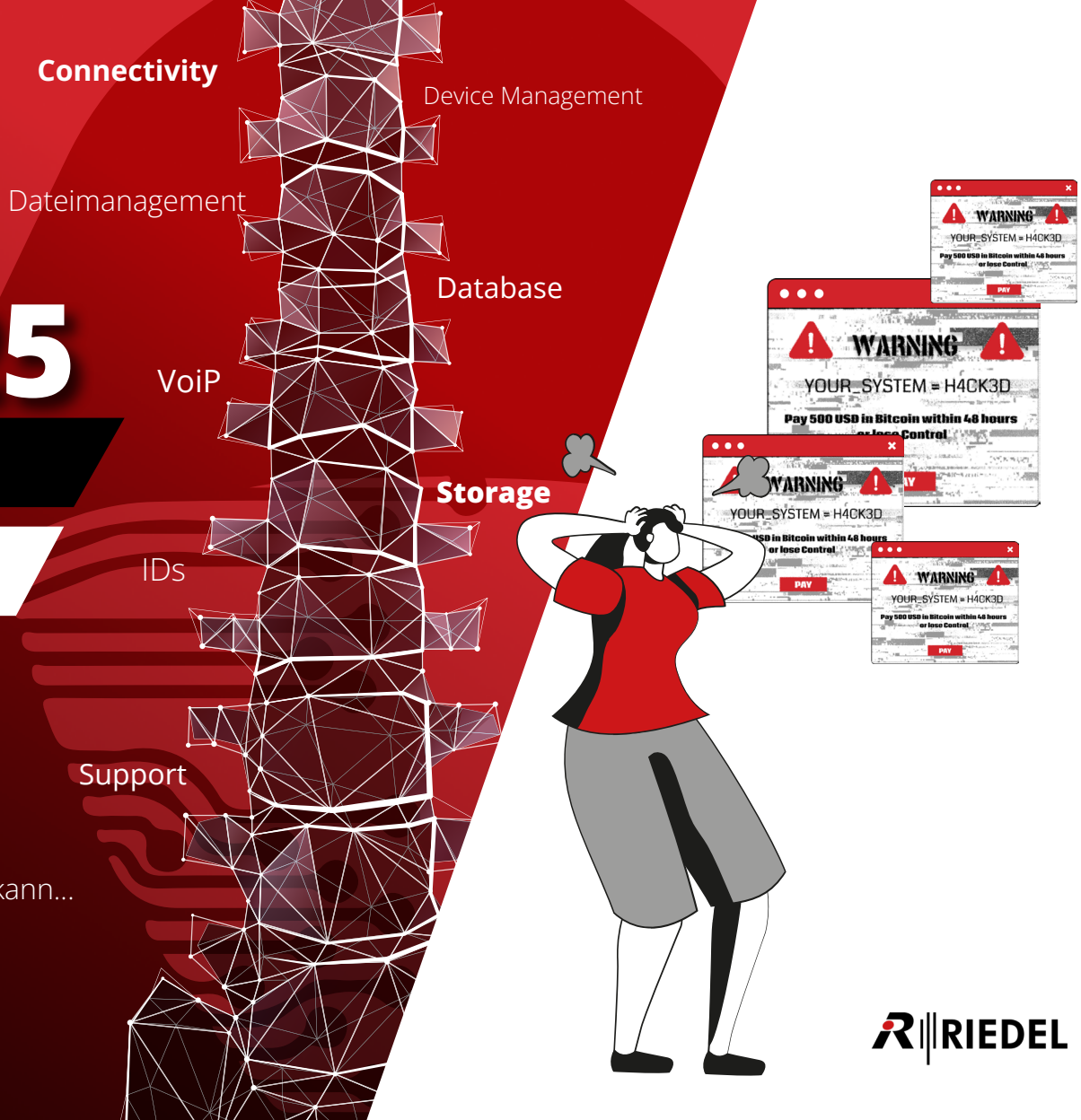
# OOPS H2-2025

## Der „hätte ich das mal früher gewusst“ Report

## SECURITY INCIDENTS GERMANY




### Die IT ist das Rückgrat jedes Unternehmens

...also sei dir bewusst, dass IT-Sicherheit über
die Handlungsfähigkeit eines Unternehmens entscheiden kann...

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

# Zwischen Fortschritt und Risiko

Cyber-Resilienz ist einer der größten Wettbewerbsvorteile der Neuzeit

## Einleitung

Cyber-Resilienz ist längst kein reines IT-Thema mehr – sie ist eine strategische Managementaufgabe. Im zweiten Halbjahr 2025 hat sich erneut gezeigt, wie verwundbar selbst etablierte Organisationen in zunehmend vernetzten, hybriden und cloudbasierten Infrastrukturen sind.

Parallel dazu verändert der rasante Einsatz von Künstlicher Intelligenz die Bedrohungslandschaft grundlegend. **KI** beschleunigt Geschäftsprozesse – aber auch Angriffe. Automatisierte Phishing-Kampagnen, präzisere Social-Engineering-Methoden und skalierbare Angriffswerkzeuge erhöhen Tempo und Qualität von Cybercrime deutlich. Unternehmen stehen damit einer neuen Dynamik gegenüber: Angriffe werden intelligenter, personalisierter und schwerer erkennbar. Die mediale Berichterstattung der vergangenen Monate verdeutlicht die Folgen: Betriebsunterbrechungen, Reputationsschäden, regulatorischer Druck, rechtliche Auseinandersetzungen und Vertrauensverlust bei Kunden und Investoren. Cybervorfälle sind keine isolierten IT-Probleme mehr, sondern entwickeln sich zu unternehmenskritischen Ereignissen mit unmittelbaren finanziellen und strategischen Auswirkungen.

Im vorliegenden **OOPS H2-2025 Report** haben wir eine Auswahl öffentlich bekannt gewordener Sicherheitsvorfälle analysiert und eingeordnet. Bewusst verzichten wir auf eine namentliche Nennung der betroffenen Organisationen. Ziel ist nicht die Bewertung einzelner Unternehmen, sondern die sachliche Einordnung von Mustern, Ursachen und Auswirkungen. Der Report soll Entscheidungsträgern helfen, aktuelle Entwicklungen zu verstehen, wiederkehrende Schwachstellen zu erkennen und die eigene Cyber-Resilienz gezielt weiterzuentwickeln – insbesondere vor dem Hintergrund einer sich durch KI rasant wandelnden Bedrohungslandschaft.

RIEDEL

# Schadensfelder durch Sicherheitsvorfälle

## Legende und Erklärung

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

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

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

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

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

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

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

Kosten für Wiederherstellung und Nachbesserung betroffener Systeme und Aufrüstung

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

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

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

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

Strategische Unternehmensrisiken wie die Beeinträchtigung von Unternehmensfusionen, Übernahmen oder Partnerschaften

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

RIEDEL

# DEZEMBER 2025

## SECURITY INCIDENTS GERMANY

RIEDEL

# Cyberangriff auf staatlichen Online-Shop: Kreditkartendaten abgegriffen

31. Dezember 2025, in Baden-Württemberg

SICHERHEITSLÜCKE

DATENDIEBSTAHL

EINBRUCH

BETRUG

**Was ist passiert?**
Ein Online-Shop einer staatlichen Einrichtung wurde Ziel eines Cyberangriffs. Unbekannte Täter nutzten eine bislang unbekannte Sicherheitslücke im Shopsystem, um eine gefälschte Zahlungsseite einzurichten. Dabei erlangten sie Zugriff auf Kreditkartendaten sowie auf Namen und E-Mail-Adressen zahlreicher Kunden. Mehrere Betroffene verloren dabei dreistellige Beträge.

**Was hätte man besser machen können?**
Durch eine ganzheitliche Sicherheitsstrategie mit kontinuierlicher Überwachung öffentlich erreichbarer Systeme durch ein **SOC** mit integriertem **SIEM**, strukturiertem Schwachstellenmanagement und abgesicherten Zahlungsprozessen hätte das Risiko des Angriffs deutlich reduziert werden können. Regelmäßige **Vulnerability Assessments** hätten Angriffspunkte frühzeitig erkennen können.

## Anzunehmende Schadensfelder:

Quellen:
https://www.swr.de/swraktuell/baden-wuerttemberg/cyber-attake-auf-the-laend-shop-100.html
https://www.staatsanzeiger.de/nachrichten/politik-und-verwaltung/einige-betrugsopfer-nach-cyberattacke-auf-the-laend-shop/

**Was lernen wir daraus:**
Eine frühzeitige Absicherung des Shopsystems, regelmäßige Sicherheitsprüfungen sowie eine strengere Kontrolle externer Zahlungsprozesse hätten dazu beitragen können, Manipulationen früher zu erkennen und deren Auswirkungen zu begrenzen.


RIEDEL

# Spacebears setzt Entsorgungsdienstleister unter Daten-Druck

30. Dezember 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

EINBRUCH

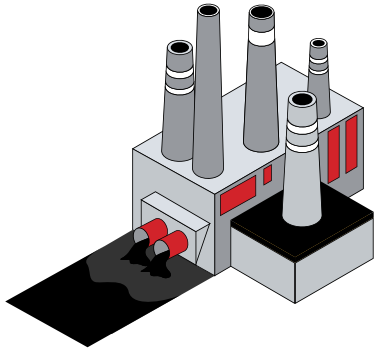
**Was ist passiert?**
Ein Bau- und Entsorgungsdienstleister wurde von der Ransomware-Gruppe **Spacebears** auf deren Leak-Seite aufgeführt. Die Angreifer behaupten, vertrauliche Unternehmensdaten abgegriffen zu haben, darunter Finanzunterlagen sowie Kunden- und Mitarbeiterinformationen. Dem Unternehmen wurde eine Frist bis zum 5. Januar 2026 gesetzt, nach deren Ablauf die Veröffentlichung der Daten angedroht wurde.

**Was hätte man besser machen können?**
Kontinuierliche Überwachung zentraler Systeme und bessere Zusammenführung sicherheitsrelevanter Ereignisse hätten Auffälligkeiten früher sichtbar gemacht. Klare Reaktionsprozesse und strukturierte Bewertung von Warnmeldungen hätten schnelleres Eingreifen ermöglicht. Ein professionelles **SOC mit SIEM** hätte den Schaden reduzieren können.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/11432-Spacebears.png

**Was lernen wir daraus:**
Durch eine ganzheitliche Sicherheitsstrategie mit kontinuierlichem Monitoring, klar definierten Incident-Response-Prozessen und der regelmäßigen Überprüfung sicherheitsrelevanter Systeme hätte das Risiko eines erfolgreichen Angriffs deutlich reduziert und der potenzielle Schaden begrenzt werden können.



RIEDEL

# Bildungseinrichtung unter Druck: LockBit 5.0 setzt Frist

29. Dezember 2025, in Berlin/Berlin

RANSOMWARE

DATENDIEBSTAHL

EINBRUCH

**Was ist passiert?**
Ein Bildungsunternehmen wurde Ende Dezember 2025 auf dem Opferportal der Ransomware-Gruppe **LockBit 5.0** aufgeführt. Die Täter setzten eine Frist bis zum 19. Januar 2026 und drohten im Anschluss mit der Veröffentlichung mutmaßlich kompromittierter Daten. Welche Informationen betroffen sind, war zu dem Zeitpunkt unklar.

**Was hätte man besser machen können?**
Der Vorfall zeigt, dass auch komplexe Bildungsorganisationen mit sensiblen Daten zunehmend Ziel professioneller Ransomware-Gruppen sind. Mehr Transparenz über sicherheitsrelevante Vorgänge und die frühzeitige Erkennung ungewöhnlicher Zugriffe hätten eine schnellere Lagebewertung ermöglicht. Eine zentrale Lösung wie **ZOLA** hätte die Überwachung vereinfacht und Risiken früher sichtbar gemacht.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/11433-Lockbit5.png

**Was lernen wir daraus:**
Bildungsträger verarbeiten Daten besonders schutzbedürftiger Personengruppen. Eine klare Trennung sensibler Datenbereiche, restriktive Zugriffsrechte und die gezielte Absicherung administrativer Systeme tragen dazu bei, Risiken zu reduzieren und potenzielle Folgen eines Ransomware-Angriffs besser kontrollierbar zu halten.

RIEDEL

# Jahreswechsel unter Druck: Safepay listet Textilhersteller

29. Dezember 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

EINBRUCH

**Was ist passiert?**

Kurz vor dem Jahreswechsel erschien ein deutscher Textilhersteller auf der Opferseite der Ransomware-Gruppe **Safepay**. Die Täter machten keine Angaben dazu, ob und welche Daten abgeflossen sind, setzten dem Unternehmen jedoch eine Frist bis zum 3. Januar 2026, um auf ihre Forderungen zu reagieren. Weitere Informationen zum Ablauf des Angriffs wurden nicht veröffentlicht.

**Was hätte man besser machen können?**

Eine bessere Sichtbarkeit sicherheitsrelevanter Vorgänge sowie die frühzeitige Erkennung ungewöhnlicher Systemaktivitäten hätten eine schnellere Einordnung ermöglicht. Der Einsatz einer integrierten Sicherheitslösung wie **RIEDEL Enterprise Defense [R.E.D.]** hätte Transparenz über mögliche Angriffspfade geschaffen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/11434-Safepay.png

**Was lernen wir daraus:**

Als aktive Ransomware-Gruppe steht Safepay für gezielte Angriffe auf Unternehmen verschiedener Branchen, häufig verbunden mit zeitlich gesetztem Erpressungsdruck. Umso wichtiger ist eine klar strukturierte IT-Landschaft mit restriktiven Zugriffsrechten und sauberer Rechtevergabe. Die gezielte Absicherung sensibler Systembereiche hilft, Risiken zu reduzieren und die Auswirkungen solcher Angriffe besser zu kontrollieren.

RIEDEL

# Massiver Datenabfluss: Ransomware-Gruppe fordert Verpackungshersteller heraus

28. Dezember 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

EINBRUCH

DATENLECK

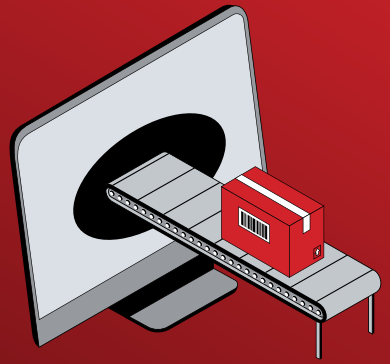
**Was ist passiert?**
Ende Dezember 2025 geriet ein deutscher Hersteller von Wellpappen- und Verpackungslösungen ins Visier der Ransomware-Gruppe **INC Ransom**. Die Täter veröffentlichten das Unternehmen auf ihrem Opferblog und geben an, rund **450 GB** interner Daten entwendet zu haben. Darunter sollen vertrauliche Geschäftsunterlagen, Kundeninformationen, Finanz- und Betriebsdaten sowie technologiebezogenes Know-how sein.

**Was hätte man besser machen können?**
Der Umfang der behaupteten Datenmenge deutet auf einen längeren, unbemerkten Zugriff hin. Eine stärkere Überwachung sensibler Dateizugriffe sowie eine frühzeitige Erkennung ungewöhnlicher Datenbewegungen hätten Risiken früher sichtbar gemacht. Der Einsatz eines **Security Information and Event Managements (SIEM)** in Kombination mit einer Data-Leak-Analyse hätte die Transparenz deutlich erhöht.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/11425-INCRansom.png

**Was lernen wir daraus:**
Gerade bei unternehmenskritischem Wissen ist eine klare Klassifizierung und Abschottung sensibler Daten entscheidend. Durch restriktive Zugriffsmodelle, segmentierte Speicherstrukturen und die gezielte Absicherung besonders schützenswerter Informationen lassen sich Umfang und Folgen eines möglichen Datenabflusses begrenzen.



RIEDEL

# Gemeinnützige Organisation betroffen: Ransomware-Angriff auf Stiftung

27. Dezember 2025, in Berlin/Berlin

RANSOMWARE

DATENDIEBSTAHL

EINBRUCH

**Was ist passiert?**

Eine Stiftung für Kinder- und Jugendhilfe wurde von der Ransomware-Gruppe **Safepay** auf deren Opferliste im Darknet aufgeführt. Die Täter setzten der gemeinnützigen Organisation eine Frist bis zum 1. Januar 2026, um auf ihre Forderungen zu reagieren. Angaben zu Art und Umfang möglicherweise kompromittierter Daten wurden nicht gemacht.

**Was hätte man besser machen können?**

Der Vorfall zeigt, dass auch gemeinnützige Organisationen zunehmend ins Visier von Ransomware-Gruppen geraten. Eine bessere Transparenz über sicherheitsrelevante Aktivitäten sowie die frühzeitige Erkennung unautorisierter Zugriffe hätten eine schnellere Lageeinschätzung ermöglicht. Der Einsatz einer zentralen Sicherheitslösung wie **ZOLA** hätte die Überwachung vereinfacht und die Reaktionsfähigkeit verbessert.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/11417-Safepay-VWadzeck.png

**Was lernen wir daraus:**

Organisationen mit sensiblen personenbezogenen Daten sollten besonderes Augenmerk auf klare Zugriffsregelungen und eine strukturierte Datenhaltung legen. Die gezielte Absicherung von Fachanwendungen sowie die regelmäßige Überprüfung von Benutzerkonten und Berechtigungen hilft, Risiken zu reduzieren und mögliche Schäden überschaubar zu halten.

RIEDEL

# Weihnachtliche Ransomware-Serie: LockBit 5.0 trifft mehrere Branchen

25. Dezember 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

EINBRUCH

**Was ist passiert?**

Die Ransomware-Gruppe **LockBit 5.0** listete mehrere deutsche Organisationen auf ihrem Opferblog. Betroffen waren eine private Bildungseinrichtung, eine Werbe- und Marketingagentur sowie ein -Dienstleister für die Automobilbranche. Die Täter setzten Fristen bis Anfang bzw. Mitte Januar 2026 und drohten nach Ablauf mit der Veröffentlichung mutmaßlich exfiltrierter Daten.

**Was hätte man besser machen können?**

Der gleichzeitige Angriff auf unterschiedliche Branchen zeigt den Bedarf an einem ganzheitlichen Sicherheitsansatz. Eine Lösung wie **RIEDEL Enterprise Defense [R.E.D.]**, die Prävention, Erkennung und Reaktion kombiniert, hätte für bessere Transparenz gesorgt und sicherheitsrelevante Auffälligkeiten früher sichtbar gemacht.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/11420-Lockbit5.png
https://www.security-incidents.de/assets/img/incidents/11419-Lockbit5.png
https://www.security-incidents.de/assets/img/incidents/11422-Lockbit5.png

**Was lernen wir daraus:**

Unternehmen mit sensiblen Kunden- und Projektdaten sollten besonderen Wert auf strukturierte Datenhaltung und restriktive Zugriffsmodelle legen. Die gezielte Absicherung zentraler Systeme sowie die regelmäßige Überprüfung von Benutzerrechten und Datenablagen tragen dazu bei, das Risiko umfangreicher Datenlecks und Folgeschäden zu reduzieren.


RIEDEL

# Sachverständigenbüro Ziel von Ransomware-Aktivitäten

24. Dezember 2025, in Deutschland

RANSOMWARE

EINBRUCH

**Was ist passiert?**

Ein Sachverständigen- und Gutachterbüro wurde von der Ransomware-Gruppe **Qilin** auf deren Opferblog gelistet. Details zu angeblich erbeuteten Daten nannten die Täter nicht. Das Unternehmen tauchte bereits im September 2025 auf der Leak-Site einer anderen Ransomware-Gruppe auf. Ob ein Zusammenhang zwischen den Vorfällen besteht, blieb unklar.

**Was hätte man besser machen können?**

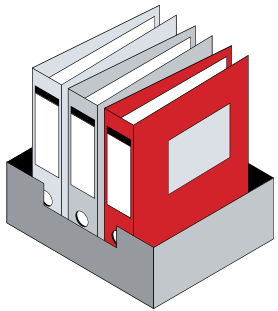
Eine systematische Überprüfung sicherheitsrelevanter Änderungen sowie eine kontinuierliche Überwachung verdächtiger Aktivitäten hätten Risiken früher sichtbar machen können. Der Einsatz eines **Vulnerability Assessments** in Kombination mit einer **Endpoint Detection and Response (EDR)-Lösung** hätte die Angriffserkennung und Absicherung verbessert.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/11426-Qilin.png

**Was lernen wir daraus:**

Gerade Gutachterbüros verarbeiten häufig vertrauliche Informationen. Eine klare Strukturierung sensibler Daten, restriktive Zugriffsmodelle und die regelmäßige Überprüfung von Benutzerrechten helfen, Risiken zu reduzieren. Zusätzlich trägt die gezielte Absicherung von Dokumentations- und Archivsystemen dazu bei, mögliche Schäden überschaubar zu halten.



RIEDEL

# Festtage mit Folgen: Ransomware-Angriff auf Autohaus

24. Dezember 2025, in Niedersachsen

RANSOMWARE

DATENDIEBSTAHL

EINBRUCH

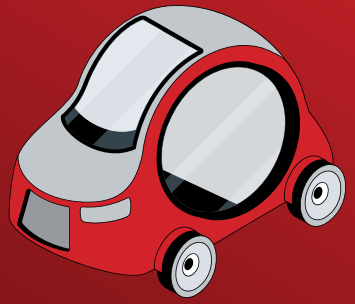
**Was ist passiert?**
Ein Autohaus mit Kfz-Servicebetrieb aus Niedersachsen wurde am 24. Dezember von der Ransomware-Gruppe **Spacebears** auf einer Leak-Site als angegriffen gelistet. Die Täter behaupten, vertrauliche Unternehmensdaten erbeutet zu haben, darunter Finanzunterlagen sowie Kunden- und Mitarbeiterdaten, und kündigten eine Veröffentlichung ab dem 30. Dezember an. Der tatsächliche Schaden blieb unklar.

**Was hätte man besser machen können?**
Der Angriff verdeutlicht das Risiko für Servicebetriebe mit sensiblen Daten. Eine frühzeitige Erkennung unautorisierter Zugriffe sowie bessere Transparenz über sicherheitsrelevante Ereignisse hätten eine schnellere Einordnung ermöglicht. Ein SIEM zur zentralen Analyse von Logdaten und gezielte **Datenschutz-Kontrollen** für Kunden- und Finanzinformationen hätten die Reaktionsfähigkeit erhöht.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/11427-Spacebears.png

**Was lernen wir daraus:**
Durch klar strukturierte Datenhaltung, restriktive Zugriffsrechte und die konsequente Absicherung von Kunden- und Finanzinformationen lassen sich Folgen eines Datenabflusses reduzieren. Regelmäßige Überprüfungen von Benutzerkonten, Datenablagen und Berechtigungen erschweren umfangreiche Leaks und helfen, Risiken schneller zu erkennen.



RIEDEL

# Eine (un)schöne Bescherung: Ransomware-Attacke gegen Bäckerei-Kette

24. Dezember 2025, in Bayern

RANSOMWARE

**Was ist passiert?**

Eine regionale Bäckerei-Kette aus Bayern wurde an Heiligabend auf dem Opferblog der Ransomware-Gruppe **Qilin** aufgeführt. Weitere Angaben zum Ablauf des mutmaßlichen Angriffs oder zu möglichen abgeflossenen Daten machten die Täter nicht. Auch seitens des betroffenen Unternehmens liegen keine öffentlichen Informationen vor.

**Was hätte man besser machen können?**

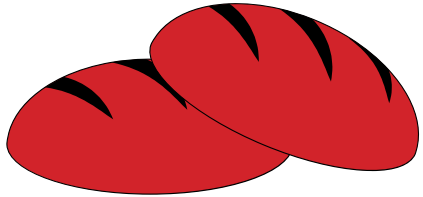
Der Vorfall zeigt, dass auch Unternehmen des täglichen Bedarfs ins Visier von Ransomware-Gruppen geraten. Eine verbesserte Transparenz über sicherheitsrelevante Ereignisse sowie die frühzeitige Erkennung auffälliger Aktivitäten hätten eine schnellere Einordnung ermöglicht. Der Einsatz einer **Endpoint Detection and Response (EDR)-Lösung** sowie einer zentralen Monitoring-Struktur hätte die Angriffserkennung gestärkt.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/11418-Qilin.png

**Was lernen wir daraus:**

Eine reduzierte Angriffsfläche durch klar geregelte Zugriffsrechte, regelmäßige Aktualisierung eingesetzter Systeme und die gezielte Absicherung von Kassensystemen und Verwaltungs-IT hätte dazu beigetragen, die Auswirkungen eines Ransomware-Vorfalls gering zu halten.



RIEDEL

# IT-Sicherheitsvorfall bei Elektronikunternehmen durch Ransomware-Gruppe

23. Dezember 2025, in Nordrhein-Westfalen

RANSOMWARE

DATENDIEBSTAHL

EINBRUCH

DATENLECK

**Was ist passiert?**
Die Ransomware-Gruppe **Lynx** hat einen Montage- und Innenausbau-Dienstleister aus Nordrhein-Westfalen auf ihrem Opferblog gelistet. Die Täter behaupten, Unternehmensinformationen verschlüsselt zu haben und veröffentlichten zugleich vertrauliche Daten als Beleg, darunter Finanzunterlagen, interne Berichte sowie Mitarbeiterdokumente. Angaben zum Gesamtschaden wurden nicht gemacht.

**Was hätte man besser machen können?**
Der Vorfall zeigt, dass Ransomware-Angriffe zunehmend mit gezielten Datenlecks kombiniert werden. Eine kontinuierliche Überwachung sicherheitsrelevanter Aktivitäten sowie die frühzeitige Erkennung unautorisierter Zugriffe hätten den Abfluss sensibler Informationen möglicherweise begrenzen können. Der Einsatz einer Data-Leak-Erkennung in Kombination mit einem **Security Operations Center (SOC)** hätte die Reaktionsfähigkeit deutlich erhöht.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/11403-Lynx_.png

**Was lernen wir daraus:**
Eine klare Trennung sensibler Datenbereiche, restriktive Zugriffsrechte und eine konsequente Absicherung interner Dokumentationssysteme hätten das Risiko eines erfolgreichen Datenabflusses verringert. Zusätzlich tragen regelmäßige Überprüfungen von Berechtigungen und Datenablagen dazu bei, Auswirkungen von Ransomware-Angriffen zu begrenzen.


RIEDEL

# Doppelschlag: Qilin zielt auf Industrie und Kommune

22. Dezember 2025, in Deutschland

RANSOMWARE

EINBRUCH

**Was ist passiert?**
Die Ransomware-Gruppe **Qilin** hat zwei deutsche Organisationen auf ihrem Opferblog gelistet. Betroffen waren ein Anbieter von Maschinen und Systemen für die industrielle Bearbeitung sowie eine bayerische Kommune. In beiden Fällen machten die Täter keine Angaben zu Art und Umfang kompromittierter Daten. Ob Zusammenhänge zu weiteren IT-Störungen im kommunalen Umfeld bestehen, blieb offen.

**Was hätte man besser machen können?**
Der Vorfall unterstreicht die Bedeutung kontinuierlicher Überwachung und schneller Reaktionsfähigkeit. Ein **Security Operations Center (SOC)** hätte verdächtige Aktivitäten frühzeitig erkennen können, während **Security Orchestration, Automation and Response (SOAR)** eine strukturierte und automatisierte Reaktion ermöglicht hätte, um Angriffe schneller einzudämmen und Folgeschäden zu reduzieren.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/11404-Qilin_.png
https://www.security-incidents.de/assets/img/incidents/11405-Qilin-Fuerth.jpg

**Was lernen wir daraus:**
Unabhängig vom Sektor ist eine reduzierte Angriffsfläche entscheidend. Dazu zählen gehärtete Systeme, eingeschränkte Zugriffsrechte und eine klare Trennung kritischer IT-Bereiche. Durch strukturierte Sicherheitsstandards und regelmäßige Überprüfung von Konfigurationen lassen sich potenzielle Einstiegspunkte für Ransomware-Angriffe deutlich verringern.

RIEDEL

# Ransomware-Welle: Safepay nimmt zahlreiche deutsche Unternehmen ins Visier

17. Dezember 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Mehrere deutsche Unternehmen aus verschiedenen Branchen wurden Ziel der Ransomware-Gruppe **Safepay**. Betroffen sind unter anderem ein Notariat, Dienstleister aus Medizintechnik, Software und Gesundheitswesen, ein Dentallabor, ein Münzhandels- und Auktionshaus sowie Betriebe aus Handwerk, Fahrzeughandel und Vermietung. Die Opfer wurden auf einem Darknet-Blog gelistet, Fristen gesetzt. Angaben zur Datenmenge fehlen.

**Was hätte man besser machen können?**
Die Vielzahl betroffener Branchen zeigt, dass Safepay gezielt nach allgemeinen Schwachstellen sucht. Eine regelmäßige Prüfung der IT-Sicherheitslage hätte Risiken früher sichtbar machen können. Insbesondere eine **IT-Musterung** zur Identifikation kritischer Schwachstellen sowie eine **Extended Detection and Response (XDR)-Lösung** zur Erkennung komplexer Angriffe hätten die Abwehrfähigkeit deutlich verbessert.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/11343-Safepay.png
https://www.security-incidents.de/assets/img/incidents/11342-Safepay.png
https://www.security-incidents.de/assets/img/incidents/11328-safepay.png
https://www.security-incidents.de/assets/img/incidents/11327-safepay.png
https://www.security-incidents.de/assets/img/incidents/11326-safepay.png
https://www.security-incidents.de/assets/img/incidents/11364-Safepay.png
https://www.security-incidents.de/assets/img/incidents/11363-Safepay.png
https://www.security-incidents.de/assets/img/incidents/11362-Safepay.png
https://www.security-incidents.de/assets/img/incidents/11365-Safepay.png

**Was lernen wir daraus:**
Unabhängig von Branche oder Unternehmensgröße ist eine ganzheitliche Sicherheitsstrategie entscheidend. Dazu zählen regelmäßige Sicherheitsüberprüfungen, aktuelle Backup-Konzepte, klar definierte Notfallprozesse und geschulte Mitarbeitende. So lassen sich Angriffsflächen reduzieren und die Auswirkungen möglicher Ransomware-Angriffe begrenzen.

RIEDEL

# Technische Störung legt zentrales Regierungsnetzwerk lahm

16. Dezember 2025, in Berlin/Berlin

AUSFALL

**Was ist passiert?**
Bei einer zentralen staatlichen Institution kam es zu einem teils flächendeckenden Ausfall der IT-Infrastruktur. Inter- und Intranet standen zeitweise nicht zur Verfügung, E-Mails und Dateien konnten nicht abgerufen werden. Laut offizieller Mitteilung handelte es sich nicht um einen Cyberangriff, sondern um ein technisches Problem im angeschlossenen Rechenzentrum.

**Was hätte man besser machen können?**
Der Vorfall verdeutlicht, dass technische Störungen auch potenzielle Sicherheitslücken begünstigen können. Fehlkonfigurationen oder eingeschränkte Schutzmechanismen während Ausfällen bieten Angreifern mögliche Ansatzpunkte. Eine regelmäßige **IT-Musterung** zur Identifikation kritischer Schwachstellen sowie ein **Security Operations Center (SOC)** zur kontinuierlichen Überwachung hätten die Resilienz erhöht und potenzielle Risiken frühzeitig sichtbar gemacht.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.heise.de//news/Internet-ausfall-im-Bundestag-kein-Cyberangriff-11115990.html

**Was lernen wir daraus:**
Auch wenn kein Angriff vorlag, unterstreicht der Vorfall die Bedeutung von Redundanzen, klaren Notfallplänen und regelmäßig getesteten Betriebsprozessen. Eine robuste Infrastruktur und transparente Kommunikationswege sind entscheidend, um Ausfälle schnell zu beherrschen.


RIEDEL

# Kundendaten kompromittiert: Online-Shop nach Cyberangriff betroffen

16. Dezember 2025, in Meerane/Sachsen

DATENDIEBSTAHL

EINBRUCH

**Was ist passiert?**
Mitte Dezember 2025 informierte ein Hersteller von Sonnenschutz- und Rollladensystemen tätiges Unternehmen seine Kunden über einen Cyberangriff auf interne Systeme. Dabei wurden Kundendaten kompromittiert, darunter Stammdaten sowie gehashte Passwörter für den firmeneigenen Online-Shop. Angaben zu Zeitpunkt oder Urhebern des Angriffs wurden nicht gemacht. Kunden wurden aufgefordert, ihre Zugangsdaten zu ändern.

**Was hätte man besser machen können?**
Eine frühzeitige Analyse sicherheitsrelevanter Ereignisse sowie ein kontinuierliches Monitoring hätten eine schnellere Reaktion ermöglicht und den Schaden begrenzen können. Der Einsatz eines **Security Information and Event Managements (SIEM)** sowie einer **Endpoint Detection and Response (EDR)-Lösung** hätte die Angriffserkennung und Systemabsicherung deutlich verbessert.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/11323-rolladen-group.png

**Was lernen wir daraus:**
Eine ganzheitliche Sicherheitsstrategie mit regelmäßigen Prüfungen von Systemen und Zugriffen, klaren Incident-Response-Prozessen sowie Sensibilisierung für IT-Sicherheit hätte das Risiko eines erfolgreichen Angriffs deutlich reduziert. Insbesondere der Schutz von Zugangsdaten und Webanwendungen sollte priorisiert werden.

RIEDEL

# Safepay droht Wasserstofftechnologie-Entwickler mit Datenveröffentlichung

15. Dezember 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

ERPRESSUNG

**Was ist passiert?**

Die Ransomware-Gruppe **Safepay** listete einen Wasserstofftechnologie-Entwickler aus dem Harz auf ihrer Darknet-Leaksite als Opfer auf. Die Täter machten keine Angaben zu Art oder Umfang der angeblich exfiltrierten Daten, drohten jedoch mit deren Veröffentlichung zum 17. Dezember 2025. Eine Bestätigung möglicher Datenabflüsse lag zunächst nicht vor.

**Was hätte man besser machen können?**

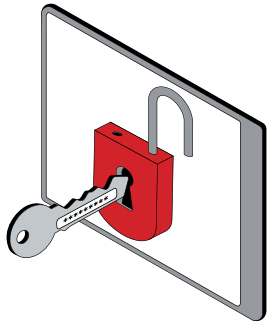
Eine frühere Identifikation möglicher Angriffsindikatoren hätte eine bessere Lageeinschätzung ermöglicht. Eine kontinuierliche Überwachung sicherheitsrelevanter Aktivitäten durch ein **Security Operations Center (SOC)** sowie eine erweiterte Bedrohungserkennung mittels **Extended Detection and Response (XDR)** hätten die Transparenz erhöht und die Reaktionsfähigkeit unterstützt.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/11316-safepay.png

**Was lernen wir daraus:**

Gerade technologiegetriebene Unternehmen mit sensiblen Entwicklungs- und Forschungsdaten stehen verstärkt im Fokus von Cyberkriminellen. Regelmäßige Sicherheitsüberprüfungen, klar geregelte Zugriffsrechte sowie definierte Abläufe zur Angriffserkennung und -reaktion können dazu beitragen, Risiken zu reduzieren und mögliche Auswirkungen eines Angriffs frühzeitig zu begrenzen.



RIEDEL

# Cyberangriff auf Streamingplattform führt zu Datenabfluss bei Nutzern

15. Dezember 2025, in Berlin/Berlin

DATENDIEBSTAHL

EINBRUCH

AUSFALL

**Was ist passiert?**
Am 11. Dezember 2025 kam es bei einer internationalen Audio-Streamingplattform zu Zugriffsproblemen für Nutzer mit VPN. Die Störungen dauerten bis zum 15. Dezember und wurden zunächst auf interne Konfigurationsänderungen zurückgeführt. Später bestätigte das Unternehmen einen Cyberangriff, bei dem E-Mail-Adressen und öffentlich sichtbare Profildaten von bis zu **20 %** der Nutzer entwendet wurden.

**Was hätte man besser machen können?**
Der Vorfall zeigt, dass sicherheitsrelevante Anomalien zunächst als technische Störung interpretiert wurden. Eine frühere Korrelation ungewöhnlicher Zugriffsmuster hätte Hinweise auf einen Angriff liefern können. **XDR-Lösungen** zur Analyse über Anwendungen, Server und Netzwerk hinweg sowie ein kontinuierliches **SOC** hätten die Bewertung beschleunigt und eine frühere Reaktion unterstützt – auch wenn sich Vorfälle nie vollständig ausschließen lassen.

## Anzunehmende Schadensfelder:

Quellen:
https://www.bleepingcomputer.com/news/security/soundcloud-confirms-breach-after-member-data-stolen-vpn-access-disrupted/

**Was lernen wir daraus:**
Bei datengetriebenen Plattformen mit Millionen Nutzern ist eine klare Trennung zwischen technischen Störungen und sicherheitsrelevanten Vorfällen entscheidend. Kontinuierliche Überwachung, klar definierte Eskalationspfade sowie regelmäßige Sicherheitsüberprüfungen können dazu beitragen, Angriffe früher zu erkennen und Auswirkungen auf Nutzer zu minimieren.

