

Ransomware 2.0: Warum die Verteidigung nicht auf wache Menschen bauen darf

Von Thomas Faß · 4. August 2026 · aktualisiert 9. September 2026

Ransomware 2.0 hat sich von der reinen Verschlüsselung zur mehrstufigen Erpressung entwickelt: Daten werden vor der Verschlüsselung gestohlen (Double Extortion), teils ergänzt um DDoS-Angriffe oder Druck auf Kunden (Triple Extortion) – klassische Backups allein schützen damit nicht mehr. Angetrieben von professionalisierter Ransomware-as-a-Service und KI-gestütztem Phishing braucht es eine mehrschichtige Antwort: Zero Trust, unveränderliche Backups, DevSecOps und phishing-resistente Authentifizierung. Datenpannen sind teuer – laut IBM lag der globale Schnitt 2026 bei 4,99 Mio. US-Dollar.

Das Wichtigste in Kürze

- Ransomware 2.0 hat sich von der reinen Verschlüsselung zur mehrstufigen Erpressung entwickelt: Daten werden vor der Verschlüsselung gestohlen (Double Extortion).
- Der Angriff läuft planmäßig dann, wenn niemand hinsieht: 88 Prozent der Ransomware-Payloads werden außerhalb der Geschäftszeiten ausgerollt, bis zum Active-Directory-Server vergehen im Schnitt 3,4 Stunden (Sophos 2026).
- Triple Extortion ergänzt den Druck um DDoS oder Druck auf Kunden – klassische Backups allein schützen damit nicht mehr.
- Angetrieben wird die Welle von professionalisierter Ransomware-as-a-Service und KI-gestütztem Phishing; kritische Infrastrukturen (ICS/OT) geraten besonders ins Visier.
- Die Antwort ist mehrschichtig: Zero Trust, unveränderliche Backups, DevSecOps und phishing-resistente Authentifizierung (Passkeys).

Ransomware hat sich von einer isolierten Bedrohung zu einem hochkomplexen und professionellen Geschäftsmodell entwickelt. Die aktuelle Inkarnation, oft als „Ransomware 2.0“ bezeichnet, übertrifft ihre Vorgänger in Raffinesse, Zielgenauigkeit und den angewandten Erpressungstaktiken. Dies stellt Unternehmen und kritische Infrastrukturen vor nie dagewesene Herausforderungen.

Ransomware 2.0: Eine Definition und ihre Ursprünge

Ransomware 2.0 stellt die nächste Phase in der Evolution von Ransomware-Angriffen dar. Sie ist gekennzeichnet durch erweiterte Fähigkeiten, heimlichere Techniken und einen höheren Grad an Anpassung. Im Gegensatz zu früheren Varianten geht Ransomware 2.0 über die bloße Dateiverschlüsselung hinaus. Sie integriert fortschrittliche Ausweichtaktiken, adaptives Verhalten und beinhaltet häufig die Exfiltration sensibler Daten vor der eigentlichen Verschlüsselung. Dies verstärkt den potenziellen Schaden und den Druck auf die Opfer erheblich.

Diese tiefgreifende Entwicklung wird durch einen strategischeren und lukrativeren Ansatz der Cyberkriminellen vorangetrieben. Moderne Angriffe sind nicht mehr nur breit gestreut und opportunistisch; sie sind schnell, leise und tiefgreifend störend. Angreifer zielen mit chirurgischer Präzision auf Daten, Infrastruktur und Wiederherstellungsprozesse ab. Diese gezielte Auswahl wertvoller Ziele und die Anpassung der Taktiken, um maximalen finanziellen oder operativen Schaden zu verursachen, markiert einen fundamentalen Wandel von der breiten Streuung zur gezielten Jagd.

Ein wesentlicher Aspekt dieser Evolution ist die Unzureichendheit traditioneller Backup-Strategien. Da Ransomware 2.0 die Exfiltration sensibler Daten vor der Verschlüsselung einschließt, werden Backups allein unwirksam. Selbst wenn Systeme aus Backups wiederhergestellt werden können, sind der Reputationsschaden und die rechtlichen Konsequenzen eines Datenlecks irreparabel. Dies verdeutlicht, dass sich das Problem von einem reinen Datenzugriffsproblem zu einem Datenexpositionsproblem verschoben hat. Unternehmen, die sich ausschließlich auf Backups zur Wiederherstellung verlassen, übersehen diese neue Dimension der Bedrohung vollständig.

Ransomware 2.0: Eine tiefere Analyse moderner Erpressungstaktiken

Die Mechanik von Ransomware 2.0 umfasst einen sorgfältig orchestrierten, mehrstufigen Prozess, der weit über die einfache Dateiverschlüsselung hinausgeht.

Jenseits der Verschlüsselung: Double und Triple Extortion

Die sogenannte Double Extortion ist zu einem neuen Standard geworden. Bei dieser bösartigen Taktik stehlen Angreifer sensible Daten wie Kundendaten, Finanzdaten oder geistiges Eigentum, bevor sie die Systeme verschlüsseln. Die Opfer stehen dann vor der Wahl: Entweder sie zahlen das Lösegeld, oder sie riskieren die öffentliche Offenlegung der gestohlenen Informationen. Einige Gruppen, wie Clap, verzichten sogar ganz auf die Verschlüsselung und verlassen sich ausschließlich auf Datendiebstahl und Erpressung.

Was ein solcher Vorfall kostet, hat IBM zuletzt für den Berichtszeitraum März 2025 bis Februar 2026 erhoben: Der globale Durchschnitt liegt bei **4,99 Millionen US-Dollar** — ein Plus von **12 Prozent** gegenüber dem Vorjahr und der höchste je in dieser Reihe gemessene Wert. Grundlage ist eine Erhebung des Ponemon Institute über 602 Organisationen in 16 Ländern und Regionen und 17 Branchen.

Die Triple Extortion fügt dem Angriff eine dritte Bedrohungsstufe hinzu. Zusätzlich zur Verschlüsselung und Datenexfiltration können Angreifer Distributed-Denial-of-Service (DDoS)-Angriffe durchführen, die Kunden des Opfers direkt bedrohen oder andere Drohungen aussprechen. Dies erweitert den potenziellen Schadensbereich eines Angriffs erheblich, da nun auch Partner, Kunden und Lieferanten des Opfers betroffen sein können. Die finanziellen Verluste können sich aus Lösegeldzahlungen, Wiederherstellungskosten, Ausfallzeiten, verlorenen Kunden und rechtlichen Gebühren zusammensetzen.

