmentierung hätten der Angriff verhindern oder zumindest die Auswirkungen minimieren können. Zudem wären regelmäßige Backups und ein klarer Notfallplan für die Wiederherstellung von Systemen entscheidend, um Ausfallzeiten zu verkürzen und eine schnelle Reaktion zu ermöglichen.

Was lernen wir daraus:

Es gibt Programme und Dienste, die versprechen, von Ransomware verschlüsselte Daten wiederherzustellen. Diese Entschlüsselungstools sind jedoch nicht immer effektiv, insbesondere bei neueren und komplexeren Varianten von Ransomware. Daher ist es ratsam ein Netzwerk schon präventiv zu schützen und eine robuste Verteidigungslinie aufzubauen bevor es zu spät ist.



Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7411-rembe-black-basta-mitteilung.png
https://www.security-incidents.de/assets/img/incidents/7411-rembe-black-basta.png

RIEDEL

Händler für KFZ-Teile wird Opfer von einem Ransomware-Angriff

19. November 2024, in Norderstedt/Schleswig-Holstein

RANSOMWARE

EINBRUCH

DATENDIEBSTAHL

Was ist passiert?
Am 19. November 2024 wurde ein Händler für Kfz-Ersatzteile auf der Darknet-Seite von RansomHub als Opfer eines Ransomware-Angriffs gelistet. Die Täter stellten einige gestohlene Dateien als Beweismittel zum Download bereit.

Was hätte man besser machen können?
Das angegriffene Unternehmen hätte den Angriff durch die Integration eines Managed-SIEM mit entsprechendem 24/7 Security Operations Center früher entdecken können. Dadurch hätte man die Entwendung der Daten durch eine frühzeitigere Reaktion ggf. vermeiden können.

Was lernen wir daraus:

Angreifer streben danach, unbemerkt in ein fremdes Netzwerk einzudringen. Dies kann durch verschiedene Methoden geschehen, wie das Versenden von Phishing-Links, der Erwerb von Anmeldedaten im Darknet oder das Installieren kostenloser Software, die heimlich „Info-Stealer"-Malware auf dem Computer eines ahnungslosen Nutzers platziert. Diese Malware sammelt vertrauliche Informationen und leitet sie weiter.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7418-RansomHub-Handelsgesellschaft-Wulff.png

RIEDEL

Kurzzeitige Systemabschaltung im Ingenieursbüro

19. November 2024, in Esslingen/Baden-Württemberg

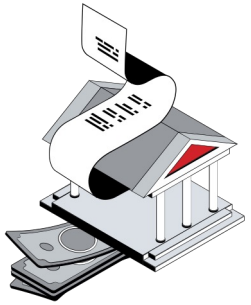
RANSOMWARE

Was ist passiert?
Laut mehreren Quellen wurde ein Ingenieursbüro am 19. November 2024 von der Ransomware-Gruppe „Safepay“ angegriffen. Das Unternehmen bestätigte den Vorfall auf seiner Webseite und gab an, seine Systeme vorübergehend offline genommen zu haben. Der Normalbetrieb sei jedoch zügig wieder aufgenommen worden, und es gebe keine Bedenken hinsichtlich der Sicherheit von Unternehmensportalen und E-Mails.

Was hätte man besser machen können?
Das Ingenieurbüro hätte auf Netzwerksegmentierung setzen können, um bei einem Angriff die Ausbreitung der Ransomware zu begrenzen. Ein Intrusion Detection System (IDS) hätte verdächtige Aktivitäten schneller identifizieren können. Verschlüsselung sensibler Daten und regelmäßige Penetrationstests wären ebenfalls sinnvoll gewesen, um Schwachstellen frühzeitig zu erkennen und zu beheben.

Was lernen wir daraus:

Ein Intrusion Detection System (IDS) ist ein Sicherheitssystem, das den Netzwerkverkehr oder die Systemaktivitäten überwacht, um verdächtige oder unbefugte Aktivitäten zu erkennen. Es kann potenzielle Angriffe oder Sicherheitsverletzungen identifizieren, indem es nach Mustern sucht, die auf eine Bedrohung hindeuten, und Alarme auslöst, wenn solche Aktivitäten festgestellt werden.



Anzunehmende Schadensfelder:

Quellen
https://www.ransomware.live/id/aWItc3BpZXRoLmRlOHNhZmVwYXk=
https://ransomfeed.it/index.php?page=post_details&id_post=18831
https://www.security-incidents.de/assets/img/incidents/7420-ib-spieth-safepay.png

RIEDEL

Unternehmen aus der Elektrobranche: 16 GB sensibler Daten entwendet

18. November 2024, in München/Bayern

DATENLECK

RANSOMWARE

EINBRUCH

DATENDIEBSTAHL

Was ist passiert?
Ein renommiertes Unternehmen aus der Elektrobranche gerät ins Visier der Akira-Ransomwaregruppe: Am 18. November 2024 veröffentlicht die Hackergruppe einen Torrent-Link zu 16 GB sensibler Daten, die angeblich von einer übernommenen Tochtergesellschaft stammen. Die gestohlenen Daten sollen Passwörter, Logins und persönliche Informationen des Personals enthalten.

Was hätte man besser machen können?
Das Unternehmen hätte eine Multifaktor-Authentifizierung (MFA) für den Zugang zu sensiblen Systemen einsetzen sollen. Zusätzlich wären regelmäßige Schulungen der Mitarbeiter zur Erkennung von Phishing-Angriffen und eine proaktive Überwachung auf verdächtige Aktivitäten hilfreich gewesen, um den Angriff frühzeitig zu erkennen und abzuwehren.

Was lernen wir daraus:

Ein Torrent-Link verweist auf eine Datei, die über das BitTorrent-Protokoll heruntergeladen wird. Dabei wird die Datei nicht von einem einzelnen Server, sondern von mehreren Nutzern gleichzeitig bereitgestellt, die die Datei bereits besitzen. Torrent-Links werden oft für große Dateien genutzt und können auch zur Verbreitung gestohlener Daten verwendet werden, da er dabei hilft Daten effizient und anonym zu verbreiten. Da die Datei über viele verschiedene Nutzer heruntergeladen wird, ist es für die Strafverfolgung schwieriger, den Ursprung des Downloads zurückzuverfolgen.

Anzunehmende Schadensfelder:

Quellen
https://www.ransomware.live/id/SGEnZXIgR3JvdXBAYWtpcmE=

RIEDEL

Datenleck in Wirtschaftsauskunftei: Millionen Bonitätsscores einsehbar

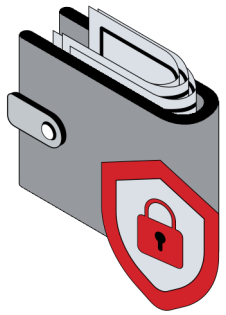
18. November 2024, in Baden-Baden/Baden-Württemberg

DATENLECK

Was ist passiert?
Die Sicherheitsforscherin Lilith Wittmann entdeckte eine gravierende Sicherheitslücke bei einer der wichtigsten Wirtschaftsauskunftei Deutschlands. Über das von Smava betriebene Portal "Scorekompass" konnte sie den Identifizierungsprozess umgehen und direkten Zugriff auf die Bonitätsdaten von Millionen Verbrauchern erhalten. Dazu gehörten Informationen über Mahnverfahren, Privatinsolvenzen und die Bonitäts-Scores aller Verbraucher in Deutschland.

Was hätte man besser machen können?
Der Identifizierungsprozess hätte mit stärkeren Verifizierungsmethoden sicherer gemacht werden sollen. Zudem wären bessere Zugriffs- und Berechtigungskontrollen sowie ein umfassendes Monitoring nötig gewesen, um unberechtigte Abfragen zu verhindern.

Was lernen wir daraus:
Dieser Vorfall hat schwerwiegende Konsequenzen für die Allgemeinheit, da er das Vertrauen in die Sicherheit persönlicher Finanzdaten erschüttert. Wenn solche sensiblen Informationen wie Bonitätsdaten und Insolvenzen so leicht zugänglich sind, gefährdet das die Privatsphäre der betroffenen Personen und eröffnet Möglichkeiten für Identitätsdiebstahl und Betrug. Zudem wird deutlich, wie wichtig es ist, dass Unternehmen, die mit persönlichen Daten arbeiten, strengere Sicherheitsvorkehrungen treffen, um das Vertrauen der Verbraucher zu wahren.



Anzunehmende Schadensfelder:

Quellen
https://www.tagesschau.de/wirtschaft/digitales/datenleck-wirtschaftsauskunftei-100.html
https://www.sueddeutsche.de/wirtschaft/auskunftei-datenleck-infoscore-lux.lCgvAaXhLkhi7GkkFMuo5s?reduced=true

RIEDEL

300 GB Daten aus Shopware-Instanz veröffentlicht

18. November 2024, in Meckesheim/Baden-Württemberg

DATENDIEBSTAHL

DATENLECK

Was ist passiert?
Insgesamt 300 GB Daten einer Shopware-Instanz eines Metalltechnologieunternehmens wurden im Darknet veröffentlicht. Die betroffenen Daten stammten aus einem Unternehmen, das eine Shopware-basierte E-Commerce-Plattform verwendet, was darauf hinweist, dass Informationen zu Kunden, Bestellungen und möglicherweise weiteren sensiblen geschäftlichen Details in den Leak involviert sein könnten.

Was hätte man besser machen können?
Mit einem Echtzeit-Monitoring wäre der Datendiebstahl wahrscheinlich bereits erkannt worden, bevor die gestohlenen Daten im Darknet auftauchten. Beim Echtzeit-Monitoring werden Netzwerksysteme nämlich kontinuierlich überwacht, um verdächtige Aktivitäten frühzeitig zu identifizieren und so potenzielle Sicherheitsvorfälle schnell zu erkennen.

Was lernen wir daraus:

Beim Hacken einer Shopware-Instanz können Angreifer auf sensible Daten zugreifen, den Shop manipulieren oder Malware einschleusen. Schwachstellen wie unzureichende Sicherheitsupdates und schwache Passwörter begünstigen solche Angriffe. Daher sind regelmäßige Updates und starke Zugriffskontrollen entscheidend für den Schutz.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7424-Stauber-Stahl-Data-Leak.png

RIEDEL

System verschlüsselt: Zeitweise Ausfälle in der Verwaltung

18. November 2024, in Bergen auf Rügen/Mecklenburg-Vorpommern

RANSOMWARE

AUSFALL

ERPRESSUNG

Was ist passiert?
Nach einem Ransomware-Angriff auf die IT-Systeme einer Amtsverwaltung auf Rügen kam es zu temporären Ausfällen. Teile der IT-Infrastruktur wurden verschlüsselt und die Täter hinterließen einen Link zu einer Darknet-Seite. Die Verwaltung öffnete diesen Link nicht und schloss eine Zahlung der Lösegeldforderungen aus. Durch den Angriff waren einige Kommunikationskanäle sowie die Bearbeitung von Ausweisen und Reisepässen betroffen, die Verwaltung blieb jedoch geöffnet und Mitarbeiter waren weiterhin telefonisch erreichbar.

Was hätte man besser machen können?
Hätte die Amtsverwaltung auf moderne Sicherheitslösungen gesetzt, wäre der Angriff schneller erkannt und besser eingedämmt worden. Beispielsweis hätte ein SIEM-System verdächtige Aktivitäten durch die Analyse von Sicherheitsdaten frühzeitig aufgedeckt, während ein SOAR-System durch automatisierte Prozesse sofort Gegenmaßnahmen eingeleitet und eine koordinierte Reaktion erleichtert hätte.

Was lernen wir daraus:

Regelmäßige Backups sind entscheidend, um im Fall eines Hackerangriffs wie einer Ransomware-Attacke schnell wieder funktionsfähig zu werden. Backups ermöglichen es, verlorene oder verschlüsselte Daten wiederherzustellen, ohne auf Lösegeldforderungen eingehen zu müssen. Dies zeigt, wie wichtig eine gut geplante und regelmäßig getestete Backup-Strategie ist, um die Auswirkungen von Cyberangriffen zu minimieren und den Geschäftsbetrieb so schnell wie möglich wieder aufzunehmen.

Anzunehmende Schadensfelder:

Quellen
https://www.ndr.de/nachrichten/mecklenburg-vorpommern/Hackerangriff-auf-Ruegen-Verwaltung-in-Bergen-stark-eingeschraenkt,mvregiogreifswald1416.html

RIEDEL

Berliner Gymnasium gehackt: Ein Schüler wird der Schule verwiesen und klagt vor Gericht

15. November 2024, in Berlin/Brandenburg

GERICHTSURTEIL

EINBRUCH

KEYLOGGER

Was ist passiert?

Drei Schüler eines Berliner Gymnasiums hatten monatelang unbefugten Zugang zu vertraulichen Lehrerdaten. Durch das Installieren eines Keyloggers, konnten sie das Admin-Passwort ermitteln und auf geschützte Kanäle zugreifen, die eigentlich nur für Lehrkräfte bestimmt waren. So konnten die drei Schüler interne Informationen im geschützten Lehrerkanal mitlesen und organisatorische Daten der Schulleitung abrufen. Nachdem der Vorfall entdeckt wurde, entschied die Schulaufsicht, den Hauptverantwortlichen an ein anderes Gymnasium zu versetzen.

Was hätte man besser machen können?

Regelmäßige Überprüfungen und Änderungen von Zugriffsrechten sowie Admin-Passwörtern wären notwendig gewesen, um unbefugtem Zugang vorzubeugen. Eine strikte Zugangskontrolle und insbesondere die Nutzung von Multi-Faktor-Authentifizierung, hätten den Zugriff auf vertrauliche Informationen besser geschützt.

Was lernen wir daraus:

Angriffe mit Keyloggern sind oft keine komplexen Cyberangriffe, sondern zeigen eher opportunistischen Missbrauch von Systemschwächen. Die Täter stehlen gezielt administrative Passwörter, um auf vertrauliche Daten zuzugreifen, was technisches Verständnis erfordert, aber keine tiefgehenden Hackerfähigkeiten. Solche Vorfälle verdeutlichen, dass viele Cyberangriffe nicht nur von organisierten Hackergruppen, sondern auch von Einzelpersonen mit einfachen, aber effektiven Methoden begangen werden.

Anzunehmende Schadensfelder:

Quellen
https://www.rbb24.de/panorama/beitrag/2024/11/schule-hacker-angriff-verweis-verwaltungsgericht.html

RIEDEL

Kontrollierte Abschaltung der IT-Systeme als Sofortmaßnahme nach Cyberangriff

14. November 2024, in Oberhausen/Nordrhein-Westfalen

EINBRUCHSVERSUCH

Was ist passiert?
Ein Trainingscenter in Oberhausen wurde am 9. November 2024 Opfer eines Cyberangriffs. Als Sofortmaßnahme wurden alle IT-Systeme des Unternehmens isoliert und kontrolliert abgeschaltet. Dies wurde schnell eingeleitet, nachdem erste Auffälligkeiten des Angriffs festgestellt wurden. Zur Klärung des Vorfalls arbeiten interne und externe IT-Experten sowie Behörden zusammen, um die Ursachen und den Umfang des Angriffs zu untersuchen. Ob und in welchem Ausmaß Daten abgeflossen sind blieb zum Zeitpunkt der Meldung unklar.

Was hätte man besser machen können?
Eine noch frühzeitigere Erkennung des Angriffs hätte durch ein effektives Monitoring-System ermöglicht werden können, insbesondere durch den Einsatz eines SIEM (Security Information and Event Management)-Systems, das verdächtige Aktivitäten automatisch analysiert und meldet.

Was lernen wir daraus:

Unternehmen können feststellen, ob Daten entwendet wurden, indem sie forensische Untersuchungen durchführen, um System- und Netzwerkprotokolle zu analysieren. Sie überwachen den Netzwerkverkehr auf unbefugte Datenübertragungen und suchen nach Spuren von Malware, die auf den Diebstahl hindeuten könnten.

Auch Datenintegritätsprüfungen und die Überwachung von Aktivitäten auf Dark-Web-Marktplätzen, wo gestohlene Daten oft verkauft werden, sind gängige Methoden.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7357-Cyberangriff-Berufsf%C3%B6rderungswerk-Oberhausen.png

RIEDEL

Verdächtiger Zugriff auf Mitarbeiter-Benutzerkonten: Rathaus schaltet System ab

14. November 2024, in Aschaffenburg/Bayern

EINBRUCH

Was ist passiert?
Am Morgen des 14. November 2024 bemerkte die Stadtverwaltung Aschaffenburg einen verdächtigen Zugriff auf Mitarbeiter-Benutzerkonten, der auf einen Hackerangriff hindeutete. Aus Sicherheitsgründen wurden daraufhin alle IT-Systeme abgeschaltet. Infolgedessen blieben sowohl das Rathaus als auch die Außenstellen vom 14. bis 15. November geschlossen. Während dieser Zeit war die Verwaltung weder telefonisch noch per E-Mail erreichbar.

Was hätte man besser machen können?
Ein entscheidender Faktor in diesem Fall war womöglich die mangelnde Cybersecurity Awareness, insbesondere im Bereich Phishing-Prävention. Ein gezieltes Awareness-Training hätte Mitarbeiter sensibilisieren können, verdächtige E-Mails oder Anmeldeversuche frühzeitig zu erkennen und zu melden. Da Phishing oft als Einstiegspunkt für Angriffe dient, hätten regelmäßige Schulungen und simulierte Phishing-Tests dazu beigetragen, das Risiko kompromittierter Benutzerkonten erheblich zu senken.

Was lernen wir daraus:

Um Hackerangriffe über Mitarbeiterkonten zu verhindern, sollten Unternehmen ihre Mitarbeiter in mehreren Bereichen schulen: Erkennen von Phishing-E-Mails, Verwendung starker Passwörter und Multi-Faktor-Authentifizierung (MFA), sowie das Bewusstsein für Social Engineering-Angriffe. Interaktive Schulungen, regelmäßige Phishing-Tests und klare Verhaltensregeln für den Umgang mit verdächtigen Anfragen sind entscheidend. Studien zeigen, dass gut geschulte Mitarbeiter Phishing-Risiken um bis zu 50% verringern können und dass menschliches Versagen in rund 90% der Fälle eine Rolle bei Cyberangriffen spielt.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7378-Stadtverwaltung-Aschaffenburg.png

RIEDEL

Hackergruppe „Akira“ hackt mittelständisches Unternehmen

14. November 2024, in Troisdorf/Nordrhein-Westfalen

DATENLECK

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?

Mitte November wurde bekannt, dass ein führender Anbieter für Automatisierungstechnik Opfer einer Ransomware-Attacke wurde. Die Hackergruppe "Akira" listete das Unternehmen aus Troisdorf auf ihrem Darknet-Blog als Ziel. Laut Berichten von Ransomfeed und Ransomware.live stand nach kurzer Zeit bereits ein erstes Datenpaket als Torrent bereit. Ob und in welchem Umfang sensible Informationen betroffen sind, bleibt noch unklar.

Was hätte man besser machen können?

Durch Echtzeit-Monitoring wäre eine fortlaufende Überwachung der Netzwerksysteme möglich gewesen, um Muster des Angriffs bzw. Auffälligkeiten frühzeitig zu identifizieren und unmittelbar Gegenmaßnahmen einzuleiten.

Was lernen wir daraus:

Die Hackergruppe Akira trat im März 2023 erstmals in Erscheinung und zählt laut Experten zu den fünf gefährlichsten Gruppen weltweit. Sie zielt vor allem auf kleine und mittelständische Unternehmen ab. Viele Beobachter vermuten, dass Akira aus Osteuropa stammt und ein Nachfolger der aufgelösten Conti-Gruppe ist.

Anzunehmende Schadensfelder:

Quellen

https://www.ransomware.live/id/bWsgVGVjaG5vbG9neSBHcm91cEBha2lyYQ==

https://www.security-incidents.de/assets/img/incidents/7385-Akira-MkTechnologyGroup.png

RIEDEL

Stromanbieter gehackt: Sensible Kundendaten im Darknet wiederzufinden

13. November 2024, in Berlin/Brandenburg

DATENDIEBSTAHL

EINBRUCH

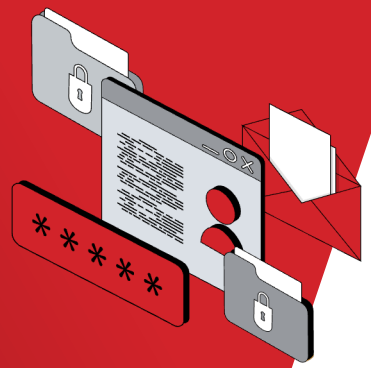
Was ist passiert?
Die Kundendaten eines großen Stromanbieters wurden durch einen Hackangriff entwendet und in einem populären Darknet-Forum zum Verkauf angeboten. Betroffen sind laut dem Unternehmen offenbar über 50.000 Kunden, allesamt aus Deutschland. Gegenläufig dazu sprechen die Hacker von etwa 243.000 erbeuteten Kundendaten. Diese umfassen persönliche Angaben wie Vor- und Nachnamen, E-Mail-Adressen, Umsatzzahlen, sowie Ort und Postleitzahl der Betroffenen.

Was hätte man besser machen können?
Das Unternehmen hätte den Angriff früher bemerken können, wenn es ein Managed-SIEM zur kontinuierlichen Überwachung und ein 24/7 besetztes Security Operations Center (SOC) eingesetzt hätte. Durch diese proaktive Überwachung wäre es möglicherweise gelungen, den Diebstahl sensibler Kundendaten zu verhindern oder den Schaden zumindest zu begrenzen.

Was lernen wir daraus:

Der Angriff auf den Energieversorger zeigt, warum die NIS-2-Richtlinie für kritische Infrastrukturen wie die Energieversorgung so wichtig ist. NIS 2 verpflichtet Unternehmen zu stärkeren Sicherheitsmaßnahmen, darunter Risikomanagement, Meldung von Vorfällen und strenge Zugangskontrollen. Wären diese Vorgaben bereits umfassend umgesetzt, hätte der Schaden möglicherweise begrenzt oder verhindert werden können.

Anzunehmende Schadensfelder:



Quellen
https://www.heise.de/news/Stromanbieter-Tibber-gehackt-50-000-deutsche-Kunden-betroffen-10030864.html

RIEDEL

444.601 Daten in unbefugten Händen

13. November 2024, in Allendorf/Hessen

Was ist passiert?
Am 13. November 2024 wurde ein Biogasunternehmen Opfer eines Ransomware-Angriffs, der von der Gruppe „Hunters“ im Darknet bekannt gemacht wurde. Die Angreifer behaupten, 1,5 TB an Daten mit 444.601 Dateien kompromittiert zu haben. Die Echtheit der Daten und eine mögliche Lösegeldforderung wurden bisher nicht bestätigt.

Was hätte man besser machen können?
Eine rund um die Uhr Überwachung der IT-Systeme hätte ermöglicht, Sicherheitsbedrohungen frühzeitiger zu identifizieren und umgehend darauf reagieren zu können.

RANSOMWARE

EINBRUCH

DATENDIEBSTAHL

Was lernen wir daraus:

Lösegeldforderungen bei Cyberangriffen erfolgen meist in Bitcoin, da diese Kryptowährung weit verbreitet und schwer nachverfolgbar ist. Die Täter stellen ihre Forderungen oft über Darknet-Websites oder verschlüsselte Nachrichten und setzen enge Fristen, um Druck auszuüben. Zahlungen laufen in der Regel über anonyme Wallets, wodurch die Nachverfolgung und Identifikation der Angreifer erheblich erschwert wird.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7343-Hunters-SchmackBiogas.png

RIEDEL

Angriff auf statistisches Bundesamt: Was wird aus den Wahlen?

12. November 2024, in Wiesbaden/Hessen

DATENDIEBSTAHL

Was ist passiert?
Die entwendeten 3,8 GB Daten des statistischen Bundesamts, die Kontaktdaten wie E-Mail-Adressen und Telefonnummern enthalten, werden für 250 US-Dollar im Darknet angeboten. Screenshots zeigen Zugangsdaten im Klartext zum IDEV-System des Bundesamts. Am 18. November 2024 nahm das Bundesinnenministerium das IDEV-System vorsorglich vom Netz, ohne Auswirkungen auf die anstehende Bundestagswahl. Am 20. November 2024 stellte das Statistische Bundesamt klar, dass keine Unternehmensdaten abgeflossen sind und die kompromittierten User-Daten durch Phishing-Angriffe erlangt wurden.

Was hätte man besser machen können?
Die Angreifer hatten Zugang zum IDEV-System, was darauf hindeutet, dass die Zugangskontrollen möglicherweise nicht ausreichten. Stärkere Authentifizierungsmethoden wie Multifaktor-Authentifizierung (MFA) hätten den unbefugten Zugriff auf das System deutlich erschwert.

Was lernen wir daraus:

Selbst kleine Details – wie die unsichere Speicherung von Zugangsdaten im Klartext – können massive Sicherheitslücken darstellen. Es wird klar, dass eine Organisation oft nicht durch einen einzelnen Fehler, sondern durch eine Kette von vernachlässigten Kleinigkeiten verwundbar wird. Das Beispiel zeigt, dass die Summe kleiner Schwächen oft zu einem großen Sicherheitsproblem führen kann, das schwerwiegende Folgen hat.

Anzunehmende Schadensfelder:

Quellen
https://www.golem.de/news/login-daten-und-datensatz-angebliches-datenleck-beim-statistischen-bundesamt-2411-190853.html

RIEDEL

Bonitätszertifikat von Jens Spahn abrufbar für jeden

12. November 2024, in München/Bayern

DATENLECK

DATENPANNE

Was ist passiert?
Am 12. November 2024 berichtete die Sicherheitsforscherin Lilith Wittmann auf X über eine schwerwiegende Sicherheitslücke in einem Online-Portal zur Bonitätsprüfung. Ihr gelang es, sensible Bonitätsdaten abzurufen und zu manipulieren, was erhebliche Risiken für betroffene Nutzer darstellt. Das Portal bezieht Daten von bekannten Auskunfteien, wodurch die Schwachstelle besonders brisant ist.
Schon im gleichen Jahr entdeckte Wittmann eine ähnliche Schwachstelle in einer Schufa-nahen App, die ebenfalls unzureichend gesichert war.

Was hätte man besser machen können?
Der Vorfall hätte möglicherweise durch stärkere Zugriffskontrollen verhindert werden können, etwa durch eine mehrstufige Authentifizierung und striktere Berechtigungssysteme, um unbefugte Änderungen an Bonitätsdaten zu verhindern. Zudem hätte eine regelmäßige Sicherheitsüberprüfung durch Penetrationstests frühzeitig auf Schwachstellen hinweisen und deren Behebung ermöglichen können.