RIEDEL

# Akira-Angriff trifft Versicherungsgruppe und Tochtergesellschaft

12. Dezember 2025, in Berlin/Berlin

RANSOMWARE

AUSFALL

**Was ist passiert?**
Eine Unternehmensgruppe aus dem Versicherungs- und Vorsorgeumfeld wurde Ziel eines Ransomware-Angriffs der Gruppe **Akira**. Zur Schadensbegrenzung wurden zentrale IT-Systeme vorsorglich abgeschaltet. Aufgrund gemeinsamer IT-Strukturen war auch ein verbundener Dienstleister im Bestattungswesen betroffen und trennte seine Systeme. Hinweise auf Datenmissbrauch lagen nicht vor. Die Wiederherstellung erfolgte schrittweise.

**Was hätte man besser machen können?**
Der Vorfall verdeutlichte die Abhängigkeiten innerhalb verbundener IT-Strukturen unterschiedlicher Geschäftsbereiche. Eine stärkere Segmentierung zwischen Konzern- und Tochtergesellschaftssystemen hätte Auswirkungen möglicherweise begrenzen können. **Endpoint Detection and Response (EDR)** zur besseren Sichtbarkeit auf Endpunkten sowie klar definierte Notfall- und Abschaltprozesse hätten die Abgrenzung betroffener Bereiche unterstützt.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.asscompact.de/nachrichten/cyberangriff-auf-die-ideal-versicherung

**Was lernen wir daraus:**
Der Fall zeigte, dass Ransomware-Angriffe zunehmend ganze Unternehmensverbände betreffen, selbst wenn Branchen und Aufgabenbereiche unterschiedlich sind. Vorsorgliche Abschaltungen bleiben ein wirksames Mittel zur Schadensbegrenzung, erfordern jedoch abgestimmte Prozesse. Für Unternehmensgruppen ist es entscheidend, IT-Abhängigkeiten transparent zu machen und Konzern-Notfallpläne regelmäßig zu prüfen.

RIEDEL

# Datenleck durch Ransomware-Gruppe Brotherhood

10. Dezember 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Anfang Dezember 2025 listete die Ransomware-Gruppe **Brotherhood** eine süddeutsche Baumschule auf ihrer Darknet-Seite als Opfer. Die Täter behaupteten, insgesamt **36 GB** an Unternehmensdaten exfiltriert zu haben. Davon stellten sie nach eigenen Angaben **10 GB** frei zum Download bereit, während weitere **26 GB** zum Verkauf angeboten wurden. Angaben zum Inhalt der Daten lagen nicht vor.

**Was hätte man besser machen können?**
Eine frühere Erkennung ungewöhnlicher Datenzugriffe hätte Hinweise auf eine laufende Exfiltration liefern können. Mechanismen zur Überwachung von Datenbewegungen sowie eine erweiterte Bedrohungserkennung über Endpunkte hätten verdächtige Aktivitäten früher sichtbar gemacht. Extended Detection and Response (XDR) in Kombination mit klar definierten Reaktionsprozessen hätte die Analyse und Eindämmung unterstützen können

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/11279-brotherhood.png

**Was lernen wir daraus:**
Auch kleinere und saisonal geprägte Betriebe geraten zunehmend ins Visier von Ransomware-Gruppen. Regelmäßige Sicherheitsüberprüfungen, klar geregelte Zugriffsrechte sowie Verfahren zur Erkennung ungewöhnlicher Datenbewegungen können dazu beitragen, Risiken zu reduzieren und Auswirkungen eines Angriffs frühzeitig zu begrenzen.

RIEDEL

# Koordinierter Doppelschlag der Ransomware-Gruppe Akira

08. Dezember 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

EINBRUCH

**Was ist passiert?**

Am 8. Dezember 2025 führte **Akira** zwei deutsche Firmen auf ihrer Leaksite: einen Lebensmittel-Großhändler und einen Filtertechnik-Anlagenbauer. Laut Tätern wurden vertrauliche Daten exfiltriert – ca. **10 GB** beim Großhändler und etwa **32 GB** beim Anlagenbauer. Die Veröffentlichungen sollten Druck erzeugen; trotz unterschiedlicher Branchen dienten beide Fälle der Eskalation mit Fristen und Drohungen.

**Was hätte man besser machen können?**

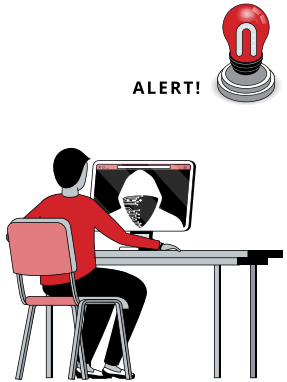
Die nahezu zeitgleiche Veröffentlichung beider Fälle deutete auf eine aktive Angriffskampagne hin. Eine frühere Erkennung ungewöhnlicher Zugriffe auf sensible Datenbereiche hätte Hinweise auf eine Kompromittierung liefern können. Der Einsatz von **Endpoint Detection and Response (EDR)** zur Überwachung kritischer Systeme sowie ein **SIEM** zur zentralen Korrelation sicherheitsrelevanter Ereignisse hätten die Transparenz erhöht und eine frühere Lagebewertung ermöglicht.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/11269-Akira-.png
https://www.security-incidents.de/assets/img/incidents/11270-Akira-.png

**Was lernen wir daraus:**

Die Akira-Fälle zeigten, dass Ransomware-Gruppen gezielt Organisationen mit sensiblen Geschäfts-, Personal- und Kundendaten angreifen, unabhängig von Branche oder Unternehmensgröße. Die öffentliche Nennung auf Leaksites diente als zentrales Druckmittel. Für Unternehmen bedeutet dies, dass insbesondere datenintensive Bereiche kontinuierlich überwacht werden müssen, um mögliche Angriffe frühzeitig einordnen und begrenzen zu können.




RIEDEL

# Cyberangriff auf Stadtentwässerung in Bayern betroffen

8. Dezember 2025, in Fürth/Bayern

DATENDIEBSTAHL

EINBRUCH

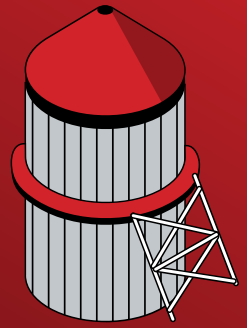
**Was ist passiert?**
Die IT-Infrastruktur einer Stadtentwässerung in Bayern war Ziel eines Cyberangriffs. Zwar wurden Teile der Systeme kompromittiert, die Abwasserentsorgung selbst blieb jedoch funktionsfähig. Städtische IT-Teams und Polizeispezialisten stoppten den Angriff und stellten die betroffenen Daten wieder her. Ein Zugriff auf einzelne Kundendaten konnte jedoch nicht ausgeschlossen werden.

**Was hätte man besser machen können?**
Der Vorfall zeigte, dass Angriffe auf kommunale Infrastrukturen trotz bestehender Schutzmaßnahmen möglich bleiben. Eine frühere Erkennung sicherheitsrelevanter Anomalien hätte die Analysephase verkürzen können. Eine zentrale Ereignis- und Logauswertung mittels **SIEM** sowie regelmäßige sicherheitstechnische Überprüfungen im Rahmen einer **IT-Musterung** hätten die Transparenz über den Sicherheitsstatus verbessert und die Reaktion unterstützt.

## Anzunehmende Schadensfelder:

Quellen:
https://www.nordbayern.de/fuerth/nach-cyberangriff-auf-stadt-furth-eindringliche-warnung-keine-akute-gefahr-fur-bevolkerung-1.14931064

**Was lernen wir daraus:**
Kommunale Betriebe tragen eine zentrale Verantwortung: Städte und Bürger sind auf ihre Dienste angewiesen, weshalb sie unter **NIS-2** oft als kritisch gelten. Umso wichtiger sind kontinuierliche Sicherheitschecks, klare Meldewege und funktionierende Notfallpläne. Regelmäßige Prüfungen der IT-Umgebung helfen, Angriffe früh zu erkennen und Auswirkungen für die öffentliche Versorgung zu minimieren.



RIEDEL

# Gefahr durch vertrauten Absender: Phishing nutzt Markenvertrauen gezielt aus

08. Dezember 2025, in Berlin/Berlin

PHISING

DATENDIEBSTAHL

**Was ist passiert?**
Ein Berliner Modeversand wurde im Dezember 2025 Opfer eines Datenlecks, bei dem Kriminelle gefälschte E-Mails an Kunden verschickten und sie zur Aktualisierung ihrer Zahlungsinformationen aufforderten. Dabei wurden Namen und Adressen kompromittiert, weshalb das Unternehmen die betroffenen Accounts vorsorglich sperrte.

**Was hätte man besser machen können?**
Der Vorfall zeigte, dass missbräuchliche Zugriffe auf Kundendaten erst nach dem Versand der Phishing-Mails erkannt wurden. Eine frühere Korrelation auffälliger Zugriffs- und Login-Muster hätte Hinweise auf die unzulässige Nutzung von Daten liefern können. Ein **Security Information and Event Management (SIEM)** zur zentralen Analyse sowie ein angebundenes **Security Operations Center (SOC)** hätten die Bewertung der Lage beschleunigt und die Reaktionszeit verkürzt.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.techniknews.net/news/outfittery-gehackt-bitte-aktualisieren-sie-ihre-zahlungsdaten-phishing-e-mails-im-umlauf/

**Was lernen wir daraus:**
Bei stark kundenorientierten Online-Geschäftsmodellen ist der Schutz personenbezogener Daten besonders kritisch. Eine regelmäßige Überprüfung sicherheitsrelevanter Prozesse, konsistente Zugriffskontrollen sowie klar definierte Abläufe zur Erkennung und Behandlung von Missbrauchsfällen können dazu beitragen, Risiken zu reduzieren und Auswirkungen eines Datenlecks frühzeitig zu begrenzen.

RIEDEL

# Koordinierte Angriffswelle: Safepay listet fünf neue Opfer gleichzeitig

05. Dezember 2025, in Deutschland

RANSOMWARE

EINBRUCH

**Was ist passiert?**
Innerhalb kurzer Zeit erschienen mehrere sehr unterschiedliche Organisationen auf der Leak-Seite der Ransomware-Gruppe **Safepay**, darunter ein Steuerbüro aus Schweinfurt, ein Film- und Fernsehstudio aus Köln, eine Gemeinde bei Heilbronn sowie Unternehmen aus der Textil- und Recyclingbranche. In allen Fällen setzten die Täter kurze Fristen zur Kontaktaufnahme. Angaben zum Umfang möglicher Datenabflüsse lagen nicht vor.

**Was hätte man besser machen können?**
Die zeitgleiche Veröffentlichung mehrerer Opfer deutete auf eine koordinierte Kampagne der Ransomware-Gruppe Safepay hin. Mehr Transparenz über sicherheitsrelevante Ereignisse hätte betroffenen Organisationen früher Hinweise auf auffällige Aktivitäten liefern können. Eine zentrale Analyse von Log- und Sicherheitsdaten mittels SIEM sowie strukturierte Reaktionsprozesse über SOAR hätten die Bewertung und Eindämmung der Vorfälle erleichtert.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/11254-Safepay.png
https://www.security-incidents.de/assets/img/incidents/11253-Safepay-.png
https://www.security-incidents.de/assets/img/incidents/11252-Safepay-Untereisesheim.png
https://www.security-incidents.de/assets/img/incidents/11248-Safepay.png
https://www.security-incidents.de/assets/img/incidents/11247-Safepay.png

**Was lernen wir daraus:**
Die Safepay-Fälle zeigten, dass Ransomware-Gruppen branchenübergreifend und opportunistisch vorgingen – von Kommunen bis hin zu Dienstleistern und Produktionsbetrieben. Öffentliche Leaksite-Einträge dienten dabei als Druckmittel mit kurzen Reaktionsfristen. Für Unternehmen bedeutet dies, dass Angriffe häufig nicht durch Individualwarnungen auffallen, sondern Teil größerer Kampagnen sind, die eine kontinuierliche und zentrale Sicherheitsüberwachung erfordern.

RIEDEL

# Design- und Markenberatung von Ransomware-Gruppe Akira gelistet

05. Dezember 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

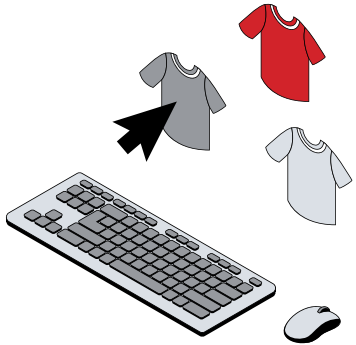
**Was ist passiert?**
Die Ransomware-Gruppe **Akira** setzte eine familiengeführte Design- und Markenberatung aus Deutschland auf ihre Opferliste. Die Angreifer machten den Vorfall öffentlich und drohten mit der Veröffentlichung kompromittierter Unternehmensdaten. Ob und in welchem Umfang Daten tatsächlich abgeflossen waren, blieb zum Zeitpunkt der Bekanntmachung unklar.

**Was hätte man besser machen können?**
Der Vorfall deutete darauf hin, dass ein möglicher Zugriff auf Unternehmensdaten erst durch die öffentliche Drohung bekannt wurde. Eine systematische Überprüfung der IT-Umgebung hätte potenzielle Schwachstellen früher aufzeigen können. Ein **Vulnerability Assessment** in Verbindung mit einer ganzheitlichen **IT-Musterung** hätte zur besseren Transparenz über Sicherheitslücken beigetragen und die Ausgangslage für eine frühere Reaktion verbessert.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/11255-Akira.png

**Was lernen wir daraus:**
Gerade in beratungsintensiven Branchen mit sensiblen Kunden- und Projektdaten ist ein angemessenes Sicherheitsniveau entscheidend. Regelmäßige Überprüfungen der IT-Strukturen, klar definierte Zugriffsrechte sowie organisatorische und technische Schutzmaßnahmen können dazu beitragen, Risiken zu reduzieren und Auswirkungen eines Angriffs zu begrenzen.



RIEDEL

# Eine Woche Stillstand im Weihnachtsgeschäft: finanzielle Ausfälle bei Fair-Trade-Unternehmen

03. Dezember 2025, in Wuppertal/Nordrhein-Westfalen

RANSOMWARE

AUSFALL

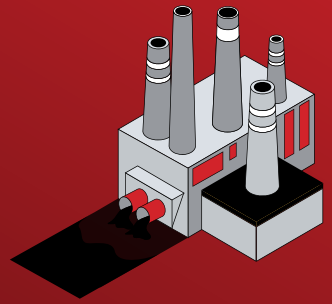
**Was ist passiert?**
Am 22. November 2025 legten unbekannte Täter die Logistiksysteme eines Fair-Trade-Unternehmens in Deutschland lahm. Durch einen Ransomware-Angriff wurden zentrale Daten verschlüsselt, Lagerbetrieb und Auslieferung kamen zum Stillstand. Laut Geschäftsführung wurde kein Lösegeld gezahlt. Nach rund einer Woche konnte ab dem 1. Dezember ein eingeschränkter Notbetrieb wieder aufgenommen werden.

**Was hätte man besser machen können?**
Der Vorfall verdeutlichte die erheblichen Auswirkungen eines Angriffs auf zentrale Logistik- und Betriebssysteme. Eine frühere Erkennung von Anomalien hätte die Reaktionszeit verkürzen können. Der Einsatz von SIEM zur zentralen Logauswertung sowie SOAR für eine strukturierte, teilautomatisierte Reaktion hätte Koordination und Eindämmung des Vorfalls unterstützt.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/11242-Gepa.png

**Was lernen wir daraus:**
Insbesondere unternehmenskritische Bereiche wie Logistik und Warenverteilung sollten durch gezielte Schutzmaßnahmen abgesichert sein. Regelmäßige Überprüfung von Systemen, klare Notfall- und Wiederanlaufpläne sowie abgestimmte Prozesse zur Angriffserkennung und -reaktion können dazu beitragen, Auswirkungen eines Ransomware-Angriffs zu begrenzen und die Betriebsfähigkeit schneller wiederherzustellen.



RIEDEL

# Festival-Betreiber aus Bayern auf Leaksite von DragonForce gelistet

02. Dezember 2025, in Chiemgau/Bayern

RANSOMWARE

DATENDIEBSTAHL

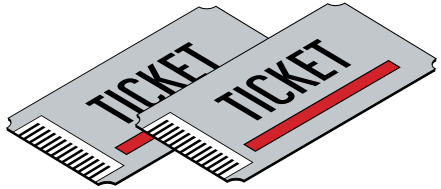
**Was ist passiert?**
Die Ransomware-Gruppe **DragonForce** führte einen Festival-Betreiber aus dem Chiemgau auf ihrer Darknet-Leaksite als Opfer auf. Die Täter behaupteten, **114,81 GB** an Daten aus den Systemen des Betreibers exfiltriert zu haben und kündigten eine Veröffentlichung der Daten für den 10. Dezember 2025 an. Eine Bestätigung des Umfangs lag nicht vor.

**Was hätte man besser machen können?**
Der Vorfall deutete darauf hin, dass ein möglicher Datenabfluss unbemerkt geblieben war. Eine frühere Erkennung ungewöhnlicher Datenbewegungen hätte die Eskalation voraussichtlich mindern können. Ein **SIEM** zur Korrelation und Alarmierung sowie **Endpoint Detection and Response (EDR)** zur Sichtbarkeit auf Endpunkten hätten verdächtige Aktivitäten eher aufgezeigt und die Eindämmung beschleunigt.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/11220-dragonforce.png

**Was lernen wir daraus:**
Insbesondere bei stark saisonabhängigen Geschäftsmodellen ist der Schutz sensibler Daten entscheidend. Regelmäßige Sicherheitsüberprüfungen, aktuelle Schutzmechanismen auf allen Endpunkten sowie klar definierte Melde- und Reaktionsprozesse hätten die Erfolgschancen eines Ransomware-Angriffs deutlich reduziert.




RIEDEL

# Ransomware-Angriff auf deutschen Formenbauer

01. Dezember 2025, in Deutschland

RANSOMWARE

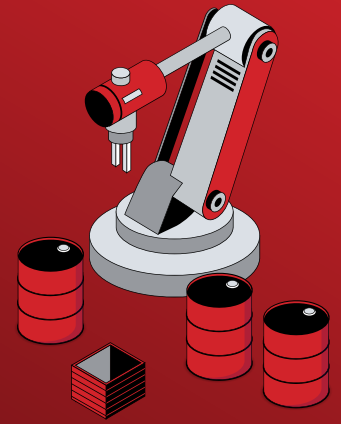
**Was ist passiert?**
Am 1. Dezember 2025 listete die Ransomware-Gruppe **Qilin** einen deutschen Formenbauer auf ihrer Darknet-Leaksite als Opfer. Mit der Veröffentlichung machte die Gruppe den Angriff öffentlich, ohne bisher Details zu möglichen Datenabflüssen oder zum Umfang der Kompromittierung zu nennen. Ob sensible Unternehmens- oder Kundendaten betroffen waren, blieb unklar.

**Was hätte man besser machen können?**
Eine zentralisierte Auswertung von Log- und Sicherheitsdaten hätte verdächtige Aktivitäten früher sichtbar machen können. Der Einsatz eines **SIEM-Systems** zur Ereigniskorrelation in Kombination mit **Security Orchestration, Automation and Response (SOAR)** hätte eine schnellere Bewertung sowie automatisierte Gegenmaßnahmen ermöglicht.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/11216-qilin.png

**Was lernen wir daraus:**
Eine konsequente Sicherheitsstrategie mit klaren Verantwortlichkeiten, regelmäßiger Überprüfung der IT-Landschaft und definierten Reaktionsprozessen hätte das Risiko eines erfolgreichen Angriffs deutlich reduziert. Vor allem die frühzeitige Erkennung und Eindämmung von Angriffen ist entscheidend, um eine Eskalation bis hin zur Veröffentlichung auf Leaksites zu verhindern.



RIEDEL

# NOVEMBER 2025

## SECURITY INCIDENTS GERMANY

RIEDEL

# Kanzlei lahmgelegt: Interne Daten vorübergehend unerreichbar

25. November 2025, in Paderborn/Nordrhein-Westfalen

RANSOMWARE

DATENDIEBSTAHL

AUSFALL

**Was ist passiert?**
Ende November 2025 erschien eine mittelständische Rechtsanwaltskanzlei auf der Leak-Seite von **Safepay**. Die Täter nannten die Webadresse des Unternehmens, jedoch mit falscher Beschreibung, und drohten mit einer Datenveröffentlichung. Das Unternehmen bestätigte den Cyberangriff, verneinte einen Zugriff auf interne Systeme, unterbrach vorsorglich den Netzwerkverkehr und schaltete Behörden ein.

**Was hätte man besser machen können?**
Eine konsequente Netzwerksegmentierung und klar definierte Zugriffsrechte und ein automatisiertes Patch- und Schwachstellenmanagement hätten den Angreifern den Einstieg deutlich erschwert. Ergänzt durch ein modernes Monitoring mit Echtzeit-Alarmierung lassen sich verdächtige Aktivitäten frühzeitig erkennen, bevor sie kritische Systeme erreichen.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/11177-safepay-kroeger-rehmann-partner-02.png
https://www.security-incidents.de/assets/img/incidents/11177-safepay-kroeger-rehmann-partner.png

**Was lernen wir daraus:**
Wer über unveränderliche, offline getrennte Backups verfügt und das Wiederherstellen regelmäßig unter Zeitdruck testet, verwandelt Erpressung in eine kalkulierbare, kurze Betriebsunterbrechung statt in eine Existenzfrage. Kurz: Nicht die perfekte Abschottung macht den Unterschied, sondern die geübte Rückkehr zum Normalbetrieb – mit sauberem Asset-Inventar, Wiederanlaufplänen und klaren Kommunikationsrouten.

RIEDEL

# Ransomware-Angriff auf Industrie-Zulieferer: Datenleak angedroht

25. November 2025, in Nordrhein-Westfalen

RANSOMWARE

DATENDIEBSTAHL

DATENLECK

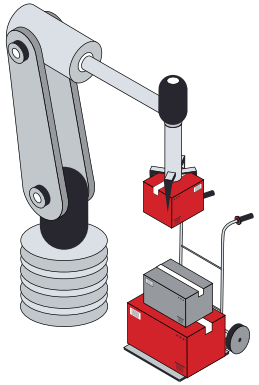
**Was ist passiert?**
Am 25. November 2025 wurde ein deutscher Zulieferer für Befestigungs- und Industrieteile auf dem Opferblog der Ransomware-Gruppe **Qilin** gelistet. Die Angreifer veröffentlichten erste Screenshots exfiltrierter Daten, um ihre Tat zu belegen. Welche Informationen betroffen waren und in welchem Umfang, war zum dem Zeitpunkt unklar.

**Was hätte man besser machen können?**
Der Vorfall zeigt, wie wichtig es ist, sensible Unternehmensdaten vor unbefugtem Zugriff zu schützen. **RIEDEL Enterprise Defense [R.E.D.]** mit **SOC** hätte eine kontinuierliche Überwachung und schnelle Reaktion ermöglicht. Zusätzlich kann eine **IT-Musterung** helfen, Schwachstellen frühzeitig zu identifizieren und zu schließen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/11183-Qilin.png

**Was lernen wir daraus:**
Ein umfassendes Sicherheitskonzept mit klaren Prozessen und kontinuierlicher Überwachung ist entscheidend, um Risiken frühzeitig zu erkennen. Ohne diese Grundlagen steigt die Wahrscheinlichkeit, dass Angriffe erfolgreich sind.



RIEDEL

# Qilin nimmt Spezialhersteller für Druckwalzen ins Visier

RANSOMWARE

25. November 2025, in Deutschland

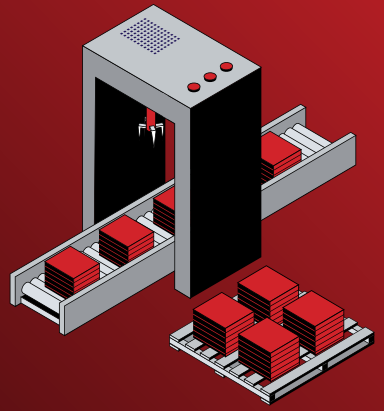
**Was ist passiert?**
Ein deutscher Spezialhersteller für Druckwalzen wurde auf dem Opferblog der Ransomware-Gruppe **Qilin** aufgelistet. Die Täter machten den Angriff öffentlich, ohne bislang Details zu Art oder Umfang möglicher Datenabflüsse zu nennen. Ob sensible Unternehmens- oder Kundendaten kompromittiert wurden, war zum Zeitpunkt der Veröffentlichung noch unklar.

**Was hätte man besser machen können?**
Der Vorfall deutete darauf hin, dass der Angriff erst mit der öffentlichen Nennung durch Qilin bekannt wurde. Eine frühere Erkennung möglicher Einstiegspunkte und Schwachstellen hätte das Risiko eines erfolgreichen Angriffs reduziert. Regelmäßige **Vulnerability Assessments** sowie eine strukturierte Sicherheitsüberprüfung im Rahmen einer **IT-Musterung** hätten geholfen, Sicherheitslücken frühzeitig zu identifizieren und gezielt zu schließen.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/11178-Qilin-Druckwalzen.png

**Was lernen wir daraus:**
Eine stärkere Ausrichtung auf präventive Sicherheitsmaßnahmen, klare Incident-Response-Prozesse und technische Schutzmechanismen hätte das Risiko eines erfolgreichen Ransomware-Angriffs deutlich reduziert. Entscheidend ist es, Angriffe frühzeitig zu erkennen und einzudämmen, bevor es zu einer öffentlichen Erpressung oder Datenveröffentlichung kommt.



RIEDEL

# IT-Stillstand an Hochschule nach schwerem Cyberangriff

24. November 2025, in Mainz/Rheinland-Pfalz

EINBRUCH

AUSFALL

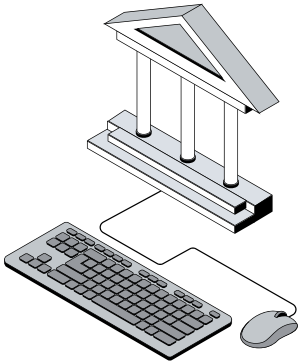
**Was ist passiert?**
Am 24. November 2025 wurde eine Hochschule Ziel eines Cyberangriffs. Vorsorglich schaltete sie alle IT-Systeme ab, wodurch viele digitale Dienste vorübergehend ausfielen. Präsenzbetrieb und Lehrveranstaltungen konnten jedoch stattfinden. Die IT analysierte den Vorfall, Behörden ermittelten, und ein Krisenstab koordinierte Maßnahmen und informierte über App und soziale Medien.

**Was hätte man besser machen können?**
Der Ausfall zentraler IT-Systeme zeigt, dass eine stärkere Trennung kritischer Dienste sowie klar definierte Notfallprozeduren für den Weiterbetrieb digitaler Kernfunktionen hilfreich gewesen wären. Zudem hätte eine kontinuierliche Netzwerküberwachung durch ein Security Operations Center (SOC) dazu führen können, dass sicherheitsrelevante Ereignisse möglicherweise früher erkannt werden, sodass ein vollständiges Abschalten weniger notwendig gewesen wäre.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.allgemeine-zeitung.de/lokales/mainz/stadt-mainz/cyberangriff-legt-it-systeme-der-hochschule-mainz-lahm-5188406
https://www.security-incidents.de/assets/img/incidents/11188-MitteilungHochschuleMainz241125.png

**Was lernen wir daraus:**
Das sofortige Abschalten der Systeme verhindert, dass Angreifer sich weiter ausbreiten, zusätzliche Daten stehlen oder weitere Schäden verursachen. Solange ein System aktiv mit dem Netzwerk verbunden ist, können unbefugte Dritte zum Beispiel weiterhin Befehle ausführen. Durch das Abschalten wird dieser Zugriff schlagartig unterbunden. Gleichzeitig ermöglicht es der IT-Abteilung, den Vorfall in einem stabilen Zustand zu analysieren, ohne dass sich Spuren verändern oder neue Schäden entstehen. So lassen sich Folgeschäden minimieren und die Wiederherstellung kontrollierter planen.



RIEDEL

# INC Ransom listet IT-Dienstleister auf Leaksite auf

22. November 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Am 22. November 2025 wurde ein deutsches Systemhaus für Datentechnik auf dem Darknet-Portal der Ransomware-Gruppe **INC Ransom** veröffentlicht. Die Täter stellten dort Screenshots mutmaßlich exfiltrierter Dateien ein. Welche Daten betroffen sind und in welchem Umfang Informationen abgeflossen sind, war unbekannt. Eine offizielle Stellungnahme zum Vorfall lag nicht vor.

**Was hätte man besser machen können?**
Der Vorfall ließ vermuten, dass der Angriff erst spät erkannt wurde, wohl erst nach der Datenveröffentlichung durch INC Ransom.
Eine kontinuierliche Überwachung hätte Anzeichen wie laterale Bewegungen oder Datenabfluss früher aufgezeigt. Ein **SOC** mit 24/7-Monitoring sowie **XDR** zur korrelierten Analyse von Endpunkten, Servern und Netzwerk hätte die Erkennungszeit verkürzt und den Schaden begrenzt.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/11186-INCRansom.png

**Was lernen wir daraus:**
Eine stärkere Fokussierung auf Prävention, frühzeitige Erkennung und strukturierte Reaktion hätte das Risiko eines erfolgreichen Ransomware-Angriffs reduziert. Dazu zählen regelmäßige Sicherheitsüberprüfungen, aktuelle Schutzmechanismen an allen Endpunkten, klar definierte Prozesse zur Angriffserkennung sowie geschulte Mitarbeitende. Entscheidend ist, Angriffe bereits in der Initial- oder Bewegungsphase zu stoppen und nicht erst bei der Androhung oder Veröffentlichung von Daten.

RIEDEL

# 286 GB Daten eines Dachdeckerbetriebs veröffentlicht

20. November 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

DATENLECK

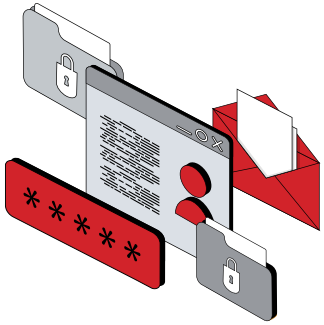
**Was ist passiert?**
Ein deutscher Dachdeckerbetrieb wurde im November 2025 von der Ransomware-Gruppe **Sarcoma** als Opfer auf deren Leak-Seite aufgeführt. Die Täter gaben an, **286 GB** Daten aus den Systemen des Unternehmens entwendet zu haben und veröffentlichten dazu einen Download-Link sowie mehrere Screenshots als Nachweis.

**Was hätte man besser machen können?**
Da die Täter 286 GB Daten entwenden und anschließend veröffentlichen konnten, wäre insbesondere eine engere Überwachung von Datenbewegungen sinnvoll gewesen. Ein Data-Loss-Prevention-System oder Logs, die ungewöhnliche große Transfers erkennen, hätten den Abfluss frühzeitig sichtbar machen können. Zudem hätte eine klarere Segmentierung der internen Systeme verhindert, dass Angreifer auf so große Datenmengen gleichzeitig zugreifen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/11136-sarcoma-soellner.png

**Was lernen wir daraus:**
Der Fall zeigt, wie wichtig es ist, die Sichtbarkeit im eigenen Netzwerk zu erhöhen. Unternehmen müssen jederzeit nachvollziehen können, wer auf welche Daten zugreift und in welchem Umfang. Ohne diese Transparenz bleibt ein massiver Datenabfluss – wie die hier entwendeten 286 GB – oft unbemerkt. Eine verbesserte Protokollierung und Auswertung von Zugriffs- und Transferaktivitäten ist daher ein zentraler Bestandteil moderner Sicherheitsstrategien.




RIEDEL

# Cyberangriff auf HMI-Technologieunternehmen: Vertrauliche Unterlagen entwendet

20. November 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Ein Unternehmen aus dem HMI-Technologie-Bereich wurde von der Ransomware-Gruppe **Akira** auf deren Darknet-Plattform als Opfer gelistet. Die Täter behaupten, **91 GB** vertrauliche Daten erbeutet zu haben – darunter Mitarbeiterinformationen, Finanz- und Buchhaltungsunterlagen sowie Kunden-, Projekt-, Vertrags- und Rechtsdokumente.

**Was hätte man besser machen können?**
Eine striktere Zugriffssteuerung, rollenbasierte Berechtigungen und eine engmaschige Überwachung von Dateiaktivitäten hätten die unbemerkte Exfiltration erschwert. Zusätzlich hätten regelmäßige Schwachstellentests und Penetrationstests, insbesondere an extern erreichbaren Systemen, potenzielle Zugriffspunkte für die Ransomware-Gruppe Akira frühzeitig aufdecken können.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/11148-Akira.png

**Was lernen wir daraus:**
Der Fall zeigt, dass Ransomware-Gruppen zunehmend gezielt Datenexfiltration einsetzen, bevor sie weiteren Schaden verursachen. Unternehmen müssen daher insbesondere Systeme einführen, die ungewöhnlich große Datenabflüsse frühzeitig erkennen und melden. Das Monitoring von Datenbewegungen wird damit zu einem zentralen Bestandteil wirksamer Sicherheitsstrategien.

RIEDEL

# 851 GB Daten bei Bildungs-Technologie-Firma entwendet

18. November 2025, in Hamburg/Hamburg

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Ein Bildungstechnologie-Unternehmen aus Hamburg wurde am 18. November 2025 Ziel einer Ransomware-Attacke. Die Ransomware-Gruppe **INC Ransom** listete das Unternehmen auf ihrem Opfer-Portal und gab an, **851 GB** vertrauliche Daten exfiltriert zu haben.

**Was hätte man besser machen können?**
Ein zentraler Punkt ist die konsequente Absicherung von Zugriffen, etwa durch Mehrfaktor-Authentifizierung, starke Passwortrichtlinien und die regelmäßige Überprüfung privilegierter Konten. Auch ein striktes Patch- und **Schwachstellenmanagement** hätte potenzielle Einstiegspunkte minimieren können, insbesondere wenn Angreifer bekannte Sicherheitslücken ausnutzen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/11117-INCRansom.png

**Was lernen wir daraus:**
Der Vorfall macht deutlich, dass Angriffe auf Unternehmen im Bildungs- und Technologiebereich längst nicht mehr Ausnahmefälle sind. Gerade dort, wo Lernplattformen, Nutzerkonten, Entwicklungsdaten oder vertrauliche Forschungsinhalte gespeichert werden, entsteht ein attraktives Ziel für Cyberkriminelle. Aus dem Fall lässt sich ableiten, wie wichtig es ist, größere Datenabflüsse in Echtzeit zu überwachen.

RIEDEL

# Stadtwerke lahmgelegt: Mitarbeiter müssen auf Notfallkanäle ausweichen

AUSFALL

18. November 2025, in Detmold/Nordrhein-Westfalen

**Was ist passiert?**
Das Kommunikationssystem eines regionalen Energie- und Wasserversorgers wurde durch einen gezielten Cyberangriff außer Betrieb gesetzt. Kunden mussten auf eine externe Störungshotline ausweichen. Die Versorgung blieb stabil. Ob Daten entwendet wurden, war unklar. Die Polizei wurde eingeschaltet.

**Was hätte man besser machen können?**
Eine zentrale Schwachstelle bei ähnlichen Vorfällen sind häufig unzureichend gesicherte Zugänge, etwa fehlende Mehrfaktor-Authentifizierung oder veraltete Passwortrichtlinien. Auch ein möglicher Angriffsvektor über ungepatchte Systeme oder veraltete Softwarekomponenten hätte durch ein strengeres Patch- und Schwachstellenmanagement reduziert werden können.

## Anzunehmende Schadensfelder:

Quellen:
https://www.heise.de/news/Stadtwerke-Detmold-nach-IT-Vorfall-offline-11082906.html
https://www1.wdr.de/nachrichten/westfalen-lippe/Hackerangriff-Stadtwerke-Detmold-100.html

**Was lernen wir daraus:**
Als Energie- und Wasserversorger zählt der Betrieb zum **NIS-2-relevanten Bereich** – und damit zu den Diensten, auf die Städte und Bürger täglich angewiesen sind. Der Vorfall zeigt, wie wichtig Cyberresilienz als fortlaufender Prozess ist: Neben technischen Schutzmechanismen braucht es klare Meldewege, geübte Notfallabläufe und geschultes Personal. Da ein Angriff auch ohne Erpressungsabsicht erhebliche Störungen auslösen kann, sind frühzeitige Erkennungssysteme wie Anomalie- und Log-Monitoring unverzichtbar.

