OOPS H1-2024

Der “hätte ich das mal früher gewusst” Report

SECURITY INCIDENTS GERMANY

You have been hacked!
CLICK HERE TO PAY BITCOIN

RIEDEL

Disclaimer

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

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

RIEDEL

Die Welt hat sich verändert

Cyber-Resilienz ist einer der größten Wettbewerbsvorteile der Neuzeit

Einleitung

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

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

Im vorliegenden Whitepaper haben wir einen Auszug der medial aufgegriffenen Sicherheitsvorfälle des ersten Halbjahres 2024 aufgelistet und eingeordnet. Wir haben uns explizit dazu entschieden, die betroffenen Unternehmen nicht direkt namentlich zu nennen. Denn das Ziel des Whitepapers ist nicht, geschädigte Unternehmen zu tadeln. Vielmehr soll das Whitepaper dabei helfen, aus Vorfällen zu lernen und Rückschlüsse für die eigene IT-Sicherheitsstrategie zu ziehen.

RIEDEL

Schadensfelder durch Sicherheitsvorfälle

Legende und Erklärung

- Finanzielle Schäden (z.B. durch Lösegeldzahlungen, externe Aufwände, etc.)
- Schaden durch zeitlichen Zusatzaufwand und Bindung von Ressourcen (z.B. für die interne IT-Abteilung, die Geschäftsführung etc.)
- Reputationsschaden durch öffentliche Bekanntmachung oder Wahrnehmung des Angriffs bei Kunden, Partnern und anderen
- Produktionsausfall durch Stilllegung von Infrastruktur (z.B. zum Schutz der Systeme gegen weitere Verbreitung von Schadsoftware)
- Verlust von geistigem Eigentum: z.B. Geschäftsgeheimnisse, Patente, Produktpläne oder Forschungsergebnisse
- Verlust von Kunden- und Geschäftsdaten mit rechtlichen Konsequenzen und/oder Vertrauensverlust von Kunden
- Rechts- und Regulierungskosten: Rechtsstreitigkeiten, Bußgelder oder Strafen wegen Datenschutzverletzungen oder Nichteinhaltung gesetzlicher Vorschriften
- Kosten für Wiederherstellung und Nachbesserung betroffener Systeme und Aufrüstung
- Verlust von Marktanteilen durch Vertrauensverlust bei Kunden, die das zum Anlass nehmen, zur Konkurrenz zu wechseln
- Anstieg von Versicherungsprämien und Kosten oder der Verlust von Versicherungsschutz nach einem großen Vorfall.
- Psychologische Belastungen und negatives Arbeitsklima, insbesondere für Mitarbeiter, die mit der Bewältigung des Vorfalls befasst sind
- Rückgang des Aktienwerts, wenn der Vorfall öffentlich wird und das Vertrauen der Investoren sinkt
- Strategische Unternehmensrisiken wie die Beeinträchtigung von Unternehmensfusionen, Übernahmen oder Partnerschaften
- Verletzung von vertraglichen Verpflichtungen gegenüber Kunden, Lieferanten oder Partnern mit rechtlichen Konsequenzen

RIEDEL

JUNI 2024

SECURITY INCIDENTS GERMANY

RIEDEL

Ingenieursbetrieb schaltet Server nach mutmaßlichem Cyberangriff ab

30. Juni 2024, in München/Bayern

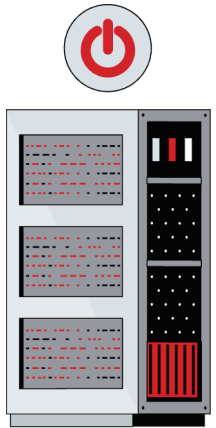
AUSFALL

Was ist passiert?
Laut einer Mitteilung des Unternehmens, die Ende Juni 2024 veröffentlicht wurde, haben Cyberkriminelle das Unternehmen mutmaßlich angegriffen. Daraufhin schaltete das Unternehmen alle Kommunikationskanäle über das Internet und die Festnetztelefonie ab. Bewerbungen von Jobinteressenten konnten nicht mehr empfangen werden.

Um die Kommunikation dennoch zu gewährleisten, richtete das Unternehmen kurzfristig eine separate E-Mail-Adresse ein.

Was hätte man besser machen können?
Informiert wurde das Unternehmen über den Angriff durch die Polizei. Erst im Anschluss wurden Security-Experten und Forensiker zur Analyse herangezogen.

Durch Einsatz eines Managed-SIEM mit entsprechendem 24/7 Security Operations Center, hätte der Angriff ggf. bereits früher entdeckt und proaktiv reagiert werden können.



Anzunehmende Schadensfelder:

Was lernen wir daraus:

- Ein Sicherheitsvorfall ist ein Ereignis, das die Informationssicherheit beeinträchtigt. Der Vorfall gefährdet die Vertraulichkeit, Verfügbarkeit oder Integrität der Daten, IT-Anwendungen, IT-Systeme oder IT-Dienste und kann für Personen, Unternehmen oder Organisation zu großen Schäden führen.
- Angreifer verweilen eine bestimmte Zeit unbemerkt in infiltrierten Systemen, bevor diese aktiv werden und der Angriff bemerkt wird. Die Zeit zwischen Eindringen und Bemerken des Angriffs nimmt stetig zu und beträgt durchschnittlich etwa 20 Tage.

RIEDEL

Quellen
https://www.meiller.com/de/wichtige-information/
https://web.archive.org/web/20240627004513/https://www.meiller.com/de/wichtige-information/

Exfiltration von Unternehmensdaten bei deutschem Weltmarktführer für Kekse

30. Juni 2024, in Aachen/Nordrhein-Westfalen

RANSOMWARE

EINBRUCH

DATENDIEBSTAHL

SUPPLY-CHAIN

Was ist passiert?
Die Ransomwaregruppe Black Basta hat den Aachener Backwarenhersteller angegriffen und behauptet, 800 GB an Unternehmensdaten, darunter Personal- und Finanzinformationen, gestohlen zu haben. Der Angriff erfolgte vermutlich über einen kompromittierten VPN-Zugang eines Dienstleisters. Das betroffene Unternehmen bestätigte den Vorfall und arbeitet mit externen Experten an der Aufklärung. Die IT-Systeme mussten neu aufgesetzt und durch eine moderne Firewall-Infrastruktur ersetzt werden, um zukünftige Angriffe zu verhindern.

Was hätte man besser machen können?
Um einen solchen Cyberangriff zu verhindern, hätte man strengerer Zugangskontrollen für VPN-Zugänge, einschließlich Multi-Faktor-Authentifizierung (MFA), um den Zugriff durch unbefugte Personen zu erschweren, einrichten können. Auch regelmäßige Sicherheits- und Penetrationstests, Netzwerksegmentierung für den Zugriff auf sensible Daten, der Einsatz von XDR und einem generellen Sicherheitsdienstleister hätten zu einem früheren Erkennen und/oder Abwehren des Angriffs führen können.

Anzunehmende Schadensfelder:

Was lernen wir daraus:

Im Rahmen der NIS2-RL müssen Unternehmen mindestens die folgenden Cybersecurity-Maßnahmen umsetzen, um IT-Infrastruktur und Netzwerke ihrer kritischen Dienstleistungen zu schützen:

- **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

Quellen
https://www.golem.de/news/cyberangriff-trifft-backwarenhersteller-hacker-gehen-lambertz-auf-den-keks-2407-186642.html

RIEDEL

Einbruch bei Technologieriesen: Angreifer erbeuten Mitarbeiterdaten und Logins

29. Juni 2024, in Göppingen/Baden-Württemberg

EINBRUCH

DATENDIEBSTAHL

Was ist passiert?
Hacker verschafften sich über einen Mitarbeiteraccount Zugang zum internen Netzwerk des Unternehmens. Hinweise deuten auf die russische Gruppe APT29 hin. Untersuchungen ergaben, dass nur das interne Verwaltungsumfeld betroffen war, nicht das Produktumfeld oder Kundendaten.

Die Angreifer stahlen Namen und Kontaktinformationen von Mitarbeitern und verschlüsselten Zugangsdaten.

Was hätte man besser machen können?
Die Trennung der Netzwerke ermöglichte es vermutlich, ein Vordringen der Angreifer in das Produktumfeld zu verhindern. Die Implementierung von Systemen zur Echtzeit-Überwachung und Erkennung verdächtiger Aktivitäten, um Angriffe schnell zu identifizieren und abzuwehren, kann hier von Vorteil sein.

Auch die Automatisierung mittels SOAR kann in Zukunft ähnliche Angriffsversuche erkennen und verhindern.

Anzunehmende Schadensfelder:

Quellen
https://thecyberexpress.com/teamviewer-data-breach-confirmed/
https://www.heise.de//news/APT-Angriff-auf-Fernwartungssoftware-Sicherheitsvorfall-bei-TeamViewer-9781567.html

Was lernen wir daraus:

An erster Stelle eines Angriffs steht immer die Kompromittierung des Systems: Das Ziel des Angreifers ist es, unbemerkt in ein fremdes Netzwerk einzudringen, sei es durch Phishing-Links, den Kauf von Anmeldedaten im Darknet oder die Installation kostenloser Programme, die unbemerkt "Info-Stealer"-Malware auf dem Computer eines ahnungslosen Benutzers platzieren, um vertrauliche Informationen auszuspionieren und weiterzuleiten.

RIEDEL

Autohaus erleidet Ransomware-Attacke: Erbeutete Daten angeblich zum Verkauf

27. Juni 2024, in Viersen/Nordrhein-Westfalen

RANSOMWARE

DATENLECK

DATENDIEBSTAHL

Was ist passiert?
Die Cloak-Gruppe behauptet im Darknet, das Unternehmen mit einer Ransomware-Attacke getroffen zu haben. Laut eigenen Angaben erlangten die Täter 148 GB an sensiblen Daten und veröffentlichten diese nach Ablauf einer Zahlungsfrist.

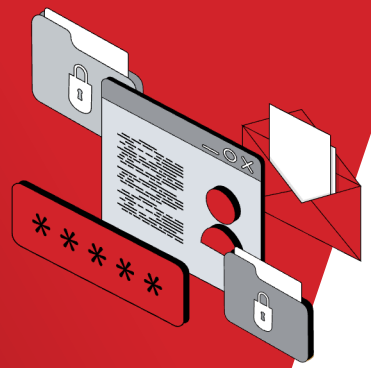
Unter den veröffentlichten Daten befinden sich Personalausweise, interne Lohntabellen und Excel-Tabellen mit zahlreichen personenbezogenen Details.

Was hätte man besser machen können?
Die Beobachtung von Dedicated Leak Sites (DLS) hätte es dem Unternehmen ermöglicht, frühzeitig auf die Veröffentlichung gestohlener Daten aufmerksam zu werden und schneller Gegenmaßnahmen zu ergreifen.

Was lernen wir daraus:

Die Attraktivität von KMUs – dazu gehört auch eine Vielzahl an deutschen Autohäusern – nimmt bei Cyberkriminellen vermehrt zu. Das liegt mitunter an den geringeren Hürden bei der möglichen Infiltration von Systemen, bei gleichzeitig sehr wertvollen Daten, die bei etlichen Weltmarktführern (sogenannter Hidden Champions) in Deutschland zu erbeuten sind.

Anzunehmende Schadensfelder:



Quellen
https://www.security-incidents.de/assets/img/incidents/5907-Ruland-Viersen-Cloak.PNG

RIEDEL

Mangels Schutzes sind Insassen-Daten verschiedener JVAs verfügbar

27. Juni 2024, in Hamburg/Hamburg

DATENLECK

SICHERHEITSLÜCKE

RANSOMWARE

Was ist passiert?
Eine Sicherheitslücke in der "Prison Control Center"-Webanwendung ermöglichte unverschlüsselten Zugriff auf sensible Daten von über 14.000 deutschen Häftlingen. Betroffen waren Verbindungsdaten von Telefonaten, einschließlich Gesprächen mit Anwälten und Psychologen. Die kompromittierten Daten umfassten Klarnamen, Haftnummern, PINs, Guthaben und Notizen sowie Details zu Telefonaten. Betroffen waren bundesweit 22 Haftanstalten.

Was hätte man besser machen können?
Nach Aussagen der Whitehead-Hackerin waren die Daten nicht mit einem Passwort geschützt, sie waren im Grunde überhaupt nicht geschützt. Erreichbar waren sie via Proxy und DynDNS. Die Nutzung von DynDNS bei kritischen Systemen sollte verhindert werden und zusätzliche Schutzmaßnahmen wie Firewalls und VPNs, um den Zugriff zu kontrollieren, sollten implementiert werden.

Was lernen wir daraus:

Sensible Daten müssen durchgehend geschützt und verschlüsselt werden, um das Risiko von Missbrauch im Falle eines Sicherheitsvorfalls zu minimieren.

Die Auswirkungen solcher Sicherheitslücken können erhebliche negative Folgen für die betroffenen Personen haben und auch rechtliche Konsequenzen für die betroffenen Organisationen nach sich ziehen.

Anzunehmende Schadensfelder:

Quellen
https://www.golem.de/news/sicherheitsluecke-ungeschuetzte-api-liefert-sensible-daten-deutscher-haeftlinge-2406-186483.html ;
https://lilithwittmann.medium.com/datenabfluss-aus-dem-knast-0f60cb597635

RIEDEL

Autozubehörunternehmen als Opfer einer Ransomwaregruppe gelistet

24. Juni 2024, in Rheda-Wiedenbrück/Nordrhein-Westfalen

DATENPANNE

DATENLECK

DATENDIEBSTAHL

EINBRUCH

Was ist passiert?
Am 24. Juni 2024 listete die Cactus-Gruppe ein Autozubehörunternehmen als Ransomware-Opfer auf ihrer Webseite. Laut den Angreifern wurden etwa 60 GB Daten gestohlen, darunter Zeichnungen, personenbezogene Informationen, Mitarbeiterakten, Finanzdaten und weitere Firmeninterna. Zur Bestätigung wurden Screenshots von Reisepässen und anderen Dokumenten veröffentlicht.

Am 2. August 2024 ist der Eintrag verschwunden und es ist unklar, ob ein Lösegeld gezahlt wurde oder die Hacker falsch lagen.

Was hätte man besser machen können?
Ein SIEM-System hätte den Ransomware-Angriff frühzeitig entdeckt und durch automatische Schutzmaßnahmen eindämmen können. Ein SIEM-System bietet eine Echtzeitüberwachung, ermöglicht rasche Reaktionen und unterstützt bei der forensischen Analyse.

Was lernen wir daraus:

Ransomwaregruppen sind Netzwerke von Cyberkriminellen, die spezialisierte Schadsoftware entwickeln und einsetzen, um Daten zu verschlüsseln und Lösegelder zu erpressen. Sie agieren oft wie Unternehmen, mit klaren Rollen wie Entwicklern, Angreifern und sogar Kundenbetreuern.

Viele Gruppen verwenden das „Ransomware-as-a-Service"-Modell, bei dem sie ihre Malware an andere Cyberkriminelle vermieten, was die Verbreitung und Effizienz ihrer Angriffe wiederum erhöht.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6122-Westfalia-Automotive.png

RIEDEL

Ransomware-Angriff trifft IT-Unternehmen

23. Juni 2024, in Leipzig/Sachsen

RANSOMWARE

DATENPANNE

DATENDIEBSTAHL

DATENLECK

Was ist passiert?
Am 23. Juni 2024 listete die Cactus-Gruppe ein IT-Unternehmen als Ransomware-Opfer auf ihrer Webseite. Die Cyberkriminellen behaupteten, über 224 GB an sensiblen Daten gestohlen zu haben. Nachdem das Unternehmen die Frist zur Erfüllung der Forderungen verstreichen ließ, wurden alle Daten veröffentlicht – darunter Personalausweise, Bankinformationen, Mitarbeiterverträge und weitere interne Dokumente.

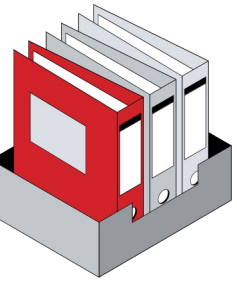
Was hätte man besser machen können?
Der Einsatz eines Security Operations Centers (SOC) ist in der IT-Sicherheit essenziell, da ein SOC die IT-Infrastruktur kontinuierlich überwacht, Bedrohungen in Echtzeit erkennt und sofortige Gegenmaßnahmen ergreift.

Zusätzlich hätte das Unternehmen regelmäßige Vulnerability Assessments durchführen sollen. Diese Bewertungen identifizieren und bewerten Sicherheitslücken in der IT-Umgebung, sodass diese proaktiv behoben werden können, bevor sie von Cyberkriminellen ausgenutzt werden.

Was lernen wir daraus:

Zusätzlich zur Verschlüsselung von Daten setzen Ransomware-Angreifer die Drohung ein, vertrauliche Informationen öffentlich zu machen, falls das geforderte Lösegeld nicht gezahlt wird. Mit dieser Methode erhöhen sie den Druck auf die Opfer, da sie nicht nur um den Verlust ihrer Daten besorgt sind, sondern auch um die Sicherheit ihrer sensiblen Informationen.

Experten empfehlen, das Lösegeld nicht zu zahlen, da es keine Garantie für die Wiederherstellung der Daten gibt.



Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents//6121-DeskCenter-Cactus.PNG

RIEDEL

Wachsamkeit geboten: Hackerangriff führt zu Datendiebstahl bei Bankkunden

22. Juni 2024, in Frankfurt am Main/Hessen

DATENDIEBSTAHL

EINBRUCH

Was ist passiert?
Am 22. Juni 2024 wurde bekannt, dass Hacker die Tochtergesellschaft einer großen deutschen Bank angegriffen haben. Dabei wurden die Daten von zehntausenden Kunden gestohlen, einschließlich Adressen, Geburtsdaten, Kontoinformationen und Steuerdaten. Das betroffene Unternehmen hat seine Kunden informiert und warnt vor E-Mails und Post von unbekannten Absendern. Der genaue Umfang des Angriffs und die Hintergründe sind noch unklar und es wird intensiv an der Aufklärung und Schadensbegrenzung gearbeitet.

Was hätte man besser machen können?
Der Einsatz eines Security Operations Centers (SOC) wäre entscheidend gewesen. Ergänzend dazu hätte ein Security Information and Event Management (SIEM)-System implementiert werden sollen.

Zusätzlich hätte das Unternehmen einen effektiven Incident-Response-Plan implementieren sollen. Ein solcher Plan legt fest, wie auf Sicherheitsvorfälle reagiert wird, einschließlich der Identifikation, Eindämmung, Beseitigung und Wiederherstellung, um Schäden zu minimieren und die Wiederherstellung der normalen Betriebsabläufe zu beschleunigen.

Anzunehmende Schadensfelder:

Was lernen wir daraus:

Ein 100%iger Schutz gegen Cyberangriffe ist nicht möglich, da Angreifer ständig neue Techniken entwickeln und Sicherheitslücken in Systemen ausnutzen. Auch menschliche Fehler, unzureichende Sicherheitsupdates und komplexe IT-Infrastrukturen erhöhen das Risiko.

Dennoch können sich Unternehmen umfangreich schützen, indem kontinuierlich Sicherheitsmaßnahmen aktualisiert und IT-Sicherheitsmaßnahmen umgesetzt werden.

Quellen
https://www.heise.de//news/Cyberattacke-auf-Immobilientochter-der-DZ-Bank-9774310.html
https://www.tagesschau.de/wirtschaft/dz-bank-cyberangriff-100.html

RIEDEL

Ingenieursunternehmen als Opfer einer Ransomwaregruppe gelistet

19. Juni 2024, in Friedberg/Bayern

RANSOMWARE

EINBRUCH

DATENDIEBSTAHL

DATENLECK

Was ist passiert?
Am 19. Juni 2024 listete die Akira-Gruppe ein Ingenieursunternehmen als Opfer auf ihrer Webseite. Die Täter gaben nicht preis, welche Daten sie erlangt haben, sondern drohten damit, 4 GB an internen Daten zu veröffentlichen, falls ihre Forderungen nicht erfüllt werden. Zuvor hatten sie behauptet, 25 GB gestohlen zu haben. Das Unternehmen hat sich bislang nicht öffentlich zu dem Vorfall geäußert.

Was hätte man besser machen können?
Um den Sicherheitsvorfall zu verhindern, hätte das Ingenieursunternehmen regelmäßige Backups, starke Zugangskontrollen, Endpunkt-Schutz und die Verschlüsselung sensibler Daten implementieren sollen.

Zudem wären umfassende Schulungen für das IT-Personal und die Nutzer entscheidend gewesen, um das Bewusstsein für Sicherheitsrisiken zu erhöhen und die Kompetenz im Umgang mit potenziellen Bedrohungen zu stärken.

Was lernen wir daraus:

„Ransomware-as-a-Service“ (RaaS) erfreut sich großer Beliebtheit unter Cyberkriminellen, da es ihnen ermöglicht, Ransomware ohne tiefgehende technische Kenntnisse zu nutzen.

Es handelt sich dabei um ein Geschäftsmodell, bei dem die Einstiegshürden geringer werden und das die Durchführung der Angriffe vereinfacht. Die Anbieter profitieren durch Provisionen und Anteilen an den Lösegeldern, die ihre Kunden einnehmen.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/5872-Lindermayr-Akira.PNG
https://ransomwareattacks.halcyon.ai/attacks/akira-ransomware-strikes-lindermayr-besitz-exfiltrates-25gb-data

RIEDEL

Cyberangriff führt zu Systemausfall im Krankenhaus

17. Juni 2024, in Hausham/Bayern

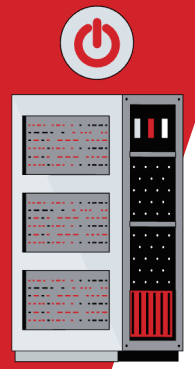
AUSFALL

Was ist passiert?
Am 17. Juni 2024 informierte ein Krankenhaus seine Patienten und später die Öffentlichkeit über einen Cyberangriff, der Teile seiner Systeme lahmlegte. Die Klinik ist nur eingeschränkt erreichbar und der Zugriff auf Daten gestaltet sich schwierig.

Was hätte man besser machen können?
Die Implementierung eines umfassenden Backup-Systems, das regelmäßige Snapshots und Offsite-Backups umfasst, hätte im Fall eines Angriffs eine schnelle Wiederherstellung der Daten ermöglicht.

Ein gut vorbereiteter Incident-Response-Plan hätte geholfen, die Reaktion auf den Angriff zu koordinieren, die Auswirkungen zu minimieren und eine zügige Wiederherstellung der Systeme zu gewährleisten.

Anzunehmende Schadensfelder:



Was lernen wir daraus:

Cyberkriminelle greifen gezielt Unternehmen kritischer Infrastrukturen an, mitunter im Gesundheitswesen, um maximalen Schaden anzurichten. Diese Angriffe können nicht nur finanzielle Verluste verursachen, sondern auch die öffentliche Sicherheit und den Betrieb wesentlicher Dienstleistungen gefährden.

Im Rahmen der NIS2-Richtlinie müssen sämtliche Unternehmen, die eine Verbindung zu kritischen Infrastrukturen (KRITIS) aufweisen, strenge Cybersecurity-Maßnahmen umsetzen, um das IT-Sicherheitsniveau zu steigern.

RIEDEL

Quellen
https://www.merkur.de/lokales/region-miesbach/hausham-ort74880/hackerangriff-auf-akrankenhaus-av-krisenstab-eingerichtet-93135734.html

Hacker verkaufen angeblich sensible Daten eines IT-Dienstleisters

16. Juni 2024, in Berlin/Berlin

RANSOMWARE

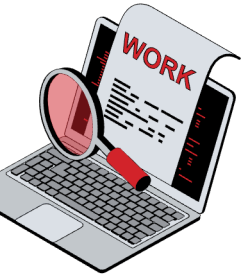
DATENPANNE

DATENDIEBSTAHL

Was ist passiert?
Cyberkriminelle der Rhysida-Gruppe listeten einen IT-Dienstleister als Opfer einer Ransomware-Attacke auf ihrer Webseite. Bis zum aktuellen Zeitpunkt wurden keine sensiblen Daten veröffentlicht. Stattdessen behauptet die Gruppe, die Daten an einen Einzelkäufer verkauft zu haben. Ob das Unternehmen ein Lösegeld gezahlt hat oder ob ein anderer Käufer beteiligt war, bleibt unklar.

Was hätte man besser machen können?
Um den Sicherheitsvorfall zu verhindern, hätte der IT-Dienstleister durch den Einsatz eines SOCs und eines SIEM-Systems frühzeitig verdächtige Aktivitäten erkennen und schneller reagieren können. Ein EDR-System hätte dabei geholfen, Angriffe auf Endgeräten zu isolieren und einzudämmen.

Zudem hätten fortlaufende Bedrohungsanalysen und automatisierte Reaktionen die Exfiltration von Daten möglicherweise verhindern können.



Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6120-CETOS-Rhysida.PNG

Was lernen wir daraus:

Hacker haben unterschiedliche Motive: Dazu gehören das Interesse an der Beschaffung von Daten für spezifische Zwecke wie Erpressung oder Spionage, die Verwirklichung schneller finanzieller Gewinne durch Lösegeldforderungen oder die Erzielung von Einnahmen durch den Verkauf gestohlener Daten im Darknet. Aber auch politische oder ideologische Beweggründe können eine Rolle spielen.

RIEDEL

Ransomware-Angreifer fordern Lösegeld von Wasseraufbereitungsunternehmen

12. Juni 2024, in Fellbach/Baden-Württemberg

RANSOMWARE

DATENPANNE

DATENDIEBSTAHL

Was ist passiert?
Cyberkriminelle der PLAY-Gruppe behaupteten, ein Wasseraufbereitungsunternehmen erfolgreich angegriffen und dabei Personaldaten, Kundendokumente, Budgeteinteilungen, Verträge, Steuerabrechnungen und weitere interne Finanzdokumente erlangt zu haben. Sie drohten mit der Veröffentlichung der Daten, falls ihre Forderungen nicht erfüllt würden. Zum aktuellen Zeitpunkt ist der Eintrag auf der Webseite der Hacker nicht mehr verfügbar, und es bleibt unklar, ob die Forderungen erfüllt wurden oder ob die Behauptungen falsch waren.

Was hätte man besser machen können?
Um den Sicherheitsvorfall zu verhindern, hätte das Wasseraufbereitungsunternehmen ein SIEM-System (Security Information and Event Management) implementieren können. Dies hätte eine schnellere Reaktion auf potenzielle Bedrohungen ermöglicht und dazu beigetragen, unbefugte Zugriffe auf Personaldaten, Kundendokumente, Budgeteinteilungen, Verträge, Steuerabrechnungen und weitere interne Finanzdokumente zu verhindern. Durch die Integration eines SIEM-Systems hätte das Unternehmen seine Sicherheitslage erheblich verbessern und das Risiko eines erfolgreichen Angriffs minimieren können.

Anzunehmende Schadensfelder:

Was lernen wir daraus:

Unternehmen, die von der NIS2-Richtlinie betroffen sind, müssen jetzt stärker auf ihre IT-Sicherheit achten. Sie sollten klare Richtlinien für den Umgang mit Risiken und Informationen aufstellen, Maßnahmen zur Vorbeugung und Reaktion auf Sicherheitsvorfälle ergreifen und sicherstellen, dass ihre Systeme im Ernstfall schnell wiederhergestellt werden können. Außerdem sind sichere Passwörter, Verschlüsselung und der Schutz der gesamten Lieferkette wichtiger denn je. Dabei geht es darum, ihre Sicherheitsvorkehrungen ständig zu überprüfen und anzupassen.

RIEDEL

Quellen
https://www.security-incidents.de/assets/img/incidents/6096-Antech_Guetling-Play.png

Regierungswebseiten durch DDoS-Attacken lahmgelegt

11. Juni 2024, in Köln/Nordrhein-Westfalen

DDoS

AUSFALL

Was ist passiert?
Die prorussische Hackergruppe NoName057(16) hat eine DDoS-Attacke gegen eine deutsche Bundesbehörde und das Innenministerium durchgeführt. Der Angriff am 11. Juni 2024 wurde angeblich als Reaktion auf den Besuch des ukrainischen Präsidenten in Deutschland initiiert. Die Website der Behörde fiel dabei einen Tag lang aus.

Was hätte man besser machen können?
Der Einsatz einer Security Orchestration, Automation, and Response (SOAR)-Plattform wäre essenziell gewesen. SOAR-Plattformen automatisieren und koordinieren die Reaktion auf Sicherheitsvorfälle, verbessern die Effizienz und verkürzen die Reaktionszeit durch die Integration verschiedener Sicherheitstools und -prozesse.

Zusätzlich hätte die Behörde DDoS Protection einsetzen sollen. Diese Lösung bietet umfassenden Schutz gegen DDoS-Angriffe, indem sie den Datenverkehr analysiert, schädliche Anfragen filtert und legitimen Traffic ungestört passieren lässt.

Anzunehmende Schadensfelder:

Quellen
https://thecyberexpress.com/noname-ransomware-attack-germany/

Was lernen wir daraus:

Ein politisch motivierter Cyberangriff, auch "Hacktivismus" genannt, wird durchgeführt, um politische oder soziale Ziele zu erreichen und ein Zeichen zu setzen.

Hacker greifen Systeme von Regierungen, Unternehmen oder Organisationen an, um Daten zu stehlen, Systeme lahmzulegen oder Propaganda zu verbreiten. Diese Angriffe sollen Aufmerksamkeit erregen, politische Veränderungen beeinflussen oder die öffentliche Meinung manipulieren.

RIEDEL

Sicherheitslücken in BundID: Verwaltungsdienste zeitweise abgeschaltet

9. Juni 2024, in Osnabrück/Niedersachsen

SICHERHEITSLÜCKE

KONFIGURATIONSFEHLER

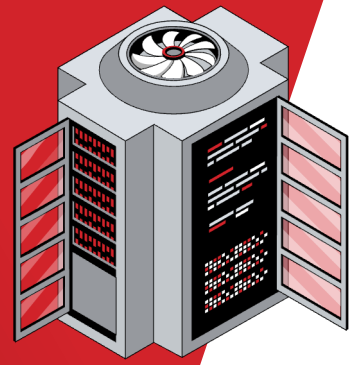
AUSFALL

Was ist passiert?

Anfang Juni 2024 entdeckte eine Sicherheitsforscherin eine Schwachstelle in der Identifikationssoftware BundID. Diese Lücke ermöglichte es, BundID-Logins auf fremden Webseiten anzubieten, was potenziell das Vertrauen der Nutzer missbrauchen könnte, um sensible Daten zu erlangen. Nachdem die Forscherin die Fehlkonfiguration in der Software öffentlich machte, wurden bis zum 9. Juni zahlreiche Verwaltungsdienste vorübergehend abgeschaltet und die Lücke geschlossen. Am 17. Juni entdeckte sie eine weitere Schwachstelle, die ebenfalls am 18. Juni zu einer vorübergehenden Abschaltung zahlreicher Verwaltungsdienste führte. Etwa 300 Kommunen waren betroffen.

Was hätte man besser machen können?

Vulnerability Scanner hätten die IT-Systeme regelmäßig auf Schwachstellen geprüft, wodurch Probleme frühzeitig erkannt und behoben werden könnten.



Was lernen wir daraus:

Die schnelle Reaktion, die zur vorübergehenden Abschaltung der betroffenen Verwaltungsdienste führte, unterstreicht die Notwendigkeit, auf Sicherheitsbedrohungen schnell und effektiv zu reagieren.

Dennoch zeigen die wiederholten Sicherheitslücken und die dadurch verursachten Störungen, dass es entscheidend ist, nicht nur bestehende Schwachstellen zu beheben, sondern auch präventive Maßnahmen zu stärken, um künftige Angriffe und Sicherheitsrisiken zu minimieren.

Anzunehmende Schadensfelder:

Quellen

https://lilithwittmann.medium.com/bundid-eine-digitale-identit%C3%A4t-schafft-falsches-vertrauen-4a1d0a3faa03

https://www.golem.de/news/sicherheitsluecke-bundid-verwaltungsdienste-von-300-kommunen-wiederholt-offline-2406-186211.html

RIEDEL

Cyberangriff verschlüsselt Systeme und stört digitale Dienste erheblich

5. Juni 2024, in Meschede/Nordrhein-Westfallen

RANSOMWARE

AUSFALL

Was ist passiert?
Unbekannte führten einen Cyberangriff auf eine Abtei durch und verschlüsselten deren Systeme. Infolge des Angriffs waren digitale Dienste wie E-Mail-Versand und Kursanmeldungen vorübergehend eingeschränkt oder nicht verfügbar. Zudem kam es zu Verzögerungen im Rechnungswesen.