Die Androhung der Datenveröffentlichung durch Double- und Triple-Extortion-Angriffe erhöht den Druck auf die Opfer erheblich. Dies geht über den reinen Betriebsstillstand hinaus und betrifft direkt den Ruf des Unternehmens sowie potenzielle rechtliche Konsequenzen, wie beispielsweise hohe Bußgelder im Rahmen von DSGVO, HIPAA oder CCPA bei Offenlegung sensibler Daten. Die Angst vor Reputationsverlust und hohen Strafen wird zum primären Hebel, selbst wenn die technischen Systeme wiederhergestellt sind.

Da Backups allein nicht ausreichen, um die Bedrohung durch Datenlecks zu neutralisieren, müssen Unternehmen ihre Verteidigungsstrategien erweitern. Der Fokus verschiebt sich von der reinen Wiederherstellung des Betriebs zur umfassenden Risikobewältigung, die die Verhinderung von Datenlecks und Reputationsschäden einschließt. Dies erfordert neue Sicherheitstechnologien und -prozesse, die gezielt auf Datenexfiltration abzielen, nicht nur auf Verschlüsselung.

Um die Unterschiede zwischen traditioneller Ransomware und Ransomware 2.0 zu verdeutlichen, lässt sich zusammenfassen:

Traditionelle Ransomware konzentrierte sich hauptsächlich auf die Verschlüsselung von Daten und beinhaltete keine Datenexfiltration oder zusätzliche Erpressungstaktiken. Die Angreifer waren oft weniger professionell oder opportunistisch und zielten auf eine breite Masse ab, um finanzielle Entschlüsselungsforderungen zu stellen. Backups waren gegen diese Art von Angriffen hoch wirksam.

Im Gegensatz dazu beinhaltet Ransomware 2.0 zwar oft noch die Verschlüsselung, macht aber die Datenexfiltration zur Standardpraxis und fügt häufig zusätzliche Erpressungsmethoden wie DDoS-Angriffe oder die direkte Bedrohung von Kunden hinzu. Die Angreifer sind hochprofessionell und organisiert und zielen gezielt auf Unternehmen oder kritische Infrastrukturen ab. Ihre Motivation geht über die reine Entschlüsselungsforderung hinaus und umfasst auch die Erpressung zur Nicht-Veröffentlichung gestohlener Daten. Die Wirksamkeit von Backups ist bei Ransomware 2.0 eingeschränkt, da sie nicht vor den Folgen eines Datenlecks schützen.

Geschwindigkeit und Tarnung: Das neue Playbook der Angreifer

Moderne Angreifer agieren extrem schnell und heimlich. Die mittlere Verweildauer im Netzwerk ist weiter gesunken: „Median dwell time declined to three days“, hält der Sophos Active Adversary Report 2026 fest – 2023 waren es in derselben Reihe noch fünf Tage. Sophos nennt dafür zwei Ursachen: Die Angreifer bewegen sich schneller, und die Verteidiger reagieren schneller.

Wie wenig Zeit dazwischen liegt, zeigt ein zweiter Wert aus derselben Erhebung: Bis zum Active-Directory-Server brauchen Angreifer im Schnitt **3,4 Stunden**. Wer den Verzeichnisdienst hat, hat das Netz. Secureworks kam bereits 2023 zu dem Befund, dass die Bereitstellung von der initialen Kompromittierung bis zur Verschlüsselung in mehr als der Hälfte der Fälle in weniger als 24 Stunden erfolgte; in 10 Prozent der Fälle wurde die Ransomware innerhalb von fünf Stunden nach dem ersten Zugriff ausgerollt.

Nach dem Sophos Active Adversary Report 2026 werden **88 Prozent der Ransomware-Payloads außerhalb der regulären Geschäftszeiten** ausgerollt. Bei der Datenexfiltration sind es **79 Prozent** (Quelle: Sophos, 2026). Der Angriff findet also planmäßig dann statt, wenn im Unternehmen niemand hinsieht – nachts, am Wochenende, über Feiertage. 2023 lag der Wert für die Payloads in derselben Reihe noch bei 81 Prozent.

Wie die Angreifer hereinkommen, hat sich dabei verschoben. Sophos hält für den Berichtszeitraum fest: „67% of all incidents investigated by Sophos Incident Response (IR) and Managed Detection and Response (MDR) teams last year were rooted in identity-related attacks.“ Brute-Force-Angriffe liegen mit **15,6 Prozent** inzwischen fast gleichauf mit dem Ausnutzen von Schwachstellen (**16 Prozent**) als Weg des Ersteinstiegs.

Und ein Wert, der die Gegenmaßnahme gleich mitliefert: „There was also a lack of MFA in 59% of cases, facilitating the abuse of stolen and compromised credentials.“ In fast sechs von zehn untersuchten Fällen fehlte eine Mehrfaktor-Authentifizierung.

Angreifer nutzen zunehmend verschlüsselte Kanäle, legitime Anmeldeinformationen und dateilose Techniken, um Daten aus Organisationen zu exfiltrieren. Dies erschwert es traditionellen Sicherheitstools erheblich, legitime von bösartigen Aktivitäten zu unterscheiden.

Wenn die Verweilzeit der Angreifer auf unter 24 Stunden sinkt und Angriffe bevorzugt außerhalb der Geschäftszeiten stattfinden, bedeutet dies, dass traditionelle, reaktive Sicherheitsmodelle, die auf menschlicher Erkennung und Reaktion basieren, nicht mehr ausreichen. Die Zeit, die einem Unternehmen bleibt, um einen Angriff zu erkennen und darauf zu reagieren, wird drastisch verkürzt. Dies unterstreicht die dringende Notwendigkeit automatisierter und proaktiver Verteidigungssysteme, insbesondere solcher, die durch Künstliche Intelligenz (KI) unterstützt werden.

Die Verwendung von legitimen Anmeldeinformationen und dateilosen Techniken sowie das Nachahmen legitimer Kommunikation erschwert es Sicherheitssystemen, bösartige Aktivitäten zu erkennen. Die Grenze zwischen „normalem“ und „anomal“ Verhalten verschwimmt zusehends. Dies macht den Einsatz von verhaltensbasierten Analysen und KI-gestützten Erkennungssystemen unerlässlich, da diese über statische Signaturen hinausgehen können, um subtile Abweichungen zu identifizieren.

Der Aufstieg von Ransomware-as-a-Service (RaaS)

Ransomware-as-a-Service (RaaS) ist ein Geschäftsmodell, bei dem Cyberkriminelle Ransomware entwickeln und diese an Affiliates verkaufen oder leasen. Diese Affiliates nutzen dann die Software, um Angriffe auf Ziele ihrer Wahl durchzuführen. Dieses Modell hat die Eintrittsbarriere für Cyberkriminelle erheblich gesenkt, sodass selbst Personen mit minimalen technischen Fähigkeiten ausgeklügelte Ransomware-Kampagnen starten können. Affiliates zahlen dafür oft nur eine wiederkehrende Gebühr, teils ab 40 US-Dollar im Monat, oder beteiligen die Betreiber am Erlös. Welche Wirkung das entfaltet, zeigt ein einzelner Monat: Im Mai 2024 gingen laut NCC Group 176 Angriffe allein auf die RaaS-Bande LockBit 3.0 zurück – 37 Prozent aller in diesem Monat registrierten Ransomware-Vorfälle.