RIEDEL

# 1,2 TB Datendiebstahl: Ransomware-Angriff legt Elektrounternehmen lahm

17. November 2025, in München/Bayern

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Ein Münchner Elektrounternehmen ist wurde Ziel einer Ransomware-Attacke. Die Hackergruppe **Payoutsking** erbeutete dabei rund **1,2 Terabyte**. Die Webseite der Firma war zwischenzeitlich nicht erreichbar.

**Was hätte man besser machen können?**
Viele Ransomware-Gruppen gelangen über ungepatchte Sicherheitslücken, kompromittierte Konten oder fehlende Mehrfaktor-Authentifizierung ins Netzwerk – Schwachstellen, die laut Analysen häufig ausgenutzt werden. Besser aufgestellte Patch-Prozesse, konsequente **MFA-Nutzung** und strengere Zugangskontrollen hätten das Risiko deutlich verringern können. Ebenso wichtig sind regelmäßige Mitarbeiterschulungen zur Erkennung von Phishing-Angriffen, da diese oft der erste Einstiegspunkt sind.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/11179-Payoutsking.png

**Was lernen wir daraus:**
Der Angriff zeigt deutlich, wie wichtig grundlegende Cyberhygiene ist: Unternehmen müssen Schwachstellen konsequent schließen, Mehrfaktor-Authentifizierung einsetzen und Mitarbeitende regelmäßig für Phishing-Gefahren sensibilisieren.


RIEDEL

# Cyberangriff legt Radiosenderbetrieb zeitweise lahm

15. November 2025, in München/Bayern

**EINBRUCH**

**AUSFALL**

**Was ist passiert?**
Ein Radiosender und sein Partnerbetrieb wurden Ziel eines Hackerangriffs. Live-Sendungen am Montagmorgen waren nicht möglich, das Team arbeitete mit zeitversetzt produzierten Beiträgen aus der Cloud. Ein Cloud-Backup verhinderte größeren Schaden. Der reguläre Betrieb wurde nach ca. 72 Stunden wieder aufgenommen, während die Systeme weiterhin untersucht wurden.

**Was hätte man besser machen können?**
Positiv hervorzuheben ist, dass das aktuelle Cloud-Backup bereits größeren Schaden verhindert hat. Zusätzlich könnte ein kontinuierliches Sicherheitsmonitoring **(SOC)** eingesetzt werden, das nicht nur ungewöhnliche Aktivitäten, sondern auch untypische Zugriffe auf Systeme und Daten erkennt. So lassen sich Angriffe schneller sichtbar machen, Schäden begrenzen und die Wiederherstellung nach Sicherheitsvorfällen effizienter gestalten.

## Anzunehmende Schadensfelder:

Quellen:
https://www.radioarabella.de/in-eigener-sache-hackerangriff-auf-arabella-muenchen-2967019/
https://www.digitalfernsehen.de/news/inhalte/radio-inhalte/naechster-radiosender-von-hackerangriff-betroffen-1164267/

**Was lernen wir daraus:**
Der Vorfall zeigt, wie kritisch kontinuierliche IT-Sicherheit für Medienbetriebe ist. Auch wenn Backups Schäden begrenzen, können Systemangriffe den Betrieb über mehrere Tage stören. Frühzeitiges Monitoring, strukturierte Wiederherstellungspläne und regelmäßige Sicherheitsüberprüfungen sind entscheidend, um Störungen zu minimieren und Abläufe aufrechtzuerhalten.

RIEDEL

# Unbefugte Weitergabe von Justizdaten löst Ermittlungen aus

14. November 2025, in Stuttgart/Baden-Württemberg

INNENTÄTER

RECHTSMISSBRAUCH

DATENLECK

DATENHEHLEREI

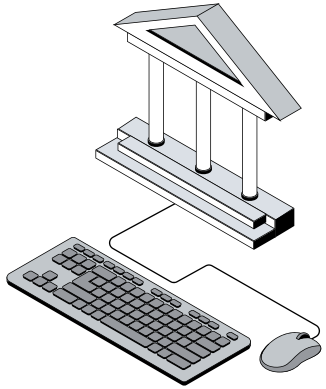
**Was ist passiert?**
Nach mehreren bewaffneten Angriffen im Frühjahr 2025 wurden im Herbst schwere Sicherheitsverstöße in einer Staatsanwaltschaft bekannt. Mindestens sieben Mitarbeitende sollen gegen Geld sensible Daten aus dem Justizsystem web.sta weitergegeben haben. Zwei mutmaßliche Auftraggeber wurden festgenommen, ein Bezug zur organisierten Kriminalität blieb unklar. Der Vorfall führte zu Disziplinarmaßnahmen und einer politischen Debatte über Sicherheitslücken in der Justizverwaltung.

**Was hätte man besser machen können?**
Eine engere Kontrolle interner Datenzugriffe sowie klar definierte **Berechtigungskonzepte** hätten dabei unterstützt, untypische Zugriffs- oder Weitergabemuster früher zu erkennen. Ergänzend könnten regelmäßige Überprüfungen von Nutzerkonten, verpflichtende **Protokollauswertungen** und strengere organisatorische Regeln wie das **Vier-Augen-Prinzip** bei besonders sensiblen Informationen die Transparenz erhöhen und das Risiko von Datenmissbrauch reduzieren.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.stuttgarter-zeitung.de/inhalt.verbindungen-in-die-justiz-der-fall-frost-wie-aus-dem-security-konflikt-ein-korruptionsskandal-wurde.5b04b18d-817f-46d0-9cc9-579e905ef797.html
https://www.tagesschau.de/inland/regional/badenwuerttemberg/wachtmeister-ermittlungen-stuttgart-100.html

**Was lernen wir daraus:**
Der Vorfall zeigt, dass nicht nur externe Angriffe, sondern auch interne Bedrohungen erhebliche Risiken für Behörden darstellen. Strenge Zugriffskontrollen, kontinuierliche Überwachung sensibler Systeme und klare Meldewege für verdächtige Aktivitäten sind essenziell, um Datenmissbrauch zu verhindern und Vertrauen in staatliche Institutionen zu sichern.



RIEDEL

# 1,4 TB Firmendaten gestohlen: Deutscher Verpackungshersteller im Visier von Sarcoma

11. November 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

DATENLECK

**Was ist passiert?**
Anfang November 2025 wurde ein deutscher Verpackungshersteller von der Ransomware-Gruppe **Sarcoma** als Opfer gelistet. Die Angreifer sollen **1,4 TB** an Firmendaten, darunter vertrauliche Dokumente wie Geheimhaltungsvereinbarungen, gestohlen und zum Download bereitgestellt haben. Das Unternehmen untersuchte den Vorfall und ergriff Sicherheitsmaßnahmen.

**Was hätte man besser machen können?**
Um die Risiken für sensible Unternehmensdaten zu verringern, könnten Unternehmen zusätzlich **Vulnerability Assessment** einsetzen, um Schwachstellen systematisch zu erkennen, SIEM zur Analyse und Korrelation von sicherheitsrelevanten Ereignissen nutzen und auf **Extended Detection & Response (XDR)** setzen, um Bedrohungen über verschiedene Systeme hinweg frühzeitig zu identifizieren.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/11038-sarcoma.png

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

RIEDEL

# Ransomware-Angriff auf IT-Systeme eines internationalen Autoglas-Dienstleisters

11. November 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

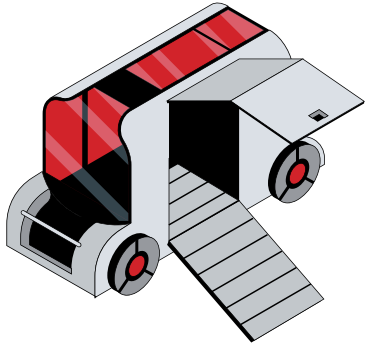
**Was ist passiert?**
Die Ransomware-Gruppe **CL0P** listet zwischenzeitlich ein internationales Autoglas-Unternehmen auf ihrer Darknet-Seite als betroffen. Der Vorfall betrifft Nutzer der eingesetzten Unternehmenssoftware, konkrete Datenabflüsse sind unklar. Das Unternehmen untersuchte die Situation und ergriff Sicherheitsmaßnahmen, um den Schäden zu begrenzen.

**Was hätte man besser machen können?**
Besserer Schutz kritischer Geschäftssysteme könnte durch kontinuierliches Sicherheitsmonitoring **SOC** zur Überwachung verdächtiger Aktivitäten, regelmäßige **IT-Musterung** zur frühzeitigen Erkennung von Sicherheitslücken und durch umfassenden Endpoint-Schutz für Arbeitsplätze und Server **EDR** erreicht werden, um Risiken deutlich zu reduzieren.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/11053-Cl0p-Carglass.png

**Was lernen wir daraus:**
Auch ohne bestätigten Datenabfluss zeigt der Vorfall, wie schnell kritische Systeme angegriffen werden können. Unternehmen müssen Risiken für Datenmissbrauch, Betriebsunterbrechungen und Reputationsverlust ernst nehmen. Proaktives Sicherheitsbewusstsein, schnelle Reaktion auf Vorfälle und regelmäßige Überprüfung der IT-Infrastruktur sind entscheidend, um Schäden zu begrenzen.



RIEDEL

# Massiver Datenangriff auf Online-Ticketsystem eines Hamburger Freizeitunternehmens

11. November 2025, in Hamburg/Hamburg

**MALWARE**

**DATENDIEBSTAHL**

**Was ist passiert?**
Zwischen Juni und Oktober 2025 wurde das Online-Ticketsystem eines großen Hamburger Freizeitunternehmens mit Schadsoftware kompromittiert. Die Angreifer erlangten Zugriff auf Kreditkartendaten zehntausender Besucher. Das Unternehmen reagierte umgehend mit verschärften Sicherheitsmaßnahmen. Ein finanzieller Schaden entstand nicht, doch das Risiko von Datenmissbrauch bleibt.

**Was hätte man besser machen können?**
Besserer Schutz sensibler Zahlungsdaten durch kontinuierliches Sicherheitsmonitoring **(SOC)**, regelmäßige **Schwachstellenanalysen** (Vulnerability Assessment) und automatisierte Bedrohungserkennung **Security Orchestration, Automation & Response – SOAR** hätte die Risiken deutlich reduziert.

**Anzunehmende Schadensfelder:**

Quellen:
https://cybernews.com/de/sicherheit/hackerangriff-auf-miniatur-wunderland-hamburg/
https://www.heise.de//news/Miniatur-Wunderland-Ziel-von-IT-Angriff-Kreditkartendaten-abgeflossen-11076011.html

**Was lernen wir daraus:**
Regelmäßige Überprüfung von IT-Systemen auf Schwachstellen, Echtzeit-Überwachung kritischer Datenflüsse und automatisierte Reaktionsprozesse sind essenziell. Selbst Unternehmen ohne direkten finanziellen Schaden können massive Risiken für Kundendaten und Reputation tragen. Sicherheitsbewusstsein und proaktive Verteidigungsstrategien verhindern teure Zwischenfälle.

RIEDEL

# Schwerer Cyberangriff trifft deutsche Radiostation und legt Betrieb lahm

10. November 2025, in Norden/Niedersachsen

EINBRUCH

AUSFALL

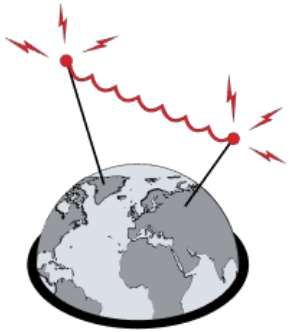
**Was ist passiert?**
Um den 10. November 2025 wurde ein deutscher Radiosender Ziel eines schweren Cyberangriffs. Teile der technischen Infrastruktur, sowohl Software als auch Hardware, wurden beschädigt, einige Systeme unwiederbringlich. Der Sender musste seine gesamte IT- und Sendetechnik in kurzer Zeit neu aufbauen, um den Betrieb wiederherzustellen.

**Was hätte man besser machen können?**
Der Vorfall zeigt, wie wichtig resiliente IT- und Broadcast-Infrastrukturen sind. Besonders hilfreich wären regelmäßige Backups, redundante Systeme und Notfallpläne für kritische Hardware, um die Betriebsfähigkeit auch nach schweren Angriffen schnell wiederherstellen zu können. Zusätzlich hilft der Einsatz eines **Security Operations Centers (SOC)** und überwachender Security-Lösungen, um frühzeitig ungewöhnliche Aktivitäten zu erkennen und schneller auf Angriffe reagieren zu können.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.radioszene.de/207744/radio-nordseewelle-hackerangriff.html
https://www.digitalfernsehen.de/news/inhalte/radio-inhalte/hackerangriff-bei-radio-nordseewelle-enorme-belastung-1163672/

**Was lernen wir daraus:**
Der Angriff verdeutlicht, dass selbst Medienunternehmen zunehmend Ziel professioneller Cyberkrimineller werden. Redundante Systeme, schnelle Wiederherstellungsprozesse und kontinuierliches Monitoring sind entscheidend, um kritische technische Infrastrukturen zu schützen und die Betriebsfähigkeit nach einem Angriff zu sichern.



RIEDEL

# IT-Störung legt städtische Dienste vorübergehend lahm

07. November 2025, in Ludwigshafen/Rheinland-Pfalz

EINBRUCH

AUSFALL

**Was ist passiert?**
Die IT einer deutschen Stadtverwaltung musste vorsorglich abgeschaltet werden, nachdem ungewöhnliche Zugriffe einen Alarm ausgelöst hatten. Seitdem waren digitale und telefonische Dienste eingeschränkt. Polizei und Datenschutzbehörden ermittelten. Bürgerbüros und die Müllabfuhr blieben weiterhin im Betrieb.

**Was hätte man besser machen können?**
Der Vorfall verdeutlicht die Notwendigkeit proaktiver Überwachung durch ein **SOC** und Zugriffskontrollen in Verwaltungs-IT-Systemen. Ergänzend können Segmentierung der Netzwerke, Sicherheitswarnsysteme und Notfallpläne dazu beitragen, die Auswirkungen solcher Angriffe zu minimieren und die Betriebskontinuität für Bürgerdienste zu sichern.

## Anzunehmende Schadensfelder:

Quellen:
https://www.rheinpfalz.de/lokal/ludwigshafen_artikel,-viele-spekulationen-nach-hackerangriff-auf-stadtverwaltung-ludwigshafen-_arid,5829403.html
https://www.borncity.com/blog/2025/11/07/cyberangriff-auf-stadtverwaltung-ludwigshafen/

**Was lernen wir daraus:**
Der Fall zeigt, dass kommunale IT-Systeme zunehmend Ziel digitaler Angriffe sind. Präventive Maßnahmen wie kontinuierliches Monitoring, klare Notfallprozesse und frühzeitige Erkennung verdächtiger Aktivitäten sind entscheidend, um die Handlungsfähigkeit der Verwaltung aufrechtzuerhalten und den Bürgerbetrieb zu sichern.

RIEDEL

# Angriff auf Luft- und Raumfahrt: Ransomware legt Systeme lahm

07. November 2025, in Deutschland

RANSOMWARE

ERPRESSUNG

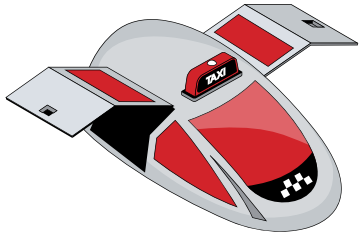
**Was ist passiert?**
Die Ransomware-Gruppe **RansomHouse** meldete einen Angriff auf ein deutsches Luft- und Raumfahrtsunternehmen. Die Täter behaupteten, Firmensysteme verschlüsselt zu haben und boten an, Beweise bereitzustellen. Das Unternehmen wurde aufgefordert, dringend Kontakt aufzunehmen. Angaben zu gestohlenen Daten oder einer Frist machten die Angreifer nicht.

**Was hätte man besser machen können?**
Der Angriff unterstreicht die Bedeutung proaktiver Sicherheitsmaßnahmen. Eine umfassende IT-Überprüfung kann helfen, potenzielle Schwachstellen früher zu erkennen, bevor sie ausgenutzt werden. Zudem bietet RIEDEL Enterprise Defense [R.E.D.] mit **SOC-Unterstützung** eine kontinuierliche Überwachung und ermöglicht eine schnelle Reaktion auf verdächtige Aktivitäten, was das Risiko ähnlicher Vorfälle deutlich reduzieren kann.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/11217-ransomhouse.png

**Was lernen wir daraus:**
Ein umfassendes Sicherheitskonzept mit regelmäßigen Schwachstellenanalysen, klaren Prozessen und einer hohen Sensibilisierung für Cyberrisiken ist entscheidend. Ohne diese Grundlagen steigt das Risiko für Ransomware-Angriffe erheblich.




RIEDEL

# Cyberattacke legt medizinische Einrichtungen in Bayern zeitweise lahm

06. November 2025, in Weiden in der Oberpfalz/Bayern

**MALWARE**

**AUSFALL**

**Was ist passiert?**
Ein medizinischer Dienstleister war Ziel eines Cyberangriffs. Nach der Einschleusung von Schadsoftware mussten die IT-Systeme an mehreren Standorten abgeschaltet werden, um eine weitere Ausbreitung zu verhindern. Digitale Dienste wie E-Rezepte waren gestört, Operationen wurden verschoben. Der Hauptstandort blieb funktionsfähig, die Wiederaufnahme des Regelbetriebs war in Vorbereitung.

**Was hätte man besser machen können?**
Der Vorfall zeigt die Bedeutung konsequenter IT-Sicherheitsstrategien im Gesundheitswesen. Besonders in sensiblen Bereichen sollten Netzwerksegmentierung, mehrstufige Zugriffskontrollen und regelmäßige Penetrationstests etabliert sein. Ergänzend helfen **Security Operations Center (SOC)-Dienste** und **SIEM-Lösungen**, Angriffe frühzeitig zu erkennen und die Reaktionszeit deutlich zu verkürzen.

## Anzunehmende Schadensfelder:

Quellen:
https://www.oberpfalzecho.de/beitrag/cyberangriff-legt-mvz-in-tirschenreuth-und-kemnath-lahm
https://www.onetz.de/oberpfalz/tirschenreuth/cyberattacke-mvz-behandlungen-tirschenreuth-id5227186.html

**Was lernen wir daraus:**
Der Angriff unterstreicht, wie stark das Gesundheitswesen im Fokus von Cyberkriminellen steht. Besonders Einrichtungen mit sensiblen Patientendaten müssen auf resiliente IT-Strukturen und ein durchdachtes Notfallkonzept setzen.

RIEDEL

# Stadtverwaltung nach DDoS-Attacke lahmgelegt

05. November 2025, in Trier/Rheinland-Pfalz

DDoS

AUSFALL

**Was ist passiert?**
Die Website einer deutschen Stadtverwaltung wurde Ziel eines massiven **DDoS-Angriffs**. Durch die Überlastung der Server war der Online-Auftritt über mehrere Tage nicht erreichbar. Erst einige Tage später konnte der Betrieb wiederhergestellt werden, die Attacken hielten jedoch weiter an.

**Was hätte man besser machen können?**
Der Vorfall unterstreicht die Bedeutung robuster Schutzmechanismen gegen Überlastungsangriffe. **DDoS-Abwehr-Services**, intelligente Traffic-Filter und eine skalierbare Cloud-Infrastruktur können helfen, Angriffe frühzeitig abzufangen und den Dienst aufrechtzuerhalten. Auch eine enge Zusammenarbeit mit spezialisierten Sicherheitsanbietern ist in solchen Fällen entscheidend.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.swr.de/swraktuell/rheinland-pfalz/trier/cyberattacke-auf-internetseite-der-stadt-trier-100.html

**Was lernen wir daraus:**
DDoS-Attacken zielen oft darauf ab, öffentliche Infrastrukturen lahmzulegen und Vertrauen zu untergraben. Prävention durch technische Redundanz, kontinuierliches Monitoring und eine klare Incident-Response-Strategie sind daher unverzichtbar, um die digitale Handlungsfähigkeit zu sichern.


RIEDEL

# Oktober 2025

## SECURITY INCIDENTS GERMANY

RIEDEL

# Safepay veröffentlicht Daten eines Büroausstatters aus Wiesbaden

31. Oktober 2025, in Wiesbaden/Hessen

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Am 31. Oktober 2025 wurde ein Büroausstatter aus Wiesbaden von der Ransomware-Gruppe **Safepay** auf deren Darknet-Seite als Opfer gelistet. Die Angreifer behaupten, Unternehmensdaten entwendet und bereits veröffentlicht zu haben. Welche Informationen konkret betroffen sind, ist unbekannt.

**Was hätte man besser machen können?**
Der Vorfall zeigt, wie wichtig eine mehrschichtige Sicherheitsstrategie ist. Durch den Einsatz von **Endpunktüberwachung (EDR/XDR)** zur Erkennung verdächtiger Aktivitäten sowie regelmäßige Backups und Zugriffskontrollen hätten sich die Auswirkungen eines Angriffs reduzieren lassen. Zusätzlich helfen Security Awareness Trainings, Mitarbeitende für verdächtige Vorgänge zu sensibilisieren.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10961-safepay.png

**Was lernen wir daraus:**
Der Angriff durch Safepay verdeutlicht, dass selbst mittelständische Unternehmen zunehmend in den Fokus professioneller Cybergruppierungen rücken. Technische Schutzmaßnahmen, Mitarbeiterschulung und klare Prozesse für den Ernstfall sind entscheidend, um Risiken zu minimieren und die Geschäftskontinuität nach einem Angriff schnell wiederherzustellen.

RIEDEL

# Angriff auf IT-Dienstleister im deutschen Händlernetz sorgt für massive Störungen

RANSOMWARE

31. Oktober 2025, in Frankfurt am Main/Hessen

**Was ist passiert?**
Ein zentraler IT-Dienstleister wurde Opfer eines gezielten Ransomware-Angriffs. Das Unternehmen verarbeitet Marketing- und Kundendaten für verschiedene Automobilmarken und musste seine gesamte Plattform kurzfristig abschalten, um eine Ausbreitung der Schadsoftware zu verhindern. Hinweise auf einen Datendiebstahl gab es offiziell nicht, Sicherheitsexperten halten diesen jedoch für wahrscheinlich.

**Was hätte man besser machen können?**
Der Angriff unterstreicht, wie wichtig ein durchgängiges Sicherheitskonzept bei Dienstleistern mit sensiblen Daten ist. Eine Zero-Trust-Architektur zur konsequenten Zugriffskontrolle, automatisierte **Security-Orchestration and Response (SOAR)** sowie regelmäßige **Vulnerability Assessments** können helfen, Risiken zu erkennen, Angriffswege zu schließen und die Reaktionsgeschwindigkeit im Ernstfall zu erhöhen.

## Anzunehmende Schadensfelder:

Quellen:
https://www.borncity.com/blog/2025/10/31/cyberangriff-auf-move-xm-dienstleister-fuer-alle-vw-audi-haendler/

**Was lernen wir daraus:**
Der Vorfall zeigt, dass Cyberangriffe auf Dienstleister in der Lieferkette weitreichende Auswirkungen auf ganze Branchen haben können. Unternehmen sollten die Sicherheit ihrer Partner regelmäßig prüfen, klare Schnittstellenrichtlinien etablieren und auf mehrstufige Zugriffskontrollen setzen, um Kundendaten zu schützen und Betriebsunterbrechungen zu vermeiden.


RIEDEL

# Datenklau bei Produktionsunternehmen: Akira droht Veröffentlichung

30. Oktober 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

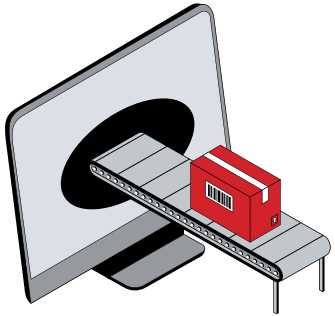
**Was ist passiert?**
Ein Hersteller von Verpackungsmaschinen und kompletten Verpackungslinien wurde Opfer der Ransomware-Gruppe **Akira**. Die Angreifer behaupten, sensible Unternehmensdaten erbeutet zu haben, darunter Finanzinformationen, Mitarbeiter- und Kundendaten.

**Was hätte man besser machen können?**
Der Vorfall zeigt, dass insbesondere Produktionsunternehmen ihre sensiblen Daten konsequent schützen müssen. Hilfreich sind kontinuierliche Überwachung kritischer Systeme, klare Rollen- und Rechteverteilungen für den Zugriff auf Daten sowie regelmäßige Penetrationstests, um Sicherheitslücken frühzeitig aufzudecken und gezielt zu schließen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10976-Akira.png

**Was lernen wir daraus:**
Der Angriff zeigt, dass insbesondere Personaldaten und andere sensible Informationen besonders schützenswert sind. Unternehmen sollten solche Daten nicht nur technisch absichern, sondern auch organisatorisch schützen, etwa durch Zugriffsbeschränkungen, Verschlüsselung und klare Verantwortlichkeiten im Datenumgang.



RIEDEL

# Phishing-Angriff auf Autohändler: Gefälschte Mobile.de-Mails verbreiten Schadsoftware

31. Oktober 2025, in Deutschland

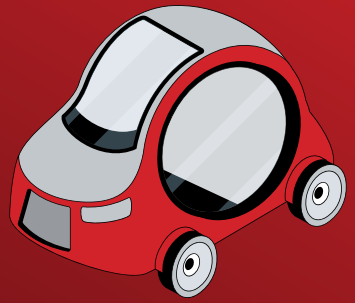
MALWARE

IDENTITÄTSDIEBSTAHL

**Was ist passiert?**
Zwischen dem 29. und 31. Oktober 2025 wurden Autohäuser in Deutschland gezielt mit gefälschten E-Mails attackiert, die angeblich von Mobile.de stammten. Die Nachrichten enthielten eine manipulierte PDF-Datei. Klickte ein Empfänger auf „Download PDF“, wurde über einen eingebetteten Dropbox-Link eine ausführbare Datei heruntergeladen, die Schadsoftware installierte. Ziel waren offenbar Händlerkonten und Kundendaten.

**Was hätte man besser machen können?**
Der Vorfall zeigt, wie gefährlich gezielte Phishing-Angriffe sein können. Hilfreich sind Mitarbeiterschulungen zur Erkennung verdächtiger E-Mails, der Einsatz von E-Mail-Sicherheitslösungen mit Malware- und Link-Scanning sowie Multi-Faktor-Authentifizierung für Händlerkonten, um das Risiko unbefugter Zugriffe zu reduzieren.

**Was lernen wir daraus:**
Der Fall verdeutlicht, dass Phishing weiterhin eine der effektivsten Methoden für Cyberangriffe ist. Unternehmen sollten neben technischen Schutzmaßnahmen auch regelmäßige Schulungen, klare Prozesse für verdächtige E-Mails und kontinuierliche Überprüfung von Zugangsdaten etablieren, um Kundendaten und Konten bestmöglich zu schützen.



## Anzunehmende Schadensfelder:

Quellen:
https://www.borncity.com/blog/2025/10/31/virenversand-ueber-mobile-de-nachrichten-teil-3/
https://www.sentiguard.eu/wissen/gefaelschte-mobile-de-nachrichten-verteilen-schadsoftware-an-autohaendler/

RIEDEL

# Chaos-Ransomware kompromittiert 650 GB Daten eines Container-Terminals

28. Oktober 2025, in Nordrhein-Westfalen

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Ende Oktober 2025 wurde ein Container-Terminal in Nordrhein-Westfalen Ziel der Ransomware-Gruppe **Chaos**. Die Angreifer gaben an, **650 GB** an Daten aus den Systemen des Betreibers erbeutet zu haben und drohten mit deren Veröffentlichung.

**Was hätte man besser machen können?**
Der Vorfall zeigt, wie wichtig eine klare Segmentierung von IT- und OT-Systemen sowie strenge Zugriffsrechte in kritischen Infrastrukturen sind. Zusätzlich können automatisierte Backup- und Wiederherstellungsprozesse sowie regelmäßige Sicherheitsaudits helfen, Datenverluste zu begrenzen und die Resilienz gegenüber Cyberangriffen zu erhöhen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10937-chaos.png

**Was lernen wir daraus:**
Der Fall zeigt, dass auch regionale Versorger mit hohem Sicherheitsbewusstsein Ziel komplexer Cyberangriffe werden können. Kritische Infrastrukturen benötigen nicht nur technische Schutzmaßnahmen, sondern auch gut trainierte Prozesse für Reaktion und Wiederanlauf. Prävention, Netzwerksegmentierung und automatisierte Reaktionssysteme sind entscheidend, um Auswirkungen von Angriffen zu minimieren und den Betrieb aufrechtzuerhalten.

RIEDEL

# Ransomware-Angriff auf Ingenieurbüro: 140 GB vertrauliche Daten betroffen

28. Oktober 2025, in Wendelstein/Bayern

RANSOMWARE

DATENDIEBSTAHL

DATENHEHLEREI

**Was ist passiert?**
Ende Oktober 2025 wurde ein Ingenieur- und Planungsbüro von der Ransomware-Gruppe **Brotherhood** als Opfer gelistet. Die Angreifer behaupteten, rund **140 GB** vertraulicher Daten erbeutet zu haben, darunter Finanzbudgets, technische Pläne und Verträge mit Großkunden. Zur Bekräftigung veröffentlichten sie Screenshots angeblich kompromittierter Dateien.

**Was hätte man besser machen können?**
Durch eine kontinuierliche Überwachung sensibler Systeme, eine strikte Segmentierung kritischer Datenbereiche sowie klar definierte Prozesse zur schnellen Erkennung und Reaktion auf ungewöhnliche Aktivitäten hätten die Auswirkungen des Vorfalls möglicherweise reduziert werden können. Unterstützend hätten ein **SOC** und ein **Vulnerability Assessment** zur frühzeitigen Erkennung beigetragen.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/11200-Brotherhood-Ingenieur.png

**Was lernen wir daraus:**
Durch eine konsequente Verschlüsselung vertraulicher Projekt- und Kundendaten, regelmäßige Backups sowie eine strikte Zugriffskontrolle für kritische Dokumente hätte das Risiko eines umfassenden Datenabflusses deutlich reduziert werden können. Ergänzend hätten vorbereitete Kommunikations- und Wiederanlaufpläne die Reaktionszeit verkürzt und Folgeschäden minimiert.

RIEDEL

# Ransomware-Angriff auf Onlinehandel für Motorsportzubehör

27. Oktober 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

ERPRESSUNG

**Was ist passiert?**
Ein deutscher Onlinehändler für Motorsportzubehör wurde Ziel der Ransomware-Gruppe **Everest**. Die Angreifer setzten dem Unternehmen zudem eine Frist. Andernfalls drohten sie, **106.872 Datensätze**, darunter personenbezogene Informationen, zu veröffentlichen.

**Was hätte man besser machen können?**
Der Angriff zeigt die Risiken unzureichend geschützter Kundendaten. Sinnvoll sind Maßnahmen wie **Endpunktüberwachung (EDR/XDR)** zur Erkennung verdächtiger Aktivitäten und ein **SIEM-System** zur zentralen Analyse von Sicherheitsereignissen. Ergänzend helfen regelmäßige **Vulnerability Assessments**, um Schwachstellen in der IT-Infrastruktur zu identifizieren und gezielt zu beheben.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10946-everest.png
https://www.security-incidents.de/assets/img/incidents/10946-everest-02.png

**Was lernen wir daraus:**
Der Fall verdeutlicht, wie stark Onlinehändler von Ransomware bedroht sind, insbesondere wenn große Mengen sensibler Daten verarbeitet werden. Präventive Maßnahmen wie kontinuierliche Überwachung, automatisierte Abwehrmechanismen und regelmäßige Schwachstellenanalysen sind entscheidend, um Angriffe frühzeitig zu erkennen, Datenverluste zu minimieren und Vertrauen bei Kunden zu erhalten.

RIEDEL

# Cyberangriff auf regionalen Energieversorger

24. Oktober 2025, in Clausthal-Zellerfeld/Niedersachsen

EINBRUCH

AUSFALL

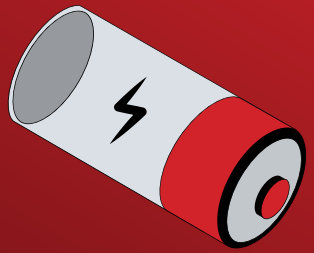
**Was ist passiert?**
Ein regionaler Energie- und Wasserversorger wurde Ziel eines Cyberangriffs durch die Gruppe **Safepay**. Der Angriff führte zu erheblichen Störungen in der internen Kommunikation, während die Versorgung der Bevölkerung laut Unternehmen stabil blieb. Nach Entdeckung des Vorfalls wurden die IT-Systeme sofort isoliert und die zuständigen Behörden informiert. Ob Daten entwendet wurden, blieb unklar.

**Was hätte man besser machen können?**
Der Vorfall verdeutlicht, wie entscheidend segmentierte IT-Netzwerke und klare Notfallpläne für den Schutz kritischer Infrastrukturen sind. Durch konsequente Netzwerksegmentierung, eine automatisierte Security-Orchestration and Response (SOAR), lassen sich Angriffswege frühzeitig erkennen und gezielt blockieren. Auch die schnelle Wiederherstellung betroffener Systeme hätte so besser unterstützt werden können.

## Anzunehmende Schadensfelder:

Quellen:
https://www.tagesschau.de/inland/regional/niedersachsen/hackerattacke-trifft-stadtwerke-clausthal-zellerfeld,hackerangriff-130.html
https://www.ndr.de/nachrichten/niedersachsen/braunschweig_harz_goettingen/hackerattacke-trifft-stadtwerke-clausthal-zellerfeld,hackerangriff-130.html

**Was lernen wir daraus:**
Der Vorfall zeigt, dass selbst regionale Versorger mit hohem Sicherheitsniveau ins Visier professioneller Gruppen geraten können. Als **NIS2-kritische** Infrastruktur müssen Energie- und Wasserversorger nicht nur technisch gut geschützt sein, sondern auch über eingeübte Reaktions- und Wiederanlaufprozesse verfügen. Prävention, Netzwerksegmentierung und automatisierte Erkennungssysteme sind entscheidend, um Angriffe früh zu stoppen und die Versorgung der Bevölkerung jederzeit sicherzustellen.



RIEDEL

# Ransomware-Angriff auf Sicherheitstechnik-Distributor

24. Oktober 2025, in Frankfurt am Main/Hessen

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Am 24. Oktober 2025 wurde ein führender Distributor für Sicherheitstechnik zum Opfer der Ransomware-Gruppe **Safepay**. Die Angreifer veröffentlichten das Unternehmen auf ihrem Opferblog und setzten eine Frist, um auf ihre Forderungen einzugehen. Es wird angenommen, dass sensible Unternehmensdaten kompromittiert wurden.

**Was hätte man besser machen können?**
Ein **Security Operations Center (SOC)** zur kontinuierlichen Überwachung und Analyse sicherheitsrelevanter Ereignisse sowie **XDR/EDR-Lösungen** zur schnellen Erkennung und Eindämmung von Bedrohungen hätten den Angriff möglicherweise verhindert. Ergänzend hätte ein regelmäßiges **Vulnerability Assessment**, das Risiko deutlich reduziert.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10926-Safepay.png

**Was lernen wir daraus:**
Der Fall zeigt, dass selbst Unternehmen in der Sicherheitsbranche nicht vor Cyberangriffen gefeit sind. Eine ganzheitliche IT-Sicherheitsstrategie, die Prävention, Überwachung und Reaktion kombiniert, ist entscheidend. Moderne Ransomware-Gruppen agieren professionell, daher sind kontinuierliches Monitoring, regelmäßige Schwachstellenanalysen und automatisierte Abwehrprozesse unerlässlich, um Angriffe frühzeitig zu erkennen und Schäden zu minimieren.

RIEDEL

# Beast-Ransomware attackiert Unternehmensberater

24. Oktober 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Ein deutscher Unternehmensberater wurde am 24. Oktober von der Ransomware-Gruppe **Beast** auf deren Leak-Portal gelistet. Die Angreifer behaupteten, **400 GB** vertrauliche Daten erbeutet zu haben und veröffentlichten Screenshots als Beweis.

**Was hätte man besser machen können?**
Der Vorfall verdeutlicht, wie wichtig es ist, sensible Daten nicht nur zu speichern, sondern aktiv zu schützen. Regelmäßige IT-Musterungen zur **Schwachstellenanalyse** und ein **Security Operations Center (SOC)** für schnelle Reaktionen hätten das Risiko deutlich reduziert.

**Was lernen wir daraus:**
Cyberkriminelle setzen zunehmend auf die Veröffentlichung vertraulicher Daten als Druckmittel. Unternehmen müssen den Schutz sensibler Informationen als strategische Priorität betrachten, nicht nur aus technischer Sicht, sondern auch durch klare Prozesse und Schulungen für Mitarbeitende.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10947-beast.png
https://www.security-incidents.de/assets/img/incidents/10947-beast-02.png

RIEDEL

# Cyber-Erpressung: Bauunternehmen im Visier von Nova

20. Oktober 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**

Ein deutsches Bauunternehmen wurde Opfer der Ransomware-Gruppe **Nova**. Die Angreifer behaupteten, **350 GB** vertrauliche Daten erbeutet zu haben und drohten mit Veröffentlichung am 31. Oktober, falls keine Zahlung erfolgte. Das Unternehmen war am 20. Oktober auf dem Darknet-Portal der Gruppe gelistet.