Was lernen wir daraus:

Sicherheitsforscher wie Lilith Wittmann spielen eine entscheidende Rolle bei der Aufdeckung von Schwachstellen, bevor sie von Cyberkriminellen ausgenutzt werden. Durch ihre Analysen helfen sie Unternehmen, Sicherheitslücken zu schließen und ihre Systeme zu verbessern.

Anzunehmende Schadensfelder:

Quellen
https://chaos.social/@Lilith/113471104043782540
https://x.com/LilithWittmann/status/1856378586011447471

RIEDEL

RANSOMWARE

EINBRUCH

DATENDIEBSTAHL

Angriff auf Betonbau Unternehmensgruppe: Datenverkauf im großen Stil

9. November 2024, in Fronhausen/Hessen

Was ist passiert?
Ein Betonbauunternehmen wurde Opfer eines Ransomware-Angriffs der Gruppe „meow“. Die Angreifer behaupten, 350 GB vertrauliche Daten gestohlen zu haben, darunter Mitarbeiter- und Kundendaten, Verträge, Finanzunterlagen sowie persönliche und medizinische Informationen. Diese Daten werden im Darknet entweder exklusiv für 25.000 US-Dollar oder für jeweils 12.000 US-Dollar pro Käufer angeboten.

Was hätte man besser machen können?
Der Angriff hätte durch den Einsatz von Sicherheitslösungen wie einem Managed-SIEM und einem rund um die Uhr besetzten Security Operations Center (SOC) früher erkannt und in seinem Ausmaß begrenzt oder gar verhindert werden können.
Auch die Überwachung von Dedicated Leak Sites (DLS) hätte dem Unternehmen geholfen, frühzeitig auf die Veröffentlichung der gestohlenen Daten aufmerksam zu werden und schnellere Gegenmaßnahmen zu ergreifen.

Anzunehmende Schadensfelder:

Was lernen wir daraus:

Prozessabläufe eines Security Operations Centers (SOC):

- Ein SOC nutzt spezialisierte Tools, um Protokolldaten zu sammeln und zu korrelieren, um relevante Sicherheitsereignisse zu identifizieren.
- Bei der Priorisierung von Alarmen wird das Geschäftsumfeld sowie die aktuelle Bedrohungslage berücksichtigt, um echte Sicherheitsvorfälle von weniger kritischen Ereignissen zu unterscheiden.
- Nach der Erkennung eines Vorfalls meldet das SOC die Bedrohung an den IT-Sicherheitsbeauftragten und unterstützt bei der Eindämmung.
- Nach der Reaktion wird der Vorfall dokumentiert und eine forensische Analyse durchgeführt, um sicherzustellen, dass die Bedrohung vollständig beseitigt wurde.

Quellen
https://www.ransomware.live/id/RmluZ2VyIEJldG9uIFVudGVybmVobWVuc2dydXBwZUBtZW93

RIEDEL

Sozialunternehmen aus München hat es schon wieder erwischt?

6. November 2024, in München/Bayern

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Die Helldown-Ransomware-Gang veröffentlicht 153 GB an Daten eines Sozialunternehmens auf ihrer Leak-Seite. Da die Angreifer keine spezifischen Informationen zu ihrem Angriff preisgaben, bleibt unklar, ob dieser Vorfall mit dem Sicherheitsvorfall zusammenhängt, den das Sozialunternehmen bereits im September 2024 gemeldet hatte.

Was hätte man besser machen können?
Verhindert werden hätte der Angriff womöglich durch regelmäßige Updates und Firmware-Patches für alle Netzwerkgeräte, insbesondere Firewalls und Router. Hinzukommt, dass eine 24/7-Überwachung der IT-Systeme entscheidend gewesen wäre, um die Bedrohung in Echtzeit erkennen und mit sofortigen Gegenmaßnahmen darauf reagieren zu können.

Was lernen wir daraus:

Cybersicherheit muss in allen Sektoren – auch bei gemeinnützigen Organisationen – oberste Priorität haben. Denn Cyberkriminalität kennt keine ethischen Grenzen. Gruppen wie Helldown machen vor Sozialunternehmen nicht halt und greifen gezielt an, indem sie bekannte Schwachstellen in Firewalls ausnutzen, um Zugriff auf Netzwerke zu erlangen.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7247-haus-des-stiftens-helldown.png

RIEDEL

Unerwartet mit der Tür ins Haus gefallen: 198 GB Daten von Türenhersteller gestohlen

4. November 2024, in Besigheim-Ottmarsheim/Baden-Württemberg

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Am 4. November 2024 wurde ein deutscher Fenster- und Türenhersteller Opfer eines Ransomware-Angriffs durch die Gruppe RansomHub. Die Angreifer behaupteten, 198 GB sensibler Daten erbeutet zu haben, und setzten dem Unternehmen eine Frist bis zum 11. November, um auf ihre Forderungen einzugehen. Nach Ablauf dieser Frist veröffentlichten sie die gestohlenen Daten.

Was hätte man besser machen können?
Es wird vermutet, dass die Angreifer Schwachstellen in der Cybersicherheitsinfrastruktur ausnutzten. Regelmäßige Sicherheitsüberprüfungen sind entscheidend, um potenziellen Schwachstellen in der IT-Infrastruktur frühzeitig entgegenzuwirken – dazu gehören Penetrationstests und Schwachstellenscans, die helfen, Sicherheitslücken zu entdecken, bevor sie von Angreifern ausgenutzt werden können.

Was lernen wir daraus:

RansomHub ist eine Ransomware-as-a-Service (RaaS) Gruppe, die im Februar 2024 erstmals in Erscheinung trat. Sie zeichnet sich durch aggressive Taktiken aus, darunter die sogenannte Doppel-Erpressung, bei der Daten sowohl verschlüsselt als auch exfiltriert werden, um zusätzlichen Druck auf die Opfer auszuüben. Die Gruppe nutzt dabei Schwachstellen in ungepatchten Systemen aus und setzt auf schnelle und effiziente Angriffe, die plattformübergreifend wirken.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7234-ransomhub-schweiker.png

RIEDEL

Florian Dalwigk
Geheimdienstexperte und Fachbuchautor
Er unterrichtet u. a. die Module „Ethical Hacking“ und „Cyberspionage“ an Hochschulen in Deutschland.

GASTARTIKEL

WIRTSCHAFTSSPIONAGE DURCH DEN EINSATZ KÜNSTLICHER INTELLIGENZ (KI)

Was ist passiert?

Wirtschaftsspionage unter Zuhilfenahme von Cyberangriffen stellt in Deutschland eine erhebliche Bedrohung für Unternehmen und Behörden dar. Laut einer Studie des Digitalverbands Bitkom aus dem Jahr 2024 wurden 81 % der Unternehmen in den vergangenen zwölf Monaten Opfer von Datendiebstahl, Industriespionage oder Sabotage, wobei der geschätzte Gesamtschaden bei 267 Milliarden Euro lag. (Bitkom, 2024) Hierbei kommt vermehrt KI in Form von automatisierten Phishing-Angriffen, Deepfakes und KI-gestützter Malware zum Einsatz.

Was hätte man besser machen können?

Die erfolgreichsten Cyberangriffe sind in der Regel die, die auf den Menschen als schwächstes Glied in der Informationssicherheitskette abzielen. Nicht umsonst werden im nachrichtendienstlichen Umfeld psychologische Operationen (PsyOps) auch vermehrt mithilfe von KI durchgeführt.

Unternehmen sollten daher verstärkt auf AI Literacy setzen. AI Literacy bezeichnet die Fähigkeit, KI zu verstehen, kritisch zu hinterfragen, sicher zu nutzen und KI-generierte Inhalte wie Deepfakes zu erkennen. Durch gezielte Schulungen, die neben klassischen Inhalten wie Phishing-Prävention auch verstärkt Themen wie Deepfakes behandeln, werden Mitarbeitende in die Lage versetzt, sich vor solchen Angriffen zu schützen.

Was lernen wir daraus?

Ein bewusster und informierter Umgang mit KI ist essenziell, um Sicherheitsrisiken zu minimieren. AI Literacy muss ein fester Bestandteil der Cybersicherheitsstrategie von Unternehmen und Behörden werden. Sensibilisierungsmaßnahmen und kontinuierliche Schulungen helfen dabei, Mitarbeiter für die Gefahren durch KI-generierte Angriffe zu wappnen. Ein umfassender Schutz erfordert daher nicht nur rein technische Sicherheitsmaßnahmen, sondern auch ein hohes Maß an KI-Kompetenz und kritischem Denken innerhalb der Organisation.

Bitkom. (2024). Wirtschaftsschutz 2024 (Dr. R. Wintergerst, Hrsg.). Bitkom. https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf [Stand: 28.02.2025].

RIEDEL

OKTOBER 2024

SECURITY INCIDENTS GERMANY

RIEDEL

Cyberkriminelle entwenden Schulungsinhalte zu Cybersicherheit

31. Oktober 2024, in Köln/Nordrhein-Westfalen

RANSOMWARE

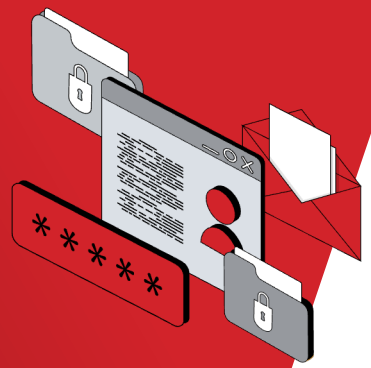
DATENLECK

DATENDIEBSTAHL

Was ist passiert?
Cyberkriminelle von Helldown gaben im Darknet an, 76 GB Daten eines Automatisierungstechnikunternehmen aus Köln durch einen Ransomware-Angriff gestohlen und veröffentlicht zu haben. Zu den gestohlenen Informationen gehören unter anderem Passwörter, Zugangsdaten, Schulungsinhalte zur Cybersicherheit und Rechnungen.

Was hätte man besser machen können?
Um den Sicherheitsvorfall zu verhindern, hätte das Unternehmen ein Security Operations Center (SOC) einsetzen können, das Bedrohungen in Echtzeit erkennt. Durch die zentrale Überwachung und Analyse sicherheitsrelevanter Ereignisse hätte ein SOC ungewöhnliche Aktivitäten frühzeitig identifizieren können.
Zusätzlich hätte ein Security Information and Event Management (SIEM)-System implementiert werden sollen, das Sicherheitsdaten aus verschiedenen Quellen innerhalb der IT-Infrastruktur sammelt und analysiert.

Anzunehmende Schadensfelder:



Was lernen wir daraus:

Cyberkriminelle greifen oft auf sogenannte Zero-Day-Exploits zurück – das sind Sicherheitslücken in Software, die vom Hersteller noch nicht erkannt oder geschlossen wurden. Diese Schwachstellen erlauben es den Angreifern, Systeme zu infiltrieren, bevor ein entsprechendes Update zur Behebung verfügbar ist. Derartige Exploits werden häufig auf Marktplätzen im Darknet gehandelt und können erhebliche Schäden anrichten.

RIEDEL

Quellen
https://www.security-incidents.de/assets/img/incidents/7248-SMARTS_Engineering-Helldown.PNG

Software-Anbieter wurde Opfer eines Ransomware-Angriffs

31. Oktober 2024, in Karlsruhe/Baden-Württemberg

DATENLECK

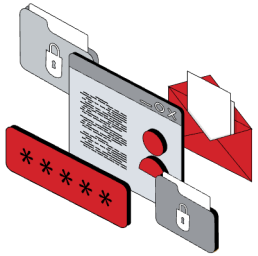
DATENDIEBSTAHL

Was ist passiert?
Bei einem Angriff der Ransomwaregruppe Sarcoma wurden 6 GB Daten eines CRM-Software-Anbieters exfiltriert. Diese umfassen SQL-Datenbanken und E-Mails aus einem MS Exchange-System. Die Täter setzten dem Unternehmen eine Frist, nach deren Ablauf die gestohlenen Daten veröffentlicht werden sollten.

Was hätte man besser machen können?
Durch den Einsatz von mehrschichtigen Sicherheitslösungen, wie etwa Firewalls, Intrusion Detection Systeme (IDS) und Endpoint Protection, hätte der Anbieter den Angriff frühzeitig erkennen und blockieren können. Regelmäßige Updates und das schnelle Einspielen von Sicherheits-Patches auf allen Systemen, einschließlich des MS Exchange-Systems, hätten bekannte Schwachstellen geschlossen und das Risiko eines erfolgreichen Angriffs verringert.

Was lernen wir daraus:

Neben der Verschlüsselung von Daten drohen Ransomware-Angreifer auch, vertrauliche Informationen öffentlich zu machen, wenn das verlangte Lösegeld nicht gezahlt wird. Diese Methode verstärkt den Druck auf die Opfer, da sie sich nicht nur um den Verlust ihrer Daten sorgen, sondern auch um die Sicherheit ihrer sensiblen Informationen.
Experten raten davon ab, das Lösegeld zu zahlen, da es keine Garantie für die Rückgabe der Daten gibt.



Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7192-cas-software-sarcoma.png

RIEDEL

Ransomware-Angriff trifft bayrischen Software-Dienstleister

29. Oktober 2024, in Fischbachau/Bayern

RANSOMWARE

DATENDIEBSTAHL

EINBRUCH

Was ist passiert?
Am 29. Oktober 2024 wurde ein deutscher Software-Dienstleister Opfer eines Ransomware-Angriffs durch die Gruppe „Apt73“. Die Täter veröffentlichten das Unternehmen auf ihrer Darknet-Leak-Seite und drohten mit der Offenlegung sensibler, bislang unbekannter Daten, falls kein Lösegeld gezahlt wird. Die Höhe der Forderung ist unklar, ebenso wie das genaue Ausmaß der gestohlenen Informationen.

Was hätte man besser machen können?
Mit einem Security Operations Center (SOC) hätte das Unternehmen eine ständige Überwachung seiner IT-Infrastruktur sicherstellen und auf Sicherheitsvorfälle in Echtzeit reagieren können. Ein SOC ermöglicht nicht nur eine frühzeitige Erkennung von Bedrohungen, sondern sorgt durch koordinierte Maßnahmen auch dafür, dass Angriffe schneller eingedämmt und Schäden minimiert werden.

Was lernen wir daraus:

Ein Security Operations Center (SOC) muss nicht zwangsläufig im eigenen Unternehmen aufgebaut und betrieben werden. Unternehmen können stattdessen auf Managed Services zurückgreifen. Dabei übernehmen spezialisierte externe Anbieter die Überwachung, Analyse und Reaktion auf Sicherheitsvorfälle rund um die Uhr. Dies spart Ressourcen, reduziert Kosten und bietet Zugang zu Expertenwissen sowie modernster Technologie.

Anzunehmende Schadensfelder:

Quellen
https://ransomfeed.it/index.php?page=post_details&id_post=18262
https://www.ransomware.live/id/d3d3LnNjb3Blc2V0LmRlOGEwdDcz

RIEDEL

Deutsche Handelskammer taucht auf Ransomware-Opferliste auf

28. Oktober 2024, in Berlin/Berlin

RANSOMWARE

Was ist passiert?
Am 28. Oktober 2024 nahm die Ransomwaregruppe „Playboy“ eine deutsche Handelskammer in ihrer Liste der Opfer auf. Die Gruppe gab bislang wenig Informationen preis, setzte der Kammer jedoch eine Frist bis November 2024, um das geforderte Lösegeld zu zahlen. Andernfalls droht die Veröffentlichung der angeblich gestohlenen Daten.

Was hätte man besser machen können?
Um einen Angriff der Ransomwaregruppe Playboy abzuwehren, hätte die Handelskammer moderne Sicherheitslösungen einsetzen können. Dazu gehören SIEM-Systeme zur Echtzeitüberwachung und Analyse von Sicherheitsereignissen, EDR-Tools zur Erkennung und Reaktion auf verdächtige Aktivitäten. Zudem hätte Antivirussoftware zur Abwehr der Schadsoftware beitragen können.

Was lernen wir daraus:

Ein Ransomware-Angriff beginnt meist mit einer Infektion, oft durch Phishing-Mails oder den Besuch kompromittierter Websites. Nach der Ausführung des Schadprogramms breitet sich die Malware im System aus, verschlüsselt Dateien und blockiert den Zugriff darauf. Als Nutzer bemerkt man den Angriff dann, wenn Dokumente, Bilder oder Programme aufgrund der Verschlüsselung nicht mehr geöffnet werden können.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7164-deutsche-industrie-und-handelskammer-playboy.png

RIEDEL

Apothekengroßhändler versucht vergebens auf seine IT-Systeme zugreifen zu können

28. Oktober 2024, in Alzenau/Bayern

EINBRUCH

AUSFALL

RANSOMWARE

Was ist passiert?
Am 28. Oktober 2024 fiel ein Apothekengroßhändler einem Cyberangriff zum Opfer. Teile der IT-Systeme wurden durch den Angriff verschlüsselt, was dazu führte, dass die betroffenen Systeme heruntergefahren werden mussten. Das Unternehmen war sowohl telefonisch als auch per E-Mail nur eingeschränkt erreichbar. Trotz der Einschränkungen versicherte das Unternehmen, dass die Medikamentenversorgung nicht gefährdet sei.

Was hätte man besser machen können?
Die Nutzung von SIEM- und EDR-Systemen hätte dabei helfen können, Bedrohungen frühzeitig zu erkennen und zu verhindern. Ein detaillierter Incident Response Plan wäre ebenfalls entscheidend gewesen, um schnell und effektiv auf den Angriff zu reagieren.

Was lernen wir daraus:

Als typisches Einfallstor für Ransomware zählt Phishing. Dabei versenden Cyberkriminelle E-Mails, die vertrauenswürdig wirken und den Empfänger dazu verleiten, schadhafte Links zu klicken oder gefährliche Anhänge zu öffnen. Durch diese scheinbar harmlosen Handlungen wird Ransomware auf dem System installiert, die daraufhin Dateien verschlüsselt und den Zugriff auf diese blockiert. Um die Daten wiederherzustellen, fordern die Angreifer ein Lösegeld.

Anzunehmende Schadensfelder:

Quellen
https://www.heise.de//news/Cyberangriff-auf-Pharmahaendler-AEP-10001097.html
https://www.security-incidents.de/assets/img/incidents/7212-AEP-Ransomware.png

RIEDEL

Kundendaten von Online-Shop auf BreachForums zum Verkauf angeboten

28. Oktober 2024, in Wiesbaden/Hessen

DATENPANNE

DATENDIEBSTAHL

Was ist passiert?
Seit dem 28. Oktober 2024 kursieren auf BreachForums angeblich gestohlene Kundendaten eines Online-Shops. Das veröffentlichte Sample enthält sensible Informationen wie MD5-Hashes, E-Mail-Adressen, Namen und Kundennummern. Die Daten werden von Cyberkriminellen zum Verkauf angeboten, was die Gefahr eines weiteren Missbrauchs der gestohlenen Informationen erhöht.

Was hätte man besser machen können?
Um den Angriff zu verhindern, hätte das Unternehmen SIEM-Systeme zur Überwachung von Sicherheitsereignissen und EDR-Tools zur schnellen Erkennung von Bedrohungen einsetzen sollen. Zudem wären regelmäßige Schwachstellen-Scans und Datenverschlüsselung wichtig gewesen, um die Angriffsfläche zu minimieren und sensible Daten zu schützen.

Was lernen wir daraus:

Immer häufiger setzen Cyberkriminelle auf Software-Updates, um Malware in Systeme einzuschleusen. Diese Angriffe erscheinen häufig als legitime Aktualisierungen und verleiten die Benutzer dazu, schadhafte Software unbewusst zu installieren. Dies kann schwerwiegende Sicherheitsrisiken wie Datenverlust und die Gefährdung des gesamten Systems nach sich ziehen. Daher ist es entscheidend, dass Updates aus verlässlichen Quellen stammen. Nutzer sollten sicherstellen, dass sie nur Updates von vertrauenswürdigen Anbietern installieren und die Integrität der Software überprüfen, um ihre Systeme zu schützen.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7692-oregano-oil.de-Data-Breach.png

RIEDEL

Stahlhändler unter Erpressung: Sarcoma-Gruppe droht mit Veröffentlichung gestohlener Daten

25. Oktober 2024, in Augsburg/Bayern

EINBRUCH

ERPRESSUNG

DATENDIEBSTAHL

Was ist passiert?
Am 25. Oktober 2024 wurde ein Stahlhändler aus Augsburg Opfer einer Ransomware-Attacke der Gruppe „Sarcoma“. Die Angreifer behaupten, 64 GB sensibler Daten gestohlen zu haben, darunter Finanzinformationen, Rechnungen und Gehaltsdaten. Als Beweis stellten sie Screenshots der gestohlenen Dokumente ins Darknet. Das Unternehmen wurde aufgefordert, ein Lösegeld zu zahlen, andernfalls droht die Veröffentlichung der gestohlenen Daten.

Was hätte man besser machen können?
Ein Security Operations Center (SOC) hätte den Angriff durch den Einsatz einer kombinierten Lösung aus SOAR (Security Orchestration, Automation and Response) und XDR (Extended Detection and Response), integriert in eine SIEM (Security Information and Event Management)-Plattform zur Echtzeitüberwachung, frühzeitig erkannt und abwehren können.

Diese Kombination ermöglicht eine automatisierte Reaktion auf Bedrohungen, eine schnellere Erkennung von Angriffsmustern und eine effizientere Analyse von Sicherheitsvorfällen, wodurch potenziellen Schäden präventiv entgegengewirkt wird.

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.

Anzunehmende Schadensfelder:

Quellen
https://ransomfeed.it/index.php?page=post_details&id_post=18187
https://www.ransomware.live/id/U1ITLVN0YWhsIEdtYkhAc2FyY29tYO==

RIEDEL

Enthüllung vertraulicher Daten eines Technologieunternehmens

25. Oktober 2024, in Unterschleißheim/Bayern

EINBRUCH

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Am 25. Oktober 2024 griffen Cyberkriminelle der MEDUSA-Gruppe ein deutsches Technologieunternehmen mit Ransomware an und setzten es auf ihrem Darknet-Blog auf die Liste ihrer Opfer. Sie drohten, vertrauliche Unternehmensdaten zu veröffentlichen und stellten Screenshots als Beweis bereit. Für 10.000 USD boten die Täter eine Fristverlängerung, während 100.000 USD entweder die Löschung oder den direkten Zugriff auf die Daten ermöglicht hätten.

Was hätte man besser machen können?
Das Technologieunternehmen hätte durch regelmäßige Sicherheitsaudits und schnelle Incident-Response-Maßnahmen den Angriff möglicherweise verhindern oder eindämmen können. Zudem wären verschlüsselte Daten und Offsite-Backups entscheidend gewesen, um den Schaden zu minimieren und Erpressungen ins Leere laufen zu lassen.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7152-Medusa-Lakesight.png
https://www.hookphish.com/blog/ransomware-group-medusa-hits-lakesighttechnologies-com/

Was lernen wir daraus:

Ransomware hat sich im Laufe der Zeit stark weiterentwickelt. Während die ersten Programme noch relativ simpel waren und einfache Verschlüsselungsmethoden verwendeten, setzen moderne Varianten mittlerweile auf komplexe Verschlüsselungsalgorithmen. Diese fortschrittlichen Techniken erschweren es erheblich, die betroffenen Daten, ohne den entsprechenden Entschlüsselungsschlüssel wiederherzustellen.

RIEDEL

Wieder was gelernt: Auch Schulen sind beliebte Opfer von Cyberkriminellen

RANSOMWARE

EINBRUCH

AUSFALL

24. Oktober 2024, in Kitzingen/Bayern

Was ist passiert?
Am 23. Oktober 2024 wurden die IT-Systeme von sieben Schulen im Landkreis Kitzingen durch Ransomware lahmgelegt. Teile der Schuldaten wurden verschlüsselt, darunter Systeme von Realschulen sowie Gymnasien. Aus Sicherheitsgründen kappte der IT-Dienstleister die Internetverbindung. Ein Notbetrieb sollte nach den Herbstferien starten. Persönliche Daten wie Noten blieben laut Landratsamt unberührt.

Was hätte man besser machen können?
Die Schulen hätten durch regelmäßige Backups, Netzwerksegmentierung und Multi-Faktor-Authentifizierung den Schaden eines solchen Angriff verringen können. Zudem wären aktuelle Software-Updates und Monitoring-Systeme zur Erkennung verdächtiger Aktivitäten wichtig gewesen.

Was lernen wir daraus:

Der Vorfall verdeutlicht, dass auch IT-Infrastrukturen in Organisationen anfällig sind und wie schnell Angriffe den Betrieb beeinträchtigen können. Zudem verdeutlich er die Notwendigkeit, IT-Systeme widerstandsfähig zu gestalten und präventiv Sicherheitsmaßnahmen zu ergreifen – ob in Unternehmen oder öffentlichen Organisationen.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7167-MitteilungLandkreisKitzingen.png
https://www.br.de/nachrichten/bayern/cyberattacke-in-kitzingen-hacker-haben-schul-daten-verschluesselt,USV5eMx

RIEDEL

Evangelische Nachrichtenagentur wurde Ziel einer Ransomware-Attacke

23. Oktober 2024, in Wetzlar/Hessen

ERPRESSUNG

RANSOMWARE

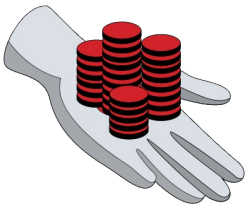
Was ist passiert?
Am 21. Oktober 2024 wurde eine evangelische Nachrichtenagentur Opfer einer Ransomware-Attacke. Eine osteuropäische Hackergruppe verschlüsselte erfolgreich einen Teil der Server und stellte eine Lösegeldforderung. Obwohl unklar ist, ob das Lösegeld gezahlt wurde, wird eine Kompromittierung der hinterlegten Daten nicht ausgeschlossen.

Was hätte man besser machen können?
Um solche Angriffe zu vermeiden, sind regelmäßige Überwachung, Zugangskontrollen und Backups entscheidend. Auch Mitarbeiterschulungen zur Bedrohungserkennung hätten das Risiko verringern können.

Was lernen wir daraus:

Cyberkriminelle nutzen zunehmend das Modell „Ransomware-as-a-Service“ (RaaS), bei dem sie ihre Ransomware an andere Täter weitervermieten.

Dieses Geschäftsmodell senkt die technischen Hürden für Angreifer, die nicht über tiefgehendes Fachwissen verfügen und fördert so eine weite Verbreitung von Ransomware.