RaaS-Kits sind im Darknet verfügbar und funktionieren ähnlich wie legitime SaaS-Produkte, komplett mit 24/7-Support, gebündelten Angeboten, Benutzerbewertungen und Foren. Die Zahl der aktiven Ransomware-Gruppen stieg laut Searchlight Cyber im ersten Halbjahr 2024 um 56 % gegenüber dem Vorjahreszeitraum – auf über 70 aktive Gruppen. Zu den damals prominentesten RaaS-Gruppen gehörten LockBit, BlackCat (ALPHV) und Conti.

Die Szene hat sich seither umsortiert. Im Berichtszeitraum von Sophos waren **Akira und Qilin** die aktivsten Marken, Akira allein in **22 Prozent** der Vorfälle. Insgesamt traten **51 Ransomware-Marken** auf – 27 wiederkehrende und 24 neue. Wer sich auf die Namen von vorgestern einstellt, verteidigt gegen die falsche Bande.

Die Senkung der Eintrittsbarriere durch RaaS und die Verfügbarkeit von „ready-made tools“ führen zu einer exponentiellen Zunahme der Angreiferzahl und der Angriffsfrequenz. Dies bedeutet, dass Unternehmen nicht mehr nur gegen wenige hochqualifizierte Gruppen kämpfen, sondern gegen eine viel

größere, diversifizierte Gruppe von Akteuren, die Zugang zu hochentwickelten Tools haben. Die Bedrohung wird dadurch breiter und schwerer zu verfolgen.

Angesichts der hohen Profitabilität bei minimalem Risiko für RaaS-Betreiber und Affiliates wird die Motivation für Angriffe weiter steigen. Dies erfordert von Verteidigern, ihre Sicherheitsmaßnahmen nicht nur zu verbessern, sondern auch zu automatisieren und zu skalieren. Nur so kann mit der steigenden Anzahl und Komplexität der Angriffe Schritt gehalten werden.

Das RaaS-Geschäftsmodell setzt sich aus verschiedenen Komponenten mit spezifischen Rollen und Auswirkungen zusammen:

- RaaS-Betreiber (Entwickler) sind für die Entwicklung und Wartung der Malware verantwortlich. Sie stellen die Tools bereit und aktualisieren den Code sowie die Infrastruktur.
- Affiliates (Angreifer) wählen die Opfer aus und führen die eigentlichen Angriffe durch, beispielsweise mittels Phishing, Social Engineering oder Schwachstellen-Exploits. Sie erhalten dafür Provisionen.
- Die Infrastruktur umfasst Command-and-Control-Server, Zahlungsportale, Leak-Sites im Darknet und Online-Dashboards.
- Support/Dienstleistungen werden den Affiliates in Form von 24/7-Support, gebündelten Angeboten, Benutzbewertungen und Foren sowie Schulungen zur Verfügung gestellt.
- Die Bezahlung der Betreiber erfolgt über Abonnementgebühren, einmalige Gebühren oder eine prozentuale Gewinnbeteiligung.

Die Professionalisierung der Cyberkriminalität

Cyberkriminelle agieren zunehmend wie etablierte Unternehmen. Sie rekrutieren Affiliates, bieten Support und Schulungen an und nutzen spezialisierte Tools und Taktiken. Ransomware-Verhandlungsführer berichten von hochstrategischen Verhandlungen, bei denen die Angreifer versuchen, die Kommunikation und den Fokus zu kontrollieren. Sie sammeln umfassende Informationen über ihre Opfer, einschließlich Finanzdaten, Technologien, Organisationsstrukturen und Führungskräfte, um den maximalen Lösegeldwert zu ermitteln. Die Fähigkeit, schnell Probleme zu lösen und strategisch zu kommunizieren, ist für Verhandlungsführer entscheidend, da neue Angriffsgruppen und -tools ständig auftauchen.

Die Beschreibung von RaaS als „Geschäftsmodell“ mit „24/7-Support, gebündelten Angeboten, Benutzbewertungen und Foren“ sowie die Existenz von „Ransomware-Verhandlungsführern“ und die detaillierte Opferprofilierung zeigen, dass Cyberkriminalität nicht mehr nur aus Einzelpersonen besteht. Vielmehr handelt es sich um organisierte Gruppen, die nach betriebswirtschaftlichen Prinzipien agieren. Dies erfordert, dass die Bedrohung nicht nur technologisch, sondern auch organisatorisch und strategisch angegangen wird.

Angreifer sammeln detaillierte Informationen über ihre Opfer, während die Opfer in einer Krisensituation oft desorganisiert sind. Dieses Informationsungleichgewicht verschafft den Angreifern einen erheblichen Vorteil in Verhandlungen. Dies unterstreicht die Notwendigkeit für Unternehmen, proaktiv Bedrohungsanalysen durchzuführen und Notfallpläne zu erstellen, um in einer solchen Situation nicht völlig unvorbereitet zu sein.

Angriffe auf Lebensadern: Kritische Infrastrukturen (ICS/OT) im Visier

Kritische Infrastrukturen (KI), insbesondere Industrial Control Systems (ICS) und Operational Technology (OT), sind zunehmend ein primäres Ziel von Ransomware-Angriffen. Diese Sektoren, darunter Energie, Gesundheitswesen, Transport und Telekommunikation, sind aufgrund ihrer strategischen Bedeutung und der Notwendigkeit eines unterbrechungsfreien Betriebs besonders anfällig.

Warum ICS/OT ein primäres Ziel ist

ICS/OT-Systeme sind aufgrund veralteter Software, begrenzter Patching-Möglichkeiten und der enormen Kosten von Ausfallzeiten besonders anfällig. Angreifer wissen, dass die Störung dieser Sektoren weitreichende physische und betriebliche Konsequenzen haben kann, die über finanzielle Verluste hinausgehen und die öffentliche Sicherheit gefährden können. Die Integration von IT- und OT-Netzwerken, oft ohne grundlegende Sicherheitsfunktionen, schafft zusätzliche Schwachstellen.

Die zunehmende Vernetzung von traditionell isolierten OT-Systemen mit IT-Netzwerken bedeutet, dass IT-Sicherheitslücken direkte Auswirkungen auf die physische Welt haben können. Ein Angriff, der in der IT-Umgebung beginnt, kann sich auf die OT ausbreiten und kritische Prozesse stören. Dies erfordert eine übergreifende Sicherheitsstrategie, die sowohl IT- als auch OT-Risiken berücksichtigt und die traditionellen Silos aufbricht.