**Was hätte man besser machen können?**

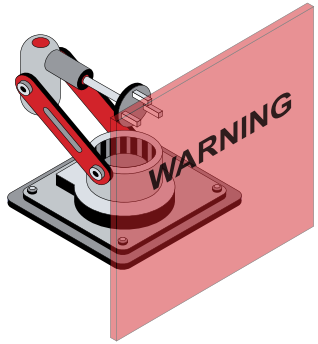
Der Angriff macht deutlich, wie entscheidend eine mehrschichtige Sicherheitsstrategie ist. Neben klassischem Perimeterschutz hätten Maßnahmen wie regelmäßige **Schwachstellenscans**, **Security Orchestration & Automation (SOAR)** und **Extended Detection & Response (XDR)** dazu beitragen können, verdächtige Aktivitäten frühzeitig zu erkennen und automatisiert einzudämmen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10908-Nova.png

**Was lernen wir daraus:**

Cyberangriffe wie dieser zeigen, dass Daten nicht nur ein wertvolles Gut, sondern auch ein Hebel für Erpressung sind. Die Veröffentlichung großer Datenmengen kann Unternehmen langfristig schaden, nicht nur finanziell, sondern auch strategisch. Entscheidend ist, dass Organisationen den Faktor „Datenintegrität“ als Teil ihrer Risikostrategie verstehen und Sicherheitsbewusstsein in allen Ebenen verankern.




RIEDEL

# Lynx-Ransomware trifft deutschen Anlagenbauer

RANSOMWARE

20. Oktober 2025, in Bremen/Bremen

**Was ist passiert?**
Ein Unternehmen für Industrie- und Schiffsbrenntechnik wurde Opfer der Ransomware-Gruppe **Lynx**. Die Angreifer veröffentlichten den Vorfall am 20. Oktober auf ihrem Leak-Portal. Details zur erbeuteten Datenmenge sind nicht bekannt.

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

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10907-Lynx.png

**Was lernen wir daraus:**
Cybersecurity muss heute proaktiv und ganzheitlich gedacht werden. Unternehmen brauchen nicht nur Schutzmechanismen, sondern auch Systeme, die Bedrohungen erkennen, bewerten und automatisiert darauf reagieren. Der Vorfall zeigt: Wer auf Prävention und schnelle Reaktion setzt, schützt nicht nur Daten, sondern auch Vertrauen, Produktivität und Zukunftsfähigkeit.

RIEDEL

# Ransomware-Angriff legt IT eines deutschen Metallverarbeiters lahm

20. Oktober 2025, in Aue-Bad Schlema/Sachsen

RANSOMWARE

AUSFALL

ERPRESSUNG

**Was ist passiert?**
Ein deutsches Unternehmen aus der Metallverarbeitung wurde am 20. Oktober Opfer eines Ransomware-Angriffs. Die interne IT war gestört, die Wiederherstellung lief an. Nach Angaben des Unternehmens wurde ein russisches Hacker-Kollektiv vermutet. Ein Lösegeld wurde nicht gezahlt. Die Ermittlungen waren zum Zeitpunkt der Meldung noch im Gange.

**Was hätte man besser machen können?**
Der Vorfall zeigt, wie wichtig es ist, Sicherheitslücken frühzeitig zu identifizieren, gerade in produktionsnahen IT-Strukturen. Ein regelmäßiger **Vulnerability Assessment** hätte potenzielle Einfallstore aufdecken können, bevor Angreifer sie ausnutzen. Ergänzend sorgt ein aktives **Security Operations Center (SOC)** für schnelle Reaktion im Ernstfall.

**Anzunehmende Schadensfelder:**

Quellen:
https://nha-aue.de/de/news/cyberangriff
https://www.mdr.de/nachrichten/sachsen/chemnitz/annaberg-aue-schwarzenberg/hacker-angriff-nickelhuette-lka-100.html

**Was lernen wir daraus:**
Ransomware-Angriffe treffen längst nicht mehr nur große Konzerne. Auch mittelständische Industrieunternehmen sind zunehmend Ziel professioneller Hackergruppen. Eine moderne Sicherheitsarchitektur mit Echtzeit-Erkennung, automatisierter Reaktion und kontinuierlicher Schwachstellenanalyse ist heute unverzichtbar.


RIEDEL

# Ransomware-Angriff legt IT einer deutschen Gemeindeverwaltung lahm

20. Oktober 2025, in Untereisesheim/Baden-Württemberg

RANSOMWARE

AUSFALL

**Was ist passiert?**
Am 20. Oktober 2025 wurde die IT einer Gemeindeverwaltung durch Ransomware lahmgelegt. Nur die Telefone blieben funktionsfähig. Die Täter forderten Lösegeld, nähere Angaben zu Schaden und Urhebern sind blieben unklar. Die Wiederherstellung begann am 29. Oktober mit Unterstützung von Landeskriminalamt und Cybersicherheitsagentur. Zentrale Dienste waren rund eine Woche eingeschränkt.

**Was hätte man besser machen können?**
Ein besserer Schutz kritischer Verwaltungsdienste könnte durch kontinuierliches Sicherheitsmonitoring **SOC**, regelmäßige **IT-Musterung** zur Erkennung von Schwachstellen und gezielten **Endpoint-Schutz EDR** unterstützt werden, um Risiken von Betriebsunterbrechungen und Datenverlust zu verringern.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.nokzeit.de/2025/10/20/cyberangriff-legt-gemeindeverwaltung-lahm/
https://www.swr.de/swraktuell/baden-wuerttemberg/heilbronn/cyber-angriff-legt-gemeindeverwaltung-untereisesheim-lahm-100.html

**Was lernen wir daraus:**
Ransomware kann selbst kleine Verwaltungen über Tage lahmlegen. Schnelle Reaktion, externe Unterstützung und transparente Kommunikation sind entscheidend, um Auswirkungen zu begrenzen. Gleichzeitig zeigt der Vorfall, wie wichtig kontinuierliche Sicherheitskontrollen und Notfallpläne sind, um kritische Dienste verfügbar zu halten.


RIEDEL

# Cyber-Erpressung im Maschinenbau: Datenverkauf für 10 BTC angekündigt

17. Oktober 2025, in Deutschland

RANSOMWARE

ERPRESSUNG

DATENHEHLEREI

**Was ist passiert?**

Ein deutscher Hersteller von Antriebstechnik wurde von der Ransomware-Gruppe **Rhysida** auf einer Leaksite gelistet. Die Angreifer bieten angeblich erbeutete Daten in einer Darknet-Auktion für **10 BTC** an. Als Beweis wurden Screenshots veröffentlicht.

**Was hätte man besser machen können?**

Der Vorfall zeigt, wie wichtig eine ganzheitliche Sicherheitsstrategie ist. Gerade Industrieunternehmen mit sensiblen Entwicklungsdaten profitieren von präventiven Maßnahmen. Lösungen wie **RIEDEL Enterprise Defense [R.E.D.]**, regelmäßige **Vulnerability Assessments** und moderne EDR-Systeme können helfen, Schwachstellen frühzeitig zu erkennen und verdächtige Aktivitäten schneller sichtbar zu machen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10860-rhysida.png

**Was lernen wir daraus:**

Ransomware-Gruppen wie Rhysida setzen gezielt auf Druck durch Datenveröffentlichung, um Unternehmen zur Zahlung zu bewegen. Der Schutz muss daher über klassische IT-Sicherheit hinausgehen: Ein aktives Security Operations Center (SOC), ein leistungsfähiges SIEM-System sowie automatisierte Reaktionsmechanismen (SOAR) sind heute essenzielle Bestandteile einer modernen Sicherheitsarchitektur.

RIEDEL

# Cyberangriff auf Maschinenbauer – Ransomware-Gruppe veröffentlicht Vorfall

17. Oktober 2025, in Bayern

RANSOMWARE

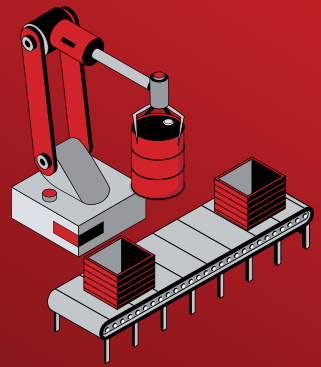
**Was ist passiert?**
Ein bayerischer Maschinen- und Anlagenbauer wurde von der Ransomware-Gruppe **Ransomhouse** auf deren Opferblog gelistet. Die Angreifer behaupten, einen erfolgreichen Angriff durchgeführt zu haben. Weder Details zu den kompromittierten Daten noch zur Reaktion des Unternehmens sind bekannt.

**Was hätte man besser machen können?**
Gerade Unternehmen mit sensiblen Konstruktions- und Produktionsdaten sollten ihre Sicherheitsstrategie auf Prävention und schnelle Reaktion ausrichten. Ein **Security Operations Center (SOC)** hätte verdächtige Aktivitäten rund um die Uhr überwacht und sofort Alarm ausgelöst. Ergänzend wären Awareness-Schulungen für Mitarbeitende wichtig gewesen, um das Risiko durch Phishing oder unsichere Zugriffe zu reduzieren.

## Anzunehmende Schadensfelder:

Quellen:
https://www.moz.de/nachrichten/panorama/paypal-down-aktuelle-stoerung-zehntausende-melden-probleme-78384251.html
https://www.focus.de/panorama/40-000-nutzer-meldeten-probleme-massive-stoerung-bei-paypal_c82ba358-123a-428f-b2b1-0819fc5e905b.html

**Was lernen wir daraus:**
Der Vorfall verdeutlicht, wie entscheidend eine ganzheitliche Sicherheitsstrategie ist. Neben technischen Maßnahmen wie Überwachung und Angriffserkennung müssen regelmäßige Schwachstellenanalysen sowie klar definierte Incident-Response-Prozesse etabliert werden, um im Ernstfall schnell und effektiv reagieren zu können.



RIEDEL

# Ransomware-Angriff auf deutsches Beratungsunternehmen

17. Oktober 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

DATENLECK

**Was ist passiert?**
Ein deutsches Beratungs- und Marktforschungsunternehmen wurde von der Ransomware-Gruppe **Sinobi** auf deren Leaksite gelistet. Die Angreifer veröffentlichten rund **20 GB** vertrauliche Unternehmensdaten, die offenbar aus dem internen Netzwerk stammen. Angaben zur Reaktion des Unternehmens oder zu den betroffenen Daten lagen nicht vor.

**Was hätte man besser machen können?**
Ein **Security Operations Center (SOC)** hätte verdächtige Aktivitäten rund um die Uhr überwacht und sofort Alarm ausgelöst. Ergänzend wäre ein **Extended Detection & Response (XDR)-System** sinnvoll gewesen, um Angriffe über Endpunkte, Netzwerk und Cloud hinweg zu erkennen und automatisiert einzudämmen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10876-Sinobi.png

**Was lernen wir daraus:**
Beratungs- und Marktforschungsunternehmen verwalten hochsensible Daten und sind damit ein attraktives Ziel für Ransomware-Gruppen. Der Vorfall zeigt, wie wichtig es ist, nicht nur technische Schutzmaßnahmen wie SOC und XDR einzusetzen, sondern auch klare Prozesse für Incident Response und Datenklassifizierung zu etablieren.

RIEDEL

# Login-Störung bei Zahlungsdienstleister betrifft Millionen Nutzer

16. Oktober 2025, in Deutschland

AUSFALL

**Was ist passiert?**
Den deutschen Kunden eines bekannten Zahlungsdienstleisters war es am Nachmittag bzw. frühen Abend nicht möglich, sich in ihr Konto einzuloggen. Gegen 16:50 Uhr häuften sich die Meldungen auf einem Störungsportal auf bis zu **40.000. Berichten** zufolge waren sogar **Millionen Nutzer** betroffen. Am Abend wurde die Störung behoben. Genauere Informationen sind nicht bekannt.

**Was hätte man besser machen können?**
Eine hochverfügbare Infrastruktur mit Lastverteilung, Redundanzen und automatisierter Fehlererkennung ist essenziell für digitale Zahlungsdienste. Unser **Security Operations Center (SOC)** überwacht Systeme rund um die Uhr, erkennt kritische Ausfälle frühzeitig und unterstützt bei der schnellen, koordinierten Wiederherstellung.

## Anzunehmende Schadensfelder:

Quellen:
https://www.moz.de/nachrichten/panorama/paypal-down-aktuelle-stoerung-zehntausende-melden-probleme-78384251.html
https://www.focus.de/panorama/40-000-nutzer-meldeten-probleme-massive-stoerung-bei-paypal_c82ba358-123a-428f-b2b1-0819fc5e905b.html

**Was lernen wir daraus:**
Auch temporäre Ausfälle können massive Auswirkungen haben, besonders bei Diensten mit Millionen Nutzern. Cyber-Resilienz bedeutet nicht nur Schutz vor Angriffen, sondern auch die Fähigkeit, auf technische Störungen schnell und strukturiert zu reagieren. Unternehmen sollten ihre IT-Infrastruktur regelmäßig prüfen, überwachen und auf Notfälle vorbereitet sein – denn Vertrauen ist ein Wettbewerbsvorteil, der schnell verloren gehen kann.


RIEDEL

# Cyberkriminelle listen Marktforschungsinstitut auf Leaksite

15. Oktober 2025, in Nordrhein-Westfalen

RANSOMWARE

DATENDIEBSTAHL

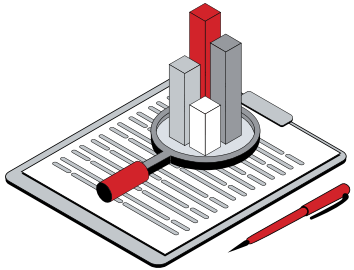
**Was ist passiert?**
Am 15. Oktober wurde ein deutsches Marktforschungsinstitut auf einer Leaksite von **Qilin** gelistet. Die Gruppierung behauptet, Daten erbeutet zu haben, Details dazu sollten folgen. Das betroffene Unternehmen hat sich nicht öffentlich geäußert, die Echtheit und der Umfang des Vorfalls sind unklar.

**Was hätte man besser machen können?**
Der Angriff hätte durch ein Managed-SIEM und ein rund um die Uhr besetztes SOC früher erkannt und begrenzt werden können. Auch die aktive Überwachung von Leaksites hätte dem Institut ermöglicht, schneller auf die Veröffentlichung möglicher Daten zu reagieren und gezielte Gegenmaßnahmen einzuleiten.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10847-qilin.png

**Was lernen wir daraus:**
Marktforschungsinstitute verwalten sensible Daten aus Studien, Kundenprojekten und Befragungen. Ein unerkannter Angriff kann nicht nur personenbezogene Informationen gefährden, sondern auch das Vertrauen in die Ergebnisse. Nur mit kontinuierlicher Überwachung, klaren Zugriffsregeln und sicherer Datenhaltung lässt sich die Integrität solcher Daten langfristig schützen.



RIEDEL

# Cybervorfall bei Logistikdienstleister: Unternehmen im Darknet gelistet

RANSOMWARE

14. Oktober 2025, in Bayern

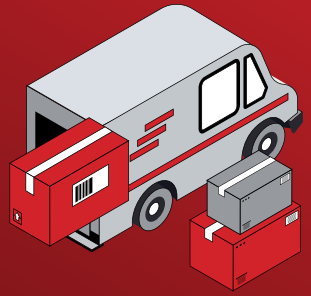
**Was ist passiert?**
Im Oktober 2025 listete die Ransomware-Gruppe **Coinbasecartel** ein deutsches Logistikunternehmen auf deren Darknet-Blog auf. Ob Daten abgeflossen sind oder welche Systeme betroffen waren, ist nicht bekannt. Eine offizielle Stellungnahme lag nicht vor.

**Was hätte man besser machen können?**
Eine kontinuierliche Überwachung durch ein **Security Operations Center (SOC)** hätte verdächtige Aktivitäten frühzeitig erkannt und eine schnelle Reaktion ermöglicht. So lassen sich Ransomware-Angriffe oft in der Entstehung stoppen, bevor sie kritische Systeme lahmlegen oder Daten verschlüsseln.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10840-Coinbasecartel.png

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



RIEDEL

# Cyberangriff mit Beleg: Hacker legen Dateistruktur offen

14. Oktober 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Ein Steuerbüro wurde von der Ransomware-Gruppe **Qilin** auf deren Leaksite gelistet. Die genaue erbeutete Datenmenge sowie der Umfang des Angriffs sind nicht bekannt. Das Unternehmen hat sich nicht öffentlich zum Vorfall geäußert.

**Was hätte man besser machen können?**
Eine strikte Zugriffskontrolle, verschlüsselte Datenhaltung und ein getesteter Notfallplan hätten die Auswirkungen begrenzen können. Unsere **Security Orchestration & Response** hilft, im Ernstfall schnell und koordiniert zu reagieren.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10845-qilin.png

**Was lernen wir daraus:**
Steuerberater verwalten hochsensible Daten und sind damit attraktive Ziele für Ransomware. Wer vertrauliche Informationen schützt, braucht mehr als Antivirensoftware: Echtzeitüberwachung, Verschlüsselung und klare Reaktionsprozesse sind essenziell.

RIEDEL

# Softwareanbieter unter Druck: Erpresser setzen Frist zur Reaktion

13. Oktober 2025, in Karlsruhe/Baden-Württemberg

RANSOMWARE

**Was ist passiert?**
Ein Anbieter von Business-Software wurde am 13. Oktober von der Ransomware-Gruppe **Coinbasecartel** auf deren Opferseite gelistet. Über Art und Umfang des Angriffs ist bislang nichts bekannt. Ob Daten abgeflossen sind oder Systeme betroffen waren, blieb unklar, das Unternehmen hat sich nicht öffentlich zum Vorfall geäußert.

**Was hätte man besser machen können?**
Der Angriff hätte besser eingedämmt werden können, wenn sensible Bereiche der IT-Infrastruktur durch **Netzwerksegmentierung** geschützt gewesen wären. Eine kontinuierliche Überwachung durch ein **SOC** hätte verdächtige Aktivitäten frühzeitig erkannt und eine schnelle Reaktion ermöglicht.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10839-Coinbasecartel.png

**Was lernen wir daraus:**
Cyberangriffe bleiben oft lange unbemerkt und gefährden sensible Daten im Hintergrund. Das zeigt, wie wichtig nicht nur die Verfügbarkeit, sondern auch Datenschutz und kontinuierliche Überwachung sind. Nur mit ganzheitlicher Sicht auf die IT-Sicherheit lassen sich versteckte Risiken frühzeitig erkennen und größere Schäden vermeiden.

RIEDEL

# IT-Sicherheitsvorfall bei Verkehrstechnik-Spezialisten: Entwicklungsbereich betroffen

11. Oktober 2025, in München/Bayern

EINBRUCH

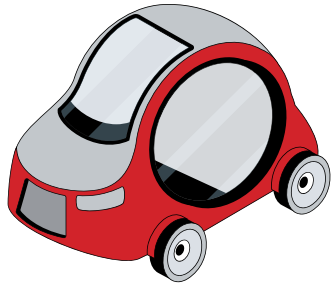
**Was ist passiert?**
Ein Münchener Verkehrstechnik-Spezialist meldete einen IT-Sicherheitsvorfall. Angreifer waren in interne Systeme eingedrungen, betroffen war die Entwicklungsabteilung. Der Kundenbetrieb blieb laut Unternehmen uneingeschränkt. Die Systeme wurden umgehend abgesichert, und es liefen Untersuchungen zu einem möglichen Datendiebstahl.

**Was hätte man besser machen können?**
Durch eine kontinuierliche Überwachung sensibler Entwicklungsumgebungen, eine strikte Segmentierung kritischer Systeme sowie klar definierte Prozesse zur schnellen Erkennung und Reaktion auf ungewöhnliche Aktivitäten hätten die Auswirkungen des Vorfalls möglicherweise reduziert werden können. Unterstützend hätten ein **Security Operations Center (SOC)** und ein **SIEM** zur frühzeitigen Erkennung beigetragen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/11083-Yunex.png

**Was lernen wir daraus:**
Regelmäßige Sicherheitsprüfungen, abgestimmte Notfallpläne und eine transparente interne Kommunikation hätten dazu beitragen können, Risiken schneller einzugrenzen und die Analyse effizienter zu gestalten.



RIEDEL

# Vakuum-Spezialist wurde zum Ziel eines Ransomware-Angriffs

RANSOMWARE

10. Oktober 2025, in Deutschland

**Was ist passiert?**
Ein deutscher Vakuum-Spezialist wurde am 10. Oktober auf dem Opferblog der Ransomware-Gruppe **Safepay** gelistet. Die Angreifer setzten dem Unternehmen eine Frist bis zum 13. Oktober, um auf ihre Forderungen zu reagieren. Details zur Art des Angriffs oder zu betroffenen Daten wurden nicht veröffentlicht.

**Was hätte man besser machen können?**
Zur Abwehr gezielter Ransomware-Angriffe braucht es mehr als Basis-IT-Schutz. **SIEM-Systeme** zur zentralen Überwachung, **EDR** zur schnellen Bedrohungserkennung und **regelmäßige Schwachstellenanalysen** schließen Einfallstore. Eine starke Datenverschlüsselung reduziert zusätzlich die Verwertbarkeit erbeuteter Informationen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10826-Safepay.png

**Was lernen wir daraus:**
Gezielte Ransomware-Angriffe treffen längst nicht mehr nur große Konzerne, sondern auch mittelständische Industriebetriebe. Wer sensible Daten speichert, muss in moderne Sicherheitsmaßnahmen investieren.

RIEDEL

# Ransomware-Gruppe veröffentlicht Hotel-Daten im Netz

08. Oktober 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

DATENLECK

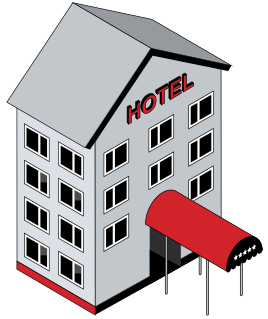
**Was ist passiert?**
Am 8. Oktober veröffentlichte die Gruppe **DragonForce** einen **12,73-GB-Datensatz**, der angeblich aus den Systemen eines deutschen Hotels stammen soll. Die Daten sind öffentlich einsehbar. Eine Bestätigung des betroffenen Unternehmens sowie Details zum tatsächlichen Umfang oder zur Echtheit liegen nicht vor.

**Was hätte man besser machen können?**
Ein mehrschichtiges Sicherheitskonzept mit EDR, Datenverschlüsselung und einer segmentierten Netzwerkstruktur hätte die Ausbreitung des Angriffs sowie den Abfluss sensibler Daten deutlich erschweren können. **Unsere Endpoint Detection & Response und Security Automation** unterstützen dabei, Angriffe frühzeitig zu erkennen, Risiken zu bewerten und schnell sowie gezielt Gegenmaßnahmen einzuleiten.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10786-dragonforce.png

**Was lernen wir daraus:**
Hotels verarbeiten täglich hochsensible Daten. Ohne moderne Schutzmechanismen wie EDR und automatisierte Reaktionsprozesse sind sie leichte Ziele für Ransomware-Gruppen. Prävention und schnelle Reaktion sind entscheidend, um Schaden zu begrenzen.




RIEDEL

# Sicherheitslücke in Hotelplattform: Buchungsdaten über Jahre einsehbar

08. Oktober 2025, in Schiffweiler/Saarland

DATENLECK

SICHERHEITSLÜCKE

**Was ist passiert?**
Sicherheitsforscher entdeckten gravierende Schwachstellen in einer deutschen Hotelbuchungsplattform. Über einfache Abfragen und SQL-Injektionen waren teils jahrzehntealte Reservierungsdaten samt personenbezogener Informationen frei zugänglich. Die Lücken wurden nach Meldung innerhalb weniger Wochen geschlossen.

**Was hätte man besser machen können?**
Solche Schwachstellen lassen sich durch regelmäßige Penetrationstests, sichere API-Architekturen und ein strukturiertes Berechtigungsmanagement vermeiden. Unsere **IT-Musterung** deckt genau solche Risiken auf, bevor sie zum Vorfall werden.

**Anzunehmende Schadensfelder:**

Quellen:
https://zerforschung.org/posts/sihot/
https://www.tagesschau.de/investigativ/ndr-wdr/hotel-daten-sicherheitsluecken-software-100.html

**Was lernen wir daraus:**
Veraltete Systeme und ungesicherte Schnittstellen sind ein hohes Risiko – besonders im Tourismus. Wer Kundendaten verarbeitet, muss auf aktuelle Sicherheitsstandards setzen. Prävention ist Pflicht, nicht Kür.

RIEDEL

# IT-Störung legt Forschungsbetrieb zeitweise lahm

07. Oktober 2025, in Bremerhaven/Bremen

AUSFALL

**Was ist passiert?**
Eine deutsche Forschungseinrichtung war mehrere Tage nur eingeschränkt erreichbar. Telefon, E-Mail und zentrale Daten waren offline. Die Leitung reagierte vorsorglich mit Systemabschaltung und Prüfung durch Fachleute. Ein Hackerangriff wurde dementiert. Alle Systeme konnten noch in derselben Woche wiederhergestellt werden.

**Was hätte man besser machen können?**
Technische Ausfälle lassen sich durch isolierte Backup-Systeme, automatisierte Wiederanlaufprozesse und ein strukturiertes Incident Response Playbook deutlich besser bewältigen. Unsere Lösungen wie **IT-Musterung** und **Security Orchestration & Response** helfen, solche Szenarien frühzeitig zu erkennen und gezielt zu steuern.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.kreiszeitung-wesermarsch.de/region/bremerhaven-awi-it-stoerung-kein-hackerangriff-systeme-323422.html
https://www.nordsee-zeitung.de/bremerhaven/bremerhaven-awi-it-stoerung-kein-hackerangriff-systeme-323422.html#google_vignette

**Was lernen wir daraus:**
Forschungseinrichtungen sind auf stabile IT angewiesen. Selbst technische Störungen können den Betrieb massiv beeinträchtigen. Prävention, Resilienz und transparente Kommunikation sind essenziell, auch ohne Fremdeinwirkung.


RIEDEL

# Cyberangriff legt kommunale Verwaltung lahm: IT-Systeme abgeschaltet

07. Oktober 2025, in Hohen Neuendorf/Brandenburg

EINBRUCH

AUSFALL

**Was ist passiert?**
Eine kommunale Verwaltung wurde Opfer eines Cyberangriffs. Die IT-Systeme wurden vorsorglich abgeschaltet, wodurch digitale Dienstleistungen ausfielen. Die Verwaltung arbeitete vorübergehend analog, während IT-Forensiker und Ermittlungsbehörden den Vorfall untersuchen. Hinweise auf Datenabfluss lagen nicht vor.

**Was hätte man besser machen können?**
Der Vorfall zeigt, wie wichtig eine robuste Krisenvorbereitung ist. Eine klare Rollenverteilung im Ernstfall, regelmäßige Tests von Wiederanlaufplänen und isolierte Backup-Systeme hätten die Handlungsfähigkeit der Verwaltung sichern können, auch bei vollständigem Systemausfall.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.moz.de/lokales/oranienburg/cyber-angriff-in-hohen-neuendorf-rathaus-schaltet-nach-hacker-attacke-systeme-ab-78363528.html

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


RIEDEL

# Cyber-Erpressung im Luxussegment: Hacker drohen mit Datenveröffentlichung

06. Oktober 2025, in Deutschland

DATENDIEBSTAHL

DATENHEHLEREI

**Was ist passiert?**
Am 6. Oktober 2025 wurde eine deutsche Juwelierskette von der Hackergruppe **World Leaks** (ehemals „Hunters International“) ins Visier genommen. Die Angreifer behaupten, vertrauliche Unternehmensdaten erbeutet zu haben und setzen das Unternehmen unter Druck: Sollte keine Reaktion erfolgen, drohen sie mit der Veröffentlichung der Beute am 17. Oktober.

**Was hätte man besser machen können?**
Ein strukturiertes Sicherheitskonzept unterstützt dabei, Risiken frühzeitig zu erkennen und Auswirkungen zu begrenzen. Ein **SOC mit SIEM-Analyse** sowie regelmäßige **Vulnerability Assessments** können Schwachstellen schneller sichtbar machen.
**RIEDEL Enterprise Defense [R.E.D.]** bündelt diese Ansätze und stärkt so die Reaktionsfähigkeit.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10767-world-leaks.png

**Was lernen wir daraus:**
Auch Anbieter von Luxusgütern sind attraktive Ziele für Cyberkriminelle. Wer mit sensiblen Kundendaten arbeitet, muss in moderne Schutzmaßnahmen investieren – etwa in SIEM, EDR und Schwachstellenanalysen. Denn ein erfolgreicher Angriff gefährdet nicht nur Daten, sondern auch Vertrauen und Markenwert.

RIEDEL

# Doppelschlag durch Qilin – Elektrotechnik-Unternehmen und Kanzlei betroffen

04. Oktober 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Anfang Oktober 2025 listete die Ransomware-Gruppe **Qilin** sowohl ein deutsches Elektrotechnik-Unternehmen als auch eine Rechtsanwaltskanzlei auf ihrer Leaksite. Im ersten Fall sollen **28 GB** Daten entwendet worden sein, im zweiten wurden Screenshots als Beweis veröffentlicht. Die Gruppe erneuerte ihre Drohungen Mitte Oktober ohne weitere Details.

**Was hätte man besser machen können?**
Gezielte Angriffe wie die von Qilin zeigen, dass klassische Schutzmaßnahmen allein nicht ausreichen. Eine Kombination aus sauberem **Zugriffsmanagement**, klarer **Datenklassifizierung** und der Überwachung sensibler Bereiche durch ein **SOC** kann verdächtige Aktivitäten – etwa unautorisierte Zugriffe auf interne Dokumente – deutlich früher sichtbar machen und das Risiko ungewollter Veröffentlichungen spürbar reduzieren.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10771-qilin.png
https://www.security-incidents.de/assets/img/incidents/10769-qilin.png

**Was lernen wir daraus:**
Ransomware-Gruppen wie Qilin zielen gezielt auf Branchen mit besonders vertraulichen Informationen – von technischen Plänen bis hin zu juristischen Dokumenten. Wer solche Daten verarbeitet, muss nicht nur auf Schutz, sondern auch auf Transparenz setzen: Nur mit klarer Datenklassifizierung, Zugriffskontrolle und kontinuierlicher Überwachung lassen sich Angriffe rechtzeitig erkennen und sensible Inhalte schützen.

RIEDEL

# Chemieunternehmen im Visier von INC Ransom – 40 GB vertrauliche Daten betroffen

03. Oktober 2025, in Lemgo/Nordrhein-Westfalen

RANSOMWARE

DATENDIEBSTAHL

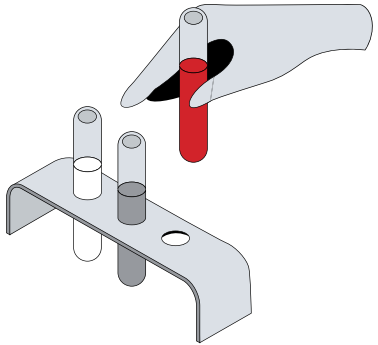
**Was ist passiert?**
Am 3. Oktober 2025 wurde ein deutsches Chemieunternehmen von der Ransomware-Gruppe **INC Ransom** auf deren Leaksite gelistet. Die Angreifer behaupteten, **40,39 GB** vertrauliche Unternehmensdaten entwendet zu haben. Details zur Art der Daten oder zur Reaktion des Unternehmens wurden nicht veröffentlicht.

**Was hätte man besser machen können?**
Der Abfluss großer Datenmengen zeigt, wie wichtig **Data-Loss-Prevention-Systeme** und ein strikt umgesetztes Rollen- und Rechtekonzept sind, um unbefugte Zugriffe deutlich zu erschweren. Ergänzend kann ein **SOC** mit Echtzeitüberwachung ungewöhnliche Datenbewegungen frühzeitig sichtbar machen und so das Risiko unkontrollierter Datenabflüsse reduzieren.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10753-INCRansom.png

**Was lernen wir daraus:**
Industrieunternehmen mit sensiblen Entwicklungsdaten sind ein attraktives Ziel für Ransomware-Gruppen. Wer seine Daten nicht nur speichert, sondern aktiv schützt – etwa durch DLP, Zugriffskontrollen und kontinuierliche Überwachung – kann das Risiko eines folgenschweren Datenlecks deutlich reduzieren.



RIEDEL

# Gezielter Datendiebstahl durch Social Engineering – Millionen Datensätze betroffen

03. Oktober 2025, in Herzogenaurach /Bayern

DATENDIEBSTAHL

SOCIAL ENGINEERING

VISHING

SUPPLY CHAIN

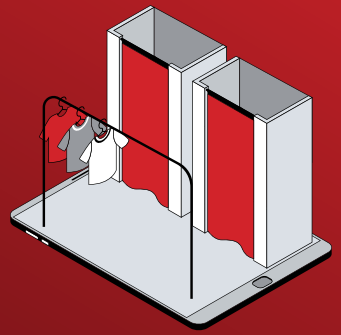
**Was ist passiert?**
Ein bekannter deutscher Sportartikelhersteller wurde von der Gruppe **Scattered Lapsus$ Hunters** angegriffen. Mittels **Social Engineering**, darunter **Vishing** und kompromittierte **OAuth-Zugänge**, verschafften sich die Täter Zugriff auf interne Systeme. Rund **3,1 GB** Daten mit über sechs Millionen sensiblen Datensätzen wurden entwendet. Eine Lösegeldfrist mit Veröffentlichungsdrohung wurde gesetzt.

**Was hätte man besser machen können?**
Durch die Kombination von **XDR und EDR** lassen sich verdächtige Aktivitäten frühzeitig erkennen und automatisiert an ein **Security Operations Center (SOC)** melden. Ein SOC überwacht alle Systeme rund um die Uhr und kann insbesondere bei Identitätsmissbrauch, etwa über kompromittierte OAuth-Zugänge, schnell reagieren. So lassen sich potenzielle Angriffe frühzeitig identifizieren und Gegenmaßnahmen zur Schadensbegrenzung einleiten.

## Anzunehmende Schadensfelder:

Quellen:
https://hackread.com/scattered-lapsus-hunters-salesforce-breach/
https://thecyberexpress.com/scattered-lapsus-hunters-salesforce-victims/

**Was lernen wir daraus:**
Angriffe über die Lieferkette und Social Engineering sind besonders heimtückisch, da sie oft außerhalb der direkten Kontrolle liegen. Unternehmen müssen nicht nur ihre eigenen Systeme absichern, sondern auch externe Zugänge und Identitäten überwachen. Lösungen wie XDR und SOAR, kombiniert mit klaren Zugriffsrichtlinien und Awareness-Trainings, sind entscheidend, um solche komplexen Angriffsmuster frühzeitig zu erkennen und abzuwehren.



RIEDEL

# September 2025

## SECURITY INCIDENTS GERMANY

RIEDEL

# Ransomware-Gruppe droht mit Datenveröffentlichung

RANSOMWARE

30. September 2025, in Deutschland

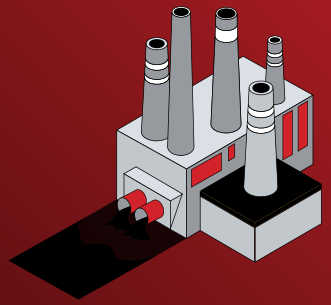
**Was ist passiert?**
Ein deutsches Metallunternehmen wurde von der Ransomware-Gruppierung **Ciphbit** auf deren Darknet-Leaksite als Opfer gelistet. Die Angreifer machten keine konkreten Angaben zur erbeuteten Datenmenge, drohten jedoch mit einer Veröffentlichung am 13. Oktober. Die Art und der Umfang der betroffenen Informationen sind unklar.

**Was hätte man besser machen können?**
Eine frühzeitige **IT-Musterung** hätten potenzielle Schwachstellen sichtbar gemacht. In Kombination mit strengen Zugriffsrechten und einer automatisierten Reaktionslösung wie **SOAR** wäre die unbemerkte Datenexfiltration deutlich erschwert worden

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10707-ciphbit.png

**Was lernen wir daraus:**
Die Drohung mit späterer Veröffentlichung zeigt: Angreifer setzen zunehmend auf psychologischen Druck. Unternehmen müssen nicht nur ihre Systeme absichern, sondern auch vorbereitet sein, schnell und strukturiert zu reagieren. Präventive Maßnahmen wie regelmäßige Schwachstellenanalysen und automatisierte Reaktionsprozesse sind dabei essenziell.