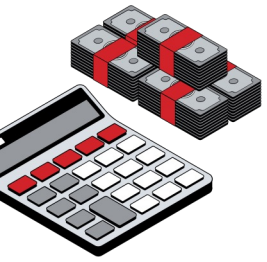
Was hätte man besser machen können?
Ein SIEM-System hätten durch kontinuierliche Überwachung und Analyse von Sicherheitsdaten frühzeitig Anomalien erkennen können. Mit einer EDR-Lösung hätten verdächtige Aktivitäten auf Endgeräten schnell identifiziert und gestoppt werden können.

Ergänzend hätten regelmäßige Vulnerability Assessments potenzielle Sicherheitslücken aufgedeckt und geschlossen, um das Risiko eines erfolgreichen Angriffs zu minimieren.

Was lernen wir daraus:

Schadsoftware kann sich extrem schnell ausbreiten und gravierende Schäden verursachen, wenn sie nicht sofort gestoppt wird. Daher ist es entscheidend, bei einem Cyberangriff umgehend zu handeln und betroffene IT-Systeme sofort abzuschalten, um die Weiterverbreitung des Schadcodes zu verhindern.

Schnelles und effektives Handeln schützt nicht nur die IT-Infrastruktur, sondern minimiert auch die operativen und finanziellen Auswirkungen eines Angriffs.



Anzunehmende Schadensfelder:

Quellen
https://koenigsmuenster.de/hackerangriff-in-der-abtei/
https://www.wp.de/staedte/meschede-und-umland/article242502000/Meschede-Abtei-Koenigsmuenster-von-Hacker-Angriff-ueberrascht.html

RIEDEL

Datenleck: Tausende Bewerberdaten öffentlich zugänglich

4. Juni 2024, in Berlin/Berlin

KONFIGURATIONSFEHLER

DATENPANNE

Was ist passiert?
Eine politische Partei entdeckte ein schwerwiegendes IT-Sicherheitsproblem, bei dem über 4.870 Bewerber-Namen auf ihrer Online-Plattform sichtbar wurden. Der Vorfall, der durch eine Fehlkonfiguration verursacht wurde, führte zu einem erheblichen Verstoß gegen die DSGVO, da viele Bewerber ihre sensiblen Daten öffentlich einsehen konnten. Die Plattform wurde sofort in den Wartungsmodus versetzt. Laut einer Erklärung sind 3.500 der Bewerber betroffen und die Behörden wurden informiert.

Was hätte man besser machen können?
Um einen Sicherheitsvorfall zu vermeiden, wäre es notwendig gewesen, die Server und Datenbanken sicher zu konfigurieren. Dazu hätten regelmäßige Sicherheitsprüfungen, strikte Zugangskontrollen sowie die Verschlüsselung sensibler Daten im Ruhezustand und während der Übertragung gehört.

Zudem wäre eine umfassende Protokollierung und Echtzeit-Monitoring erforderlich gewesen, um unbefugte Zugriffe umgehend zu erkennen.

Was lernen wir daraus:

Es gibt eine Vielzahl von Vorschriften und Standards, die Unternehmen, abhängig von ihrer Branche und ihrem geografischen Standort, kennen müssen.

Die Einhaltung von Vorschriften wie der DSGVO, NIS2-Richtlinie und ISO/IEC 27001 ist entscheidend für den Schutz und die Sicherheit von Daten. Unternehmen sollten sicherstellen, dass sie alle relevanten gesetzlichen Anforderungen erfüllen und geeignete Compliance-Management-Systeme implementieren.

Anzunehmende Schadensfelder:

Quellen
https://www.heise.de/news/CDU-Liste-von-Bewerbern-stand-frei-zugaenglich-im-Netz-9747811.html
https://www.heise.de//news/CDU-Bewerber-Datenleck-Betroffene-sollen-zeitnah-informiert-werden-9758571.html

RIEDEL

Ransomwaregruppe stiehlt 24 GB sensible Daten

4. Juni 2024, in Altdorf/Bayern

DATENDIEBSTAHL

EINBRUCH

Was ist passiert?
Am 4. Juni 2024 behauptete die Akira-Ransomwaregruppe, ein deutsches Unternehmen gehackt und 24 GB an Daten gestohlen zu haben. Zu den gestohlenen Daten gehören Kundendaten, Non-Disclosure-Agreements, Finanzunterlagen und personenbezogene Daten von Mitarbeitenden. Die Webseite des Unternehmens zeigte jedoch keine sichtbaren Einschränkungen.

Was hätte man besser machen können?
Regelmäßige Schwachstellen-Scans hätten dazu beigetragen, Sicherheitslücken in der IT-Infrastruktur des Unternehmens frühzeitig zu identifizieren und zu beheben. Durch das regelmäßige Scannen nach Schwachstellen und das sofortige Schließen entdeckter Lücken wäre es schwieriger für Angreifer gewesen, in das System einzudringen und Daten zu stehlen.

Was lernen wir daraus:

Begrifflichkeiten aus dem Bereich der IT-Sicherheit wie

- ✓ **SIEM & SOC**
- ✓ **XDR**
- ✓ **EDR**
- ✓ **SOAR**
- ✓ **(D)DoS Protection**
- ✓ **Next Generation Firewalls**
- ✓ **SD-WAN**
- ✓ **SASE**

sind keine leeren Cybersecurity-Versprechen. Sie tragen präventiv dazu bei, Unternehmen vor Cyberangriffen zu schützen und potenziellen Bedrohungen stets einen Schritt voraus zu sein. Mit diesen Technologien und Strategien wird die Resilienz und Sicherheit von IT-Infrastrukturen erheblich erhöht.

Anzunehmende Schadensfelder:

Quellen
https://thecyberexpress.com/akira-ransomware-claims-ccyberattack-e-t-a/

RIEDEL

Ransomware: Transportunternehmen auf Darknet-Opferliste

4. Juni 2024, in Remscheid/Nordrhein-Westfalen

RANSOMWARE

EINBRUCH

Was ist passiert?
Cyberkriminelle griffen ein Transportunternehmen mit Ransomware an. Die Gruppe Arcus Media verschlüsselte sensible Daten und setzte das Unternehmen auf ihre Opferliste im Darknet. Details zum Angriff, zur Menge der gestohlenen Daten und zur Höhe des Lösegelds sind noch unklar. Ob das Unternehmen ein Lösegeld zahlte, ist unbekannt.

Was hätte man besser machen können?
Regelmäßige Backups hätten sicherstellen können, dass alle wichtigen Daten an mehreren, voneinander getrennten Orten gespeichert und im Falle eines Angriffs schnell wiederhergestellt werden können. Dadurch hätte das Unternehmen den Schaden minimieren und den Betrieb schneller wieder aufnehmen können, ohne auf Lösegeldforderungen eingehen zu müssen.

Zusätzlich wären regelmäßige Schulungen für Mitarbeiter essenziell gewesen.

Was lernen wir daraus:

Viele Ransomwaregruppen setzen die Methode der doppelten Erpressung ein. Dabei verschlüsseln die Angreifer nicht nur die Daten des Opfers und verlangen ein Lösegeld für deren Wiederherstellung, sondern drohen zusätzlich damit, vertrauliche Informationen zu veröffentlichen oder weiterzuverbreiten. Diese Taktik dient dazu, den Druck auf die Opfer zu erhöhen und die Wahrscheinlichkeit zu steigern, dass sie den geforderten Betrag zahlen.

Anzunehmende Schadensfelder:

Quellen
https://ransomwareattacks.halcyon.ai/attacks/arcus-media-ransomware-strikes-langescheid-gbr
https://themoloch.com/infosec/new-threat-actor-drop-arcus-media/

RIEDEL

EINBRUCH

AUSFALL

Cyberattacke eine Woche vor Europawahl trifft deutsche Partei hart

1. Juni 2024, in Berlin/Berlin

Was ist passiert?
Eine politische Partei erlebte kurz vor der Europawahl einen Cyberangriff. Die Partei stellte Teile ihrer IT-Infrastruktur vorübergehend offline, während die Website weiterhin funktionierte. Die Täter hatten zwei Wochen Zugriff auf das Netzwerk durch eine Sicherheitslücke in der verwendeten Software. Details zum Angriff, zu den Verantwortlichen und zu möglichen Datenverlusten sind noch unklar. Die Partei arbeitet mit Sicherheitsbehörden und Experten zusammen.

Was hätte man besser machen können?
Um den Sicherheitsvorfall zu verhindern, hätte die politische Partei ein Security Operations Center (SOC) einrichten sollen. Ein SOC erkennt Bedrohungen in Echtzeit und ermöglicht dadurch einen schnelleren Eingriff.

Regelmäßige Sicherheitsüberprüfungen, die Verschlüsselung von Zugangsdaten, sowie eine schnelle Reaktion durch ein Incident-Response-Team wären wichtig gewesen.

Was lernen wir daraus:

Hacktivisten sind ideologisch motivierte Akteure, die Cyberangriffe als Mittel nutzen, um politische, soziale oder ökologische Botschaften zu verbreiten. Ihre Angriffe zielen oft darauf ab, Aufmerksamkeit auf eine bestimmte Sache zu lenken, Missstände anzuprangern oder gegen Organisationen vorzugehen, die sie als ungerecht betrachten.

Anzunehmende Schadensfelder:

Quellen
https://www.spiegel.de/politik/deutschland/cdu-cyber-angriff-auf-parteizentrale-verfassungsschutz-eingeschaltet-a-b47d65ef-999b-4ded-a124-4f8cd325c40b
https://www.zeit.de/politik/deutschland/2024-06/cyber-angriff-cdu-verfassungsschutz

RIEDEL

MAI 2024

SECURITY INCIDENTS GERMANY

RIEDEL

DATENDIEBSTAHL

RAMSOMWARE

Ransomware-Attacke auf große Bäckereikette: Sensible Daten gestohlen und veröffentlicht

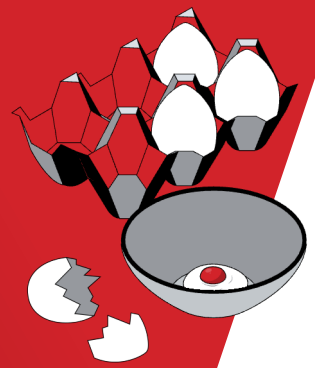
31. Mai 2024, in Gröditz/Sachsen

Was ist passiert?
Eine Bäckerei mit mehreren Filialen wurde von der Ransomwaregruppe "Cloak" angegriffen. Die Hacker stahlen und veröffentlichten sensible Informationen, einschließlich Finanz- und Versicherungsdaten.

Was hätte man besser machen können?
Um den Sicherheitsvorfall zu verhindern, hätte die Bäckerei ein Security Operations Center (SOC) einsetzen können, 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.

Anzunehmende Schadensfelder:



Was lernen wir daraus:

Ein besorgniserregendes Phänomen ist die Demokratisierung von Cyberkriminalität. Wo früher technisches Fachwissen und erhebliche Ressourcen für Cyberangriffe erforderlich waren, können heute auch technisch weniger versierte Personen mit nur wenigen Klicks hochentwickelte Malware aus dem Darknet erwerben oder Phishing-Kampagnen starten. Diese Entwicklungen erhöhen den Druck auf Unternehmen, ihre Sicherheitsstrategien anzupassen und kontinuierlich weiterzuentwickeln.

Quellen
https://www.breachsense.com/breaches/b%C3%A4ckerei-raddatz-data-breach/
https://www.security-incidents.de/assets/img/incidents/5888-ransomlook-raddatz.png

RIEDEL

DDoS-Angriff stört Ticketkäufe auf Webseite und App

29. Mai 2024, in Hamburg/Hamburg

DDoS

AUSFALL

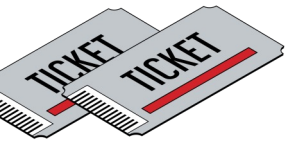
Was ist passiert?
Hacker griffen einen Verkehrsverbund an und legten dessen Webseite sowie App zeitweise lahm. An beiden Tagen war es unmöglich, Fahrkarten online zu erwerben. Die App zeigte eine Fehlermeldung an, jedoch konnten Tickets ohne Anmeldung gekauft werden. Der Angriff deutet auf einen DDoS-Angriff hin.

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

Was lernen wir daraus:

Bei einer DDoS-Attacke wird ein Netzwerk, Server oder Dienst mit einer überwältigenden Menge an Datenverkehr überflutet, um dessen Funktion zu stören oder komplett lahmzulegen. Solche Angriffe können verheerende Auswirkungen auf die Geschäftskontinuität haben und werden oft als Druckmittel bei Erpressungen eingesetzt.

Anzunehmende Schadensfelder:



Quellen
https://www.ndr.de/nachrichten/hamburg/Hackerangriff-auf-HVV-Internetseite-und-App-waren-betroffen,hvv770.html
https://www.mopo.de/hamburg/hackerangriff-auf-den-hvv-ticketkauf-im-internet-lahmgelegt/

RIEDEL

Webseiten von Polizei und Regierung durch Hackerangriff lahmgelegt

23. Mai 2024, in Schwerin/Mecklenburg-Vorpommern

DDoS

AUSFALL

Was ist passiert?
Hacker griffen die Webseiten mehrerer Landesbehörden in Mecklenburg-Vorpommern an, darunter die Seiten der Regierung und der Polizei. Der Angriff führte dazu, dass die Webseiten vorübergehend nicht erreichbar waren. Die genauen Details des Angriffs, einschließlich der verwendeten Angriffsmethoden und der möglichen Auswirkungen auf die Sicherheit, sind noch unklar. Die betroffenen Behörden arbeiten an der Wiederherstellung der Dienste und der Sicherheitsüberprüfung.

Was hätte man besser machen können?
Die Landesbehörden in Mecklenburg-Vorpommern hätten den Angriff durch den Einsatz zusätzlicher DDoS-Schutzdienste und einen umfassenderen Incident-Response-Plan besser bewältigen können.

Zudem hätte Threat Intelligence zur proaktiven Überwachung potenzieller Bedrohungen und eine offenere Kommunikation über IT-Sicherheitsmaßnahmen geholfen.

Was lernen wir daraus:

Eine erfolgreiche Cybersicherheitsstrategie beginnt mit einem ganzheitlichen Ansatz, der alle Aspekte der IT-Infrastruktur einer Organisation abdeckt. Dazu gehört:

- **Risikobewertung**: Organisationen sollten regelmäßig Sicherheitsaudits und Risikobewertungen durchführen, um Schwachstellen in ihren Systemen zu identifizieren und zu priorisieren.
- **Sicherheitsrichtlinien**: Die Entwicklung und Durchsetzung klarer Richtlinien und Verfahren für den Umgang mit sensiblen Daten, Zugriffsrechten und IT-Sicherheitsvorfällen.
- **Notfallpläne**: Organisationen sollten über detaillierte Incident-Response-Pläne verfügen, die regelmäßig getestet und aktualisiert werden. Dazu gehört auch ein Plan zur Sicherstellung der Geschäftskontinuität im Falle eines Angriffs.

Anzunehmende Schadensfelder:

Quellen
https://www.welt.de/regionales/mecklenburg-vorpommern/article251653642/Hackerangriff-auf-Webseiten-von-Regierung-und-Polizei.html

RIEDEL

Cyberangriff legt Kommunikation und Produktion eines Anlagenbauers lahm

22. Mai 2024, in Emmendingen/Baden-Württemberg

AUSFALL

Was ist passiert?
Ein Anlagenbauer wurde Ziel einer Cyberattacke, die zu einem vorübergehenden Produktionsstopp führte. Die Angreifer verschlüsselten Unternehmensdaten, was die Produktion beeinträchtigte. Der genaue Umfang des Schadens und die Art des Angriffs sind noch nicht vollständig geklärt. Das Unternehmen arbeitet an der Wiederherstellung der Systeme und an der Verbesserung der IT-Sicherheit.

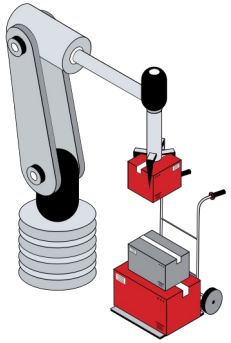
Was hätte man besser machen können?
Regelmäßige Backups der Unternehmensdaten hätten sicherstellen können, dass im Falle einer Cyberattacke die verschlüsselten Daten schnell wiederhergestellt werden können. Diese Backups sollten an mehreren, voneinander getrennten Orten gespeichert werden, um die Verfügbarkeit und Integrität der Daten zu gewährleisten.

Ein Incident-Response-Plan mit klaren Schritten hätte dem IT-Team ermöglicht, schnell auf den Angriff zu reagieren und den Schaden zu minimieren.

Was lernen wir daraus:

Wenn Cyberkriminelle Unternehmensdaten stehlen, riskieren Firmen nicht nur finanzielle Einbußen, sondern auch Betriebsunterbrechungen. Die Wiederherstellung von Daten und die Implementierung neuer Sicherheitsmaßnahmen können den Betrieb erheblich stören.

Als langfristige Auswirkung entsteht die Notwendigkeit, umfassende Sicherheitsstrategien zu etablieren und zu stärken.



Anzunehmende Schadensfelder:

Quellen
https://www.badische-zeitung.de/cyberattacke-auf-wehrle-werk-ag
https://youtu.be/xuHrftoNc3o

RIEDEL

AUSFALL

Massive technische Störung führt zu landesweiten Ausfällen bei Internet und Telefon

21. Mai 2024, in Bonn/Nordrhein-Westfalen

Was ist passiert?
Eine technische Störung bei einem großen Telekommunikationsanbieter führte zu deutschlandweiten Beeinträchtigungen bei Festnetz und Internet. Die Störung begann am frühen Morgen und betraf auch Kunden anderer Anbieter, da der Telekommunikationsanbieter als Dienstleister für diese fungiert. Die Ausfälle hielten den gesamten Tag über an, wobei einige Betroffene die Störungen am späten Morgen als beendet meldeten. Auch ein Streaming-Dienst des Anbieters war betroffen.

Was hätte man besser machen können?
Echtzeit-Monitoring hätte die kontinuierliche Überwachung der Netzwerksysteme ermöglicht, um technische Probleme frühzeitig zu erkennen und sofortige Maßnahmen zu ergreifen. Dies hätte dazu beigetragen, die Störung schnell zu identifizieren und zu beheben, bevor sie sich auf eine große Anzahl von Kunden auswirkt.

Eine Incident-Response-Strategie hätte klare Schritte zur Identifikation, Eindämmung, Beseitigung und Wiederherstellung bei Sicherheitsvorfällen festgelegt.

Was lernen wir daraus:

Cyberkriminelle nutzen häufig Zero-Day-Exploits, also Schwachstellen in Software, die vom Hersteller noch nicht entdeckt oder behoben wurden.

Diese Sicherheitslücken ermöglichen es Angreifern, Systeme zu kompromittieren, bevor ein Patch verfügbar ist. Solche Exploits werden oft im Darknet-Markt gehandelt und können schwerwiegende Schäden verursachen.

Anzunehmende Schadensfelder:

Quellen
https://hilfe.o2online.de/dsl-kabel-glasfaser-router-software-internet-telefonie-34/beendet-ausfallinfo-21-mai-2024-festnetzanschluesse-teilweise-gestoert-635094
https://www.chip.de/news/Massive-Stoerungen-bei-Telekom-und-o2-Tausende-Nutzer-berichten-ueber-Probleme_185282287.html

RIEDEL

Hackerangriff auf Flughafen Hamburg: Externes Überwachungssystem betroffen

21. Mai 2024, in Hamburg/Hamburg

SUPPLY CHAIN

EINBRUCH

Was ist passiert?
Am 19. Mai 2024 gab die Hackergruppe Just Evil/Kill Milk bekannt, den Flughafen Hamburg angegriffen zu haben. Der Flughafen bestätigte den Vorfall und stellte klar, dass das kompromittierte System ein extern verwaltetes Überwachungssystem für Wachgänge war. Kritische Infrastruktur des Flughafens blieb unberührt.

Was hätte man besser machen können?
Um den Sicherheitsvorfall zu verhindern, hätte der Flughafen Hamburg ein Security Operations Center (SOC) einrichten können, das kontinuierlich die IT-Infrastruktur überwacht. Dies hätte ermöglicht, ungewöhnliche Aktivitäten frühzeitig zu identifizieren.

Zusätzlich hätte die Implementierung von Multi-Faktor-Authentifizierung (MFA) die Sicherheit erhöht. MFA verlangt von Benutzern, sich durch mindestens zwei verschiedene Verifizierungsfaktoren zu authentifizieren, bevor sie Zugriff auf das System erhalten

Was lernen wir daraus:

Unternehmen müssen im Rahmen der NIS2-Richtlinie diverse Cybersecurity-Maßnahmen ergreifen, um ihre IT-Infrastruktur und Netzwerke zu schützen. Dazu gehören Richtlinien für Risikomanagement und Informationssicherheit sowie Maßnahmen zur Prävention, Erkennung und Bewältigung von Sicherheitsvorfällen. Auch die Geschäftskontinuität muss durch Backup-Management und Desaster Recovery sichergestellt werden. Verschlüsselung und Zugangskontrollen wie Multi-Faktor-Authentifizierung sind essenziell, ebenso wie sichere Kommunikation und die Absicherung der Lieferkette.

Anzunehmende Schadensfelder:

Quellen
https://www.csoonline.com/de/a/flughafen-hamburg-wehrt-hackerangriff-ab,3681367
https://www.golem.de/news/ueberwachungssystem-infiltriert-cyberangriff-trifft-flughafen-hamburg-2405-185322.html

RIEDEL

Ransomware-Angriff auf Klebstoffhersteller

17. Mai 2024, in Münster/Nordrhein-Westfalen

RANSOMWARE

DATENPANNE

DATENDIEBSTAHL

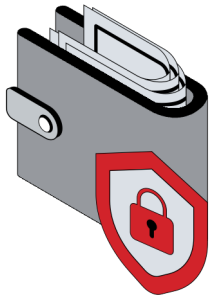
DATENLECK

Was ist passiert?
Cyberkriminelle der Gruppe Medusa bekannten sich zu einer Ransomware-Attacke auf einen deutschen Hersteller für Klebe- und Dichtstoffe. Die Täter behaupteten, 175,5 GB an hochsensiblen Daten erlangt zu haben. Nach Ablauf der Frist für ihre Forderungen veröffentlichten sie die Daten, die unter anderem interne Excel-Tabellen, Reisepässe und Geheimhaltungsvereinbarungen umfassen.

Was hätte man besser machen können?
Das Unternehmen hätte den Angriff früher entdeckt, wenn es ein Managed-SIEM und ein rund um die Uhr besetztes Security Operations Center (SOC) eingesetzt hätte. Eine schnellere Reaktion hätte möglicherweise verhindert, dass sensible Unternehmensdaten entwendet werden.

Was lernen wir daraus:

Cyberkriminelle sind oft finanziell motiviert und nutzen das Internet, um illegale Aktivitäten durchzuführen. Ihr Hauptziel ist es, Daten zu stehlen, die entweder direkt zu Geld gemacht oder für Erpressungen genutzt werden können. Ein gängiges Vorgehen ist der Einsatz von Ransomware, bei dem Daten verschlüsselt und ein Lösegeld für deren Entschlüsselung gefordert wird.



Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6074-Weicon-Medusa.PNG

RIEDEL

Fehler bei Datenmigration führt zur unwiderruflichen Löschung aller Cloud-Daten

16. Mai 2024, in Nürnberg/Bayern

MENSCHLICHES VERSAGEN

DATENVERLUST

Was ist passiert?
Ein Hosting-Provider informierte am 16. Mai 2024 einen Kunden, dass bei einer Migration alle Daten seiner Nextcloud gelöscht wurden. Ein Zusammenspiel aus menschlichem Versagen und automatisierten Säuberungs-Tasks führte zur Löschung aller Kundendaten und Backups, ohne Möglichkeit zur Wiederherstellung. Die Cloud wurde deaktiviert, um weitere Löschungen zu verhindern. Der Kunde wurde angewiesen, Daten aus Synchronisationsordnern anderswo zu sichern und sich wegen der nächsten Schritte beim Provider zu melden. Benutzer und Kalender seien nicht betroffen.

Was hätte man besser machen können?
Um den Sicherheitsvorfall zu verhindern, hätte das Unternehmen regelmäßige, mehrstufige Backups der Daten an mehreren, voneinander getrennten Speicherorten durchführen sollen. Diese Backups sollten sowohl lokal als auch in verschiedenen Cloud-Diensten gespeichert werden, um sicherzustellen, dass selbst bei einem kompletten Ausfall eines Systems die Daten noch wiederhergestellt werden können.

Zusätzlich wären umfassende Schulungen für das IT-Personal entscheidend gewesen.

Anzunehmende Schadensfelder:

Was lernen wir daraus:

- **Backup-Strategien überprüfen:** Regelmäßige, isolierte Backups sind entscheidend, um Datenverluste durch menschliches Versagen oder automatisierte Fehler zu vermeiden.
- **Fehlervermeidung bei Migrationen:** Sorgfältige Planung und Tests sind notwendig, um Migrationen sicher durchzuführen und Datenverlust zu verhindern.
- **Schnelles Krisenmanagement:** Bei Vorfällen sofortige Maßnahmen ergreifen, wie Deaktivierung von Systemen zur Verhinderung weiterer Schäden und klare Kommunikation mit Kunden.
- **Datenmanagement optimieren:** Sicherstellen, dass Synchronisationsordner regelmäßig gesichert werden und nicht nur auf zentrale Backups vertrauen.

Quellen
https://www.security-incidents.de/assets/img/incidents/5231-netways-infomail.png

RIEDEL

Ransomware-Angriff: Daten der Hochschule seit 2010 betroffen

16. Mai 2024, in Wiesbaden/Hessen

RANSOMWARE

DATENPANNE

DATENDIEBSTAHL

Was ist passiert?
Cyberkriminelle führten einen Ransomware-Angriff auf eine Hochschule durch und stahlen dabei personenbezogene Daten. Zu den erbeuteten Informationen gehören Namen, Adressen, E-Mail-Adressen, Bilder, Telefonnummern und Fahrzeug-Kennzeichen. Es besteht die Möglichkeit, dass auch Steuernummern, Bankverbindungen und Gesundheitsdaten betroffen sind. Die Daten reichen bis ins Jahr 2010 zurück. Die betroffenen Systeme wurden abgeschaltet und vom Netz getrennt.

Was hätte man besser machen können?
Ein Security Operations Center (SOC) hätte rund um die Uhr Bedrohungen überwachen und sofort auf Sicherheitsvorfälle reagieren können.

Was lernen wir daraus:

Während große Unternehmen und Organisationen häufig Ziel von Ransomware-Angriffen sind, geraten auch immer häufiger Universitäten und Hochschulen ins Visier von Cyberkriminellen.

Bildungseinrichtungen sind attraktive Ziele, da sie zum einen über persönliche Daten verfügen und zum anderen Zugriff auf wertvolle Forschungsergebnisse haben.

Anzunehmende Schadensfelder:

Quellen
https://www.presseportal.de/blaulicht/pm/103085/5780955
https://www.golem.de/news/daten-abgeflossen-cyberangriff-trifft-hessische-polizeihochschule-2405-185202.html

RIEDEL

Ransomware-Angriff: Produktion gestoppt und Daten veröffentlicht

11. Mai 2024, in Alpen/Nordrhein-Westfalen

RANSOMWARE

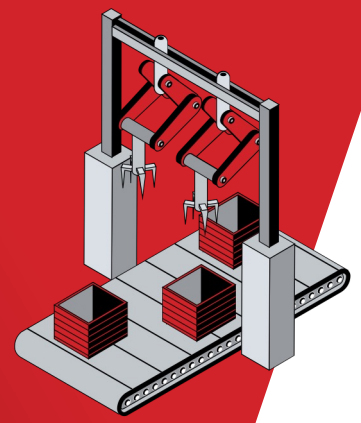
EINBRUCH

AUSFALL

Was ist passiert?
Ein Landtechnik-Spezialist wurde vermutlich mit Ransomware angegriffen. Die Hacker legten die IT-Systeme des Unternehmens weltweit lahm, was zu Produktionsstillständen und Bürobeeinträchtigungen führte. Das Unternehmen schaltete die Systeme ab und engagierte externe IT-Experten zur Analyse. Es ist unklar, ob Kundendaten betroffen sind. Später bekannte sich die Ransomwaregruppe 8Base zu dem Angriff und behauptete, vertrauliche Informationen veröffentlicht zu haben.

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.

Zudem hätten regelmäßige Backups und deren sichere Speicherung geholfen, im Falle eines Angriffs schnell wiederhergestellt zu werden.



Was lernen wir daraus:

Sobald ein Unternehmen angegriffen wurde, sind oft hohe Kosten für Wiederherstellung und Sicherheitsverbesserungen erforderlich.

Präventive Investitionen in umfassende IT-Sicherheitslösungen helfen jedoch, potenzielle Angriffe zu vermeiden und sowohl finanzielle als auch operationale Schäden erheblich zu reduzieren.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/5207-Lemken-8Base.PNG
https://lemken.com/de-de/lemken-aktuelles/landtechnik-news/detail/lemken-von-cyberattacke-betroffen

RIEDEL

Angreifer drohen mit Veröffentlichung von 18 GB Daten nach Ransomware-Angriff

15. Mai 2024, in Repperndorf/Bayern

RANSOMWARE

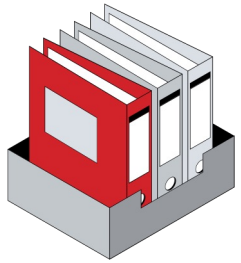
EINBRUCH

DATENDIEBSTAHL

Was ist passiert?
Cyberkriminelle der Ra Group erklärten eine Winzergemeinschaft im Darknet als Ransomware-Opfer und behaupteten, 18 GB an sensiblen Informationen erlangt zu haben, einschließlich finanzieller, Kunden-, Rechts- und Personaldaten. Die Angreifer drohen mit der Veröffentlichung der Daten, falls das Unternehmen ihre Forderungen nicht innerhalb einer gesetzten Frist erfüllt.

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.

Zudem ist Echtzeit-Monitoring unerlässlich. Durch kontinuierliche Überwachung der Systeme können Bedrohungen sofort erkannt und entsprechende Gegenmaßnahmen eingeleitet werden, um Angriffe abzuwehren und Schäden zu minimieren.



Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6040-GWF_Frankenwein-Ra_Group.png

Was lernen wir daraus:

Um Risiken von Cyberangriffen zu minimieren, sollten Unternehmen eine umfassende Sicherheitsstrategie entwickeln, Mitarbeiter schulen, mehrschichtige Sicherheitslösungen einsetzen und regelmäßig Sicherheitsüberprüfungen durchführen.

Der Einsatz von Managed Security Services kann zusätzlichen Schutz bieten und die Reaktionsfähigkeit verbessern.

RIEDEL

Datenleck bei Telemedizin-Service: Bis zu 20 % der Rezepte durch Suchmaschinen einsehbar

14. Mai 2024, in Hamburg/Hamburg

SICHERHEITSLÜCKE

DATENPANNE

DATENLECK

Was ist passiert?
Der Rezeptservice eines Telemediziners war bis zum 14. Mai 2024 über Suchmaschinen wie DuckDuckGo und Bing durchsuchbar. Dadurch konnten bis zu 20 % der ausgestellten Rezepte, einschließlich personenbezogener Daten und Versicherungsinformationen, ausgelesen werden.

Das Datenleck, verursacht durch eine Sicherheitslücke eines ehemaligen Mitarbeitenden, wurde am 14. Mai 2024 geschlossen. Betroffene Kunden werden informiert. Der Ex-Mitarbeiter, der ein Konkurrenzunternehmen betreibt, veröffentlichte eine Anleitung zum Abgreifen der Daten. Der Unternehmenschef forderte die Suchmaschinen zur sofortigen Löschung der Patientendaten auf.

Was hätte man besser machen können?
Das Unternehmen hätte regelmäßige Schulungen für alle Mitarbeiter durchführen sollen, um sie über Sicherheitsrisiken und Datenschutzbestimmungen aufzuklären. Solche Schulungen helfen, das Bewusstsein für Sicherheitsrisiken zu erhöhen und den sicheren Umgang mit sensiblen Daten zu gewährleisten.

Was lernen wir daraus:

Nicht alle Bedrohungen kommen von außen. Insider-Bedrohungen entstehen durch (ehemalige) Mitarbeitende, die entweder absichtlich oder unbeabsichtigt Sicherheitslücken ausnutzen.

Diese Angriffe sind besonders gefährlich, da Insider oft Zugang zu sensiblen Daten haben und Sicherheitsmaßnahmen leichter umgehen können.