Ransomware-Angriffe auf das Gesundheitswesen können die Patientenversorgung verzögern und kritisch kranke Patienten gefährden. Im Energiesektor können sie die Kraftstoffversorgung unterbrechen. Diese direkten Auswirkungen auf die öffentliche Sicherheit und das Leben von Menschen erhöhen den Druck auf die Opfer, Lösegeld zu zahlen, erheblich. Dies macht ICS/OT-Angriffe besonders lukrativ und gefährlich.

Bemerkenswerte Angriffe und ihre Auswirkungen

Die Geschichte der Cyberangriffe auf kritische Infrastrukturen ist reich an bemerkenswerten Beispielen, die die verheerenden Auswirkungen solcher Attacken verdeutlichen:

- Colonial Pipeline (2021): Dieser Ransomware-Angriff zwang das Unternehmen, den Betrieb für mehrere Tage einzustellen, was zu einer Kraftstoffversorgungskrise an der US-Ostküste führte. Das Unternehmen zahlte rund 75 Bitcoin Lösegeld; der Vorstandsvorsitzende bezifferte den Betrag in einer Anhörung des US-Senats auf 4,4 Millionen US-Dollar (Quellen: US-Justizministerium, 2021; US-Senat, HSGAC, 2021).
- Universal Health Services (UHS, 2020): Ein großer Krankenhausverbund erlitt einen Ransomware-Angriff, der den Zugang zu digitalen Krankenakten in über 400 Krankenhäusern in den USA blockierte, Behandlungen verzögerte und Patienten in Gefahr brachte.
- Ukrainischer Stromnetz-Angriff (2015): Hacker nutzten Spear-Phishing, um Zugang zu den Kontrollsystemen eines ukrainischen Versorgungsunternehmens zu erhalten, was zu Stromausfällen für über 230.000 Menschen führte.
- Stuxnet (2010 entdeckt): Dieser hochkomplexe Wurm zielte auf industrielle Steuerungen in iranischen Nuklearanlagen ab und sabotierte physische Anlagen auf cybernetischem Wege.

- Triton/Trisis Malware (2017): Diese Malware griff ein sicherheitsgerichtetes System (SIS) in einer petrochemischen Anlage an, mit dem Ziel, Sicherheitskontrollen zu deaktivieren und gefährliche Bedingungen zu schaffen.

Diese Beispiele zeigen, dass Angriffe auf ICS/OT nicht nur Daten oder IT-Systeme betreffen, sondern direkte physische Auswirkungen haben können, wie Stromausfälle, Kraftstoffknappheit oder die Störung von Sicherheitssystemen. Dies hebt die Dringlichkeit und das Potenzial für katastrophale Folgen hervor, die über die traditionellen Cyber-Risiken hinausgehen.

Der ukrainische Stromnetz-Angriff und die allgemeine Anfälligkeit von OT-Personal für Phishing-Angriffe zeigen, dass menschliche Schwachstellen weiterhin ein primäres Einfallstor sind. Gepaart mit der Herausforderung, veraltete OT-Systeme zu patchen, entsteht eine gefährliche Kombination, die Angreifern leichtes Spiel macht und die Notwendigkeit einer umfassenden Sicherheitsstrategie für diese kritischen Bereiche unterstreicht.

Das KI-Wettrüsten: Künstliche Intelligenz als Waffe und Schild

Künstliche Intelligenz (KI) ist zu einem zentralen Element im Cyber-Wettrüsten geworden, das sowohl Angreifern beispiellose Fähigkeiten verleiht als auch Verteidigern neue Werkzeuge an die Hand gibt.

KI als Offensivwaffe: Von Phishing bis adaptiver Malware

KI, insbesondere Large Language Models (LLMs), ermöglicht die Erstellung grammatikalisch perfekter, kontextuell relevanter und hyper-personalisierter Phishing-E-Mails, die den Schreibstil von Führungskräften oder Kollegen nachahmen. Wie Angreifer KI im Einzelnen einsetzen, steht in [KI in der Cyberkriminalität](#). Diese Angriffe sind oft nicht von legitimer Kommunikation zu unterscheiden und können traditionelle Spamfilter umgehen. Branchenanalysen zufolge ist inzwischen ein erheblicher Teil der globalen Phishing-Vorfälle mit KI-Taktiken verbunden.

Deepfakes, also KI-generierte Audio-, Video- oder Bilddateien, werden verwendet, um Personen täuschend echt zu imitieren. Beispiele umfassen die Klonung von Stimmen von CEOs, um Finanztransaktionen zu autorisieren, oder die Erstellung überzeugender Videoanrufe, die Führungskräfte imitieren. Die Technologie dahinter, wie Generative Adversarial Networks (GANs) und Diffusion Models, ermöglicht die Erzeugung hochrealistischer Inhalte.

KI-gestützte Malware kann ihren Code dynamisch modifizieren, Ausführungsmuster ändern und Kommunikationsmethoden an die Sicherheitsumgebung anpassen. Dies macht sie erheblich schwerer zu erkennen und zu eliminieren, da sie signaturbasierte Erkennung umgeht und sich autonom im Netzwerk verbreiten kann. Agentic AI (autonome KI-Systeme) kann selbstständig Schwachstellen identifizieren, Angriffe starten und sich in Echtzeit anpassen, oft mit minimaler menschlicher Aufsicht.

Zudem beschleunigt KI die Schwachstellen-Entdeckung und die Entwicklung von Exploits. Sie kann riesige Datensätze aus sozialen Medien, öffentlichen Aufzeichnungen und geleakten Datenbanken analysieren, um hochgradig zielgerichtete Spear-Phishing-Kampagnen zu erstellen und den Zeitpunkt von Angriffen gezielt zu wählen.

Die Fähigkeit von KI, „fehlerfreie, schnelle und fokussierte“ Phishing-E-Mails zu generieren, die traditionelle Spamfilter umgehen, sowie die polymorphe Natur adaptiver Malware, die Signaturen umgeht, führt dazu, dass herkömmliche, signaturbasierte Erkennungssysteme zunehmend unwirksam werden. Dies zwingt Unternehmen dazu, von reaktiven zu proaktiven, verhaltensbasierten und KI-gestützten Erkennungsmethoden überzugehen.

Die Verfügbarkeit von Tools wie WormGPT und die Möglichkeit, LLMs für die Generierung von Phishing-Inhalten zu nutzen, ohne „Jailbreaking“, senkt die technische Eintrittsbarriere für Angreifer erheblich. Dies bedeutet, dass auch weniger erfahrene Cyberkriminelle Zugang zu hochentwickelten Angriffsmethoden erhalten, was die Häufigkeit und Skalierung von Angriffen erhöht.