Anzunehmende Schadensfelder:

Quellen
https://www.idea.de/artikel/idea-wurde-opfer-eines-cyberangriffs
https://www.csoonline.com/article/3586560/ransomware-attacke-auf-medienhaus-idea.html

RIEDEL

FOG-Ransomwaregruppe stiehlt 118 GB Daten von Logistikunternehmen

21. Oktober 2024, in Sauerlach/Bayern

DATENPANNE

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Am 21. Oktober 2024 hat die FOG-Ransomwaregruppe ein bayrisches Logistikunternehmen als Opfer eines Angriffs im Darknet bekanntgegeben. Die Cyberkriminellen haben dabei 118 GB sensible Daten gestohlen, darunter Finanzdaten, E-Mail-Korrespondenz und vertrauliche Verträge mit Kunden und Mitarbeitern.

Was hätte man besser machen können?
Um Angriffe zu vermeiden, hätte man umfassende Sicherheitsmaßnahmen implementieren sollen. Dazu gehören regelmäßige Systemüberwachung, starke Passwörter, Multi-Faktor-Authentifizierung und Verschlüsselung sensibler Daten.

Regelmäßige Backups und Mitarbeiterschulungen zur Erkennung von Phishing-Angriffen wären ebenfalls wichtig gewesen, um die Angriffsfläche zu reduzieren.

Was lernen wir daraus:

Für Logistikunternehmen ist die Umsetzung der NIS2-Richtlinie nicht nur eine gesetzliche Pflicht, sondern auch eine Chance, das Vertrauen ihrer Kunden und Partner zu gewinnen. In einer zunehmend digitalen Welt, in der Lieferketten und Informationssysteme immer stärker miteinander verknüpft sind, bietet eine solide Cybersicherheitsstrategie den Schutz vor Datenverlust, Betriebsstörungen und finanziellen Schäden.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7058-Schweiger_Transport.PNG

RIEDEL

Millionen Kundendaten durch Fehlkonfiguration öffentlich zugänglich

17. Oktober 2024, in Königs Wusterhausen/Brandenburg

KONFIGURATIONSFEHLER

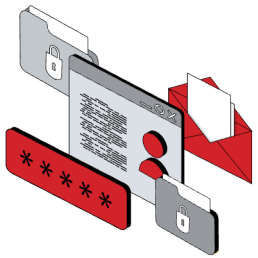
DATENPANNE

Was ist passiert?
Sicherheitsforscher entdeckten eine ungeschützte Datenbank eines führenden Brillenhändlers in Europa. Über 3,5 Millionen Datensätze, darunter Namen, Adressen, E-Mails und Zahlungsdetails, waren frei zugänglich. Betroffen waren Kunden aus Deutschland, Spanien und Österreich. Die Sicherheitslücke, verursacht durch eine Fehlkonfiguration, wurde zwei Tage nach Entdeckung geschlossen.

Was hätte man besser machen können?
Der Brillenhändler hätte durch präventive Maßnahmen den Vorfall vermeiden können. Dazu gehören regelmäßige Vulnerability Assessments, um Fehlkonfigurationen frühzeitig zu erkennen. Eine strengere Zugangskontrolle und Verschlüsselung sensibler Daten hätten die Risiken minimiert

Was lernen wir daraus:

Das rechtzeitige Auffinden und Schließen von Sicherheitslücken ist für Unternehmen essenziell, um sensible Daten und die eigene IT-Infrastruktur zu schützen. Unentdeckte Schwachstellen können Cyberkriminellen Tür und Tor öffnen, was zu Datenverlust, finanziellen Schäden und einem Vertrauensverlust bei Kunden führen kann.



Anzunehmende Schadensfelder:

Quellen
https://www.heise.de//news/Datenleck-bei-brillen-de-Details-zu-den-Ursachen-10178182.html
https://cybernews.com/security/brillen-data-leak/

RIEDEL

Ransomwaregruppe RA World stürzt sich auf Transportunternehmen

17. Oktober 2024, in Bremen/Bremen

DATENPANNE

DATENLECK

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Die Ransomwaregruppe RA World behauptet, Ende Oktober 2024 ein Transportunternehmen aus Bremen angegriffen und dabei 50 GB sensibler Daten gestohlen zu haben – darunter Kundendaten, Geschäftsverträge und Personaldetails. Zur Untermauerung ihrer Forderungen veröffentlichten die Täter erste Dateien und drohten mit der Veröffentlichung der übrigen Daten, insofern es zu keiner Einigung kommt.

Was hätte man besser machen können?
Das Transportunternehmen hätte durch regelmäßige Sicherheitsüberprüfungen und Netzwerksegmentierung den Angriff möglicherweise verhindern können. Zudem wären verschlüsselte Backups und ein Notfallplan zur schnellen Reaktion auf Sicherheitsvorfälle entscheidend gewesen, um die Auswirkungen zu minimieren und die Sicherheit der Kundendaten zu gewährleisten.

Was lernen wir daraus:

Die Ransomwaregruppe RA World nutzt in der Regel Phishing-E-Mails oder schwache Passwörter, um Zugang zu Systemen zu erhalten. Benutzer stellen dabei eine zentrale Schwachstelle dar. Durch gezielte Security Awareness Trainings können Mitarbeitende lernen, sichere Passwörter zu erstellen und verdächtige E-Mails oder Webseiten frühzeitig zu erkennen, wodurch das Risiko erfolgreicher Angriffe deutlich reduziert wird.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/7098-P_B_Cargo-RaWorld.PNG

RIEDEL

Stormous schlägt zu: 12 GB sensible Daten von Identitätsplattform geleakt

16. Oktober 2024, in Berlin/Berlin

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Am 16. Oktober 2024 behauptete die Ransomwaregruppe Stormous, 12 GB sensibler Daten von einer führenden Plattform für digitale Identitätsprüfung erbeutet zu haben. Der Datensatz soll persönliche Fotos, Kontoauszüge, Adressen sowie Etherium- und Bitcoin-Adressen enthalten. Der Vorfall könnte mit einem früheren Angriff zusammenhängen, den die Plattform bereits im Juli 2024 gemeldet hatte.

Was hätte man besser machen können?
Mithilfe eines SOC hätte man den Angriff besser abwehren können. Ein SOC arbeitet mit Cybersecurity-Tools wie SIEM (zur zentralen Überwachung und Analyse von Sicherheitsvorfällen), EDR (zur Absicherung von Endgeräten) und Vulnerability Scanner (zur regelmäßigen Identifizierung und Behebung von Schwachstellen).

Was lernen wir daraus:

Moderne IT-Sicherheitslösungen wie

- **SIEM & SOC**
- **XDR**
- **EDR**
- **SOAR**

tragen präventiv dazu bei, Unternehmen vor Cyberangriffen zu schützen und potenziellen Bedrohungen stets einen Schritt voraus zu sein. Diese Technologien und Strategien erhöhen die Resilienz und Sicherheit von IT-Infrastrukturen erheblich.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6986-fractal-id-stormous.png

RIEDEL

Rückkehr zur Papierdokumentation in Pflegeeinrichtung nach Cyberangriff

16. Oktober 2024, in Gaggenau/Baden-Württemberg

RANSOMWARE

ERPRESSUNG

Was ist passiert?
Ein Cyberangriff legte in der Nacht vom 12. auf den 13. Oktober 2024 die IT-Systeme einer Pflegeeinrichtung lahm. Ein Verschlüsselungstrojaner führte dazu, dass auf Papierdokumentation umgestellt werden musste, um die Versorgung in der Pflegeeinrichtung und die ambulanten Dienste sicherzustellen. Dank regelmäßiger Backups konnten Daten schnell wiederhergestellt und Systeme sukzessive reaktiviert werden. Die Staatsanwaltschaft ermittelt.

Was hätte man besser machen können?
Durch den Einsatz eines SOC, das automatisierte Überwachung und Incident-Response-Tools umfasst, hätte der Angriff besser verhindert werden können. Ein SOC kann kontinuierlich das Netzwerk überwachen, Bedrohungen automatisch erkennen und sofortige Maßnahmen ergreifen, um Angriffe frühzeitig zu stoppen.

Was lernen wir daraus:

Trojaner sind eine der gefährlichsten Formen von Malware. Sie tarnen sich als harmlose Software oder Dateien, um unbemerkt in Systeme einzudringen. Einmal installiert, ermöglichen sie Cyberkriminellen den Zugriff auf sensible Daten, das Stehlen von Informationen oder das Kontrollieren infizierter Geräte. Schutzmaßnahmen wie aktuelle Sicherheitssoftware, regelmäßige Updates und Vorsicht beim Öffnen unbekannter Anhänge sind essenziell, um Trojaner abzuwehren.

Anzunehmende Schadensfelder:

Quellen
https://www.gaggenauer-altenhilfe.de/gaggenauer-altenhilfe-ist-ziel-eines-cyber-angriffs-geworden/

RIEDEL

Tausende Login-Datensätze zum Verkauf angeboten

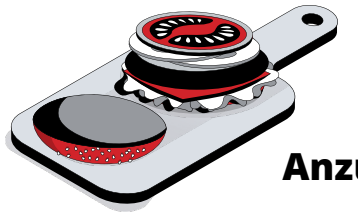
14. Oktober 2024, in Mannheim/Baden-Württemberg

DATENLECK

DATENDIEBSTAHL

Was ist passiert?
Am 14. Oktober 2024 wurde auf BreachForums ein Datenbank-Dump angeboten, der 23.000 Datensätze von einem Lebensmittelzusteller enthält. Die gestohlenen Daten umfassen unter anderem User-IDs, IP-Adressen, Zeitstempel der letzten Anmeldungen und User-Agent-Strings. Die Veröffentlichung auf der Plattform deutet darauf hin, dass diese sensiblen Informationen von Cyberkriminellen erbeutet und zum Verkauf angeboten wurden.

Was hätte man besser machen können?
Strengere Zugriffsrechte hätten sicherstellen können, dass nur autorisierte Personen Zugriff auf die Datenbank erhalten. Die Verschlüsselung der gespeicherten Daten, auch solcher, die auf den ersten Blick harmlos erscheinen, hätte den Missbrauch durch Cyberkriminelle deutlich erschwert. Regelmäßige Sicherheitsprüfungen wären hilfreich gewesen, um potenzielle Schwachstellen in der IT-Infrastruktur frühzeitig zu erkennen und zu beheben.



Was lernen wir daraus:

Ein Datenbank-Dump ist eine Datei, die eine exportierte Kopie einer Datenbank enthält, einschließlich Tabellenstrukturen und gespeicherter Daten. In Cyberangriffen wird ein solcher Dump oft von Hackern gestohlen und auf Foren wie BreachForums angeboten. Er kann in diesem Fall sensible Informationen wie Benutzer-IDs, IP-Adressen oder Anmeldezeitstempel enthalten, die für Identitätsdiebstahl, Phishing oder weitere Angriffe genutzt werden können.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6956-Datenleck-liefermars.png

RIEDEL

Cyberangriff auf diakonische Gesundheitseinrichtungen

13. Oktober 2024, in Berlin/Berlin

AUSFALL

RANSOMWARE

EINBRUCH

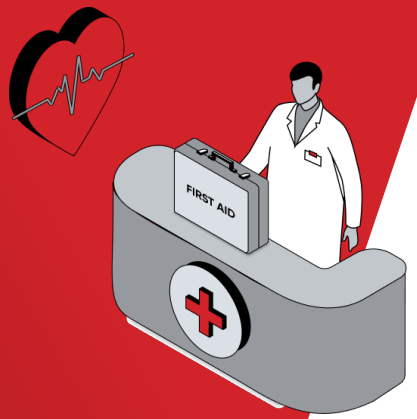
Was ist passiert?
Eine diakonische Organisation, die in mehreren Bundesländern Gesundheitseinrichtungen betreibt, wurde Opfer eines Cyberangriffs. Dabei wurden alle Server verschlüsselt, wodurch die meisten IT-Systeme in den Einrichtungen ausfielen. Betroffen waren unter anderem Patientendaten und die Personaleinsatzplanung. Notfallsysteme wurden aktiviert, und einige planbare Eingriffe mussten verschoben werden. Die Versorgung war jedoch nicht gefährdet.

Was hätte man besser machen können?
Eine 24/7-Überwachung der IT-Systeme wäre entscheidend gewesen, um Bedrohungen in Echtzeit zu erkennen und sofortige Gegenmaßnahmen zu ergreifen.

Darüber hinaus wäre eine regelmäßige Schulung der Mitarbeiter im Umgang mit Sicherheitsbedrohungen hilfreich gewesen, um menschliche Fehler zu minimieren und die Reaktionsfähigkeit auf potenzielle Angriffe zu erhöhen.

Was lernen wir daraus:

Gesundheitseinrichtungen müssen besonders auf den Schutz personenbezogener und sensibler Patientendaten achten. Ein Angriff auf Gesundheitseinrichtungen betrifft nicht nur die IT-Systeme, sondern auch die Sicherheit der Gesundheitsdaten von Patienten. Angesichts des Risikos von Datenexfiltration sollten Verschlüsselung und regelmäßige Backups, sowie strenge Zugriffsrichtlinien zum Standard gehören.



Anzunehmende Schadensfelder:

Quellen
https://www.johannesstift-diakonie.de/cyberangriff
https://www.aerztezeitung.de/Wirtschaft/Cyberangriff-auf-ueberregionalen-Krankenhausbetreiber-453559.html
https://www.golem.de/news/johannesstift-diakonie-cyberangriff-auf-grosses-deutsches-gesundheitsunternehmen-2410-189808.html

RIEDEL

Cyberangriff stört Produktionssysteme bei globalem Druckfarbenhersteller

11. Oktober 2024, in Celle/Niedersachsen

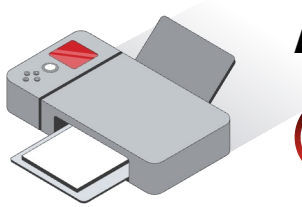
AUSFALL

MALWARE

Was ist passiert?
Ein weltweit führender Hersteller von Druckfarben wurde Ziel eines Cyberangriffs, bei dem Malware das SAP-System und die Internetverbindung des Unternehmens störte. Der Angriff beeinträchtigte vor allem regionale IT-Systeme, während die internationalen Operationen weitgehend verschont blieben. Um die Ausbreitung zu verhindern, wurden betroffene Systeme isoliert. Es kam zu Produktions- und Auslieferungsverzögerungen, während das IT-Team mit externen Experten an der Wiederherstellung arbeitete.

Was hätte man besser machen können?
Man hätte den Schaden durch frühzeitige Erkennung und schnelle Reaktion auf den Angriff minimieren können. Ein gut funktionierendes SOC hätte durch Überwachung und frühzeitige Warnungen den Angriff möglicherweise früher eindämmen können. Zudem hätte eine schnelle Isolierung der betroffenen Systeme und eine gründliche Untersuchung des Vorfalls dazu beigetragen, den Umfang des Datenlecks zu verstehen und effektive Maßnahmen zur Schadensbegrenzung zu ergreifen.

Was lernen wir daraus:
Der Diebstahl von Unternehmensdaten durch Cyberkriminelle stellt Firmen vor enorme Risiken, die über finanzielle Verluste hinausgehen, da auch der Betrieb gestört werden kann. Die Wiederherstellung von Daten und die Einführung zusätzlicher Sicherheitsvorkehrungen können den Geschäftsbetrieb erheblich beeinträchtigen. Langfristig ist eine starke und umfassende Sicherheitsstrategie in sämtlichen Unternehmen erforderlich, um zukünftige Risiken zu minimieren.



Anzunehmende Schadensfelder:

Quellen
https://www.celleheute.de/post/cyberangriff-auf-hubergroup-regionale-it-systeme-beeintr%C3%A4chtigt#google_vignette
https://www.cz.de/lokales/celle-lk/celle/hackerangriff-auf-hubergroup-so-reagiert-das-unternehmen-mit-standort-in-celle-auf-den-vorfall-PXS47HGOCVGCLPFI535V36MFQE.html

RIEDEL

Führender Automobilhersteller wurde erneut Ziel von Cyberkriminellen

EINBRUCH

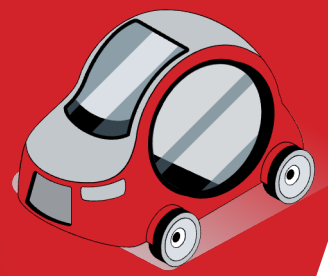
RANSOMWARE

DATENDIEBSTAHL

9. Oktober 2024, in Wolfsburg/Niedersachsen

Was ist passiert?
Im Oktober 2024 bekannte sich ein führender deutscher Autohersteller zu einem Ransomware-Angriff, bei dem die Ransomwaregruppe "8Base" behauptete, vertrauliche Unternehmensdaten erbeutet zu haben. Die gestohlenen Informationen umfassen Rechnungen, Personalakten und viele weitere sensible Daten. Trotz einer Drohung wurden bisher keine Daten veröffentlicht. Das Unternehmen versicherte, dass seine IT-Infrastruktur nicht betroffen sei und beobachtete die Situation weiterhin genau. Erst im April 2024 wurde der Automobilhersteller Opfer eines Cyberangriffs.

Was hätte man besser machen können?
Um den Angriff besser abwehren zu können, hätte der Autohersteller kontinuierliche Investitionen in seine IT-Sicherheit tätigen müssen. IT-Sicherheit ist ein fortlaufender Prozess, der nie endet. Regelmäßige Sicherheitsupdates, ständige Schulungen der Mitarbeiter und die Einführung neuer, fortschrittlicher Sicherheitstechnologien hätten potenzielle Schwachstellen schließen und die Abwehrbereitschaft stärken können.



Was lernen wir daraus:

Eine starke IT-Infrastruktur ist entscheidend, um Ausfälle im Betrieb durch Cyberangriffe zu verhindern. Unternehmen, die in leistungsfähige und stabile Systeme investieren, gewährleisten die Kontinuität ihrer Geschäftsprozesse und reduzieren das Risiko teurer Unterbrechungen.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6902-8Base-Ransomware-Volkswagen-Group.png
https://www.ransomware.live/id/Vm9sa3N3YWdlbiBncm91cEA4YmFzZQ==
https://www.securityweek.com/volkswagen-says-it-infrastructure-not-affected-after-ransomware-gang-claims-data-theft/

RIEDEL

Gemeindeverwaltung und anhängende Ämter durch Cyberangriff gestört

8. Oktober 2024, in Börde/Sachsen-Anhalt

Was ist passiert?
Eine Gemeindeverwaltung in Sachsen-Anhalt wurde Ziel eines Cyberangriffs, der am 8. Oktober 2024 entdeckt wurde. Zur Abwehr schaltete die Verwaltung alle Systeme ab, was zu erheblichen Einschränkungen bei digitalen Diensten führte. Auch angeschlossene Ämter waren nur begrenzt erreichbar. Die genauen Hintergründe des Angriffs und die potenziellen Schäden werden untersucht.

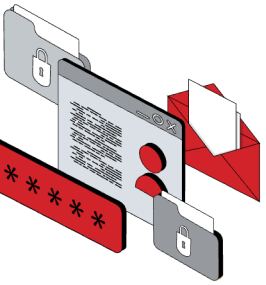
Was hätte man besser machen können?
Sicherheitsüberprüfungen und kontinuierliche Überwachung der IT-Systeme sind entscheidend, um Netzwerke wirksam zu schützen. Solche Maßnahmen hätten möglicherweise auch dazu beigetragen, den Cyberangriff auf die betroffene Gemeindeverwaltung zu verhindern.

AUSFALL

EINBRUCH

Was lernen wir daraus:

Effektives Krisenmanagement ist entscheidend: Im Ernstfall sollten im ersten Schritt sämtliche Systeme umgehend abgeschaltet werden, um den Schaden einzudämmen. Parallel neben der Krisenbewältigung ist eine transparente Kommunikation wichtig, um das Vertrauen der Kunden zu bewahren.



Anzunehmende Schadensfelder:

Quellen
https://www.elbe-heide.de/news/1/987561/nachrichten/eingeschr%C3%A4nkte-erreichbarkeit-der-verwaltung-der-verbandsgemeinde-elbe-heide.html

RIEDEL

Ransomware-Angriff auf bekannten Online-Händler: Daten in Gefahr

7. Oktober 2024, in Berlin/Berlin

EINBRUCH

RANSOMWARE

DATENDIEBSTAHL

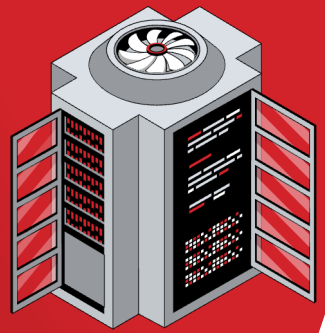
Was ist passiert?
Ein führender Online-Händler für Autoteile wurde offenbar Ziel eines Ransomware-Angriffs. Die Gruppe "RansomHub" behauptet, sensible persönliche und geschäftliche Daten des Unternehmens kompromittiert zu haben und hat Beweis-Screenshots veröffentlicht. Sie drohen mit der Veröffentlichung der Daten, sollte kein Lösegeld gezahlt werden.

Was hätte man besser machen können?
Ein Security Operations Center (SOC) hätte den Schaden durch die frühzeitige Identifikation des Angriffs, eine zügige Eindämmung sowie klare und gezielte Kommunikation erheblich begrenzen können.

Was lernen wir daraus:

Technologien wie SIEM, SOC, XDR, EDR, SOAR, (D)DoS-Abwehr, moderne Firewalls, SD-WAN und SASE gehen über reine Schlagworte hinaus. Sie sind zentrale Werkzeuge für den Schutz vor Cyberangriffen und helfen Unternehmen, proaktiv auf Bedrohungen zu reagieren. Durch ihre Anwendung werden IT-Infrastrukturen widerstandsfähiger und Sicherheitslücken gezielt minimiert.

Anzunehmende Schadensfelder:



Quellen
https://www.security-incidents.de/assets/img/incidents/6869-Ransomhub-AutodocPro.png
https://www.ransomware.live/id/YXV0b2RvYy5wcm9AcmFuc29taHVi

RIEDEL

Erhöhtes Phishing-Risiko durch E-Mail-Server-Kompromittierung

6. Oktober 2024, in Berlin/Berlin

EINBRUCH

DATENDIEBSTAHL

Was ist passiert?
Ein führendes Unternehmen im Bereich Reise-Technologie wurde in der Nacht zum 3. Oktober 2024 Ziel eines Cyberangriffs. Dank rascher Gegenmaßnahmen konnten Buchungs- und Zahlungsdaten geschützt werden. Allerdings beeinträchtigte der Angriff den E-Mail-Server, wodurch das Risiko von Phishing erhöht ist. Kunden und Partner wurden zur Wachsamkeit aufgerufen, während Sicherheitsmaßnahmen weiter verstärkt wurden.

Was hätte man besser machen können?
Man hätte durch frühzeitige Bedrohungserkennung und proaktive Sicherheitsmaßnahmen den Angriff möglicherweise verhindern können. Der Einsatz von SIEM & SOC hätte verdächtige Aktivitäten schneller erkannt und darauf reagiert. Zudem hätten regelmäßige Sicherheitsüberprüfungen und Updates der Systeme dazu beigetragen, Schwachstellen zu schließen.

Was lernen wir daraus:

Cyberangriffe verlaufen häufig in mehreren Phasen, wobei Angreifer nach dem Eindringen oft unbemerkt in den Systemen verbleiben, um Informationen zu sammeln oder weitere Schwachstellen auszunutzen. Dieser Zeitraum, die sogenannte "Dwell Time," wird immer länger und beträgt im Durchschnitt mittlerweile rund 20 Tage. Während dieser Zeit bereiten die Angreifer ihre eigentlichen Aktivitäten vor, wie etwa Datenexfiltration oder Systemverschlüsselung. Diese verzögerte Entdeckung erhöht das Schadenspotenzial erheblich, da Angreifer wertvolle Einblicke in die IT-Struktur gewinnen können.

Anzunehmende Schadensfelder:

Quellen
https://www.reisevor9.de/inside/traffics-systemlandschaft-mit-cyberangriff-konfrontiert

RIEDEL

Sensible Daten von Bauunternehmen im Darknet veröffentlicht

5. Oktober 2024, in Gelsenkirchen/Nordrhein-Westfalen

RANSOMWARE

EINBRUCH

DATENDIEBSTAHL

Was ist passiert?
Am 4. Oktober 2024 wurde ein deutsches Bauunternehmen Opfer eines Ransomware-Angriffs durch die Gruppe "INC Ransom". Die Angreifer veröffentlichten sensible Daten im Darknet, darunter Rechnungen, gescannte Ausweisdokumente sowie Excel-Tabellen mit gespeicherten Passwörtern.

Was hätte man besser machen können?
Ein Security Operations Center (SOC) hätte den Vorfall durch Präventionsmaßnahmen und effektives Management besser handhaben können. Bedrohungen wären durch kontinuierliches Monitoring und regelmäßige Sicherheitsprüfungen frühzeitig erkannt worden. Während des Angriffs hätte das SOC schnelle Eindämmungsmaßnahmen und koordinierte Reaktionen eingeleitet.

Was lernen wir daraus:

INC Ransom nutzt hochentwickelte Methoden, darunter gezielte Phishing-Kampagnen und Exploits in ungepatchter Software, um in Netzwerke einzudringen. Nach der Infektion werden Daten verschlüsselt und sensible Informationen exfiltriert. Ihre "Double Extortion"-Taktik – die Drohung, Daten öffentlich zu machen – erhöht den Druck auf Opferunternehmen, Lösegeld zu zahlen.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6842-INC-Ransom-STORCK-Ausbaugesellschaft.png

RIEDEL

Vertrauliche Firmendokumente eines Pharmaunternehmens gestohlen

3. Oktober 2024, Oberhaching/Bayern

EINBRUCH

DATENLECK

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Eine deutsches Pharmaunternehmen ist Ziel eines Ransomware-Angriffs geworden. Am 3. Oktober 2024 tauchte das Unternehmen auf der Darknet-Leakseite der Hackergruppe „Dragonforce“ auf. Die Angreifer behaupten, über 51 GB sensible Daten gestohlen zu haben, darunter vertrauliche Firmendokumente, und drohten mit einer Veröffentlichung. Ob ein Lösegeld gefordert wurde, bleibt unklar.

Was hätte man besser machen können?
Um den Cyber-Angriff auf das Pharmaunternehmen zu verhindern oder die Auswirkungen zu minimieren, wären stärkere Netzwerksicherheitsmaßnahmen, regelmäßige Updates und Patches sowie verbesserte Zugriffskontrollen wichtig gewesen.

Zusätzlich hätten die Verschlüsselung kritischer Daten, regelmäßige Datensicherungen und eine permanente Überwachung der IT-Infrastruktur dazu beigetragen, Schäden zu begrenzen.