Anzunehmende Schadensfelder:

Quellen
https://www.heise.de/news/Dr-Ansay-aeussert-sich-zu-online-einsehbaren-Cannabis-Rezepten-9719920.html
https://dransay.com/gesundheits-blog/rezept/datenleck/

RIEDEL

Ransomware-Angriff auf Sicherheitsdienstleister: Wichtige Daten offengelegt

13. Mai 2024, in Frankfurt am Main/Hessen

RANSOMWARE

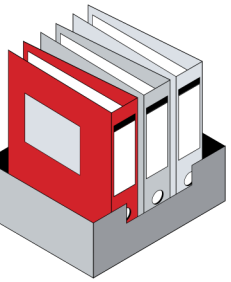
DATENLECK

DATENDIEBSTAHL

Was ist passiert?
Die Ransomwaregruppe 8Base erklärte im Darknet, einen Sicherheitsdienstleister angegriffen und zahlreiche sensible Informationen veröffentlicht zu haben. Dazu gehören Rechnungen, interne Finanzdokumente, personenbezogene Daten, Zertifikate, Mitarbeiterverträge und Geheimhaltungsvereinbarungen. Der betroffene Dienstleister hat sich bisher nicht öffentlich zu dem Vorfall geäußert.

Was hätte man besser machen können?
Um den Sicherheitsvorfall zu verhindern, hätte das Unternehmen ein Security Operations Center (SOC) einsetzen sollen. Ein SOC überwacht die IT-Infrastruktur kontinuierlich und erkennt Bedrohungen in Echtzeit, sodass sofortige Gegenmaßnahmen ergriffen werden können.

Zudem hätte das Unternehmen einen Incident-Response-Plan implementieren sollen. Ein solcher Plan legt fest, wie auf Sicherheitsvorfälle reagiert wird, einschließlich Identifikation, Eindämmung, Beseitigung und Wiederherstellung.



Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/5870-WIS_Sicherheit-8Base.png

Was lernen wir daraus:

Abhängig von Einsatzbereich und Zielgruppe kann auch dieser Sicherheitsdienstleister von der NIS2-Richtlinie betroffen sein.

Dienstleister, die in Verbindung mit kritischen Sektoren (KRITIS) stehen, sind verpflichtet, umfassende Sicherheitsmaßnahmen zu implementieren, Vorfälle umgehend zu melden und transparente Kommunikationsstrategien zu verfolgen. Werden diese Anforderungen nicht erfüllt, drohen dem Dienstleister erhebliche Bußgelder in Millionenhöhe.

RIEDEL

Angreifer drohen Kunststoffunternehmen mit Datenveröffentlichung

9. Mai 2024, in Köln/Nordrhein-Westfalen

DATENDIEBSTAHL

DATENPANNE

RANSOMWARE

Was ist passiert?
Am 14. Mai 2024 proklamierte die Ransomwaregruppe LockBit die deutsche Domain eines Herstellers von technischen Artikeln als Opfer ihrer Attacke. Zuvor, am 9. Mai 2024, hatte die Gruppe bereits eine andere Domain des Unternehmens im Darknet gelistet. Die Täter behaupten, sensible Daten erlangt zu haben und drohen mit deren Veröffentlichung am 16. Mai 2024 sowie am 23. Mai 2024, falls ihre Forderungen nicht erfüllt werden. Es ist unklar, welche spezifischen Daten betroffen sind.

Was hätte man besser machen können?
Um den Sicherheitsvorfall zu verhindern, hätte das Unternehmen SIEM-Systeme und regelmäßige Sicherheitsüberprüfungen einsetzen sollen.

SIEM-Systeme sammeln und analysieren Sicherheitsdaten in Echtzeit, wodurch Bedrohungen frühzeitig erkannt und darauf reagiert werden kann. Regelmäßige Sicherheitsüberprüfungen wie Penetrationstests und Schwachstellenscans decken Schwachstellen auf und beheben sie, bevor sie ausgenutzt werden können.

Was lernen wir daraus:

Auch wenn die spezifischen Daten nicht bekannt sind, unterstreicht der Vorfall die Notwendigkeit für Unternehmen, ihre Daten kritisch zu klassifizieren, zu schützen und robuste Sicherheitsmaßnahmen zu implementieren, um das Risiko solcher Angriffe zu minimieren.

Sowohl präventive Maßnahmen gegen Cyber-Angriffe sind erforderlich als auch die Einführung eines effektives Incident-Response-Managements.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6049-ACLA-LockBit.png
https://www.security-incidents.de/assets/img/incidents/6049-ALCA2-LockBit.png

RIEDEL

DATENDIEBSTAHL

EINBRUCH

Hacker bietet sensible Daten von Computersicherheitsdienst zum Verkauf an

8. Mai 2024, in München/Bayern

Was ist passiert?
Ein Hacker bot auf BreachForums Daten eines Computersicherheitsdienstes zum Verkauf an, darunter angebliche SSL-Passkeys, -Zertifikate, vertrauliche Logs und Zugangsdaten. Er verlangte 20.000 USD in Kryptowährung und behauptete, die Daten bereits verkauft zu haben. Das Unternehmen fand zunächst keine Beweise für den Angriff, entdeckte jedoch später, dass eine isolierte, aus dem Internet zugängliche Testumgebung offline genommen wurde. Es wird betont, dass keine Kundendaten betroffen sind und der Diebstahl dementiert wird.

Was hätte man besser machen können?
Durch die Einführung eines 24/7-Überwachungsdienstes für die Netzwerksysteme hätte das Unternehmen einen bedeutenden Sicherheitsvorteil erzielen können.

Ein rund um die Uhr arbeitendes Security Operations Center (SOC) kann auch Anomalien erkennen, die außerhalb der normalen Arbeitszeiten oder an Wochenenden auftreten.

Anzunehmende Schadensfelder:

Quellen
https://trust.zscaler.com/zscaler.net/posts/18686
https://www.security-incidents.de/assets/img/incidents/5168-ZScaler-IntelBroker-Logs-with-credentials-sold.png

Was lernen wir daraus:

Als Zahlungsmethoden nutzen Cyberkriminelle meist Kryptowährungen - wie Bitcoin und Monero. Zahlungen mit Kryptowährungen bieten Anonymität und erleichtern die Übertragung über internationale Grenzen hinweg, wodurch die Verfolgung durch Behörden erschwert wird. Die dezentrale Natur der Kryptowährungen schützt die Identität der Täter und erhöht ihre Chancen, das Lösegeld zu erhalten.

RIEDEL

83 GB sensible Daten eines Blumengroßhändlers erbeutet

7. Mai 2024, in Kevelaer/Nordrhein-Westfalen

RANSOMWARE

Was ist passiert?
Cyberkriminelle der Ransomwaregruppe MetaEncryptor listeten im Mai 2024 einen Blumengroßhändler im Darknet als Opfer ihrer Attacke. Die Täter behaupten, über 83 GB an sensiblen Daten erlangt zu haben. Ein Countdown für die Veröffentlichung der Daten ist abgelaufen, jedoch sind die hochgeladenen Daten aktuell noch nicht abrufbar

Was hätte man besser machen können?
Das Unternehmen hätte durch den Einsatz von EDR- und SIEM-Technologien Bedrohungen frühzeitig identifizieren können. Regelmäßige Schwachstellenanalysen hätten Sicherheitslücken aufgedeckt, und durch die Implementierung von Datenschutzmaßnahmen wäre zusätzlicher Schutz gewährleistet gewesen.

Was lernen wir daraus:

Die Realität zeigt, dass viele Unternehmen, obwohl sie über grundlegende Sicherheitsmaßnahmen verfügen, oft nicht ausreichend gegen die immer raffinierteren und anpassungsfähigeren Cyberbedrohungen geschützt sind.

Die Bedrohungslandschaft entwickelt sich stetig weiter, wobei Angreifer zunehmend auf moderne Technologien wie künstliche Intelligenz und maschinelles Lernen setzen, um ihre Angriffe zu automatisieren und schwerer erkennbar zu machen.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/5507-MetaEncryptor-Elbers1.PNG

RIEDEL

32 GB Daten gestohlen: Lösegeldforderung nach Cyberangriff

7. Mai 2024, in Hamburg/Hamburg

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Cyberkriminelle der Ransomwaregruppe MetaEncryptor stahlen am 7. Mai 2024 bei einer Reederei 32 GB Daten. Die Täter verschlüsselten die Daten und forderten bis zum 8. Mai 2024 ein Lösegeld für die Entschlüsselung. Details zum Ablauf des Angriffs und zur Höhe des Lösegelds sind unklar. Das Unternehmen meldete den Vorfall den Behörden und arbeitet mit IT-Experten an der Datenwiederherstellung. Ob das Lösegeld gezahlt wurde, ist nicht bekannt.

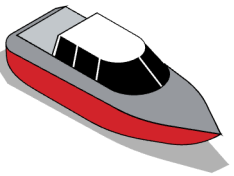
Was hätte man besser machen können?
Um den Sicherheitsvorfall zu verhindern, hätte das Unternehmen ein Security Operations Center (SOC) einsetzen sollen, das die IT-Infrastruktur rund um die Uhr überwacht und Bedrohungen in Echtzeit erkennt und darauf reagiert.

Regelmäßige Schwachstellenscans wären ebenfalls wichtig gewesen, um potenzielle Sicherheitslücken frühzeitig zu identifizieren und zu beheben, bevor sie von Cyberkriminellen ausgenutzt werden können

Was lernen wir daraus:

Zwar gibt es Programme und Dienste, die versprechen, von Ransomware verschlüsselte Daten wiederherzustellen. Jedoch sind solche Entschlüsselungstools oft nicht effektiv, insbesondere bei neueren und komplexeren Varianten von Ransomware.

Deshalb gilt es, Unternehmensnetzwerke präventiv zu schützen, um eine robuste Verteidigungslinie gegen potenzielle Angriffe zu gewährleisten.



Anzunehmende Schadensfelder:

Quellen
https://ransomwareattacks.halcyon.ai/attacks/ransomware-attack-on-vega-reederei-gmbh-co-kg-metaencryptor-strikes-shipping-company
https://ransomfeed.it/index.php?page=post_details&id_post=15255

RIEDEL

Hacker nutzen gestohlene Konten für Ticketbetrug bei Taylor Swift-Tour

6. Mai 2024, in Bremen/Bremen

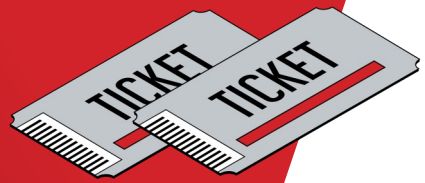
CREDENTIAL STUFFING

Was ist passiert?
Im Vorfeld der Taylor-Swift-Tour im Sommer 2024 verschafften sich Hacker Zugang zu Kundenkonten bei Eventim und kauften mittels Passwortlisten, die im Darknet angeboten wurden, Tickets für die Konzerte. Eventim benachrichtigte die betroffenen Nutzer, setzte ihre Passwörter zurück und bestätigte, dass nur eine zweistellige Anzahl an Tickets betrügerisch erbeutet wurde. Das Unternehmen versichert, dass alle betroffenen Bestellungen rückgängig gemacht wurden.

Was hätte man besser machen können?
Das Unternehmen hätte den Angriff durch die Implementierung einer Zwei-Faktor-Authentifizierung (2FA) für Kundenkonten besser verhindern können.

Regelmäßige Sicherheitsüberprüfungen und die Nutzung von Passwort-Manager-Tools hätten zudem die Sicherheit der Kundenkonten erhöht und den Missbrauch durch im Darknet angebotene Passwortlisten erschwert.

Anzunehmende Schadensfelder:



Was lernen wir daraus:

Shopping im Darknet funktioniert ähnlich wie in einem regulären Onlineshop, jedoch auf anonymen, oft illegalen Plattformen.

Nutzer greifen über spezielle Browser wie Tor darauf zu, um ihre Identität zu verbergen. Produkte wie Drogen, gestohlene Daten oder gefälschte Dokumente werden in Kategorien angeboten. Die Bezahlung erfolgt meist in Kryptowährungen wie Bitcoin, um die Transaktionen schwer nachverfolgbar zu machen. Vertrauen zwischen Käufer und Verkäufer basiert oft auf Bewertungen, ähnlich wie bei herkömmlichen E-Commerce-Websites.

Quellen
https://www.spiegel.de/netzwelt/web/taylor-swift-hacker-angriff-auf-konzerttickets-a-d1ac68a8-513d-4fc0-996e-445dad9ddd2c
https://stadt-bremerhaven.de/eventim-setzt-passwoerter-zurueck/

RIEDEL

Cyberangreifer drohen mit Veröffentlichung sensibler Daten nach Angriff auf Universität

7. Mai 2024, in Ilmenau/Thüringen

RANSOMWARE

DATENPANNE

DATENDIEBSTAHL

DATENLECK

Was ist passiert?
Cyberkriminelle der LockBit-Gruppe erklärten am 7. Mai 2024 eine deutsche technische Universität als Opfer eines Ransomware-Angriffs. Die Täter behaupteten, über sensible Daten zu verfügen, und drohten mit deren Veröffentlichung am 5. Juni 2024, falls ihre Forderungen nicht erfüllt werden. Zur Bestätigung ihrer Behauptungen luden die Angreifer Screenshots von internen Tabellen und Dateiverzeichnissen der Hochschule hoch.

Was hätte man besser machen können?
Um den Ransomware-Angriff auf die technische Universität effektiver abwehren zu können, wäre ein Security Operations Center (SOC) von großer Bedeutung gewesen.

Durch kontinuierliche Überwachung und fortschrittliche Bedrohungserkennung hätte ein SOC schnell auf verdächtige Aktivitäten reagieren können. Regelmäßige Sicherheitsüberprüfungen und Schwachstellenanalysen hätten dabei geholfen, potenzielle Sicherheitslücken frühzeitig zu erkennen und zu schließen.

Was lernen wir daraus:

Neben großen Unternehmen und Organisationen werden zunehmend auch Universitäten ein beliebtes Angriffsziel für Cyberkriminelle. Oftmals haben Bildungseinrichtungen nicht ausreichend robuste Sicherheitsmaßnahmen, was sie anfällig macht. Demnach müssen die Einrichtungen ihre Sicherheitsstrategien stärken und regelmäßig überprüfen, um solchen Bedrohungen präventiv entgegenzuwirken.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6047-TU-Ilmenau-LockBit.png

RIEDEL

Drohung mit Veröffentlichung sensibler Daten bei Kunststoffunternehmen

6. Mai 2024, in Neureichenau/Bayern

DATENDIEBSTAHL

RANSOMWARE

DATENPANNE

Was ist passiert?
Cyberkriminelle einer Ransomwaregruppe proklamierten den Angriff auf ein Kunststoffunternehmen und behaupteten, über sensible Daten zu verfügen. Sie drohten damit, diese Daten zu veröffentlichen, falls ihre Forderungen nicht erfüllt werden.

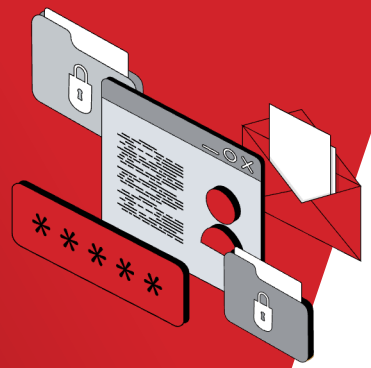
Was hätte man besser machen können?
Das Kunststoffunternehmen hätte den Angriff durch die Integration eines Managed-SIEM und eines 24/7 Security Operations Centers frühzeitig erkennen und abwehren können.

Regelmäßige Sicherheitsprüfungen, eine robuste Backup-Strategie und ein umfassender Incident-Response-Plan hätten den Schaden weiter minimieren und die Veröffentlichung sensibler Daten verhindern können.

Was lernen wir daraus:

Bei herstellenden Unternehmen ist das Risiko eines Produktionsstillstands, der bei den Herstellern zu erheblichen finanziellen Verlusten und Betriebsstörungen führen kann, besonders kritisch. Daher ist es unerlässlich, robuste Sicherheitsmaßnahmen und einen effektiven Notfallplan zu haben, um solche Angriffe abzuwehren und schnell reagieren zu können.

Anzunehmende Schadensfelder:



Quellen
https://www.security-incidents.de/assets/img/incidents/6044-PARAT-LockBit.png

RIEDEL

Datenveröffentlichung droht nach Ransomware-Angriff

6. Mai 2024, in Rheinbach/Nordrhein-Westfalen

RANSOMWARE

DATENPANNE

DATENDIEBSTAHL

DATENLECK

Was ist passiert?
Cyberkriminelle einer Ransomwaregruppe erklärten den Angriff auf einen Hersteller elektronischer Geräte und behaupteten, sensible Daten erlangt zu haben. Sie drohten damit, diese Daten am 21. Mai 2024 zu veröffentlichen, falls ihre Forderungen nicht erfüllt werden.

Was hätte man besser machen können?
Eine 24/7-Überwachung durch ein Security Operations Center (SOC) und der Einsatz einer SOAR-Plattform hätten den Angriff frühzeitig erkennen und eindämmen können. Regelmäßige Mitarbeiterschulungen zur Bedrohungserkennung hätten zusätzlich das Risiko eines erfolgreichen Angriffs verringert.

Was lernen wir daraus:

Durch den Einsatz fortschrittlicher IT-Sicherheits-lösungen wie:

- **SIEM & SOC**
- **XDR**
- **EDR**
- **SOAR**
- **(D)DoS Protection**
- **Next Generation Firewalls**
- **SASE**

verhindern Unternehmen nicht nur Datenverluste, sondern sorgen zugleich für die Einhaltung gesetzlicher Vorschriften zur Steigerung des Sicherheitsniveaus.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6046-REMA-LockBit.png

RIEDEL

Massive Sicherheitslücke bei Videokonferenzen der Bundeswehr entdeckt

4. Mai 2024, Berlin/Berlin

SICHERHEITSLÜCKE

DATENLECK

Was ist passiert?
Experten entdeckten eine schwerwiegende Sicherheitslücke bei der Bundeswehr, bei der Videokonferenz-Links der Cisco-Software WebEx öffentlich im Internet zugänglich waren. Bis zum Abend des 3. Mai 2024 waren mindestens 6.000 Konferenzen einsehbar, darunter auch vertrauliche Meetings. Die Links konnten leicht durch Hoch- und Herunterzählen von Zahlen gefunden werden. Einige Konferenzen waren nicht passwortgeschützt, was es Unbefugten ermöglichte, beizutreten. Die Bundeswehr erklärte, dass nur Metadaten ablesbar waren und die Lücke nun geschlossen sei.

Was hätte man besser machen können?
Die Bundeswehr hätte sicherstellen sollen, dass alle Videokonferenzen standardmäßig durch Passwörter geschützt sind, um unbefugten Zugriff zu verhindern.

Darüber hinaus hätten die Meeting-Links sicher und zufällig generiert werden müssen, anstatt einfache hochzählbare Zahlen zu verwenden, um das Erraten der Links unmöglich zu machen. Regelmäßige Sicherheitsüberprüfungen und Penetrationstests der eingesetzten Software hätten zudem dazu beitragen können, Sicherheitslücken frühzeitig zu entdecken und zu beheben.

Anzunehmende Schadensfelder:

Quellen
https://www.zeit.de/digital/datenschutz/2024-05/bundeswehr-webex-sicherheitsluecke-it-sicherheit
https://www.tagesspiegel.de/politik/videomeetings-wohl-frei-zuganglich-neue-grosse-sicherheitslucke-bei-bundeswehr-entdeckt-11617103.html

Was lernen wir daraus:

Durch Schwachstellen bei vertraulichen militärischen Informationen können Sicherheitsstrategien, Verteidigungspläne oder Informationen über militärische Kapazitäten an die Öffentlichkeit gelangen. Auf diese Weise könnte es Gegnern oder feindlichen Nationen ermöglicht werden, gezielte Angriffe zu planen oder Sicherheitsvorkehrungen zu umgehen.

Auch die Bundeswehr muss im Rahmen der NIS2-Richtlinie diverse Cybersecurity-Maßnahmen ergreifen, um ihre IT-Infrastruktur und Netzwerke zu schützen.

RIEDEL

Fehler bei Fluggesellschaft ermöglicht unbefugten Zugriff auf Flugdaten

3. Mai 2024, in Köln/Nordrhein-Westfalen

DATENLECK

DATENPANNE

KONFIGURATIONSFEHLER

Was ist passiert?
Am Nachmittag des 8. April 2024 konnten Kunden einer großen deutschen Luftfahrt-Firma sowie deren Tochterfirmen aufgrund eines Konfigurationsfehlers in der App und Webseite auf die Flugdaten anderer Kunden zugreifen. Der Fehler, der Buchungscodes falsch anzeigte, wurde schnell behoben. Allerdings hatte Apples Siri-Assistent zuvor die versehentlich offengelegten Daten erfasst und in mindestens zwei Fällen in die Kalender von unbefugten Personen eingetragen. Die Flüge blieben Wochen später noch in den Kalendern der Betroffenen sichtbar.

Was hätte man besser machen können?
Lufthansa hätte regelmäßige Vulnerability Assessments durchführen sollen, um Konfigurationsfehler frühzeitig zu erkennen und zu beheben. Zudem hätte eine schnelle Benachrichtigung der betroffenen Kunden sowie eine Anleitung zur Entfernung der eingetragenen Flugdaten den Schaden minimieren können.

Was lernen wir daraus:

Unternehmen müssen proaktive Maßnahmen ergreifen, um solche Sicherheitslücken zu schließen und 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.

Anzunehmende Schadensfelder:

Quellen
https://www.nzz.ch/wirtschaft/hey-siri-zeige-mir-ein-datenleck-bei-der-lufthansa-und-der-swiss-ld.1828640
https://www.golem.de/news/datenpanne-bei-der-lufthansa-siri-ruft-buchungsdaten-fremder-fluggaeste-ab-2405-184805.html

RIEDEL

Schuhhersteller kämpft seit Wochen mit IT-Ausfall nach Cyberangriff

3. Mai 2024, in Wuppertal/Nordrhein-Westfalen

AUSFALL

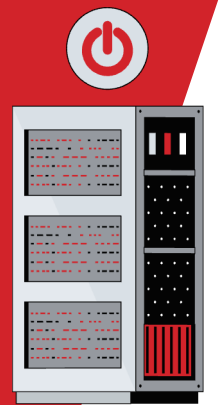
EINBRUCH

Was ist passiert?
Ein Schuhhersteller kämpft seit Wochen mit den Auswirkungen eines Cyberangriffs. Die IT-Systeme wurden heruntergefahren, um den Schaden zu begrenzen, wodurch der Onlineshop nicht erreichbar ist und stattdessen eine Entschuldigungsseite angezeigt wird. Auch in den Filialen gibt es Einschränkungen. Der Betreiber konnte wichtige Geschäftsprozesse teilweise wiederherstellen. Es ist derzeit unklar, ob es sich um eine Ransomware-Attacke handelt, ob Daten gestohlen wurden oder ob Lösegeldforderungen vorliegen.

Was hätte man besser machen können?
Durch den Einsatz fortschrittlicher Endpoint Protection und Intrusion Detection Systeme hätte die Angriffsfläche reduziert und verdächtige Aktivitäten frühzeitig erkannt werden können.

Die Implementierung eines robusten Backup-Systems mit regelmäßigen Snapshots und Offsite-Backups hätte eine schnelle Wiederherstellung der IT-Systeme ermöglicht. Zudem hätte ein Incident-Response-Plan aktiviert werden müssen, um die Auswirkungen des Angriffs zu minimieren und eine zügige Wiederherstellung der Dienste sicherzustellen.

Anzunehmende Schadensfelder:



Was lernen wir daraus:

Nachdem ein Unternehmen Ziel eines Angriffs geworden ist, können die Kosten für Wiederherstellung und Sicherheitsverbesserungen oft erheblich sein. Präventive Investitionen in umfassende IT-Sicherheitslösungen sind jedoch der Schlüssel, um solche Angriffe im Vorfeld zu verhindern und dadurch sowohl finanzielle als auch operationale Schäden erheblich zu verringern.

Quellen
https://www.heise.de//news/Schuhhaendler-Salamander-nach-Cyberattacke-offline-9707690.html
https://shoez.biz/cyberangriff-auf-klauser-und-salamander/

RIEDEL

Angreifer drohen mit Datenveröffentlichung nach Cyberangriff auf Reederei

3. Mai 2024, in Haren/Niedersachsen

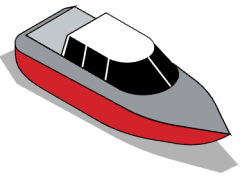
RANSOMWARE

DATENPANNE

DATENDIEBSTAHL

Was ist passiert?
Cyberkriminelle der Ra Group haben eine Reederei als Ransomware-Opfer deklariert und behaupten, 424 GB an sensiblen Daten erlangt zu haben. Die Informationen umfassen finanzielle, Kunden-, Rechts- und Personaldaten. Die Angreifer drohen mit einer Veröffentlichung der Daten, falls ihre Forderungen bis zum 15. Mai nicht erfüllt werden.

Was hätte man besser machen können?
Hätte die Reederei ein 24/7 Security Operations Center (SOC) und moderne Technologien und Systeme im Einsatz gehabt, hätte sie durch eine starke Verteidigungslinie gegen Cyberbedrohungen die Veröffentlichung sensibler Unternehmensdaten vermeiden können.



Anzunehmende Schadensfelder:

Quellen
https://www.borncity.com/blog/2024/05/03/reederei-ingerhans-opfer-der-ra-world-ransomware-gruppe/
https://www.security-incidents.de/assets/img/incidents/6038-Reederei_I%C3%BCngerhans-Ra_Group.png

Was lernen wir daraus:

AI-basierte Cyberangriffe nutzen Künstliche Intelligenz, um Angriffe zu automatisieren und zu optimieren. Diese Technologie kann dazu verwendet werden, Muster zu erkennen, die menschliche Sicherheitsanalysten möglicherweise übersehen, und ermöglicht hochgradig zielgerichtete Angriffe.

RIEDEL

Datenleck nach Ransomware-Angriff auf Technologieunternehmen

3. Mai 2024, in Gangelt/Nordrhein-Westfalen

DATENDIEBSTAHL

RANSOMWARE

DATENLECK

Was ist passiert?
Cyberkriminelle der Qilin-Gruppe haben ein Technologieunternehmen als Opfer eines Ransomware-Angriffs proklamiert. Die Angreifer haben Personalausweise, Excel-Tabellen, Rechnungen, Führerscheine und Vertraulichkeitserklärungen des Unternehmens veröffentlicht.

Was hätte man besser machen können?
Das angegriffene Technologieunternehmen 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 sensibler Unternehmensdaten möglicherweise vermeiden können.

Was lernen wir daraus:

Ein robuster Aufbau der IT-Infrastruktur ist entscheidend, um Betriebsausfälle aufgrund von Cyberangriffen vorzubeugen. Durch Investitionen in eine starke und zuverlässige IT-Infrastruktur sichern Unternehmen ihre Betriebsabläufe und minimieren das Risiko kostspieliger Ausfälle.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6041-Tohlen_Building-Qilin.PNG

RIEDEL

APRIL 2024

SECURITY INCIDENTS GERMANY

RIEDEL

Cyberangriff wirkt sich auf Unimedizin aus: Verletzung der Privatsphäre von Patienten

30. April 2024, in Mainz/Rheinland-Pfalz

EINBRUCH

DATENDIEBSTAHL

Was ist passiert?
Bei einem Cyberangriff auf den IT-Dienstleister einer Universitätsmedizin wurden E-Mail-Adressen von 280.000 Personen entwendet und im Darknet veröffentlicht. Die Unimedizin teilte mit, dass unbekannte Hacker verantwortlich sind.

Der Angriff betrifft E-Mails, die zwischen September 2022 und Juni 2023 versendet wurden, jedoch keine Inhalte oder Anhänge. Die Universitätsmedizin informierte die Betroffenen per E-Mail und warnte vor Phishing-Angriffen.

Was hätte man besser machen können?
Beim Outsourcing von IT-Diensten sollte darauf geachtet werden, dass der Dienstleister regelmäßige Sicherheitsüberprüfungen von Systemen und Netzwerken durchführt, um Schwachstellen zu identifizieren und zu beheben. Dazu gehören auch regelmäßige Überprüfungen der Sicherheitsprotokolle, Software-Patches und der Einhaltung von Sicherheitsrichtlinien.

Mit einem **Vulnerability Assessment** kann einem solchen Vorfall vorgebeugt werden, indem potenzielle Schwachstellen erkannt werden, noch bevor sie sich Cyberkriminelle zu Nutzen machen.

Was lernen wir daraus:
Sicherheitsvorfälle bei Kliniken gefährden die Vertraulichkeit, Verfügbarkeit und Integrität der Patientendaten. Sensible Informationen, die für eine effektive medizinische Versorgung unerlässlich sind, könnten kompromittiert werden.

Dies kann nicht nur ein direktes Risiko für die betroffenen Patienten darstellen, sondern hat auch tiefgreifende Konsequenzen für die Kliniken selbst. Neben möglichen rechtlichen und finanziellen Belastungen führt ein solcher Vorfall zu einem erheblichen Reputationsverlust.

Anzunehmende Schadensfelder:

Quellen
SWR
Heise

RIEDEL

Deutscher Spediteur taucht nach Ransomware-Angriff auf Darknet-Opferliste auf

30. April 2024, in Limbach-Oberfrohna/Sachsen

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Im April 2024 wurde ein deutsches Speditionsunternehmen mutmaßlich Opfer eines Ransomware-Angriffs. Die Attacke wurde bekannt, als die Ransomwaregruppe Cloak das Unternehmen am 30. April 2024 auf ihrer Darknet-Opferliste veröffentlichte.

Laut den Angreifern ereignete sich der Angriff bereits am 5. April 2024. Sie veröffentlichten nach abgelaufener Zahlungsfrist gestohlene Daten wie interne Excel-Tabellen, Personalausweis-Kopien und Kundenkommunikation.

Was hätte man besser machen können?
Das angegriffene Unternehmen hätte den Angriff frühzeitiger entdecken können durch die Integration eines Managed-SIEM mit entsprechendem 24/7 Security Operations Center. Den Datendiebstahl hätte man durch die frühzeitigere Reaktion ggf. vermeiden können.

Was lernen wir daraus:

Ransomware-Angreifer sind fleißig am Sammeln und Beobachten in den infiltrierten Systemen. Nach getaner Arbeit kann es bei den Opfern zu erheblichen finanziellen Verlusten durch Lösegeldzahlungen, Betriebsunterbrechungen und Wiederherstellungskosten kommen. Langfristig gesehen haben die Opfer mit dem Verlust von Kundenvertrauen und möglichen rechtlichen Konsequenzen wegen Datenschutzverletzungen zu rechnen.

Logistikunternehmen, die eine Schnittstelle zu kritischen Sektoren (KRITIS) aufweisen, müssen mit Bußgeldern in Millionenhöhe rechnen, wenn sie der EU-weiten Gesetzgebung NIS-2 nicht nachkommen.

Anzunehmende Schadensfelder:

Quellen
https://www.breachsense.com/breaches/spedition-weise-data-breach/
https://x.com/FalconFeedsio/status/1785203219418722775

RIEDEL

Name & Shame Taktik erwischt deutschen Maschinenbauer

29. April 2024, in Gutach im Breisgau/Baden-Württemberg

DATENPANNE

DATENDIEBSTAHL

Was ist passiert?
Im April 2024 meldete die Ransomwaregruppe 8Base einen Angriff auf ein Maschinenbauunternehmen in Baden-Württemberg. Sie drohten, sensible Daten wie Rechnungen, Finanzdokumente, Verträge und personenbezogene Informationen zu veröffentlichen, falls ihre Forderungen nicht erfüllt würden. Die Frist zur Einigung betrug sechs Tage.

Die Ransomwaregruppe setzt auf eine „Name-and-Shame"-Taktik und greift laut eigener Aussage nur Unternehmen an, die „die Privatsphäre und Bedeutung der Daten ihrer Mitarbeiter und Kunden vernachlässigen".

Was hätte man besser machen können?
Hätte das Maschinenbauunternehmen seine IT-Infrastruktur weniger nachlässig aufgebaut, wäre es ggf. nicht ins Visier der Ransomwaregruppe 8Base geraten. Durchgehende Datenverschlüsselungen und die Implementierung strenger Zugriffskontrollen hätten dazu führen können, die Daten ihrer Mitarbeiter und Kunden zu schützen.

Was lernen wir daraus:

Die „Name and Shame"-Taktik zielt darauf ab, den Ruf der Opfer zu schädigen, indem sie öffentlich als Cybercrime-Opfer geoutet werden. Cyberkriminelle veröffentlichen die Namen von Unternehmen oder Organisationen, die sie angegriffen haben, um den Eindruck zu erwecken, dass diese erhebliche Mängel in ihrer IT-Sicherheit aufweisen.