Die Diskussion um „Agentic AI“ und autonome Waffensysteme wirft zudem tiefgreifende ethische Fragen der Verantwortlichkeit („accountability gap“), Transparenz („black boxes“) und möglicher Voreingenommenheit („bias in algorithms“) auf, wenn diese Systeme selbstständig Entscheidungen treffen. Obwohl der Fokus hier auf Cyberangriffen liegt, impliziert die Existenz solcher Fähigkeiten auf der Angreiferseite, dass auch Verteidigungssysteme zunehmend autonom werden müssen, was die gleichen ethischen Fragen aufwirft.

Die KI-gestützten Angriffsvektoren und ihre Mechanismen lassen sich wie folgt zusammenfassen:

Personalisierte Phishing-E-Mails: Hier generieren LLMs überzeugende Inhalte, imitieren Stil und Ton und nutzen öffentliche Daten für die Personalisierung.

Deepfakes: GANs und Diffusion Models erzeugen realistische Audio-, Video- oder Bilddateien zur Nachahmung von Personen.

Adaptive Malware: ML-Algorithmen modifizieren ihren Code und passen ihr Verhalten an, um die Erkennung zu umgehen.

Autonome Angriffe (Agentic AI): KI-Agenten identifizieren Schwachstellen, planen und führen Angriffe selbstständig aus.

KI-gestützte Aufklärung/Schwachstellen-Entdeckung: Es erfolgt eine schnelle Analyse großer Datenmengen zur Identifizierung von Zielen und Optimierung von Angriffen.

KI als Verteidigungsschild: Prädiktive Analysen und automatisierte Reaktion

Trotz der Bedrohungen durch offensive KI ist KI auch ein entscheidender Faktor für die Cybersicherheitsverteidigung. Defensive KI-Systeme können riesige Datenmengen in Echtzeit analysieren, Anomalien identifizieren und potenzielle Verstöße erkennen, bevor sie eskalieren.

Prädiktive Analysen: KI-Algorithmen können historische Nutzungsdaten analysieren, um zukünftige Anforderungen vorherzusagen und Ressourcen dynamisch zuzuweisen, was Kosten und Leistung optimiert. Sie erkennen ungewöhnliche Nutzungsmuster und prognostizieren Bedrohungen, bevor diese eintreten.

Anomalieerkennung: Machine-Learning (ML)-Algorithmen lernen aus historischen Daten, um normale und anomale Aktivitätsmuster zu erkennen. Dies ermöglicht die Identifizierung von Abweichungen, die auf

Bedrohungen hindeuten können, wie z. B. ungewöhnliche Anmeldeversuche oder Datenzugriffsmuster.

Automatisierte Reaktion: KI-gesteuerte Systeme können bei Erkennung einer Bedrohung sofort Maßnahmen ergreifen, wie z. B. kompromittierte Endpunkte isolieren, verdächtige Transaktionen blockieren oder Multi-Faktor-Authentifizierung dynamisch erzwingen. SOAR-Plattformen (Security Orchestration, Automation, and Response) nutzen KI, um Vorfalldreaktions-Workflows zu automatisieren und ähnliche Bedrohungen vorherzusagen.

Da Angreifer zunehmend KI einsetzen, um ihre Angriffe zu perfektionieren und zu skalieren, ist es für Verteidiger unerlässlich, ebenfalls auf KI zu setzen, um überhaupt mithalten zu können. Manuelle Prozesse können mit der Geschwindigkeit und dem Volumen automatisierter Bedrohungen nicht mithalten. Dies führt zu einem „AI-Wettrüsten“, bei dem der Ausgang davon abhängt, welche Seite sich schneller anpasst.

Die Effektivität von KI-basierten Verteidigungssystemen hängt stark von der Qualität und dem Volumen der Trainingsdaten ab. Ungenügende oder voreingenommene Daten können zu Fehllarmen (False Positives) führen, die Sicherheitsteams überfordern und die Effizienz beeinträchtigen. Dies erfordert kontinuierliches Training, Verfeinerung der Modelle und menschliche Aufsicht, um die Genauigkeit zu gewährleisten und die „AI-Müdigkeit“ zu vermeiden.

Durch die Automatisierung von Routineaufgaben und die prädiktive Erkennung von Bedrohungen werden menschliche Sicherheitsexperten von zeitaufwändigen, repetitiven Aufgaben entlastet. Ihre Rolle verschiebt sich hin zur strategischen Planung, zur Untersuchung komplexer, unbekannter Bedrohungen und zur Überwachung und Feinabstimmung der KI-Systeme.

Verteidigungsstrategien: Umfassende Prävention und Reaktion

Angesichts der sich ständig weiterentwickelnden Bedrohungslandschaft ist ein mehrschichtiger und proaktiver Ansatz zur Cybersicherheit unerlässlich.

Proaktive Cybersicherheit: Zero Trust und DevSecOps

Zero Trust: Dieses Sicherheitsmodell basiert auf dem Prinzip „Niemals vertrauen, immer überprüfen“. Es eliminiert das implizite Vertrauen in Netzwerken und erfordert eine kontinuierliche Überprüfung jeder Zugriffsanfrage, unabhängig vom Standort oder der Herkunft.

Die Schlüsselprinzipien des Zero Trust umfassen:

- **Kontinuierliche Verifizierung:** Jede Entität – ob Benutzer, Gerät oder Anwendung – wird kontinuierlich authentifiziert und autorisiert.
- **Geringstes Privileg (Least Privilege Access):** Benutzern und Geräten wird nur der minimal benötigte Zugriff gewährt. Dies minimiert den potenziellen Schadensradius eines Verstoßes.
- **Mikrosegmentierung:** Das Netzwerk wird in kleinere, isolierte Segmente unterteilt, um die laterale Bewegung von Angreifern zu begrenzen und die Angriffsfläche zu reduzieren.
- **Kontinuierliche Überwachung und Analyse:** Dies beinhaltet die Echtzeit-Überwachung von Benutzerverhalten, Netzwerkverkehr und Systemaktivitäten zur Erkennung von Anomalien und potenziellen Bedrohungen.

Die Integration von Zero Trust mit Legacy-Systemen ist komplex, da diesen oft grundlegende Sicherheitsfunktionen wie Multi-Faktor-Authentifizierung (MFA) und API-Sicherheit fehlen. Zudem erschweren Netzwerkprobleme wie fest codierte IPs und veraltete Protokolle die Implementierung, und Überwachungsbeschränkungen durch begrenzte Protokollierung sind eine weitere Hürde. Kultureller Widerstand und die Notwendigkeit einer umfassenden Umschulung der Mitarbeiter stellen ebenfalls erhebliche Herausforderungen dar. Lösungsansätze umfassen den Einsatz von Single Sign-On (SSO) mit adaptiver Authentifizierung, API-Gateway-Overlays, Next-Gen-Firewalls, zentralisierten Überwachungssystemen und eine schrittweise Implementierung.