Was lernen wir daraus:

Im Zuge der NIS2-Richtlinie sind Unternehmen verpflichtet, die nachfolgenden grundlegenden Cybersicherheitsmaßnahmen einzuführen, um die IT-Infrastruktur und Netzwerke, die ihre kritischen Dienstleistungen unterstützen, effektiv abzusichern:

- Policies: Richtlinien für Risiken und Informationssicherheit
- Incident Management: Prävention, Detektion und Bewältigung von Sicherheitsvorfällen
- Business Continuity: Backup-Management, Desaster Recovery, Krisenmanagement
- Effektivität: Vorgaben zur Messung von Cyber- und Risikomaßnahmen
- Kryptographie: Verschlüsselung wo immer möglich
- Zugangskontrolle: Einsatz von Multi-Faktor-Authentifizierung und Single Sign-on
- Kommunikation: Einsatz sicherer Sprach-, Video- und Text-Kommunikation
- Einkauf: Sicherheit in der Beschaffung von IT und Netzwerk-Systemen
- Supply Chain: Sicherheit in der Lieferkette

Anzunehmende Schadensfelder:

Quellen
https://www.ransomware.live/id/THlvbWFyayBOaGFybWFAZHIhZ29uZm9yY2U=
https://www.security-incidents.de/assets/img/incidents/6826-Dragonforce-LyomarkPharma.jpg

RIEDEL

Patientenversorgung blieb bei Angriff auf Lungenfachklinik unberührt

2. Oktober 2024, in Münnerstadt/Bayern

AUSFALL

Was ist passiert?
Anfang Oktober 2024 fiel eine bayrische Lungenfachklinik einer Cyberattacke zum Opfer, wodurch die IT-Systeme stark beeinträchtigt wurden. Die Klinik reagierte prompt mit Untersuchungen und Wiederherstellungsmaßnahmen. Trotz des Angriffs bleibt die Patientenversorgung laut Klinikangaben sichergestellt.

Was hätte man besser machen können?
Regelmäßige, isolierte Backups sind essenziell, um nach einem Angriff schnell wieder handlungsfähig zu sein. Sie minimieren Datenverluste und üben bei Lösegeldforderungen weniger Druck aus. Wichtig sind regelmäßige Sicherungen, eine sichere Aufbewahrung außerhalb des Netzwerks, regelmäßige Tests der Wiederherstellung sowie der Einsatz moderner Technologien.

Was lernen wir daraus:

Kriminelle Hacker nehmen gezielt Unternehmen aus systemrelevanten Sektoren – wie dem Gesundheitswesen – ins Visier, um größtmöglichen Schaden anzurichten. Solche Attacken gefährden die Funktion lebenswichtiger Dienste und die öffentliche Sicherheit.

Anzunehmende Schadensfelder:

Quellen
https://www.mainpost.de/regional/bad-kissingen/cyberangriff-auf-das-thoraxzentrum-muennerstadt-it-systeme-der-lungen-fachklinik-funktionieren-nur-eingeschraenkt-art-11623472
https://www.security-incidents.de/assets/img/incidents/6855-Thoaxzentrum_Muennerstadt.PNG

RIEDEL

Labor muss wegen unzureichender IT-Sicherheit bluten: 120 GB gestohlene Daten

1. Oktober 2024, in Hamburg/Hamburg

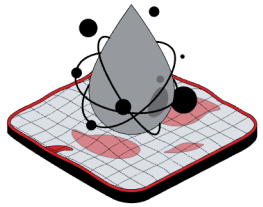
EINBRUCH

DATENDIEBSTAHL

ERPRESSUNG

Was ist passiert?
Am 1. Oktober 2024 gab die Erpressergruppe Cactus bekannt, dass sie 120 GB an Daten eines Laboratoriums aus Hamburg entwendet hat. Der Angriff, der als Ransomware-Attacke identifiziert wurde, führte zur Exfiltration von sensiblen Unternehmensinformationen. Laut den Tätern befinden sich darunter Datenbank-Backups, Projektdaten, Zeichnungen und weitere geschäftskritische Informationen. Die Hintergründe des Vorfalls und die Auswirkungen auf das Unternehmen sind unklar.

Was hätte man besser machen können?
Das Laboratorium hätte durch frühzeitige und kontinuierliche Sicherheitsüberprüfungen sowie proaktive Überwachung der IT-Systeme besser vorbereitet sein können. Eine sofortige und umfassende Reaktion auf den vorherigen IT-Sicherheitsvorfall hätte mögliche Schwachstellen identifiziert und behoben, bevor sie ausgenutzt werden konnten. Zudem hätten regelmäßige Penetrationstests und ein robuster Incident-Response-Plan den aktuellen Angriff möglicherweise verhindert oder dessen Auswirkungen reduziert.



Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6798-GALAB-Laboratories-Cactus-Ransomware.png

Was lernen wir daraus:

Eine umfassende Cybersicherheitsstrategie vereint Prävention, Detektion und Reaktion.

- **Prävention** beginnt mit robusten Sicherheitslösungen wie Firewalls und regelmäßigen Updates sowie Mitarbeiterschulungen, um Risiken zu minimieren.
- **Detektion** nutzt Technologien wie SIEM und EDR zur frühzeitigen Erkennung von Bedrohungen in Echtzeit.
- **Reaktion** erfordert einen klaren Incident-Response-Plan und die Unterstützung von Experten, um schnell auf Vorfälle zu reagieren und Schäden zu begrenzen.

Alle drei Aspekte zusammen gewährleisten einen effektiven Schutz der IT-Infrastruktur.

RIEDEL

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

GASTARTIKEL

CLARIUS.LEGAL

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.LEGAL 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.LEGAL Data & Security GmbH mit der RIEDEL Networks GmbH & Co. KG zusammen. Während CLARIUS.LEGAL 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.LEGAL 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.LEGAL 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.LEGAL von Dr. Ernst Georg Berger und Nils Oberschelp. Mit über 180 Kunden zählt sie zu den Vorreitern innovativer Rechtsberatung.

RIEDEL

SEPTEMBER 2024

SECURITY INCIDENTS GERMANY

RIEDEL

Ransomware-Angriff trifft Sozialunternehmen: Sensible Daten in Gefahr

30. September 2024, in München/Bayern

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Ende September 2024 wurde ein Sozialunternehmen Ziel eines Ransomware-Angriffs, bei dem Cyberkriminelle Daten erbeuteten und Server verschlüsselten. Es wird vermutet, dass personenbezogene Daten von Spendern, darunter Namen, Adressen, Kontoinformationen und Steuerdaten, gestohlen wurden. Bei der Analyse des Vorfalls wurde festgestellt, dass in erheblichem Umfang personenbezogene Daten betroffen sind – die betroffenen Personen wurden informiert. Aufgrund des Angriffs wurden einige Systeme zwischenzeitlich offline genommen.

Was hätte man besser machen können?
Um den Ransomware-Angriff zu verhindern, hätte der Einsatz von fortschrittlichen SOC-Systemen helfen können. Dazu zählen EDR für die frühzeitige Erkennung von Bedrohungen, regelmäßige Schwachstellen-Scans und Patch-Management zur Beseitigung von Sicherheitslücken.

Zudem hätte ein robustes Backup- und Wiederherstellungssystem den Schaden minimieren können.

Was lernen wir daraus:

Um das Risiko von Missbrauch zu minimieren, müssen sensible Daten jederzeit umfassend geschützt und verschlüsselt werden. Sicherheitslücken können nicht nur schwerwiegende Auswirkungen auf die betroffenen Personen haben, sondern auch schwerwiegende rechtliche und betriebliche Folgen für die Organisation nach sich ziehen, die diese Daten unzureichend absichert. Ein durchgehender Schutz ist daher entscheidend, um potenzielle Schäden und rechtliche Konsequenzen zu vermeiden.

Anzunehmende Schadensfelder:

Quellen
https://www.hausdesstiftens.org/ueber-uns/cyberangriff/

RIEDEL

Angriff auf deutschen Automobilzulieferer

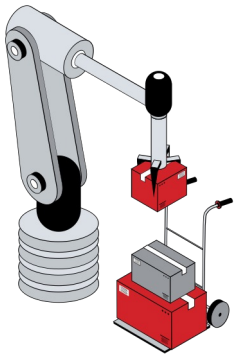
29. September 2024, Leutenbach/Baden-Württemberg

RANSOMWARE

Was ist passiert?
Am 29. September 2024 meldete die Ransomwaregruppe "Play" einen deutschen Zulieferer der Automobilindustrie als Opfer auf ihrer Leak-Seite. Sie behaupten, sensible Daten erbeutet zu haben, darunter Kundendokumente, Lohn- und Steuerdaten sowie weitere vertrauliche Finanz- und personenbezogene Informationen. Die Gruppe droht, die gestohlenen Daten zu veröffentlichen, sollte keine Einigung erzielt werden.

Was hätte man besser machen können?
Um die Auswirkungen des Cyberangriffs zu verringern, hätte das Unternehmen strengere Sicherheitsvorkehrungen ergreifen, umfassende Notfallpläne entwickeln und diese regelmäßig auf ihre Effektivität hin testen sollen. Eine verbesserte Aufteilung der IT-Systeme, regelmäßige Backups sowie fortlaufende Schulungen der Mitarbeiter wären ebenfalls entscheidende Maßnahmen gewesen. Darüber hinaus hätte eine kontinuierliche Überwachung und der Einsatz von Bedrohungsanalysen frühzeitig Hinweise auf potenzielle Risiken geben können.

Was lernen wir daraus:
In Zukunft könnten sich Angreifer noch raffinierter in ihre Angriffe integrieren, beispielweise durch die Nutzung von KI, um spezifische Schwächen von Zielunternehmen – wie die des Automobilzulieferers – zu ermitteln. Umgekehrt können Unternehmen KI-basierte Systeme einsetzen, um Muster in ihren Netzwerken zu erkennen und potenzielle Bedrohungen frühzeitig zu identifizieren.



Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6784-reutter-play.png

RIEDEL

Daten einer deutschen Bäckereikette tauchen im Darknet auf

26. September 2024, in Limburg/Hessen

EINBRUCH

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Am 26. September 2024 meldete die Ransomwaregruppe Akira auf ihrer Darknet-Seite einen Angriff auf eine deutsche Bäckereikette. Die Täter behaupten, 14 GB sensible Daten erbeutet zu haben, darunter Informationen zu Mitarbeitern, Finanzunterlagen und Verträge.

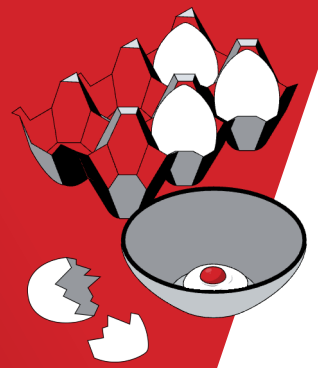
Was hätte man besser machen können?
Um den Sicherheitsvorfall zu verhindern, hätte die Bäckerei ein Security Operations Center (SOC) einsetzen sollen, das Bedrohungen in Echtzeit erkennt. Ein SOC hätte durch die zentrale Überwachung und Analyse sicherheitsrelevanter Ereignisse ungewöhnliche Aktivitäten frühzeitig identifizieren können.

Zusätzlich hätte ein Security Information and Event Management (SIEM)-System eingesetzt werden sollen. Ein SIEM-System sammelt und analysiert Sicherheitsdaten aus verschiedenen Quellen innerhalb der IT-Infrastruktur.

Was lernen wir daraus:

Ein alarmierender Trend ist die zunehmende vereinfachte Zugänglichkeit von Cyberkriminalität. Was früher fundiertes technisches Wissen und hohe Ressourcen erforderte, ist heute durch das Darknet leicht zugänglich. Selbst Laien können ausgefeilte Schadsoftware erwerben oder Phishing-Angriffe starten. Diese Entwicklung zwingt Unternehmen dazu, ihre Schutzmaßnahmen stetig zu verbessern und flexibel auf neue Bedrohungen zu reagieren.

Anzunehmende Schadensfelder:



Quellen
https://www.security-incidents.de/assets/img/incidents/6747-Akira-Sch%C3%A4fer-mein-B%C3%A4cker.png

RIEDEL

Produktionsstopp und Datenkompromittierung nach Angriff auf Metallwarenhersteller

24. September 2024, in Aachen/ Nordrhein-Westfalen

RANSOMWARE

EINBRUCH

DATENDIEBSTAHL

Was ist passiert?

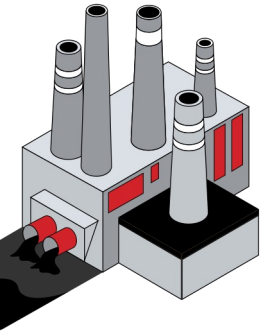
Ein renommierte Metallwarenhersteller aus Aachen wurde Ende September 2024 Ziel einer Ransomware-Attacke durch die Gruppe 8Base. Die Täter luden vertrauliche Daten wie Verträge, Arbeitnehmerinformationen und Geschäftsdaten herunter. Nach einer Warnung des LKA München stellte das Unternehmen seine IT-Systeme ab. Die Produktion wurden nach kurzer Zeit zum Teil wieder aufgenommen, doch die vollständige Wiederherstellung dauerte einige Tage. Da keine Lösegeldzahlung erfolgte, wurden die Daten öffentlich zugänglich.

Was hätte man besser machen können?

Im Vorfeld hätte Der Metallwarenhersteller spezialisierte Sicherheitslösungen und kontinuierliche Schwachstellenanalysen durchführen sollen. Eine umfassende Incident-Response-Strategie, regelmäßige Notfallübungen und fortschrittliche Bedrohungserkennungssysteme wären ebenfalls wichtig gewesen. Zudem hätten isolierte Backups und gezielte Mitarbeiterschulungen die Reaktionsfähigkeit und Sicherheit verbessert.

Was lernen wir daraus:

Wenn Cyberkriminelle sensible Daten entwenden, stehen Unternehmen vor erheblichen Herausforderungen. Neben finanziellen Verlusten sind auch Betriebsunterbrechungen häufig die Folge, da die Wiederherstellung von Systemen und die Einführung neuer Sicherheitsmaßnahmen erhebliche Ressourcen beanspruchen können. Langfristig sind solche Vorfälle ein Weckruf, die Sicherheitsinfrastruktur zu stärken und präventive Strategien umfassend zu etablieren, um zukünftige Angriffe zu vermeiden.



Anzunehmende Schadensfelder:

Quellen

https://www.aachener-zeitung.de/lokales/region-aachen/aachen/grossangelegter-hacker-angriff-auf-schumag-ag/20807681.html

https://www.it-daily.net/shortnews/hackerangriff-zwingt-traditionsunternehmen-in-die-insolvenz

RIEDEL

Daten von gesetzlicher Unfallversicherung gefährdet nach Angriff

20. September 2024, in Hamburg/Hamburg

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Eine der größten Träger der gesetzlichen Unfallversicherung in Deutschland wurde Opfer einer Ransomware-Attacke, bei der ein Server des Online-Campus kompromittiert wurde. Die Angreifer erlangten möglicherweise Zugriff auf personenbezogene Daten wie Namen, E-Mail-Adressen, Telefonnummern, Arbeitgeber und Adressen. Der betroffene Server wurde offline genommen, und die betroffenen Nutzer wurden informiert. Details zu den Tätern und einem möglichen Lösegeldforderungen sind unklar.

Was hätte man besser machen können?
Um die Folgen des Ransomware-Angriffs zu minimieren, hätte der Träger der Unfallversicherung mehrere präventive und reaktive Maßnahmen ergreifen sollen. Ein verbessertes Risikomanagement durch regelmäßige Schwachstellenanalysen und den Einsatz spezialisierter Bedrohungserkennungssysteme hätte frühe Hinweise auf den Angriff geliefert.

Anzunehmende Schadensfelder:

Was lernen wir daraus:

Eine effektive Cybersicherheitsstrategie erfordert einen umfassenden Ansatz, der alle Bereiche der IT-Infrastruktur eines Unternehmens berücksichtigt. Dazu zählen:

- **Risikomanagement**: Unternehmen sollten regelmäßig Sicherheitsprüfungen und Risikoanalysen durchführen, um Schwachstellen zu identifizieren und deren Priorität zu bestimmen.
- **Sicherheitsrichtlinien**: Es sollten klare Regeln und Verfahren für den Umgang mit vertraulichen Informationen, Zugriffsrechten und Sicherheitsvorfällen etabliert und durchgesetzt werden.
- **Notfallmanagement**: Unternehmen müssen über gut definierte Pläne für die Reaktion auf Sicherheitsvorfälle verfügen, die regelmäßig überprüft und aktualisiert werden. Dies umfasst auch Maßnahmen zur Sicherstellung der Betriebsfähigkeit im Falle eines Cyberangriffs.

Quellen
https://www.heise.de//news/Ransomware-Unfallversicherung-Pharmafirmen-in-den-USA-und-andere-betroffen-9863136.html
https://fragdenstaat.de/anfrage/benachrichtigung-nach-art-34-dsgvo-sicherheitsvorfall-bei-der-verwaltungs-berufsgenossenschaft/

RIEDEL

Ransomware-Angriff auf Mineralöl-Lieferant: Sensible Daten im Darknet aufgetaucht

19. September 2024, in Straubing/Bayern

DATENDIEBSTAHL

EINBRUCH

RANSOMWARE

DATENLECK

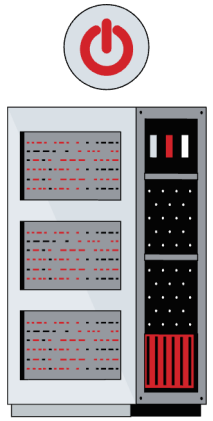
Was ist passiert?
Am 19. September 2024 wurde ein Mineralöl-Lieferant aus Straubing auf dem Opferblog einer Ransomwaregruppe im Darknet aufgeführt. Die Angreifer hatten offenbar auf sensible Daten des Unternehmens zugegriffen, darunter Finanz- und Personaldaten sowie Verträge und Kundendaten. Das Unternehmen hat sich bislang nicht öffentlich zu dem Vorfall geäußert.

Was hätte man besser machen können?
Der Einsatz fortschrittlicher IT-Sicherheitslösungen hätte den Angriff möglicherweise verhindert. SIEM & SOC hätten Bedrohungen frühzeitig erkannt, XDR und EDR hätten umfassende Schutzmaßnahmen geboten und SOAR hätte automatisierte Reaktionen ermöglicht.

Next-Generation Firewalls, (D)DoS Protection, SD-WAN und SASE hätten zusätzlichen Schutz und Netzwerksicherheit gewährleistet.

Was lernen wir daraus:

Die EU-weite NIS2-Richtlinie, die strengere Sicherheitsanforderungen für kritische Infrastrukturen (KRITIS) festlegt, hebt die Bedeutung umfassender Cyberabwehrmaßnahmen hervor. Unternehmen, die unter diese Richtlinie fallen, sind verpflichtet, fortschrittliche Sicherheitsvorkehrungen zu treffen. Dazu gehören kontinuierliche Überwachung, der Schutz wesentlicher Systeme und die Implementierung effektiver Notfallpläne.



Anzunehmende Schadensfelder:

Quellen
https://www.ransomware.live/id/TnVzc2VyIE1pbmVyYWzDtmwgR21iSEBpbmNyYW5zb20=
https://www.security-incidents.de/assets/img/incidents/6643-incransom-nusser.png

RIEDEL

Sicherheitsvorfall: Datenlecks bei Vergleichsportalen

17. September 2024, in München/Bayern

DATENLECK

SICHERHEITSLÜCKE

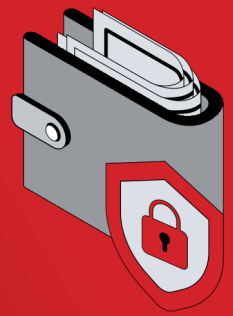
Was ist passiert?
Zwei der bekanntesten deutschen Vergleichsportale, die Finanzdienstleistungen wie Kredite vermitteln, haben gravierende Sicherheitslücken in ihren Systemen aufgewiesen. Unbefugte konnten durch diese Lücken auf sensible Kundendaten zugreifen, darunter persönliche und finanzielle Informationen. Die Schwachstellen betrafen insbesondere den Bereich der Kreditvermittlung und könnten Millionen von Nutzern betroffen haben. Die Anbieter bestätigten die Fehler und behoben die Sicherheitslücken, jedoch bleibt unklar, ob Daten missbraucht wurden. Die zuständigen Datenschutzbehörden haben den Fall übernommen und rechtliche Konsequenzen sind möglich.

Was hätte man besser machen können?
Um den Vorfall zu verhindern, hätten die betroffenen Unternehmen regelmäßige und gründlichere Sicherheitsprüfungen durchführen sollen. Eine verbesserte Verschlüsselung und striktere Zugangskontrollen hätten den Zugriff auf persönliche Daten verhindert. Zudem wäre eine schnellere und transparente Kommunikation mit den Nutzern entscheidend gewesen, um Vertrauen zu bewahren und mögliche Schäden frühzeitig zu minimieren.

Was lernen wir daraus:

Der Fall zeigt, wie entscheidend eine robuste IT-Sicherheit in Unternehmen ist, die mit sensiblen Daten arbeiten. Er verdeutlicht, dass selbst große Vergleichsportale mit erheblichen Sicherheitslücken zu kämpfen haben, wodurch Angreifer potenziell Millionen Nutzer gefährden können. Regelmäßige Sicherheitsprüfungen und das schnelle Schließen von entdeckten Lücken sind jedoch für jede Unternehmensgröße essenziell.

Anzunehmende Schadensfelder:



Quellen
https://correctiv.org/aktuelles/datenschutz/2024/09/17/kreditvermittlung-bei-check24-und-verivox-kritische-datenlecks-entdeckt/
https://www.ccc.de/de/check24-und-verivox-darlehensvertrage-im-datenleckvergleich

RIEDEL

Ransomware-Angriff trifft Schulen in Düren

17. September 2024, in Düren/Nordrhein-Westfalen

AUSFALL

RANSOMWARE

Was ist passiert?
Zwei Schulen in Düren wurden im September 2024 Ziel von Cyber-Angriffen. Die Server der betroffenen Schulen fielen fast zeitgleich aus. Die Stadt reagierte sofort und trennte die Server aller städtischen Schulen vom Netz, um größeren Schaden zu verhindern. Die Ursache für die Ausfälle war vermutlich eine Ransomware-Attacke. Die Stadtverwaltung und IT-Dienstleister arbeiteten daran, die Systeme wiederherzustellen.

Was hätte man besser machen können?
Regelmäßige Sicherheitsüberprüfungen sind entscheidend, um potenzielle Schwachstellen in der IT-Infrastruktur frühzeitig zu identifizieren und zu beheben. Dazu gehören Penetrationstests und Schwachstellenscans, die helfen, Sicherheitslücken zu entdecken, bevor sie von Angreifern ausgenutzt werden können.

Was lernen wir daraus:

Neben Unternehmen sind auch Schulen Ziel von Cyberkriminellen. Bildungseinrichtungen sind sogar besonders attraktive Ziele, da sie persönliche Daten von Schülern, Lehrkräften und Mitarbeitenden speichern und zudem oft Zugang zu sensiblen Informationen und Forschungsergebnissen haben. Angreifer nutzen diese Daten, um Lösegeld zu erpressen oder andere kriminelle Aktivitäten durchzuführen.

Anzunehmende Schadensfelder:

Quellen
https://www.radiorur.de/artikel/cyber-angriff-auf-duerener-schulen-2106077.html
https://dn-news.de/dueren/2024/09/17/server-in-zwei-duerener-schulen-ausgefallen/

RIEDEL

Ransomware-Angriff auf Radiosender – Musikdateien verschlüsselt

15. September 2024, in Geretsried/Bayern

RANSOMWARE

AUSFALL

ERPRESSUNG

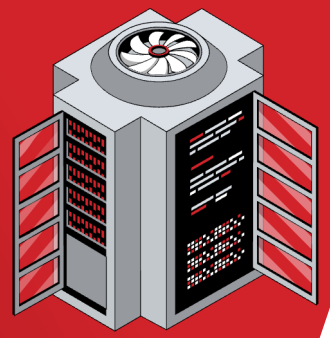
Was ist passiert?
In der Nacht vom 14. auf den 15. September 2024 wurde ein deutscher Radiosender Opfer einer Ransomware-Attacke. Die Angreifer verschlüsselten alle Musikdateien und fordern ein hohes Lösegeld. Der Sender arbeitete daran, auf zugängliche Daten zuzugreifen und plante, die Systeme neu zu installieren. Rund eine Woche lief nur ein Notprogramm. Der Sender informierte seine Hörer via Social Media, sobald der Normalbetrieb wiederhergestellt ist.

Was hätte man besser machen können?
Im Vorfeld hätte der Radiosender ein fortschrittliches EDR-System implementieren sollen. EDR hätte dabei geholfen, ungewöhnliche Aktivitäten frühzeitig zu erkennen und zu analysieren, um potenzielle Angriffe schnell zu identifizieren und darauf zu reagieren. Zusätzlich wären regelmäßige Schwachstellenanalysen und umfassende Incident-Response-Strategien wichtig gewesen, um die Sicherheitslage weiter zu verbessern.

Was lernen wir daraus:

Viele Ransomwaregruppen wenden die Taktik der doppelten Erpressung an. Sie verschlüsseln zunächst die Daten des Opfers und fordern ein Lösegeld für deren Freigabe. Zusätzlich drohen sie, vertrauliche Informationen zu veröffentlichen oder weiterzugeben. Diese Vorgehensweise erhöht den Druck auf die Opfer erheblich und steigert die Wahrscheinlichkeit, dass sie das geforderte Lösegeld zahlen.

Anzunehmende Schadensfelder:



Quellen
https://www.radio-geretsried.de/index.php/2024/09/15/eilmeldung-grosser-hackerangriff-auf-radio-geretsried-wir-arbeiten-an-der-loesung/

RIEDEL

Wiederholter Angriff zeigt Lücken in Sicherheitsstrategien

11. September 2024, in Kempen/Nordrhein-Westfalen

EINBRUCH

DATENDIEBSTAHL

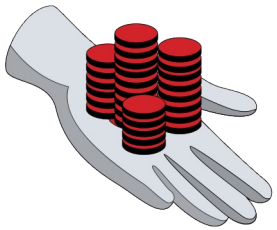
RANSOMWARE

Was ist passiert?
Ende August 2024 wurde ein Elektrogerätegroßhändler Ziel der Blacksuit-Ransomwaregruppe. Mitte September meldete die Hackergruppe FOG einen weiteren Angriff auf dasselbe Unternehmen und behauptete, 469 GB Daten entwendet zu haben. Ob sensible Informationen betroffen sind oder ein Zusammenhang zwischen den Vorfällen besteht, ist unklar.