RIEDEL

# Ransomware-Gruppe veröffentlicht 187 GB – Medientechnik-Anbieter betroffen

30. September 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

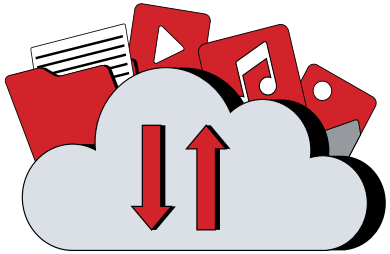
**Was ist passiert?**
Am 30. September 2025 wurde ein Anbieter von Medientechnik von der Ransomware-Gruppe **J** auf deren Darknet-Leaksite als Opfer gelistet. Die Angreifer behaupteten, **187 GB** an Daten erbeutet zu haben – darunter Kunden- und Zahlungsdaten, Mitarbeiterinformationen, Quellcode, Marketing-Assets und interne Berichte.

**Was hätte man besser machen können?**
Ein frühzeitiges **Vulnerability Assessment** kann dazu beitragen, sicherheitsrelevante Schwachstellen früher sichtbar zu machen. In Verbindung mit einer **SOAR-Lösung** lassen sich verdächtige Aktivitäten automatisiert erkennen und bewerten, was die Chancen erhöht, schwerwiegende Datenabflüsse frühzeitig zu begrenzen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10729-j.png
https://www.security-incidents.de/assets/img/incidents/10729-j-02.png

**Was lernen wir daraus:**
Technologieunternehmen sind besonders gefährdet, da sie oft große Mengen sensibler Daten und geistiges Eigentum verwalten. Wer Quellcode, Kundendaten und interne Assets nicht nur speichert, sondern aktiv schützt, etwa durch Zugriffskontrollen, Verschlüsselung und Echtzeitüberwachung, reduziert das Risiko eines folgenschweren Datenlecks erheblich.



RIEDEL

# Cyberangriff auf kommunale Verwaltung – IT-Systeme gestört

28. September 2025, in Glatten/Baden-Württemberg

AUSFALL

EINBRUCH

**Was ist passiert?**
Eine deutsche Gemeinde wurde Opfer eines Cyberangriffs. Die Angreifer verschickten ein Erpresserschreiben an die Verwaltung, und ein möglicher Diebstahl sensibler Daten konnte nicht ausgeschlossen werden. Die IT-Systeme und Kommunikationsmittel waren über mehrere Tage hinweg gestört, was die Erreichbarkeit der Verwaltung stark einschränkte.

**Was hätte man besser machen können?**
Eine stärkere Segmentierung von Netzwerken sowie restriktivere Zugriffsrechte können die Ausbreitung von Angriffen erschweren. Ergänzend kann eine kontinuierliche Überwachung, etwa durch ein Security Operations Center (SOC), sowie der Einsatz von Mehrfaktor-Authentifizierung dazu beitragen, verdächtige Aktivitäten früher zu erkennen und Auswirkungen auf zentrale Verwaltungsprozesse zu begrenzen.

## Anzunehmende Schadensfelder:

Quellen:
https://www.schwarzwaelder-bote.de/inhalt.cyber-angriff-in-glatten-hackergruppe-schickt-erpresserschreiben-ans-rathaus.ca0e0f93-24e9-49b2-810b-7728eba82081.html

**Was lernen wir daraus:**
Kommunale Einrichtungen sind zunehmend Ziel professioneller Angreifer. Ohne zentrale Sicherheitsüberwachung bleiben viele Vorfälle zu lange unentdeckt. Ein externes SOC kann hier entscheidend sein: Es erkennt Bedrohungen frühzeitig, reagiert automatisiert und schützt kritische Verwaltungsprozesse, bevor der Betrieb eingeschränkt wird.

RIEDEL

# Ransomware-Angriff auf kommunales Wohnungsunternehmen

26. September 2025, in Lüdenscheid/Nordrhein-Westfalen

RANSOMWARE

DATENDIEBSTAHL

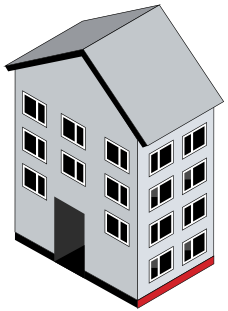
**Was ist passiert?**
Ein kommunales Wohnungsunternehmen wurde Opfer eines Ransomware-Angriffs durch **Dragonforce**. Unbekannte Täter verschlüsselten Daten, forderten Lösegeld und kompromittierten sensible Informationen. Das Unternehmen reagierte mit der Einrichtung eines Notfallzentrums und konnte den Geschäftsbetrieb aufrechterhalten, trotz zeitweiser Störungen bei Telefon- und E-Mail-Kommunikation.

**Was hätte man besser machen können?**
Die Einrichtung eines Notfallzentrums war wichtiger Schritt. Ein **SOC** in Kombination mit **SIEM** oder **XDR** hätte verdächtige Aktivitäten frühzeitig erkannt und automatisiert reagiert, so wären Kommunikationsausfälle bei Mail und Telefon vermutlich vermeidbar gewesen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10685-Dragonforce.png

**Was lernen wir daraus:**
Selbst gut vorbereitete IT-Teams stoßen bei plötzlichen Angriffen schnell an ihre Grenzen. Externe SOC-Lösungen mit Echtzeitüberwachung helfen, Bedrohungen frühzeitig zu erkennen und objektiv zu bewerten, bevor zentrale Prozesse wie Mail und Telefon gestört werden.



RIEDEL

# Werbeartikel-Anbieter im Visier von Ransomware-Gang

25. September 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

DATENLECK

**Was ist passiert?**
Ende September 2025 wurde ein deutscher Anbieter von Werbeartikeln von der Ransomware-Gruppe **Sarcoma** auf deren Darknet-Leaksite gelistet. Die Angreifer behaupteten, **285 GB** aus den Unternehmenssystemen entwendet zu haben, darunter auch Ausweiskopien – und stellten die Daten öffentlich zum Download bereit.

**Was hätte man besser machen können?**
Der Angriff zeigt, wie wichtig segmentierte Netzwerke, verschlüsselte Backups und Mehrfaktor-Authentifizierung sind, um unbefugte Zugriffe deutlich zu erschweren. Auch kontinuierliche Überwachung und klar **geregelte Zugriffsrechte** spielen eine zentrale Rolle, damit sensible Daten wie Kunden- oder Bankinformationen nicht unbemerkt abgeflossen wären.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10673-sarcoma.png

**Was lernen wir daraus:**
Ransomware-Gruppen setzen zunehmend auf Datenexfiltration statt reine Verschlüsselung. Der gezielte Diebstahl sensibler Informationen – wie Ausweiskopien oder Finanzdaten – erhöht den Druck auf Unternehmen massiv. Wer seine Daten nicht nur speichert, sondern auch schützt, etwa durch Zugriffskontrollen und Verschlüsselung, reduziert das Erpressungspotenzial deutlich.

RIEDEL

# Ransomware-Angriff auf kommunales Wohnungsunternehmen

25. September 2025, in Senftenberg/Brandenburg

RANSOMWARE

DATENDIEBSTAHL

AUSFALL

**Was ist passiert?**
Ein kommunales Wohnungsunternehmen wurde Opfer eines Ransomware-Angriffs. Unbekannte Täter verschlüsselten Daten, forderten Lösegeld und kompromittierten sensible Informationen. Das Unternehmen reagierte mit der Einrichtung eines Notfallzentrums und konnte den Geschäftsbetrieb aufrechterhalten, trotz zeitweiser Störungen bei Telefon- und E-Mail-Kommunikation.

**Was hätte man besser machen können?**
Die Einrichtung eines Notfallzentrums stellte einen wichtigen Schritt dar. Ein **SOC in Kombination mit SIEM oder XDR** hätte dazu beitragen können, verdächtige Aktivitäten früher sichtbar zu machen und Reaktionsprozesse zu unterstützen. Dadurch hätten sich Auswirkungen auf Kommunikationsdienste wie E-Mail oder Telefon möglicherweise begrenzen lassen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.lr-online.de/lausitz/senftenberg/hacker-in-senftenberg-kriminelle-erpressen-vermieter-kwg-nach-massivem-cyberangriff-78336325.html

**Was lernen wir daraus:**
Selbst gut vorbereitete IT-Teams stoßen bei plötzlichen Angriffen schnell an ihre Grenzen. Externe SOC-Lösungen mit Echtzeitüberwachung helfen, Bedrohungen frühzeitig zu erkennen und objektiv zu bewerten, bevor zentrale Prozesse wie Mail und Telefon gestört werden.

RIEDEL

# Ransomware-Angriff auf Maschinenbau-Tochter – Daten verschlüsselt, Systeme lahmgelegt

25. September 2025, in Krefeld/Nordrhein-Westfalen

RANSOMWARE

DATENDIEBSTAHL

EINBRUCH

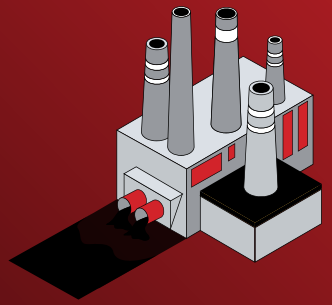
**Was ist passiert?**
Ein deutsches Tochterunternehmen eines japanischen Maschinenbaukonzerns wurde Opfer eines Ransomware-Angriffs. Unbekannte drangen in die Serverstruktur ein, verschlüsselten Daten und kompromittierten vermutlich auch vertrauliche Mitarbeiter- und Unternehmensinformationen. Die zuständigen Behörden wurden informiert und die Wiederherstellungsmaßnahmen eingeleitet.

**Was hätte man besser machen können?**
Ein **Security Operations Center (SOC)** hätte durch den kombinierten Einsatz von **XDR-Funktionen** und einer **SIEM-gestützten** Überwachung dazu beitragen können, auffällige Aktivitäten früher sichtbar zu machen und Reaktionsprozesse zu unterstützen. Eine solche Verzahnung kann die Analyse von Sicherheitsereignissen erleichtern und eine schnellere Einordnung von Angriffsmustern ermöglichen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.okuma.co.jp/english/news/2025/250925.php
https://www.security.land/okumas-german-subsidiary-hit-by-Ransomware-attack/

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



RIEDEL

# Produktionsausfall bei Lebensmittelhersteller: Cyberangriff stört Abläufe

AUSFALL

25. September 2025, in Mönchengladbach/Nordrhein-Westfalen

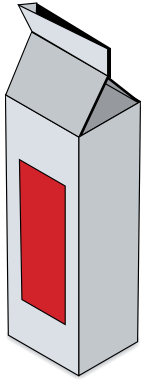
**Was ist passiert?**
Ein internationaler Getränkeproduzent wurde von einem Cyberangriff getroffen, der zentrale Produktionssysteme lahmlegte und die Logistik beeinträchtigte. Dadurch kam es zeitweise zu Verzögerungen im Warenfluss. Um die Auswirkungen für Kunden gering zu halten, wickelte das Unternehmen Bestellungen vorübergehend über alternative Kanäle wie E-Mail ab.

**Was hätte man besser machen können?**
In stark automatisierten Produktionsumgebungen ist die Verfügbarkeit digitaler Systeme geschäftskritisch. Eine robuste Sicherheits- und Netzwerkarchitektur mit kontinuierlicher Überwachung und einem aktiven **Security Operations Center (SOC)** hätte dazu beitragen können, sicherheitsrelevante Auffälligkeiten früher sichtbar zu machen und Auswirkungen gezielt zu begrenzen. Ein abgestimmter Notfallplan für Produktionsausfälle unterstützt zudem eine strukturierte Reaktion in solchen Szenarien.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.lebensmittelzeitung.net/tech-logistik/nachrichten/cybersecurity-refresco-kaempft-mit-hacker-attacke-186845

**Was lernen wir daraus:**
Wenn IT-Systeme in der Produktion ausfallen, steht nicht nur die Technik still – es gerät die gesamte Lieferkette ins Wanken. Der Vorfall zeigt, wie zentral digitale Prozesse heute für die Aufrechterhaltung des Tagesgeschäfts sind. IT muss deshalb nicht nur funktionieren, sondern auch widerstandsfähig gegenüber Angriffen sein. Resilienz entsteht nicht durch einzelne Tools, sondern durch ein Zusammenspiel aus Technik, Prozessen und klarer Verantwortlichkeit.



RIEDEL

# Technikunternehmen im Fokus von Ransomware-Gruppierung

23. September 2025, in Heinsdorfergrund/Sachsen

RANSOMWARE

DATENDIEBSTAHL

DATENLECK

**Was ist passiert?**
Ein deutsches Unternehmen aus der Heizungs- und Klimatechnikbranche wurde von der Ransomware-Gruppe **Sarcoma** auf deren Leakseite gelistet. Die Angreifer behaupten, **2,9 Terabyte** an Daten aus den Systemen des Unternehmens entwendet und veröffentlicht zu haben. Zur Untermauerung ihrer Angaben wurden mehrere Screenshots bereitgestellt.

**Was hätte man besser machen können?**
Ein **SOC mit integriertem SIEM** hätte dazu beitragen können, auffällige Muster früher sichtbar zu machen, insbesondere bei umfangreichen Datenbewegungen. In dieser Kombination wäre eine koordiniert abgestimmte Reaktion denkbar gewesen, um Auswirkungen eines möglichen Datenabflusses zu begrenzen und sicherheitsrelevante Ereignisse zeitnah einzuordnen.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10651-sarcoma.png
https://www.freiepresse.de/vogtland/reichenbach/vogtlaendisches-unternehmen-opfer-von-cyberangriff-wir-kaempfen-um-die-produktion-am-laufen-zu-halten-artikel13970410#google_vignette

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

RIEDEL

# Ransomware-Gruppe Akira erbeutet sensible Daten

23. September 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

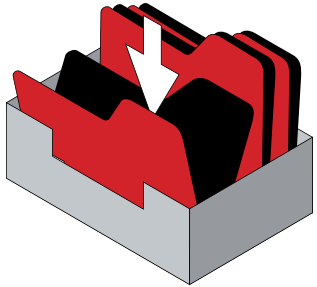
**Was ist passiert?**
Am 23. September 2025 tauchte ein deutscher Elektrogroßhändler auf dem Darknet-Blog der Ransomware-Gruppe **Akira** auf. Laut den Angreifern wurden umfangreiche Datenbestände kompromittiert, darunter persönliche Informationen von Mitarbeitenden (wie Ausweisdaten, Adressen und Kontaktdaten), Finanz- und Kundendaten sowie vertrauliche Vereinbarungen. Die Veröffentlichung sensibler Dokumente wurde durch Screenshots belegt.

**Was hätte man besser machen können?**
Ein kontinuierlich aktives Security Operations Center (SOC) hätte verdächtige Aktivitäten wie ungewöhnliche Zugriffe auf sensible Daten oder großvolumige Datenabflüsse frühzeitig erkennen können. Durch eine 24/7-Überwachung wäre eine schnelle Reaktion auf die Bedrohung möglich gewesen, noch bevor es zur Veröffentlichung der Daten kommt.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10654-Akira.png

**Was lernen wir daraus:**
IT-Sicherheit ist längst kein Spezialthema mehr – sie ist Grundvoraussetzung für den Geschäftsbetrieb. Wer Daten speichert, trägt Verantwortung. Gerade in Unternehmen mit komplexen IT-Strukturen und vielfältigen Schnittstellen braucht es klare Zuständigkeiten, aktuelle Systeme und ein Sicherheitskonzept, das mit dem Unternehmen mitwächst. Denn Angreifer nutzen nicht nur technische Schwächen, sondern auch organisatorische Lücken.



RIEDEL

# 2,8 Terabyte Datenleck bei Luftfahrt-Dienstleister: Ransomware-Gruppe schlägt zu

23. September 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Ein deutscher Privatflug-Dienstleister wurde auf der Darknet-Leakseite der Ransomware-Gruppe **J** gelistet. Die Täter behaupten, über **2,8 TB** sensible Daten erbeutet zu haben – darunter Patienteninformationen, Projektunterlagen, interne Dokumente, Personalakten und Berichte zu Gewaltvorfällen. Zur Untermauerung veröffentlichten sie Screenshots.

**Was hätte man besser machen können?**
Die Vielzahl sensibler Daten zeigt, wie wichtig konsequente **Datenklassifizierung und Zugriffskontrolle** sind. Besonders in sicherheitskritischen Bereichen wie der Luftfahrt müssen Systeme so aufgebaut sein, dass nicht alles zentral kompromittiert werden kann. Starke Verschlüsselung, Netzwerksegmentierung und regelmäßige Sicherheitschecks sind entscheidend, um massive Datenabflüsse zu verhindern.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10658-J.png

**Was lernen wir daraus:**
Wenn sensible Informationen aus unterschiedlichsten Bereichen, von Technik über Personal bis hin zu Gesundheitsdaten in einem Angriff kompromittiert werden, ist das ein klares Zeichen für fehlende Trennung und Schutzmechanismen in der IT-Infrastruktur. Unternehmen mit sicherheitsrelevanten Dienstleistungen müssen ihre IT nicht nur als Werkzeug, sondern als kritischen Schutzraum begreifen, mit klaren Regeln, starker Architektur und regelmäßiger Überprüfung.

RIEDEL

# Finanzdienstleister im Visier von Ransomware-Gruppe „Qilin“

RANSOMWARE

23. September 2025, in Deutschland

**Was ist passiert?**
Am 23. September 2025 wurde ein auf Autohäuser spezialisierter Buchhaltungs- und Controllingdienstleister von der Ransomware-Gruppe **Qilin** auf deren Darknet-Leakseite gelistet. Zum Umfang oder Inhalt der kompromittierten Daten machte die Gruppe keine Angaben.

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

**Anzunehmende Schadensfelder:**

Quellen:
https://www.dsgvo-portal.de/sicherheitsvorfaelle/ransomware_angriff_buchhaltung--und-controllingunternehmen-10661.php

**Was lernen wir daraus:**
Auch kleinere, spezialisierte Dienstleister geraten zunehmend ins Visier professioneller Ransomware-Gruppen. Gerade in datenintensiven Branchen wie Buchhaltung und Controlling ist eine stabile IT-Sicherheitsarchitektur entscheidend. Veraltete Systeme, unklare Zugriffsrechte oder fehlende Netzwerksegmentierung bieten Angriffsflächen, die gezielt ausgenutzt werden.

RIEDEL

# Cyberkriminelle veröffentlicht 588 GB Daten einer Forschungseinrichtung

21. September 2025, in Bonn/Nordrhein-Westfalen

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Am 21. September 2025 wurde eine deutsche Forschungseinrichtung von der Ransomware-Gruppe **Qilin** auf deren Darknet-Leakseite gelistet. Die Angreifer behaupten, **588 GB** an Daten aus den Systemen der Organisation entwendet zu haben. Zur Untermauerung ihrer Angaben veröffentlichten sie mehrere Screenshots.

**Was hätte man besser machen können?**
Gerade im Forschungsumfeld ist der Schutz sensibler Daten essenziell – sei es für wissenschaftliche Integrität oder den Schutz internationaler Kooperationen. Eine bessere **Trennung kritischer Systeme**, regelmäßige **Sicherheitsüberprüfungen** und klar definierte Abläufe für den Ernstfall hätten dazu beitragen können, den Vorfall frühzeitig zu erkennen und gezielter zu reagieren.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10642-qilin-zef.png

**Was lernen wir daraus:**
Cyberangriffe auf Forschungseinrichtungen gefährden nicht nur Daten, sondern auch Vertrauen, internationale Zusammenarbeit und langfristige Projekte. Wer Wissen schafft, trägt Verantwortung – auch für den Schutz digitaler Infrastrukturen. Der Vorfall zeigt, dass Cybersicherheit längst kein Randthema mehr ist, sondern zur Grundvoraussetzung für verlässliche Wissenschaft gehört.

RIEDEL

# Cyberangriff auf IT-Dienstleister legt Flughäfen lahm

20. September 2025, in Deutschland

SUPPLY CHAIN

AUSFALL

**Was ist passiert?**
Ein Cyberangriff auf einen IT-Dienstleister führte an mehreren Flughäfen zu erheblichen Störungen. An einem großen deutschen Flughafen musste die Passagierabfertigung zeitweise manuell erfolgen; noch eine Woche später kam es wegen neu aufzuschaltender Systeme zu Ausfällen und langen Wartezeiten. Ein anderer Flughafen blieb dank schneller Reaktion und sofortiger Trennung vom betroffenen System nahezu störungsfrei.

**Was hätte man besser machen können?**
Der Vorfall verdeutlicht die hohe Abhängigkeit der Luftfahrt von externen IT-Dienstleistern – besonders, wenn Passagiere direkt betroffen sind. Eine bessere Segmentierung, regelmäßige **Schwachstellenanalysen** und **EDR/XDR-Lösungen** hätten die Auswirkungen verringert. Entscheidend wäre zudem ein klarer Incident-Response-Plan, der auch Dienstleister einbezieht, um Reaktionszeiten zu verkürzen und Störungen für Passagiere und Abläufe zu minimieren.

**Anzunehmende Schadensfelder:**

Quellen:
https://industrialcyber.co/transport/cyberattack-on-collins-aerospace-disrupts-flights-at-heathrow-other-european-airports/
https://www.spiegel.de/panorama/bruessel-cyberangriff-auf-flughafen-sorgt-fuer-verspaetungen-und-ausfaelle-a-f14bf1a1-935c-4b96-a76f-8c1b314ef7e9

**Was lernen wir daraus:**
Der Fall verdeutlicht, wie wichtig es ist, auch bei ausgelagerten IT-Diensten auf Resilienz und Notfallpläne zu setzen. Flughäfen und andere kritische Einrichtungen sollten ihre Abhängigkeiten regelmäßig überprüfen und sicherstellen, dass sie im Ernstfall schnell und eigenständig reagieren können.

RIEDEL

# Ransomware-Gruppe setzt internationalem Industriekonzern ein Ultimatum

18. September 2025, in Deutschland

RANSOMWARE

ERPRESSUNG

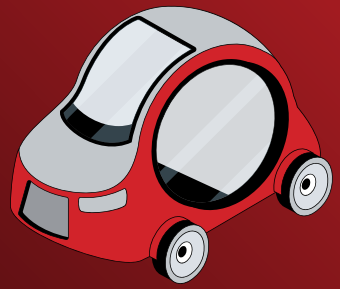
**Was ist passiert?**
Ein weltweit führender Automobilhersteller wurde von der Ransomware-Gruppe **Everest** auf deren Darknet-Leaksite gelistet. Die Angreifer setzten zwei Fristen: eine zur Veröffentlichung interner Audit-Dokumente und eine zur Kontaktaufnahme durch das Unternehmen. Nach Ablauf beider Deadlines veröffentlichte die Gruppe am 22. September mehrere Beweis-Screenshots sowie Download-Links. Details zur vollständigen Datenmenge wurden nicht genannt.

**Was hätte man besser machen können?**
Gezielte Erpressungsversuche mit gestaffelten Drohkulissen zeigen, wie professionell Gruppen wie **Everest** vorgehen. Eine robuste Sicherheitsarchitektur mit **EDR und XDR** hätte verdächtige Aktivitäten möglicherweise frühzeitig erkannt. Auch ein kontinuierliches **Vulnerability Management** wäre essenziell gewesen, um potenzielle Schwachstellen zu schließen, besonders in komplexen, globalen IT-Strukturen.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10613-bmw-everest.png
https://www.security-incidents.de/assets/img/incidents/10613-bmw-everest-03.png
https://www.security-incidents.de/assets/img/incidents/10613-bmw-everest-02.png

**Was lernen wir daraus:**
Ransomware-Gruppen setzen zunehmend auf psychologischen Druck durch Fristen und gestaffelte Veröffentlichungen. Besonders bei großen, international tätigen Unternehmen ist es entscheidend, nicht nur auf technische Schutzmaßnahmen zu setzen, sondern auch auf klare Prozesse für Incident Response und Krisenkommunikation. Prävention, Transparenz und schnelle Reaktion sind der Schlüssel zur Schadensbegrenzung.



RIEDEL

# Sozialorganisation im Visier: Angriff auf eine Arbeiterwohlfahrt

18. September 2025, in Karlsruhe/Baden-Württemberg

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Am 18. September 2025 wurde eine Arbeiterwohlfahrt von der Ransomware-Gruppe **INC Ransom** auf deren Darknet-Leaksite gelistet. Die Angreifer veröffentlichten über **66 GB** an Daten aus den Systemen der Organisation. Angaben zum konkreten Inhalt der Beute wurden nicht gemacht. Bereits im August war die Wohlfahrt Ziel eines Ransomware-Angriffs.

**Was hätte man besser machen können?**
Dass die Organisation innerhalb kurzer Zeit erneut Opfer eines Ransomware-Angriffs wurde, deutet auf bestehende Schwachstellen in der IT-Sicherheitsarchitektur hin. Eine gründliche **Schwachstellenanalyse** hätte mögliche Einfallstore aufdecken können. Mit Lösungen wie **EDR und XDR** wären verdächtige Aktivitäten womöglich frühzeitig erkannt worden, bevor es zu einem zweiten Vorfall kommen konnte.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10677-arbeiterwohlfahrt-karlsruhe-land-inc-ransom.png

**Was lernen wir daraus:**
Auch gemeinnützige Organisationen sind längst im Fadenkreuz professioneller Ransomware-Gruppen. Der wiederholte Angriffzeigt, wie wichtig nachhaltige Sicherheitsmaßnahmen und kontinuierliche Überwachung sind – insbesondere im sozialen Sektor, wo sensible personenbezogene Daten verarbeitet werden.

RIEDEL

# Sarcoma zielt auf Mittelstand: Drei deutsche Unternehmen gleichzeitig betroffen

17. September 2025, in Deutschland

RANSOMWARE

DATENLECK

**Was ist passiert?**
Mitte September 2025 listete die Ransomware-Gruppe **Sarcoma** drei deutsche Unternehmen auf ihrer Darknet-Leaksite: ein Weiterbildungsunternehmen aus Erfurt **(43 GB Daten)**, ein Wohnungsbauunternehmen **(989 GB)** und einen Garagentor-Anbieter **(643 GB inkl. Screenshots)**. Die koordinierte Veröffentlichung deutet auf eine gezielte Kampagne gegen mittelständische Unternehmen mit sensiblen Daten hin.

**Was hätte man besser machen können?**
Die Vorfälle zeigen, dass technische Schutzmaßnahmen wie eine stärkere **Netzwerksegmentierung** dazu beitragen können, die Ausbreitung von Angreifern nach einem initialen Zugriff zu begrenzen. Ergänzend wären insbesondere eine **frühzeitige Erkennung** ungewöhnlicher Aktivitäten, **restriktive Zugriffskontrollen** sowie der gezielte Schutz sensibler Daten relevant gewesen, um Risiken einer umfangreichen Datenexfiltration zu reduzieren.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10604-sarcoma.png
https://www.security-incidents.de/assets/img/incidents/10603-sarcoma.png
https://www.security-incidents.de/assets/img/incidents/10602-sarcoma.png

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

RIEDEL

# Ransomware-Gruppe droht Gutachterbüro mit Datenleck

16. September 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Am 16. September 2025 wurde ein Sachverständigenbüro von der Ransomware-Gruppe **Thegentlemen** auf deren Opferblog gelistet. Ob und welche Daten betroffen sind, war bislang unklar. Die Angreifer haben jedoch einen Countdown gesetzt, der am 26. September endet, danach droht die Veröffentlichung der erbeuteten Informationen.

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

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10584-Thegentlemen.png

**Was lernen wir daraus:**
Ransomware-Gruppen wie Thegentlemen setzen zunehmend auf psychologischen Druck durch Countdown-Veröffentlichungen. Unternehmen, auch kleinere Dienstleister, sollten sich nicht in falscher Sicherheit wiegen. Eine kontinuierliche Überwachung und frühzeitige Erkennung verdächtiger Aktivitäten sind essenziell, um Angriffe rechtzeitig zu stoppen.

RIEDEL

# 520 GB sensible Daten bei Kölner Großhändler entwendet

16. September 2025, in Köln/Nordrhein-Westfalen

RANSOMWARE

DATENDIEBSTAHL

DATENLECK

**Was ist passiert?**
Die Ransomware-Gruppe Sarcoma hat am 16. September 2025 einen Modegroßhändler aus Köln auf ihrem Opferblog gelistet. Laut den Angreifern wurden **520 GB** vertrauliche Daten, darunter Ausweisdokumente und interne Kommunikation – exfiltriert und über einen Downloadlink veröffentlicht.

**Was hätte man besser machen können?**
Ein rechtzeitiges **Vulnerability Assessment** hätte potenzielle Einfallstore identifizieren können, bevor sie ausgenutzt wurden. Mit **Endpoint Detection & Response (EDR) sowie Extended Detection & Response (XDR)** wären verdächtige Aktivitäten vermutlich früher aufgefallen und der Angriff hätte möglicherweise eingedämmt oder sogar verhindert werden können.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10593-Sarcoma.png

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


RIEDEL

# Ransomware-Angriff auf Münchner Werbeplattform

15. September 2025, in München/Bayern

RANSOMWARE

DATENDIEBSTAHL

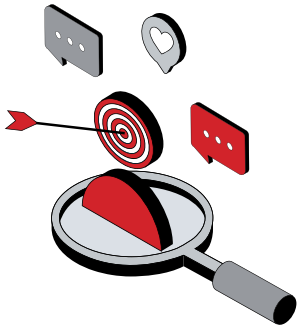
**Was ist passiert?**
Am 15. September 2025 wurde ein führender Advertising-Marktplatz aus München von der Ransomware-Gruppe **Coinbasecartel** auf einem Darknet-Blog gelistet. Ob und in welchem Umfang Daten kompromittiert wurden, war zu dem Zeitpunkt nicht eindeutig.

**Was hätte man besser machen können?**
Der Vorfall verdeutlicht die Bedeutung eines ganzheitlichen Sicherheitsansatzes. Durch kontinuierliche **Vulnerability Assessments** hätten potenzielle Schwachstellen unter Umständen früher erkannt werden können. Der Einsatz von **EDR- und XDR-Lösungen** sowie ein aktives **Security Operations Center (SOC)** können dazu beitragen, Angriffe früher zu erkennen und deren Auswirkungen zu begrenzen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10586-Coinbasecartel.png

**Was lernen wir daraus:**
Ransomware-Gruppen wie Coinbasecartel nutzen gezielt Schwachstellen in IT-Infrastrukturen. Unternehmen sollten auf proaktive Sicherheitsmaßnahmen setzen: regelmäßige Schwachstellenanalysen, Echtzeitüberwachung und automatisierte Reaktionen sind entscheidend. Der Vorfall unterstreicht die Bedeutung eines modernen, mehrschichtigen Sicherheitskonzepts.



RIEDEL

# Störungen bei Kommunalwahl-Ergebnissen in NRW

14. September 2025, in Nordrhein-Westfalen

AUSFALL

**Was ist passiert?**
Am Wahlabend der nordrhein-westfälischen Kommunalwahl kam es zu erheblichen technischen Problemen bei der Online-Darstellung der Ergebnisse. Ein Defekt im Rechenzentrum Niederrhein sowie eine Serverüberlastung beim IT-Dienstleister führten zu Ausfällen. Die Polizei schloss einen Cyberangriff aus, und laut Behörden verlief die Auszählung dennoch ordnungsgemäß und ohne Beeinträchtigungen.

**Was hätte man besser machen können?**
Auch ohne Cyberangriff zeigt der Vorfall, wie wichtig belastbare IT-Infrastrukturen für demokratische Prozesse sind. Ein **Security Operations Center (SOC)** mit Monitoring-Funktionen, kombiniert mit **Vulnerability Assessment** und Load-Management-Strategien, hätte helfen können, technische Schwachstellen frühzeitig zu erkennen und Ausfälle zu vermeiden.

## Anzunehmende Schadensfelder:

Quellen:
https://www1.wdr.de/nachrichten/wahlen/kommunalwahlen-2025/wahlergebnisse-uebermittlung-probleme100.html
https://www.heise.de//news/IT-Stoerungen-bei-Kommunalwahl-Keine-Hinweise-auf-Cyberangriff-10643923.html

**Was lernen wir daraus:**
Auch technische Defekte können die Integrität öffentlicher Prozesse gefährden. Der Vorfall zeigt, dass IT-Sicherheit nicht nur vor Angriffen schützen muss, sondern auch vor Ausfällen. Kommunale Einrichtungen brauchen stabile, skalierbare und überwachte Systeme, besonders bei öffentlichkeitswirksamen Ereignissen wie Wahlen.


RIEDEL

# Ransomware-Gruppe erpresst Kreditunternehmen

09. September 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

ERPRESSUNG

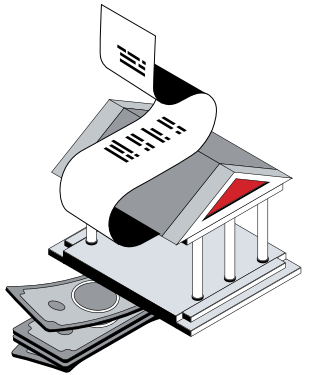
**Was ist passiert?**
Ein Kreditunternehmen einer deutschen Bank wurde auf der Darknet-Seite der Ransomware-Gruppe **Everest** gelistet. Die Angreifer behaupteten, Namen, Adressen, E-Mails, Telefonnummern und weitere Kundendaten erbeutet zu haben. Sie drohten mit Veröffentlichung, falls bis zum 16. September kein Kontakt zustande kam.

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

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10536-everest.png

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



RIEDEL

# Münchener Fachanwaltskanzlei: 330 GB gestohlen

09. September 2025, in München/Bayern

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Eine Fachanwaltskanzlei aus München wurde auf dem Opferblog der Ransomware-Gruppe **Qilin** gelistet. Die Angreifer behaupten, rund **330 GB** sensibler Daten entwendet zu haben, darunter Polizeiakten, Finanzinformationen und Mandantendaten. Eine unabhängige Bestätigung stand noch aus.

**Was hätte man besser machen können?**
In Kanzleien sind Daten nicht nur sensibel – sie sind geschäftskritisch. Mandanteninformationen, Polizeiakten und Finanzdaten müssen besonders geschützt werden. Eine konsequente Datenklassifizierung, kombiniert mit **Endpoint Detection & Response (EDR)**, hätte verdächtige Zugriffe früh erkannt. Ergänzend sorgt ein **Security Operations Center (SOC)** für die lückenlose Überwachung und schnelle Reaktion im Ernstfall.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10544-Qilin.png

**Was lernen wir daraus:**
Juristische Dienstleister sind besonders gefährdet, nicht wegen ihrer Größe, sondern wegen der Brisanz ihrer Daten. Der Schutz vertraulicher Informationen ist nicht nur Pflicht, sondern Grundlage für Vertrauen und Mandantenbindung. Wird dieses Vertrauen durch einen Cyberangriff erschüttert, drohen nicht nur rechtliche Konsequenzen, sondern auch langfristige Reputationsverluste und der Verlust wertvoller Mandate.

RIEDEL

# 600 GB entwendet: Ransomware-Angriff auf Maschinenbauer

09. September 2025, in Ansbach/Bayern

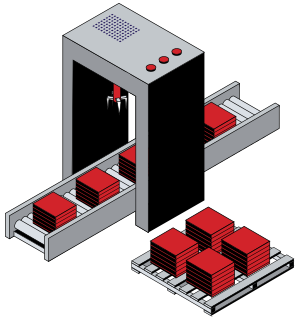
RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Am 9. September 2025 wurde ein deutscher Hersteller von Verpackungs- und Palettierlösungen auf dem Opferblog der Ransomware-Gruppe **INC Ransom** gelistet. Die Angreifer behaupten, rund **600 GB** sensibler Daten gestohlen zu haben, darunter E-Mails, Finanzunterlagen und Kundenverträge.

**Was hätte man besser machen können?**
Bei der Verarbeitung großer Datenmengen ist eine strikte Zugriffskontrolle entscheidend. Ein **Zero-Trust-Ansatz**, kombiniert mit **Endpoint Detection & Response (EDR)**, hätte unautorisierte Aktivitäten früh erkannt. Ergänzend hilft ein **Vulnerability Assessment**, die Datenhaltung regelmäßig zu bewerten und abzusichern.

**Was lernen wir daraus:**
Maschinenbauer sind zunehmend digitalisiert von Konstruktion bis Kundenkommunikation. Große Datenmengen bedeuten große Verantwortung. Wer hier nicht auf moderne Sicherheitsarchitekturen setzt, riskiert nicht nur Datenverlust, sondern auch den Stillstand ganzer Lieferketten und das Vertrauen der Industriepartner.



**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10553-INCRansom.png

RIEDEL

# Ransomware trifft kommunalen Wasserversorger

06. September 2025, in Saarland

RANSOMWARE

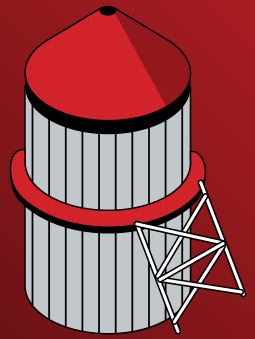
**Was ist passiert?**
Ein kommunaler Wasserversorger wurde im Saarland Ziel eines Ransomware-Angriffs. Die Gruppe **Obscura** bekannte sich öffentlich dazu. Die Täter setzten eine Frist, um die Veröffentlichung mutmaßlich erbeuteter Daten abzuwenden.