DevSecOps: Dieses Konzept integriert Sicherheit von Anfang an in den gesamten Softwareentwicklungslebenszyklus (SDLC). Die Schlüsselprinzipien umfassen:

Shift Left Security: Sicherheitsmaßnahmen werden frühzeitig im Entwicklungsprozess integriert.

Automatisierte Sicherheitstests: Kontinuierliche Überwachung und Erkennung potenzieller Bedrohungen innerhalb der CI/CD-Pipeline.

Kollaboration: Fördert die Zusammenarbeit zwischen Entwicklungs-, Sicherheits- und Betriebsteams.

In Cloud-Umgebungen beschleunigt DevOps die Softwarebereitstellung, verbessert die Zuverlässigkeit und Skalierbarkeit und optimiert die Kosten. Dies ermöglicht eine schnellere Markteinführung neuer Funktionen.

Zero Trust ist nicht nur eine Sicherheitsstrategie, sondern ein Fundament für die digitale Transformation und die Unterstützung von Remote- und Hybrid-Arbeitsmodellen. Durch die kontinuierliche Überprüfung von Identitäten und Geräten ermöglicht es sicheren Zugriff von überall, was für die moderne, verteilte Arbeitswelt unerlässlich ist. Dies macht Sicherheit vom Hindernis zum geschäftlichen Vorteil.

Zero Trust-Prinzipien wie Least Privilege Access und Mikrosegmentierung sind entscheidend für die Absicherung von DevSecOps-Pipelines. Umgekehrt ermöglicht DevSecOps die Automatisierung der Zero Trust-Implementierung durch „Policy as Code“ und die Integration von Sicherheitstests in den CI/CD-Prozess. Diese beiden Ansätze verstärken sich gegenseitig, um eine durchgängig sichere und agile Softwareentwicklung zu gewährleisten.

Sowohl Zero Trust als auch DevSecOps erfordern einen erheblichen kulturellen Wandel in Organisationen, weg von Silos und hin zu mehr Zusammenarbeit und geteilter Verantwortung. Ohne diesen kulturellen Wandel können selbst die besten Technologien und Strategien scheitern. Dies bedeutet, dass Change Management und das Engagement der Führungskräfte genauso wichtig sind wie technische Implementierungen.

Resilienz durch Datenschutz: Unveränderliche Backups und Disaster Recovery

Unveränderliche Backups (Immutable Backups): Diese Backups können nach dem Schreiben nicht verändert, manipuliert oder gelöscht werden – weder von Administratoren noch von Malware oder Cyberkriminellen. Sie bieten einen robusten Schutz vor Ransomware, da selbst bei einer Infektion eine saubere Wiederherstellung ohne Lösegeldzahlung möglich ist. Der Markt für Objektspeicher mit Unveränderlichkeits-Unterstützung wächst entsprechend dynamisch.

Disaster Recovery (DR) und Business Continuity (BC): Regelmäßige Backups und ein gut orchestrierter Wiederherstellungsplan minimieren Datenverlust und Ausfallzeiten. Multi-Cloud-Strategien verbessern die Ausfallsicherheit und das Disaster Recovery, indem sie Daten und Workloads über mehrere Cloud-Umgebungen verteilen. Dies gewährleistet die Geschäftskontinuität auch bei Ausfällen eines Anbieters.

Während Backups entscheidend für die Wiederherstellung nach Verschlüsselung sind, sind sie gegen Datenexfiltration und die damit verbundene Erpressung wirkungslos. Unveränderliche Backups sind eine notwendige Weiterentwicklung, um die Integrität der Wiederherstellungspunkte zu gewährleisten. Sie müssen jedoch in eine umfassendere Strategie eingebettet sein, die auch die Verhinderung von Datenlecks und die Bewältigung von Reputationsschäden umfasst.

Die Verteilung von Daten und Anwendungen über mehrere Cloud-Anbieter (Multi-Cloud) erhöht die Redundanz und minimiert das Risiko eines Single Point of Failure. Dies ist eine direkte Antwort auf die zunehmende Professionalisierung von Ransomware-Angreifern, die versuchen, auch Backup-Systeme zu kompromittieren. Eine Multi-Cloud-DR-Strategie bietet eine robustere Absicherung gegen großflächige Ausfälle oder gezielte Angriffe auf einen einzelnen Cloud-Anbieter.

Der menschliche Faktor: Cybersicherheitsbewusstsein und Schulung

Menschliches Versagen bleibt eine der Hauptursachen für Datenlecks. Viele Ransomware-Infektionen beginnen mit Phishing-E-Mails, die ahnungslose Mitarbeiter dazu verleiten, bösartige Inhalte zu öffnen oder herunterzuladen. Umfassende Cybersicherheitsschulungen können die Wahrscheinlichkeit menschlicher Fehler, die zu Verstößen führen, erheblich reduzieren.

Schulungsprogramme sollten realistische Szenarien, interaktive Lernmodule und gamifizierte Aktivitäten umfassen, um das Engagement zu fördern. Themen sollten KI-gestützte Bedrohungen, Social Engineering, Internet-Sicherheit, physische Bedrohungen und Insider-Bedrohungen abdecken.

Die Daten zeigen, dass trotz aller technologischen Fortschritte der Mensch oft das schwächste Glied in der Sicherheitskette bleibt. Dies bedeutet, dass Investitionen in Technologie ohne gleichzeitige Investitionen in das Bewusstsein und die Schulung der Mitarbeiter nur begrenzt wirksam sind. Die Mitarbeiter müssen zu proaktiven Teilnehmern der Sicherheitsstrategie werden.

Da KI-gestützte Phishing-Angriffe immer ausgefeilter und personalisierter werden, müssen auch die Schulungsinhalte kontinuierlich angepasst werden. Statische Schulungen sind nicht mehr ausreichend; es bedarf dynamischer Simulationen und Echtzeit-Feedback, um Mitarbeiter auf die neuesten Angriffstaktiken vorzubereiten.

Fortgeschrittene Incident Response: SOAR und EDR

SOAR (Security Orchestration, Automation, and Response): SOAR-Plattformen koordinieren, führen aus und automatisieren Aufgaben zwischen verschiedenen Personen und Tools auf einer einzigen Plattform. Sie nutzen KI, um Verhaltensmuster zu lernen und ähnliche Bedrohungen vorherzusagen. Die Vorteile umfassen eine beschleunigte Reaktion auf Vorfälle, die Reduzierung menschlicher Fehler, eine erhöhte Effizienz und eine proaktivere Sicherheitshaltung. SOAR kann Phishing-Vorfälle und Malware-Ausbrüche automatisieren, indem es E-Mails unter Quarantäne stellt oder infizierte Systeme isoliert.