Was hätte man besser machen können?
Um den Schaden zu begrenzen, hätte das Unternehmen durch den Einsatz von Sicherheitslösungen wie SIEM, die eine frühzeitige Erkennung von ungewöhnlichen Aktivitäten ermöglichen, sowie EDR, das eine schnelle Reaktion auf Bedrohungen erlaubt, besser vorbereitet sein können. Zusätzlich hätten regelmäßige und sichere Backups die schnelle Wiederherstellung von Daten im Falle eines Angriffs gewährleistet.

Was lernen wir daraus:

Nach dem ersten Ransomware-Angriff könnte man erwarten, dass das Unternehmen schnell eine umfassende Sicherheitsinfrastruktur aufgebaut hat, um erneute Angriffe zu verhindern. Die Realität ist jedoch, dass die Nachbearbeitung eines solchen Vorfalls oft eine langwierige und ressourcenintensive Aufgabe ist. Die Wiederherstellung von Daten und die Schließung von Sicherheitslücken erfordern Zeit. Zudem ist der Aufbau eines robusten Sicherheitskonzepts ein kontinuierlicher Prozess, der nicht von heute auf morgen abgeschlossen werden kann. Angreifer nutzen oft diese Phase, um erneut zuzuschlagen. Dies verdeutlicht, wie entscheidend es ist, IT-Sicherheit als langfristige, proaktive und reaktive Strategie zu betrachten.



Anzunehmende Schadensfelder:

Quellen
https://ransomfeed.it/index.php?page=post_details&id_post=17362
https://x.com/TMRansomMon/status/1833850106950344794

RIEDEL

Cyberangriff auf Bundesliga-Account: Zwei Hacks in drei Tagen

10. September 2024, in Gelsenkirchen/Nordrhein-Westfalen

BETRUG

EINBRUCH

Was ist passiert?
Im September 2024 wurde der X-Account eines großen Fußballclubs aus der 2. Bundesliga mit über 800.000 Followern von Cyberkriminellen übernommen. Die Angreifer nutzten das Profil, um Werbung für eine angebliche Kryptowährung zu machen und eine fragwürdige Webseite zu verlinken. Der Club entschuldigte sich etwa 30 Minuten später und stellte den Account wieder her. Drei Tage später wurde der Account erneut gehackt. Dabei veröffentlichten die Angreifer falsche Informationen, wie die Nachricht, dass ein verletzter Spieler für kommende Spiele des Vereins auflaufen würde, obwohl er zu dieser Zeit bei einem anderen Verein unter Vertrag stand.

Was hätte man besser machen können?
Um den Angriff auf den Social-Media-Account zu verhindern, wäre der Einsatz von Zwei-Faktor-Authentifizierung (2FA) entscheidend gewesen. Diese zusätzliche Sicherheitsebene hätte es Angreifern erschwert, allein mit einem gestohlenen Passwort Zugriff zu erhalten. Ebenso wichtig ist die Verwendung sicherer Passwörter, die regelmäßig aktualisiert werden, um das Risiko durch bekannte oder geleakte Zugangsdaten zu minimieren.

Was lernen wir daraus:

Der Angriff auf den Social-Media-Account verdeutlicht, wie schnell Reputationsschäden entstehen, wenn Follower mit betrügerischen Inhalten konfrontiert werden. Zudem besteht die Gefahr, dass Falschinformationen sich rasant verbreiten und dadurch finanzielle Verluste sowie langfristige Vertrauensverluste nach sich ziehen.

Anzunehmende Schadensfelder:

Quellen
https://www.aachener-zeitung.de/region-nrw/schalkes-x-account-gehackt-jetzt-hat-es-auch-uns-erwischt/19769973.html
https://www.reviersport.de/fussball/2bundesliga/a608548---schalke-s04-x-account-gehackt-steckte-dahinter.html

RIEDEL

Christliches Sozialunternehmen wird erpresst

6. September 2024, in Köln/Nordrhein-Westfalen

DATENDIEBSTAHL

EINBRUCH

RANSOMWARE

Was ist passiert?
Ein Sozialunternehmen, das mehrere Senioren- und Pflegeeinrichtungen betreibt, wurde Anfang September 2024 Opfer eines Ransomware-Angriffs. Die Gruppe „RansomHub" nahm das Unternehmen auf ihre Darknet-Liste und behauptete, 263 GB gestohlene Daten zu besitzen. Sie forderten ein Lösegeld, andernfalls drohten sie, die Daten zu veröffentlichen.

Was hätte man besser machen können?
Das Unternehmen hätte den Schaden durch den Cyberangriff verringern können, indem es regelmäßige Sicherheitsüberprüfungen, Backups durchgeführt und seine Mitarbeiter geschult hätte. Der Einsatz von spezialisierten Cybersecurity-Teams und redundanten IT-Systemen hätte ebenfalls geholfen, den Betrieb schneller wiederherzustellen und die Auswirkungen des Angriffs zu minimieren.

Was lernen wir daraus:

Wenn Pflege- und Altersheime von Ransomware betroffen sind, kann das gravierende Folgen haben. Patientendaten können wie in diesem Fall verschlüsselt oder gestohlen werden, was Datenschutzverletzungen und Identitätsdiebstahl zur Folge hätte. Zudem kann ein digitaler Systemausfall die Versorgung gefährdet – etwa bei Medikamentenplänen oder Notfallkommunikation. Ein solcher Angriff kann Menschenleben gefährden und dessen Risiko müssen sich Sozialunternehmen bewusst sein.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6492-RansomHub-CBT.png

RIEDEL

Angriff auf Reha-Klinik: Patienten- und Mitarbeiterdaten gefährdet

4. September 2024, in Bad Wildungen/Hessen

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
In der Nacht des 27. August 2024 wurde eine Reha-Klinik Ziel eines Ransomware-Angriffs, bei dem einige Daten verschlüsselt und andere, vermutlich personenbezogene, gestohlen wurden. Die betroffenen Systeme wurden nach der Entdeckung des Vorfalls sofort offline genommen und gesichert. Die Klinik gab an, dass der Betrieb weitestgehend unbeeinträchtigt blieb. Zwei Monate später bekannte sich die Hackergruppe Helldown zu dem Angriff und veröffentlichte 117 GB gestohlene Daten, darunter Zugangsinformationen und E-Mail-Adressen.

Was hätte man besser machen können?
Um einen solchen Vorfall zu verhindern, wären strengere Sicherheitsvorkehrungen wie die Einführung von Zwei-Faktor-Authentifizierung und robusten Passwortrichtlinien erforderlich gewesen. Durch regelmäßige Sicherheitsanalysen und Systemüberprüfungen hätten potenzielle Schwachstellen frühzeitig erkannt und behoben werden können. Auch die Verschlüsselung sensibler Daten sowie eine klare Kontrolle des Zugriffs hätten unbefugten Zugriff erschwert.

Was lernen wir daraus:

Ein Sicherheitsvorfall tritt auf, wenn die Integrität eines Systems gefährdet wird. Solche Ereignisse können die Vertraulichkeit, Verfügbarkeit oder Integrität von Daten, Anwendungen oder IT-Diensten beeinträchtigen und erheblichen Schaden anrichten. Angreifer bleiben oft unentdeckt, während sie auf ihre Gelegenheit warten, aktiv zu werden. Im Schnitt vergehen rund 20 Tage zwischen dem Eindringen in ein System und dessen Entdeckung, was die Bedeutung einer kontinuierlichen Überwachung hervorhebt.

Anzunehmende Schadensfelder:

Quellen
https://www.hessenschau.de/panorama/hackerangriff-auf-klinik-am-kurpark-in-bad-wildungen-v1,hackerangriff-klinik-kur-reinhardshausen-100.html
https://www.hessenschau.de/panorama/hackerangriff-auf-klinik-am-kurpark-in-bad-wildungen-v1,hackerangriff-klinik-kur-reinhardshausen-100.html

RIEDEL

Daten gestohlen und Buchungssysteme lahmgelegt

3. September 2024, in Detmold/Nordrhein-Westfalen

RANSOMWARE

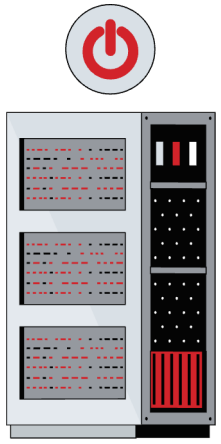
AUSFALL

DATENDIEBSTAHL

Was ist passiert?
Im September 2024 griff die Ransomwaregruppe Hunters International die Website eines bekannten Beherbergungsbetriebs an und forderte eine Lösegeldzahlung, mit der Drohung, die gestohlenen Daten zu veröffentlichen.

Bereits wenige Tage vor dem Angriff gab es Netzwerkprobleme, die möglicherweise auf denselben Angriff zurückzuführen sind, einschließlich der Unfähigkeit, Online-Buchungen vorzunehmen und Schlüsselkarten auszustellen.

Was hätte man besser machen können?
Um einen solchen Angriff zu verhindern, wären regelmäßige, sichere Backups und eine zuverlässige Datensicherungslösung notwendig gewesen. Zudem hätte der Einsatz von modernen Erkennungs- und Reaktionssystemen wie EDR und XDR Bedrohungen früher identifizieren und stoppen können. Nicht zu vernachlässigen sind außerdem Schulungen der Mitarbeiter zur Sensibilisierung für Phishing und andere Gefahren.



Anzunehmende Schadensfelder:

Quellen
https://www.swr.de/swraktuell/rheinland-pfalz/koblenz/jugendherbergen-durch-computerpanne-lahmgelegt-100.html
https://www.heise.de//news/Jugendherbergen-offenbar-Opfer-von-Ransomware-Bande-Hunters-9938226.html

Was lernen wir daraus:

Cyberkriminelle handeln oft aus finanziellen Interessen und nutzen das Internet für illegale Aktivitäten. Ihr Ziel ist in der Regel der Diebstahl von Daten, die entweder direkt verkauft oder für Erpressungsversuche verwendet werden können. Ein häufig angewandtes Verfahren ist der Einsatz von Ransomware, bei dem die betroffenen Daten verschlüsselt werden und die Opfer zur Zahlung eines Lösegeldes aufgefordert werden, um die Entschlüsselung zu erhalten.

RIEDEL

Gestohlene Kundendaten auf BreachForums angeboten

2. September 2024, in Leipzig/Sachsen

DATENLECK

Was ist passiert?
Seit dem 2. September 2024 ist auf BreachForums eine Datenbank mit angeblich gestohlenen Kundendaten eines Hockey-Ausrüsters erhältlich. Die Datensätze umfassen persönliche Informationen wie Namen, E-Mail-Adressen und gehashte Passwörter (MD5).

Was hätte man besser machen können?
Um den Vorfall zu verhindern, wären der Einsatz von SIEM für die zentrale Überwachung und Analyse von Sicherheitsereignissen sowie SOAR zur automatisierten Reaktion auf Bedrohungen für den Hockey-Ausrüsters entscheidend gewesen. Zudem hätten EDR und XDR zur Überwachung und umfassenden Analyse von Endpunkten und Netzwerken beigetragen.

Was lernen wir daraus:

BreachForums ist ein Online-Forum, das von Cyberkriminellen genutzt wird, um gestohlene Daten zu verkaufen und zu tauschen. Es hat sich als zentrale Anlaufstelle für Hacker etabliert, die auf illegale Weise auf persönliche Informationen zugreifen. Nach mehrfachen Angriffen und Polizeiaktionen bleibt das Forum ein aktiver Markt für gestohlene Daten. Trotz Versuchen, das Forum zu schließen, gelang es den Betreibern das Forum aufrecht zu erhalten.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6719-BHP-Hckeydirekt.png

RIEDEL

Cyberangriff auf Deutsche Flugsicherung: APT28 im Verdacht

1. September 2024, in Langen/Hessen

EINBRUCH

Was ist passiert?
Die IT-Infrastruktur der Deutschen Flugsicherung wurde Ziel eines Cyberangriffs, der den Bürokommunikationsbereich betraf. Die Sicherheitsbehörden wurden informiert, während Abwehrmaßnahmen ergriffen wurden, um die Auswirkungen zu begrenzen. Erste Hinweise deuteten auf eine Verbindung zu APT28 ("Fancy Bear") hin, einer mutmaßlich vom russischen Geheimdienst GRU unterstützten Hackergruppe. Erst kürzlich vor dem Angriff entdeckten zwei Experten eine Sicherheitslücke im Flugbetrieb, bei der sie sich durch eine SQL-Injection als Mitarbeiter ausgeben konnten, um Zugang zu sicherheitsrelevanten Bereichen zu erhalten.

Was hätte man besser machen können?
Um Schwachstellen – wie die kürzlich vor dem Angriff entdeckte SQL-Injection-Lücke – zu identifizieren, sind regelmäßige Penetrationstests durch Experten essenziell. Auch der Einsatz von Threat-Intelligence-Systemen und spezialisierter Endpoint Detection and Response (EDR)-Software hätte helfen können, Anomalien frühzeitig zu erkennen.

Anzunehmende Schadensfelder:

Quellen
https://www.heise.de//news/Cyberangriff-auf-Deutsche-Flugsicherung-steckt-APT28-dahinter-9853967.html
https://www.spiegel.de/netzwelt/web/deutsche-flugsicherung-wurde-ziel-von-hackerangriff-buerokommunikation-betroffen-a-34b98e09-f17a-4fe1-baaa-5c461df93ac6

Was lernen wir daraus:

Die Deutsche Flugsicherung (DFS) gilt als kritische Infrastruktur (KRITIS) und ist eine Schlüsselorganisation für die Sicherheit und Effizienz des Luftverkehrs in Deutschland. Dementsprechend fällt die DFS unter die NIS-2-RL. Ein Ausfall oder eine Störung ihrer Systeme könnte erhebliche Auswirkungen auf den Luftverkehr, die öffentliche Sicherheit und die Wirtschaft haben.

RIEDEL

IT-Ausfall in Kliniken: Eingeschränkter Betrieb und abgesagte OPs

1. September 2024, in Schwabmünchen/Bayern

AUSFALL

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
In den frühen Stunden am ersten September 2024 wurden in zwei deutschen Kliniken erhebliche IT-Störungen festgestellt. Untersuchungen zeigten, dass zentrale Datenzugriffe blockiert und virtuelle Server im Krankenhaus-Informationssystem verschlüsselt wurden. Sicherheitsbehörden und Polizei wurden informiert. Die Kliniken arbeiteten mit IT-Experten an einer Lösung und stellten den Betrieb auf ein eingeschränktes analoges System um.

Was hätte man besser machen können?
Um Vorfälle wie diesen in Kliniken zu vermeiden, wären regelmäßige Sicherheitschecks von Krankenhausinformationssystemen und medizinischen Geräten nötig gewesen. Ein getestetes Backup-System hätte die Wiederherstellung erleichtert, während Netzwerksegmentierung den Schaden begrenzt hätte. Zudem hätten Schulungen des Personals und ein Incident-Response-Plan die Reaktionszeit womöglich verbessert und kritische Prozesse geschützt.

Was lernen wir daraus:
Sicherheitsvorfälle in Gesundheitseinrichtungen gefährden die Sicherheit und Integrität von Patientendaten. Wichtige medizinische Informationen, die für eine angemessene Behandlung erforderlich sind, könnten kompromittiert werden. Solche Vorfälle stellen nicht nur ein Risiko für die betroffenen Patienten dar, sondern können auch schwerwiegende Auswirkungen auf die betroffenen Kliniken haben, einschließlich rechtlicher, finanzieller und reputationsbezogener Folgen.

Anzunehmende Schadensfelder:

Quellen
https://www.br.de/nachrichten/bayern/hackerangriff-auf-wertachkliniken-betrieb-massiv-eingeschraenkt,UNCpg7p
https://www.augsburger-allgemeine.de/schwabmuenchen/cyber-angriff-legt-wertachkliniken-lahm-operationen-abgesagt-103013013

RIEDEL

Chris Rock
Cyber Mercenary, CISO & Co-founder of SIEMonster

GASTARTIKEL

SIEMonster

SEEING THE GLITCH: A HACKER'S INTUITION

I like to refer to myself as a *glitch hacker*—someone who instinctively spots flaws in systems when a pattern breaks. I don't actively hunt for vulnerabilities; they reveal themselves to me. In a world governed by patterns, any deviation stands out like a glitch in the Matrix.

What do I mean by this?

Take the time I discovered a flaw in the Birth and Death Industry—where I found a way to electronically create and erase people from existence. I didn't wake up one day deciding to investigate this sector. Instead, a news report caught my attention: a hospital in Australia had accidentally issued death notices for 200 living patients due to a simple clerical error. That single incident led me down a three-year research path, where I interviewed doctors, funeral directors, sociologists, and government officials to explore the vulnerabilities in this system.

These glitches have repeated itself throughout my career. Another example: a documentary on mercenaries aired for just one day before being pulled from the network. That fleeting moment sparked my deep dive into the world of private military contractors, leading to my collaboration with Simon Mann, an ex-British SAS soldier turned mercenary coup leader active in Africa. Working with him shaped my understanding of how digital warfare could replace traditional military tactics. I later applied these concepts in Kuwait, where I orchestrated a digital coup, not with soldiers, but by compromising banks, telecoms, and industrial systems, using cyber tactics analogous to military strategies.

My most recent Defcon talk, *Terrorists Win*, emerged from a similar process. When Julian Assange was in the Ecuadorian embassy in London, his communications were heavily jammed. This single event sparked four years of research into defeating signal jamming. The breakthrough came when I noticed a pattern—jammers rarely operated below 20 MHz Why? What was special about that frequency? Physics provided the answer: effective jamming antennas at such low frequencies would need to be kilometres tall, making them impractical. Recognizing this gap, I found a way to use the Earth itself as an antenna, leveraging magnetic fields to communicate in the 3–9 kHz range—completely immune to traditional jammers.

I don't *seek out* system flaws; I recognize them when they appear. These glitches shape my career, guiding my research in unexpected directions.

The human brain is an extraordinary pattern-recognition machine. Over millennia, this ability ensured our survival, helping early humans distinguish predator from prey and recognize safe food sources. But a *hacker's brain* goes a step further—not only recognizing patterns but instinctively detecting when something *doesn't fit.* When a pattern breaks, when an anomaly appears, the hacker brain zeroes in, exposing flaws that others overlook.

This is why I call myself a glitch hacker. While others focus on what *should* work, I see breaks in process, when systems crack, where the illusion of order falters. In those moments, new possibilities emerge, waiting to be explored.

Chris Rock is a Cyber Mercenary who has worked in the Middle East, US and Asia for the last 30 years working for both government and private organizations. He is the Chief Information Security Officer and co-founder of SIEMonster.
Chris has presented three times at the largest hacking conference in the world, DEFCON in Las Vegas on controversial vulnerabilities including.

- How hackers could create fake people and kill them using vulnerabilities in the Birth and Death Registration systems around the world.
- How cyber mercenaries can overthrow a government working with coup mercenary Simon Mann.
- How cyber mercenaries can bypass modern day Jammers using the earth as an antenna to trigger and IED at 2kHz

Chris is also the author of the Baby Harvest, a book based on criminals and terrorists using virtual babies and fake deaths for financing. He has also been invited to speak at TED global. Chris Rock appeared in Darknet Diaries Episode 151.

RIEDEL

Chris Rock
Cyber Mercenary, CISO & Co-founder of SIEMonster

GASTARTIKEL

SIEMonster

DIE INTUITION EINES HACKERS: GLITCHES SEHEN UND NUTZEN

Ich bezeichne mich gerne als „Glitch-Hacker" – jemand, der instinktiv Fehler in Systemen erkennt, sobald ein Muster durchbrochen wird. Ich suche also nicht aktiv nach Schwachstellen; sie offenbaren sich mir. In einer Welt, die von Mustern bestimmt wird, sticht jede Abweichung hervor – wie ein Glitch in der Matrix.

Was meine ich damit?

Ein Beispiel: Ich entdeckte eine gravierende Schwachstelle in der Geburts- und Sterbeindustrie – eine Möglichkeit, Menschen elektronisch zu erschaffen oder deren Existenz zu löschen. Ich hatte nicht geplant, dieses System zu untersuchen, vielmehr war es ein Bericht in den Nachrichten, der meine Aufmerksamkeit weckte: Ein Krankenhaus in Australien hatte versehentlich 200 lebenden Patienten Totenscheine ausgestellt – aufgrund eines simplen Schreibfehlers. Was ich zu diesem Zeitpunkt noch nicht ahnte, war, dass mich dieser eine Sicherheitsvorfall für die nächsten drei Jahre beschäftigen würde. Denn für mich folgte eine dreijährige Forschung, bei der ich mit Ärzten, Bestattungsunternehmern, Soziologen und Regierungsvertretern sprach, um die Verwundbarkeit dieses Systems zu verstehen.

Solche Glitches begegneten mir immer wieder in meiner Laufbahn. Ein weiteres Beispiel: Eine Dokumentation über Söldner wurde nur einen Tag lang ausgestrahlt, bevor sie wieder aus dem Netz genommen wurde. Dieser kurze Moment reichte aus, um meine Neugier zu wecken und neue Recherchen aufzunehmen. Ich begann, mich intensiv mit privaten Militärfirmen zu befassen – eine Recherche, die schließlich zu einer Zusammenarbeit mit Simon Mann führte, einem ehemaligen britischen SAS-Soldaten, der als Söldner in Afrika aktiv war. Die Arbeit mit ihm zeigte mir, wie digitale Kriegsführung herkömmliche militärische Taktiken ersetzen könnte. Später wendete ich dieses Wissen in Kuwait an, wo ich einen digitalen Staatsstreich organisierte – nicht mit Soldaten, sondern durch das gezielte Kompromittieren von Banken, Telekommunikationsunternehmen und Industrieanlagen. Cyberangriffe als militärische Strategie.

Mein jüngster Vortrag auf der Defcon, Terrorists Win, entstand auf ähnliche Weise. Als Julian Assange in der ecuadorianischen Botschaft in London festsaß, wurden seine Kommunikationswege massiv gestört. Dieses Ereignis löste eine vierjährige Forschungsarbeit aus, in der ich Wege suchte, Signalstörungen zu umgehen. Der Durchbruch kam, als ich ein Muster erkannte: Störsender arbeiteten selten unterhalb von 20 MHz. Warum? Was machte diesen Frequenzbereich so besonders? Die Antwort lieferte die Physik: Effektive Störsender für so niedrige Frequenzen hätten kilometerhohe Antennen benötigt – schlichtweg unpraktisch. Diese Lücke nutzend, entwickelte ich eine Methode, das Erdmagnetfeld als natürliche Antenne zu verwenden und im 3–9 kHz-Bereich zu kommunizieren – vollkommen immun gegen herkömmliche Störsender.

Ich suche keine Systemfehler – ich erkenne sie, wenn sie auftreten. Diese Glitches prägen meine Laufbahn und steuern meine Forschungen in unvorhergesehene Richtungen.

Das menschliche Gehirn ist eine außergewöhnliche Mustererkennungsmaschine. Über Jahrtausende sicherte uns diese Fähigkeit das Überleben – half uns, Raubtiere von Beutetieren zu unterscheiden oder essbare von giftigen Pflanzen zu trennen. Doch das Gehirn eines Hackers geht noch einen Schritt weiter: Es erkennt nicht nur Muster, sondern spürt instinktiv auf, wenn etwas nicht passt. Sobald ein Muster bricht, eine Anomalie auftaucht, schaltet das Hacker-Gehirn auf höchste Wachsamkeit – und entlarvt Fehler, die anderen entgehen.

Deshalb nenne ich mich einen Glitch-Hacker. Während andere sich darauf konzentrieren, wie Dinge funktionieren sollen, sehe ich, wo Prozesse zusammenbrechen, wo Systeme rissig werden und die Illusion von Ordnung ins Wanken gerät. Genau in diesen Momenten entstehen neue Möglichkeiten – bereit, entdeckt zu werden.

Chris Rock ist ein Cyber-Söldner mit 30 Jahren Erfahrung im Nahen Osten, den USA und Asien. Er hat sowohl für Regierungen als auch für private Organisationen gearbeitet und ist Mitbegründer sowie Chief Information Security Officer (CISO) von SIEMonster. Er hat bereits dreimal auf der weltweit größten Hacking-Konferenz, DEFCON in Las Vegas, präsentiert und dabei kontroverse Sicherheitslücken aufgezeigt, darunter:

- Wie Hacker mithilfe von Schwachstellen in Geburts- und Sterberegistrierungssystemen weltweit künstliche Identitäten erschaffen und „töten" könnten.
- Wie Cyber-Söldner gemeinsam mit Putsch-Söldner Simon Mann eine Regierung stürzen können.
- Wie Cyber-Söldner moderne Störsender umgehen und mithilfe der Erde als Antenne eine Sprengladung bei 2 kHz auslösen können.

Chris Rock ist außerdem Autor des Buches Baby Harvest, das sich mit Kriminellen und Terroristen befasst, die virtuelle Babys und gefälschte Todesfälle zur Finanzierung nutzen. Er wurde zudem als Redner zu TED Global eingeladen und war in Episode 151 des Podcasts Darknet Diaries zu hören.

RIEDEL

AUGUST 2024

SECURITY INCIDENTS GERMANY

RIEDEL

Website einer Partei aufgrund eines massiven Cyberangriffs offline

29. August 2024, in Brandenburg

DDoS

AUSFALL

Was ist passiert?
Im August 2024 wurde die Website einer politischen Partei in Brandenburg Opfer eines Hackerangriffs, wodurch sie vorübergehend offline ging. Der Angriff äußerte sich durch eine Flut von gefälschten Anfragen, die die Seite zum Absturz brachten. Die Partei beschrieb den Angriff als professionell durchgeführt, mit erheblichen technischen und finanziellen Ressourcen. Dieser Vorfall erinnert an frühere Angriffe auf andere politische Parteien.

Was hätte man besser machen können?
Um sich besser gegen DDoS-Angriffe zu schützen, hätte die betroffene Partei spezielle DDoS-Schutzmaßnahmen implementieren und ihre Netzwerke durch Lastverteilung und Redundanz widerstandsfähiger gestalten können. Ein detaillierter Notfallplan zur schnellen Reaktion wären ebenfalls sinnvoll gewesen.

Was lernen wir daraus:

Hacktivismus ist ein Begriff, der sich aus "Hacking" und "Aktivismus" zusammensetzt. Er bezeichnet die Nutzung von Hacking-Techniken als Mittel des politischen oder sozialen Protests. Hacktivisten greifen oft auf DDoS-Angriffe, Datenklau oder die Veröffentlichung sensibler Informationen zurück, um auf Missstände aufmerksam zu machen oder gegen Regierungen und Unternehmen zu protestieren.