Diese öffentliche Bloßstellung wird genutzt, um zusätzlichen Druck auszuüben, indem sie die Opfer als nachlässig darstellen, was nicht nur ihren Ruf schädigt, sondern auch potenzielle Kunden und Partner abschrecken kann.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6020-Wasserkraft_Volk-8Base.png

RIEDEL

Datendiebstahl bei Fliesenfachhandel in Ludwigshafen am Rhein

29. April 2024, in Ludwigshafen am Rhein/Rheinland-Pfalz

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Ende April 2024 gab die Ransomwaregruppe Space Bears bekannt, einen deutschen Fliesenfachhandel angegriffen und Daten gestohlen zu haben. Im Juli 2024 veröffentlichten sie die entwendeten Daten.

Was hätte man besser machen können?
Auf die Größe kommt es nicht an – auch kleine und mittlere Unternehmen müssen eine robuste IT-Infrastruktur aufbauen. Hätte der Fliesenfachhandel ein 24/7 Security Operations Center (SOC) und moderne Technologien und Systeme im Einsatz gehabt, hätte man durch eine starke Verteidigungslinie gegen Cyberbedrohungen die Veröffentlichung sensibler Unternehmensdaten vermeiden können.

Was lernen wir daraus:

Während große Unternehmen und Organisationen häufig Ziel von Ransomware-Angriffen sind, sind auch kleinere Unternehmen und Einzelpersonen gefährdet. Angreifer zielen auf alle, die möglicherweise in der Lage sind, Lösegeld zu zahlen und nutzen oft automatisierte Angriffe, um eine große Anzahl von potenziellen Opfern zu erreichen.

Anzunehmende Schadensfelder:

Quellen
https://ransomfeed.it/index.php?page=post_details&id_post=15049
https://www.security-incidents.de/assets/img/incidents/6029-fliesenstudio-am-rhein-space-bears.png

RIEDEL

IT-Systeme werden runtergefahren: Operative Einschränkungen und Ausfälle

26. April 2024, in Berkheim/Baden-Württemberg

DATENLECK

DATENDIEBSTAHL

RANSOMWARE

AUSFALL

Was ist passiert?
Ein Bau- und Logistikunternehmen aus Berkheim wurde von Cyberkriminellen angegriffen. Der Angriff wurde laut Unternehmensangaben gestoppt, indem zahlreiche IT-Systeme abgeschaltet wurden, um die Ausbreitung von Schadsoftware zu verhindern. Aufgrund des Angriffs gibt es operative Einschränkungen und Ausfälle der E-Mail-Kommunikation.

Im Mai 2024 hat sich die Gruppe MetaEncryptor zum Angriff geäußert und 85 GB der gestohlenen Daten veröffentlicht.

Was hätte man besser machen können?
Durch den Einsatz einer SOAR-Plattform (Security Orchestration, Automation and Response) hätte man womöglich schneller auf die Bedrohung reagieren und die Ausbreitung des Schadcodes effizienter eindämmen können. Automatisierte Bedrohungserkennung und Reaktionsmaßnahmen hätten zudem geholfen, Sicherheitsvorfälle sofort zu isolieren und zu analysieren.

Was lernen wir daraus:

Schadsoftware kann sich rasend schnell verbreiten und erhebliche Schäden verursachen, wenn sie nicht sofort eingedämmt wird. Daher ist es entscheidend, bei einem Cyberangriff schnell zu reagieren und betroffene IT-Systeme sofort abzuschalten, um die Ausbreitung des Schadcodes zu verhindern. Schnelle und effiziente Maßnahmen schützen nicht nur die IT-Infrastruktur, sondern minimieren auch die operativen und finanziellen Auswirkungen eines Angriffs.

Anzunehmende Schadensfelder:

Quellen
https://web.archive.org/web/20240503221248/https://www.maxwild.com/unternehmen/news/cyberangriff-auf-max-wild-gmbh/
https://www.security-incidents.de/assets/img/incidents/6065-Max_Wild-Metaencryptor.PNG

RIEDEL

Softwareunternehmen kommt teilweise zum Erliegen

26. Juni 2024, in Lübeck/Schleswig-Holstein

EINBRUCH

DATENLECK

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Ein Softwareunternehmen in der Automobilindustrie erlitt im April 2024 eine schwere Ransomware-Attacke, die den Betrieb erheblich beeinträchtigte.

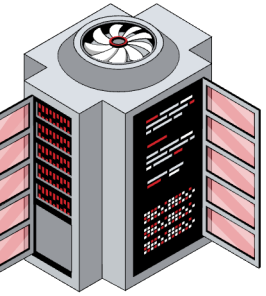
Die Gruppe APT73 drang in die Systeme ein, verschlüsselten sensible Daten und veröffentlichten einen Auszug der kompromittierten Informationen, darunter ein Admin-Passwort. Am 26. April 2024 tauchte das Unternehmen auf der Opferliste im Darknet auf, gefolgt von einer Lösegeldforderung.

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.

Was lernen wir daraus:

Die Ransomwaregruppe APT73 ist bekannt für ihre hochspezialisierten und zielgerichteten Angriffe auf Unternehmen und Institutionen, insbesondere im Bereich der Technologie und Automobilindustrie. Diese Gruppe verwendet ausgeklügelte Methoden zur Verschlüsselung und Erpressung, wodurch sie erhebliche Schäden verursachen kann.



Anzunehmende Schadensfelder:

Quellen
https://ransomwareattacks.halcyon.ai/attacks/apt73-ransomware-attack-on-melting-mind-gmbh-a-closer-look
https://www.csoonline.com/de/a/ransomware-attacke-auf-luebecker-systemhaus,3681346

RIEDEL

Vertrauliche Dokumente geraten in die Hände von Cyberkriminellen

23. April 2024, in Achern/Baden-Württemberg

EINBRUCH

DATENDIEBSTAHL

ERPRESSUNG

Was ist passiert?
Im April 2024 wurde ein deutscher Anbieter von Sicherheitstechnik Opfer einer Ransomware-Attacke durch die cyberkriminelle Gruppe 8BASE. Die Angreifer stehlen Finanzdaten, Arbeitsverträge, Vertraulichkeitsvereinbarungen und andere vertrauliche Dokumente des Unternehmens.

Was hätte man besser machen können?
Der Einsatz einer Kombination moderner Technologien – wie mitunter eines SIEM-Tools – hätten eine erfolgreiche Prävention und Erkennung des Cyberangriffs sicherstellen können.

Ein SIEM-Tool erkennt Anomalien in Echtzeit und schlägt sofort Alarm, wodurch Angriffe frühzeitig abgewehrt werden können.

Was lernen wir daraus:

Hacker haben unterschiedliche Motive: Das kann das Interesse an einer Datenbeschaffung für spezifische Zwecke sein, die Realisierung von schnellen finanziellen Gewinnen durch Lösegeldforderungen oder finanzielle Einnahmen durch den Verkauf der entwendeten Daten im Darknet.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/4953-BielerLang-Ransom-8BASE-Listing.png
https://www.security-incidents.de/assets/img/incidents/4953-BielerLang-Ransom-8BASE.png

RIEDEL

Kleiner Betrieb in Bayern: 30.000 € Schaden

23. April 2024, in Bad Wörishofen/Bayern

EINBRUCH

ERPRESSUNG

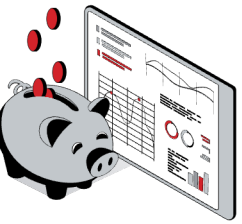
RANSOMWARE

Was ist passiert?
Ein kleiner Gewerbebetrieb wurde durch einen Cyberangriff betroffen, bei dem Unbekannte die Systeme des Unternehmens verschlüsselten. Der Geschäftsführer entdeckte an einem Wochenende, dass sämtliche Dateien auf seinem PC blockiert waren und ein Erpresserschreiben auf dem Bildschirm hinterlassen wurde.

Die Polizei sowie ein externer IT-Dienstleister wurden hinzugezogen. Der verursachte Schaden wird auf etwa 30.000 Euro geschätzt.

Was hätte man besser machen können?
Eine kontinuierliche Überwachung ermöglicht eine schnelle Reaktion auf Bedrohungen und minimiert das Risiko, dass Angriffe unbemerkt bleiben und großen Schaden anrichten.

Das Unternehmen hätte durch die Implementierung einer 24/7-Überwachung seiner Netzwerksysteme einen erheblichen Sicherheitsvorteil erzielen können. Ein rund um die Uhr tätiges Security Operations Center (SOC) erkennt Anomalien frühzeitig, auch wenn diese außerhalb der regulären Arbeitszeiten oder am Wochenende auftreten.



Anzunehmende Schadensfelder:

Quellen
https://www.polizei.bayern.de/aktuelles/pressemitteilungen/066059/index.html
https://www.merkur.de/bayern/schwaben/mindelheim-kurier/bad-woerishofen-cyberangriff-auf-gewerbebetrieb-etwa-30-000-euro-schaden-93028864.html

Was lernen wir daraus:

Cyberkriminelle arbeiten rund um die Uhr und machen keinen Feierabend, wenn es die Büroangestellten tun. Daher ist eine kontinuierliche Überwachung durch ein 24/7 Security Operations Center (SOC) entscheidend, um Bedrohungen auch außerhalb der regulären Arbeitszeiten schnell zu erkennen und abzuwehren.

Eine ständige Überwachung schützt vor Angriffen, die außerhalb der üblichen Geschäftszeiten stattfinden.

RIEDEL

Jahrelange Spionage verschafft Konkurrenten Wettbewerbsvorteile

19. April 2024, in Wolfsburg/Niedersachsen

PHISHING

DATENDIEBSTAHL

SPIONAGE

SOCIAL ENGINEERING

Was ist passiert?
Zwischen 2010 und 2015 griffen mutmaßlich chinesische Staatshacker mehrfach einen der größten Automobilhersteller und dessen Schwesterfirmen an. Etwa 19.000 vertrauliche Dokumente, darunter Informationen zu Ottomotoren, Getrieben und Elektromobilität, wurden gestohlen. Die Angreifer nutzten Methoden wie Schadsoftware, Phishing und Social Engineering. Der Schaden wird auf mehrere Millionen Euro geschätzt.

Was hätte man besser machen können?
Gezielte Schulungen zur Sensibilisierung der Mitarbeiter für Social Engineering und Phishing-Angriff hätten helfen können, den Vorfall möglicherweise zu vermeiden. Diese Arten von Angriffen sind besonders ärgerlich, da sie auf menschliche Fehler und Vertrauen setzen, um Sicherheitsbarrieren zu umgehen.

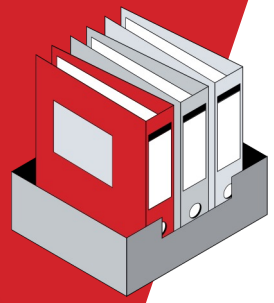
Zusätzlich hätten regelmäßige Schwachstellenanalysen im Unternehmensnetzwerk helfen können, Sicherheitslücken frühzeitig zu identifizieren und zu schließen.

Was lernen wir daraus:

Cyberangriffe zielen nicht nur auf finanzielle Gewinne ab, sondern auch auf kritisches Fachwissen, das für Unternehmen von zentraler Bedeutung ist.

Die Folgen können weitreichend sein – der Datendiebstahl kann die Entwicklung neuer Technologien beeinträchtigen und zu einer geschwächten Marktposition führen.

Anzunehmende Schadensfelder:



Quellen
https://www.spiegel.de/netzwelt/web/volkwagen-vw-konzern-wurde-jahrelang-ausspioniert-von-china-a-f9971315-c342-42b5-b97b-8650b91d60d4
https://www.businessinsider.de/wirtschaft/vw-soll-ueber-jahre-von-chinesischen-staatshackern-ausspioniert-worden-sein/

RIEDEL

Planung und Beratung von Krankhäusern gerät ins Stocken

18. April 2024, in Krefeld/Nordrhein-Westfalen

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Im April 2024 listete die Gruppe Blackout ein Unternehmen auf ihrer Webseite, das auf die Beratung und Planung von Krankenhäusern und Universitätskliniken spezialisiert ist.

Die Angreifer behaupten, 15 GB an Daten, einschließlich Projektdokumenten und Finanzinformationen, sowie 5 TB an Inhalten von verschlüsselten NAS-Laufwerken erbeutet zu haben.

Was hätte man besser machen können?
Ein effektives SOC mit einem gut konfigurierten SIEM-Tool hätte den Cyberangriff frühzeitig erkennen und vereiteln können. Das SIEM hätte verdächtige Aktivitäten, wie unautorisierte Zugriffe oder ungewöhnliche Datenbewegungen, in Echtzeit identifiziert und das SOC alarmiert. Im Falle eines erfolgreichen Angriffs hätte das SOC die Vorfälle sofort bestätigen, die Bedrohung eindämmen und Maßnahmen zur Schadensbegrenzung einleiten können, um die Auswirkungen auf kritische Systeme zu minimieren.

Was lernen wir daraus:

Unternehmen aller Art müssen sich vor Cyberangriffen schützen. Besonders kritisch wird es, wenn Organisationen mit systemrelevantem Einfluss von Cyberkriminellen betroffen sind. In solchen Fällen können die Auswirkungen weitreichend sein und sämtliche Menschen betreffen, insbesondere wenn IT-Systeme ausfallen, die für lebenswichtige Behandlungen und die medizinische Versorgung unerlässlich sind.

Anzunehmende Schadensfelder:

Quellen
https://ransomfeed.it/index.php?page=post_details&id_post=14349
https://ransomwareattacks.halcyon.ai/attacks/cybersecurity-breach-report-hospitaltechnik-planungsgesellschaft-mbh-targeted-by-blackout-ransomware

RIEDEL

Patienten- und Gesundheitsdaten von Bayerns größtem Sozialunternehmen gestohlen

17. April 2024, in Augsburg/Bayern

DATENPANNE

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Ein Träger von Gesundheitseinrichtungen wurde Opfer eines Cyberangriffs durch die Ransomwaregruppe LockBit. Die Angreifer behaupten, private Informationen von internen Servern gestohlen zu haben und drohen mit einer Veröffentlichung, falls ihre Forderungen nicht erfüllt werden. Später bestätigte die gemeinnützige Organisation, dass sensible Daten wie Personaldaten, Finanzdaten, Patientendaten und Gesundheitsdaten betroffen sind, jedoch keine Behandlungsdokumentation oder Arztbriefe.

Was hätte man besser machen können?
Die Organisation hätte durch die Einführung strenger Zugriffs- und Authentifizierungskontrollen sicherstellen können, dass nur autorisierte Personen Zugang zu sensiblen Daten haben.

Eine konsequente Überwachung der Netzwerksicherheit, kombiniert mit der Nutzung von Echtzeit-Überwachungstools zur Erkennung und Abwehr von ungewöhnlichen Aktivitäten, wären womöglich entscheidend gewesen.

Was lernen wir daraus:

Cyberangriffe auf Unternehmen und Organisationen führen häufig dazu, dass persönliche Daten gestohlen werden. Für die betroffenen Personen – in diesem Fall die Patienten – birgt der Diebstahl solch sensibler Informationen erhebliche Risiken. Die gestohlenen Daten, insbesondere medizinische Informationen, können für Betrug oder Erpressung missbraucht werden, was zu schwerwiegenden psychologischen und finanziellen Belastungen führen kann.

Anzunehmende Schadensfelder:

Quellen
https://www.kif-augsburg.de/cyberangriff/
https://www.security-incidents.de/assets/img/incidents/4950-KIF-Augsburg-LockBit.PNG

RIEDEL

Cyberattacke auf Universität mittels gestohlener Zugangsdaten von Studierenden

16. April 2024, in Düsseldorf/Nordrhein-Westfalen

DATENDIEBSTAHL

EINBRUCH

DATENPANNE

Was ist passiert?
Eine Universität in NRW wurde Ziel eines Cyberangriffs. Kriminelle verschafften sich über gestohlene Zugangsdaten von Studierenden Zugriff auf archivierte Datensätze des E-Klausurensystems, die Prüfungsfragen, Antworten und Namen von etwa 15.000 Studierenden enthielten.

Eine weitere Sicherheitslücke ermöglichte den Zugriff auf eine zweite Datenbank mit 60.000 Datensätzen, darunter E-Mail-Adressen und Matrikelnummern. Die Universität erkannte den Angriff schnell, sperrte betroffene Accounts und schaltete das IT-System ab.

Was hätte man besser machen können?
Die Universität hätte durch die Implementierung einer Multi-Faktor-Authentifizierung (MFA) den unbefugten Zugriff auf Studentenaccounts erschweren können. Eine regelmäßige Überprüfung und Aktualisierung der Sicherheitsprotokolle, insbesondere im E-Klausurensystem, hätten Schwachstellen frühzeitig identifizieren und beheben können.

Was lernen wir daraus:

Während große Unternehmen und Organisationen häufig Ziel von Ransomware-Angriffen sind, sind auch Universitäten zunehmend betroffen. Bildungseinrichtungen sind attraktive Ziele, da sie oft über wertvolle Forschungsergebnisse und persönliche Daten verfügen. Angreifer zielen auf jede Institution, die möglicherweise Lösegeld zahlen kann und setzen häufig automatisierte Angriffe ein, um eine Vielzahl potenzieller Opfer zu erreichen. Auch kleinere Bildungseinrichtungen sind nicht sicher vor diesen Bedrohungen.

Anzunehmende Schadensfelder:

Quellen
https://www.hhu.de/news-einzelansicht/hackerangriff-auf-it-systeme-der-hhu
https://www.nrz.de/staedte/duesseldorf/article242112184/Hackerangriff-Duesseldorfer-Heinrich-Heine-Uni-erneut-Ziel.html

RIEDEL

Kanzlei in Leipzig: vertrauliche Klientendaten wurden gestohlen

12. April 2024, in Leipzig/Sachsen

DATENPANNE

DATENDIEBSTAHL

Was ist passiert?
Im April 2024 griff die Qilin-Gruppe eine Rechtsanwaltskanzlei mit einer Ransomware-Attacke an und erklärte die Kanzlei wenige Tage später öffentlich zum Opfer. Laut den Angreifern konnten sie sämtliche vertraulichen Informationen von Klienten und Mitarbeitern sowie finanzielle Daten stehlen.

Die Kanzlei bestätigte den Angriff auf ihrer Webseite, leitete sofortige Untersuchungen ein und behob einen temporären E-Mail-Ausfall.

Was hätte man besser machen können?
Ein kontinuierlicher, umfassender Überblick über die gesamte Sicherheitslage ist unerlässlich, um Bedrohungen frühzeitig zu erkennen und effektiv einzudämmen.

Durch die Einbindung von XDR wäre eine Erkennung und Abwehr der Cyberbedrohung möglich gewesen, da hier der Blick auf die gesamte IT-Infrastruktur ausgerichtet wird.

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/6037-Dr.Fingerle-Qilin2.PNG
https://www.security-incidents.de/assets/img/incidents/6037-Dr.fingerle-Rechtsanwaelte-Qilin.png

RIEDEL

Mit Trojaner Zugang zur Kinderwunschklinik verschafft

10. April 2024, in Bielefeld/Nordrhein-Westfalen

EINBRUCH

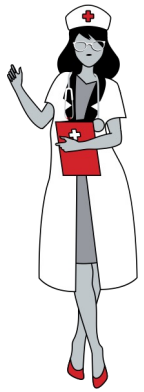
ERPRESSUNG

RANSOMWARE

Was ist passiert?
Deutsche Kinderwunschzentrum wurde Opfer eines Ransomwareangriffs, bei dem Hacker über einen Trojaner Zugang zum System erhielten. Sie verschlüsselten wichtige Server und forderten ein hohes Lösegeld. Dank des schnellen Eingreifens eines IT-Mitarbeiters, der das Netzwerk trennte und der Wiederherstellung aus einem Backup konnten die Daten von 80.000 Patienten geschützt werden.

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.



Anzunehmende Schadensfelder:

Quellen
https://www.heise.de//news/Ransomware-bei-Kinderwunsch-Zentrum-Cyberangriff-auf-franzoesischen-Gemeinden-9682909.html
https://web.archive.org/web/20240416133340/https://www.kinderwunsch-bielefeld.de/2024/04/10/wichtige-patienteninformation/

Was lernen wir daraus:

Trojaner tarnen sich oft als harmlose Software, um unbemerkt in Systeme einzudringen. Einmal installiert, können sie Daten stehlen, Systeme ausspionieren oder zusätzliche Malware nachladen. Diese Angriffe nutzen häufig Phishing-E-Mails oder gefälschte Software-Updates, um Benutzer zur Installation zu verleiten.

RIEDEL

Cyberangriff auf Spedition: Erpresser drohen mit Datenveröffentlichung

DATENPANNE

DATENDIEBSTAHL

9. April 2024, in Mönchengladbach/Nordrhein-Westfalen

Was ist passiert?
Anfang April wurde ein deutsches Speditionsunternehmen von der Hackergruppe Mallox auf deren Darknet-Seite als Opfer eines Angriffs aufgeführt. Dabei wurden sensible Daten gestohlen, die laut den Tätern zur Veröffentlichung bereitstehen.

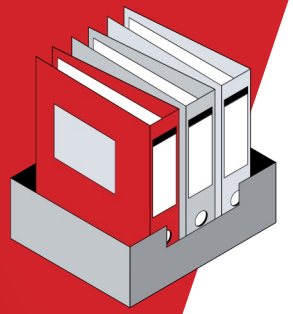
Was hätte man besser machen können?
Das Unternehmen hätte regelmäßige Sicherheitsüberprüfungen, Schulungen für Mitarbeiter und starke Verschlüsselung einsetzen sollen. Darüber hinaus wären regelmäßige Backups und die Implementierung einer Zwei-Faktor-Authentifizierung wichtige Maßnahmen gewesen, um den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

Was lernen wir daraus:

Zukünftig müssen Speditionsunternehmen, die Teil der Lieferkette kritischer Infrastrukturen sind, den Anforderungen der NIS2-Richtlinie (Netz- und Informationssystemsicherheit) nachkommen. Das bedeutet höhere IT-Sicherheitsanforderungen, regelmäßige Sicherheitsprüfungen und Meldung von Vorfällen.

Dabei ist jedes Unternehmen eigenverantwortlich dafür, dass dessen Sicherheitsmaßnahmen den neuen Standards entsprechen und Mitarbeiter geschult sind.

Anzunehmende Schadensfelder:



Quellen
https://ransomfeed.it/index.php?page=post_details&id_post=14169
https://www.security-incidents.de/assets/img/incidents/6026-spedition-langen-mallox.png

RIEDEL

Server eines Datenbankanbieters für mehrere Tage lahmgelegt

8. April 2024, in München/Bayern

EINBRUCH

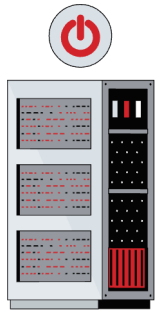
AUSFALL

RANSOMWARE

Was ist passiert?
Ein Anbieter von Wirtschaftsdatenbanken wurde durch einen Ransomware-Angriff lahmgelegt. Die Server blieben mehrere Tage offline, was Bibliotheken, Hochschulen und Unternehmen betraf, die auf Zeitungsartikel, Unternehmensinfos und E-Books zugriffen. Ob Daten verschlüsselt oder gestohlen wurden, ist unklar.

Was hätte man besser machen können?
Der Anbieter hätte durch den Einsatz fortschrittlicher Endpoint Protection und Intrusion Detection Systeme die Angriffsfläche reduzieren können. Regelmäßige Patching- und Update-Management-Prozesse wären wichtig gewesen, um Sicherheitslücken zu schließen.

Die Implementierung eines robusten Backup-Systems mit regelmäßigen Snapshots und offsite-Backups hätte eine schnelle Wiederherstellung ermöglicht. Zudem hätte ein Incident-Response-Plan aktiviert werden müssen, um die Auswirkungen zu minimieren und eine zügige Wiederherstellung der Dienste sicherzustellen.



Anzunehmende Schadensfelder:

Quellen
https://www.heise.de//news/Angriff-auf-Wissenschaftsdatenbank-Cyberkriminelle-legen-Genios-lahm-9678712.html
https://www.security-incidents.de/assets/img/incidents/4829-Genios-Ransomware.png

Was lernen wir daraus:

Der Angriff hat nicht nur das betroffene Unternehmen beeinträchtigt, sondern auch zahlreiche Dritte, die auf die Dienste angewiesen waren. Dies verdeutlicht, wie wichtig es ist, Sicherheitslücken zu minimieren, da ein Angriff weitreichende Konsequenzen für Partner und Kunden haben kann.

RIEDEL

Unternehmensnetzwerk kirchlicher Stiftung vom Internet getrennt

EINBRUCH

8. April 2024, in Bad Waldsee/Baden-Württemberg

Was ist passiert?
Eine Stiftung wurde Opfer eines Hackerangriffs. Zusammen mit einem externen IT-Dienstleister wurde der Angriff analysiert und es wurden Maßnahmen ergriffen. Laut dem Leiter der Kommunikation reagierten die Sicherheitssysteme der Stiftung, was den Angriff frühzeitig bemerkbar machte. Zur Sicherheit wurde das Netzwerk vom Internet getrennt. Die internen Prozesse und die Kommunikation blieben stabil.

Was hätte man besser machen können?
Man hätte durch die Implementierung einer umfassenden Sicherheitsarchitektur, die fortlaufend durch SIEM überwacht wird, und durch Netzwerksegmentierung den Angriff besser eingrenzen können. Regelmäßige Schwachstellenanalysen hätten Sicherheitslücken vorab schließen können. Die schnelle Trennung vom Internet war eine gute Reaktion, doch ein robuster Incident-Response-Plan und regelmäßige Notfallübungen hätten die internen Prozesse und Kommunikation weiter stabilisiert.

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.schwaebische.de/regional/oberschwaben/bad-waldsee/cyberangriff-auf-die-st-elisabeth-stiftung-2418920
https://www.st-elisabeth-stiftung.de/index.php?id=1257&tx_news_pi1%5Bnews%5D=2728&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail

RIEDEL

Das Zahnrad klemmt nach Ransomware-Angriff auf Metallunternehmen

8. April 2024, in Kohlberg/Baden-Württemberg

EINBRUCH

DATENDIEBSTAHL

ERPRESSUNG

Was ist passiert?
Deutsches Metallverarbeitungsunternehmen wurde zum Opfer einer Ransomware-Attacke. Die Erpressergruppe 8BASE konnte bei dem Angriff Daten stehlen – darunter Finanzdaten, Arbeitsverträge und andere vertrauliche Dokumente. Die entwendeten Daten wurden inzwischen von den Erpressern veröffentlicht.

Was hätte man besser machen können?
Das Unternehmen hätte das Risiko erheblich verringern können, indem es EDR-Lösungen und Netzwerksegmentierung implementiert hätte. Regelmäßige Sicherheitsupdates und ein umfassendes Backup-System wären ebenfalls entscheidende Maßnahmen gewesen, um zusätzlichen Schutz zu gewährleisten.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/4954-Ringhoffer-Verzahnungstechnik-Ransom-Listing-8BASE.png
https://www.security-incidents.de/assets/img/incidents/4954-Ringhoffer-Verzahnungstechnik-Cyberangriff-St%C3%B6rmeldung.png

Was lernen wir daraus:

Ein Sicherheitsvorfall stellt ein Ereignis dar, das die Informationssicherheit beeinträchtigt. Solche Vorfälle bedrohen die Vertraulichkeit, Verfügbarkeit oder Integrität von Daten, IT-Anwendungen, IT-Systemen oder IT-Diensten und können erhebliche Schäden für Einzelpersonen, Unternehmen oder Organisationen verursachen.

Oft bleiben Angreifer eine Zeit lang unentdeckt in den kompromittierten Systemen, bevor sie aktiv werden und der Angriff bemerkt wird. Im Durchschnitt dauert es etwa 20 Tage, bis ein solcher Angriff erkannt wird.

RIEDEL

Design-Zeichnungen und weitere Daten von Automobilzulieferer gestohlen

RANSOMWARE

DATENDIEBSTAHL

3. April 2024, in Hainichen/Sachsen

Was ist passiert?
Anfang April 2024 gab die RA World-Ransomwaregruppe einen Autoteileproduzenten als Opfer bekannt. Kurz darauf veröffentlichten die Täter ihre Beute vollständig und behaupteten, 20 GB an Daten erbeutet zu haben, darunter Finanzdokumente, Verträge und Design-Zeichnungen.

Was hätte man besser machen können?
Der Autoteileproduzent hätte durch den Aufbau eines SOC eine frühzeitige Erkennung der Ransomware-Attacke erreichen können. Ein SOC hätte kontinuierliche Überwachung und Analyse der Netzwerksicherheit ermöglicht, um ungewöhnliche Aktivitäten schnell zu identifizieren und darauf zu reagieren.

Dies hätte die Reaktionszeit verkürzt und möglicherweise die Veröffentlichung der Daten verhindert.

Was lernen wir daraus:

Datendiebstahl kann die Vertraulichkeit von Geschäftsgeheimnissen und geistigem Eigentum gefährden. Dies kann zu einem Verlust von Wettbewerbsvorteilen führen, da vertrauliche Informationen über Produkte, Strategien oder Forschungsergebnisse in die Hände von Wettbewerbern gelangen könnten.

Nicht nur die Marktposition kann durch eine solche Ransomware-Attacke beeinträchtigt werden, es kann auch zu langfristigen geschäftlichen Nachteilen kommen.

Anzunehmende Schadensfelder:

Quellen
https://ransomfeed.it/index.php?page=post_details&id_post=14082
https://www.security-incidents.de/assets/img/incidents/6025-innomotive-systems-hainichen-ra-world.png

RIEDEL

Ransomware-Angriff hinterlässt Scherben bei Glasherstellers

3. April 2024, in Hann. Münden/Niedersachsen

EINBRUCH

DATENDIEBSTAHL

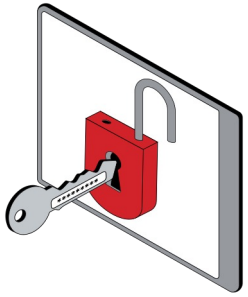
ERPRESSUNG

Was ist passiert?
Ende März 2024 wurde ein deutscher Glashersteller Opfer einer Ransomware-Attacke. Die Erpressergruppe 8BASE exfiltrierte dabei Finanzdaten, Arbeitsverträge und weitere vertrauliche Informationen. Diese Daten wurden mittlerweile veröffentlicht.

Was hätte man besser machen können?
Der Glashersteller hätte durch die Implementierung eines SOC und die Nutzung von SIEM die Ransomware-Attacke besser überwachen und frühzeitiger erkennen können. Ein SOC hätte eine kontinuierliche Überwachung und schnelle Reaktion auf verdächtige Aktivitäten ermöglicht, während SIEM eine umfassende Analyse und Korrelation von Sicherheitsereignissen bereitgestellt hätte, um die Bedrohung frühzeitig zu identifizieren und zu bekämpfen.

Was lernen wir daraus:

Wird ein Unternehmen Opfer von Datendiebstahl, kann das Vertrauen der Kunden erheblich beeinträchtigt werden. Negative Berichterstattung und der Verlust von Kundendaten können das Ansehen des Unternehmens schädigen und langfristige Auswirkungen auf die Kundenbindung und den Geschäftserfolg haben. Die Wiederherstellung des beschädigten Rufs erfordert oft erhebliche Anstrengungen und Investitionen.



Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/4955-isophon-glas-8BASE-Ransom-Listing.png

RIEDEL

Schwachstelle bei Hotelriesen: Sicherheitslücke gefährdet Hotelgäste

SICHERHEITSLÜCKE

DATENLECK

2. April 2024, in Hamburg/Hamburg

Was ist passiert?
Eine schwerwiegende Sicherheitslücke bei einer großen Hotelkette wurde aufgedeckt. Über das Check-in-Terminal in einem Hotel in Hamburg-Altona konnten unbefugte Personen auf Buchungsdaten anderer Gäste zugreifen, einschließlich Zimmernummern und Zugangscodes. Das Terminal, das sowohl Gästen als auch Personal das Einchecken ermöglichte, zeigte nach Eingabe der Reservierungsnummer sensible Informationen an. Es wurde darauf hingewiesen, dass diese Sicherheitslücke es Einbrechern erleichtern könnte, Zugang zu den Zimmern zu erhalten.

Was hätte man besser machen können?
Die Systeme hätten regelmäßigen Sicherheitsüberprüfungen unterzogen werden müssen, um potenzielle Schwachstellen frühzeitig zu erkennen und zu beheben – beispielsweise mit Penetrationstests.

Was lernen wir daraus:

Daten, die einmal im Darknet verkauft wurden, können erneut gehandelt oder weitergegeben werden. Käufer können die Informationen weiter verkaufen oder an andere Kriminelle weitergeben, die sie für ihre eigenen Zwecke nutzen. Dieser Kreislauf kann die betroffenen Daten über Jahre hinweg im Darknet zirkulieren lassen, wodurch das Risiko für die Opfer kontinuierlich steigt.