**Was hätte man besser machen können?**
Versorger kritischer Infrastrukturen sind auf besonders hohe Sicherheitsstandards angewiesen. Maßnahmen wie ein **Security Operations Center (SOC)** zur kontinuierlichen Überwachung, **Endpoint Detection & Response (EDR)** zur verbesserten Angriffserkennung sowie ein **Security Orchestration & Automation (SOAR)-Ansatz** können dabei helfen, sicherheitsrelevante Vorfälle früher zu erkennen und schneller darauf zu reagieren, um mögliche Auswirkungen zu begrenzen.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10522-Obscura-WZVWarndt.png

**Was lernen wir daraus:**
Wasserversorger zählen nach **NIS-2** klar zur kritischen Infrastruktur und sind daher besonders attraktive Ziele für Cyberangriffe. Der Vorfall zeigt, wie wichtig professionelle Sicherheitsmaßnahmen auch in kommunalen Einrichtungen sind. Ein erfolgreicher Angriff gefährdet nicht nur sensible Daten, sondern auch das Vertrauen der Bevölkerung – weshalb robuste Schutzmechanismen, klare Prozesse und kontinuierliche Überwachung unverzichtbar sind.



RIEDEL

# Gezielte Angriffe auf technische Dienstleister: Lynx nimmt Industrie-Zulieferer ins Visier

04. September 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Am 4. September 2025 bekannte sich die Ransomware-Gruppe **Lynx** zu Angriffen auf drei deutsche Unternehmen aus dem technischen Dienstleistungssektor. Betroffen sind ein Beratungsunternehmen für Maschinenhersteller, ein Dienstleister für technische Dokumentationen aus Thüringen sowie ein Anbieter für Praxiseinrichtungen aus Bayern. Die Täter behaupten, Daten gestohlen und verschlüsselt zu haben.

**Was hätte man besser machen können?**
Technische Dienstleister sind häufig eng in die IT-Umgebungen ihrer Kunden eingebunden und damit ein potenziell attraktives Ziel für Angreifer. Sicherheitskonzepte wie **Zero Trust** in Kombination mit **Endpoint Detection & Response (EDR)** können helfen, verdächtige Zugriffe früher zu erkennen. Ein begleitendes **Security Operations Center (SOC)** unterstützt die kontinuierliche Analyse von Ereignissen und eine abgestimmte Reaktion.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10506-Lynx-Technischer_Beratungsdienstleister.PNG
https://www.security-incidents.de/assets/img/incidents/10496-Lynx_1.png
https://www.security-incidents.de/assets/img/incidents/10497-Lynx.png

**Was lernen wir daraus:**
Die Angriffe zeigen, dass Ransomware-Gruppen wie Lynx gezielt auf Unternehmen setzen, die als Schnittstelle zwischen Industrie und Endkunden agieren. Gerade technische Dienstleister sind oft digital gut vernetzt – aber nicht immer ausreichend geschützt. Wer hier nicht in IT-Sicherheit investiert, gefährdet nicht nur sich selbst, sondern auch die Lieferketten seiner Kunden.

RIEDEL

# Stahlhart getroffen: Ransomware-Angriff auf Metallspezialisten

01. September 2025, in Deutschland

RANSOMWARE

DATENPANNE

DATENLECK

EINBRUCH

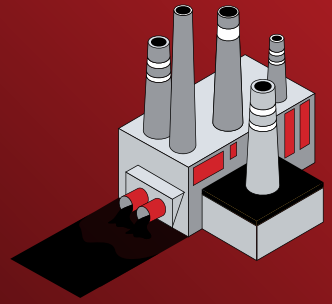
**Was ist passiert?**
Die Ransomware-Gruppe **Safepay** bekannte sich zu einem Angriff auf ein deutsches Unternehmen, das sich auf die Herstellung von Warenpräsentationen aus Metall spezialisiert hat. Die Täter veröffentlichten anschließend zahlreiche mutmaßlich erbeutete Daten auf ihrer Leak-Seite im Darknet.

**Was hätte man besser machen können?**
Gerade in der Industrie mit digitalisierten Produktions- und Konstruktionsdaten ist eine klare Zugriffskontrolle essenziell. Ein Zero-Trust-Ansatz, kombiniert mit **Endpoint Detection & Response (EDR)**, hätte verdächtige Aktivitäten frühzeitig erkannt. Ergänzend hilft ein **Schwachstellen-Scan** um potenzielle Schwachstellen in der Infrastruktur zu identifizieren.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10434-safepay.png

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



RIEDEL

# Ransomware-Gruppe erpresst Wohlfahrtsorganisation

01. September 2025, in Karlsruhe/Baden-Württemberg

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Eine gemeinnützige Organisation aus dem sozialen Bereich wurde Opfer eines Ransomware-Angriffs durch die Gruppe **Lynx**. Die Täter legten zentrale IT-Systeme lahm und forderten ein Lösegeld von **200.000 Euro**. Die Infrastruktur konnte bereits am Folgetag vollständig wiederhergestellt werden. Ob personenbezogene Daten betroffen sind, war noch nicht bekannt.

**Was hätte man besser machen können?**
Organisationen mit großen Datenmengen und sensiblen Informationen sind auf klar definierte Sicherheitsprozesse angewiesen. Strukturen wie ein **Security Operations Center (SOC)**, unterstützt durch automatisierte Abläufe etwa über **SOAR sowie Endpoint Detection & Response (EDR)**, können dazu beitragen, auffällige Aktivitäten früher zu erkennen und die Reaktion auf Sicherheitsvorfälle sowie die Wiederherstellung effizienter zu gestalten.

**Anzunehmende Schadensfelder:**

Quellen:
https://bnn.de/kraichgau/bruchsal/cyberangriff-legt-it-systeme-der-awo-karlsruhe-land-lahm
https://landfunker.de/cyberangriff-auf-awo-ka-land-it-systeme-nach-einem-tag-wiederhergestellt/

**Was lernen wir daraus:**
Soziale Einrichtungen geraten zunehmend in den Fokus von Cyberangriffen – auch aufgrund ihrer gesellschaftlichen Bedeutung. Der vergleichsweise schnelle Wiederanlauf verdeutlicht den Wert vorbereiteter Notfall- und Wiederherstellungsprozesse. Gleichzeitig zeigt der Vorfall, wie wichtig präventive Maßnahmen sind: Der verantwortungsvolle Umgang mit personenbezogenen Daten trägt dazu bei, Vertrauen, Handlungsfähigkeit und den eigenen Auftrag langfristig zu sichern.

RIEDEL

# Ransomware-Gruppe stiehlt 250 GB Daten von Gartenbauunternehmen

01. September 2025, in Rheinland-Pfalz

RANSOMWARE

DATENDIEBSTAHL

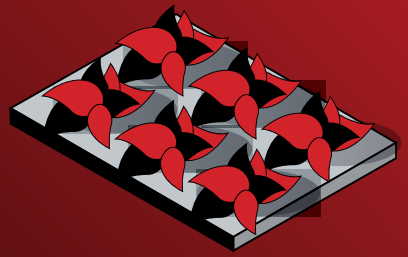
**Was ist passiert?**
Am 1. September 2025 veröffentlichte die Ransomware-Gruppe **INC Ransom** auf ihrem Darknet-Blog einen mutmaßlichen Angriff auf ein Garten- und Landschaftsbauunternehmen aus Rheinland-Pfalz. Die Angreifer behaupten, genau **255,795750525 GB** Geschäftsdaten entwendet zu haben, darunter vermutlich auch sensible Kunden- und Projektdaten.

**Was hätte man besser machen können?**
Bei der Verarbeitung großer Datenmengen, wie in diesem Fall über 250 GB – ist eine strikte Zugriffskontrolle entscheidend. Ein **Zero-Trust-Ansatz** kombiniert mit **Endpoint Detection & Response (EDR)** hätte unautorisierte Aktivitäten früh erkannt. Ergänzend hilft ein **Vulnerability Assessment**, die Datenhaltung kritisch zu prüfen: Müssen alle Daten online verfügbar sein – und wenn ja, unter welchen Schutzmaßnahmen?

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10521-INCransom.png

**Was lernen wir daraus:**
Ein Datenabfluss in dieser Größenordnung deutet oft darauf hin, dass kein wirksames Monitoring für ungewöhnliche Dateiaktivitäten oder Transfers bestand. Wer sich mit dem Thema IT-Sicherheit beschäftigen möchte, sollte sich grundlegende Fragen stellen: Welche Daten sind wirklich schützenswert? Wo liegen sie? Wer hat Zugriff? Schon diese einfache Inventur kann der erste Schritt zu wirksameren Schutzmaßnahmen sein.



RIEDEL

# AUGUST 2025

## SECURITY INCIDENTS GERMANY

RIEDEL

# Druck auf der Leitung: Armaturen-Hersteller von DragonForce attackiert

30. August 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

DATENLECK

**Was ist passiert?**
Am 30. August 2025 veröffentlichte die Ransomware-Gruppe **DragonForce** einen mutmaßlichen Angriff auf einen deutschen Hersteller von Armaturen. Die Angreifer stellten rund **11,72 GB** Daten zum Download bereit, darunter laut eigenen Angaben Finanzunterlagen und Klientendaten.

**Was hätte man besser machen können?**
Ein Security Operations Center (SOC) mit lückenloser Überwachung hätte verdächtige Aktivitäten deutlich früher erkennen und gezielt Gegenmaßnahmen einleiten können. Durch klar definierte Reaktionsprozesse, automatisierte Abläufe und abgestimmte Analysewerkzeuge lassen sich Angriffe wie dieser schneller eingrenzen, bewerten und im Idealfall vollständig verhindern.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10463-dragonforce.png
https://www.security-incidents.de/assets/img/incidents/10463-dragonforce-02.png

**Was lernen wir daraus:**
Hersteller industrieller Komponenten wie Armaturen sind oft tief in kritische Lieferketten eingebunden, von Bauprojekten bis zur Energieversorgung. Ein erfolgreicher Angriff gefährdet nicht nur interne Daten, sondern kann auch regulatorische Anforderungen und Kundenbeziehungen ins Wanken bringen. Wer hier nicht in IT-Sicherheit investiert, riskiert mehr als nur einen Produktionsstopp, sondern den Verlust von Vertrauen und Marktposition.

RIEDEL

# Schön verpackt, aber angreifbar: Kosmetikhersteller im Visier von Safepay

29. August 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

DATENLECK

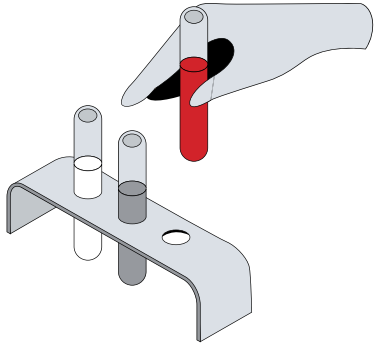
**Was ist passiert?**
Ende August 2025 wurde ein deutscher Hersteller von konventioneller und Naturkosmetik auf der Leak-Seite der Ransomware-Gruppe **Safepay** gelistet. Die Angreifer behaupten, interne Daten erbeutet zu haben, konkrete Details zur Datenmenge oder zum Inhalt wurden jedoch nicht veröffentlicht.

**Was hätte man besser machen können?**
Produzierende Unternehmen sollten ihre Cybersecurity regelmäßig per **Penetrationstests** und Sicherheitsaudits prüfen. Im industriellen Umfeld empfiehlt sich eine integrierte Sicherheitsstrategie für **OT und IT**, da Angriffe beide Bereiche treffen können. So werden Schutzmaßnahmen über alle Ebenen hinweg transparent umgesetzt und Produktionsprozesse effektiv abgesichert.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10464-safepay.png

**Was lernen wir daraus:**
Die Veröffentlichung auf einer Leak-Seite ist oft nur der erste Schritt: Sie dient als Warnsignal und Druckmittel. Wer hier nicht vorbereitet ist, riskiert nicht nur Datenverlust, sondern auch Imageschäden und Vertrauensbrüche. IT-Sicherheit muss deshalb auch in der Markenstrategie mitgedacht werden.



RIEDEL

# Ransomware-Angriff auf Ferienportal

28. August 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

DATENPANNE

EINBRUCH

**Was ist passiert?**
Die Ransomware-Gruppe **Safepay** hat sich zu einem Angriff auf ein deutsches Portal für Ferienunterkünfte bekannt. Nach eigenen Angaben haben die Täter sensible Unternehmens- und Kundendaten entwendet und drohen nun mit deren Veröffentlichung, falls keine Zahlung erfolgt.

**Was hätte man besser machen können?**
Der Vorfall unterstreicht die Bedeutung einer ganzheitlichen Sicherheitsstrategie. Strukturen wie ein **Security Operations Center (SOC)** in Verbindung mit einem **SIEM-System** können dazu beitragen, auffällige Aktivitäten früher zu erkennen und einzuordnen. Ergänzend kann ein regelmäßiges **Vulnerability Assessment** helfen, potenzielle Schwachstellen frühzeitig sichtbar zu machen und Prioritäten für geeignete Maßnahmen abzuleiten.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10417-safepay-ferienwohnungen-de.png
https://www.heise.de/news/Offenbar-datenleck-bei-Ferienwohnungen-de-10624445.html

**Was lernen wir daraus:**
Die Ransomware-Gruppe Safepay gehört zu den Akteuren, die gezielt auf doppelte Erpressung setzen: Sie verschlüsseln nicht nur Daten, sondern drohen auch mit deren Veröffentlichung – oft unter Zeitdruck. Diese Taktik erhöht den psychologischen Druck auf betroffene Unternehmen und erschwert eine ruhige, strategische Reaktion. Solche Gruppen agieren professionell, nutzen automatisierte Leak-Seiten im Darknet und setzen auf maximale Wirkung bei minimalem Aufwand.

RIEDEL

# Webseite vorsorglich abgeschaltet: Öffentliche Verwaltung reagiert auf Cybervorfall

AUSFALL

28. August 2025, in Schmalkalden-Meiningen/Thüringen

**Was ist passiert?**
Eine kommunale Verwaltungseinheit in Thüringen nahm Ende August 2025 ihre öffentliche Webseite vorsorglich offline, nachdem ein Cybervorfall festgestellt wurde. Interne Systeme und Fachportale blieben laut Angaben der Behörde uneingeschränkt funktionsfähig. Die digitale Erreichbarkeit soll über eine provisorische Seite wiederhergestellt werden.

**Was hätte man besser machen können?**
Eine regelmäßige Vulnerability Assessment hätte potenzielle Schwachstellen in der Webinfrastruktur frühzeitig aufdecken können. Ergänzend hätte eine Security Orchestration & Automation (SOAR) automatisiert auf verdächtige Aktivitäten reagieren und die Abschaltung möglicherweise vermeiden können.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.lra-sm.de/internetseite-offline-landratsamt-nimmt-website-des-landkreises-vom-netz/
https://www.mz.de/panorama/cybervorfall-internetseite-von-landkreis-abgeschaltet-4106008

**Was lernen wir daraus:**
Auch wenn nur die Webpräsenz betroffen war, zeigt der Fall, wie wichtig es ist, digitale Kommunikationskanäle abzusichern. Gerade öffentliche Einrichtungen sollten ihre externen Systeme regelmäßig prüfen und mit klaren Reaktionsmechanismen ausstatten, um die Erreichbarkeit im Ernstfall sicherzustellen.


RIEDEL

# Angriff auf Versicherungsmakler: Lynx droht mit Datenveröffentlichung

27. August 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Ein deutscher Industrie-Versicherungsmakler wurde von der Ransomware-Gruppe **Lynx** angegriffen. Die Täter listeten das Unternehmen auf ihrer Darknet-Leakseite und veröffentlichten interne Daten als Beweis.

**Was hätte man besser machen können?**
Gerade bei Dienstleistern mit großen Datenmengen kann eine kontinuierliche Überwachung von Endpunkten eine wichtige Rolle spielen. Lösungen wie **Endpoint Detection and Response (EDR)** können dabei helfen, auffällige Aktivitäten frühzeitig sichtbar zu machen und einzuordnen. Ergänzend kann eine **IT-Musterung** unterstützen, bestehende Schwachstellen strukturiert zu identifizieren und Ansatzpunkte für Verbesserungen aufzuzeigen.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10449-lynx.png
https://www.security-incidents.de/assets/img/incidents/10449-lynx-02.png

**Was lernen wir daraus:**
Versicherungsdienstleister verwalten hochsensible Kunden- und Vertragsdaten. Der Vorfall zeigt, wie wichtig es ist, nicht nur technische Schutzmaßnahmen zu etablieren, sondern auch organisatorische Prozesse zur schnellen Reaktion im Ernstfall. Ransomware-Gruppen wie Lynx setzen gezielt auf datenintensive Branchen mit hohem Erpressungspotenzial.

RIEDEL

# Vierfacher Ransomware-Schlag: Bildung, Industrie und Handel im Visier von Safepay

26. August 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

DATENPANNE

EINBRUCH

**Was ist passiert?**
Am 26. August 2025 bekannte sich die Ransomware-Gruppe **Safepay** zu Angriffen auf **vier deutsche Einrichtungen**: eine evangelische Bildungseinrichtung, eine Realschule, ein Kunststoffverarbeitungsunternehmen sowie einen Händler für Landtechnik. In allen Fällen drohten die Täter mit der Veröffentlichung sensibler Daten, sollten ihre Forderungen bis zum 28. August nicht erfüllt werden.

**Was hätte man besser machen können?**
Gerade in heterogenen IT-Umgebungen wie Schulen, Bildungseinrichtungen oder mittelständischen Betrieben ist eine automatisierte Sicherheitsüberwachung entscheidend. Eine Kombination aus **SIEM** zur zentralen Ereignisanalyse und **SOAR** zur schnellen Reaktion hätte verdächtige Muster frühzeitig erkannt und Gegenmaßnahmen automatisiert eingeleitet.

**Was lernen wir daraus:**
Ransomware-Gruppen wie Safepay setzen gezielt auf Branchen mit sensiblen Daten und begrenzten Schutzmechanismen. Die gleichzeitige Veröffentlichung mehrerer Opfer erhöht den Druck und erschwert die Reaktion. Der Fall zeigt, wie wichtig es ist, auch kleinere Organisationen mit skalierbaren Sicherheitslösungen auszustatten.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10419-Safepay-ev-Bildungseinrichtung.PNG
https://www.security-incidents.de/assets/img/incidents/10418-Safepay-Kunststoffhersteller.PNG
https://www.security-incidents.de/assets/img/incidents/10416-Safepay-Realschule.PNG
https://www.security-incidents.de/assets/img/incidents/10415-Safepay-Landwirtschaftshaendler%20(2).PNG

RIEDEL

# Ransomware-Erpressung im Onlinehandel

21. August 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

ERPRESSUNG

**Was ist passiert?**
Die Ransomware-Gruppe **Medusa** listete den Onlinehandelszweig einer bekannten deutschen Elektrofachmarkt-Kette als Opfer. Die Angreifer behaupten, **114 GB** an Unternehmensdaten gestohlen zu haben. Diese sollen am 25. August veröffentlicht werden, es sei denn, das Unternehmen zahlt 200.000 USD oder verlängert die Frist für 10.000 USD pro Tag.

**Was hätte man besser machen können?**
Eine klarer strukturierte und segmentierte IT-Infrastruktur kann dazu beitragen, Zugriffe innerhalb der Systeme besser zu begrenzen und Auswirkungen von Angriffen zu reduzieren. Ergänzend können Lösungen wie **Extended Detection and Response (XDR)** unterstützen, ungewöhnliche Datenbewegungen früher zu erkennen, einzuordnen und gezielte Gegenmaßnahmen einzuleiten.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10372-medusa.png
https://www.security-incidents.de/assets/img/incidents/10372-medusa-02.png

**Was lernen wir daraus:**
Der Fall zeigt, wie gezielt Ransomware-Gruppen auf digitale Vertriebskanäle setzen, um maximalen Druck aufzubauen. Besonders im E-Commerce, wo sensible Kundendaten und Zahlungsinformationen verarbeitet werden, kann ein erfolgreicher Angriff nicht nur den Betrieb stören, sondern auch das Vertrauen der Kundschaft dauerhaft beschädigen.


RIEDEL

# 675.000 Dateien kompromittiert: Qilin nimmt deutschen Hersteller ins Visier

21. August 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

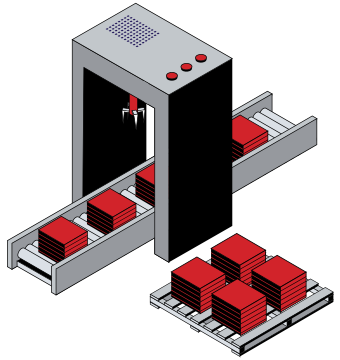
**Was ist passiert?**
Die Ransomware-Gruppe **Qilin** listete am 21. August 2025 einen deutschen Hersteller von Steuerelementen als Opfer auf ihrer Darknet-Seite. Die Angreifer behaupten, **675.000 Dateien** erbeutet zu haben und veröffentlichten **17 Screenshots** als Beweis. Angaben zum Inhalt der Daten wurden nicht gemacht.

**Was hätte man besser machen können?**
Eine **segmentierte Netzwerkarchitektur** mit klar definierten Zugriffsrechten kann dazu beitragen, verdächtige Aktivitäten früher zu erkennen und deren Auswirkungen zu begrenzen. Ergänzend unterstützen **Data-Loss-Prevention-Systeme (DLP)** und ein strukturierter **Incident-Response-Plan** dabei, ungewöhnliche Datenbewegungen schneller sichtbar zu machen und im Ernstfall geordnet zu reagieren.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10384-qilin.png

**Was lernen wir daraus:**
Die Veröffentlichung von Screenshots ist Teil einer Eskalationsstrategie: Sie erhöht den Druck auf das betroffene Unternehmen, ohne sofort alle Daten preiszugeben. So wird Unsicherheit erzeugt, ein typisches Muster bei Ransomware-Gruppen, um Zahlungen zu erzwingen.



RIEDEL

# DragonForce-Angriffe: Vier sensible Gesundheits- und Technikbetriebe betroffen

21. August 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

DATENLECK

EINBRUCH

**Was ist passiert?**

Die Ransomware-Gruppe **DragonForce** bekannte sich zu Cyberangriffen auf vier deutsche Einrichtungen: ein Ingenieurbüro, einen Hörgerätehersteller, eine Arztpraxis sowie einen IT-Dienstleister. Insgesamt wurden über **130 GB** an sensiblen Daten entwendet. Da keine Lösegeldzahlungen erfolgten, wurden die gestohlenen Informationen laut Täterangaben vollständig veröffentlicht.

**Was hätte man besser machen können?**

Ein **Security Operations Center (SOC)** mit Echtzeitüberwachung kann verdächtige Aktivitäten deutlich früher sichtbar machen. Ergänzend unterstützen **Data-Loss-Prevention-Systeme (DLP)** und ein strukturierter **Incident-Response-Plan** dabei, ungewöhnliche Datenbewegungen schneller zu erkennen und im Ernstfall geordnet zu reagieren, wodurch das Risiko größerer Datenabflüsse reduziert werden kann.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10392-IT_Unternehmen-DragonForce.PNG
https://www.security-incidents.de/assets/img/incidents/10391-Ingenieurb%C3%BCro-DragonForce.PNG
https://www.security-incidents.de/assets/img/incidents/10390-Hoergeraetehersteller.PNG
https://www.security-incidents.de/assets/img/incidents/10389-Arzpraxis-DragonForce.PNG

**Was lernen wir daraus:**

Der Fall zeigt, wie wichtig es ist, auf doppelte Erpressung vorbereitet zu sein, also sowohl auf die Verschlüsselung von Systemen als auch auf die Veröffentlichung sensibler Daten. Besonders IT-Dienstleister sind attraktive Ziele, da sie oft Zugang zu Kundennetzwerken und kritischen Infrastrukturen haben.

RIEDEL

# Zwei Handelsunternehmen im Visier von Ransomware-Gruppe „Everest“

20. August 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**

Die Ransomware-Gruppe **Everest** listete zwei Handelsunternehmen als Opfer: einen der größten europäischen Gebrauchtwagenhändler sowie einen Elektrofachmarkt. Insgesamt sollen **über 247.000** Datensätze entwendet worden sein, darunter Namen, E-Mail-Adressen, Anschriften, Fahrzeug- und Produktinformationen.

**Was hätte man besser machen können?**

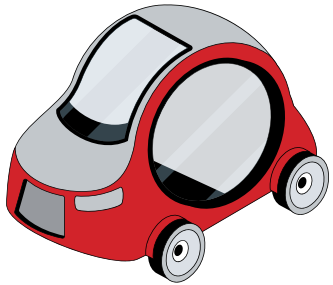
Ein **Security Operations Center (SOC) mit SIEM** hätte verdächtige Datenbewegungen frühzeitig erkannt. Ergänzend wären Verschlüsselung sensibler Daten und regelmäßige **Schwachstellenanalysen** sinnvoll gewesen, um Einfallstore zu schließen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10360-everest.png
https://www.security-incidents.de/assets/img/incidents/10361-everest.png

**Was lernen wir daraus:**

Ransomware-Gruppen wie „Everest“ setzen auf doppelte Erpressung: Datenverschlüsselung und Veröffentlichung. Besonders Handelsunternehmen mit großen Kundendatenbanken sind attraktive Ziele. Der Schutz personenbezogener Daten ist nicht nur rechtlich verpflichtend, sondern auch geschäftskritisch.



RIEDEL

# Cyberangriff auf kirchliche Institution legt IT-Systeme lahm

19. August 2025, in Berlin/Berlin

SPIONAGE

MALWARE

SOCIAL ENGINEERING

EINBRUCH

**Was ist passiert?**
Eine hochrangige politische Führungskraft wurde Opfer eines gezielten Cyberangriffs. Die Angreifer, mutmaßlich aus dem Umfeld der iranischen Gruppe **Charming Kitten**, nutzten Social Engineering und Malware, um Zugriff auf Kalender- und Maildaten zu erlangen. Ein Bewegungsprofil konnte erstellt werden und der infizierte Rechner wurde anschließend isoliert.

**Was hätte man besser machen können?**
Ein Zero-Trust-Ansatz mit Multi-Faktor-Authentifizierung hätte den Zugriff erschwert. Ergänzend wären **Awareness-Schulungen** und ein **SOC** mit Echtzeitüberwachung hilfreich gewesen, um Social-Engineering-Angriffe frühzeitig zu erkennen und Malware-Aktivitäten zu stoppen.

**Was lernen wir daraus:**
Der Fall zeigt, wie effektiv Social Engineering in Kombination mit gezielter Malware sein kann, selbst bei hochrangigen politischen Ämtern. Besonders gefährlich: Die Täuschung war glaubwürdig und auf persönliche Interessen abgestimmt. IT-Sicherheit muss daher technische, organisatorische und menschliche Faktoren gleichermaßen berücksichtigen.


## Anzunehmende Schadensfelder:

Quellen:
https://www.tagesschau.de/inland/regional/berlin/hacker-erbeuten-persoenliche-daten-von-justizsenatorin-badenberg-100.html

RIEDEL

# Ransomware-Gruppe droht mit Veröffentlichung vertraulicher Kanzleidaten

18. August 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Die deutsche Niederlassung einer international tätigen Anwaltskanzlei wurde Mitte August 2025 von der Ransomware-Gruppe **Crypto24** als Opfer gelistet. Die Angreifer behaupten, im Besitz „höchst vertraulicher Daten“ zu sein und drohen mit deren Veröffentlichung am 22. August 2025.

**Was hätte man besser machen können?**
Ein Security Operations Center (SOC) mit Echtzeitüberwachung hätte verdächtige Aktivitäten frühzeitig erkennen können. Ergänzend wären Verschlüsselung sensibler Daten und regelmäßige Schwachstellenanalysen sinnvoll gewesen, um potenzielle Einfallstore zu schließen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10350-crypto24.png

**Was lernen wir daraus:**
Gerade Kanzleien verwalten hochsensible Mandantendaten. Der Fall zeigt, wie wichtig es ist, nicht nur technische Schutzmaßnahmen zu etablieren, sondern auch organisatorische Prozesse zur schnellen Reaktion im Ernstfall. Ransomware-Gruppen wie Crypto24 setzen gezielt auf doppelte Erpressung – Verschlüsselung und Veröffentlichung.

RIEDEL

# Koordinierte DDoS-Angriffe auf politische Webseiten in Sachsen-Anhalt

14. August 2025, in Sachsen-Anhalt

DDoS

AUSFALL

**Was ist passiert?**
Mehrere Landtagsfraktionen in Sachsen-Anhalt wurden im August 2025 Opfer koordinierter **DDoS-Angriffe**. Betroffen waren die Webseiten von fünf politischen Gruppierungen. Die prorussische Gruppe **DDoSia** gilt als Urheber. Die Angriffe führten zu teils mehrstündigen Ausfällen und erschwerten die digitale Kommunikation der Fraktionen.

**Was hätte man besser machen können?**
Zur Abwehr solcher Angriffe wären spezialisierte **DDoS-Schutzlösungen** sinnvoll gewesen, etwa durch vorgelagerte Filterdienste, Lastverteilung und skalierbare Cloud-Infrastrukturen. Ergänzend hätte ein **Security Operations Center (SOC)** mit Echtzeit-Monitoring verdächtige Traffic-Muster frühzeitig erkennen und Gegenmaßnahmen automatisiert einleiten können.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.it-daily.net/shortnews/ddos-cdu-afd-spd-websites-offline

**Was lernen wir daraus:**
DDoS-Angriffe sind ein beliebtes Mittel, um politische Organisationen gezielt zu stören, oft mit dem Ziel, Aufmerksamkeit zu erzeugen oder demokratische Prozesse zu behindern. Der Fall zeigt, wie wichtig es ist, auch öffentliche Einrichtungen und politische Akteure technisch gegen solche Angriffe zu wappnen. IT-Sicherheit ist hier nicht nur Schutzmaßnahme, sondern Teil der digitalen Resilienz demokratischer Strukturen.


RIEDEL

# Cyberwarnung vor dem Angriff: IT-Ausfall bei Gemeindeverwaltung

13. August 2025, in Hoppegarten/Brandenburg

AUSFALL

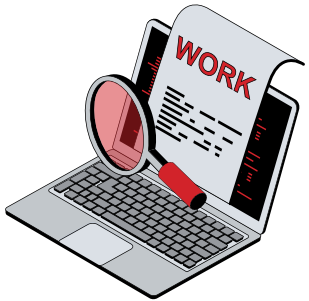
**Was ist passiert?**
Eine Verwaltung wurde vom zuständigen Landeskriminalamt vor einem bevorstehenden Cyberangriff gewarnt. Infolge der präventiven Maßnahmen kam es zu erheblichen Ausfällen in der IT-Infrastruktur. Die Verwaltung war weder telefonisch noch per E-Mail erreichbar, stattdessen wurden temporäre Rufnummern eingerichtet, um die Kommunikation aufrechtzuerhalten.

**Was hätte man besser machen können?**
Ein aktives **Security Operations Center (SOC)** hätte verdächtige Aktivitäten frühzeitig erkennen und die Bedrohungslage besser einschätzen können. Ergänzend wäre eine **Netzwerksegmentierung** sinnvoll gewesen, um kritische Systeme gezielt zu isolieren. Auch ein vorausschauendes **Schwachstellenmanagement** hätte potenzielle Einfallstore identifizieren und absichern können.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.rbb24.de/panorama/beitrag/2025/08/hackerangriff-verwaltung-hoppegarten-maerkischoderland-lka-computer-buergerservice-internet.html

**Was lernen wir daraus:**
Frühwarnungen durch Behörden sind wertvoll, doch ohne technische und organisatorische Vorbereitung bleibt oft nur die Notabschaltung. Der Fall zeigt, wie wichtig es ist, nicht nur auf akute Bedrohungen zu reagieren, sondern kontinuierlich in Prävention, Monitoring und Notfallpläne zu investieren. Besonders Kommunen mit kritischer Infrastruktur sollten ihre Cyberresilienz aktiv stärken.




RIEDEL

# Ransomware-Gruppen „Qilin“ schlägt erneut zu

12. August 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

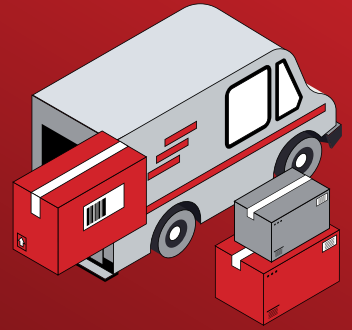
**Was ist passiert?**
Ein deutsches Logistikunternehmen wurde auf dem Opferblog der Ransomware-Gruppe **Qilin** gelistet. Die Angreifer veröffentlichten **neun Screenshots**, die vertrauliche Geschäftsdokumente zeigen sollen, darunter Aufträge, Abrechnungen und interne Prozesse. Eine offizielle Stellungnahme des Unternehmens lag nicht vor.

**Was hätte man besser machen können?**
Ein **Security Operations Center** hätte verdächtige Aktivitäten frühzeitig erkannt und die Reaktion koordiniert. Für Unternehmen mit komplexen Lieferketten ist es entscheidend, Sicherheitslücken systematisch zu identifizieren, etwa durch ein **Vulnerability Assessment** und automatisierte Gegenmaßnahmen mit **SOAR** zu etablieren, um Angriffe direkt einzudämmen.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10326-Qilin-1.png

**Was lernen wir daraus:**
Logistikunternehmen sind attraktive Ziele für Ransomware-Gruppen, da sie oft mit großen Datenmengen und zeitkritischen Prozessen arbeiten. Die Veröffentlichung interner Dokumente kann nicht nur den Betrieb stören, sondern auch das Vertrauen von Kunden und Partnern nachhaltig beschädigen.



RIEDEL

# Druckdienstleister reagiert schnell auf Cyberangriff – später von Qilin gelistet

12. August 2025, in Reutlingen/Baden-Württemberg

AUSFALL

EINBRUCH

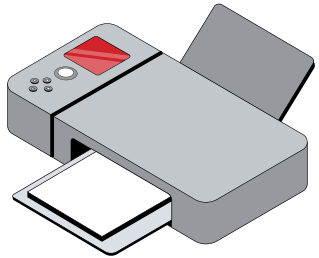
**Was ist passiert?**
Ein führender Anbieter von Drucklösungen wurde Ziel eines Cyberangriffs. Das Unternehmen stoppte den Angriff frühzeitig und fuhr seine Systeme vorsorglich herunter. In den Folgetagen lief der Betrieb eingeschränkt weiter, während Polizei und Forensiker die IT prüften. Hinweise auf kompromittierte Fernwartungszugänge wurden öffentlich.

**Was hätte man besser machen können?**
Ein Security Operations Center hätte verdächtige Aktivitäten frühzeitig erkannt. Besonders bei Fernwartungslösungen wie TeamViewer ist es wichtig, Zugriffskontrollen zu verschärfen und externe Schnittstellen regelmäßig zu prüfen. Auch ein **klarer Notfallplan** für Kommunikation und Wiederherstellung ist essenziell.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.borncity.com/blog/2025/08/12/morgenstern-ag-opfer-eines-cyberangriffs/

**Was lernen wir daraus:**
Angriffe über Fernzugänge sind ein häufig genutzter Einstiegspunkt für Ransomware-Gruppen. Unternehmen mit digitalisierten Prozessen müssen nicht nur technisch vorbereitet sein, sondern auch klare Abläufe für Krisenmanagement und schnelle Wiederherstellung definieren. Frühes Handeln kann größere Schäden verhindern.



RIEDEL

# Zwei Industrieunternehmen von Akira als Opfer gelistet – Details bleiben unklar

11. August 2025, in Deutschland

RANSOMWARE

**Was ist passiert?**
Am 11. August 2025 wurden ein deutscher Bohrmaschinen-Hersteller und ein Anbieter von Umweltmesstechnik auf dem Opferblog der Ransomware-Gruppe **Akira** aufgeführt. Die Unternehmen erschienen neben weiteren Fällen, doch konkrete Informationen zu Datenmenge, Art der betroffenen Systeme oder veröffentlichten Inhalten wurden nicht bekannt gegeben.

**Was hätte man besser machen können?**
Ein SOC (Security Operations Center) hätte verdächtige Aktivitäten frühzeitig erkannt und die Angriffsfläche reduziert. Gerade bei Industrieunternehmen mit sensiblen Entwicklungs- oder Messdaten ist es wichtig, Zugriffsrechte regelmäßig zu prüfen und kritische Systeme durch segmentierte Netzwerke abzusichern.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10299-Akira.png
https://www.security-incidents.de/assets/img/incidents/10298-Akira.png

**Was lernen wir daraus:**
Wenn Angreifer Unternehmen öffentlich als Opfer benennen, ohne Details zu veröffentlichen, ist das oft Teil einer Eskalationsstrategie. Die Unsicherheit erzeugt Druck. Unternehmen sollten vorbereitet sein, nicht nur technisch, sondern auch kommunikativ, um im Ernstfall schnell und kontrolliert reagieren zu können.