Anzunehmende Schadensfelder:

Quellen
https://www.rbb24.de/politik/beitrag/2024/08/brandenburg-politik-afd-beklagt-hackerangriff-webseite.html
https://www.berliner-zeitung.de/news/afd-brandenburg-beklagt-hackerangriff-auf-internetseite-li.2249266

RIEDEL

Cyberangriff auf Haushaltsgerätehersteller in Kempen

29. August 2024, in Kempen/Nordrhein-Westfalen

DATENPANNE

RANSOMWARE

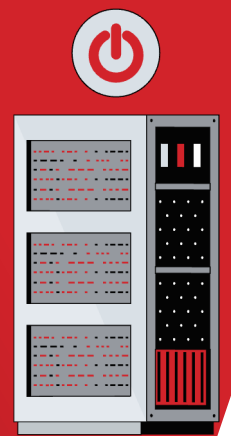
DATENDIEBSTAHL

DATENLECK

Was ist passiert?
Ende August 2024 führte die Ransomwaregruppe BlackSuit einen Angriff auf einen Hersteller von Haushaltsgeräten durch und veröffentlichte anschließend die erbeuteten Daten. Darunter sollen sich auch personenbezogene Informationen befinden, die ein erhöhtes Risiko für die Betroffenen darstellen, da diese für Identitätsdiebstahl, Phishing oder andere kriminelle Aktivitäten genutzt werden könnten.

Was hätte man besser machen können?
Um solche Vorfälle effektiver zu handhaben, wäre der Einsatz von XDR und EDR für eine verbesserte Erkennung und Reaktion auf Bedrohungen auf allen Endpunkten und Netzwerken sinnvoll gewesen. Auch die Einführung von SIEM-Systemen zur fortlaufenden Überwachung und Analyse von Sicherheitsereignissen hätte sich als nützlich erwiesen.

Anzunehmende Schadensfelder:



Was lernen wir daraus:

Die folgenden Strategien sind entscheidend, um Angriffe frühzeitig zu erkennen und abzuwehren, ohne Schaden zu verursachen:

•SIEM: Laufende Überwachung und Analyse von sicherheitsrelevanten Ereignissen.

•XDR & EDR: Erweiterte Erkennung und Reaktion auf Bedrohungen in allen Endpunkten und Netzwerken.
•Schwachstellenbewertungen: Regelmäßiges Aufspüren und Beheben von Sicherheitslücken.

•SOAR: Automatisierung und Abstimmung von Sicherheitsmaßnahmen.

•Proaktive Cybersicherheitsstrategie: Ein ganzheitlicher Ansatz zur Verbesserung der Sicherheitslage und Minimierung der Auswirkungen von Cyberangriffen.

RIEDEL

Quellen
https://www.security-incidents.de/assets/img/incidents/6417-Clatronic_International-BlackSuit.PNG

Angriff auf neu gegründete politische Partei

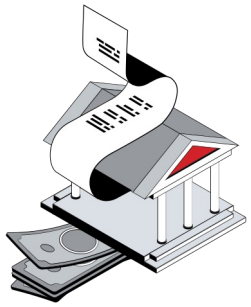
27. August 2024, in Berlin/Berlin

DATENLECK

Was ist passiert?
Eine neu gegründete politische Partei warnte Mitglieder über ein mögliches Datenleck in ihrer IT-Infrastruktur. Betroffen sind rund 70.000 Personen, die den Newsletter der Partei abonniert hatten. Nach eigenen Angaben wurde Strafanzeige gestellt und Datenschutzbehörden sowie Betroffene wurden informiert. Der Vorfall erhöht das Risiko für gezielte Angriffe auf die Privatsphäre politisch aktiver Personen.

Was hätte man besser machen können?
Sensible Daten wie Mitgliederlisten und Newsletter-Abonnentendaten sollten nur auf Servern gespeichert werden, die hohen Sicherheitsstandards entsprechen. Dazu gehört der Einsatz von Firewalls, Verschlüsselung und Zwei-Faktor-Authentifizierung.

Regelmäßige Penetrationstests und Vulnerability Assessments hätten Schwachstellen in der IT-Infrastruktur frühzeitig identifiziert, sodass sie hätten behoben werden können, bevor die Partei zum Opfer wurde.



Anzunehmende Schadensfelder:

Quellen
https://www.heise.de//news/Gezielter-Angriff-Datenleck-bei-Buendnis-Sahra-Wagenknecht-9849076.html
https://www.focus.de/politik/deutschland/70-000-personenbezogene-daten-erneutes-datenleck-beim-buendnis-sahra-wagenknecht_bfcbf067-8950-4a10-a96f-b7d5d7a2b705.html

Was lernen wir daraus:

Politische Organisationen verwalten oft Informationen, die durch die DSGVO besonders geschützt sind, etwa Angaben zu politischen Ansichten oder Unterstützern. Ein Datenleck birgt nicht nur rechtliche Konsequenzen, sondern auch ein enormes Risiko, dass Betroffene Ziel von Angriffen oder unerwünschter Kontaktaufnahme werden. Umso wichtiger ist eine robuste IT-Sicherheitsinfrastruktur, um solche Lecks zu verhindern.

RIEDEL

Datenleak bei Ingenieursunternehmen mit brisanten Informationen

26. August 2024, in Dormagen/Nordrhein-Westfalen

DATENPANNE

EINBRUCH

DATENDIEBSTAHL

DATENLECK

Was ist passiert?
Die Ransomwaregruppe RansomHub hat Ende August 2024 einen deutschen Ingenieursdienstleister als Opfer benannt. Die Angreifer behaupten, 10 GB sensibler Daten erbeutet zu haben und drohten mit der Veröffentlichung der Daten, sollten ihre Forderungen nicht erfüllt werden. Zu den geleakten Informationen zählen Verträge, Geheimhaltungsvereinbarungen und Bankdaten eines großen Automobilherstellers.

Was hätte man besser machen können?
Um den Ransomware-Angriff auf den Dienstleister effektiver zu verhindern oder zu bewältigen, hätte ein SOC entscheidend sein können.

Ein SOC hätte durch kontinuierliche Überwachung, fortschrittliche Bedrohungserkennung und automatisierte Reaktionen schnell auf ungewöhnliche Aktivitäten reagieren können. Auch hätte das SOC einen großen und wichtigen Teil zur Prävention des Angriffs beigetragen.

Was lernen wir daraus:

IT-Sicherheitsvorfälle können erhebliche Schäden an Geschäftsbeziehungen verursachen. Kunden und Partner verlieren Vertrauen, wenn sensible Daten kompromittiert oder Betriebsabläufe gestört werden. Dies führt häufig zu Vertragsstrafen, Verlust von Aufträgen und einem beschädigten Ruf. Langfristig kann dies auch die Wettbewerbsfähigkeit eines Unternehmens mindern und zu finanziellen Einbußen führen.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6372-Spie_Tec-Ransomhub.PNG

RIEDEL

Cyberangriff legt Netzwerk eines führenden Antriebsriemenherstellers lahm

26. August 2024, in Höxter/Nordrhein-Westfalen

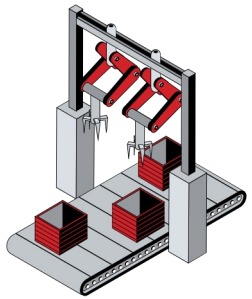
AUSFALL

Was ist passiert?
Am 25. August 2024 wurde ein führender Hersteller von Antriebsriemen Ziel eines Cyberangriffs. Das interne Netzwerk fiel aus, ebenso die telefonische Kommunikation. Mitarbeitende wurden in den Überstundenabbau geschickt, während die Leitung nur mobil erreichbar war. Zudem musste die Eröffnung eines neuen Logistikzentrums verschoben werden.

Was hätte man besser machen können?
Um solche Angriffe zu verhindern, wäre die Implementierung von SIEM und EDR wichtig gewesen. SIEM hätte durch kontinuierliche Überwachung und Analyse von Sicherheitsdaten frühzeitig Anomalien erkannt, während EDR verdächtige Aktivitäten auf Endgeräten schnell identifiziert und neutralisiert hätte.

Was lernen wir daraus:

Der Vorfall zeigt, wie stark Unternehmen von einer funktionierenden IT-Infrastruktur abhängig sind und welche weitreichenden Folgen Cyberangriffe haben können. Neben finanziellen Schäden entstehen operative Einschränkungen, die Produktion und Geschäftsabläufe massiv beeinträchtigen. Zudem wird deutlich, wie wichtig schnelle Entscheidungsfähigkeit und klare Kommunikationswege in Krisensituationen sind.



Anzunehmende Schadensfelder:

Quellen
https://www.radiohochstift.de/nachrichten/paderborn-hoexter/detailansicht/cyber-angriff-auf-arntz-optibelt-in-hoexter.html
https://www.westfalen-blatt.de/owl/kreis-hoexter/hoexter/hacker-angriff-optibelt-ausmass-schaeden-polizei-ermittlungen-3113923?pid=true

RIEDEL

Datenexfiltration durch Helldown bei deutschen Immobilienanbieter

21. August 2024, in Weißenfels/Sachsen-Anhalt

EINBRUCH

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Am 21. August 2024 wurde ein deutscher Immobilienanbieter Ziel eines Angriffs der Ransomwaregruppe „Helldown". Am folgenden Tag stellte die Gruppe das Unternehmen auf ihrer Opferliste im Darknet und behauptete, vertrauliche Daten exfiltriert zu haben. Der genaue Umfang der gestohlenen Daten ist nicht bekannt und das betroffene Unternehmen hat sich nicht öffentlich zu dem Vorfall geäußert.

Was hätte man besser machen können?
Der Angriff hätte durch eine frühzeitige Identifizierung, rasche Gegenmaßnahmen und ein effizientes Incident-Response-Management besser eingedämmt werden können.

Zusätzlich hätten regelmäßige Sicherheitsüberprüfungen sowie eine robuste Backup-Strategie dazu beigetragen, den Schaden zu begrenzen und eine schnelle Wiederherstellung zu ermöglichen.

Was lernen wir daraus:

Helldown nutzt maßgeschneiderte Schadsoftware wie „hellenc.exe“ und Schwachstellen in Netzwerkgeräten wie Zyxel-Firewalls. Ihre Angriffe umfassen Datenverschlüsselung, das Löschen von Spuren und die Verbreitung über interne Netzwerke. Ihre Techniken erschweren forensische Analysen und erfordern strenge Sicherheitsmaßnahmen.

Anzunehmende Schadensfelder:

Quellen
https://ransomfeed.it/index.php?page=post_details&id_post=16983
https://www.security-incidents.de/assets/img/incidents/6323-helldown-rsk.png

RIEDEL

Sensible Mitarbeiterdaten von Ransomwaregruppe veröffentlicht

19. August 2024, in Wandlitz/Brandenburg

DATENLECK

RANSOMWARE

EINBRUCH

DATENDIEBSTAHL

Was ist passiert?
Die Cloak-Gruppe erklärte am 19. August 2024 eine Ingenieursgesellschaft zur Zielscheibe einer Ransomware-Attacke. Laut eigener Aussage erbeuteten die Angreifer 136 GB sensibler Daten – darunter Ausweisdokumente, Bewerbungen und Krankmeldungen von Mitarbeitenden. Nach verweigerter Lösegeldzahlung wurden die gestohlenen Informationen veröffentlicht, wodurch Betroffene erhöhtem Risiko von Identitätsdiebstahl und Missbrauch ausgesetzt wurden.

Was hätte man besser machen können?
Ein SIEM-System hätte den Ransomware-Angriff frühzeitig identifizieren und durch automatisierte Maßnahmen begrenzen können. Echtzeitüberwachung und schnellen Reaktionsmöglichkeiten ermöglichen es, Bedrohungen effektiv abzuwehren und forensisch zu analysieren. Darüber hinaus stärkt es die Sicherheitsarchitektur langfristig, indem es detaillierte Berichte und Audits bereitstellt, die dazu beitragen, zukünftige Angriffe zu verhindern.

Was lernen wir daraus:

Die Verarbeitung sensibler Daten wie Ausweisdokumenten und Krankmeldungen verlangt höchste Sicherheitsstandards, da Missbrauch zu Identitätsdiebstahl oder Erpressung führen kann. Regelmäßige IT-Audits, Zugriffsbeschränkungen, Datenverschlüsselung und Echtzeit-Monitoring sind unerlässlich bei der Verwaltung solcher Daten.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6324-Hvb_Ingenieure-Cloak.PNG

RIEDEL

Ransomwaregruppe Dragonforce droht Ingenieurbüro mit Datenveröffentlichung

18. August 2024, in Schönkirchen/Schleswig-Holstein

EINBRUCH

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Am 18. August 2024 meldete die Ransomwaregruppe Dragonforce einen Angriff auf ein Ingenieurbüro und behauptete, 544,75 GB an Daten entwendet zu haben. Der genaue Inhalt der gestohlenen Daten bleibt unklar. Die Täter forderten ein nicht näher beziffertes Lösegeld und drohten, die Daten andernfalls offenzulegen. Das betroffene Unternehmen hat keine weiteren Details zum Vorfall veröffentlicht.

Was hätte man besser machen können?
Next-Generation Firewalls und eine starke VPN-Nutzung hätten das Risiko eines Angriffs verringert. Eine regelmäßige Überprüfung der Sicherheitsinfrastruktur und das Implementieren eines Backup-Systems hätten zusätzlich dazu beigetragen, den drohenden Datenverlust zu verhindern.

Was lernen wir daraus:

Hacker agieren mit unterschiedlichen Zielen, die von der gezielten Informationsbeschaffung bis hin zu finanziellen Interessen reichen. Sie können Daten sammeln, um diese für spezifische Zwecke zu nutzen, Lösegeld durch Ransomware-Angriffe fordern oder gestohlene Informationen im Darknet gewinnbringend verkaufen. Ihre Motivation variiert je nach Strategie und reicht von wirtschaftlichem Profit bis hin zu gezielten Cyber-Spionageaktivitäten.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6295-Dragonforce-SMK.png

RIEDEL

Vertrauliche Daten von Ingenieurbüro veröffentlicht

13. August 2024, in Osnabrück/Niedersachsen

DATENLECK

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Am 13. August 2024 listete die Ransomwaregruppe Helldown ihre ersten Opfer im Darknet, darunter ein deutsches Ingenieurbüro. Die Angreifer veröffentlichten laut eigenen Angaben 53 GB sensibler Unternehmensdaten. Einsehbare Dateien beinhalteten unter anderem Rechnungen, Kontoauszüge und Informationen zu Firmenwagen.

Was hätte man besser machen können?
Der Vorfall hätte effektiver bewältigt werden können, wenn sowohl ein SIEM- als auch ein SOAR-System im Einsatz gewesen wären. Ein SIEM hätte durch die Erfassung und Auswertung von Sicherheitsdaten geholfen, den Angriff frühzeitig zu identifizieren. Ein SOAR-System hätte automatisierte Gegenmaßnahmen eingeleitet und eine koordinierte Reaktion ermöglicht.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6257-Schlattner-Helldown.png

Was lernen wir daraus:

Der Vorfall zeigt, wie wichtig es ist, strikte Sicherheitsmaßnahmen zum Schutz sensibler Unternehmensdaten zu implementieren. Daten wie Rechnungen, Kontoauszüge oder interne Vereinbarungen sind attraktiv für Angreifer und können bei Veröffentlichung schwerwiegende wirtschaftliche und rechtliche Folgen haben. Regelmäßige Sicherheitsprüfungen, Verschlüsselung und Zugangskontrollen sind essenziell, um Angriffe zu verhindern oder deren Auswirkungen zu minimieren.

RIEDEL

Datendiebstahl und Erpressung bei Metallbauunternehmen im Schwarzwald

6. August 2024, in Schonach im Schwarzwald/Baden-Württemberg

DATENLECK

EINBRUCH

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Ein deutsches Metallbauunternehmen das komplexe Präzisionsteile und Baugruppen herstellt, wurde am 6. August 2024 Ziel eines Angriffs der Ransomwaregruppe Mydata/Alphalocker. Die Täter behaupten, 100 GB sensibler Daten gestohlen zu haben und drohen, diese zu veröffentlichen, falls ihre Forderungen nicht erfüllt werden. Das betroffene Unternehmen hat keine Stellungnahme zum Sicherheitsvorfall abgegeben.

Was hätte man besser machen können?
Um den Schaden eines Cyberangriffs zu begrenzen, wären stärkere Sicherheitsmaßnahmen und ein gezielter Notfallplan hilfreich gewesen. Eine regelmäßige Sicherung der Daten hätte im Fall eines Angriffs die schnelle Wiederherstellung ermöglicht. Zudem hätte eine proaktive Überwachung der IT-Infrastruktur Risiken frühzeitig erkannt und rechtzeitig Gegenmaßnahmen ausgelöst.

Was lernen wir daraus:

Cyberkriminelle handeln häufig aus finanziellen Gründen und nutzen das Internet, um illegale Aktivitäten auszuführen. Ihr Hauptziel ist es, wertvolle Daten zu stehlen, die entweder direkt zu Geld gemacht oder für Erpressungszwecke verwendet werden können. Ein häufig angewandtes Vorgehen ist der Einsatz von Ransomware, bei dem wichtige Daten verschlüsselt werden und das Opfer zur Zahlung eines Lösegelds aufgefordert wird, um die Daten wieder freizugeben.

Anzunehmende Schadensfelder:

Quellen
https://x.com/FalconFeedsio/status/1820925876332105994
https://ransomfeed.it/index.php?page=post_details&id_post=16729

RIEDEL

Cactus-Gruppe erbeutet sensible Daten bei Medizingerätehersteller

5. August 2024, in Frankenthal/Rheinland-Pfalz

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Am 5. August 2024 wurde ein deutsches Unternehmen, das medizinische Geräte herstellt, Opfer eines Cyberangriffs durch die Ransomwaregruppe Cactus. Die Täter gaben an, 251 GB an sensiblen Daten gestohlen zu haben, einschließlich personenbezogener Informationen, Firmendaten, Kunden- und Finanzdokumenten sowie privater Daten von Mitarbeitenden und Führungskräften.

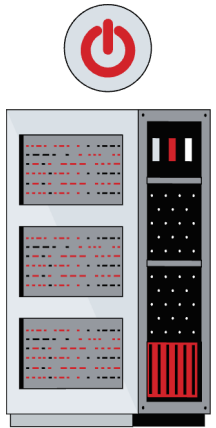
Was hätte man besser machen können?
Das Unternehmen hätte den Angriff voraussichtlich früher entdeckt, wenn es ein Managed-SIEM und ein rund um die Uhr besetztes Security Operations Center (SOC) eingesetzt hätte. Mit einer schnelleren Reaktion hätte man den Diebstahl sämtlicher sensibler Unternehmensdaten womöglich verhindern können.

Was lernen wir daraus:

Der Einsatz moderner IT-Sicherheitslösungen wie

- **SIEM & SOC**
- **XDR**
- **EDR**
- **SOAR**
- **Next Generation Firewalls**
- **SASE**

schützt Unternehmen nicht nur vor Datenverlusten, sondern trägt auch zur Einhaltung gesetzlicher Vorgaben bei und erhöht somit das gesamte Sicherheitsniveau.



Anzunehmende Schadensfelder:

Quellen
https://x.com/FalconFeedsio/status/1820372200035348876
https://ransomfeed.it/index.php?page=post_details&id_post=16710

RIEDEL

Ransomware-Angriff auf Solaranbieter: Behörden und Betroffene alarmiert

2. August 2024, in Bitterfeld-Wolfen/Sachsen-Anhalt

EINBRUCH

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?

Am 2. August wurde ein Strom- und Solaranbieter von der Ransomwaregruppe Abyss angegriffen. Die Täter stahlen 5,4 Terabyte an sensiblen Daten, darunter Namen, Adressen, Passwörter und Kontodaten von Kunden und Geschäftspartnern. Anschließend drohten sie mit der Veröffentlichung der Daten. Das Unternehmen informierte die Betroffenen und hat dazu geraten, Passwörter zu ändern, um Phishing und Credential-Stuffing zu verhindern. Auch die Behörden wurden eingeschaltet.

Was hätte man besser machen können?

Um solche Angriffe zu verhindern, wäre eine zentrale SIEM-Überwachung hilfreich gewesen. Zudem hätten regelmäßige Schwachstellenscans und ein optimiertes Asset-Management zur Risikominimierung beigetragen. Eine strengere Netzwerksegmentierung hätte die Verbreitung des Angriffs eingeschränkt. Ein SOC hätte diese Sicherheitsmaßnahmen gebündelt, koordiniert und den Angriff frühzeitig identifizieren können.

Was lernen wir daraus:

- Mehrfaktorauthentifizierung (MFA) ist essenziell, um unbefugten Zugriff durch gestohlene Passwörter zu verhindern.
- Zentrale und kontinuierliche Überwachung ermöglicht die frühzeitige Erkennung verdächtiger Aktivitäten und potenzieller Bedrohungen.
- Regelmäßige Updates und effektives Asset-Management sind entscheidend, um Sicherheitslücken zu schließen und Systeme stets auf dem neuesten Stand zu halten.
- Netzwerksegmentierung kann helfen, die Ausbreitung eines Angriffs innerhalb der IT-Infrastruktur einzudämmen.
- Ein etabliertes Security Operations Center (SOC) sorgt für eine koordinierte Sicherheitsstrategie und verbessert die Reaktionsfähigkeit auf Cyberangriffe.

Anzunehmende Schadensfelder:

Quellen

https://www.heise.de//news/Nach-Cyberangriff-Solaranbieter-Qcells-informiert-Kunden-ueber-Datenleck-9852641.html

https://ransomfeed.it/index.php?page=post_details&id_post=16683

RIEDEL

Chris Rock
Cyber Mercenary, CISO & Co-founder of SIEMonster

GASTARTIKEL

SIEMonster

SECURITY RESEARCHER: IT'S TIME TO MATURE OUR RESEARCH AND LOOK AT THE BIGGER PICTURE

The role of the security researcher is evolving, but our industry still has a long way to go. Many researchers lack rigorous scientific methodologies and academic backgrounds to produce verifiable results. Instead, some prioritize headlines and notoriety over genuine research. This isn't entirely their fault. The industry often celebrates unconventional paths, valuing experience over formal education and embracing short-term coding boot camps.

Security research is frequently leveraged for corporate publicity, with full-time researchers focusing on isolated technologies such as Bluetooth, firewalls, and operating system vulnerabilities. The pursuit of sensational headlines "*Billions of devices at risk*!" without solid methodologies does more harm than good. A recent example is the ESP32 Bluetooth vulnerability announcement in March, where the company Tarlogic claimed a backdoor in Espressif's ESP32 MCU affected a billion Bluetooth devices. The media, including *Forbes*, quickly spread fear, uncertainty, and doubt (FUD), only for it to later be clarified as a routine manufacturer firmware update, like those from Texas Instruments and Broadcom. This kind of misinformation risks creating a "cry wolf" scenario, where legitimate vulnerabilities may be dismissed or overlooked.

As more security researchers document and present findings, we must elevate our standards beyond those of our predecessors. If we are to call ourselves researchers, we should follow the practices of established fields such as science and medicine.

This means referencing academic papers, government studies, and expert publications to support our work. We must move away from the quick reward "bug bounty" culture, which prioritizes finding vulnerabilities over fully understanding and documenting them. Research should not stop at exposing a flaw—it must include an analysis of why the flaw exists, short-term fixes, and long-term strategies to prevent recurrence

Collaboration is essential. Research should be thoroughly reviewed, challenged, and refined with additional evidence, fostering a supportive environment where findings are either validated or corrected. We must also move beyond publishing research through Twitter with vague claims like "I hacked an airplane's entertainment system." This damages our credibility. Without comprehensive documentation and peer-reviewed analysis, we risk losing respect from researchers within and outside our field.

Security research should be a living discipline, evolving as new information emerges. If my research is flawed, it should be challenged, updated, and improved—contributing to a body of work that continually refines our understanding and enhances incident alerting heuristics. It's time to mature our approach and ensure that security research maintains the credibility it deserves.

Chris Rock is a Cyber Mercenary who has worked in the Middle East, US and Asia for the last 30 years working for both government and private organizations. He is the Chief Information Security Officer and co-founder of SIEMonster.
Chris has presented three times at the largest hacking conference in the world, DEFCON in Las Vegas on controversial vulnerabilities including.

- How hackers could create fake people and kill them using vulnerabilities in the Birth and Death Registration systems around the world.
- How cyber mercenaries can overthrow a government working with coup mercenary Simon Mann.
- How cyber mercenaries can bypass modern day Jammers using the earth as an antenna to trigger and IED at 2kHz

Chris is also the author of the Baby Harvest, a book based on criminals and terrorists using virtual babies and fake deaths for financing. He has also been invited to speak at TED global. Chris Rock appeared in Darknet Diaries Episode 151.

RIEDEL

Chris Rock
Cyber Mercenary, CISO & Co-founder of SIEMonster

GASTARTIKEL

SIEMonster

SICHERHEITSFORSCHUNG: ZEIT FÜR MEHR REIFE UND DEN BLICK AUFS GROßE GANZE

Die Rolle des Sicherheitsforschers entwickelt sich weiter – doch unsere Branche hat noch einen langen Weg vor sich. Viele Forscher verfügen nicht über eine fundierte wissenschaftliche Methodik oder akademische Ausbildung, um belegbare Ergebnisse zu liefern. Stattdessen stehen oft Schlagzeilen und Aufmerksamkeit im Vordergrund, anstatt echte Forschung. Dies ist nicht allein ihre Schuld. Die Branche selbst fördert unkonventionelle Werdegänge, setzt mehr auf Erfahrung als auf formale Bildung und begrüßt kurzfristige Coding-Bootcamps als Qualifikation.

Sicherheitsforschung wird häufig für PR-Zwecke genutzt, wobei sich viele Vollzeitforscher auf isolierte Technologien wie Bluetooth, Firewalls oder Betriebssystem-Schwachstellen konzentrieren. Die Jagd nach reißerischen Schlagzeilen à la „Milliarden von Geräten in Gefahr!“ ohne fundierte Methodik schadet mehr, als sie nützt. Ein aktuelles Beispiel ist die im März gemeldete ESP32-Bluetooth-Sicherheitslücke: Das Unternehmen Tarlogic behauptete, eine Backdoor in Espressifs ESP32-MCU gefährde eine Milliarde Bluetooth-Geräte. Medien wie Forbes verbreiteten die Meldung schnell und schürten Angst, Unsicherheit und Zweifel (FUD) – nur um später klarzustellen, dass es sich lediglich um ein routinemäßiges Firmware-Update handelte, wie es auch bei Texas Instruments oder Broadcom üblich ist. Solche Fehlinformationen führen zu einer „Cry Wolf“-Situation, in der ernsthafte Schwachstellen möglicherweise ignoriert oder unterschätzt werden.