Anzunehmende Schadensfelder:

Quellen
https://www.golem.de/news/per-check-in-terminal-angreifer-konnten-in-fremde-ibis-hotelzimmer-eindringen-2404-183816.html
https://www.pentagrid.ch/de/blog/preisgabe-tastenschloss-codes-check-in-terminal-ibis-hotel/

RIEDEL

Cyberkriminelle knacken das Netzwerk eines Schlossherstellers

2. April 2024, in Halver/Nordrhein-Westfalen

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Anfang April 2024 gab die Ransomwaregruppe RA World einen deutschen Schlosshersteller als Opfer auf ihrer Darknet-Seite bekannt. Die Täter gaben an, Daten erbeutet zu haben, ohne genaue Details zum Umfang oder Inhalt zu nennen und kündigten deren Veröffentlichung an.

Was hätte man besser machen können?
Der Schlösserhersteller hätte durch EDR und SIEM die Bedrohung frühzeitig erkennen können. Regelmäßige Vulnerability Assessments hätten Schwachstellen identifiziert, während DLP und MFA zusätzlichen Schutz geboten hätten.

Was lernen wir daraus:

Cyberkriminelle nutzen häufig Zero-Day-Exploits, also Schwachstellen in Software, die vom Hersteller noch nicht entdeckt oder behoben wurden.

Diese Sicherheitslücken ermöglichen es Angreifern, Systeme zu kompromittieren, bevor ein Patch verfügbar ist. Solche Exploits werden oft im Darknet-Markt gehandelt und können schwerwiegende Schäden verursachen.

Anzunehmende Schadensfelder:

Quellen
https://ransomfeed.it/index.php?page=post_details&id_post=14076
https://www.security-incidents.de/assets/img/incidents/6024-kico-group-ra-world.png

RIEDEL

Anwaltskanzlei landet auf Opferliste im Darknet

DATENPANNE

DATENLECK

1. April 2024, in Kaufbeuren/Bayern

Was ist passiert?
Am 1. April 2024 listete die LockBit-Gruppe eine bayrische Anwaltskanzlei als Opfer auf ihrer Darknet-Seite. Die Cyberkriminellen drohten damit, sämtliche Mandantendaten der Kanzlei zu veröffentlichen.

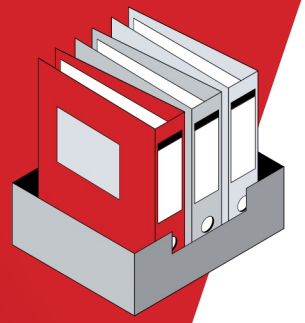
Was hätte man besser machen können?
Die Anwaltskanzlei hätte durch ein SOC eine kontinuierliche Überwachung und schnelle Reaktion auf Bedrohungen sicherstellen können, um die Veröffentlichung von Mandantendaten zu verhindern.

Was lernen wir daraus:

Anwaltskanzleien sind attraktive Ziele für Ransomware-Angriffe, da sie oft hochsensible Daten verwalten, einschließlich vertraulicher Mandanteninformationen und juristischer Dokumente.

LockBit und andere Gruppen zielen auf solche Kanzleien ab, weil die Erpressung von Lösegeldern durch die Drohung, diese Daten zu veröffentlichen oder zu nutzen, einen besonders hohen Druck auf die Opfer ausübt.

Anzunehmende Schadensfelder:



Quellen
https://www.golem.de/news/ueber-gehackte-konten-familie-bereichert-sich-an-payback-punkten-fremder-nutzer-2404-183774.html
https://www.justiz.bayern.de/gerichte-und-behoerden/generalstaatsanwaltschaft/bamberg/presse/2024/6.php

RIEDEL

MÄRZ 2024

SECURITY INCIDENTS GERMANY

RIEDEL

Freier Zugang im Internet zu 900.000 Dateien eines Sportanbieters

28. März 2024, in Berlin/Berlin

DATENLECK

DATENPANNE

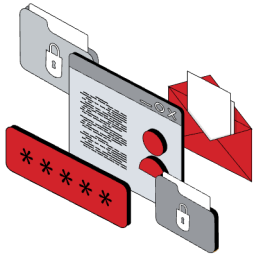
Was ist passiert?
Ein Sportanbieter meldete ein massives Datenleck, das bis zu 50.000 Mitglieder betrifft. Kundendaten wie Namen, Adressen, Telefonnummern sowie Kopien von Ausweisen und Reisepässen waren ungeschützt im Internet zugänglich. Dies birgt erhebliche Risiken für Identitätsdiebstahl und Betrug. Besonders besorgniserregend ist, dass die Daten auch Informationen zu besuchten Fitnessstudios enthalten, was Rückschlüsse auf die Bewegungsgewohnheiten der Kunden des Sportanbieters ermöglicht.

Was hätte man besser machen können?
Der Sportanbieter hätte sicherstellen müssen, dass sensible Kundendaten nicht ungeschützt im Internet zugänglich sind, indem er grundlegende Sicherheitsmaßnahmen wie Datenverschlüsselung und ordnungsgemäße Zugriffsberechtigungen implementiert.

Regelmäßige Sicherheitsüberprüfungen hätten helfen können, solche schwerwiegenden Konfigurationsfehler frühzeitig zu erkennen.

Was lernen wir daraus:

Ein Datenleck bezeichnet den ungewollten und unautorisierten Zugang zu sensiblen Daten, oft durch Sicherheitslücken oder Fehlkonfigurationen, die es Dritten ermöglichen, auf Informationen zuzugreifen. Sie können schwerwiegende rechtliche und geschäftliche Folgen haben, daher ist es essenziell, präventive Sicherheitsmaßnahmen zu implementieren und regelmäßig zu überprüfen.



Anzunehmende Schadensfelder:

Quellen
https://www.heise.de//news/Datenleck-bei-Urban-Sports-Club-Daten-Tausender-Mitglieder-waren-oeffentlich-9668240.html
https://www.spiegel.de/netzwelt/web/urban-sports-club-panne-bei-legt-daten-von-tausenden-mitgliedern-offen-a-a6818c6e-d421-4374-ade2-378099839e0e

RIEDEL

Ransomware-Angriff auf Laser- und Ätzgravurunternehmen

RANSOMWARE

DATENDIEBSTAHL

27. März 2024, in Solingen/Nordrhein-Westfalen

Was ist passiert?
Im März 2024 schrieb sich die LockBit-Ransomwaregruppe ein Laser- und Ätzgravurunternehmen auf ihre Opferliste, die sie im Web veröffentlichten. Die Cyberkriminellen drohten, gestohlene Daten zu veröffentlichen, wenn das Opfer ihre Forderungen nicht erfüllt.

Was hätte man besser machen können?
Das Unternehmen hätte durch die Implementierung eines SOC eine kontinuierliche Überwachung und schnelle Reaktion auf Sicherheitsvorfälle gewährleisten können.

Was lernen wir daraus:

Ransomwaregruppen sind organisierte Gruppen von Cyberkriminellen, die Ransomware entwickeln und einsetzen, um Daten von Opfern zu verschlüsseln und Lösegelder zu erpressen. Sie agieren oft wie Unternehmen mit spezialisierten Rollen, einschließlich Entwicklern und Angreifern.

Viele nutzen das „Ransomware-as-a-Service“-Modell, um ihre Malware zu vermieten. Diese Gruppen arbeiten international und nutzen das Darknet um anonym zu bleiben.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/5036-Kr%c3%bcth-LockBit.PNG

RIEDEL

Deutschlands größtes Opernhaus wurde Opfer eines Cyberangriffs

27. März 2024, in Baden-Baden/Baden-Württemberg

RANSOMWARE

DATENLECK

DATENPANNE

Was ist passiert?
Im März 2024 erklärte die Ransomwaregruppe PLAY Deutschlands größtes Opernhaus zum Opfer eines Cyberangriffs. Laut den Tätern wurden zahlreiche sensible Daten erbeutet, darunter Besucherinformationen, Budgetdokumente, Verträge, Personalausweise und finanzielle Daten. Nachdem das Opern- und Konzerthaus die Forderungen der Angreifer nicht erfüllte, veröffentlichte die Gruppe im April 2024 sämtliche 580 GB an gestohlenen Daten.

Was hätte man besser machen können?
Um den Angriff der Ransomwaregruppe PLAY zu verhindern, hätte das Opernhaus fortschrittliche Cybersecurity-Tools nutzen können, wie SIEM zur Echtzeitanalyse von Sicherheitsdaten, EDR zur Überwachung und Reaktion auf verdächtige Aktivitäten, Firewalls und Intrusion Prevention Systeme zum Schutz des Netzwerks, sowie Antivirus- und Anti-Malware-Software zur Abwehr von Schadsoftware. Zusätzlich hätte Vulnerability Management helfen können, Schwachstellen zu identifizieren und zu beheben.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6015-Festspielhaus_Baden-Baden-PLAY.PNG

Was lernen wir daraus:

Neben der Verschlüsselung der Daten drohen Ransomwaregruppen damit, vertrauliche Informationen öffentlich zu machen, wenn das geforderte Lösegeld nicht gezahlt wird. Diese Taktik erhöht den Druck auf die Opfer, da sie nicht nur um ihre Daten fürchten, sondern auch um die Sicherheit ihrer vertraulichen Informationen.

Experten raten davon ab, das Lösegeld zu zahlen, da dies keine Garantie für die Wiederherstellung der Daten bietet.

RIEDEL

Personalausweise von Mitarbeitern landen im Darknet nach Cyberangriff

27. März 2024, in Lenningen/Baden-Württemberg

DATENLECK
DATENPANNE
RANSOMWARE
DATENDIEBSTAHL

Was ist passiert?
Die BlackBasta-Gruppe listete im Märze 2024 eine schwäbische Etikettendruckerei als Opfer ihres Ransomware-Angriffs. Die Täter drohten, sensible Daten, darunter persönliche Informationen und Buchhaltungsunterlagen, zu veröffentlichen. Als das Unternehmen die Forderungen nicht erfüllte, setzten die Angreifer ihre Drohungen in die Tat um und veröffentlichten 400 GB an Daten, darunter Personalausweise von Mitarbeitern.

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:
Im Darknet gekaufte persönliche Daten, wie Sozialversicherungsnummern oder Personalausweise, können für Identitätsdiebstahl verwendet werden. Angreifer nutzen diese Informationen, um sich als die betroffenen Personen auszugeben, Bankkonten zu eröffnen oder Kredite aufzunehmen. Dies kann zu erheblichen finanziellen und rechtlichen Problemen für die Opfer führen, die oft Monate oder Jahre dauern, um vollständig gelöst zu werden.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6016-Ero_Etikett-BlackBasta2.PNG
https://www.security-incidents.de/assets/img/incidents/6016-Ero_Etikett-BlackBasta.PNG

RIEDEL

Daten von medizinischem Institut im Darknet nach Ransomware-Attacke

23. März 2024, in Bochum/Nordrhein-Westfalen

EINBRUCH

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Ein deutsches Pathologie-Institut wurde im März 2024 von der LockBit-Gruppe auf ihrer Darknet-Seite als Opfer gelistet. Die Cyberkriminellen drohten damit, sensible Daten zu veröffentlichen, falls kein Lösegeld gezahlt werde. Letztendlich wurde von den Cyberkriminellen ein 3,2 GB großer Datensatz hochgeladen, dessen genauer Inhalt jedoch unbekannt ist.

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

Was lernen wir daraus:

Selbst wenn ein Lösegeld gezahlt wird, garantieren die Angreifer nicht immer die vollständige Wiederherstellung der Daten.

Wurde ein Unternehmen erstmal angegriffen, muss es oft erhebliche Mittel für die Wiederherstellung und Verbesserung ihrer Sicherheitsmaßnahmen aufwenden. Durch präventive Investitionen in umfassende IT-Sicherheitslösungen können Unternehmen potenzielle Angriffe vermeiden und sowohl den finanziellen als auch den operationellen Schaden erheblich reduzieren.

Anzunehmende Schadensfelder:

Quellen
https://www.dsgvo-portal.de/sicherheitsvorfaelle/ransomware_angriff_institut-f%C3%BCr-4742.php

RIEDEL

300 GB Daten von Heizungs- und Klimatechnikbetrieb gestohlen

23. März 2024, in Hamburg/Hamburg

EINBRUCH

ERPRESSUNG

DATENDIEBSTAHL

Was ist passiert?
Die RA World Ransomwaregruppe griff eines der größten Unternehmen der technischen Gebäudeausrüstung und des Anlagenbaus in Norddeutschland an und entwendete 300 Gigabyte an Daten – darunter vertrauliche Finanz- und Personalunterlagen, Geschäftsverträge und rechtliche Dokumente. Die Angreifer setzten dem Unternehmen eine Frist bis Ende März 2024, um das Lösegeld zu zahlen.

Was hätte man besser machen können?
Ein SOC hätte den Angriff durch den Einsatz von SOAR und XDR, kombiniert in einer SIEM-Lösung zur Echtzeitüberwachung effektiv verhindern können.

Was lernen wir daraus:

Durch den Einsatz fortschrittlicher IT-Sicherheitslösungen wie:

- ✓ SIEM & SOC
- ✓ XDR
- ✓ EDR
- ✓ SOAR
- ✓ (D)DoS Protection
- ✓ Next Generation Firewalls
- ✓ SD-WAN
- ✓ SASE

können Unternehmen nicht nur ihre vertraulichen Geschäftsgeheimnisse schützen, sondern auch die Vertraulichkeit persönlicher Daten ihrer Mitarbeiter wahren.

Anzunehmende Schadensfelder:

Quellen
https://ransomfeed.it/index.php?page=post_details&id_post=13911
https://ransomwareattacks.halcyon.ai/attacks/ra-world-attacks-schwarz-grantz-hamburg-gmbh

RIEDEL

Ungeschützter Webserver: Daten von 11.000 Bildungseinrichtungen sind betroffen

22. März 2024, in Freiburg im Breisgau/Baden-Württemberg

DATENLECK

SICHERHEITSLÜCKE

KONFIGURATIONSFEHLER

Was ist passiert?
Ein Sicherheitsvorfall bei einem Softwareentwickler, der eine App für über 11.000 Bildungseinrichtungen bereitstellt, führte zur Kompromittierung der Daten von 842.280 Nutzern.

Die ungeschützte Datenbank, die durch eine Webserver-Fehlkonfiguration offen zugänglich war, enthielt unter anderem Avatare, PDF-Anhänge, Unterschriften, Profilbilder sowie 1.500 CSV-Dateien mit sensiblen Daten von Minderjährigen. Der Vorfall wurde im März 2024 entdeckt und die Sicherheitslücke umgehend geschlossen. Weitere Fehlkonfigurationen wurden seitdem behoben, jedoch bleibt die vollständige Nachverfolgung unbefugter Zugriffe aufgrund von Serverprotokolleinstellungen schwierig.

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 Protokollierung und Echtzeit-Monitoring erforderlich, um unbefugte Zugriffe schnell zu erkennen.

Was lernen wir daraus:

- **Konfigurationsmanagement**: Offene Datenbanken aufgrund fehlerhafter Webserver-Konfigurationen sind ein ernstes Risiko.
- **Datenverschlüsselung**: Sensible Daten, insbesondere von Minderjährigen, müssen stets geschützt werden.
- **Schnelle Reaktion**: Sicherheitslücken müssen umgehend geschlossen werden, aber auch eine umfassende Nachverfolgung ist notwendig.

Sicherheitsvorfälle wie dieser verdeutlichen die Bedeutung präventiver Sicherheitsmaßnahmen und kontinuierlicher Überprüfung.

Anzunehmende Schadensfelder:

Quellen
https://www.heise.de//news/Datenleck-bei-beliebter-KiTa-App-Stay-Informed-9662578.html
https://www.heise.de//news/Nach-Datenleck-bei-Kita-App-Stay-Informed-richtet-Informationsseite-und-FAQ-ein-9667323.html

RIEDEL

Veröffentlichung von Gehaltsinformationen, Kontoauszügen etc. durch Ransomwaregruppe

21. März 2024, in Bad Homburg vor der Höhe/Hessen

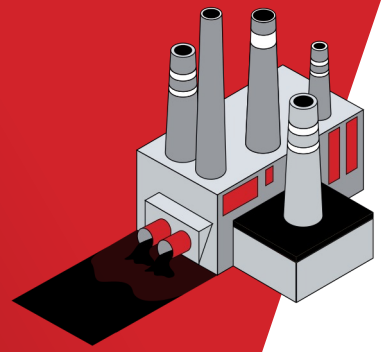
RANSOMWARE

DATENDIEBSTAHL

DATENLECK

Was ist passiert?
Die Ransomwaregruppe Cloak gab im März 2024 auf deren Opferliste, die sie im Darknet veröffentlichten, die Betroffenheit eines Chemieunternehmens bekannt, das auf Wasserstoff, Ammoniak und Methanol spezialisiert ist. Die Angreifer behaupten, 180 GB sensibler Daten gestohlen zu haben, darunter Kontoauszüge, interne Buchhaltungsdaten und Gehaltsinformationen. Da die Zahlungsfrist bereits abgelaufen ist, wurden alle erbeuteten Daten inzwischen online veröffentlicht.

Was hätte man besser machen können?
Das Unternehmen hätte durch ein effektives SOC mit kontinuierlicher Überwachung den Angriff frühzeitig erkennen können.



Was lernen wir daraus:

Die EU-weite NIS2-Richtlinie, die erweiterte Sicherheitsanforderungen für KRITIS-Unternehmen festlegt, unterstreicht die Notwendigkeit robuster Cyberabwehrmaßnahmen. Unternehmen, die unter diese Richtlinie fallen, müssen erweiterte Sicherheitsvorkehrungen treffen, einschließlich der kontinuierlichen Überwachung, des Schutzes kritischer Systeme und der Einführung von Notfallplänen.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/5909-Gascontec-Cloak.PNG

RIEDEL

Holzhändler aus Sachsen wurde durch Cyberangriff Unternehmensdaten entwendet

21. März 2024, in Plauen/Sachsen

EINBRUCH

ERPRESSUNG

DATENDIEBSTAHL

Was ist passiert?
Im März 2024 wurde ein Anbieter von Holz und Holzwerkstoffen Opfer einer Ransomware-Attacke. Die Erpressergruppe RA World konnte bei dem Angriff 72 GB Unternehmensdaten entwenden.

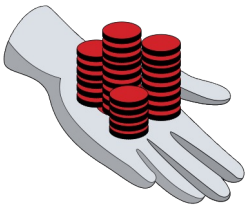
Was hätte man besser machen können?
Um Datendiebstahl zu vermeiden, sind regelmäßige Überwachung, Zugangskontrollen und Backups entscheidend. Auch Mitarbeiterschulungen zur Bedrohungserkennung hätten das Risiko verringern können.

Was lernen wir daraus:

Die RA World-Gruppe ist eine Ransomwaregruppe, die sich durch eine doppelte Erpressungsstrategie auszeichnet.

Das heißt die Angreifer verschlüsseln nicht nur Daten und fordern Lösegeld, sondern drohen auch damit sensible Informationen zu veröffentlichen oder weiterzuverbreiten, um zusätzlichen Druck auf die Opfer auszuüben.

Bei einem Angriff verschlüsselt die Ransomwaregruppe RA World Dateien und ändert deren Erweiterung zu „.RAWLD“, z.B. „1.jpg“ wird zu „1.jpg.RAWLD“. Nach der Verschlüsselung erstellt sie eine Lösegeldnotiz.



Anzunehmende Schadensfelder:

Quellen
https://hackmanac.com/news/hacks-of-today-21-03-2024
https://ransomfeed.it/index.php?page=post_details&id_post=13851

RIEDEL

Cyberkriminelle entwenden und verschlüsseln Unternehmensdaten von Frachtspediteur

19. März 2024, in Leuna/Sachsen-Anhalt

EINBRUCH

DATENDIEBSTAHL

RANSOMWARE

Was ist passiert?
Ein Frachtspeditionsdienstleister aus Sachsen-Anhalt wurde laut einer Cyberangriffsgruppe im März 2024 Opfer einer Ransomware-Attacke. Die Gruppe Hunters International entwendete und verschlüsselte 51 GB Unternehmensdaten bei diesem Angriff.

Was hätte man besser machen können?
Um Angriffe zu vermeiden, hätte man Sicherheitsmaßnahmen implementieren können. 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. Ein gut vorbereitetes Incident-Response-Team hätte zudem schneller auf verdächtige Aktivitäten reagieren können.

Anzunehmende Schadensfelder:

Was lernen wir daraus:

Speditionsunternehmen, die Teil der Lieferkette kritischer Infrastrukturen sind, müssen den Anforderungen der NIS2-Richtlinie (Netz- und Informationssystemsicherheit) nachkommen.

Mindestens die folgenden Cybersecurity-Maßnahmen müssen umgesetzt werden, um IT-Infrastruktur und Netzwerke kritischer Dienstleistungen zu schützen:

- **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

Quellen
https://www.ransomlook.io/group/hunters
https://x.com/RansomwareNews/status/1770175700907012529

RIEDEL

Münchner Ingenieurbüro soll Lösegeld zahlen

16. März 2024, in München/Bayern

EINBRUCH

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Die LockBit-Gruppe nannte im März 2024 ein Münchener Ingenieurbüro auf ihrer Darknet-Seite als eines ihrer Opfer. Die Cyberkriminellen drohten damit, die gestohlenen Daten zu veröffentlichen, wenn das Unternehmen nicht auf ihre Lösegeldforderung – deren Höhe unbekannt ist – eingeht.

Was hätte man besser machen können?
Das Ingenieurbüro 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.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/4743-LockBit-Bergmeister.PNG

Was lernen wir daraus:

Ransomware entwickelt sich ständig weiter. Anfangs waren Ransomware-Programme relativ einfach und nutzten grundlegende Verschlüsselungstechniken. Heute sind sie jedoch hochentwickelt und verwenden fortgeschrittene Verschlüsselungsalgorithmen, die es extrem schwierig machen, die Daten ohne den Entschlüsselungsschlüssel wiederherzustellen.

RIEDEL

Angriff auf IT-Dienstleister: Black Suite Gruppe bekennt sich zum Angriff

14. März 2024, in Bonn/Nordrhein-Westfalen

EINBRUCH

RANSOMWARE

Was ist passiert?
Im März 2024 wurde ein IT-Dienstleister aus NRW Ziel eines Cyberangriffs. Obwohl die Kommunikationssysteme nicht betroffen waren, könnten Kundendaten kompromittiert worden sein. Die Ransomwaregruppe "Black Suite" behauptet, hinter dem Angriff zu stecken. Auf der Darknet-Seite der Gruppe sind Daten zum Download verfügbar, doch deren genauer Inhalt ist noch unklar.

Was hätte man besser machen können?
Der IT-Dienstleister 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:

Viele Cyberkriminelle verwenden „Ransomware-as-a-Service“ (RaaS), ein Geschäftsmodell, das es ihnen ermöglicht, ihre Ransomware an andere Kriminelle zu vermieten.

RaaS senkt die technischen Barrieren für Angreifer, denen ein gewisses Know-how fehlt und erweitert die Verbreitung von Ransomware erheblich. Die Anbieter verdienen durch Provisionen und an den Lösegeldern, die ihre „Mieter“ einbringen.

Anzunehmende Schadensfelder:

Quellen
https://www.borncity.com/blog/2024/03/14/hacks-franzsische-arbeitsagentur-hansen-gieraths-und-mehr/
https://www.heise.de//news/Cyberangriffe-Keine-Ehre-unter-Kriminellen-Millionen-Franzosen-betroffen-9656333.html

RIEDEL

IT-Security bei Autohändler wirkt weniger sportlich wie dessen Verkaufsfahrzeuge

13. März 2024, in Hockenheim/Baden-Württemberg

RANSOMWARE

Was ist passiert?
Ein Autohändler aus Hockenheim wurde zum Opfer einer Ransomware-Attacke. Im Dezember 2023 tauchte das Unternehmen auf der Leakseite der Ransomwaregruppe "Snatch" im Darknet auf.

Was hätte man besser machen können?
Man hätte durch den Einsatz eines SOC den Angriff besser abwehren können. Wichtige Cybersecurity-Tools eines SOCs umfassen ein SIEM-System zur zentralen Überwachung und Analyse von Sicherheitsvorfällen, EDR zur Absicherung von Endgeräten, sowie Vulnerability Scanner zur regelmäßigen Identifizierung und Behebung von Schwachstellen.

Was lernen wir daraus:

Begrifflichkeiten aus dem Bereich der IT-Sicherheit wie

- **SIEM & SOC**
- **XDR**
- **EDR**
- **SOAR**
- **(D)DoS Protection**
- **Next Generation Firewalls**
- **SD-WAN**
- **SASE**

sind keine leeren Cybersecurity-Versprechen. Sie 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://x.com/H4ckManac/status/1767850424978100246
https://www.ransomlook.io/group/Snatch

RIEDEL

2 GB exfiltrierte Daten von Gebäudetechnik-Dienstleister in Hamburg

12. März 2024, in Hamburg/Hamburg

EINBRUCH

DATENDIEBSTAHL

ERPRESSUNG

Was ist passiert?
Im März 2024 wurde ein Dienstleistungsunternehmen für Gebäudetechnik von der Ransomwaregruppe Black Basta angegriffen. Dabei exfiltrierten die Täter 2 GB an sensiblen Daten, darunter Mitarbeiterinformationen, Verträge, Firmendaten und Buchhaltungsunterlagen.

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:

Angesichts der wachsenden Bedrohung durch Schadsoftware wie Ransomware ist es unerlässlich, eine robuste IT-Sicherheitsinfrastruktur aufzubauen.

Mit einer umfassenden Sicherheitslösung, die präventive Schutzmaßnahmen und regelmäßige Sicherheitsupdates integriert, können Unternehmen das Risiko, Opfer eines Angriffs zu werden, reduzieren und ihre sensiblen Daten vor Verschlüsselung und Erpressung schützen.

Anzunehmende Schadensfelder:

Quellen
https://x.com/explodingsec/status/1767606687341420622
https://www.breachsense.com/breaches/elmatic-data-breach/

RIEDEL

IT-Struktur eines Berliner Systemhauses wurde angegriffen

12. März 2024, in Berlin/Berlin

EINBRUCH

ERPRESSUNG

DATENDIEBSTAHL

Was ist passiert?
Ein Berliner Systemhaus für IT- und Cloud-Lösungen, wurde Mitte Februar 2024 Ziel eines Cyber-Angriffs. Obwohl weitere Standorte des Unternehmens und dessen Cloud-Dienste nicht betroffen waren, wurden vorsorglich alle internen IT-Systeme vom Internet getrennt, um Datenverluste zu minimieren.

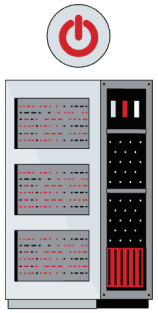
Es wurden 455 GB an sensiblen Daten gestohlen – darunter mutmaßlich Produktschlüssel, die für Kunden betreut werden und Zugangsdaten von Systemen.

Was hätte man besser machen können?
Um den Cyber-Angriff auf das Berliner Systemhaus zu verhindern oder die Auswirkungen zu minimieren, wären stärkere Netzwerksicherheitsmaßnahmen, regelmäßige Updates und Patches sowie verbesserte Zugriffskontrollen wichtig gewesen. Zudem hätten die Verschlüsselung sensibler Daten, regelmäßige Backups und eine kontinuierliche Überwachung der Systeme zur Prävention beigetragen.

Was lernen wir daraus:

Ein erfolgreicher Angriff gefährdet nicht nur die Sicherheit der eigenen Systeme, sondern auch die vertraulichen Daten und Geschäftsprozesse der Kunden.

Ein solcher Vorfall kann das Vertrauen in die Dienstleistung nachhaltig beschädigen, die Kundenbindung schwächen und den Wettbewerbsvorteil gefährden. Investitionen in fortschrittliche IT-Sicherheitslösungen sind essenziell, um sich und Kunden vor Cyberbedrohungen zu schützen und die Dienstleistungsqualität aufrechtzuerhalten.



Anzunehmende Schadensfelder:

Quellen
https://www.borncity.com/blog/2024/05/20/nachbetrachtung-blackbasta-angriff-auf-die-gfad-im-februar-2024/
https://web.archive.org/web/20240413183129/https://gfad.de/aktuelles/

RIEDEL

Deutscher Fensteranbieter taucht als Opfer im Darknet auf

11. März 2024, in Kronau/Baden-Württemberg

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Am 11. März 2024 listete die Ransomwaregruppe PLAY einen deutschen Fensterhersteller als Opfer auf ihrer Darknet-Seite. Vier Tage später, am 15. März, veröffentlichten die Hacker Teile der gestohlenen Daten, ohne die Art der Informationen genau zu benennen.

Was hätte man besser machen können?
Ein SOC hätte den Schaden durch frühzeitige Erkennung des Angriffs, schnelle Reaktion zur Eindämmung und effektive Kommunikation an das Management deutlich reduzieren können.

Was lernen wir daraus:

Als häufiges Einfallstor für Ransomware-Angriffe zählt Phishing. Angreifer senden täuschend echte E-Mails, um Benutzer dazu zu bringen, schadhafte Links zu klicken oder Anhänge zu öffnen. Diese Aktionen installieren Ransomware, die Dateien verschlüsselt und ein Lösegeld fordert.

Oft zielt Phishing darauf ab, Zugangsdaten zu stehlen, um weitere Sicherheitslücken im Unternehmensnetzwerk auszunutzen.

Anzunehmende Schadensfelder:

Quellen
https://ransomfeed.it/index.php?page=post_details&id_post=13682
https://www.security-incidents.de/assets/img/incidents/6001-bechtold-fenster-play-ransomware.png

RIEDEL

Ransomwaregruppe „PLAY“ und die Schokoladenfabrik

11. März 2024, in Mannheim/Baden-Württemberg

Was ist passiert?
Am 11. März 2024 wurde eine deutsche Schokoladenfabrik von der PLAY-Ransomwaregruppe als Opfer auf deren Darknet-Seite genannt. Am 15. März veröffentlichten die Angreifer nach eigenen Angaben die gesamte gestohlene, jedoch nicht näher spezifizierte Datenmenge.

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 erkannt. 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.

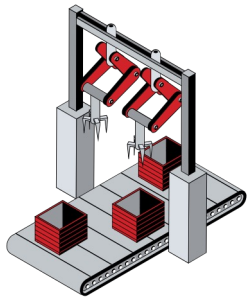
RANSOMWARE

DATENDIEBSTAHL

Was lernen wir daraus:

Wenn Cyberkriminelle Unternehmensdaten stehlen, riskieren Firmen nicht nur finanzielle Einbußen, sondern auch Betriebsunterbrechungen. Die wiederholte Wiederherstellung von Daten und die Implementierung neuer Sicherheitsmaßnahmen können den Betrieb erheblich stören.

Als langfristige Auswirkung entsteht die Notwendigkeit, umfassende Sicherheitsstrategien zu etablieren und zu stärken.



Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6002-schokinag-play-ransomware.png
https://ransomfeed.it/index.php?page=post_details&id_post=13680

RIEDEL

Cyberkriminelle verschafften sich Zugang zu hunderttausenden Datensätzen

8. März 2024, in Berlin/Berlin

DATENDIEBSTAHL

Was ist passiert?
Am 13. März 2024 meldete ein Berliner Druckerpatronenshop einen möglichen Cyberangriff, nachdem zwei Wochen zuvor eine Sicherheitslücke entdeckt und geschlossen wurde.

Ein Hacker namens Soni behauptet 344.000 Datensätze des Unternehmens erbeutet zu haben, die Namen, E-Mail-Adressen, Zahlungsinformationen und Geschlechtsidentitäten enthalten. Es gibt auch Hinweise, dass Soni Passwörter erbeutet hat, diese sind jedoch stark verschlüsselt.

Was hätte man besser machen können?
Man hätte nach der Schließung der Sicherheitslücke umfassende Tests durchführen und das System besser überwachen sollen. Bei Verdacht auf einen Angriff wäre eine sofortige Reaktion und Isolierung betroffener Systeme wichtig gewesen. Zudem hätten betroffene Nutzer sofortige Passwortänderungen und Sicherheitswarnungen erhalten sollen, um das Risiko zu minimieren.

Was lernen wir daraus:

Der Diebstahl von Passwörtern birgt erhebliche Risiken für Unternehmen, da Angreifer mit gestohlenen Anmeldedaten sehr einfach unbefugten Zugang zu sensiblen Systemen und Daten erhalten können. So können interne Netzwerke kompromittiert werden oder sogar Finanztransaktionen durchgeführt werden.

Anzunehmende Schadensfelder:

Quellen
https://www.golem.de/news/moegliches-datenleck-tonerdumping-kundendaten-stehen-zum-verkauf-2403-183194.html
https://www.toner-dumping.de/blog/sind-ihre-daten-in-unserem-onlineshop-sicher/

RIEDEL

Premiumhersteller von Gartenbauprodukten von Ransomware betroffen

5. März 2024, in Vechta/Niedersachsen

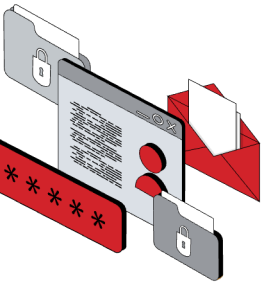
RANSOMWARE

Was ist passiert?
Im März 2024 wurde ein Premiumhersteller von Gartenbauprodukten von der Ransomwaregruppe Qilin angegriffen. Am 5. März 2024 tauchte das Unternehmen auf der Opferliste von Qilins Leakseite im Darknet auf.