EDR (Endpoint Detection and Response): EDR-Lösungen zeichnen Endpunkt-Systemverhalten auf, nutzen Datenanalysen zur Erkennung verdächtigen Verhaltens, blockieren bösartige Aktivitäten und geben Empfehlungen zur Wiederherstellung. Sie ermöglichen schnelle und entschlossene Gegenmaßnahmen, indem potenziell kompromittierte Hosts vom Netzwerk isoliert werden („Network Containment“). EDR bietet Echtzeit-Sichtbarkeit und ermöglicht die direkte Behebung von Bedrohungen ohne Leistungseinbußen.

Digitale Forensik und Log-Analyse: KI beschleunigt die forensische Analyse durch die Automatisierung der Log-Korrelation und Speicheranalyse. Sie kann Ereignisse sequenzieren und grafische Zeitlinien erstellen, um den Fortschritt eines Angriffs zu visualisieren.

Angesichts der extrem kurzen „Dwell Times“ von Ransomware-Angriffen (laut Secureworks 2023 unter 24 Stunden in über der Hälfte der Fälle) ist eine manuelle Incident Response nicht mehr praktikabel. SOAR und EDR ermöglichen eine Reaktion in Maschinengeschwindigkeit, indem sie Erkennung, Analyse und Eindämmung automatisieren. Dies ist entscheidend, um den „Breakout Time“ der Angreifer zu unterbieten und den Schaden zu minimieren.

SOAR-Plattformen integrieren Daten und Tools aus verschiedenen Sicherheitslösungen zu einer zentralen Sicht auf Vorfälle. Dies ist besonders wichtig in komplexen, verteilten Cloud-Umgebungen, wo fragmentierte Sichtbarkeit zu blinden Flecken führen kann. Die Orchestrierung über verschiedene Tools hinweg stellt sicher, dass Reaktionen koordiniert und konsistent sind.

Die Zukunft der Authentifizierung: Passkeys

Passkeys sind eine neue Authentifizierungsmethode, die auf FIDO-Standards basiert. Sie ermöglichen Benutzern, sich bei Apps und Websites mit demselben Prozess anzumelden, den sie zum Entsperren ihres Geräts verwenden, wie Biometrie, PIN oder Muster. Sie verwenden Public-Key-Kryptographie, wodurch der private Schlüssel sicher auf dem Gerät des Benutzers gespeichert und niemals an den Server übertragen wird.

Die Vorteile von Passkeys sind vielfältig:

- **Phishing-resistent:** Passkeys sind an die Identität einer Website oder App gebunden, was bedeutet, dass sie nicht für Phishing-Angriffe verwendet werden können.
- **Verbesserte Benutzererfahrung:** Sie bieten eine schnellere und nahtlosere Anmeldung, da keine komplexen Passwörter eingegeben werden müssen.
- **Sichere Alternative zu 2FA/MFA:** Passkeys können traditionelle MFA-Methoden wie SMS-OTPs ersetzen, die anfällig für SIM-Swapping und Abfangen sind. Sie erfüllen MFA-Anforderungen in einem einzigen Schritt.
- **Plattformübergreifende Kompatibilität:** Große Plattformen wie Apple, Google und Microsoft unterstützen FIDO-basierte Passkeys und arbeiten aktiv an deren Interoperabilität.

Trotz der Vorteile gibt es Herausforderungen: Die kontinuierliche Unterstützung und Kompatibilität über alle Geräte und Dienste hinweg ist noch nicht konsistent. Zudem ist die Wiederherstellung von Konten immer noch an Passwörter oder Benutzer-IDs gebunden.

Da Passkeys phishing-resistent sind und keine Passwörter übertragen werden, adressieren sie direkt die größte Schwachstelle in der Cybersicherheit: den Menschen, der durch Social Engineering manipuliert wird. Dies ist ein entscheidender Schritt, um die Effektivität von KI-gestützten Phishing-Angriffen zu reduzieren.

Trotz der Vorteile gibt es Herausforderungen bei der Akzeptanz und Implementierung von Passkeys, insbesondere bei der Kompatibilität mit älteren Systemen und Geräten. Unternehmen müssen eine klare Übergangsstrategie entwickeln, die die Benutzerakzeptanz durch Schulung und eine nahtlose Benutzererfahrung fördert, um die Vorteile dieser Technologie voll ausschöpfen zu können.

Fazit: Navigation in einer sich entwickelnden Bedrohungslandschaft

Die Evolution von Ransomware zu „Ransomware 2.0“ und die zunehmende Professionalisierung der Cyberkriminalität, verstärkt durch den Einsatz von Künstlicher Intelligenz, stellen eine existenzielle Bedrohung für Unternehmen und kritische Infrastrukturen dar. Die Angreifer agieren schneller, gezielter und nutzen ausgeklügelte Taktiken wie Double und Triple Extortion.

Um dieser Bedrohung zu begegnen, ist ein proaktiver, mehrschichtiger und adaptiver Sicherheitsansatz unerlässlich. Dies beinhaltet die Implementierung von Zero Trust-Architekturen, die Integration von DevSecOps-Praktiken, den Einsatz unveränderlicher Backups und robuster Disaster-Recovery-Strategien. Der menschliche Faktor bleibt dabei entscheidend: Umfassende und kontinuierliche Schulungen zum Cybersicherheitsbewusstsein sind unerlässlich, um Mitarbeiter zur ersten Verteidigungslinie zu machen. Fortgeschrittene Incident-Response-Systeme wie SOAR und EDR, die durch KI unterstützt werden, sind notwendig, um Angriffe in Maschinengeschwindigkeit zu erkennen und einzudämmen. Schließlich bieten neue Authentifizierungsmethoden wie Passkeys einen vielversprechenden Weg, um die größte Schwachstelle – das Passwort – zu eliminieren und die Phishing-Resistenz zu erhöhen.

Die Zukunft der Cybersicherheit ist ein kontinuierliches Wettrüsten zwischen Angreifern und Verteidigern, bei dem KI eine immer zentralere Rolle spielen wird. Unternehmen, die in der Lage sind, ihre Verteidigungsstrategien kontinuierlich anzupassen, in fortschrittliche Technologien zu investieren und eine starke Sicherheitskultur zu fördern, werden am besten positioniert sein, um in dieser sich entwickelnden Bedrohungslandschaft zu bestehen.