RIEDEL

# Qilin greift zwei Technikunternehmen gleichzeitig an und veröffentlicht sensible Daten

11. August 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Am 11. August 2025 wurden ein Hersteller von Flächenheizungen und ein Dienstleister für automatische Türanlagen von der Ransomware-Gruppe **Qilin** als Opfer gelistet. Die Angreifer veröffentlichten insgesamt **21 Screenshots** und behaupten, interne Informationen zu Arbeitsprozessen, Komponentenherkunft und sicherheitsrelevanten Kundenprojekten entwendet zu haben.

**Was hätte man besser machen können?**
Ein **Security Operations Center** hätte verdächtige Aktivitäten frühzeitig erkannt und die Angriffsfläche verkleinert. Zusätzlich wäre es sinnvoll gewesen, sensible Daten zu verschlüsseln, externe Zugriffe zu begrenzen und die IT-Infrastruktur regelmäßig auf **Schwachstellen** zu prüfen, besonders bei sicherheitsrelevanten Kundenprojekten.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10308-qilin.png
https://www.security-incidents.de/assets/img/incidents/10307-qilin.png

**Was lernen wir daraus:**
Technikunternehmen, die mit sicherheitsrelevanten Infrastrukturen oder Gebäudetechnik arbeiten, sind besonders anfällig für gezielte Ransomware-Angriffe. Die Veröffentlichung interner Informationen erhöht den Druck auf betroffene Organisationen und kann zu Vertrauensverlust bei Kunden und Partnern führen.

RIEDEL

# DDoS-Angriff legt Webseite der Stadt Trier zeitweise lahm

05. August 2025, in Trier/Rheinland-Pfalz

DDoS

AUSFALL

**Was ist passiert?**
Am 5. August 2025 wurde die Webseite einer deutschen Stadtverwaltung durch eine **DDoS-Attacke** überlastet. Die Seite war zeitweise nicht erreichbar. Der Angriff könnte Teil einer größeren Welle von Überlastungsversuchen auf kommunale Webportale gewesen sein. Weitere technische Details wurden bislang nicht veröffentlicht.

**Was hätte man besser machen können?**
DDoS-Angriffe lassen sich durch vorgelagerte Filterdienste, intelligente Lastverteilung und skalierbare Infrastruktur besser abwehren. Ein Echtzeit-Monitoring mit automatischer Alarmierung hätte frühzeitig reagiert und die Verfügbarkeit schneller wiederhergestellt.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.swr.de/swraktuell/rheinland-pfalz/trier/internetseite-der-stadt-trier-nach-hackerangriff-nicht-erreichbar-100.html

**Was lernen wir daraus:**
DDoS-Angriffe zielen nicht auf Daten, sondern auf die Verfügbarkeit. Gerade öffentliche Einrichtungen müssen sicherstellen, dass ihre digitalen Dienste auch bei hoher Last erreichbar bleiben. Prävention durch technische Schutzmaßnahmen und klare Notfallprozesse ist entscheidend, um handlungsfähig zu bleiben.


RIEDEL

# Vierfacher Angriff durch DragonForce auf Immobilien- und IT-Branche

04. August 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

DATENLECK

**Was ist passiert?**

Am 4. August 2025 wurden vier deutsche Unternehmen gleichzeitig von der Ransomware-Gruppe **DragonForce** angegriffen. Betroffen waren zwei Hausverwaltungen, ein Immobiliendienstleister und ein IT-Dienstleister. Die Angreifer behaupten, insgesamt rund **380 GB** an sensiblen Daten entwendet und veröffentlicht zu haben. Die Daten sollen unter anderem Verträge, Kundendaten und interne Dokumente enthalten.

**Was hätte man besser machen können?**

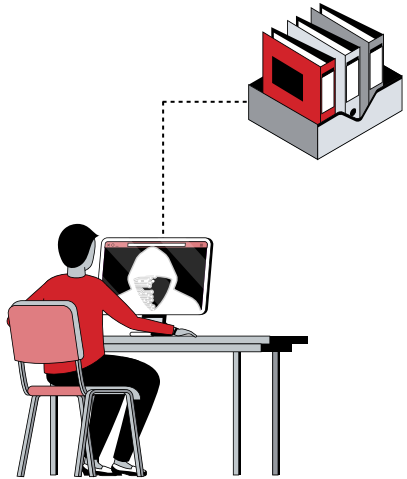
Die parallelen Angriffe zeigen, wie wichtig ein durchdachtes Sicherheitskonzept ist. Ein **Security Operations Center** mit Echtzeitüberwachung hätte verdächtige Aktivitäten frühzeitig erkannt. Ergänzend helfen **Schwachstellenscans**, segmentierte Netzwerke und automatisierte Reaktionen, um Angriffe schnell zu stoppen und Schäden zu begrenzen.

**Anzunehmende Schadensfelder:**

Quellen:
https://deltasecure.de/hacker-angriffe/dragonforce-soll-koenig-hausverwaltung-gehackt-haben/
https://www.security-incidents.de/assets/img/incidents/10234-%20Hausverwaltung_DragonForce.PNG

**Was lernen wir daraus:**

Ransomware-Gruppen agieren zunehmend koordiniert und branchenübergreifend. Besonders gefährdet sind Unternehmen mit hohem Datenvolumen und digitalisierten Prozessen. Wer keine zentrale Sicherheitsüberwachung etabliert, läuft Gefahr, Angriffe zu spät zu erkennen. Prävention, schnelle Reaktion und klare Zuständigkeiten sind heute Pflicht.



RIEDEL

# IT-Systemintegrator aus Köln im Visier von Lynx – Daten verschlüsselt

02. August 2025, in Köln/Nordrhein-Westfalen

RANSOMWARE

**Was ist passiert?**
Ein IT-Systemintegrator mit Sitz in Köln wurde am 2. August 2025 von der Ransomware-Gruppe **Lynx** auf deren Leaksite gelistet. Die Angreifer behaupten, Daten verschlüsselt zu haben. Weitere Details zur Datenmenge oder zu betroffenen Informationen sind nicht bekannt.

**Was hätte man besser machen können?**
Als IT-Systemintegrator tragen Unternehmen Verantwortung für die eigene Infrastruktur und oft auch für die Sicherheit von Kundennetzwerken. Maßnahmen wie ein **Security Operations Center (SOC)** mit kontinuierlichem Monitoring können helfen, sicherheitsrelevante Auffälligkeiten früher zu erkennen. Ergänzend können **Schwachstellenscans** und segmentierte Netzwerke dazu beitragen, Risiken zu begrenzen und kritische Systeme besser abzusichern.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10224-Lynx.png

**Was lernen wir daraus:**
Wenn Angreifer nur die Verschlüsselung bestätigen, aber keine Daten veröffentlichen, ist das oft Teil einer Eskalationsstrategie. Unternehmen sollten nicht nur auf technische Schutzmaßnahmen setzen, sondern auch auf klare Kommunikations- und Wiederherstellungsprozesse. Denn im Ernstfall zählt nicht nur, ob man geschützt ist, sondern wie schnell man wieder handlungsfähig wird.

RIEDEL

# Ransomware-Angriffe auf deutsche Unternehmen: Über 44 GB Daten betroffen

01. August 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**

Anfang August 2025 wurden zwei deutsche Unternehmen Opfer von Ransomware-Angriffen durch die Gruppe **Akira**. Betroffen waren eine Holdinggesellschaft für Lager- und Logistikdienstleistungen sowie ein Fensterbauer. Die Angreifer behaupteten, insgesamt rund **44 GB** vertraulicher Daten exfiltriert zu haben, darunter Mitarbeiterdokumente, Kundendaten, Finanzinformationen und Vertragsunterlagen.

**Was hätte man besser machen können?**

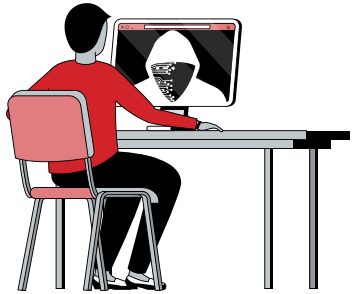
Die Kombination aus **Extended Detection & Response** und regelmäßigen **Schwachstellenanalysen** hätte verdächtige Aktivitäten frühzeitig sichtbar gemacht und die Angriffsfläche reduziert. Gerade bei komplexen IT-Strukturen ist es entscheidend, dass Sicherheitsprozesse automatisiert und systemübergreifend orchestriert sind.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10215-Akira.png
https://www.security-incidents.de/assets/img/incidents/10214-Akira.png

**Was lernen wir daraus:**

Vorbereitete Notfallpläne, regelmäßige Backups und eine schnelle interne Eskalation hätten dazu beitragen können, den Schaden einzugrenzen und die Wiederherstellung zu beschleunigen.

RIEDEL

# IT-Ausfall bei gemeinnütziger Einrichtung – Ransomware legt Systeme lahm

01. August 2025, in Düsseldorf/Nordrhein-Westfalen

RANSOMWARE

DATENDIEBSTAHL

EINBRUCH

AUSFALL

**Was ist passiert?**
Eine gemeinnützige Organisation wurde Ziel eines Cyberangriffs. Unbekannte legten zentrale IT-Systeme durch eine Verschlüsselungsattacke lahm. Ein Krisenstab wurde einberufen, externe IT-Forensiker hinzugezogen. Teile der digitalen Infrastruktur, darunter wissenschaftliche Inhalte, waren zeitweise nicht verfügbar.

**Was hätte man besser machen können?**
Die frühzeitige Auswertung sicherheitsrelevanter Ereignisse über ein **SIEM-System** sowie eine koordinierte Reaktion mithilfe von **Security Orchestration, Automation and Response (SOAR)** können dazu beitragen, Sicherheitsvorfälle besser einzugrenzen. Gerade bei Organisationen mit sensiblen Daten ist es wichtig, technische Schutzmechanismen sinnvoll mit klar definierten Prozessen zu verzahnen.

## Anzunehmende Schadensfelder:

Quellen:
https://x.com/_ungerm/status/1951051478279291262
https://www.security-incidents.de/assets/img/incidents/10286-HansB%C3%B6cklerStiftung-1.png

**Was lernen wir daraus:**
Cyberangriffe auf gesellschaftsnahe Organisationen zeigen, dass digitale Bedrohungen nicht nach Branche oder Größe unterscheiden. Besonders dort, wo Forschung, Bildung oder soziale Leistungen digital unterstützt werden, kann ein Ausfall weitreichende Folgen haben. Der Vorfall unterstreicht die Notwendigkeit, IT-Sicherheit als strategisches Thema zu begreifen – nicht nur als technische Pflicht.

RIEDEL

# JULI 2025

## SECURITY INCIDENTS GERMANY

RIEDEL

# Sporthändler im Visier von INC Ransom

31. Juli 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

EINBRUCH

**Was ist passiert?**
Am 31. Juli 2025 wurde ein Unternehmen aus dem Sportartikelhandel von der Ransomware-Gruppe **INC Ransom** als Opfer einer Cyberattacke benannt. Die Täter behaupten, sensible Daten gestohlen zu haben und drohen mit deren Veröffentlichung, sollte keine Lösegeldzahlung erfolgen. Die Erpressung wurde öffentlich über einschlägige Kanäle kommuniziert.

**Was hätte man besser machen können?**
Eine frühzeitige Erkennung auffälliger Aktivitäten durch ein **Security Operations Center** in Verbindung mit **Endpoint Detection & Response (EDR)** kann dazu beitragen, potenzielle Angriffe früher sichtbar zu machen und Auswirkungen zu begrenzen. Wichtig ist zudem, dass Sicherheitsmaßnahmen nicht nur eingeführt, sondern regelmäßig überprüft, getestet und bei Bedarf weiterentwickelt werden.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10191-Sportutensilienh%C3%A4ndler-INC_Ransom.PNG

**Was lernen wir daraus:**
Der Fall zeigt, wie gezielt Ransomware-Gruppen mittelständische Unternehmen ins Visier nehmen, oft mit dem Ziel, vertrauliche Daten zu monetarisieren. Eine schnelle Reaktion, transparente Kommunikation und technische Resilienz sind entscheidend, um den Schaden zu begrenzen und das Vertrauen von Kunden und Partnern zu erhalten.


RIEDEL

# Digitale Angriffsserie: Auch Wittenberg von DDoS-Welle betroffen

31. Juli 2025, in Wittenberg/Sachsen-Anhalt

DDoS

AUSFALL

**Was ist passiert?**
Im Zuge einer breit angelegten Angriffswelle auf kommunale Webportale wurde auch eine Stadtverwaltung Opfer einer **DDoS-Attacke**. Der Internetauftritt war zeitweise nicht erreichbar. Die Attacke reiht sich ein in eine Serie von Überlastungsangriffen, die mehrere Städte in Mitteldeutschland trafen.

**Was hätte man besser machen können?**
Eine robuste Sicherheitsarchitektur mit automatisierter Angriffserkennung, Echtzeitüberwachung und klaren Eskalationsprozessen kann dazu beitragen, die Auswirkungen von Vorfällen zu begrenzen. Besonders bei ausgelagerten Webdiensten ist es wichtig, technische und organisatorische Schutzmaßnahmen, einschließlich **DDoS-Schutz** – regelmäßig zu prüfen und aufeinander abzustimmen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.mz.de/lokal/wittenberg/cyberangriff-trifft-wittenberg-digitale-dienste-zeitweise-gestort-4090823

**Was lernen wir daraus:**
Der Vorfall zeigt, wie wichtig es ist, digitale Verwaltungsangebote gegen Überlastungsangriffe abzusichern. DDoS-Attacken sind technisch simpel, aber effektiv und sie treffen dort, wo Bürger auf digitale Services angewiesen sind. Kommunen müssen ihre digitale Resilienz strategisch und technisch stärken.


RIEDEL

# Cybercrime-Gruppe „Global“ attackiert Türen- und Torbauer

30. Juli 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

DATENLECK

DATENPANNE

**Was ist passiert?**
Am 30. Juli 2025 wurde ein mittelständisches Unternehmen aus dem Türen- und Torbau Ziel eines Ransomware-Angriffs durch die Cybercrime-Gruppe **Global**. Die Täter behaupten, umfangreiche Daten gestohlen zu haben und drohen mit deren Veröffentlichung, sollte keine Zahlung bis zum 13. August erfolgen.

**Was hätte man besser machen können?**
Ein mehrschichtiger Sicherheitsansatz mit regelmäßigen **Schwachstellenanalysen**, **Endpoint-Überwachung** und verlässlichen Backup-Konzepten kann dazu beitragen, die Angriffsfläche zu reduzieren. Gerade bei KMU ist es wichtig, dass Sicherheitsmaßnahmen nicht nur technisch umgesetzt, sondern auch organisatorisch verankert und in regelmäßigen Abständen überprüft werden.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/10172-Tischlereiunternehmen-Global.PNG

**Was lernen wir daraus:**
Ransomware-Angriffe zielen nicht nur auf große Konzerne – auch spezialisierte Mittelständler geraten zunehmend ins Visier. Der Vorfall zeigt, wie wichtig es ist, sensible Unternehmensdaten systematisch zu schützen und auf Erpressungsszenarien vorbereitet zu sein. Prävention, Transparenz und schnelle Reaktion sind entscheidend für die Schadensbegrenzung.

RIEDEL

# Koordinierte Überlastung: DDoS-Angriff legt kommunale Webportale lahm

29. Juli 2025, in Deutschland

DDoS

AUSFALL

**Was ist passiert?**
Am 29. Juli 2025 wurden die Internetauftritte mehrerer Stadtverwaltungen in Mitteldeutschland zeitweise lahmgelegt. Betroffen waren u. a. Erfurt, Magdeburg, Halberstadt, Lützen und der Burgenlandkreis. Ursache war eine koordinierte **DDoS-Attacke** auf einen gemeinsamen externen Dienstleister mit bis zu **4,5 Mio. Zugriffen** pro Stunde.

**Was hätte man besser machen können?**
Ein abgestimmtes Sicherheitskonzept mit zentralisierter Angriffserkennung, automatisierten Reaktionsabläufen und kontinuierlicher Überwachung kann dazu beitragen, Auswirkungen von Vorfällen zu begrenzen. Gerade bei ausgelagerten Diensten ist es wichtig, dass Sicherheitsstandards – einschließlich **DDoS-Schutz**, durch geeignete Orchestrierung eingehalten und über ein **Security Operations Center** begleitet werden.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.mz.de/lokal/weissenfels/internetseiten-des-burgenlandkreises-und-der-stadt-lutzen-nicht-erreichbar-4090022
https://www.mdr.de/nachrichten/sachsen-anhalt/hacker-angriff-webseiten-kommunen-102.html

**Was lernen wir daraus:**
Der Vorfall zeigt, wie verwundbar kommunale IT-Systeme sind, wenn externe Partner nicht in die Sicherheitsstrategie eingebunden sind. DDoS-Angriffe sind technisch simpel, aber wirkungsvoll und sie treffen dort, wo digitale Grundversorgung beginnt. Nur durch ganzheitliche Ansätze lässt sich die digitale Handlungsfähigkeit öffentlicher Einrichtungen sichern.


RIEDEL

# Autohandelsplattform von Ransomware-Gruppe Everest gelistet

29. Juli 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

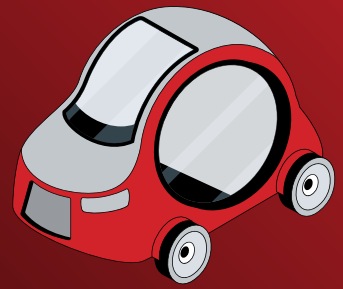
**Was ist passiert?**
Eine Plattform für Fahrzeughandel wurde von der Ransomware-Gruppe **Everest** auf ihrer Darknet-Seite als Opfer genannt. Die Angreifer behaupteten, **109.000 Datensätze** gestohlen zu haben, darunter persönliche Daten und Infos zu gekauften Automodellen. Nach Ablauf einer Frist wurden Links zu mutmaßlichen Leaks veröffentlicht. Die Echtheit ist unbestätigt.

**Was hätte man besser machen können?**
Ein **Security Operations Center (SOC)** in Kombination mit einer **SIEM-Plattform** kann dabei unterstützen, ungewöhnliche Datenbewegungen oder unautorisierte Zugriffe früher sichtbar zu machen und einzuordnen. Ergänzend kann eine **Endpoint Detection & Response (EDR)-Lösung** helfen, auffällige Endpunkte schneller zu identifizieren und geeignete Maßnahmen einzuleiten.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10133-everest.png
https://www.security-incidents.de/assets/img/incidents/10133-Everest-2.png

**Was lernen wir daraus:**
Der gezielte Diebstahl personenbezogener Daten zeigt, wie attraktiv digitale Handelsplattformen für Cyberkriminelle sind. Besonders kritisch: Die Kombination aus Kundendaten und Fahrzeuginformationen kann für Identitätsdiebstahl und Betrug missbraucht werden. Unternehmen mit großen Datenbeständen müssen ihre IT-Sicherheit strategisch aufstellen, mit Fokus auf Prävention, Echtzeitüberwachung und schnelle Reaktion.



RIEDEL

# Pharmaunternehmen von World Leaks unter Druck gesetzt

28. Juli 2025, in Deutschland

DATENDIEBSTAHL

**Was ist passiert?**
Ein deutsches Unternehmen aus der Pharmabranche wurde von der Ransomware-Gruppe **World Leaks** auf deren Darknet-Leakseite als neues Opfer aufgeführt. Die Gruppierung, ehemals unter dem Namen Hunters International aktiv, behauptete vertrauliche Informationen entwendet zu haben. Details zur Art und Menge der Daten wurden nicht veröffentlicht. Dem Unternehmen wurde eine Frist gesetzt, andernfalls drohe die Veröffentlichung der kompromittierten Inhalte.

**Was hätte man besser machen können?**
Ein Security Operations Center (SOC) mit angebundener **Extended Detection & Response (XDR)-Lösung** hätte verdächtige Aktivitäten über verschiedene IT-Komponenten hinweg korrelieren und frühzeitig Alarm schlagen können. Auch ein strukturierter **Incident Response Plan** inklusive klarer Kommunikationswege und technischer Sofortmaßnahmen wäre hilfreich gewesen, um im Ernstfall schnell und koordiniert zu reagieren.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10161-WorldLeaks.png

**Was lernen wir daraus:**
Ransomware-Gruppen arbeiten oft mit Fristen und Drohungen, um Druck auf Unternehmen auszuüben. Besonders in regulierten Branchen wie der Pharmaindustrie kann die Unsicherheit über potenziell geleakte Daten zu erheblichen Reputations- und Compliance-Risiken führen. Eine schnelle, strukturierte Reaktion ist entscheidend, um Schaden zu begrenzen und Vertrauen zu erhalten.

RIEDEL

# Digitale Gemeindesitzung durch Fremdzugriff gestört

25. Juli 2025, in Bodman-Ludwigshafen/Baden-Württemberg

DEFACEMENT

**Was ist passiert?**
Während einer öffentlichen Sitzung wurde eine kommunale Einrichtung Opfer eines digitalen Angriffs: Zwei Unbekannte schalteten sich in die per Videoplattform übertragene Sitzung ein und ersetzten die Präsentation durch extremistische und pornografische Inhalte. Die Störung war im Saal und online sichtbar. Polizei und Staatsschutz ermitteln, die Organisation will künftig eine andere Plattform nutzen.

**Was hätte man besser machen können?**
Der Vorfall hätte durch eine geschützte Zugangskontrolle und eine moderierte Teilnehmerverwaltung verhindert werden können. Ergänzend wäre der Einsatz von **Endpoint Detection & Response (EDR)** sinnvoll gewesen, um ungewöhnliche Aktivitäten auf Endgeräten frühzeitig zu erkennen und automatisiert zu unterbinden.

## Anzunehmende Schadensfelder:

Quellen:
https://www.swr.de/swraktuell/baden-wuerttemberg/friedrichshafen/bei-gemeinderatssitzung-in-bodeman-ludwigshafen-spielen-hacker-porno-ab-100.html
https://www.wochenblatt.net/bodman-ludwigshafen/c-nachrichten/erotikfilme-und-hakenkreuze-bei-gemeinderatsuebertragung-in-bodman-ludwigshafen_a151523

**Was lernen wir daraus:**
Digitale Formate im öffentlichen Raum sind zunehmend Angriffsziel auch ohne klassisch Datendiebstahl-Motive. Der Vorfall zeigt, wie wichtig es ist, selbst bei scheinbar harmlosen Online-Übertragungen auf technische Absicherung und klare Moderationsprozesse zu achten. IT-Sicherheit beginnt nicht erst beim Datenzugriff, sondern bei der Plattformwahl und dem Umgang mit digitalen Schnittstellen.


RIEDEL

# Etikettenhersteller von DragonForce auf Leaksite genannt – 66 GB Daten betroffen

25. Juli 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

DATENLECK

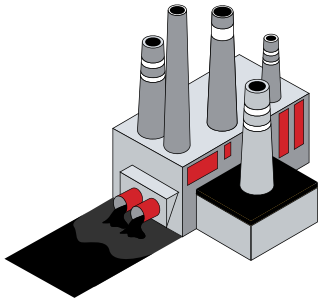
**Was ist passiert?**
Ein deutscher Hersteller von Etiketten wurde von der Ransomware-Gruppe **DragonForce** am 25. Juli 2025 auf deren Leaksite als Opfer aufgeführt. Die Angreifer behaupten, **66 GB** vertraulicher Unternehmensdaten exfiltriert zu haben. Die angeblichen Inhalte sind laut Gruppe über deren Darknet-Blog einsehbar. Ob und welche konkreten Daten betroffen sind, ist nicht bestätigt.

**Was hätte man besser machen können?**
Ein Angriff dieser Art hätte durch den Einsatz eines **Security Operations Center (SOC)** mit angebundener **SIEM-Plattform** möglicherweise frühzeitig erkannt und eingedämmt werden können. Auch eine automatisierte Reaktion über **Security Orchestration, Automation and Response (SOAR)** hätte geholfen, verdächtige Aktivitäten direkt zu isolieren und Folgeeffekte zu minimieren.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10162-Dragonforce.png

**Was lernen wir daraus:**
Der Fall zeigt, dass auch spezialisierte Produktionsbetriebe mit digitalisierten Prozessen zunehmend ins Visier von Ransomware-Gruppen geraten. Selbst ohne bestätigte Datenveröffentlichung kann die öffentliche Nennung auf Leakseiten zu Unsicherheit bei Kunden und Partnern führen. Prävention und schnelle Reaktion sind entscheidend, um Vertrauen zu erhalten und Folgeschäden zu vermeiden.



RIEDEL

# Cyberangriff auf S-Bahn-Betreiber sorgt für Ausfälle

24. Juli 2025, in Hannover/Niedersachsen

EINBRUCH

AUSFALL

**Was ist passiert?**
Eine Organisation aus dem öffentlichen Verkehrssektor wurde Ziel eines IT-Sicherheitsvorfalls. Die zentrale Website war über zwei Stunden nicht erreichbar, was die digitale Kommunikation beeinträchtigte. Laut Medienberichten handelte es sich um einen gezielten Einbruch, der früh erkannt und abgewehrt wurde. Bereits zwei Wochen zuvor war die Organisation von einer **DDoS-Attacke** betroffen.

**Was hätte man besser machen können?**
Zur Abwehr solcher Störungen ist eine robuste **DDoS-Schutzlösung** essenziell, etwa durch vorgelagerte Filterdienste und intelligente Lastverteilung. Ergänzend hätte ein **Security Information & Event Management (SIEM)-System** verdächtige Muster frühzeitig erkennen und automatisiert Alarm schlagen können. Auch eine redundante Infrastruktur für kritische Webdienste wäre hilfreich gewesen, um die Verfügbarkeit zu sichern.

## Anzunehmende Schadensfelder:

Quellen:
https://www.haz.de/lokales/hannover/hackerangriff-website-der-s-bahn-hannover-nicht-erreichbar-4FLKZCLGQZBAHAYXZSAKM4J6CM.html
https://www.t-online.de/region/hannover/id_100835350/cyberangriff-hannover-hacker-legen-s-bahn-website-fuer-zwei-stunden-lahm.html

**Was lernen wir daraus:**
Wiederholte Angriffe auf öffentliche Verkehrsunternehmen zeigen, wie wichtig es ist, digitale Resilienz nicht nur technisch, sondern auch organisatorisch zu denken. Eine schnelle Reaktion ist gut, aber nachhaltiger Schutz entsteht durch vorausschauende Planung, klare Zuständigkeiten und kontinuierliche Überwachung. Besonders bei kritischer Infrastruktur zählt jede Minute.


RIEDEL

# Gesundheitsverband von Ransomware-Gruppe BrainCipher attackiert – 1 TB Daten betroffen

24. Juli 2025, in Baden-Württemberg

RANSOMWARE

DATENDIEBSTAHL

DATENLECK

AUSFALL

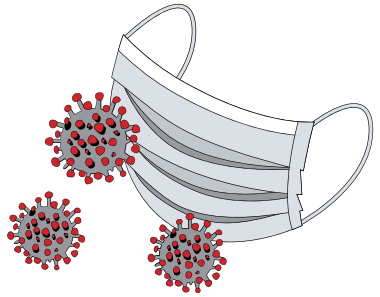
**Was ist passiert?**
Ein gemeinnütziger Landesverband im Gesundheitswesen wurde von der Ransomware-Gruppe **BrainCipher** auf einer Darknet-Leakseite gelistet. Die Angreifer behaupteten, rund **1 Terabyte** Daten entwendet zu haben, darunter vermutlich sensible Informationen. Die Patientenversorgung blieb gewährleistet, dennoch kam es zu digitalen Einschränkungen. Eine Untersuchung wurde eingeleitet, die Datenlage blieb unklar.

**Was hätte man besser machen können?**
Organisationen im Gesundheitsbereich sollten besonders auf die Absicherung ihrer digitalen Infrastruktur achten. Ein **Security Operations Center (SOC)** mit angebundener **SIEM-Plattform** kann helfen, auffällige Aktivitäten früher zu erkennen und geeignete Maßnahmen einzuleiten. Ergänzend tragen **regelmäßiges Schwachstellenmanagement**, verschlüsselte Backups und eine klare Netzwerksegmentierung dazu bei, Risiken zu begrenzen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10231-BaWue_Pr%C3%A4vention-BrainCipher.PNG
https://www.security-incidents.de/assets/img/incidents/10231-BaWue_Pr%C3%A4vention-BrainCipher2.PNG

**Was lernen wir daraus:**
Der Vorfall zeigt, wie verletzlich auch gemeinnützige Organisationen im Gesundheitswesen gegenüber gezielten Cyberangriffen sind. Selbst wenn die Versorgung nicht direkt betroffen ist, können digitale Einschränkungen und Unsicherheit über den Datenabfluss zu Vertrauensverlust und organisatorischen Belastungen führen. IT-Sicherheit muss auch hier als Teil der Daseinsvorsorge verstanden und strategisch verankert werden.



RIEDEL

# Camper-Spezialist im Visier von Ransomware-Gruppe – 53 GB sensible Daten betroffen

23. Juli 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

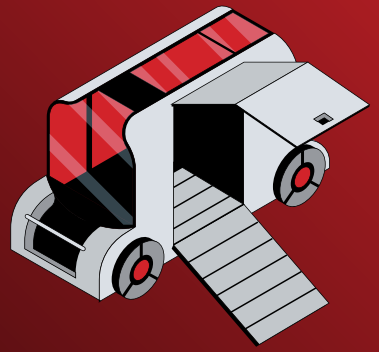
**Was ist passiert?**
Ein Hersteller, spezialisiert auf Wohnmobil- und Camper-Umbauten, wurde von der Ransomware-Gruppe **Akira** auf ihrer Darknet-Leakseite als Opfer gelistet. Die Angreifer behaupten, rund **53 GB** an vertraulichen Unternehmensdaten gestohlen zu haben, darunter personenbezogene Mitarbeiterinformationen, Projekt- und Kundendaten, Finanzunterlagen sowie Geheimhaltungsvereinbarungen (NDAs).

**Was hätte man besser machen können?**
Unternehmen mit komplexen Projekten und sensiblen Kundendaten benötigen klare Zugriffskontrollen und datenklassifizierte Sicherheitsmaßnahmen. Ein **XDR-System** hätte verdächtige Aktivitäten frühzeitig erkennen können. Ebenso wären regelmäßige Security Audits zur Prüfung von Datenflüssen und Backup-Strategien sinnvoll gewesen.

## Anzunehmende Schadensfelder:

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

**Was lernen wir daraus:**
Der Fall zeigt, dass auch spezialisierte Mittelständler mit hohem Individualisierungsgrad im Produktportfolio ein attraktives Ziel für Ransomware-Gruppen sind. Besonders kritisch: Der Diebstahl von NDAs und Finanzdaten kann nicht nur rechtliche Folgen haben, sondern auch das Vertrauen von Geschäftspartnern nachhaltig beschädigen. Wer personenbezogene und projektbezogene Daten verarbeitet, muss deren Schutz strategisch priorisieren.



RIEDEL

# Ransomware-Gruppe listet Missions- und Bildungswerk als Opfer im Darknet

22. Juli 2025, in Deutschland

DATENDIEBSTAHL

RANSOMWARE

**Was ist passiert?**
Ein evangelisches Bildungs- und Missionswerk wurde von der Ransomware-Gruppe **INC Ransom** auf einer Darknet-Leakseite als Opfer gelistet. Die Angreifer machten keine Angaben zur Art oder Menge der gestohlenen Daten und nannten bislang kein Datum für eine mögliche Veröffentlichung.

**Was hätte man besser machen können?**
Organisationen mit sensibler gesellschaftlicher Rolle sollten ihre IT-Infrastruktur regelmäßig auf Schwachstellen prüfen, etwa durch ein **Vulnerability Assessment**. Auch ein **Security Orchestration & Response (SOAR)-System** hätte helfen können, verdächtige Muster automatisiert zu erkennen und schnell zu reagieren. Besonders bei Einrichtungen mit hohem Vertrauensanspruch ist eine klare Rollenvergabe bei Zugriffsrechten und eine robuste Backup-Strategie essenziell.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10067-inc-ransom.png

**Was lernen wir daraus:**
Auch gemeinnützige und religiöse Organisationen sind längst keine Randziele mehr für Cyberkriminelle. Der Fall zeigt, wie wichtig es ist, IT-Sicherheit nicht nur als technische Maßnahme zu verstehen, sondern als Teil der institutionellen Verantwortung gegenüber Mitarbeitenden, Partnern und der Öffentlichkeit. Unklarheiten über den Datenabfluss können zu Vertrauensverlust und Reputationsschäden führen, selbst ohne konkrete Veröffentlichung.

RIEDEL

# Koordinierte Ransomware-Angriffe durch „World Leaks“ – über 4 TB Daten gestohlen

22. Juli 2025, in Deutschland

DATENDIEBSTAHL

DATENLECK

**Was ist passiert?**
Am 22. Juli 2025 listete die Ransomware-Gruppe **World Leaks** drei gehackte deutsche Unternehmen auf ihrer Darknet-Leakseite: ein Robotikhersteller **(3,2 TB Daten)**, ein Sanitätshaus **(700 GB)** und eine Rechtsanwaltskanzlei. In allen Fällen wurden mutmaßlich sensible Kunden-, Mitarbeiter- und Geschäftsdaten gestohlen und veröffentlicht.

**Was hätte man besser machen können?**
Die Angriffe zeigen, wie wichtig eine ganzheitliche Sicherheitsstrategie ist. Ein **Security Operations Center (SOC)** mit Echtzeitüberwachung hätte verdächtige Aktivitäten frühzeitig erkennen und eindämmen können. Ergänzend wären regelmäßige **Schwachstellenanalysen**, Zero-Trust-Architekturen und verschlüsselte Backups essenziell gewesen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10074-world-leaks.png
https://www.security-incidents.de/assets/img/incidents/10075-world-leaks.png

**Was lernen wir daraus:**
Die koordinierte Veröffentlichung mehrerer Opfer an einem Tag deutet auf eine systematische Kampagne hin. Unternehmen jeder Größe und Branche müssen damit rechnen, ins Visier zu geraten. Wer keine zentrale Sicherheitsüberwachung etabliert und grundlegende Schutzmaßnahmen vernachlässigt, läuft Gefahr, Angriffe zu spät zu erkennen und empfindliche Daten zu verlieren. Besonders kritisch: Die Veröffentlichung im Darknet erhöht den Druck auf die Opfer und kann zu erheblichen Reputations- und Folgeschäden führen.

RIEDEL

# Gezielter Cyberangriff auf Verlagshaus

22. Juli 2025, in Stuttgart/Baden-Württemberg

EINBRUCH

**Was ist passiert?**
Am 22. Juli kam es bei einer großen Medienholding zu einem kritischen IT-Sicherheitsvorfall. Unbefugte drangen in interne Systeme ein, woraufhin sofortige Schutzmaßnahmen eingeleitet wurden. Digitale Angebote waren zeitweise eingeschränkt, die Printausgaben erschienen planmäßig. Hinweise auf Datenabfluss oder Erpressung liegen bislang nicht vor. Die Ermittlungen laufen in Zusammenarbeit mit den Behörden.

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

**Anzunehmende Schadensfelder:**

Quellen:
https://www.swr.de/swraktuell/baden-wuerttemberg/stuttgart/stuttgarter-zeitung-nachrichten-hacker-angriff-100.html
https://www.sn.at/panorama/medien/hackerangriff-suedwestdeutsche-medienholding-181772656

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

RIEDEL

# Phishing-Angriff auf Berufsorganisation – sensible Mitgliedsdaten betroffen

22. Juli 2025, in Bochum/Nordrhein-Westfalen

PHISING

DATENDIEBSTAHL

EINBRUCH

**Was ist passiert?**
Eine Berufsorganisation wurde Ziel eines Phishing-Angriffs. Drei E-Mail-Konten von Mitarbeitenden wurden kompromittiert, worüber weitere Phishing-Nachrichten versendet wurden. Zunächst wurde das Risiko als gering eingestuft, später kam es jedoch zu einem Betrugsversuch unter Verwendung interner Informationen. Betroffen sind unter anderem Namen, Kontaktdaten, E-Mail-Inhalte sowie Angaben zur politischen Meinung und Gewerkschaftszugehörigkeit.

**Was hätte man besser machen können?**
Ein Security Operations Center (SOC) kann dazu beitragen, ungewöhnliche Aktivitäten rund um kompromittierte E-Mail-Konten früher zu erkennen und geeignete Maßnahmen einzuleiten. Ebenso wichtig sind **regelmäßige Schulungen**, um das Bewusstsein für Phishing und Social Engineering zu stärken. Technische Schutzmaßnahmen wirken am besten, wenn auch die menschliche Komponente entsprechend sensibilisiert ist.