Was hätte man besser machen können?
Man hätte den Angriff durch frühzeitige Sicherheitsüberprüfungen und kontinuierliche Überwachung der IT-Systeme verhindern können. Zudem hätte eine proaktive Incident-Response-Strategie es ermöglicht, bei ersten Anzeichen eines Angriffs schnell zu reagieren und Schäden zu minimieren.

Was lernen wir daraus:

Qilin – benannt nach dem chinesischen Fabeltier Einhorn – wurde erstmals im Juli 2022 gesichtet. Die Ransomwaregruppe ist bekannt für die Verbreitung der in Golang programmierten Agenda-Ransomware.



Anzunehmende Schadensfelder:

Quellen
https://www.borncity.com/blog/2024/03/05/sicherheit-hawita-gruppe-opfer-von-ransomware-nutzerdaten-von-klinik-gmp-academy-gl-sh-und-dasauge-im-netz/
https://ransomwareattacks.halcyon.ai/attacks/qilin-attacks-the-hawita-group

RIEDEL

Datendiebstahl bei Elektrogroßhandel aus Hessen

2. März 2024, in Freigericht/Hessen

DATENLECK

RANSOMWARE

EINBRUCH

DATENDIEBSTAHL

Was ist passiert?
Am 2. März 2024 meldete die LockBit-Gruppe, dass sie einen Elektrogroßhandel angegriffen habe. Die Angreifer veröffentlichten eine Vielzahl sensibler Daten des Elektrogroßhandels – darunter Inventurberichte, Rechnungen und andere interne Dokumente.

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:

Begriffe wie SIEM & SOC, XDR, EDR, SOAR, (D)DoS Protection, Next Generation Firewalls, SD-WAN und SASE sind weit mehr als nur Cybersecurity-Schlagworte. Sie sind entscheidende Komponenten für den proaktiven Schutz von Unternehmen gegen Cyberangriffe und helfen, Bedrohungen kontinuierlich einen Schritt vorauszubleiben. Diese Technologien und Konzepte stärken die Sicherheit und Widerstandsfähigkeit von IT-Infrastrukturen erheblich.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/5038-StarkPower-LockBit.PNG

RIEDEL

Druckerei wird Opfer eines Ransomware-Cyberangriffs

2. März 2024, in Bretten/Baden-Württemberg

DATENDIEBSTAHL

Was ist passiert?
Am 2. März 2024 listete LockBit 3.0 eine deutsche Druckerei als Opfer auf ihrer Darknet-Seite. Bisher fehlen genaue Informationen über den Umfang und die Details des Angriffs.

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.

Eine klare Kommunikation und transparente Berichterstattung über den Angriff hätten ebenfalls dazu beigetragen, den Umfang und die Details schneller zu klären.

Was lernen wir daraus:

Während große Unternehmen und Organisationen häufig Ziel von Ransomware-Angriffen sind, sind auch kleinere Unternehmen gefährdet. Angreifer zielen auf alle, die möglicherweise in der Lage sind, Lösegeld zu zahlen, und nutzen oft automatisierte Angriffe, um eine große Anzahl von potenziellen Opfern zu erreichen.

Anzunehmende Schadensfelder:

Quellen
https://ransomfeed.it/index.php?page=post_details&id_post=13559
https://thecyberexpress.com/lockbit-ransomware-group-claims-8-new-victims/

RIEDEL

Eingeschränkte Lieferfähigkeit nach Sicherheitsvorfall bei Leuchtmittel-Unternehmen

2. März 2024, in Springe/Niedersachsen

DATENLECK
RANSOMWARE
DATENPANNE
DATENDIEBSTAHL

Was ist passiert?
Am 8. April 2024 listete die Ransomwaregruppe Hunters International ein deutsches Leuchtmittel-Unternehmen auf ihrem Darknet-Blog als Opfer. Die Cyberkriminellen behaupteten, 320 GB an Daten gestohlen und veröffentlicht zu haben, nachdem ihre Forderungen nicht erfüllt wurden.

Das Unternehmen hatte bereits im Januar 2024 einen IT-Sicherheitsvorfall im Logistikbereich gemeldet, der vorübergehend die Lieferfähigkeit beeinträchtigte, bevor die Situation Mitte Februar wieder stabilisiert wurde.

Was hätte man besser machen können?
Das Unternehmen 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.

Was lernen wir daraus:

Ein robuster Aufbau der IT-Infrastruktur ist entscheidend, um Betriebsausfälle aufgrund von Cyberangriffen vorzubeugen. Durch Investitionen in eine starke und zuverlässige IT-Infrastruktur sichern Unternehmen ihre Betriebsabläufe und minimieren das Risiko kostspieliger Ausfälle.

Anzunehmende Schadensfelder:

Quellen
https://www.ndz.de/lokales/springe/hacker-erpressen-heimische-firmen-auch-paulmann-licht-in-voelksen-betroffen-YAD7DBFYF47ZZYA2A3B6ZEC433.html
https://www.security-incidents.de/assets/img/incidents/6019-Paulmann_Licht-Hunters.PNG

RIEDEL

Cyber-Spionage: Mitschnitte von deutschen Militärgesprächen in russischen Nachrichtenkanal

1. März 2024

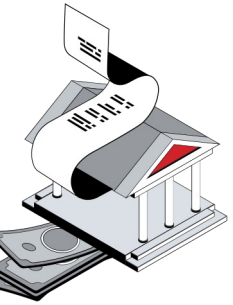
SPIONAGE

Was ist passiert?
Am 2. März 2024 wurde ein Gespräch deutscher Luftwaffen-Offiziere von Russia Today (RT) veröffentlicht. Der Mitschnitt, der über Cisco WebEx stattfand, deutet auf einen möglichen MITM-Angriff hin. Es wird vermutet, dass sich ein unbefugter Teilnehmer aus einem Hotel in Singapur zugeschaltet hat, möglicherweise über das Hotel-WLAN.

Was hätte man besser machen können?
Um den MITM-Angriff zu verhindern, hätte man Ende-zu-Ende-Verschlüsselung für die Kommunikation nutzen, gesicherte Netzwerke oder VPNs statt unsicherer Hotspots verwenden und strenge Zugangskontrollen für Webkonferenzen einführen sollen. Zudem wären Schulungen zur sicheren Nutzung von Kommunikationsplattformen hilfreich gewesen.

Was lernen wir daraus:

Man-in-the-Middle (MITM) Angriffe sind eine Methode, die Cyberkriminelle verwenden, um Daten abzufangen. Bei diesem Angriffstyp positioniert sich der Angreifer zwischen zwei kommunizierenden Parteien, um die übermittelten Informationen zu überwachen oder zu manipulieren, ohne dass die Opfer dies bemerken. Diese Technik wird oft in ungesicherten Netzwerken angewendet, wie bei offenen Wi-Fi-Hotspots.



Anzunehmende Schadensfelder:

Quellen
https://www.tagesspiegel.de/internationales/bundesregierung-in-erklarungsnot-russland-will-deutsche-luftwaffe-abgehort-haben-11301268.html
https://www.tagesschau.de/inland/bundeswehr-abhoerfall-100.html

RIEDEL

Phishing-Angriff auf Uniklinik

1. März 2024, in Brandenburg an der Havel/Brandenburg

EINBRUCH

AUSFALL

PHISHING

Was ist passiert?
Am 29. Februar 2024 wurde ein deutsches Universitätsklinikum Ziel eines Phishing-Angriffs. Cyberkriminelle infiltrierten die E-Mail-Systeme des Klinikums und versendeten von dort aus massenhaft Phishing-Nachrichten an die Kontakte des Krankenhauses. Die Sicherheitslücke betraf die interne Kommunikation und verbreitete potenziell schädliche E-Mails an externe Empfänger.

Was hätte man besser machen können?
Man hätte den Phishing-Angriff durch Schulungen zur Erkennung von Phishing-Mails, den Einsatz fortschrittlicher E-Mail-Sicherheitslösungen, Mehrstufige Authentifizierung für E-Mail-Konten und regelmäßige Sicherheitsüberprüfungen besser verhindern können.

Was lernen wir daraus:

Cyberkriminelle greifen gezielt Unternehmen kritischer Infrastrukturen an, mitunter im Gesundheitswesen, um maximalen Schaden anzurichten.

Diese Angriffe können nicht nur finanzielle Verluste verursachen, sondern auch öffentliche Sicherheit und den Betrieb wesentlicher Dienstleistungen gefährden. Derartige Angriffe zielen darauf ab, erhebliche Störungen und Panik zu verursachen.

Anzunehmende Schadensfelder:

Quellen
https://www.uk-brandenburg.de/aktuelles/details-zu/SPAM-Versand-hackerangriff

RIEDEL

FEBRUAR 2024

SECURITY INCIDENTS GERMANY

RIEDEL

Cyberangriff auf Behörde: Trojaner legt IT-Systeme lahm und verursacht Ausfälle

27. Februar 2024, in Neuburg-Schrobenhausen/Nordrhein-Westfalen

RANSOMWARE

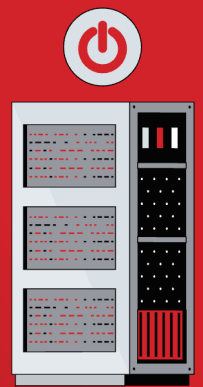
EINBRUCH

DATENDIEBSTAHL

Was ist passiert?
Am 27. Februar 2024 wurde eine Behörde aufgrund einer Trojaner-Infektion vom Internet getrennt, um die weitere Verbreitung des Virus zu verhindern.
Der E-Mail-Verkehr war stark beeinträchtigt, was dazu führte, dass bestimmte Abteilungen, die auf externe Netzwerke angewiesen sind, nicht arbeiten konnten. Bis zum Abend des 27. Februars war die Behörde nur telefonisch erreichbar. Es wurden keine Daten gestohlen.

Was hätte man besser machen können?
Um solche Vorfälle besser bewältigen zu können, hätte man den Einsatz von XDR und EDR zur erweiterten Bedrohungserkennung und -reaktion auf allen Endpunkten und Netzwerken in Betracht ziehen sollen. Die Implementierung von SIEM-Systemen zur kontinuierlichen Überwachung und Analyse von Sicherheitsereignissen wäre ebenfalls hilfreich gewesen.

Anzunehmende Schadensfelder:



Was lernen wir daraus:

Folgende Strategien helfen immens dabei, Angriffe zu erkennen und zu verhindern, ohne Schaden an kritischer Infrastruktur zu verursachen.

- **XDR und EDR**: Erweiterte Bedrohungserkennung und -reaktion auf allen Endpunkten und Netzwerken.
- **SIEM**: Kontinuierliche Überwachung und Analyse von Sicherheitsereignissen.
- **Schwachstellenbewertungen**: Regelmäßige Identifizierung und Schließung von Sicherheitslücken.
- **SOAR**: Automatisierung und Koordination der Sicherheitsmaßnahmen.
- **Proaktive Cybersicherheitsstrategie**: Ganzheitlicher Ansatz zur Stärkung der Gesamtsicherheit und Minimierung der Auswirkungen von Cyberangriffen.

Quellen
https://www.donaukurier.de/lokales/landkreis-neuburg-schrobenhausen/trojaner-legt-landratsamt-lahm-15534301

RIEDEL

Einbruch bei Hochschule: Angreifer verschlüsseln und löschen Daten

AUSFALL

27. Februar 2024, in Allgäu/Bayern

Was ist passiert?
Am 27. Februar 2024 wurde eine Hochschule Ziel eines Cyberangriffs, wie in einer öffentlichen Mitteilung bekanntgegeben wurde. Demnach gelang es den Angreifern, auf Teile der IT-Infrastruktur der Bildungseinrichtung zuzugreifen. Der Präsident der Hochschule berichtete, dass einige Laufwerke verschlüsselt oder gelöscht wurden.

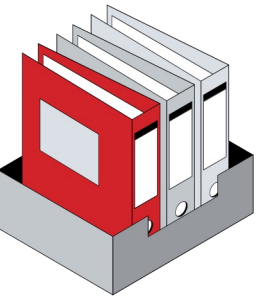
Als Reaktion auf den Vorfall wurde der Zugang zu mehreren IT- und Kommunikationssystemen eingeschränkt.

Was hätte man besser machen können?
Durch den Einsatz von SIEM-Systemen hätten Sicherheitsereignisse und -warnungen in Echtzeit überwacht und analysiert werden können, um frühzeitig auf verdächtige Aktivitäten zu reagieren.

Auch durch die Implementierung von XDR-Lösungen hätte die Hochschule eine umfassende, integrierte Sicherheitsüberwachung erhalten.

Was lernen wir daraus:

- **Integrierte Sicherheitslösungen** nutzen: XDR bietet umfassende Überwachung und schnelle Reaktion.
- **Echtzeit-Überwachung** ist entscheidend: Systeme wie SIEM und EDR verbessern die Bedrohungserkennung.
- **Regelmäßige Backups** sind unerlässlich: Sicherstellen, dass Daten im Notfall schnell wiederhergestellt werden können.
- **Transparente Kommunikation**: Klare und zeitnahe Informationen helfen, Vertrauen zu erhalten.
- **Nachbereitung** nutzen: Analyse des Vorfalls zur Verbesserung der Sicherheitsstrategien.



Anzunehmende Schadensfelder:

Quellen
https://www.hs-kempten.de/hochschule/aktuelles/artikel/hacker-angriff-auf-die-hochschule-kempten-2598

RIEDEL

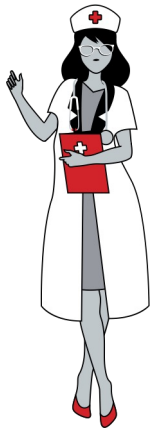
Cyberangriff lähmt Deutsches Rotes Kreuz

AUSFALL

26. Februar 2024, in Mannheim/Baden-Württemberg

Was ist passiert?
In der Nacht vom 26. auf den 27. Februar 2024 wurde das Deutsche Rote Kreuz (DRK) Ziel eines Cyberangriffs. Der Angriff führte zur Einschränkung der telefonischen und per E-Mail erreichbaren Kommunikation, da die IT-Infrastruktur präventiv heruntergefahren wurde. Zusätzlich verzögern sich Zahlungsvorgänge. Obwohl die Angreifer versuchten, die Firewalls zu überwinden, gelang ihnen dies nicht. Die Abschaltung des Systems war eine vorsorgliche Maßnahme.

Was hätte man besser machen können?
Man hätte den Cyberangriff besser bewältigen können, indem man proaktive Sicherheitsüberprüfungen und regelmäßige Tests der IT-Infrastruktur durchgeführt hätte, um Schwachstellen frühzeitig zu identifizieren. Ein robuster Notfallplan hätte sicherstellen können, dass Kommunikationskanäle und Zahlungsvorgänge weniger beeinträchtigt werden. Zudem wäre eine stärkere Segmentierung der IT-Systeme sinnvoll gewesen, um sicherzustellen, dass ein Angriff nicht alle Bereiche des Systems gleichzeitig lahmlegt.



Anzunehmende Schadensfelder:

Quellen
https://www.sentiguard.eu/wissen/drk-mannheim-nach-hackerangriff-schwer-erreichbar/
https://www.drk-mannheim.de/aktuelles/presse/meldung/aktuell-kommt-es-zu-stoerungen.html

Was lernen wir daraus:

Obwohl eine vollständige Sicherheit vor Cyberangriffen nicht gewährleistet werden kann, können Unternehmen einen effektiven Schutz erreichen, indem sie regelmäßig ihre Sicherheitsmaßnahmen aktualisieren und bewährte Praktiken umsetzen.

Der Grund, warum ein 100% Schutz nicht möglich ist, liegt darin, dass Cyberkriminelle stets neue Techniken entwickeln und Schwachstellen in Systemen ausnutzen. Zudem müssen Unternehmen auch menschliche Fehler einkalkulieren. Obwohl Schulungen helfen können, diese zu minimieren, können sie nie ganz ausgeschlossen werden.

RIEDEL

Ransomware Angriff auf Deutschlands größten Stahlhersteller

23. Februar 2024, in Essen/Nordrhein-Westfalen

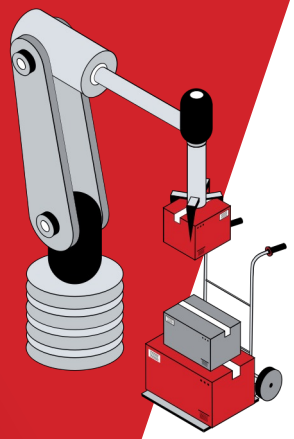
RANSOMWARE

EINBRUCH

Was ist passiert?
Am 23. Februar 2024 erlebte Deutschlands größter Stahlhersteller einen Cyberangriff, der mehrere Werke, insbesondere in der Automotive-Sparte, zum Stillstand brachte. Ein Werk im Saarland mit 1000 Mitarbeitern war betroffen.
Die Durchführung des Angriffs wurde erst im Nachhinein festgestellt. Andere Bereiche des Unternehmens blieben unversehrt. Am 29. Februar 2024 bestätigte ein Sprecher, dass es sich um einen vereitelten Ransomware-Angriff handelte.

Was hätte man besser machen können?
Um den Ransomware-Angriff auf den Stahlhersteller 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:

Prävention und die Implementierung von Protokollen sind entscheidend, um sich sowohl proaktiv als auch reaktiv vor Angriffen zu schützen. Ein spezialisiertes Security Operations Center (SOC) spielt dabei eine zentrale Rolle. Es dient nicht nur als präventive Maßnahme, sondern ist auch in der Lage, zusätzliche Sicherheitslösungen und Protokolle einzuführen, um die Sicherheit einer Institution umfassend zu gewährleisten.

Anzunehmende Schadensfelder:

Quellen
https://www.donaukurier.de/lokales/landkreis-neuburg-schrobenhausen/trojaner-legt-landratsamt-lahm-15534301

RIEDEL

Ransomware-Angriff auf hessische Verbraucherorganisation

22. Februar 2024, in Frankfurt am Main/Hessen

AUSFALL

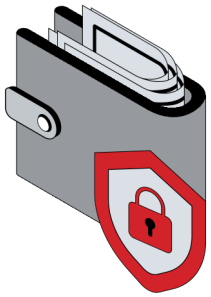
RANSOMWARE

Was ist passiert?
Am 22. Februar 2024 verschlüsselten unbekannte Angreifer die Server und Backup-Systeme einer hessischen Verbraucherorganisation und hinterließen eine Nachricht für Polizei und IT-Experten. Obwohl die Webseite anfänglich funktionierte, waren später auch Telefon- und E-Mail-Dienste eingeschränkt. Am 1. März wurde bekannt, dass die Ransomwaregruppe ALPHV/BlackCat die Organisation als Opfer gelistet hatte. Die genaue Vorgehensweise blieb bislang unklar.

Was hätte man besser machen können?
Um solche Angriffe zu verhindern, hätte man SIEM und EDR implementieren sollen. SIEM hätte durch kontinuierliche Überwachung und Analyse von Sicherheitsdaten frühzeitig Anomalien erkannt, während EDR verdächtige Aktivitäten auf Endgeräten schnell identifiziert und neutralisiert hätte.
Ergänzend hätte ein Vulnerability Assessment potenzielle Sicherheitslücken erkannt und geschlossen, um das Risiko eines erfolgreichen Angriffs zu minimieren.

Was lernen wir daraus:

Der Angriff auf sowohl Server als auch Backup-Systeme zeigt, wie wichtig es ist, Backups physisch oder digital getrennt vom Hauptsystem zu speichern. Dies kann durch Nutzung von Offsite-Backups, Cloud-Diensten oder sogar physischen Medien an getrennten Standorten erfolgen. Dadurch wird sichergestellt, dass im Falle eines Angriffs oder einer Katastrophe die Daten weiterhin wiederhergestellt werden können.



Anzunehmende Schadensfelder:

Quellen
https://www.verbraucherzentrale-hessen.de/pressemeldungen/verbraucherzentrale/hackerangriff-auf-verbraucherzentrale-hessen-92732

RIEDEL

Monti-Ransomwaregruppe veröffentlicht gestohlene Daten

23. Februar 2024, in Hamburg/Hamburg

RANSOMWARE

DATENDIEBSTAHL

Was ist passiert?
Am 23. Februar 2024 erklärte die Monti-Ransomwaregruppe, dass ein Hamburger Speditionsunternehmen Opfer eines Cyberangriffs wurde. Am 27. Februar aktualisierte die Gruppe ihre Darknet-Seite und gab bekannt, dass alle erbeuteten Daten veröffentlicht wurden.

Was hätte man besser machen können?
Man hätte den Angriff durch frühzeitige Erkennung, schnelle Reaktion und effektives Incident-Response besser abwehren können.

Zudem hätten regelmäßige Sicherheitsprüfungen und eine solide Backup-Strategie den Schaden möglicherweise minimiert.

Was lernen wir daraus:

Viele Cyberkriminelle nutzen „Ransomware-as-a-Service“ (RaaS), ein Modell, das ihnen erlaubt, Ransomware an andere Kriminelle zu vermieten. Mit RaaS werden die technischen Barrieren für Angreifer ohne tiefgehendes Know-how gesenkt und die Verbreitung von Ransomware massiv erhöht. Anbieter des Service verdienen durch Provisionen und Anteile an den Lösegeldern, die ihre „Mieter“ erbeuten, und bieten oft zusätzliche Unterstützung und maßgeschneiderte Tools.

Anzunehmende Schadensfelder:

Quellen
https://ransomfeed.it/index.php?page=post_details&id_post=13413
https://www.security-incidents.de/assets/img/incidents/6000-apex-spedition-monti.png

RIEDEL

Ransomware-Angriff auf kirchliche Organisation

18. Februar 2024, in Hannover/Niedersachsen

AUSFALL

RANSOMWARE

Was ist passiert?
Am 18. Februar 2024 fiel eine kirchliche Organisation einem Ransomware-Angriff zum Opfer. Die Organisation bestätigte den Vorfall am nächsten Tag und teilte mit, dass die Angreifer unbefugten Zugriff auf ihre IT-Infrastruktur erlangt hatten. Um die Sicherheit zu gewährleisten, wurden daraufhin mehrere zentrale Computersysteme vorsorglich abgeschaltet.

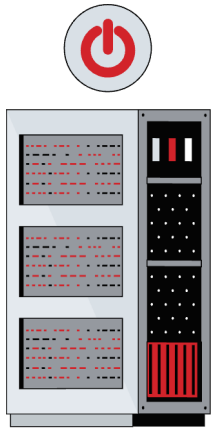
Betroffen von den Maßnahmen waren unter anderem die zentralen Verwaltungsbüros und weitere wichtige Abteilungen der Organisation.

Was hätte man besser machen können?
Ein SIEM-System hätte den Ransomware-Angriff frühzeitig erkennen und durch automatische Gegenmaßnahmen eindämmen können. Es bietet Echtzeitüberwachung, ermöglicht schnelle Reaktionen und unterstützt die forensische Analyse.

Zudem verbessert es kontinuierlich die Sicherheitsinfrastruktur durch detaillierte Berichte und Audits, was zukünftige Angriffe erschwert.

Was lernen wir daraus:

Kirchliche Organisationen sammeln oft umfangreiche persönliche Daten von Mitgliedern und Spendern, einschließlich Adressen, Finanzdaten und religiöser Präferenzen. Diese Informationen sind wertvoll für Identitätsdiebstahl, Phishing-Angriffe oder Erpressung. Hinzu kommt, dass viele kirchliche Organisationen begrenzte Ressourcen für IT-Sicherheit und –Schutz haben, was sie anfälliger für Angriffe macht.



Anzunehmende Schadensfelder:

Quellen
https://www.landeskirche-hannovers.de/presse/pressemeldungen-landeskirche/2024/02/19-hackerangriff-auf-zentrale-it-systeme-der-landeskirche-hannovers

RIEDEL

PLAY-Ransomware attackiert Designstudio: Drohung mit Datenveröffentlichung

15. Februar 2024, in Blomberg/Nordrhein-Westfalen

ERPRESSUNG

DATENDIEBSTAHL

Was ist passiert?
Am 15. Februar 2024 listete die PLAY-Gruppe ein deutsches Designstudio als Opfer auf. Die Cyberkriminellen behaupten, zahlreiche sensible Informationen, einschließlich interner Finanzdaten, Klientendetails und Personalinformationen, gestohlen zu haben. Sie drohen, diese Daten am 21. Februar 2024 zu veröffentlichen.

Was hätte man besser machen können?
Um den Schaden zu minimieren, hätte das Designstudio durch den Einsatz von XDR zur umfassenden Bedrohungserkennung und SOAR zur automatisierten Reaktion auf Sicherheitsvorfälle besser vorbereitet sein können. Zudem hätten Next-Generation Firewalls und eine starke VPN-Nutzung das Risiko eines Angriffs verringert. Eine regelmäßige Überprüfung der Sicherheitsinfrastruktur und das Implementieren eines soliden Backup-Systems hätten zusätzlich dazu beigetragen, den drohenden Datenverlust zu verhindern.

Was lernen wir daraus:

Hacker verfolgen verschiedene Ziele, darunter das Sammeln von Daten für spezifische Zwecke, das Erzielen schneller finanzieller Gewinne durch Lösegeldforderungen oder das Verdienen von Geld durch den Verkauf gestohlener Daten im Darknet. Ihre Motivationen sind vielfältig und reichen von finanziellen Anreizen bis hin zu gezielten Informationsbeschaffungen.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/5997-vonHagen-PLAY.png

RIEDEL

AUSFALL

Cyberangriff auf Software-Dienstleister

15. Februar 2024, in Berlin/Berlin

Was ist passiert?
Nach einem Ransomware-Angriff auf ein deutsches Softwareunternehmen wurden die IT-Systeme vom Internet getrennt, um Datenschutzverletzungen zu verhindern. Die Webseite wurde vorübergehend offline genommen. Eine statische Seite mit Vorfall-Informationen wurde eingerichtet.
Das Bundesamt für Sicherheit in der Informationstechnik und das Landeskriminalamt Berlin wurden informiert. IT-Forensiker prüften die Auswirkungen des Angriffs, der keine Kundensysteme oder Remote-Zugänge betraf.

Was hätte man besser machen können?
Man hätte den Vorfall besser bewältigen können, wenn sowohl ein SIEM als auch ein SOAR eingesetzt worden wären. Das SIEM-System hätte durch die Sammlung und Analyse von Sicherheitsdaten zur frühzeitigen Erkennung des Angriffs beigetragen. Das SOAR-System hätte automatisierte Reaktionen und koordinierte Maßnahmen ermöglicht, um den Vorfall effizient zu verwalten. Zusätzlich hätten regelmäßige Sicherheitsüberprüfungen und sichere, getrennte Backup-Systeme eine schnellere Wiederherstellung unterstützt und den Schaden minimiert.

Anzunehmende Schadensfelder:

Quellen
https://www.heise.de//news/Cyberangriff-auf-PSI-Software-Kunden-wohl-nicht-betroffen-Ermittlungen-laufen-9632088.html

Was lernen wir daraus:

Cyberangriffe sind meist geschäftsschädigend, da sie oft zu erheblichen finanziellen Verlusten führen, sei es durch direkte Schäden wie Diebstahl von Daten oder durch teure Wiederherstellungsmaßnahmen. Zudem kann der Verlust von Kundenvertrauen langfristige Auswirkungen haben: Kunden könnten sich von einem Unternehmen abwenden, wenn ihre Daten gefährdet wurden, was zu einem nachhaltigen Rückgang der Umsätze führt.

RIEDEL

Automobilgigant leidet an Datenleck durch internen Fehler

14. Februar 2024, in München/Bayern

DATENLECK

FEHLER

Was ist passiert?
Ein Datenleck auf einem MS Azure Cloud-Server eines bekannten Automobilgiganten wurde durch einen Sicherheitsscan entdeckt. Der Server war aufgrund einer Fehlkonfiguration versehentlich öffentlich zugänglich, was den Zugriff auf Zugangsdaten, geheime Schlüssel und vertrauliche Unternehmensinformationen ermöglichte.

Ein Pressesprecher des Unternehmens bestätigte, dass keine personenbezogenen Daten betroffen waren.

Was hätte man besser machen können?
Regelmäßige, automatisierte Sicherheitsscans hätten frühzeitig Fehlkonfigurationen erkennen können und sollten Teil eines kontinuierlichen Überwachungsprozesses sein. Zudem hätten vertrauliche Daten wie geheime Schlüssel und Unternehmensinformationen zusätzlich verschlüsselt gespeichert werden müssen, sodass ein potenzieller Datenleck diese nicht sofort zugänglich macht.

Was lernen wir daraus:

Dieser Vorfall verdeutlicht, dass Bedrohungen nicht nur von außen, sondern auch aus dem Inneren eines Systems stammen können. Fehlkonfigurationen stellen ebenso große Risiken dar wie externe Angriffe. Um sowohl interne als auch externe Gefahren frühzeitig zu identifizieren und zu beheben, sind regelmäßige Sicherheitsüberprüfungen und automatisierte Reaktionssysteme wie SOAR von entscheidender Bedeutung.

Anzunehmende Schadensfelder:

Quellen
https://techcrunch.com/2024/02/14/bmw-security-lapse-exposed-sensitive-company-information-researcher-finds/

RIEDEL

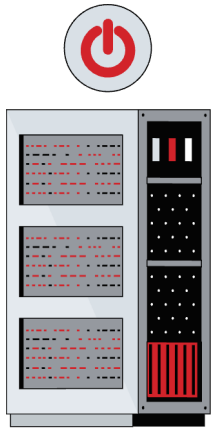
AUSFALL

Serviceausfall: Kundenwebseiten und Control Panels vorübergehend offline

14. Februar 2024, in Karlsruhe/Baden-Württemberg

Was ist passiert?
Am 14. Februar 2024 kam es am frühen Nachmittag bei einem Netzwerk-Host zu einem Ausfall, der mehrere Services, einschließlich Kundenwebseiten und Control Panels, unerreichbar machte. Auch die Status-Webseite war zeitweise nicht verfügbar. Um 15:59 wurde das Problem vorläufig behoben, vollständige Entwarnung gab es jedoch erst abends. Informationen zur Ursache des Ausfalls wurden nicht bereitgestellt.

Was hätte man besser machen können?
Um den Ausfall besser zu bewältigen, hätte man proaktive Monitoring-Tools wie ein umfassendes Netzwerk-Überwachungssystem einsetzen können, um Probleme frühzeitig zu erkennen und sofortige Benachrichtigungen zu erhalten. Eine schnellere Reaktionszeit durch ein gut organisiertes Incident-Response-Team hätte dazu beigetragen, den Ausfall schneller zu beheben. Zudem hätte eine transparente Kommunikation über den Status der Problemlösung und regelmäßige Updates zur Ursache des Ausfalls die Situation für Kunden und interne Stakeholder klären können.



Anzunehmende Schadensfelder:

Quellen
https://x.com/julklr/status/1757769582553526568?s=20
https://www.netcup-status.de/

Was lernen wir daraus:

Systemausfälle können erhebliche Störungen für Unternehmen verursachen, da sie den Zugriff auf kritische Daten und Anwendungen unterbrechen. Sie können durch Hardwarefehler, Softwareprobleme oder Cyberangriffe verursacht werden und führen oft zu Betriebsunterbrechungen und finanziellen Verlusten.

Eine präventive Wartung, regelmäßige Sicherheitsüberprüfungen und effektive Notfallpläne sind daher unerlässlich, um die Auswirkungen von Systemausfällen zu minimieren und die Betriebskontinuität sicherzustellen.

RIEDEL

Cyber-Attacke auf Berliner Hochschule

14. Februar 2024, in Berlin/Berlin

EINBRUCH

VERSCHLÜSSELUNG

AUSFALL

Was ist passiert?
Am 14. Februar 2024 erlangten Angreifer Zugang zu einem Campus-Account einer Berliner Hochschule und begannen, das Netzwerk zu durchsuchen und zu infiltrieren. Am 20. Februar verschlüsselten sie 252 virtuelle Server. Das Hochschulrechenzentrum stoppte die Verschlüsselung und unterbrach alle IT-Dienste, um weiteren Schaden zu verhindern.

Das Hochschulnetzwerk wurde getrennt und eine forensische Analyse wurde gestartet.

Was hätte man besser machen können?
Zur Vermeidung solcher Angriffe hätte eine zentrale SIEM-Überwachung geholfen. Regelmäßige Schwachstellenscans und besseres Asset-Management wären ebenfalls wichtig gewesen. Eine stärkere Netzwerksegmentierung hätte die Ausbreitung begrenzt.