Ihr nächster Schritt

Wenn 88 Prozent der Angriffe außerhalb der Arbeitszeit laufen, entscheidet sich die Abwehr an einer unbequemen Frage: Was passiert bei Ihnen zwischen Freitagabend und Montagmorgen, wenn ein Konto sich anmeldet, das sich sonst nie anmeldet? Wir gehen das mit Ihnen durch – Erkennung, Eskalationsweg, unveränderliche Backups, besetzt aus unserer [Cybersecurity-Expertise](#) und senior gesteuert aus Deutschland.

Häufige Fragen

Warum reichen Backups gegen moderne Ransomware nicht mehr?

Weil Ransomware 2.0 die Daten erst stiehlt und dann verschlüsselt (Double Extortion). Selbst wer sauber wiederherstellen kann, wird mit der Veröffentlichung der gestohlenen Daten erpresst. Backups bleiben essenziell – am besten unveränderlich –, sind aber nur noch ein Baustein von mehreren.

Was macht Ransomware heute so gefährlich?

Die Professionalisierung. Ransomware-as-a-Service verkauft fertige Angriffsbaukästen inklusive Support, und KI macht Phishing überzeugender und skalierbarer. Angriffe sind schneller, leiser und gezielter geworden – oft mit vorheriger Ausspähung des Opfers.

Wie schützt man sich wirksam?

Mehrschichtig statt mit einer einzelnen Maßnahme: Zero-Trust-Architektur, unveränderliche Backups mit getestetem Wiederherstellungsplan, Sicherheit im Entwicklungszyklus (DevSecOps), phishing-resistente Authentifizierung wie Passkeys sowie automatisierte Erkennung und Reaktion (SOAR/EDR). Dazu Schulung, denn menschliches Versagen bleibt ein Hauptrisiko.

Was bedeuten Double und Triple Extortion?

Bei Double Extortion stehlen Angreifer die Daten vor der Verschlüsselung und drohen mit Veröffentlichung – ein Backup allein löst das Problem nicht mehr. Triple Extortion setzt zusätzlich Druck auf, etwa über DDoS-Angriffe oder direkte Drohungen gegen Kunden und Partner des Opfers.

Was ist Ransomware-as-a-Service (RaaS)?

RaaS ist ein arbeitsteiliges Geschäftsmodell der Cyberkriminalität: Entwickler stellen Schadsoftware und Infrastruktur bereit, Partner führen die Angriffe aus und teilen die Beute. Diese Professionalisierung senkt die Einstiegshürde und erhöht Zahl und Wirksamkeit der Angriffe.

Warum sind kritische Infrastrukturen (ICS/OT) besonders gefährdet?

Industrielle Steuerungs- und Betriebstechnik (ICS/OT) ist oft langlebig, schwer zu patchen und zunehmend vernetzt – ein Ausfall hat unmittelbare physische und gesellschaftliche Folgen. Das macht diese Systeme zu einem attraktiven, druckstarken Ziel für Erpresser.

Wie verschärft KI die Ransomware-Bedrohung?

KI macht die vorgelagerten Schritte gefährlicher: überzeugenderes Phishing als Einstieg und anpassungsfähige Schadsoftware, die Erkennung umgeht. Dieselbe Technik stärkt allerdings auch die Verteidigung – über prädiktive Analysen und automatisierte Reaktion.

Thematische Vertiefungen

[Cybersecurity-Expertise](#)

[Zero Trust](#)

[KI im Kampf gegen Cyberkriminalität](#)

Quellen

- **NCC Group: Monthly Threat Pulse, Review of May 2024.** Belegt 176 Angriffe der RaaS-Bande LockBit 3.0 im Mai 2024, entsprechend 37 % aller in diesem Monat registrierten Ransomware-Vorfälle. – <https://www.nccgroup.com/us/newsroom/ncc-group-monthly-threat-pulse-review-of-may-2024/>
- **IBM: Cost of a Data Breach Report 2024.** Historischer Vergleichswert: globaler Schnitt 4,88 Mio. USD. – <https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs>
- **US-Justizministerium: Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside,** Pressemitteilung vom 07.06.2021. Belegt die Loesegeldzahlung von rund 75 Bitcoin durch Colonial Pipeline am 8. Mai 2021 und die Beschlagnahme von 63,7 Bitcoin. – <https://www.justice.gov/archives/opa/pr/departement-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>
- **US-Senat, Committee on Homeland Security and Governmental Affairs: Anhoerung mit Colonial-Pipeline-CEO Joseph Blount,** 08.06.2021. Belegt die Bezifferung des Loesegelds auf 4,4 Mio. US-Dollar durch das Unternehmen selbst. – <https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Testimony-Blount-2021-06-08.pdf>
- **CISA: #StopRansomware Guide** – <https://www.cisa.gov/stopransomware/ransomware-guide>
- **Sophos: Active Adversary Report for Tech Leaders 2023.** Historischer Vergleichswert: Dwell Time 5 Tage, 81 % der Payloads außerhalb der Arbeitszeiten. – <https://www.sophos.com/en-us/press/press-releases/2023/08/dwell-time-time-start-attack-when-its-detected-shrinks-8-days-first>
- **Secureworks: State of the Threat 2023 (Ransomware-Dwell-Time unter 24 h in über 50 % der Fälle)** – <https://www.prnewswire.com/apac/news-releases/ransomware-dwell-time-hits-low-of-24-hours-301999828.html>
- **Searchlight Cyber: Ransomware in H1 2024 (+56 % aktive Gruppen, über 70 Gruppen)** – <https://slcyber.io/press/searchlight-cyber-report-reveals-rapid-changes-in-the-ransomware-landscape-over-six-months/>
- **Sophos: Active Adversary Report 2026 – Identity attacks dominate as threat groups proliferate.** Auswertung von 661 IR- und MDR-Fällen zwischen dem 1.11.2024 und dem 31.10.2025 in 70 Ländern und 34 Branchen. Belegt 88 % der Payloads und 79 % der Datenexfiltration außerhalb der Geschäftszeiten, drei Tage mittlere Verweildauer, 3,4 Stunden bis zum AD-Server, 67 % identitätsbezogene Vorfälle, fehlende MFA in 59 % der Fälle sowie 51 Ransomware-Marken. – <https://www.sophos.com/en-us/press/press-releases/sophos-active-adversary-report-2026-identity-attacks-dominate-as-threat-groups-proliferate>
- **IBM: Cost of a Data Breach Report 2026.** Erhebung des Ponemon Institute über 602 Organisationen in 16 Ländern und Regionen und 17 Branchen, Datenpannen von März 2025 bis Februar 2026. Belegt den globalen Durchschnitt von 4,99 Mio. USD und das Plus von 12 % gegenüber dem Vorjahr. – <https://www.ibm.com/reports/data-breach>