Da immer mehr Sicherheitsforscher ihre Erkenntnisse dokumentieren und veröffentlichen, müssen wir unsere Standards über die unserer Vorgänger hinausheben.

Wenn wir uns als Forscher bezeichnen, sollten wir auch den etablierten Wissenschafts- und Medizinbereichen folgen: Das bedeutet, akademische Arbeiten, Regierungsstudien und Fachpublikationen als Grundlage für unsere Forschung heranziehen. Wir müssen uns von der schnellen Bug-Bounty-Mentalität lösen, die das bloße Finden von Sicherheitslücken über deren tiefgehende Analyse stellt. Forschung darf nicht bei der Entdeckung eines Fehlers enden – sie muss auch untersuchen, warum die Schwachstelle existiert, welche kurzfristigen Lösungen es gibt und wie sich solche Fehler langfristig vermeiden lassen.

Zusammenarbeit ist essenziell. Forschung sollte sorgfältig geprüft, infrage gestellt und mit weiteren Beweisen untermauert werden. Eine offene und unterstützende Umgebung ermöglicht es, Ergebnisse entweder zu bestätigen oder zu korrigieren. Zudem müssen wir über vage Twitter-Behauptungen wie „Ich habe das Entertainment-System eines Flugzeugs gehackt“ hinausgehen. Solche Aussagen – ohne umfassende Dokumentation und wissenschaftliche Überprüfung – schaden unserer Glaubwürdigkeit und wir verlieren den Respekt von Experten innerhalb und außerhalb unseres Fachgebiets.

Sicherheitsforschung sollte ein lebendiges, sich stetig weiterentwickelndes Feld sein. Wenn meine Forschung fehlerhaft ist, sollte sie hinterfragt, überarbeitet und verbessert werden, sodass sie zu einer fortlaufenden Arbeit beiträgt, die unser Verständnis schärft und die Heuristiken zur Erkennung von Vorfällen optimiert. Es ist an der Zeit, unseren Ansatz zu professionalisieren und sicherzustellen, dass die Sicherheitsforschung die Glaubwürdigkeit erhält, die sie verdient.

Chris Rock ist ein Cyber-Söldner mit 30 Jahren Erfahrung im Nahen Osten, den USA und Asien. Er hat sowohl für Regierungen als auch für private Organisationen gearbeitet und ist Mitbegründer sowie Chief Information Security Officer (CISO) von SIEMonster. Er hat bereits dreimal auf der weltweit größten Hacking-Konferenz, DEFCON in Las Vegas, präsentiert und dabei kontroverse Sicherheitslücken aufgezeigt, darunter:

- Wie Hacker mithilfe von Schwachstellen in Geburts- und Sterberegistrierungssystemen weltweit künstliche Identitäten erschaffen und „töten“ könnten.
- Wie Cyber-Söldner gemeinsam mit Putsch-Söldner Simon Mann eine Regierung stürzen können.
- Wie Cyber-Söldner moderne Störsender umgehen und mithilfe der Erde als Antenne eine Sprengladung bei 2 kHz auslösen können.

Chris Rock ist außerdem Autor des Buches Baby Harvest, das sich mit Kriminellen und Terroristen befasst, die virtuelle Babys und gefälschte Todesfälle zur Finanzierung nutzen. Er wurde zudem als Redner zu TED Global eingeladen und war in Episode 151 des Podcasts Darknet Diaries zu hören.

RIEDEL

JULI 2024

SECURITY INCIDENTS GERMANY

RIEDEL

Datendiebstahl bei MZV für Laboratoriumsmedizin und Mikrobiologie

30. Juli 2024, in Koblenz/Rheinland-Pfalz

EINBRUCH

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Am 29. Juli 2024 tauchte auf der Darknet-Plattform von RansomHub ein medizinisches Versorgungszentrum für Laboratoriumsmedizin und Mikrobiologie aus Rheinland-Pfalz auf. Laut Angaben der Angreifer wurde das MVZ Opfer eines Cyberangriffs, bei dem insgesamt 304 GB sensible Daten gestohlen wurden.

Was hätte man besser machen können?
Um den Ransomwareangriff abzuwehren, hätte ein SOC mit einem SIEM und einer Endpunkterkennungslösung frühzeitig Bedrohungen erkennen können.

Eine gründliche Schwachstellenbewertung und der Einsatz einer erweiterten Erkennungslösung hätten Sicherheitslücken geschlossen. Automatisierte Sicherheitsprozesse hätten die Reaktionszeiten optimiert, und regelmäßige Datensicherungen hätten eine schnelle Wiederherstellung ermöglicht.

Was lernen wir daraus:

Wenn Angreifer unerkannt in ein Netzwerk eindringen, versuchen sie, den Zugriff unbemerkt zu erhalten. Dafür setzen sie oft einen Command-and-Control-Server ein und installieren Malware.

Ihr Hauptziel ist es, an ein leistungsstarkes Benutzerkonto zu gelangen – meist einen Administrator-Account. Damit sichern sie sich umfassende Rechte und können sich im Netzwerk unbemerkt bewegen und weiter vordringen

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6105-RansomHub-MVZ-Labor-Koblenz.png

RIEDEL

Medusa-Ransomware erpresst Beratungsunternehmen

29. Juli 2024, in Falkensee/Brandenburg

RANSOMWARE

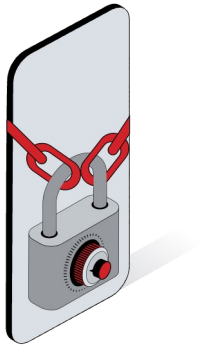
DATENDIEBSTAHL

Was ist passiert?
Am 29. Juli 2024 wurde ein deutsches Beratungsunternehmen von der Medusa-Ransomwaregruppe als Angriffsziel aufgeführt. Die Gruppe behauptet, 218,4 GB Daten entwendet zu haben, und fordert ein Lösegeld von 100.000 USD. Sie setzten eine Frist bis zum 5. August 2024, nach deren Ablauf die Daten veröffentlicht werden sollten, insofern die Zahlung ausgeblieben ist.

Was hätte man besser machen können?
Das Unternehmen hätte seine Cybersicherheitsstrategie optimieren können, indem es auf präventive Maßnahmen wie frotschrittliche Überwachung und regelmäßige Penetrationstests setzt. Auch kontinuierliche Schulungen für die Mitarbeitenden könnten die Verteidigung gegen zukünftige Angriffe verbessern.

Was lernen wir daraus:

Um die IT-Infrastruktur wirksam zu sichern, ist eine enge Zusammenarbeit zwischen IT-Teams und der Unternehmensführung entscheidend. Regelmäßiger Austausch und eine umfassende Sicherheitsstrategie, die alle Abteilungen einbezieht, ermöglichen dem Unternehmen, eine robuste Verteidigung aufzubauen und sich gezielt gegen Cyberbedrohungen zu schützen.



Anzunehmende Schadensfelder:

Quellen
https://ransomfeed.it/index.php?page=post_details&id_post=16597
https://www.security-incidents.de/assets/img/incidents/6098-gentlemen-group-medusa.png

RIEDEL

Cyberangriff auf Wirtschaftsprüfer

RANSOMWARE

DATENDIEBSTAHL

25. Juli 2024, in Witten/Nordrhein-Westfalen

Was ist passiert?
Am 25. Juli 2024 gab die Space Bears-Ransomwaregruppe bekannt, einen deutschen Wirtschaftsprüfer als Ziel ihres Angriffs ausgewählt zu haben. Sie setzten eine Frist bis zum 31. Juli 2024, nach deren Ablauf sie drohten, die gestohlenen, nicht näher spezifizierten Daten zu veröffentlichen, falls das geforderte Lösegeld nicht gezahlt wird.

Was hätte man besser machen können?
Gerade für kleine Unternehmen, die möglicherweise nicht über die nötigen Ressourcen oder Fachkenntnisse im Bereich IT-Sicherheit verfügen, ist es entscheidend, Fachleute hinzuzuziehen. Experten können eine umfassende Sicherheitslösung entwickeln, die präventive Schutzmaßnahmen gegen Ransomware umfasst, um das Risiko eines erfolgreichen Angriffs zu minimieren.

Was lernen wir daraus:

Hacker verfolgen verschiedene Ziele: Sie können an bestimmten Daten für gezielte Zwecke interessiert sein, schnelle finanzielle Gewinne durch Lösegeldforderungen anstreben oder durch den Verkauf der gestohlenen Daten im Darknet Einnahmen erzielen wollen.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6081-stienemann-space-bears.png
https://x.com/FalconFeedsio/status/1816337943482581269

RIEDEL

Blockchain-Identitätsplattform beraubt

17. Juli 2024, in Berlin/Berlin

DATENDIEBSTAHL

EINBRUCH

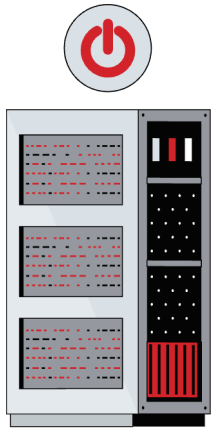
BLOCKCHAIN

Was ist passiert?
Am 14. Juli 2024 wurde eine Blockchain-ID Plattform von unbekannten Tätern angegriffen. Sie gelangten in ein Betreiberkonto und stahlen persönliche Daten von rund 50.000 Nutzern, was etwa 0,5 % der Gesamtzahl ausmacht. Erbeutet wurden Namen, E-Mail-Adressen, Wallet-Adressen und hochgeladene Dokumente. Der Angriff wurde nach zwei Stunden entdeckt und gestoppt.

Was hätte man besser machen können?
Um solche Angriffe zu verhindern, wäre eine zentrale SIEM-Überwachung hilfreich gewesen. Zudem wären regelmäßige Schwachstellenanalysen und ein effektiveres Asset-Management notwendig gewesen. Ein Security Operations Center (SOC) hätte diese Maßnahmen koordiniert und den Angriff frühzeitig identifizieren können.

Was lernen wir daraus:

Prävention und die Einführung geeigneter Protokolle sind entscheidend, um sich sowohl vorbeugend als auch im Falle eines Angriffs zu schützen. Ein spezialisiertes Security Operations Center (SOC) übernimmt dabei eine Schlüsselrolle. Es fungiert nicht nur als präventive Maßnahme, sondern kann auch zusätzliche Sicherheitslösungen und Protokolle implementieren, um den umfassenden Schutz einer Organisation sicherzustellen.



Anzunehmende Schadensfelder:

Quellen
https://cointelegraph.com/news/blockchain-identity-platform-fractal-id-suffers-data-breach
https://thecyberexpress.com/fractal-id-data-breach-confirmed/
https://www.hypersign.id/blogs/tpost/5x1z71zpk1-data-breach-hits-blockchain-identity-pla

RIEDEL

Cyberangriff auf Entsorgungs- und Recyclingbetrieb: Daten kompromittiert

16. Juli 2024, in Achern/Baden-Württemberg

DATENDIEBSTAHL

EINBRUCH

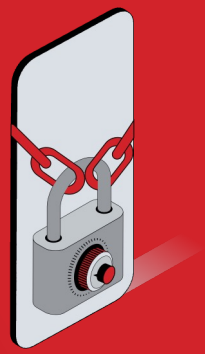
Was ist passiert?
Ein mehrtätiger Cyberangriff hat am 13. Juli ein mittelständisches Unternehmen aus dem Bereich Entsorgung und Recycling getroffen, bei dem einige Firmendaten kompromittiert wurden. Das Unternehmen erhielt rechtzeitig einen Hinweis, der ein schnelles Handeln ermöglichte. Obwohl der genaue Angriffstyp nicht genannt wird, deutet der Datenverlust auf Ransomware hin. Das Unternehmen ist jedoch zuversichtlich, die verlorenen Daten aus Backups wiederherstellen zu können.

Was hätte man besser machen können?
Um einen solchen Cyberangriff zu vermeiden, hätten strengere Zugangskontrollen für VPN-Verbindungen, einschließlich der Nutzung von Multi-Faktor-Authentifizierung (MFA), implementiert werden sollen, um unbefugten Zugriff zu erschweren. Zudem hätte der Einsatz von XDR geholfen, den Angriff frühzeitiger zu erkennen und abzuwehren.

Was lernen wir daraus:

Unternehmen, die unter die NIS2-Richtlinie fallen – womöglich auch dieser Entsorgungsbetrieb – sind im Falle eines Cyberangriffs nicht nur den direkten Auswirkungen des Vorfalls ausgesetzt, sondern riskieren auch erhebliche Strafen, wenn sie keine NIS2-konformen Sicherheitsmaßnahmen in ihrer IT-Infrastruktur implementiert haben.

Anzunehmende Schadensfelder:



Quellen
https://www.bo.de/lokales/achern-oberkirch/cyberangriff-bei-der-firma-merb-in-achern

RIEDEL

Kryptobörse erleidet Millionenverlust durch Sicherheitslücke

16. Juli 2024, in Berlin/Berlin

DATENLECK

SICHERHEITSLÜCKE

Was ist passiert?
Eine in Deutschland ansässige, Kryptobörse wurde am 16. Juli 2024 Ziel eines Cyberangriffs, bei dem Angreifer rund 11,6 Millionen USD erbeuteten. Die Täter nutzten dabei eine Sicherheitslücke aus, die durch eine kürzlich eingeführte Funktion entstanden war. Drei Tage später war die Schwachstelle behoben, und die kritische Lücke ließ sich nicht mehr ausnutzen.

Was hätte man besser machen können?
Um die Auswirkungen der Sicherheitslücke zu mindern, wären gründliche Sicherheitsüberprüfungen der neuen Funktion und strengere Zugangskontrollen hilfreich gewesen. Auch ein Incident-Response-Plan sowie der Einsatz eines SIEM-Systems zur frühzeitigen Erkennung von Sicherheitsvorfällen hätten zur Risikominimierung beitragen können.

Was lernen wir daraus:

Neue Funktionen in Software können erhebliche Sicherheitsrisiken darstellen, wenn sie nicht umfassend geprüft werden bevor sie live gehen. Unentdeckte Schwachstellen bieten Angreifern eine Angriffsfläche, die in diesem Fall zu finanziellen Verlusten geführt hat. Besonders in sensiblen Bereichen wie Finanz- und Kryptosystemen sind gründliche Tests essenziell, um solche Gefahren frühzeitig zu erkennen und zu vermeiden.

Anzunehmende Schadensfelder:

Quellen
https://de.cointelegraph.com/news/lifi-releases-incident-report-following-hack
https://thecyberexpress.com/lifi-hacked-defi-protocol-loses-10-million/
https://x.com/CertiKAlert/status/1813189183533383713

RIEDEL

Daten des CEOs eines Ultraschallmaschinen-Herstellers gestohlen

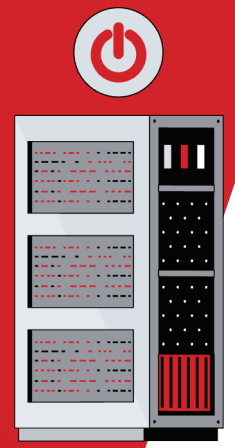
15. Juli 2024, in Spaichingen/Baden-Württemberg

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Berichten zufolge wurde ein Unternehmen aus der Technologiebranche von der Hackergruppe HUNTERS INTERNATIONAL mit Ransomware angegriffen. Die Gruppe behauptet, 3,7 Terabyte an sensiblen Daten, darunter Informationen des CEOs und der Personalabteilung, gestohlen zu haben. HUNTERS INTERNATIONAL drohte damit, die Daten zu veröffentlichen, sollte das Unternehmen kein Lösegeld zahlen.

Was hätte man besser machen können?
Durch regelmäßige Sicherheitsüberprüfungen und Penetrationstests hätte das Unternehmen potenzielle Schwachstellen frühzeitig erkennen können. Ein aktives SOC-Team wäre in der Lage gewesen, schnell und koordiniert auf den Angriff zu reagieren. Backup-Systeme hätten eine zügige Wiederherstellung von wichtigen Daten und Funktionen ermöglicht.



Was lernen wir daraus:

Hunters International ist eine Ransomwaregruppe, die erstmals im Oktober 2023 auftrat und sich schnell in der Cyberkriminalitätsszene einen Namen machte. Obwohl sie viele Ähnlichkeiten mit der inzwischen aufgelösten Hive-Gruppe aufweist, handelt es sich nicht um ein Rebranding. Die Gruppe agiert als Ransomware-as-a-Service (RaaS) und stellt ihre Tools auch weniger erfahrenen Cyberkriminellen zur Verfügung.

Anzunehmende Schadensfelder:

Quellen
https://ransomfeed.it/index.php?page=post_details&id_post=16331
https://x.com/FalconFeedsio/status/1812872807295967248
https://x.com/H4ckManac/status/1812860041340358669

RIEDEL

Angriff auf Deutschlands größtes Telekommunikationsunternehmen

13. Juli 2024, Bonn/Nordrhein-Westfalen

DATENLECK

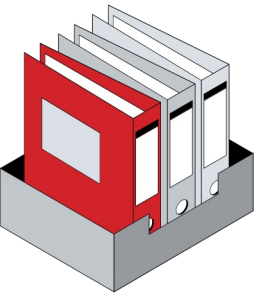
SICHERHEITSLÜCKE

Was ist passiert?
Eine Sicherheitslücke bei Deutschlands größtem Telekommunikationsunternehmen ermöglichte es, personenbezogene Kundendaten anhand der IP-Adresse auszulesen. Dabei wurden Tarifinformationen, Datenraten, Anschlussvorwahl und eine permanente ID offengelegt. Grund waren intern gespeicherte Daten für Komfortfunktionen. Nach Meldung durch eine Sicherheitsforscherin wurde das Problem behoben, einschließlich der potenziellen Möglichkeit, Anschlüsse bis auf den Häuserblock genau zu lokalisieren.

Was hätte man besser machen können?
Um den Vorfall zu verhindern, hätte das Telekommunikationsunternehmen stärkere Sicherheitsvorkehrungen treffen sollen, etwa durch eine starke Verschlüsselung und Anonymisierung der gespeicherten Daten. Zudem wären striktere Zugriffskontrollen und eine verbesserte Authentifizierung erforderlich gewesen, um unbefugten Zugriff zu verhindern.

Was lernen wir daraus:

Die IT-Landschaft ändert sich ständig, ebenso wie die Bedrohungen. Durch regelmäßige Sicherheitsbewertungen und Penetrationstests können Unternehmen Schwachstellen in ihrer Infrastruktur identifizieren und beheben, bevor sie von Angreifern ausgenutzt werden.



Anzunehmende Schadensfelder:

Quellen
https://lilithwittmann.medium.com/festnetz-cool-got-acquired-by-x-forward-for-ventures-der-deutschen-telekom-ag-d3fbe59f7365
https://x.com/LilithWittmann/status/1812095744767099045

RIEDEL

IT-Sicherheit eines Flugzeugtechnik-Unternehmens ist abgestürzt

12. Juli 2024, in Neunkirchen/Saarland

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Eine Hackergruppe führte im Juli 2024 einen Ransomware-Angriff auf ein deutsches Unternehmen aus dem Bereich der Flugzeugtechnik & Metallverarbeitung durch. Die Angreifer behaupten, mehr als 500 GB Unternehmensdaten, einschließlich sensibler Kundendaten, gestohlen zu haben. Das Unternehmen wurde erpresst, ein Lösegeld zu zahlen, andernfalls drohten die Hacker, die gestohlenen Daten zu veröffentlichen.

Was hätte man besser machen können?
Das Unternehmen hätte im Vorfeld ein modernes EDR-System einsetzen können, um verdächtige Aktivitäten frühzeitig zu erkennen und zu bewerten. Dadurch wären potenzielle Angriffe schneller identifiziert und effektiv abgewehrt worden. Ergänzend wären regelmäßige Überprüfungen auf Sicherheitslücken sowie durchdachte Strategien zur Reaktion auf Vorfälle entscheidend gewesen, um die allgemeine IT-Sicherheit zu stärken.

Was lernen wir daraus:

Nach einem Ransomware-Angriff fallen nicht nur die direkten Kosten des Lösegelds an. Unternehmen müssen auch mit hohen Ausgaben für Wiederherstellung, IT-Forensik und mögliche Betriebsunterbrechungen rechnen.

Die Investition in präventive Sicherheitsmaßnahmen kann helfen, solche finanziellen Belastungen zu vermeiden und die Auswirkungen eines Angriffs zu minimieren.

Anzunehmende Schadensfelder:

Quellen
https://x.com/_venarix_/status/1811795815398248875
https://ransomfeed.it/index.php?page=post_details&id_post=16292

RIEDEL

RansomHub entwendet deutscher Hotelkette Finanz- und Personaldaten

11. Juli 2024, in Hamburg/Hamburg

DATENDIEBSTAHL

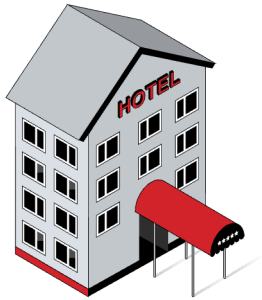
RANSOMWARE

Was ist passiert?
Eine deutsche Hotelkette wurde offenbar Ziel eines Ransomware-Angriffs durch die Hackergruppe RansomHub. Am 11. Juli 2024 tauchte das Unternehmen auf einer Opferliste im Darknet auf. Die Angreifer behaupten, 10 GB Daten, darunter Finanz- und Personaldaten, entwendet zu haben.

Was hätte man besser machen können?
Um den Sicherheitsvorfall zu verhindern, hätte man eine sichere Konfiguration der Server und Datenbanken sicherstellen sollen. Dazu gehören regelmäßige Sicherheitsüberprüfungen, strikte Zugangskontrollen und die Verschlüsselung sensibler Daten sowohl im Ruhezustand als auch während der Übertragung. Zudem wären umfassende Protokollierungen und Echtzeit-Monitoring erforderlich gewesen, um unbefugte Zugriffe schnell zu erkennen.

Was lernen wir daraus:

Die Ransomware-as-a-Service-Gruppe (RaaS) RansomHub trat Anfang 2024 in Cybercrime-Foren in Erscheinung und wurde schnell bekannt für ihre aggressiven Kampagnen gegen Windows-, macOS-, Linux- und VMware-Umgebungen. Im Monat vor dem Angriff auf die Hotelkette war RansomHub für 21 Prozent der bekannten Angriffe verantwortlich. Experten vermuten, dass RansomHub eine Weiterentwicklung der früheren Ransomware Knight ist.



Anzunehmende Schadensfelder:

Quellen
https://www.csoonline.com/article/3495139/ransomware-attacke-auf-eurostrand.html
https://x.com/TMRansomMon/status/1811443749962010734

RIEDEL

Sämtliche gestohlene Daten eines Bauunternehmens veröffentlicht

10. Juli 2024, in Siegen/Nordrhein-Westfalen

EINBRUCH

RANSOMWARE

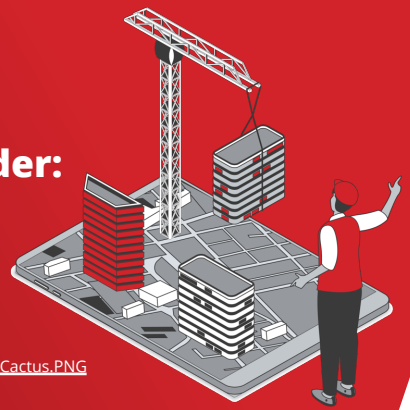
DATENLECK

DATENDIEBSTAHL

Was ist passiert?
Cyberkriminelle der Cactus-Gruppe griffen im Juni 2024 ein deutsches Bauunternehmen an und erklärten, 650 GB sensibler Daten entwendet zu haben. Als Beweis veröffentlichten die Täter Dokumente wie Rechnungen, Auftragsbescheinigungen und Bürgschaften. Sie drohten, alle gestohlenen Daten offenzulegen, falls ihre Forderungen nicht erfüllt würden. Am 10. Juli 2024 setzten sie ihre Drohung um und veröffentlichten die gesamten Daten.

Was hätte man besser machen können?
Um einen Ransomware-Angriff zu verhindern, hätte das Bauunternehmen umfassende Sicherheitsmaßnahmen ergreifen sollen. Dazu gehören u.a. regelmäßige, offline gespeicherte Backups, die im Ernstfall eine schnelle Wiederherstellung der Daten ermöglichen, sowie die Implementierung starker Sicherheitsprotokolle wie Multi-Faktor-Authentifizierung und Zugriffsbeschränkungen. Schulungen für Mitarbeiter wären ebenfalls essenziell gewesen, um sie im Umgang mit Phishing-Mails und anderen Angriffsmethoden zu sensibilisieren.

Anzunehmende Schadensfelder:



Was lernen wir daraus:

Ransomware-Angriffe zielen häufig auf Sicherheitslücken in schlecht geschützten Systemen ab. Deshalb sind regelmäßige Überprüfungen und Aktualisierungen der Systeme von großer Bedeutung. Indem Unternehmen Schwachstellen frühzeitig erkennen und beheben, können sie das Risiko solcher Angriffe deutlich reduzieren und ihre IT-Systeme besser vor Gefahren schützen.

Quellen
https://www.security-incidents.de/assets/img/incidents/6109-Hundhausen-Cactus.PNG

RIEDEL

Bundesübergreifender Datendiebstahl bei deutschen Notarkammern

9. Juli 2024, in Zweibrücken/Rheinland-Pfalz

DATENPANNE

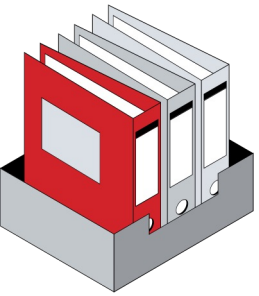
RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Im Juni 2024 startete die Ransomwaregruppe Akira einen Cyber-Angriff auf deutsche Notarkammern. Die Täter behaupten, über 200 GB Daten entwendet zu haben. Das Schadprogramm verschlüsselte Teile der Serverdaten, sodass diese nicht mehr verwendbar waren. Betroffen sind vorrangig personenbezogene Daten wie Namen, Adressen, Geburtsdaten, Telefonnummern, E-Mails und Sozialversicherungsnummern. Die betroffenen Organisationen trennten ihre IT-Infrastruktur vom Netz, schlossen den Zugriffsweg der Schadsoftware und informierten die zuständigen Behörden. Zudem wurden externe IT-Dienstleister beauftragt, den Vorfall zu analysieren.