Ein SOC hätte all diese Maßnahmen koordiniert und den Angriff frühzeitig erkennen können.

Was lernen wir daraus:

- **Mehrfaktorauthentifizierung (MFA)** ist unerlässlich, um das Risiko von Zugang durch gestohlene Passwörter zu minimieren.
- **Umfassende und zentrale Überwachung** sind notwendig, um frühzeitig Anzeichen von Infektionen zu erkennen.
- **Regelmäßige Updates und effektives Asset-Management** sind wichtig, um Schwachstellen zu schließen und Systeme aktuell zu halten.
- **Stärkere Netzwerksegmentierung** kann die Ausbreitung von Angriffen innerhalb des Netzwerks begrenzen.
- **Ein gut etabliertes SOC (Security Operations Center)** kann helfen, Sicherheitsmaßnahmen zentral zu koordinieren und Angriffe effektiv zu überwachen und zu verhindern.

Anzunehmende Schadensfelder:

Quellen
https://www.bht-berlin.de/fileadmin/oe/hrz/akira-post-mortem.pdf
https://www.tagesspiegel.de/wissen/sicherheitsvorfall-berliner-hochschule-fur-technik-von-cyberangriff-betroffen-11243161.html

RIEDEL

Black Basta-Ransomware veröffentlicht 585 GB Daten eines Eventdienstleisters

13. Februar 2024, in Düsseldorf/Nordrhein-Westfalen

EINBRUCH

Was ist passiert?
Am 13. Februar 2024 listete die Ransomwaregruppe Black Basta einen großen deutschen Eventdienstleister auf deren Webseite als Opfer. Die Cyberkriminellen behaupten, etwa 585 GB an Daten erbeutet zu haben, darunter Personaldokumente, Kundendateien, Unternehmensdokumente und Finanzunterlagen. Laut ihrer Darknet-Seite wurden die gestohlenen Daten vollständig veröffentlicht.

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:

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.

Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/5999-btl-group-black-basta.png
https://ransomfeed.it/index.php?page=post_details&id_post=13266

RIEDEL

SYSTEMFEHLER

Systemfehler bei Software-Dienstleister

14. Februar 2024, in Essen/Nordrhein-Westfalen

Was ist passiert?
Durch einen Konfigurationsfehler am 25. Dezember 2023 wurden Zugangsdaten zu einem Arzttermin-Vergabedienst öffentlich zugänglich, wodurch Sicherheitsforscher Zugriff auf Hunderttausende Patientendaten erhielten. Die Ursache war ein öffentlich erreichbarer PHP Symfony Profiler, der Zugangsdaten im Klartext speicherte. Nachdem die Sicherheitslücke Anfang Januar 2024 gemeldet wurde, wurde das Problem behoben. Es gibt derzeit keine Hinweise auf Datenmissbrauch und die betroffenen Kunden wurden informiert.

Was hätte man besser machen können?
Um den Vorfall zu verhindern, hätten Debug-Logs und sensible Daten nicht öffentlich zugänglich sein dürfen.

Regelmäßige Sicherheitsüberprüfungen, die Verschlüsselung von Zugangsdaten, sowie eine schnelle Reaktion durch ein Incident-Response-Team wären wichtig gewesen.

Anzunehmende Schadensfelder:

Was lernen wir daraus:

Gefahren können nicht nur von außen, sondern auch aus dem Inneren eines Unternehmens entstehen. Es ist nicht immer ein externer Hacker, der Schaden anrichtet – manchmal genügen bereits einfache Fehler. Daher ist es entscheidend, umfassende Vorkehrungen zu treffen, um sich sowohl vor externen Bedrohungen als auch vor internen Risiken zu schützen.

Quellen
https://www.dubidoc.de/presse/sicherheitsluecke-bei-dubidoc-und-was-wir-daraus-gelernt-haben/

RIEDEL

Hackerangriff auf ehemaligen SDAX-Konzern

EINBRUCH

12. Februar 2024, Ellwangen/Baden-Württemberg

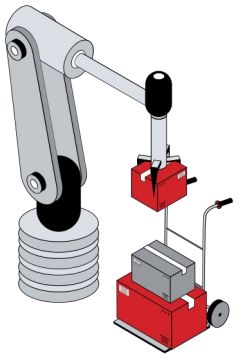
Was ist passiert?
Am 12. Februar 2024 wurde ein Batteriehersteller von einem Hackerangriff getroffen, der alle Produktionsstandorte und die Verwaltung betraf. Die IT-Systeme wurden heruntergefahren und Internetverbindungen getrennt. Bis Mitte März lief die Produktion wieder weitgehend normal, doch die Erreichbarkeit blieb eingeschränkt.

Der Geschäftsbericht konnte nicht rechtzeitig eingereicht werden, was das Risiko eines Verlusts des SDAX-Platzes erhöhte.

Was hätte man besser machen können?
Um die Auswirkungen des Angriffs zu minimieren, hätte man stärkere Sicherheitsvorkehrungen treffen, Notfallpläne ausarbeiten und regelmäßig testen können. Eine bessere Segmentierung der IT-Systeme, regelmäßige Backups und Mitarbeiter-Schulungen wären ebenfalls hilfreich gewesen. Proaktive Überwachung und Threat Intelligence hätten zudem frühzeitig auf potenzielle Bedrohungen hingewiesen.

Was lernen wir daraus:

Cyberangriffe auf SDAX-Unternehmen nehmen zu und stellen eine ernste Bedrohung dar. Die mittelgroßen Firmen sind oft weniger stark abgesichert als große Konzerne, was sie zu attraktiven Zielen macht. Angriffe können Betriebsabläufe stören, sensible Daten stehlen und den Ruf nachhaltig schädigen. Die finanziellen Verluste und die Wiederherstellung der Sicherheitssysteme sind erheblich. Daher müssen SDAX-Unternehmen verstärkt in Cybersicherheit investieren, um sich zu schützen.



Anzunehmende Schadensfelder:

Quellen
https://www.golem.de/news/nach-cyberangriff-varta-kann-geschaeftsbericht-nicht-fristgerecht-vorlegen-2403-183239.html

RIEDEL

E-Rezepte bundesweit blockiert

AUSFALL

14. Februar 2024, in Berlin/Berlin

Was ist passiert?
Am 14. Februar 2024 fiel die Telematik-Infrastruktur für fast eine Stunde komplett aus. Ein Fehler bei der Überprüfung von Gerätezertifikaten führte zu einer Störung der zentralen Dienste. Während des Ausfalls konnten bundesweit keine E-Rezepte ausgestellt oder eingelöst werden, wodurch Arztpraxen und Apotheken auf Papierrezepte umsteigen mussten.

Was hätte man besser machen können?
Eine umfassendere Testphase bei der Einführung oder Änderung von Zertifikatsüberprüfungen hätte potenzielle Fehler identifizieren können. Zudem wäre eine stärkere Redundanz in der Infrastruktur hilfreich gewesen, um den Ausfall kritischer Dienste zu vermeiden. Ein schnelleres und klareres Krisenmanagement, einschließlich Notfallplänen für Arztpraxen und Apotheken, hätte die Auswirkungen des Ausfalls weiter minimieren können.

Was lernen wir daraus:

Die fortschreitende Digitalisierung bringt viele Vorteile, birgt jedoch auch Risiken, insbesondere bei Systemausfällen. Wenn digitale Systeme versagen, können wichtige Geschäftsprozesse, Daten und Kommunikationswege beeinträchtigt werden. Solche Ausfälle können zu erheblichen Betriebsstörungen, finanziellen Verlusten und einem Rückgang der Kundenvertrauen führen. Daher ist es entscheidend, robuste Notfallpläne und Wiederherstellungsstrategien zu entwickeln, um die Auswirkungen solcher Ausfälle zu minimieren und den Betrieb aufrechtzuerhalten.

Anzunehmende Schadensfelder:

Quellen
https://www.gematik.de/newsroom/news-detail/aktuelles-ausfall-telematikinfrastruktur

RIEDEL

Hackerangriff auf Krankenhaus in Niedersachsen

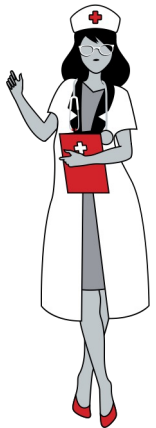
9. Februar 2024, in Coppenbrügge/Niedersachsen

RANSOMWARE

AUSFALL

Was ist passiert?
Ein Krankenhaus in Niedersachsen wurde am Freitag von einem Cyberangriff getroffen, der EDV-Systeme und die Telekommunikation lahmlegte. Die Polizei bestätigte den Vorfall und externe IT-Experten untersuchten die Systeme, um sie wiederherzustellen. Die Angreifer forderten ein Lösegeld, auf das das Krankenhaus nicht einging. In der Zwischenzeit half die Feuerwehr mit Funkgeräten aus und das Krankenhaus stellte auf schriftliche Patientenakten um. Die genaue Art des Angriffs blieb unklar.

Was hätte man besser machen können?
Im Vorfeld hätte das Krankenhaus spezialisierte Sicherheitslösungen und kontinuierliche Schwachstellenanalysen durchführen können. 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.



Anzunehmende Schadensfelder:

Quellen
https://www.ndr.de/nachrichten/niedersachsen/hannover_weser-leinegebiet/Nach-Cyberangriff-Klinik-versucht-Schaden-zu-beheben,cyberangriff170.html

Was lernen wir daraus:

Der Cyberangriff auf das Krankenhaus in Niedersachsen verdeutlicht die wachsende Relevanz von Sicherheitsvorgaben wie der NIS2-Richtlinie (Network and Information Security Directive 2), die in der EU für den Schutz kritischer Infrastrukturen wie das Gesundheitswesen eingeführt wurde. Diese Richtlinie fordert von betroffenen Einrichtungen, robuste Cybersecurity-Maßnahmen zu implementieren und regelmäßig zu überprüfen, um solchen Angriffen besser begegnen zu können.

RIEDEL

Exotischer Nahrungsexporteur erleidet Ransomware-Angriff

12. Februar 2024, in Verden/Niedersachsen

RANSOMWARE

EINBRUCH

DIEBSTAHL

Was ist passiert?
Am 12. Februar 2024 wurde ein Nahrungs-Exporteur Ziel einer Ransomware-Attacke. Die Erpressergruppe Hunters International behauptete, dass sie eine erhebliche Menge an Daten exfiltriert hatte. Insgesamt sollen 438,9 GB an Informationen gestohlen worden sein, darunter Audits und Anrufbeantworter-Aufnahmen. Am 15. Februar 2024 veröffentlichte die Gruppe die gesamten erbeuteten Daten.

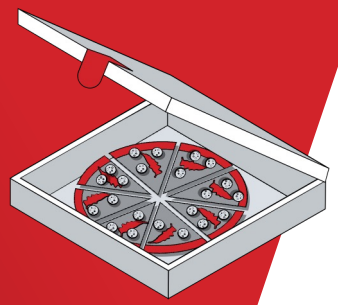
Was hätte man besser machen können?
Zur Minimierung der Angriffsfolgen hätte das Unternehmen fortschrittliche Sicherheitslösungen wie fortlaufende Schwachstellenanalysen und spezialisierte Bedrohungserkennungssysteme nutzen können. Zudem wäre eine effektive Reaktion auf Sicherheitsvorfälle, unterstützt durch gezielte Mitarbeiterschulungen und umfassende Backup-Strategien, entscheidend gewesen.

Die Implementierung von Zugriffs- und Netzwerkssegmentierung hätte zudem geholfen, die Schadensausbreitung zu begrenzen.

Was lernen wir daraus:

Für Nahrungsexporteure ist starke Cybersicherheit essenziell, da ihre Branche zu den Kritischen Infrastrukturen (KRITIS) gehört. Ein Cyberangriff könnte die Versorgungskette stören, was weitreichende Folgen für die Bevölkerung haben kann. Zudem sind Exporteure durch die internationale Vernetzung besonders gefährdet. Schutzmaßnahmen sind daher unerlässlich, um die Integrität der Lieferkette, sensible Daten und das Vertrauen der Kunden zu sichern.

Anzunehmende Schadensfelder:



Quellen
https://x.com/H4ckManac/status/1756998095370387548

RIEDEL

Ransomwaregruppe stiehlt 810 GB Unternehmensdaten

6. Februar 2024, in Gründau/Hessen

DATENDIEBSTAHL

EINBRUCH

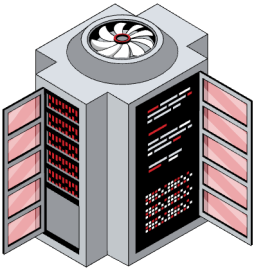
ERPRESSUNG

Was ist passiert?
Am 6. Februar 2024 wurde ein hessischer Anbieter von Sicherheitsschränken Opfer einer Ransomware-Attacke durch die Gruppe Black Basta. Die Angreifer behaupten, 810 GB an Daten erbeutet zu haben, einschließlich sensibler Buchhaltung-, Controlling- und Personalinformationen.

Was hätte man besser machen können?
Der Angriff hätte durch regelmäßige Backups, starke Zugangskontrollen, Endpunkt-Schutz und Verschlüsselung sensibler Daten besser abgewehrt werden können.

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://twitter.com/FalconFeedsio/status/1754837348678865267
https://ransomfeed.it/index.php?page=post_details&id_post=13120

RIEDEL

Ausfall durch Cyberangriff auf Wasserverband

9. Februar 2024, in Fritzlar/Hessen

AUSFALL

Was ist passiert?
Seit der Nacht zum 9. Februar 2024 waren die Systeme eines Wasserverbandes infolge eines unbekannten Cyberangriffs außer Betrieb. Externe Sicherheitsberater wurden umgehend hinzugezogen, um die Situation zu beurteilen und die notwendigen Maßnahmen zu ergreifen. Trotz des Vorfalls blieben die Verwaltungsabläufe, die Betriebstechnik und die Wasserversorgung selbst vollständig funktionsfähig und wurden nicht beeinträchtigt.

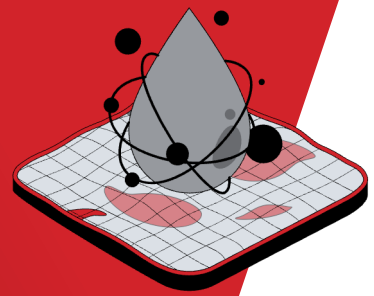
Was hätte man besser machen können?
Ein SOC hätte den Vorfall durch bessere Vorbereitung und Nachbereitung effektiver bewältigen können. Vorab hätte es durch ständige Überwachung und regelmäßige Sicherheitsanalysen frühzeitig Bedrohungen erkannt. Während des Vorfalls hätte ein SOC schnelle Maßnahmen zur Eindämmung des Angriffs und koordinierte Reaktionen ermöglicht. Nach dem Vorfall hätte es gründliche Untersuchungen zur Ursachenforschung und Verbesserung der Sicherheitsmaßnahmen durchgeführt sowie eine klare Kommunikation sichergestellt.

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.heise.de/news/Ransomware-Angriffe-auf-kritische-Infrastrukturen-und-Hoergeraetekette-Kind-9628904.html

RIEDEL

Grundstücksinformationen versehentlich online verfügbar

9. Februar 2024, in Konstanz/Baden-Württemberg

DATENPANNE

DATENLECK

Was ist passiert?
Bis Ende Januar 2024 waren Informationen zum Energienutzungsplan 2018 einer Stadt in Baden-Württemberg öffentlich einsehbar. Die Daten umfassten Adressen, Flurstücksnummern, Kundennummern der Stadtwerke sowie Angaben zu Gas- und Stromverbräuchen von 2014 bis 2017. Der betroffene Kartendienst wurde inzwischen offline genommen. Die betroffene Stadt sieht jedoch keine Gefahr für Identitätsdiebstahl.

Was hätte man besser machen können?
Der Vorfall hätte durch striktere Zugriffsrechte, Anonymisierung sensibler Daten und regelmäßige Sicherheitsüberprüfungen vermieden werden können. Zudem wäre eine sorgfältigere Prüfung vor der Veröffentlichung der Daten entscheidend gewesen.

Was lernen wir daraus:

Sensible Daten sollten jederzeit geschützt und verschlüsselt sein, um das Risiko von Missbrauch im Falle eines Sicherheitsvorfalls zu verringern. Sicherheitslücken können gravierende Folgen für die betroffenen Personen haben und auch erhebliche rechtliche und betriebliche Probleme für die Organisation verursachen, die die Daten unzureichend schützt. Ein durchgängiger Schutz ist daher unerlässlich, um potenzielle Schäden und rechtliche Konsequenzen zu vermeiden.

Anzunehmende Schadensfelder:

Quellen
https://www.tagesschau.de/inland/regional/badenwuerttemberg/swr-stadt-konstanz-raeumt-datenpanne-ein-100.html

RIEDEL

Hackergruppe stiehlt Daten von Internationalem Autohersteller

8. Februar 2024, in Offenbach am Main/Hessen

RANSOMWARE

DIEBSTAHL

Was ist passiert?
Anfang Januar 2024 wurde bekannt, dass ein Unternehmen Opfer eines Cyberangriffs wurde, nachdem zunächst nur von IT-Problemen die Rede war. Die Hackergruppe Black Basta behauptete, 3 Terabyte an Daten erbeutet zu haben. Während keine genauen Details veröffentlicht wurden, zeigen Bilddateien Informationen vom Autohersteller und betroffenen Abteilungen wie IT, Personal und Management. Das Unternehmen leitete Untersuchungen ein und informierte die Behörden.

Was hätte man besser machen können?
Im Vorfeld hätte das Unternehmen 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:

Black Basta ist eine Ransomware-Gruppe die das Ransomware-as-a-Service Modell (RaaS) betreibt. Die Gruppe trat erstmals Anfang 2022 in Erscheinung und etablierte sich schnell als einer der aktivsten Akteure in der RaaS-Szene. Bereits in den ersten Monaten ihrer Operationen verzeichnete sie 19 bekannte Opfer und insgesamt über 100 bestätigte Angriffe.

Anzunehmende Schadensfelder:

Quellen
https://www.golem.de/news/cyberangriff-hacker-haben-wohl-interne-daten-von-hyundai-erbeutet-2402-182034.html

RIEDEL

Ransomwaregruppe droht Textilunternehmen mit Datenveröffentlichung

7. Februar 2024, in Bodelshausen/Baden-Württemberg

DATENPANNE

DATENDIEBSTAHL

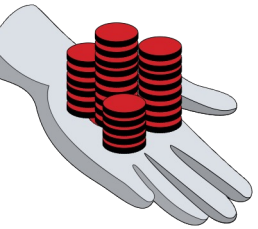
RANSOMWARE

Was ist passiert?
Am 7. Februar 2024 listete die Ransomwaregruppe 8Base ein Textilunternehmen im Darknet als Opfer auf. Die Cyberkriminellen behaupten, personenbezogene Daten, Rechnungen, Geheimhaltungsvereinbarungen und Zertifikate gestohlen zu haben. Sie drohen mit der Veröffentlichung dieser Informationen, falls ihre Forderungen nicht innerhalb einer Woche erfüllt werden.

Was hätte man besser machen können?
Um den Schaden zu minimieren, hätte das Textilunternehmen durch den Einsatz von Tools wie SIEM zur frühzeitigen Erkennung von Anomalien und EDR zur schnellen Reaktion auf Bedrohungen besser vorbereitet sein können. Zudem hätten regelmäßige Backups und deren sichere Speicherung dafür gesorgt, dass im Falle eines Angriffs eine zügige Wiederherstellung der Daten möglich wäre.

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.security-incidents.de/assets/img/incidents/5993-Karl_Rieker-8Base.png

RIEDEL

Hessische Gemeinde kämpft mit gestörter Kommunikation und Systemproblemen

7. Februar 2024, in Petersberg/Hessen

AUSFALL

Was ist passiert?
Am 7. Februar 2024 wurde eine hessische Gemeinde von einem Cyberangriff getroffen, der die EDV-Anlage lahmlegte. Die Telefon- und E-Mail-Kommunikation mit dem Rathaus war bis zum 15. Februar gestört. Der Rathausbetrieb war eine Zeit lang eingeschränkt, insbesondere bei der Abbuchung von Steuern und Kita-Beiträgen. IT-Experten verhinderten größeren Schaden und eine umfassende Untersuchung des Vorfalls wurde eingeleitet.

Was hätte man besser machen können?
Um den Cyberangriff auf die hessische Gemeinde besser abzuwehren, hätten präventive Maßnahmen wie regelmäßige Sicherheitsupdates und der Einsatz von Firewall- und Intrusion-Detection-Systemen helfen können. Eine gezielte Schulung der Mitarbeiter zur Erkennung von Phishing-Angriffen sowie ein umfassender Notfallplan, der eine schnelle Wiederherstellung der Systeme ermöglicht, wären ebenfalls wichtig gewesen. Zudem hätte eine regelmäßige Sicherung kritischer Daten den Betrieb schneller wiederherstellen können.

Was lernen wir daraus:

Cyberkriminelle nutzen zunehmend gefälschte Software-Updates, um Malware unbemerkt in Systeme einzuschleusen. Diese Angriffe präsentieren sich oft als legitime Aktualisierungen und täuschen die Benutzer, wodurch sie unwissentlich schadhafte Software installieren. Dies kann zu ernsthaften Sicherheitsproblemen führen, einschließlich Datenverlust und Systemkompromittierung. Daher sind regelmäßige und verifizierte Updates von entscheidender Bedeutung. Benutzer sollten sicherstellen, dass Updates nur aus vertrauenswürdigen Quellen stammen und die Integrität der Software stets überprüft wird, um ihre Systeme effektiv zu schützen.

Anzunehmende Schadensfelder:

Quellen
https://petersberg.de/index_main.php?modules=news&callmode=1&unid=1225&ispar=1&websiteid=petersberg&PHPSESSID=51f354cf9547930c7b6dea05d229c2a5

RIEDEL

Ransomware-Angriff auf Hörgerät-Hersteller

6. Februar 2024, in Hannover/Niedersachsen

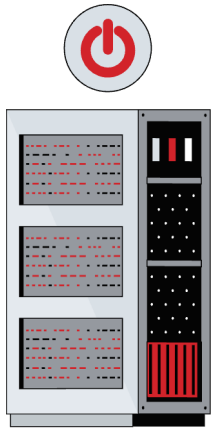
AUSFALL

EINBRUCH

RANSOMWARE

Was ist passiert?
Anfang Februar 2024 wurde ein Unternehmen aus der Hörgerätebranche von einem Cyberangriff getroffen. Die Attacke führte zu massiven IT-Störungen, wodurch Telefonanlagen und E-Mail-Kommunikation ausfielen. Rund 600 Filialen mussten auf manuelle Prozesse umstellen, da zentrale IT-Dienste nicht mehr verfügbar waren. Experten arbeiteten mehrere Tage daran, die Systeme wiederherzustellen. Es wurde kein Datendiebstahl bestätigt, doch der Vorfall legte große Teile des Geschäftsbetriebs lahm.

Was hätte man besser machen können?
Das Unternehmen hätte den Schaden durch den Cyberangriff verringern können, indem es regelmäßige Sicherheitsüberprüfungen und Backups durchgeführt, Mitarbeiter besser geschult und einen Notfallplan für Cybervorfälle vorbereitet 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.



Anzunehmende Schadensfelder:

Quellen
https://www.golem.de/news/keine-neuen-hoergeraete-kind-gruppe-kann-nach-cyberangriff-filialen-nicht-beliefern-2402-182251.html

Was lernen wir daraus:

Es verdeutlicht die Relevanz einer Notfallplanung mit alternativen Prozessen: Der Ausfall von IT-Diensten zeigt die Notwendigkeit robuster Notfallpläne. Unternehmen sollten für den Fall von Systemausfällen oder Cyberangriffen alternative manuelle Prozesse und Kommunikationswege etablieren, um den Geschäftsbetrieb aufrechterhalten zu können.

Die Stärkung der IT-Sicherheit und eine kontinuierliche Überwachung sollte nicht ausbleiben: Der Angriff verdeutlicht die Dringlichkeit, in präventive Sicherheitsmaßnahmen und kontinuierliche Überwachung zu investieren. Selbst wenn kein Datendiebstahl erfolgt, können erhebliche Störungen und Ausfallzeiten eintreten, die zu Betriebsunterbrechungen und finanziellen Einbußen führen.

RIEDEL

Daten von 56.000 Privatpersonen und 960 Unternehmen monatelang ungeschützt

5. Februar 2024, in Lörrach/Baden-Württemberg

SICHERHEITSLÜCKE

DATENLECK

Was ist passiert?
Monatelang waren bis Januar 2024 Daten von etwa 56.000 Privatpersonen und 960 Unternehmen im Landkreis Lörrach ungeschützt online einsehbar. Die Informationen betrafen über 200.000 Flurstücke sowie persönliche Daten wie Namen und Geburtsdaten. Ein zusätzlicher Datensatz enthielt E-Mail-Adressen und Adressen überfluteter Häuser. Der Fehler, der durch unzureichenden Passwortschutz entstand, wurde am 5. Januar 2024 behoben. Das Landratsamt warnt vor möglichem Missbrauch der Daten.

Was hätte man besser machen können?
Um den Vorfall zu vermeiden, hätten stärkere Sicherheitsmaßnahmen wie Zwei-Faktor-Authentifizierung und strenge Passwortanforderungen implementiert werden müssen. Regelmäßige Audits und Sicherheitsüberprüfungen hätten Schwachstellen frühzeitig erkannt. 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:

Ein Sicherheitsvorfall bezeichnet ein Ereignis, bei dem die Informationssicherheit eines Systems gefährdet wird. Solche Vorfälle können die Vertraulichkeit, Verfügbarkeit oder Integrität von Daten, IT-Anwendungen, Systemen oder Diensten beeinträchtigen und erhebliche Schäden für Einzelpersonen, Unternehmen oder Organisationen verursachen. Oft bleiben Angreifer längere Zeit unentdeckt in den infiltrierten Systemen, bevor sie aktiv werden. Im Durchschnitt vergehen etwa 20 Tage zwischen dem Eindringen und der Entdeckung eines Angriffs, was die Notwendigkeit effektiver Überwachungsmaßnahmen unterstreicht.

Anzunehmende Schadensfelder:

Quellen
https://www.loerrach-landkreis.de/aktuell?view=publish&item=article&id=6710

RIEDEL

Cyberangriff auf Krankenhausnetzwerk: Patientendaten betroffen

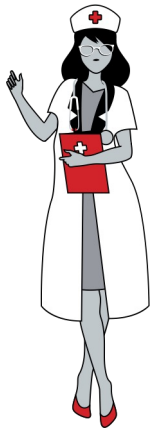
3. Februar 2024, in Soest/Nordrhein-Westfalen

RANSOMWARE

AUSFALL

Was ist passiert?
Anfang Februar 2024 wurde die IT-Infrastruktur eines Hospitals und der angeschlossenen Einrichtungen von Hackern angegriffen. Die Systeme wurden verschlüsselt und Patientendaten sind betroffen. Notfallversorgungen bleiben möglich, aber neue Aufnahmen und Operationen sind gestoppt. Der Systemwiederaufbau ist noch nicht abgeschlossen und aufgrund der fehlenden Rechnungsstellung musste die Stadt Lippstadt eine Bürgschaft von fünf Millionen Euro gewähren.

Was hätte man besser machen können?
Um den Angriff auf das Hospital zu verhindern, wären regelmäßige, sichere Backups und eine robuste Datensicherungslösung erforderlich gewesen. Der Einsatz von EDR und XDR hätte die Erkennung und Abwehr von Bedrohungen verbessert. Zwei-Faktor-Authentifizierung und strenge Zugangskontrollen hätten unbefugten Zugriff erschwert. Zudem hätten regelmäßige Schulungen des Personals zur Sensibilisierung für Phishing und andere Sicherheitsrisiken einen wichtigen Beitrag zur Vorbeugung geleistet.



Was lernen wir daraus:

Sicherheitsvorfälle in Kliniken gefährden die Vertraulichkeit, Verfügbarkeit und Integrität von Patientendaten. Kompromittierte sensible Informationen, die für eine effektive medizinische Versorgung unerlässlich sind, stellen ein direktes Risiko für die betroffenen Patienten dar. Gleichzeitig haben solche Vorfälle weitreichende Konsequenzen für die Kliniken selbst. Neben rechtlichen und finanziellen Belastungen führt ein solcher Vorfall zu erheblichem Reputationsverlust und erschüttert das Vertrauen in die Einrichtung. Daher ist es essenziell, robuste Sicherheitsmaßnahmen und präventive Strategien zu implementieren, um solche Risiken zu minimieren und die Patientensicherheit zu gewährleisten.

Anzunehmende Schadensfelder:

Quellen
https://www.golem.de/news/kreis-soest-und-berlin-cyberangriffe-auf-mehrere-deutsche-kliniken-2402-181846.html

RIEDEL

Nutzerdaten von 18.000 Accounts zum Verkauf angeboten

3. Februar 2024, in Stuttgart/Baden-Württemberg

DATENDIEBSTAHL

MALWARE

Was ist passiert?

Nach einem Angriff auf einen Hersteller von Remote-Desktop-Software entdeckten Sicherheitsforscher am 3. Februar 2024 Einträge in Cyberkriminellen-Foren, in dem Nutzerdaten von 18.000 Accounts zum Verkauf angeboten wurden. Die durch Infostealer-Programme erbeuteten Daten umfassen Kontoinformationen von Privatpersonen und Firmen. Einige Screenshots sind vom selben Tag datiert, was darauf hinweist, dass manche Nutzer ihre Passwörter noch nicht geändert haben. Es wird vermutet, dass die Täter die Daten verkaufen wollen, bevor die Passwörter aktualisiert werden.

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 entscheidend gewesen. Zudem hätten EDR und XDR zur Überwachung und umfassenden Analyse von Endpunkten und Netzwerken beigetragen. Schnelle Passwortänderungen und die Implementierung von Multi-Faktor-Authentifizierung wären ebenfalls wichtige Maßnahmen gewesen.

Anzunehmende Schadensfelder:

Was lernen wir daraus:

Infostealer sind Malware-Programme, die speziell darauf ausgelegt sind, vertrauliche Informationen von einem Opfer zu sammeln. Sie infiltrieren Systeme oft durch Phishing-E-Mails oder unsichere Downloads und erfassen Daten wie Passwörter, Kreditkarteninformationen und persönliche Details. Diese Informationen werden dann an die Angreifer weitergeleitet. Infostealer können erhebliche Schäden verursachen, darunter finanzieller Verlust und Identitätsdiebstahl.

Quellen
https://thehackernews.com/2024/02/anydesk-hacked-popular-remote-desktop.html

RIEDEL

Netzwerkausfall bei Universitätsmedizin: Klinikbetrieb eingeschränkt

2. Februar 2024, in Mainz/Hessen

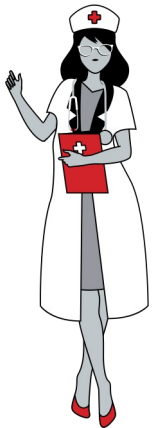
AUSFALL

Was ist passiert?
Am 2. Februar 2024 fiel das Netzwerk der Universitätsmedizin gegen 5:00 Uhr aus und beeinträchtigte mehrere Stunden lang den Klinikbetrieb. Alle internen Systeme, einschließlich Patientendokumentation und Labor, waren betroffen. Der Ausfall wurde durch eine interne Fehlsteuerung in einer zentralen Netzwerkkomponente verursacht und von einem IT-Krisenstab schnell behoben. Die Patientenversorgung blieb durchgängig gewährleistet. Das Netzwerk war ab 11:00 Uhr wieder in Betrieb, und um 13:00 Uhr liefen alle Abläufe normal.

Was hätte man besser machen können?
Um den Vorfall besser zu vermeiden, hätten redundante Netzwerkknoten und Systeme implementiert werden können, um die Auswirkungen eines Ausfalls zu minimieren. Regelmäßige Systemüberprüfungen und eine detaillierte Notfallstrategie hätten zudem eine schnellere Wiederherstellung ermöglicht.

Was lernen wir daraus:

Mit der fortschreitenden Digitalisierung in Kliniken treten neue Sicherheitsherausforderungen auf. Eine zügige Reaktion und gut organisierte Krisenbewältigung sind entscheidend, um die Auswirkungen von IT-Ausfällen zu minimieren. Daher sind regelmäßige Überprüfungen und Tests der IT-Systeme sowie präventive Maßnahmen zur Vermeidung interner Fehler unerlässlich, um solche Störungen zu verhindern und die Kontinuität der Patientenversorgung sicherzustellen.