## Anzunehmende Schadensfelder:

Quellen:
https://www.vmf-online.de/download/information-cyberangriff-22-07-2025

**Was lernen wir daraus:**
Phishing bleibt einer der effektivsten Angriffsvektoren – besonders bei Organisationen mit sensiblen Mitgliedsdaten. Der Fall zeigt, wie wichtig es ist, nicht nur technische Schutzmaßnahmen zu etablieren, sondern auch klare Prozesse zur Risikobewertung und Kommunikation zu definieren. Frühzeitige Erkennung und transparente Reaktion sind entscheidend, um Vertrauen zu erhalten und Folgeschäden zu begrenzen.


RIEDEL

# 100 GB Daten veröffentlicht: Steuerberatungskanzlei geriet ins Visier

22. Juli 2025, in Nordrhein-Westfalen

RANSOMWARE

DATENDIEBSTAHL

DATENLECK

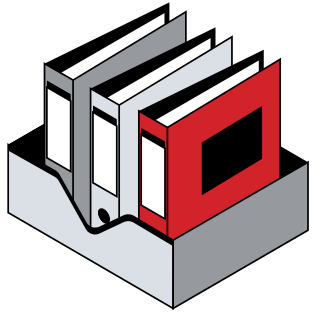
**Was ist passiert?**
Eine Steuerberatungskanzlei aus dem Rhein-Ruhr-Gebiet wurde von der Ransomware-Gruppe **Cloak** auf deren Leaksite gelistet. Zunächst wurde nur eine anonymisierte Domain genannt, später folgte die vollständige Webadresse sowie rund **100 GB** an gestohlenen Geschäftsdaten als Download. Angaben zur Reaktion des Unternehmens liegen bislang nicht vor.

**Was hätte man besser machen können?**
Gerade bei Kanzleien mit sensiblen Mandantendaten ist eine frühzeitige Erkennung entscheidend. Ein **Security Operations Center (SOC)** hätte verdächtige Aktivitäten rund um die Uhr überwachen und automatisiert reagieren können. Ergänzend wäre eine **Security Orchestration, Automation and Response (SOAR)-Lösung** sinnvoll gewesen, um bei einem Angriff sofort Gegenmaßnahmen einzuleiten und die Ausbreitung zu stoppen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10284-Cloak-Steuerberatungskanzlei.png

**Was lernen wir daraus:**
Steuerkanzleien sind besonders attraktive Ziele für Ransomware-Gruppen – nicht wegen ihrer Größe, sondern wegen der Daten, die sie verwalten. Der Fall zeigt, wie wichtig es ist, nicht nur technische Schutzmaßnahmen zu etablieren, sondern auch klare Reaktionsprozesse zu definieren. Wer frühzeitig erkennt und automatisiert reagiert, kann den Schaden begrenzen und Vertrauen bewahren.



RIEDEL

# Cyberangriff legt Vertrieb bundesweit lahm

17. Juli 2025, in Frankfurt a.M./Hessen

ERPRESSUNG

AUSFALL

EINBRUCH

SUPPLY CHAIN

**Was ist passiert?**
Ein Cyberangriff auf einen bekannten Telekommunikationsanbieter hat das zentrale Vertriebsportal lahmgelegt. Der Vorfall beeinträchtigt bundesweit Vertragsabschlüsse und Kundenberatungen. Obwohl die internen Systeme laut Unternehmen nicht betroffen sind, gibt es Kritik an der mangelnden Kommunikation des Unternehmens bezüglich Schwere und Dauer der Einschränkungen.

**Was hätte man besser machen können?**
Eine durchgängige Sicherheitsüberwachung durch ein **Security Operations Center (SOC)** wäre hier sinnvoll gewesen, das auch externe Partnerstrukturen einbezieht. Ergänzend hätte ein **Extended Detection and Response (XDR)-System** helfen können, verdächtige Aktivitäten über verschiedene IT-Komponenten hinweg frühzeitig zu erkennen und automatisiert darauf zu reagieren, bevor kritische Plattformen wie das Vertriebsportal Ausfallen.

## Anzunehmende Schadensfelder:

Quellen:
https://www.it-daily.net/shortnews/cyberangriff-auf-vodafone
https://www.telecom-handel.de/consumer-communications/vodafone/vodafone-kappt-zugang-sales-world-2967553.html

**Was lernen wir daraus:**
Cyberangriffe auf Dienstleister können sich direkt auf die operative Leistungsfähigkeit großer Konzerne auswirken – selbst wenn deren eigene Systeme nicht kompromittiert sind. Der Fall zeigt, wie wichtig es ist, auch externe Partner in die Sicherheitsstrategie einzubeziehen. Transparente Kommunikation, technische Resilienz und ein vorausschauendes Sicherheitskonzept sind entscheidend, um Vertrauen zu erhalten und Schäden zu begrenzen.


RIEDEL

# Handwerksunternehmen im Visier von Cyberkriminellen

17. Juli 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**

Am 17. Juli 2025 wurde ein Zimmermannsunternehmen von der Ransomware-Gruppe **Pear** auf deren Leaksite als Opfer gelistet. Die Angreifer veröffentlichten eine angebliche Datenbeute, machten jedoch keine weiteren Angaben zum Umfang oder Inhalt. Auch das Unternehmen selbst äußerte sich nicht öffentlich zum Vorfall.

**Was hätte man besser machen können?**

In diesem Fall hätte ein kontinuierliches Schwachstellenmanagement, etwa durch ein regelmäßiges **Vulnerability Assessment**, potenzielle Einfallstore frühzeitig sichtbar gemacht. Ergänzend wäre der Einsatz eines **Endpoint Detection & Response (EDR)-Systems** sinnvoll gewesen, um verdächtige Aktivitäten auf Endgeräten zu erkennen und automatisiert zu unterbinden – bevor Daten exfiltriert werden können.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10245-pear.png

**Was lernen wir daraus:**

Auch kleine und mittelständische Handwerksbetriebe sind längst keine Randziele mehr für Cyberkriminelle. Der Fall zeigt, dass selbst ohne konkrete Angaben zur Datenmenge bereits die Nennung auf einer Leaksite erheblichen Druck erzeugt. Wer keine grundlegenden Schutzmaßnahmen wie Zugriffskontrollen, Endgeräteüberwachung oder regelmäßige Schwachstellenanalysen etabliert hat, läuft Gefahr, im Ernstfall handlungsunfähig zu sein.

RIEDEL

# Gaming-Plattform von Datenleak betroffen – Klartext-Passwörter kursieren auf Telegram

15. Juli 2025, in Franktfurt a.M./Hessen

DATENLECK

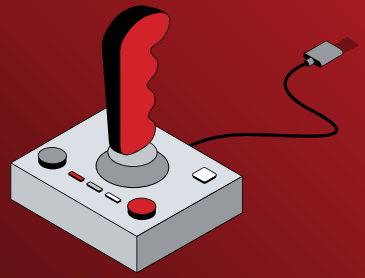
**Was ist passiert?**
Bei einer deutschen Gaming-Plattform kursierten seit Anfang Juli Nutzerdaten auf Telegram, darunter E-Mail-Adressen und Klartext-Passwörter. Die Betreiber bestritten ein aktuelles internes Datenleck und identifizierten die Daten als Altlasten aus einem früheren Breach sowie aus Infostealer-Logs. Ein internationaler Sicherheitsexperte bestätigte diese Einschätzung. Als Reaktion wurden Passwort-Resets erzwungen und die Aktivierung von Zwei-Faktor-Authentifizierung empfohlen.

**Was hätte man besser machen können?**
Bei Plattformen mit vielen Nutzerkonten ist eine frühzeitige Erkennung entscheidend. Ein regelmäßiges **Vulnerability Assessment** hätte unsichere Speicherorte oder veraltete Authentifizierungsmechanismen aufdecken können. Ergänzend hätte ein **SIEM-System** verdächtige Aktivitäten wie massenhafte Login-Versuche oder Datenabflüsse frühzeitig erkannt und automatisiert Gegenmaßnahmen eingeleitet.

## Anzunehmende Schadensfelder:

Quellen:
https://www.heise.de//news/Moegliches-datenleck-bei-Minecraft-Server-GommeHD-10487200.html

**Was lernen wir daraus:**
Auch veraltete Datenbestände können Jahre später noch Schaden anrichten – besonders wenn Passwörter im Klartext gespeichert wurden. Der Fall zeigt, wie wichtig es ist, Zugangsdaten regelmäßig zu prüfen, kompromittierte Accounts frühzeitig zu sperren und Nutzer aktiv zur Absicherung ihrer Konten zu befähigen. IT-Sicherheit endet nicht mit dem Vorfall, sie beginnt mit nachhaltiger Prävention.



RIEDEL

# Ransomware-Angriffe: Umfangreicher Datenabfluss veröffentlicht

15. Juli 2025, in Deutschland

RANSOMWARE

DATENDIEBSTAHL

DATENLECK

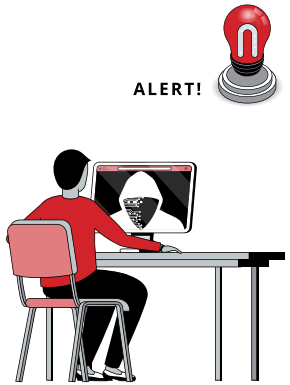
**Was ist passiert?**
Mitte Juli 2025 wurden zwei regionale Unternehmen in Deutschland Ziel von der Ransomware-Gruppe **DragonForce**. Betroffen waren unter anderem ein Farbenfachhändler sowie ein Immobilienunternehmen. Die Angreifer listeten beide Organisationen auf ihrer Leak-Seite und behaupteten, insgesamt rund **126 Gigabyte** vertraulicher Unternehmensdaten exfiltriert zu haben, von denen Teile öffentlich zugänglich gemacht wurden.

**Was hätte man besser machen können?**
Gerade bei mittelständischen Betrieben mit umfangreichen Kunden- und Geschäftsdaten ist eine frühzeitige Erkennung entscheidend. In diesem Fall hätte eine **strukturierte Datenklassifizierung** dabei geholfen, besonders sensible Informationen gezielt zu schützen – etwa durch abgestufte Zugriffsrechte und Verschlüsselung. Ergänzend wäre ein regelmäßiger **Schwachstellenscan** sinnvoll gewesen, um potenzielle Einfallstore in der IT-Infrastruktur frühzeitig zu identifizieren.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10055-Dragonforce.png
https://www.security-incidents.de/assets/img/incidents/9999-Dragonforce.png

**Was lernen wir daraus:**
Die Veröffentlichung großer Datenmengen im Darknet zeigt, dass Angreifer nicht nur auf Konzerne abzielen, sondern gezielt Schwachstellen bei kleineren Unternehmen ausnutzen. Wer keine automatisierten Schutzmechanismen etabliert hat, riskiert nicht nur Datenverlust, sondern auch langfristige Vertrauensschäden bei Kunden und Partnern.




RIEDEL

# Defaced & Exposed: Hacker zeigen mehr als nur Headlines

13. Juli 2025, in Berlin/Berlin

DEFACEMENT

DATENLECK

**Was ist passiert?**
Ein Nachrichtenportal wurde Ziel eines **Defacement-Angriffs**. Die Angreifer ersetzten sämtliche Überschriften der Website durch einen Link zu .json-Dateien, die mutmaßlich personenbezogene Daten von rund **5.700 Abonnenten** enthielten, darunter Namen, E-Mail-Adressen, verkürzte Zahlungsdaten und Abo-Informationen. Auch technische Details zur verwendeten Webinfrastruktur wurden veröffentlicht. Die Daten waren zeitweise abrufbar, später bestätigte der Betreiber deren Echtheit.

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

## Anzunehmende Schadensfelder:

Quellen:
https://www.heise.de/news/Cyberangriff-auf-nius-de-mutmasslich-Nutzerdaten-veroeffentlicht-10485362.html
https://www.it-daily.net/shortnews/hacker-angriff-nius-de

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


RIEDEL

# Cyberangriff auf Explosionsschutz-Hersteller

12. Juli 2025, in Bad Mergentheim/Baden-Württemberg

RANSOMWARE

DATENDIEBSTAHL

**Was ist passiert?**
Am 12. Juli 2025 wurde ein weltweit tätiger Hersteller für Sicherheitstechnik im Bereich Explosionsschutz Opfer eines Ransomware-Angriffs. Die Hackergruppe **Safepay** listete das Unternehmen auf ihrer Leaksite im Darknet und behauptet, rund **21 GB** sensibler Unternehmensdaten exfiltriert zu haben, darunter offenbar technische Dokumentationen, interne Präsentationen und Geschäftsdaten. Das Unternehmen bestätigte den Vorfall später und verwies auf einen betroffenen Server im Ausland.

**Was hätte man besser machen können?**
Durch eine frühere Erkennung ungewöhnlicher Aktivitäten auf Servern sowie eine kontinuierliche Überwachung verteilter IT-Umgebungen hätten Auffälligkeiten möglicherweise schneller sichtbar werden können. Eine zentrale Auswertung sicherheitsrelevanter Ereignisse und eine abgestimmte Reaktion über Lösungen wie **SIEM und SOC** können dabei unterstützen, potenzielle Vorfälle früher einzuordnen und geeignete Maßnahmen einzuleiten.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/9987-Safepay.png

**Was lernen wir daraus:**
Internationale IT-Strukturen sind besonders anfällig für gezielte Angriffe, insbesondere, wenn lokale Sicherheitsstandards variieren. Der Vorfall zeigt, wie wichtig es ist, auch entfernte Standorte in ein zentrales Sicherheitskonzept zu integrieren. Moderne Ransomware-Gruppen setzen auf Druck durch Fristen und Datenleaks – wer vorbereitet ist, kann schneller reagieren und Schäden begrenzen.

RIEDEL

# Ransomware-Gruppe Incransom erpresst Tiergesundheitszentrum

10. Juli 2025, in Königslutter/Niedersachsen

RANSOMWARE

DATENDIEBSTAHL

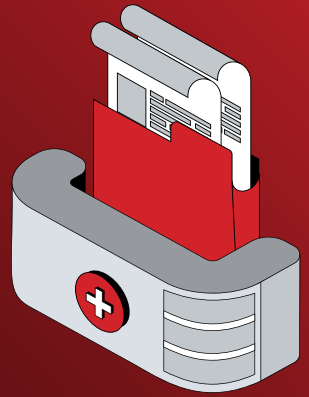
**Was ist passiert?**
Anfang Juli 2025 wurde ein Tiergesundheitszentrum Opfer eines Ransomware-Angriffs durch die Gruppe **Incransom**. Die Angreifer behaupten, rund **12 GB** sensibler Daten exfiltriert zu haben, darunter vermutlich Patienteninformationen, interne Dokumente und Geschäftsdaten.

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

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/9967-incransom-Tierarztpraxis.PNG

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



RIEDEL

# Phishing-Angriff auf Landratsamt: Mitarbeiterkonten kompromittiert

10. Juli 2025, in Odenwaldkreis/Hessen

PHISING

DATENPANNE

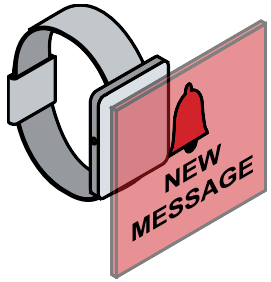
**Was ist passiert?**
Eine kommunale Verwaltungsbehörde wurde Ziel einer **Phishing-Attacke**. Mitarbeitende gaben ihre Zugangsdaten auf einer gefälschten Webseite ein, wodurch Angreifer Zugriff auf mehrere interne Benutzerkonten erlangen konnten. Nach Bekanntwerden des Vorfalls leitete die Verwaltung umgehend Gegenmaßnahmen ein und sperrte die betroffenen Accounts.

**Was hätte man besser machen können?**
Eine stärkere Sensibilisierung und regelmäßige **Schulungen der Mitarbeitenden** im Umgang mit verdächtigen E-Mails und Anmeldeaktivitäten sowie **klarere interne Meldewege** hätten zur früheren Erkennung möglicher Risiken beitragen können. Ergänzende technische Maßnahmen hätten zudem helfen können, unbefugte Zugriffe schneller zu begrenzen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.odenwaldkreis.de/de/pressemitteilungen/2025/juli/it-sicherheitsvorfall-im-landratsamt/

**Was lernen wir daraus:**
Regelmäßige Schulungen, technische Schutzmechanismen für Benutzerkonten und klar geregelte Reaktionsprozesse hätten dazu beitragen können, den Umfang des Zugriffs zu begrenzen und potenzielle Folgeschäden frühzeitig zu minimieren.




RIEDEL

# Politisch motivierte DDoS-Angriffe auf öffentliche Verwaltung in Deutschland

10. Juli 2025, in Deutschland

DDoS

HACKTIVISMUS

AUSFALL

**Was ist passiert?**
Es kam zu mehreren **DDoS-Angriffen** auf Webseiten öffentlicher Einrichtungen in Deutschland. Betroffen waren unter anderem das Online-Portal einer Großstadt sowie mehrere Ministerien eines Bundeslandes. Die Angriffe führten zeitweise zu eingeschränkter Erreichbarkeit zentraler Webseiten und Bürger-Portale. Spätere Ermittlungen führten die Angriffe auf die politisch motivierte Gruppe **NoName057(16)** zurück.

**Was hätte man besser machen können?**
Zur Abwehr solcher Angriffe wäre der Einsatz eines Security Information and **Event Management (SIEM)-Systems** hilfreich gewesen, um ungewöhnliche Zugriffsmuster frühzeitig zu erkennen. Ergänzend hätte eine **Security Orchestration, Automation and Response (SOAR)-Lösung** automatisiert Gegenmaßnahmen einleiten können – etwa die dynamische Filterung von schädlichem Datenverkehr oder die Umleitung auf redundante Systeme.

## Anzunehmende Schadensfelder:

Quellen:
https://www.odenwaldkreis.de/de/pressemitteilungen/2025/juli/it-sicherheitsvorfall-im-landratsamt/

**Was lernen wir daraus:**
DDoS-Angriffe auf öffentliche Einrichtungen sind längst nicht mehr nur technische Störungen, sondern Teil gezielter politischer Einflussnahme. Sie zielen auf die digitale Handlungsfähigkeit und das Vertrauen der Bevölkerung. Der Fall zeigt, wie wichtig es ist, digitale Verwaltungsstrukturen resilient zu gestalten – durch vorausschauende Sicherheitsarchitektur, automatisierte Reaktionsmechanismen und klare Kommunikationsstrategien im Ernstfall.


RIEDEL

# Zugriff entgleist: DDoS-Attacke legt S-Bahn-Website lahm

9. Juli 2025, in Hannover/Niedersachsen

DDoS

AUSFALL

**Was ist passiert?**
Am 9. Juli 2025 wurde die Website eines deutschen Ziel einer DDoS-Attacke. Die massenhaften Zugriffe übeVerkehrsunternehmensrlasteten den Server, woraufhin der Betreiber Sicherheitsfilter aktivierte, die auch zeitweise legitime Nutzeranfragen blockierten. IT-Spezialisten konnten die Systeme einen Tag später stabilisieren.

**Was hätte man besser machen können?**
DDoS-Angriffe zielen auf die Verfügbarkeit und treffen insbesondere öffentliche Dienste besonders hart. Eine skalierbare Infrastruktur mit automatischer Lastverteilung, kombiniert mit **Security Orchestration, Automation and Response (SOAR)**, hätte die Angriffsfläche reduziert und die Reaktionszeit verkürzt. Ergänzend wären **SIEM-Systeme** zur Echtzeiterkennung sowie regelmäßige **Vulnerability Assessments** zur präventiven Absicherung sinnvoll gewesen.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.ndr.de/nachrichten/niedersachsen/hannover_weser-leinegebiet/nach-cyberattacke-website-der-s-bahn-hannover-wieder-erreichbar,sbahn-106.html
https://www.schiene.de/news-9442/Website-der-S-Bahn-Hannover-nach-Angriff-wieder-erreichbar.html

**Was lernen wir daraus:**
DDoS-Angriffe sind oft der Einstieg in komplexere Bedrohungsszenarien oder dienen als Ablenkung. Gerade bei öffentlichen Plattformen ist eine robuste IT-Architektur entscheidend. Unternehmen sollten nicht nur auf Schutz, sondern auch auf schnelle Wiederherstellung setzen. Proaktive Überwachung, klare Notfallpläne und automatisierte Reaktionen sind heute Pflicht.


RIEDEL

# Technischer Ausfall legt Notaufnahmen lahm

8. Juli 2025, in Reutlingen/Baden-Württemberg

STROMAUSFALL

AUSFALL

**Was ist passiert?**
Infolge eines Kurzschlusses kam es zu einem IT-Ausfall in zwei Kreiskliniken. Telefone und Computer funktionierten zwischenzeitlich nicht und auch die Notaufnahmen mussten vorübergehend schließen, geplante Operationen wurden abgesagt. Der Ausfall dauerte rund fünf Stunden. Laut Klinikleitung handelte es sich um ein **technisches Versagen** und nicht um einen Cyberangriff.

**Was hätte man besser machen können?**
Durch eine stärkere technische Resilienz der IT-Infrastruktur, redundante Systeme sowie regelmäßige Überprüfungen kritischer Komponenten hätte die Ausfallzeit möglicherweise reduziert werden können. Klare **Notfall- und Wiederanlaufpläne** hätten dazu beigetragen, medizinische Prozesse schneller zu stabilisieren und Patientenversorgung gezielter abzusichern.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.tagesschau.de/inland/regional/badenwuerttemberg/swr-technischer-ausfall-in-den-kliniken-reutlingen-und-muensingen-100.html
https://www.swr.de/swraktuell/baden-wuerttemberg/tuebingen/technischer-ausfall-kreisklinik-reutlingen-100.html

**Was lernen wir daraus:**
Durch eine stärkere technische Resilienz der IT-Infrastruktur, redundante Systeme sowie regelmäßige Überprüfungen kritischer Komponenten hätte die Ausfallzeit möglicherweise reduziert werden können. Klare Notfall- und Wiederanlaufpläne hätten dazu beigetragen, medizinische Prozesse schneller zu stabilisieren und Patientenversorgung gezielter abzusichern.

RIEDEL

# Ransomware-Angriff auf Münchener Technologiekonzern

07. Juli 2025, in München/Bayern

RANSOMWARE

DATENDIEBSTAHL

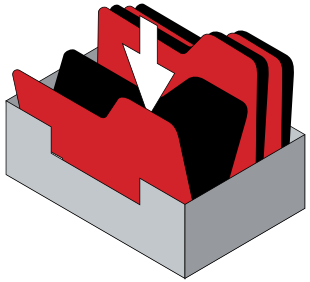
**Was ist passiert?**
Ein international tätiger Automotive- und Industrie-Technologie-Lieferant mit Sitz in München wurde im Juli 2025 Ziel eines Ransomware-Angriffs durch **Payoutsking**. Die Täter listeten das Unternehmen auf ihrem Opferblog und behaupteten, rund **2,5 Terabyte** sensibler Firmendaten kompromittiert zu haben. Erste Dateien wurden als Beleg veröffentlicht. Nach Ablauf einer Frist drohte die vollständige Offenlegung der Daten.

**Was hätte man besser machen können?**
Durch eine ganzheitliche Sicherheitsstrategie mit kontinuierlicher Überwachung kritischer Systeme und einer strukturierten Analyse von Sicherheitsereignissen hätten verdächtige Aktivitäten früher erkannt werden können. Eine zentrale Auswertung von Logdaten sowie ein professionelles Incident-Handling, unterstützt durch **SIEM und ein SOC**, hätten die Reaktionsfähigkeit verbessert und den Schaden begrenzen können.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.security-incidents.de/assets/img/incidents/10001-Payoutsking.jpg

**Was lernen wir daraus:**
Eine verbesserte Transparenz über Datenabflüsse, klar definierte Eskalationsprozesse sowie eine regelmäßige Überprüfung von Zugriffsrechten und Backup-Strategien hätten dazu beitragen können, die Folgen des Angriffs frühzeitig einzugrenzen.



RIEDEL

# Vertrauliche Daten bei Automobilzulieferer abgeflossen

05. Juli 2025, in Nordrhein-Westfalen

RANSOMWARE

DATENDIEBSTAHL

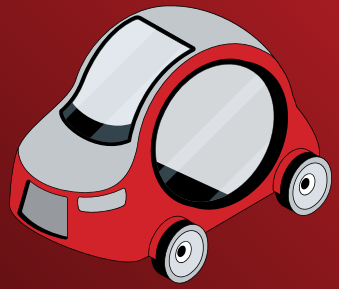
**Was ist passiert?**
Ein auf Oberflächenbeschichtung spezialisierter Automobilzulieferer aus Nordrhein-Westfalen wurde am 5. Juli 2025 Ziel eines Ransomware-Angriffs. Die Hackergruppe **Devman** veröffentlichte das Unternehmen auf ihrem Opferblog im Darknet. Laut den Angaben der Angreifer wurden dabei vertrauliche Daten wie Finanzberichte, Mitarbeiterinformationen, Präsentationen und Bilder entwendet.

**Was hätte man besser machen können?**
Zum besseren Schutz sensibler Unternehmensdaten könnte kontinuierliches Sicherheitsmonitoring **SOC** eingesetzt werden. Damit lassen sich ungewöhnliche Aktivitäten in Echtzeit erkennen, potenzielle Angriffe schneller identifizieren und Gegenmaßnahmen einleiten. So können Risiken wie Datenverlust, unbefugter Zugriff oder längere Betriebsunterbrechungen deutlich reduziert werden.

## Anzunehmende Schadensfelder:

Quellen:
https://www.security-incidents.de/assets/img/incidents/9947-Devman.png

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



RIEDEL

# IT-Störung im Eventzentrum – Betrieb läuft weiter

03. Juli 2025, in Saarbrücken/Saarland

EINBRUCH

AUSFALL

**Was ist passiert?**
Anfang Juli kam es zu einem Cyberangriff auf das Netzwerk eines großen Veranstaltungszentrums im Saarland. Die Betreibergesellschaft bestätigte den Vorfall. Während IT-Teams an der Wiederherstellung arbeiteten und die Polizei Ermittlungen aufnahm, konnten geplante Veranstaltungen ohne Einschränkungen stattfinden. Zur Art des Angriffs wurden keine Details veröffentlicht.

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

**Anzunehmende Schadensfelder:**

Quellen:
https://www.saarbruecker-zeitung.de/saarland/saarbruecken/hackerangriff-auf-congress-centrum-saar-veranstaltungen-sicher_aid-130437537
https://www.sr.de/sr/saarbruecken_hackerangriff_congresshalle_saarlandhalle_100.html

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

RIEDEL

# Politische Botschaften auf Bäckerei-Bildschirmen

03. Juli 2025, in Hildesheim/Niedersachsen

**DEFACEMENT**

**MANIPULATION**

**EINBRUCH**

**Was ist passiert?**
Anfang Juli 2025 wurden mehrere Filialen einer Bäckereikette Ziel eines Cyberangriffs. Unbekannte Täter spielten politische Inhalte auf die Werbebildschirme des Unternehmens aus. Laut Medienberichten sind insgesamt **26 Filialen** betroffen. Ein ähnlicher Vorfall ereignete sich zuvor bereits bei einer anderen Bäckerei.

**Was hätte man besser machen können?**
Eine bessere Absicherung der Werbebildschirme durch strikt geschützte Zugänge, regelmäßige Updates und eine getrennte Netzwerkanbindung hätte den Angriff erschwert. Zusätzlich hätten Monitoring-Systeme Manipulationen frühzeitig erkannt, sodass falsche Inhalte weniger Filialen erreichen konnten.

**Anzunehmende Schadensfelder:**

Quellen:
https://www.t-online.de/region/hannover/id_100802840/hannover-antisemitische-werbung-im-cafe-engelke-betreiber-reagiert.html
https://www.hildesheimer-allgemeine.de/meldung/sensenmann-statt-broetchenwerbung-baeckerei-engelke-wird-ziel-von-hackerangriff.html

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

RIEDEL

# Ransomware-Angriff auf niedersächsisches Tiefbauunternehmen

01. Juli 2025, in Niedersachsen

RANSOMWARE

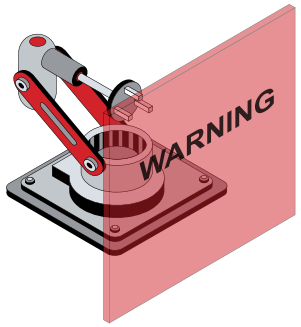
DATENDIEBSTAHL

**Was ist passiert?**
Ein niedersächsisches Straßen- und Tiefbauunternehmen wurde Ziel eines Ransomware-Angriffs. Die Hackergruppe **Safepay** veröffentlichte am 1. Juli 2025 einen Eintrag auf ihrem Opferblog, in dem sie darlegt, rund **119 Gigabyte** Unternehmensdaten entwendet zu haben.

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

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

**Anzunehmende Schadensfelder:**




Quellen:
https://www.security-incidents.de/assets/img/incidents/9917-Safepay.png

RIEDEL

# Erkenntnisse

## OOPS REPORT H2-2025

RIEDEL

# Summary

Welche Erkenntnisse stechen besonders hervor?

Die Branchenverteilung zeigt sich im zweiten Halbjahr 2025 wie folgt:

- **Industrie/Produktion – 34,6%**
- **IT & Software / Dienstleister –21%**
- **Handel & E-Commerce – 17,9%**
- **Öffentliche Verwaltung – 9,9 %**
- **Events/ Medien – 6,2 %**
- **Bildung & Forschung – 4,9%**
- **Sonstige – 4,7%**

Im zweiten Halbjahr 2025 trifft die Cyberkriminalität vor allem Industrie, IT-Dienstleister und den Handel: Diese drei Sektoren vereinen fast drei Viertel aller Fälle auf sich, während öffentliche Verwaltung, Medien und Bildungsinstitutionen ein stabiles Mittelfeld bilden.

Die Verteilung der Angreifertypen zeigt sich im zweiten Halbjahr 2025 wie folgt:

- **Cyberkriminelle: 86,5%**
- **Sonstige/ unklar 11%**
- **Hacktivisten: 1,2%**
- **Staatlich / Spionage: 0,6 %**
- **Insider / interne Täter: 0,6 %**

Das zweite Halbjahr wird wieder klar von Cyberkriminellen dominiert: Fast 90 % aller Vorfälle gehen auf ihr Konto, während Insider, staatliche Akteure und hacktivistische Gruppen nur in Einzelfällen auftreten.

Die Verteilung der Angriffsarten zeigt sich im zweiten Halbjahr 2025 wie folgt:

- **Datendiebstahl/ Exfiltration: 33,4%**
- **Ransomware: 32,5%**
- **Einbruch: 11,8%**
- **Ausfall: 11,2%**
- **Sonstige: 11%**

Die Angriffe im zweiten Halbjahr 2025 werden von Datendiebstahl und Ransomware geprägt, die gemeinsam zwei Drittel aller Schadensmuster ausmachen; Einbruch und Ausfall bilden das operative Mittelfeld. Malware, DDoS oder andere Formen waren im zweiten Halbjahr zwar präsent, traten jedoch nur in sehr geringem Umfang auf.

RIEDEL

# Summary

Welche Erkenntnisse stechen besonders hervor?

1. Ransomware bleibt eines der häufigsten Angriffe, immer häufiger flankiert von gezieltem Datendiebstahl, der sich zum zentralen Hebel moderner Erpressungstaktiken entwickelt.

2. Bildung & Forschung und Kommunen sind überproportional betroffen, häufig mit sensiblen Personen- und Projektdaten bzw. mit Betriebsrelevanz für Bürgerdienste.

3. Mehrere Gruppen (z. B. Safepay, Qilin, DragonForce) agieren kampagnenartig und listen in kurzer Zeit zahlreiche deutsche Ziele, was auf opportunistische Massenkompromittierungen statt einzelner, gezielter Angriffe hinweist.

4. Ein erheblicher Anteil der Vorfälle führt zu Betriebsunterbrechungen durch Abschaltungen oder Ausfälle, besonders bei kommunalen Einrichtungen, wo zusätzlich DDoS-Angriffe auftreten.

5. Das Angreiferbild ist klar von finanziell motivierten Cyberkriminellen geprägt, während staatliche Akteure, Hacktivisten und Insider selten im Report auftreten.

6. Viele Vorfälle beinhalten sehr große Datenexfiltrationen im dreistelligen Gigabyte- bis Terabyte-Bereich, was den wachsenden Fokus auf maximale Erpressungswirkung durch Leaks unterstreicht.

RIEDEL

# Vergleich

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

**Ransomware bleibt die dominierende Bedrohung**
- In beiden Berichtszeiträumen war Ransomware mit einer der häufigsten Angriffstypen.
- H1 2025: 38 % aller Angriffe waren Ransomware.
- H2 2025: Sinkt der Anteil leicht auf 32,5 %.

**Cyberkriminelle übernehmen das Feld**
- In beiden Berichtszeiträumen stellen Cyberkriminelle die größte Angreifergruppe dar.
- H1 2025: 71 % der Fälle werden durch finanziell motivierte Cyberkriminelle ausgelöst.
- H2 2025: Cyberkriminelle dominieren erneut mit 86,95 %.

**Datenexfiltration ist in beiden Halbjahren ein zentraler Bestandteil moderner Angriffe**
- H1 2025: Datendiebstahl liegt bei 22 % und ist direkt hinter Ransomware die zweitgrößte Kategorie.
- H2 2025: Datendiebstahl/Exfiltration steigt auf 33,4 % und liegt damit im zweiten Halbjahr sogar vor Ransomware als häufigste Schadensart.

**Betroffene Branchen**
- Öffentliche Einrichtungen sowie klassische Unternehmensbranchen wie Industrie und IT gehören in H1 und H2 durchgängig zu den meistbetroffenen Bereichen.

RIEDEL

# Vergleich

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

| | H1-2025 | H2-2025 | Veränderung |
|---|---|---|---|
| **Angriffsarten** | Ransomware (38%), Datendiebstahl (22%), Einbruch (15%), Sicherheitslücken (11%), DDoS (7%) , Sonstige (7%) | Datendiebstahl (33,4%), Ransomware (32,5%), Einbruch (11,8%), Ausfall (11,2%), Sonstige (11%) | Schwerpunkt verschiebt sich von Ransomware hin zu Datendiebstahl, während Ausfälle spürbar stärker in den Fokus rücken und klassische Kategorien wie Sicherheitslücken und DDoS im Vergleich weniger Gewicht haben |
| **Angreifertypen** | Cyberkriminelle (71%), Hacktivisten (12%), Staatliche Spionage (9%), Insider (5%), Unbekannt (3%) | Cyberkriminelle (86,5%), Sonstige/unklar (11,1%), Hacktivisten (1,2%), Staatliche Spionage (0,6%), Insider (0,6%) | Cyberkriminelle dominieren in H2 noch ausgeprägter, während staatliche Akteure, Hacktivisten und Insider stark an Bedeutung verlieren und der Anteil unklarer bzw. sonstiger Akteure zunimmt |
| **Betroffene Branchen** | Industrie (26%), IT (18%), Öffentlicher Sektor (17%), Handel (14%), Finanzsektor (10%), Gesundheitswesen (8%), Sonstige (7%) | Industrie (34,6%), IT (21%), Handel (17,9%), Öffentliche Verwaltung (9,9%), Events & Medien (6,2%), Bildung & Forschung (4,9%), Sonstiges (4,7%) | Industrie, IT und Handel verzeichnen in H2 einen deutlichen Anstieg, während der öffentliche Sektor zurückgeht und neue Bereiche wie Events & Medien sowie Bildung & Forschung stärker sichtbar werden |
| **Neue Trends** | Diversifizierung der Angriffsformen, Sicherheitslücken, DDoS und neue Angriffstypen gewinnen an Bedeutung | Stärkere datengetriebene Angriffe, Professionalisierung von cyberkrimineller Gruppen sowie einem breiteren Spektrum betroffener Branchen | Verschiebung von breit gefächerten Angriffsformen hin zu datengetriebene professionell ausgeführten Attacken, die sich zunehmen auf wirtschaftlich relevante Branchen konzentrieren |

RIEDEL

“

H2 2025 zeigt, wie sich Cyberangriffe weiter professionalisieren und strategisch ausrichten: Die Methoden werden ausgefeilter, die Akteure entschlossener und vor allem geraten wirtschaftlich und gesellschaftlich kritische Branchen stärker denn je in den Fokus.

”

RIEDEL

# Get in Touch

Der beste Schutz entsteht nicht durch Abwarten,
sondern durch den ersten Schritt – hin zu einer resilienten IT-Security

**RIEDEL Networks GmbH & Co. KG**

RN-sales@riedel.net

+49 (0) 6033 9169 100

*Noch nicht überzeugt?*
*Vielleicht hilft unser „Faule-Ausreden-Quartett“ zum Thema Cybersicherheit.*
*Wir freuen uns auf einen weiteren Austausch mit Ihnen.*

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

RIEDEL