Was hätte man besser machen können?
Um die Auswirkungen der Sicherheitslücke zu minimieren, hätte man regelmäßige Sicherheitsüberprüfungen und stärkere Zugangskontrollen implementieren sollen. Ein Incident-Response-Plan sowie der Einsatz von SIEM-Systemen zur frühzeitigen Erkennung von Sicherheitsvorfällen wären ebenfalls hilfreich gewesen.

Was lernen wir daraus:
Durch kontinuierliche Sicherheitsüberprüfungen können potenzielle Schwachstellen frühzeitig erkannt und behoben werden, bevor sie von Angreifern ausgenutzt werden. Eine proaktive Schwachstellenanalyse hilft, Sicherheitslücken zu schließen, bevor sie zu ernsthaften Problemen oder Datenverlust führen können. Dies schützt nicht nur die Integrität und Vertraulichkeit der Daten, sondern bewahrt auch das Vertrauen der Kunden und vermeidet teure Ausfallzeiten und rechtliche Konsequenzen.



Anzunehmende Schadensfelder:

Quellen
https://www.notare.bayern.de/presse/pressemitteilungen/betroffenenbenachrichtigung-nach-art-34-dsgvo/
https://www.security-incidents.de/assets/img/incidents/6060-Notarkammer_Pfalz-Akira.PNG

RIEDEL

„IT-Systeme der Hochschule sind runtergefahren“

8. Juli 2024, in Frankfurt/Hessen

AUSFALL

EINBRUCH

Was ist passiert?
Im Juli 2024 wurde eine Frankfurter Hochschule für angewandte Wissenschaften Ziel eines Cyberangriffs. Die Angreifer drangen in die IT-Systeme der Hochschule ein, woraufhin alle externen Zugänge blockiert und mehrere Systeme heruntergefahren wurden. Betroffen sind unter anderem die Online-Einschreibung, Kommunikationskanäle und Aufzüge. Der Präsenz-Lehrbetrieb lief jedoch weiter, während der externe Kontakt per Telefon und E-Mail nicht möglich war.

Was hätte man besser machen können?
Um den Ausfällen an einer Frankfurter Hochschule vorzubeugen, hätte man ein SIEM nutzen sollen. Ein SIEM-System hätte geholfen, Sicherheitsvorfälle frühzeitig zu erkennen und zu analysieren, indem es Echtzeit-Überwachung und zentrale Protokollierung bot. Dies hätte eine schnellere Reaktion auf den Cyberangriff ermöglicht, die Sicherheitslage verbessert und dazu beigetragen, Datenverluste zu verhindern.

Was lernen wir daraus:

Um Risiken zu minimieren, sollten Unternehmen und Organisationen eine umfassende Sicherheitsstrategie entwickeln und ihre Mitarbeiter regelmäßig schulen. Der Einsatz mehrschichtiger Sicherheitslösungen und regelmäßiger Sicherheitsüberprüfungen ist ebenfalls wichtig. Dabei kann die Inanspruchnahme von Managed Security Services wertvollen Schutz bieten und die Reaktionsfähigkeit auf Bedrohungen verbessern.

Anzunehmende Schadensfelder:

Quellen
https://www.hessenschau.de/panorama/hacker-attacke-auf-frankfurter-university-of-applied-sciences-v1,uas-frankfurt-hacker-100.html
https://www.security-incidents.de/assets/img/incidents/5887-frankfurter-university-of-applied-sciences-wartungsseite.png

RIEDEL

Produktionsausfall in mehreren Werken wegen Cyberangriff

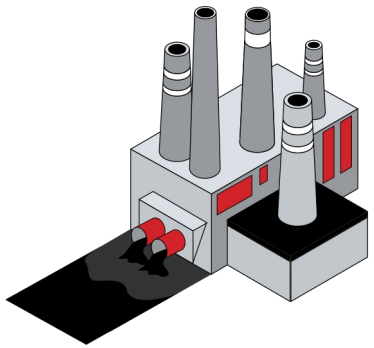
4. Juli 2024, in Hofgeismar/Hessen

AUSFALL

MALWARE

Was ist passiert?
Anfang Juli 2024 wurde ein deutscher Hersteller von Hochleistungskühlern und Wärmetauschern Ziel eines Cyberangriffs. Der Angriff legte die IT-Systeme lahm, was zu Produktionsausfällen und Kommunikationsstörungen führte. Die Produktion in den meisten Werken konnte zügig wieder aufgenommen werden. Die genaue Höhe des Schadens und das Ausmaß möglicher Datenlecks sind jedoch nicht bekannt.

Was hätte man besser machen können?
Eine kontinuierliche 24/7-Überwachung der IT-Systeme wäre entscheidend gewesen, um Bedrohungen in Echtzeit zu identifizieren und sofortige Gegenmaßnahmen einzuleiten. Darüber hinaus hätten regelmäßige Backups und deren sichere Speicherung es ermöglicht, im Falle eines Angriffs schnell eine Wiederherstellung der Systeme vorzunehmen.



Was lernen wir daraus:

Nach einem Angriff entstehen häufig hohe Kosten für die Wiederherstellung und Verbesserung der Sicherheit. Präventive Investitionen in robuste IT-Sicherheitslösungen hingegen können dazu beitragen, potenzielle Angriffe zu verhindern und so sowohl finanzielle als auch betriebliche Schäden erheblich zu verringern.

Quellen
https://www.security-incidents.de/assets/img/incidents/5968-AKG-1.png
https://www.facebook.com/AKGGruppe/posts/pfbid02w8ImnCaKan4cnb4UIGjpG3W4XT4iPcWs3ow54vEFmviEvBywtyKhosEvxZV7R2DVl

RIEDEL

Stahlriese kämpft mehrere Wochen gegen Cyberkriminelle an

4. Juli 2024, in Plettenberg/Nordrhein-Westfalen

DATENDIEBSTAHL

RANSOMWARE

AUSFALL

Was ist passiert?
Mehrere Wochen kämpfte ein deutsches Stahlunternehmen im Juli 2024 gegen einen Ransomware-Angriff. Die Gruppe LockBit3.0 verschlüsselte Unternehmensdaten und forderte ein Lösegeld. Es ist unklar, ob das Unternehmen zahlte. Betroffen sind Produktions-, Mitarbeiter- und Kundendaten. Der Angriff führte zudem zu Produktionsausfällen und unterbrach mehrere Tage lang die Lagerhaltung und Logistik des Unternehmens.

Was hätte man besser machen können?
Um den Vorfall zu vermeiden, hätten stärkere Sicherheitsmaßnahmen wie Zwei-Faktor-Authentifizierung und strenge Passwortanforderungen implementiert werden müssen. Zusätzlich hätte die Verschlüsselung der sensiblen Daten und eine strikte Zugangskontrolle den unbefugten Zugriff verhindern können. Eine kontinuierliche Überwachung der Systeme wäre ebenfalls wichtig gewesen, um Sicherheitslücken rechtzeitig zu schließen.

Was lernen wir daraus:

Bei Unternehmen, die selbst produzieren ist das Risiko eines Produktionsstopps besonders kritisch, da dies zu erheblichen finanziellen Verlusten und Betriebsstörungen führen kann. Deshalb ist es entscheidend, starke Sicherheitsvorkehrungen zu treffen und einen effektiven Notfallplan zu entwickeln, um solche Angriffe abzuwehren und schnell handeln zu können.

Anzunehmende Schadensfelder:

Quellen
https://x.com/H4ckManac/status/1808758479198261573
https://www.security-incidents.de/assets/img/incidents/5978-Lockbit3-WS-Stahl2.png

RIEDEL

Kompromittierte Daten bei Online-Shop für Medizin- und Arztbedarf

2. Juli 2024, in Neunkirchen/Saarland

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Ein deutscher Online-Shop für Medizin- und Arztbedarf wurde Opfer eines Ransomware-Angriffs. Die Gruppe RansomHub gab am 1. Juli 2024 bekannt, dass sie 100 GB an Daten des Unternehmens kompromittiert hat. Die Hacker setzten dem Unternehmen eine Frist von 18 Tagen, um das geforderte Lösegeld zu zahlen, andernfalls drohten sie mit der Veröffentlichung der gestohlenen Daten.

Was hätte man besser machen können?
Eine 24/7-Überwachung des Unternehmensnetzwerk mit Hilfe eines Security Operations Center (SOC) hätten verdächtige Aktivitäten frühzeitig erkannt und abgewehrt werden können.

Eine kontinuierliche Analyse und proaktive Bedrohungserkennung hätten es ermöglicht, den Angriff zu verhindern, bevor sensible Daten kompromittiert wurden.

Anzunehmende Schadensfelder:

Quellen
https://ransomfeed.it/index.php?page=post_details&id_post=16189
https://x.com/DailyDarkWeb/status/1808471838810333197

Was lernen wir daraus:

Unternehmen müssen proaktive Maßnahmen ergreifen, um Sicherheitslücken zu schließen, um die Vertraulichkeit und Integrität von Kundendaten zu gewährleisten. Dazu gehört die regelmäßige Durchführung von Sicherheitsüberprüfungen und Schwachstellenanalysen, die Implementierung von fortschrittlichen Sicherheitsprotokollen und -technologien sowie die Schulung von Mitarbeitern in den besten Praktiken für Cybersicherheit.

RIEDEL

Zugriff auf die Datensammlung des deutschen Gesundheitswesens

1. Juli 2024, in Bonn/Nordrhein-Westfalen

SICHEREHEITSLÜCKE

AUSFALL

Was ist passiert?
Ab Mitte Juni 2024 ging ein Portal für Gesundheitsdaten offline, nachdem eine Sicherheitslücke entdeckt wurde. Die Plattform, die umfassende Informationen über das deutsche Gesundheitswesen bietet, befand sich im Wartungsmodus. Die Lücke betraf die Nutzerverwaltung, wodurch Angreifer mit einem Usernamen und Passwort auf persönliche Daten zugreifen und diese ändern konnten. Außerdem war es möglich, XSS-Angriffe auszuführen. Etwa 500 Nutzerprofile waren betroffen.

Was hätte man besser machen können?
Um diesen Vorfall zu verhindern, hätte man bei dem Informationssystem proaktive Sicherheitsmaßnahmen wie regelmäßige Sicherheitsüberprüfungen und Schwachstellenanalysen durchführen sollen, um potenzielle Lücken unmittelbar zu identifizieren. Eine sichere Verwaltung von Nutzerzugängen, etwa durch Multi-Faktor-Authentifizierung, sowie die konsequente Anwendung von sicheren Codierungspraktiken hätten das Risiko eines solchen Angriffs verringern können.

Anzunehmende Schadensfelder:

Was lernen wir daraus:

Aus diesem Sicherheitsvorfall wird deutlich, wie gravierend Schwachstellen in der Nutzerverwaltung sein können. Die Möglichkeit, Daten zu ändern, birgt erhebliche Risiken, darunter die Manipulation sensibler Informationen und potenzieller Missbrauch. Beispielsweise könnten Angreifer falsche Daten einfügen, um Nutzer zu täuschen oder den Zugang zu weiteren Systemen zu erschleichen.

Quellen
https://www.heise.de//news/Gesundheitsberichterstattung-des-Bundes-Sicherheitsluecke-traf-Favoritenliste-9785918.html
https://www.golem.de/news/sicherheitsluecke-bei-gbe-gesundheitsdatensammlung-des-bundes-seit-tagen-offline-2407-186586.html

RIEDEL

Fehlkonfiguration ermöglicht unautorisierten Zugriff auf Kundendaten

1. Juli 2024, in Waldkirch/Baden-Württemberg

SICHERHEITSLÜCKE

AUSFALL

KONFIGURATIONSFEHLER

SUPPLY CHAIN

Was ist passiert?
Ein Unternehmen aus der Sensortechnologiebranche entdeckte eine Sicherheitslücke in seinem Support-Portal, verursacht durch eine Fehlkonfiguration eines externen Dienstleisters. Dadurch waren zeitweise Kundendaten, einschließlich betrieblicher E-Mail-Adressen, ohne Login einsehbar. Die Firma hatte das Portal deaktiviert, den Zugang gesichert und arbeitete mit IT-Experten an der Analyse. Kunden wurden über potenzielle Risiken informiert.

Was hätte man besser machen können?
Regelmäßige Überprüfungen der IT-Sicherheit sind essenziell, um Schwachstellen frühzeitig aufzudecken und zu beseitigen. Dazu zählen beispielsweise Penetrationstests und Scans nach Schwachstellen, die mögliche Angriffsflächen erkennen, bevor sie missbraucht werden.

Eine kontinuierliche Überwachung der Systeme spielt ebenfalls eine zentrale Rolle, da Bedrohungen in Echtzeit erkannt und durch schnelle Gegenmaßnahmen effektiv abgewehrt werden können.

Was lernen wir daraus:

Die Zusammenarbeit mit externen Dienstleistern sollte gut durchdacht und strategisch gewählt werden, da sie zusätzliche Risiken birgt. Ohne klar definierte Verantwortlichkeiten, vertraglich geregelte Sicherheitsstandards und regelmäßige Sicherheitsaudits können solche Partnerschaften anfällig für Schwachstellen sein. Ein sorgfältiger Auswahlprozess und kontinuierliches Monitoring sind unerlässlich, um potenzielle Sicherheitsprobleme zu vermeiden.

Anzunehmende Schadensfelder:

Quellen
https://www.heise.de//news/Sensorhersteller-Sick-Kein-Cyberangriff-Sicherheitsluecke-im-Support-Portal-9785547.html
https://www.security-incidents.de/assets/img/incidents/5819-sick-ag-sicherheitsluecke-mitteilung.png

RIEDEL

Ransomexx-Angriff auf Schulungsnetzwerk: 650 GB Daten betroffen

1. Juli 2024, in Köln/Nordrhein-Westfalen

DATENDIEBSTAHL

SUPPLY CHAIN

Was ist passiert?
Am 1. Juli 2024 meldete die Ransomwaregruppe Ransomexx, 650 GB Daten eines deutschen Unternehmens aus dem Bereich Prüf- und Schulungsdienstleistungen gestohlen zu haben. Laut dem Unternehmen betraf der Angriff das abgekapselte Schulungsnetzwerk einer Tochtergesellschaft. Entwendet wurden Schulungsinhalte, Raumbelegungen und möglicherweise Zugangsdaten. Das betroffene Netzwerk wurde umgehend deaktiviert und die Server neu installiert.

Was hätte man besser machen können?
Das angegriffene Unternehmen hätte den Angriff frühzeitiger entdecken können durch die Integration eines Managed-SIEM mit einem rund um die Uhr besetzten Security Operations Center (SOC). Durch eine frühzeitigere Reaktion hätte man die Veröffentlichung von Schulungsinhalte, Raumbelegungen und Zugangsdaten möglicherweise vermeiden können.

Was lernen wir daraus:

Der Angriff zeigt, wie wichtig es ist, Netzwerke klar voneinander zu trennen. Ein abgekapseltes Schulungsnetzwerk minimierte den Schaden und schützte das Unternehmensnetzwerk vor direkten Auswirkungen. Diese Trennung sollte Best Practice sein, um sensible Bereiche voneinander abzuschirmen.

Anzunehmende Schadensfelder:

Quellen
https://www.golem.de/news/cyberangriff-hacker-erbeuten-daten-von-tuev-rheinland-2407-186665.html
https://x.com/FalconFeedsio/status/1807748723986039131

RIEDEL

Erkenntnisse

OOPS Report H2-2024

RIEDEL

Summary

Welche Erkenntnisse stechen besonders hervor?

Branchen

Im OOPS-Report H2-2024 werden mehrere Branchen genannt, die von Sicherheitsvorfällen betroffen waren, sowie deren prozentuale Verteilung. Die betroffenen Branchen sind:

1.Finanzsektor** - 25%**
2.Gesundheitswesen** - 20%**
3.Industrie** - 18%**
4.Öffentlicher Sektor** - 15%**
5.IT-Dienstleister** - 12%**
6. **Bildungswesen - 10%**

Diese Zahlen zeigen, dass der Finanzsektor weiterhin am stärksten betroffen ist, während auch das Gesundheitswesen und industrielle Unternehmen zunehmend Ziel von Angriffen werden.

Angreifertypen

Die prozentuale Verteilung der Angreifertypen im OOPS-Report H1-2024 sieht wie folgt aus:

1. **Erpresser: 42%**
2. **Staatliche Spionage: 23%**
3. **Bösartige Hacker: 25%**
4. **Whitehacker: 10%**

Diese Zahlen zeigen, dass Erpressungsangriffe weiterhin die größte Bedrohung darstellen, während staatlich geförderte Spionage ebenfalls einen erheblichen Anteil ausmacht.

Angriffstypen

Im OOPS-Report H1-2024 werden folgende Angriffstypen und ihre prozentuale Verteilung genannt:

1. **Ransomware: 47%**
2. **Datendiebstahl: 30%**
3. **Phishing & Social Engineering: 12%**
4. **DDoS-Angriffe: 6%**
5. **Exploits bekannter Sicherheitslücken: 5%**

Die Zahlen zeigen, dass Ransomware weiterhin die größte Bedrohung darstellt, während gezielter Datendiebstahl ebenfalls eine signifikante Rolle spielt.

RIEDEL

Summary

Welche Erkenntnisse stechen besonders hervor?

1. Ransomware dominiert weiterhin – Mit 47% bleibt Ransomware der häufigste Angriffstyp. Das deutet darauf hin, dass Unternehmen trotz steigender Abwehrmaßnahmen weiterhin anfällig für solche Angriffe sind.

2. Erpresser sind die größte Angreifergruppe (42%) – Das zeigt, dass Cyberkriminalität zunehmend wirtschaftlich motiviert ist. Angriffe zielen darauf ab, Unternehmen zur Zahlung von Lösegeld zu zwingen, anstatt nur Daten zu stehlen oder Schaden anzurichten.

3. Steigender Anteil staatlicher Spionage (23%) – Dies unterstreicht, dass Cyberangriffe nicht nur aus finanziellen Motiven erfolgen, sondern auch politische und wirtschaftliche Interessen eine immer größere Rolle spielen.

4. Wichtige Branchen sind besonders betroffen – Der Finanzsektor (25%), das Gesundheitswesen (20%) und die Industrie (18%) stehen besonders im Visier der Angreifer. Vor allem im Gesundheitswesen sind Datenschutzprobleme kritisch, da Patientendaten extrem sensibel sind.

5. Phishing & Social Engineering bleibt ein Problem – Mit 12% der Angriffe zeigt sich, dass menschliche Fehler weiterhin eine große Schwachstelle in der IT-Sicherheit darstellen.

6. Whitehacker spielen nur eine kleine Rolle (10%) – Das deutet darauf hin, dass ethische Hacker zwar Schwachstellen aufdecken, aber in der Gesamtstatistik eine vergleichsweise geringe Bedeutung haben.

Der Report zeigt, dass Unternehmen sich weiterhin verstärkt gegen Ransomware und Erpressung schützen müssen. Gleichzeitig steigt die Bedrohung durch staatlich gelenkte Spionage, was insbesondere kritische Infrastrukturen und den öffentlichen Sektor betrifft. Auch Social Engineering bleibt ein wichtiges Angriffswerkzeug, was die Notwendigkeit für verstärkte Schulungen und Sensibilisierung der Mitarbeiter verdeutlicht.

RIEDEL

Summary

Welche Erkenntnisse stechen besonders hervor?

Zunahme von Cyberangriffen: Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) war die IT-Sicherheitslage in Deutschland im Jahr 2024 besorgniserregend. Cyberkriminelle professionalisierten ihre Methoden und etablierten kriminelle Dienstleistungsstrukturen.

· **Herkunft der Angriffe:** Eine Studie des Digitalverbands Bitkom ergab, dass 45% der befragten deutschen Unternehmen Cyberangriffe China zuschreiben, gefolgt von Russland (39%) und Deutschland selbst (20%).

Anstieg von E-Mail-basierten Angriffen: Der Acronis Cyberthreats Report für das zweite Halbjahr 2024 berichtete von einem Anstieg der E-Mail-basierten Angriffe um 197% im Vergleich zum Vorjahreszeitraum.

· **Zunahme von DDoS-Angriffen:** Die Europäische Union Agency for Cybersecurity (ENISA) stellte fest, dass DDoS-Angriffe im ersten Halbjahr 2024 um mehr als ein Viertel zunahmen, mit einer bemerkenswerten Zunahme von sogenannten "Turbo-Attacken".

· **Steigende Cyberversicherungsschäden:** Allianz Commercial berichtete, dass die Häufigkeit und die Kosten großer Cyber-Versicherungsschäden im ersten Halbjahr 2024 im Vergleich zum Vorjahr um 14% bzw. 17% gestiegen sind, wobei in zwei Dritteln der Fälle Datenschutzverletzungen eine Rolle spielten.

Im zweiten Halbjahr 2024 erlebten europäische Länder eine deutliche Zunahme von Cyberangriffen, insbesondere in Form von E-Mail-basierten Attacken und DDoS-Angriffen. Deutschland war dabei besonders betroffen, wobei ein signifikanter Anteil der Angriffe aus China und Russland stammte. Diese Entwicklungen unterstreichen die Notwendigkeit verstärkter Sicherheitsmaßnahmen und internationaler Zusammenarbeit im Bereich der Cybersicherheit.

RIEDEL

“

Der Report zeigt, dass Unternehmen sich weiterhin verstärkt gegen Ransomware und Erpressung schützen müssen. Gleichzeitig steigt die Bedrohung durch staatlich gelenkte Spionage, was insbesondere kritische Infrastrukturen und den öffentlichen Sektor betrifft. Auch Social Engineering bleibt ein wichtiges Angriffswerkzeug, was die Notwendigkeit für verstärkte Schulungen und Sensibilisierung der Mitarbeiter verdeutlicht.

Im zweiten Halbjahr 2024 verzeichneten europäische Länder eine signifikante Zunahme von Cyberangriffen, wobei verschiedene Angriffstypen und -vektoren beobachtet wurden.

”

RIEDEL

Vergleich

Welche Gemeinsamkeiten bestehen zwischen dem ersten und zweiten Halbjahr 2024?

Ransomware bleibt die dominierende Bedrohung

- In beiden Berichtszeiträumen war Ransomware der häufigste Angriffstyp.
- H1: 45% aller Angriffe waren Ransomware.
- H2: Dieser Wert stieg leicht auf 47%.

Erpressung als Hauptmotiv der Angreifer

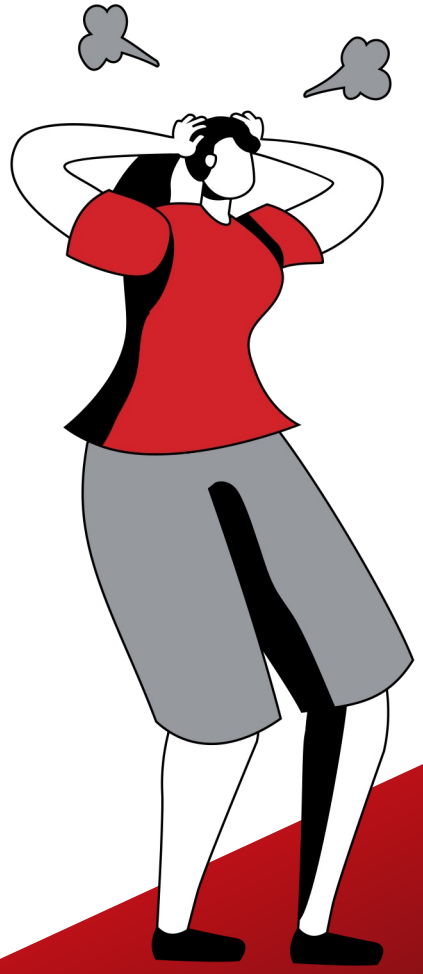
- In beiden Berichten stellen Erpresser die größte Angreifergruppe dar.
- H1: 40% der Angriffe gingen von Erpressern aus.
- H2: Der Anteil stieg auf 42%.

Betroffene Branchen

- Der Finanzsektor und das Gesundheitswesen sind in beiden Berichten stark betroffen.
- Industrie und Fertigung haben in beiden Zeiträumen eine hohe Anzahl an Vorfällen verzeichnet.

Staatliche Spionage als wachsendes Problem

- Sowohl in H1 als auch in H2 spielen staatlich gesteuerte Cyberangriffe eine große Rolle.
- Besonders betroffen sind der öffentliche Sektor und Unternehmen mit sensiblen Daten.



RIEDEL

Vergleich

Welche Gemeinsamkeiten bestehen zwischen dem ersten und zweiten Halbjahr 2024?

	H1-2024	H2-2024	Veränderung
Angriffstypen	Ransomware (45%), Datendiebstahl (30%), Einbruch (15%), Erpressung (10%)	Ransomware (47%), Datendiebstahl (30%), Phishing & Social Engineering (12%), DDoS (6%), Exploits (5%)	Phishing & Social Engineering nimmt zu, DDoS-Angriffe werden relevanter
Angreifertypen	Erpresser (40%), Staatliche Spionage (25%), Böse (20%), Whitehacker (15%)	Erpresser (42%), Staatliche Spionage (23%), Böse (25%), Whitehacker (10%)	Zunahme von bösartigen Hackern, Rückgang bei Whitehackern
Betroffene Branchen	Finanzsektor (28%), Gesundheitswesen (22%), Industrie (18%), Öffentlicher Sektor (15%), IT (10%), Bildung (7%)	Finanzsektor (25%), Gesundheitswesen (20%), Industrie (18%), Öffentlicher Sektor (15%), IT (12%), Bildung (10%)	IT und Bildung werden stärker ins Visier genommen
Neue Trends	Fokus auf klassische Angriffe (Ransomware, Einbruch)	Mehr Angriffe auf Cloud-Systeme, stärkere Automatisierung durch KI-gestützte Malware	Cyberkriminelle nutzen vermehrt KI-Technologien für Angriffe

RIEDEL

Erpressung und Ransomware bleiben zentrale Bedrohungen, aber Social Engineering und DDoS nehmen zu.
· Angriffe auf den Bildungs- und IT-Sektor steigen, während klassische Branchen (Finanzen, Gesundheit) weiterhin stark betroffen sind.

· Cyberkriminelle professionalisieren sich weiter, nutzen mehr automatisierte Angriffe und greifen vermehrt Cloud-basierte Systeme an.

· Whitehacker spielen eine geringere Rolle in H2-2024, während bösartige Hacker einen stärkeren Anteil ausmachen.

Get in Touch

Beim Thema IT-Security ist der erste Schritt immer, überhaupt anzufangen!

RIEDEL Networks GmbH & Co. KG

RN-sales@riedel.net

+49 (0) 6033 9169 100

Nicht überzeugt? Gerne senden wir Ihnen unser Cyber Security Faule Ausreden-Quartett".

Dann unterhalten wir uns erneut.

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

RIEDEL