Anzunehmende Schadensfelder:

Quellen
https://www.swr.de/swraktuell/rheinland-pfalz/mainz/netzwerkausfall-an-der-unimedizin-in-mainz-100.html
https://www.aerztezeitung.de/Wirtschaft/Netzwerkausfall-legt-Mainzer-Uniklinik-ueber-Stunden-lahm-446828.html

RIEDEL

JANUAR 2024

SECURITY INCIDENTS GERMANY

RIEDEL

Cyberangriff auf Volkshochschule: IT-Ausfall und Datenleck bestätigt

31. Januar 2024, in Vaterstetten/Bayern

AUSFALL

Was ist passiert?
Am 28. Januar 2024 wurde eine bayrische Volkshochschule Ziel eines Cyberangriffs. Bis zum 31. Januar 2024 konnten E-Mails nicht abgerufen werden und mehrere Kurse fielen aus. Am 21. März 2024 listete die Cloak-Gruppe die Einrichtung als Opfer und veröffentlichte 150 GB personenbezogene Daten. Der Zeitpunkt der vollständigen Wiederherstellung der Systeme ist noch unklar.

Was hätte man besser machen können?
Der Einsatz zusätzlicher SOC-Tools hätte den Angriff besser eindämmen können. Mit Threat Intelligence-Plattformen hätten aktuelle Bedrohungen frühzeitig erkannt und präventive Maßnahmen getroffen werden können. Network Traffic Analysis hätte dabei geholfen, anomale Netzwerkaktivitäten zu identifizieren und den Datenfluss zu überwachen. Zudem hätte SOAR automatisierte Reaktionen und ein Vorfallsmanagement ermöglicht, um den Angriff schneller zu beheben und den Betrieb zügiger wiederherzustellen.

Was lernen wir daraus:

Nachdem Angreifer unbemerkt in ein Netzwerk eingedrungen sind, suchen sie Persistenz, indem sie einen Command-and-Control-Server nutzten und Malware installieren.

Ziel ist der Zugang zu einem leistungsstarken Benutzerkonto, üblicherweise einem Administrator-Account, um weitreichende Rechte zu erlangen und im Netzwerk unentdeckt zu agieren (Lateral Movement).

Anzunehmende Schadensfelder:

Quellen
https://www.grasbrunn-aktuell.de/hackerangriff-auf-die-vhs-vaterstetten/2024-01-30
https://www.merkur.de/lokales/ebersberg/vaterstetten-ort29638/cyberangriff-auf-die-vhs-vaterstetten-helmut-ertel-polizei-sicherungsmassnahmen-92804982.html

RIEDEL

Cyberangriff auf Reifenhändler: Server von Handelsplattformen betroffen

31. Januar 2024, in Kaiserslautern/Rheinland-Pfalz

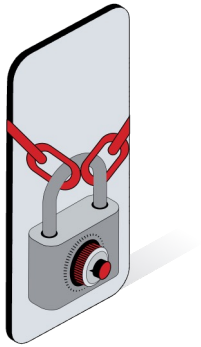
EINBRUCH

Was ist passiert?
Am 31. Januar 2024 wurden die Server eines Reifenhändlers angegriffen, einschließlich der Systeme von Handelsplattformen. Das Unternehmen berichtete, dass keine sensiblen Daten kompromittiert wurden und es keine Serverausfälle gab. Die zuständigen Behörden wurden informiert.

Was hätte man besser machen können?
Das Unternehmen hätte seine Cybersicherheitsstrategie durch proaktive Maßnahmen wie fortschrittliche Überwachung und regelmäßige Penetrationstests verbessern können. Regelmäßige Schulungen der Mitarbeiter könnten ebenfalls die Abwehr gegen zukünftige Angriffe stärken.

Was lernen wir daraus:

Die Sicherung der IT-Infrastruktur erfordert eine enge Zusammenarbeit zwischen IT-Teams und Führungskräften. Durch regelmäßige Kommunikation und die Implementierung einer umfassenden Sicherheitsstrategie, die alle Abteilungen einbezieht, kann das Unternehmen eine starke Verteidigung aufbauen und sich effektiv gegen Cyberbedrohungen wappnen.



Anzunehmende Schadensfelder:

Quellen
https://tyre24.alzura.com/de/de/press/download/dl/NTE2Mi5wZGY./name/QW5ncmlmZl9hdWZfZGllX0lUX0luZnlhc3RydWt0dXlfZGVyX0FMWlVSOV9BRy5wZGY
,

RIEDEL

AUSFALL

Landratsamt stellt IT-Systeme offline

30. Januar 2024, in Kelheim/Bayern

Was ist passiert?
Am 31. Januar 2024 nahm ein Bayrisches Landratsamt aufgrund eines vermuteten Cyberangriffs seine IT-Systeme offline. Dies führte dazu, dass keine Kfz-Zulassungen bearbeitet werden konnten und das Amt weder telefonisch noch per E-Mail erreichbar war. Auch die Städte und Gemeinden des Landkreises waren bis zum Nachmittag des 1. Februar betroffen. Das Landratsamt erwartete nach fünf Tagen wieder telefonisch erreichbar zu sein.

Was hätte man besser machen können?
Das Landratsamt hätte durch bessere Notfallpläne, schnellere Wiederherstellung der IT-Systeme und alternative Kommunikationswege den Betrieb zügiger aufrechterhalten können. Auch die Einrichtung von Backup-Systemen und -Kanälen hätte den Ausfall möglicherweise minimiert.

Was lernen wir daraus:

Cyberangriffe auf Landratsämter können u. a. zu Datenschutzverletzungen führen, was rechtliche und finanzielle Konsequenzen haben kann. Die Einhaltung der Datenschutzgrundverordnung (DSGVO) und die Implementierung robuster Datensicherheitsmaßnahmen sind unerlässlich, um die Vertraulichkeit, Integrität und Verfügbarkeit von Bürgerdaten zu gewährleisten.

Neben der DSGVO bestehen weitere regulatorische Anforderungen und Compliance-Vorgaben wie die NIS2-Richtlinie und die ISO/IEC 27001, die Unternehmen und öffentliche Einrichtungen dazu verpflichten, ihre IT-Sicherheitsmaßnahmen zu verstärken.

Anzunehmende Schadensfelder:

Quellen
https://www.donaukurier.de/lokales/landkreis-kelheim/it-probleme-im-landkreis-kehlheim-rathaeuser-und-landratsamt-teilweise-offline-15342089
https://www.landkreis-kelheim.de/index0102.html

RIEDEL

Cyberangriff führt zu Ausfall von Kommunikationssystemen in Klinik

29. Januar 2024, in Berlin/Berlin

AUSFALL

EINBRUCH

Was ist passiert?
Ende Januar 2024 wurde eine Klinik Opfer eines Cyberangriffs, der am 29. Januar entdeckt wurde. Der Vorfall sorgte für den Ausfall zahlreicher Kommunikationssysteme, sodass die Klinik nur über provisorische Telefonnummern erreichbar war. Die Patientensicherheit war nicht gefährdet, aber die Notfallversorgung wurde vorübergehend eingestellt, und Notfallpatienten wurden in andere Kliniken verlegt. Es ist noch unklar, welche Bereiche betroffen sind und ob Daten kompromittiert wurden.

Was hätte man besser machen können?
Um den Cyberangriff besser zu bewältigen, hätten regelmäßige Sicherheitsüberprüfungen und der Einsatz von SIEM- und EDR-Systemen zur frühzeitigen Erkennung und Reaktion auf Bedrohungen helfen können. Robuste Backup-Systeme und ein klarer Notfallplan für Kommunikationssysteme wären auch entscheidend gewesen, um die Erreichbarkeit und Patientensicherheit zu gewährleisten.

Was lernen wir daraus:

Cyberangriffe auf Kliniken können kritische Gesundheitsdaten gefährden und den Betrieb erheblich stören. Die Sicherstellung einer robusten IT-Sicherheit durch Firewalls, Intrusion Detection Systeme und regelmäßige Sicherheitsüberprüfungen ist daher unerlässlich, um Patientendaten zu schützen und den reibungslosen Betrieb der medizinischen Dienste zu gewährleisten.

Anzunehmende Schadensfelder:

Quellen
https://www.heise.de/news/Naechster-Cyberangriff-auf-Krankenhaus-Caritas-Klinik-Dominikus-betroffen-9616113.html?wt_mc=rss.red.security.security.atom.beitrag.beitrag

RIEDEL

Ransomwaregruppe veröffentlicht 121 GB Daten

28. Januar 2024, in Glauchau/Sachsen

DATENDIEBSTAHL

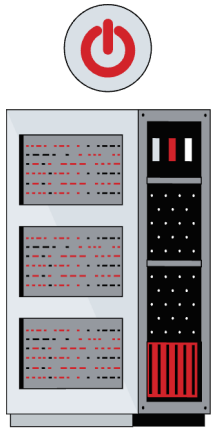
DATENPANNE

RANSOMWARE

DATENLECK

Was ist passiert?
Zwischen dem 28. und 29. Januar 2024 wurde ein Unternehmen für Batterien und Energiespeicher von Cyberkriminellen angegriffen. Der Vorfall beeinträchtigte die Geschäftstätigkeit in Deutschland, den USA und Australien. Um Produktionsstörungen zu minimieren, wurden vorübergehende Systeme eingerichtet. Am 1. Mai 2024 bekannte sich eine Ransomwaregruppe im Darknet zu dem Angriff und behauptete, 121,1 GB an sensiblen Daten gestohlen zu haben. Diese Daten wurden am 22. Juli 2024 veröffentlicht, nachdem möglicherweise keine Forderungen erfüllt wurden.

Was hätte man besser machen können?
Das Unternehmen hätte durch den Einsatz von Threat Intelligence-Plattformen frühzeitig gewarnt werden können, um den Angriff rechtzeitig zu erkennen und zu verhindern. Mit Network Segmentation hätte die Ausbreitung des Angriffs auf verschiedene Länder eingedämmt werden können. Automatisierte Backup- und Wiederherstellungslösungen hätten zudem dafür gesorgt, dass Daten schneller und effizienter wiederhergestellt werden können.



Anzunehmende Schadensfelder:

Quellen
https://www.security-incidents.de/assets/img/incidents/6039-Triathlon_Group-Team_Underground.PNG

Was lernen wir daraus:

Das Risiko für ein global tätiges Unternehmen wird durch die enge Vernetzung seiner Standorte in verschiedenen Ländern erheblich verstärkt. Wenn ein Cyberangriff wie dieser erfolgreich ist, kann er nicht nur einen Standort, sondern die gesamte globale Infrastruktur des Unternehmens beeinträchtigen.

Da die Standorte in Deutschland, den USA und Australien vermutlich miteinander vernetzt und aufeinander angewiesen sind, kann ein solcher Angriff zu weitreichenden Produktionsstörungen und Lieferengpässen führen.

RIEDEL

Ransomware-Angriff auf Klinikverbund: Systeme verschlüsselt, Patientendaten betroffen

27. Januar 2024, in Mittelfranken/Bayern

DATENDIEBSTAHL

AUSFALL

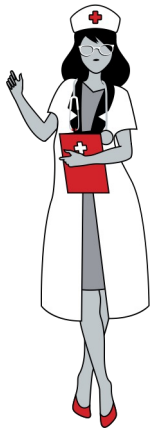
RANSOMWARE

Was ist passiert?
Am 27. Januar 2024 verschlüsselten Hacker die IT-Systeme eines Klinikverbunds und exfiltrierten vermutlich personenbezogene und interne Daten. Der Verbund nahm alle Systeme offline und meldete sich von der Notfallversorgung ab. Die Kliniken waren weiterhin telefonisch erreichbar, aber digitale Prozesse waren eingeschränkt. Am 6. Februar wurde bestätigt, dass auch Patientendiagnosen gestohlen wurden. Verhandlungen mit den Tätern werden ausgeschlossen.

Was hätte man besser machen können?
Der Klinikverbund hätte durch den Einsatz von SOC-Tools wie einem SIEM-System frühzeitig verdächtige Aktivitäten erkennen und schneller reagieren können. EDR hätte dabei geholfen, Angriffe auf Endgeräte zu isolieren und einzudämmen. Zudem hätten fortlaufende Bedrohungsanalysen und automatisierte Reaktionen die Exfiltration von Daten möglicherweise verhindern können.

Was lernen wir daraus:

Ein Ransomware-Angriff kann das Kundenvertrauen erheblich schädigen. Kunden erwarten, dass ihre Daten sicher sind und bei einem Sicherheitsvorfall kann es zu einem Vertrauensverlust kommen. Unternehmen müssen daher nicht nur ihre Sicherheitsmaßnahmen verstärken, sondern auch transparent über Vorfälle kommunizieren und gegebenenfalls Schadensersatz leisten.



Anzunehmende Schadensfelder:

Quellen
https://www.aerztezeitung.de/Wirtschaft/Hackerangriff-Kliniken-gehen-auf-Erpressungsversuch-nicht-ein-446816.html
https://www.br.de/nachrichten/bayern/hackerangriff-auf-bezirkskliniken-mittelfranken,U2jU9a2

RIEDEL

Bundestag Ziel eines großangelegten DDoS-Angriffs

27. Januar 2024, in Berlin/Berlin

DDoS

Was ist passiert?
Der Deutsche Bundestag wurde Opfer eines schweren Cyberangriffs. Ein großangelegter DDoS-Angriff sollte die Verfügbarkeit des Internetangebots beeinträchtigen, doch der IT-Abwehrschirm des Bundestages hielt stand, sodass das Angebot durchgehend erreichbar blieb. Eine Spur zu den Tätern gibt es nicht, jedoch wurde auf eine mögliche Beteiligung der pro-russischen Hackergruppe "Killnet" hingewiesen. Die Bundestags-Pressestelle gab keine Auskunft zur IT-Sicherheit.

Was hätte man besser machen können?
Der Bundestag hätte den Angriff durch den Einsatz zusätzlicher DDoS-Schutzdienste und einen umfassenderen Incident Response Plan besser bewältigen können. Zudem hätte Threat Intelligence zur proaktiven Überwachung potenzieller Bedrohungen und eine offenere Kommunikation über IT-Sicherheitsmaßnahmen geholfen.

Anzunehmende Schadensfelder:

Was lernen wir daraus:

Ein Angriff auf den Bundestag zeigt, warum die NIS2-Richtlinie so wichtig ist. Sie verlangt, dass u. a. öffentliche Einrichtungen strengere Sicherheitsvorkehrungen und Notfallpläne implementieren.

Mit strengen IT-Sicherheitsmaßnahmen erhöhen die Widerstandsfähigkeit gegen komplexe Cyberangriffe und trägt dazu bei, die nationale Sicherheit zu wahren.

Quellen
https://rp-online.de/politik/deutschland/cyberanfgriff-auf-internetangebot-des-bundestages-keine-spur-zu-taetern_aid-83804413

RIEDEL

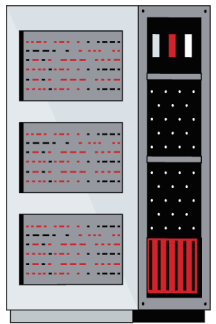
Github-Fehler: Sensible Daten von deutschen Autohersteller versehentlich preisgegeben

26. Januar 2024, in Stuttgart/Baden-Württemberg

DATENLECK

Was ist passiert?
Im September 2023 veröffentlichte ein Mitarbeiter von einem der größten Autobauer der Welt versehentlich ein Authentifizierungstoken in einem öffentlichen Github-Repository, das uneingeschränkten Zugriff auf den Github Enterprise Server ermöglichte. Dadurch waren private Quellcodes, Cloudzugangs- und API-Schlüssel, Passwörter sowie Designdokumente zugänglich. Sicherheitsforscher entdeckten die Panne und informierten das betroffene Unternehmen im Januar 2024, woraufhin das Token widerrufen wurde. Es ist unklar, ob Cyberkriminelle das Token entdeckt haben.

Was hätte man besser machen können?
In diesem Fall hätte das Unternehmen durch gezielte Maßnahmen präventiv handeln können. Die Einführung eines Secrets Management Systems hätte verhindert, dass sensible Daten versehentlich öffentlich gemacht werden. Automatisierte Scans auf öffentlich zugänglichen Code-Repositories könnten solche Pannen frühzeitig aufdecken. Zudem wäre Schulung und Sensibilisierung der Mitarbeiter für sichere Praktiken im Umgang mit Authentifizierungstoken und vertraulichen Informationen hilfreich gewesen.



Anzunehmende Schadensfelder:

Quellen
https://techcrunch.com/2024/01/26/mercedez-benz-token-exposed-source-code-github/
https://www.golem.de/news/token-leak-quellcode-von-mercedes-benz-lag-wohl-frei-zugaenglich-im-netz-2401-181606.html

Was lernen wir daraus:

Präventive Maßnahmen wie regelmäßige Sicherheitsüberprüfungen und Schwachstellenanalysen sind entscheidend, um potenzielle Datenlecks frühzeitig zu erkennen und zu verhindern. Durch eine kontinuierliche Überwachung und Aktualisierung der Sicherheitsinfrastruktur können Unternehmen ihre Abwehrkräfte stärken.

RIEDEL

Cyberangriff legt Volkshochschule lahm

AUSFALL

23. Januar 2024, in Bad Oeynhausen/Nordrhein-Westfalen

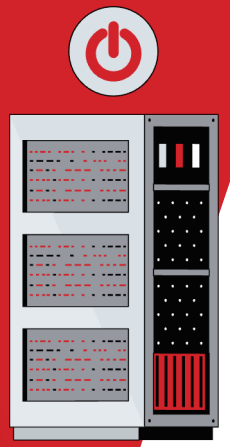
Was ist passiert?
Am 22. Januar 2024 wurde eine deutsche Volkshochschule von Cyberkriminellen angegriffen. Die betroffenen Server wurden sofort isoliert und eine Untersuchung eingeleitet. Aufgrund des Angriffs war die Volkshochschule nicht per E-Mail erreichbar und teilweise arbeitsunfähig. Auch die Festsetzung von Anmeldeterminen für die Bildungseinrichtung war eine Zeit lang nicht möglich.

Was hätte man besser machen können?
In diesem Fall hätte die Volkshochschule durch regelmäßige Sicherheitsüberprüfungen und Penetrationstests Schwachstellen frühzeitig identifizieren können. Ein einsatzbereites SOC-Team hätte eine koordinierte Reaktion auf den Angriff ermöglicht. Backup-Systeme hätten die Wiederherstellung wichtiger Daten und Funktionen beschleunigt. Zudem hätte eine bessere Schulung der Mitarbeiter zu Cybersicherheit menschliche Fehler minimieren können.

Was lernen wir daraus:

Viele Cyberangriffe beginnen mit menschlichem Versagen, wie dem Öffnen einer Phishing-E-Mail. Regelmäßige Schulungen der Mitarbeiter in Sicherheitsbewusstsein und Best Practices können das Risiko solcher Angriffe erheblich reduzieren. Informierte Mitarbeiter sind die erste Verteidigungslinie gegen Cyberbedrohungen.

Anzunehmende Schadensfelder:



Quellen
https://www.radiowestfalica.de/nachrichten/muehlenkreis/detailansicht/vhs-minden-bad-oeynhausen-wurde-gehackt.html

RIEDEL

LockBit-Ransomware attackiert Turnverein: Daten erbeutet

21. Januar 2024, in Rheine/Nordrhein-Westfalen

DATENDIEBSTAHL

EINBRUCH

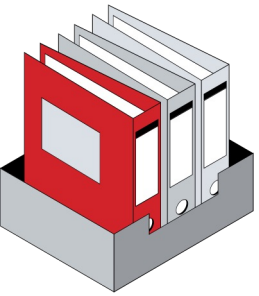
ERPRESSUNG

Was ist passiert?
Am 21. Januar 2024 wurde ein Turnverein von der Erpressergruppe LockBit als Opfer gelistet. Laut Angaben der Ransomwaregruppe wurden bei dem Angriff große Mengen an Daten, darunter Buchhaltungsdaten, E-Mail-Verläufe und Personalinformationen, exfiltriert. Der Verein erhielt eine Frist bis zum 25. Januar 2024, um den Forderungen der Angreifer nachzukommen.

Was hätte man besser machen können?
Der Turnverein hätte durch den Einsatz von SOC-Systemen den Angriff besser abwehren können. Ein SIEM hätte verdächtige Aktivitäten frühzeitig erkannt und eine schnelle Reaktion ermöglicht. EDR hätte dabei geholfen, die betroffenen Systeme schnell zu isolieren und den Schaden zu begrenzen. NTA hätte ungewöhnliche Datenbewegungen identifizieren können, bevor große Mengen exfiltriert wurden. Zudem hätte eine TI-Platform zur proaktiven Überwachung und Abwehr von Bedrohungen beigetragen.

Was lernen wir daraus:

Ransomware-Angriffe nehmen weltweit zu und betreffen auch Vereine. Angreifer verschlüsseln Daten und fordern Lösegeld für die Wiederherstellung. Ohne angemessene Sicherheitsvorkehrungen riskieren die Vereine erhebliche finanzielle Verluste. Eine proaktive Sicherheitsstrategie und regelmäßige Backups sind unerlässlich, um sich vor solchen Bedrohungen zu schützen.



Anzunehmende Schadensfelder:

Quellen
https://ransomfeed.it/index.php?page=post_details&id_post=12905
https://x.com/FalconFeedsio/status/1748986288261214550

RIEDEL

Ransomware-Angriff auf Unternehmen: 70 GB Daten gestohlen

11. Januar 2024, in Hannover/Hannover

EINBRUCH

DATENDIEBSTAHL

ERPRESSUNG

Was ist passiert?
Am 11. Januar 2024 fiel ein Unternehmen einer Ransomware-Attacke der Erpressergruppe Akira zum Opfer. Die Angreifer behaupten, 70 GB an Daten gestohlen zu haben, darunter Finanzdokumente und interne Unternehmensinformationen.

Was hätte man besser machen können?
Um einem Ransomware-Angriff besser vorzubeugen, hätte das Unternehmen Daten verschlüsseln, strikte Zugangskontrollen implementieren und regelmäßige Sicherheitsüberprüfungen durchführen sollen. Zudem wäre der Aufbau eines Incident-Response-Teams und die Schulung der Mitarbeiter hilfreich gewesen.

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://ransomfeed.it/index.php?page=post_details&id_post=12800

RIEDEL

Qilin-Ransomware fordert Lösegeld nach Datendiebstahl

10. Januar 2024, in Schwabach/Bayern

DATENDIEBSTAHL

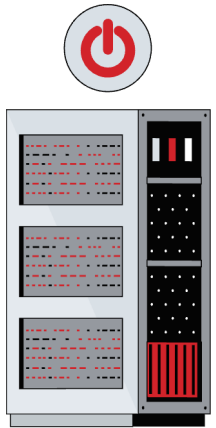
RANSOMWARE

Was ist passiert?
Am 10. Januar 2024 meldete die Ransomwaregruppe Qilin, dass sie ein deutsches Unternehmen angegriffen habe. Die Angreifer behaupten, verschiedene Dokumente und Dateien ausgelesen zu haben, darunter Finanzinformationen, Rechnungen und Kundendaten. Sie setzten eine Deadline vom 15. Januar 2024 und drohten an, ihre Beute an diesem Datum zu veröffentlichen, falls ihre Forderungen nicht erfüllt würden.

Was hätte man besser machen können?
Bei der Vorbereitung wären ein solider Incident-Response-Plan und Mitarbeiterschulungen entscheidend gewesen. Nach einem Angriff sind schnelle Wiederherstellung, gründliche Analyse des Vorfalls und Aktualisierung der Sicherheitsmaßnahmen wichtig. In der Kommunikation hätten zeitnahe Informationen der Betroffenen und die Zusammenarbeit mit den Behörden geholfen, Vertrauen zu bewahren und den Schaden zu begrenzen.

Was lernen wir daraus:

Selbst wenn ein Lösegeld gezahlt wird, gibt es keine Garantie, dass die Angreifer die Daten vollständig wiederherstellen. Nach einem Angriff müssen Unternehmen häufig beträchtliche Ressourcen in die Wiederherstellung und Verbesserung ihrer Sicherheitsvorkehrungen investieren. Durch präventive Investitionen in umfassende IT-Sicherheitslösungen können Unternehmen potenziellen Angriffen vorbeugen und sowohl finanzielle als auch operationale Schäden erheblich reduzieren.



Anzunehmende Schadensfelder:

Quellen
https://ransomfeed.it/index.php?page=post_details&id_post=12790
https://x.com/H4ckManac/status/1745091279631880549
https://x.com/TMRansomMonitor/status/1745167436578509220

RIEDEL

Radiosender nach Ransomware-Angriff im Notbetrieb

10. Januar 2024, in Ulm/Baden-Württemberg

RANSOMWARE

AUSFALL

Was ist passiert?
Am Nachmittag des 10. Januar 2024 wurde ein Radiosender Ziel eines Ransomware-Angriffs, was zu Ausfällen der IT-Systeme führte. Medienberichten vom 19. Januar zufolge waren die Computer bis dahin weiterhin nicht betriebsfähig und alle Dateien gesperrt. Der Sender nutzte zwei externe Laptops, Schallplatten, CDs und Live-Musik, um den Sendebetrieb aufrechtzuerhalten.

Was hätte man besser machen können?
Um einem Ransomware-Angriff vorzubeugen, hätte der Radiosender regelmäßige Backups und starke Sicherheitsprotokolle implementieren sollen. Auch Schulungen für Mitarbeiter und aktuelle Antivirus-Software wären wichtig gewesen.

Was lernen wir daraus:

Ransomware-Angreifer nutzen oft Schwachstellen in unzureichend gesicherten Systemen. Regelmäßige Sicherheitsüberprüfungen und Updates sind daher essenziell. Durch die Identifikation und Behebung von Schwachstellen können Unternehmen das Risiko eines Angriffs erheblich senken und ihre IT-Infrastruktur robuster gegen Bedrohungen machen.

Anzunehmende Schadensfelder:

Quellen
https://www.swp.de/lokales/ulm/cyberangriff-in-ulm-radio-wie-frueher-_-computer-bei-donau-3-fm-lahmgelegt-72809737.html
https://www.golem.de/news/radio-wie-frueher-deutscher-sender-greift-nach-cyberangriff-zu-platten-und-cds-2401-181351.html

RIEDEL

Fernzugriff auf Landtagssysteme wegen Sicherheitslücke abgeschaltet

9. Januar 2024, in Düsseldorf/Nordrhein-Westfalen

AUSFALL

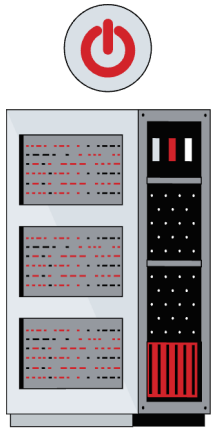
SICHERHEITSLÜCKE

Was ist passiert?
Am 9. Januar 2024 wurde der Fernzugriff auf das Netzwerk eines Landtags durch das Bundesamt für Sicherheit in der Informationstechnik abgeschaltet. Grund war eine Sicherheitslücke in einem nicht genannten Programm. Dadurch konnten Mitarbeiter nicht aus dem Home-Office arbeiten und der mobile E-Mail-Zugriff war beeinträchtigt. Nachdem die Sicherheitslücke geschlossen wurde, wurde der Fernzugriff am 16. Januar 2024 wiederhergestellt.

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. Klarere Kommunikation mit den Mitarbeitern über alternative Arbeitsmöglichkeiten hätte die Störungen im Home-Office verringert.

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.landtag.nrw.de/files/live/sites/landtag-r20/files/WWW/PB2/Pressemitteilungen/2024/01/2024-01-12%20PM%20Sicherheitsl%c3%bccke%20Fernzugriff.pdf

RIEDEL

IT-Dienstleister gehackt: Handwerkskammern von Serverausfällen betroffen

AUSFALL

9. Januar 2024, in Straubing/Bayern

Was ist passiert?
Seit der ersten Januarwoche 2024 kam es bei mehreren Handwerkskammern in Deutschland zu Serverausfällen, nachdem ein IT-Dienstleister einem Cyberangriff zum Opfer fiel. Betroffen sind Kammern in Aachen, Arnsberg, Bielefeld, Dortmund, Düsseldorf und Köln. Die meisten Kammern sind weiterhin telefonisch und per Mail erreichbar. Das Ausmaß des Angriffs und ob Daten abgeflossen sind, ist derzeit unbekannt

Was hätte man besser machen können?
Um den Serverausfällen der Handwerkskammern 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://www1.wdr.de/nachrichten/rheinland/ihk-website-rechenzentrum-sicherheitsvorfall-100.html
https://www.handwerksblatt.de/betriebsfuehrung/sicherheitsvorfall-bei-it-dienstleister-der-handwerkskammern

RIEDEL

DDoS-Massenangriff in Deutschland

Januar 2024, in Deutschland

AUSFALL

DDoS

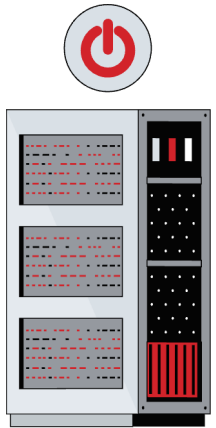
Was ist passiert?
Zwischen dem 8. und 16. Januar 2024 wurde eine Vielzahl an Unternehmen und Organisationen von der Hackergruppe NoName057(16) mit DDoS-Attacken angegriffen. Diese Angriffe betrafen zahlreiche Webseiten, wodurch deren Verfügbarkeit erheblich beeinträchtigt wurde.

Die Webseiten mehrerer Städte, Verkehrsgesellschaften, Logistikunternehmen und anderer Dienste waren betroffen. Alle Angriffe wurden von den Tätern auf ihrem Telegram-Kanal gemeldet

Was hätte man besser machen können?
Um sich besser gegen DDoS-Angriffe zu schützen, hätten die betroffenen Organisationen DDoS-Schutzdienste nutzen, ihre Netzwerk-Infrastruktur stärken und Notfallpläne erstellen sollen. Zudem wäre es hilfreich gewesen, den Verkehr zu überwachen und eng mit Internetdienstanbietern zusammenzuarbeiten.

Was lernen wir daraus:

Ein DDoS-Angriff (Distributed Denial of Service) legt eine Website lahm, indem er sie mit einer massiven Menge an Datenverkehr überflutet. Der Angreifer verwendet oft ein Netzwerk aus vielen kompromittierten Computern, um die Website mit so vielen Anfragen zu bombardieren, dass die Server überlastet werden und legitime Nutzer keinen Zugriff mehr erhalten.



Anzunehmende Schadensfelder:

Quellen
https://check-host.net/check-report/14a91af0k1d2
https://check-host.net/check-report/14995f94k73d

RIEDEL

Erkenntnisse

OOPS Report H1-2024

RIEDEL

Summary

Welche Erkenntnisse stechen besonders hervor?

Branchen

Im OOPS-Report H1-2024 werden mehrere Branchen genannt, die von Sicherheitsvorfällen betroffen waren, sowie deren prozentuale Verteilung. Die betroffenen Branchen sind:

1.Finanzsektor** - 28%**
2.Gesundheitswesen** - 22%**
3.Industrie** - 18%**
4.Öffentlicher Sektor** - 15%**
5.IT-Dienstleister** - 10%**
6. **Bildungswesen - 7%**

Diese Verteilung zeigt, dass der Finanzsektor und das Gesundheitswesen am stärksten betroffen waren, während das Bildungswesen am wenigsten betroffen war.

Angreifertypen

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

1. **Erpresser: 40%**
2. **Staatliche Spionage: 25%**
3. **Bösartige Hacker: 20%**
4. **Whitehacker: 15%**

Diese Verteilung zeigt, dass Erpresser den größten Anteil ausmachen, gefolgt von staatlicher Spionage und allgemeinen kriminellen Angreifern. Whitehacker machen den kleinsten Anteil aus.

Angriffstypen

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

1. **Ransomware: 55%**
2. **Datendiebstahl: 30%**
3. **Einbruch: 15%**

RIEDEL

Ein auffälliges Merkmal des OOPS-Report H1-2024 ist die Dominanz bestimmter Angriffs- und Angreifertypen. Ransomware, beispielsweise, macht 45% aller Sicherheitsvorfälle aus, was darauf hindeutet, dass diese Angriffsmethode besonders effektiv und weit verbreitet ist. Ebenso stellen Erpresser die größte Gruppe unter den Angreifern dar (40%), was die finanzielle Motivation hinter vielen Cyberangriffen unterstreicht.

Ein weiteres bemerkenswertes Detail ist die vergleichsweise geringe Rolle von Whitehackern (15%). Dies könnte darauf hindeuten, dass entweder weniger ethische Hacker auf Sicherheitslücken hinweisen oder dass ihre Aktivitäten weniger öffentlich gemacht werden.

Zusätzlich fällt auf, dass staatliche Spionage mit 25% einen signifikanten Anteil an den Vorfällen hat, was die zunehmende Rolle von staatlich geförderten Cyberoperationen in der heutigen globalen Landschaft widerspiegelt.

RIEDEL

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