



Booklet | Oktober 2025

Ransomware

PAY, BABY, PAY

OPSWAT.

Schutz der kritischen Infrastrukturen weltweit

Cyberbedrohungsprävention von Endpoint bis Cloud

OPSWAT-Lösungen werden von mehr als 1.700 Organisationen, Regierungen und Institutionen weltweit genutzt, um ihre kritischen Netzwerke zu schützen. Unsere Plattform löst ein breites Spektrum spezifischer Kundenherausforderungen im Bereich kritischer Infrastrukturen.

- E-Mail-Sicherheit
- Anwendungs- und Dateisicherheit
- Speichersicherheit
- Schutz von Wechseldatenträgern
- Lieferkettensicherheit
- Cross-Domain-Sicherheit
- OT-Sicherheit
- Zugriffs- und Endpunktsicherheit
- Sicheres Managed File Transfer
- Malware-Analyse und Threat Intelligence
- OEM

opswat.com

DER NEUE IT SECURITY CYBER RISK INDEX: DER PULS DER CYBER-RESILIENZ



LIEBE LESERINNEN UND LESER,

Der neue it security Cyber Risk Index Deutschland (ITSCRI-DE) zeigt mit einem Score von 73 Punkten ein deutliches Warnsignal: Das Cyberrisiko für deutsche Unternehmen ist dramatisch gestiegen – allein im Vergleich zum Vorjahr um 29%. Ransomware, Zero-Day-Exploits und Angriffe auf Lieferketten setzen die größten Hebel an – und treffen damit genau die Achillesfersen unserer digitalisierten Wirtschaft.

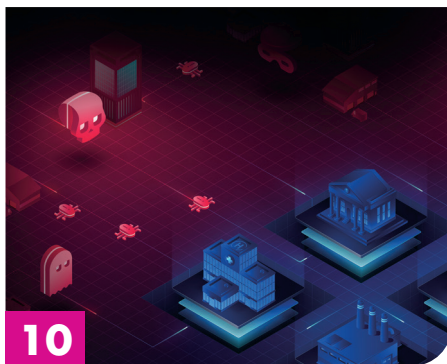
Der Index entlarvt eine unbequeme Wahrheit: Cybersicherheit ist längst nicht mehr optional, sondern entscheidet über Wettbewerbsfähigkeit und Zukunftsfähigkeit. Wer glaubt, klassische Antivirenlösungen oder jährliche Security-Audits reichen aus, riskiert nicht nur IT-Ausfälle, sondern massive Reputations- und Finanzschäden.

Gerade weil Cyberangriffe zunehmend durch KI, Automatisierung und Ransomware-as-a-Service skaliert werden, ist der ITSCRI-DE mehr als eine statistische Momentaufnahme. Er ist ein Weckruf.

Die Botschaft ist klar: Cyberrisiken lassen sich nicht „wegreden“. Sie sind messbar, vergleichbar – und brandgefährlich. Der Index zeigt, wo wir stehen. Die Frage ist: Wer handelt rechtzeitig, und wer liest diese Zahlen später im Rückblick – als Mahnung eines verpassten Moments?

Herzlichst, Ihr

Ulrich Parthier
Publisher it security



6 | Cyber-Profiling

Wenn Angreifer mehr über Unternehmen wissen als sie selbst

10 | Mehrschichtige Sicherheit für KRITIS

Abwehrstrategien gegen Ransomware und andere Bedrohungen

14 | Ransomware in ihre Schranken weisen

Definition, Angriffsphasen und Tipps zur Prävention

20 | Ransomware bleibt hochrisiko

3 Gründe für die wachsende Gefahr

26 | Insider-Bedrohungen

Technische Schutzarchitekturen gegen Insider-Bedrohungen

36 | Ransomware: Wer stillsteht, verliert

Kein Pardon

40 | Ransomware-Schutz

Ganzheitliche Abwehr, schnelle Reaktion, sichere Wiederherstellung

44 | Ransomware-Abwehr

Mehrstufige Verteidigungsstrategien erforderlich



IT Verlag
für Informationstechnik GmbH

Ludwig-Ganghofer-Str. 51
83624 Otterfing
Tel: +49 8104 6494-0
Fax: +49 8104 6494-22
www.it-daily.net

Herausgeber: Ulrich Parthier
Geschäftsführer: Ulrich Parthier und Vasiliki Miridakis
Chefredaktion: Silvia Parthier
Redaktionsassistentz und Sonderdrucke: Eva Neff
E-Mail für Leserbriefe: redaktion@it-verlag.de
Objektleitung: Ulrich Parthier

Autoren: Sören Kohls (Kaspersky), Holger Fischer (OPSWAT), Ulrich Parthier, Kay Ernst (Zero Networks), Philip Huisgen (DATAKOM), Andreas Müller (Delinea).

Alle Autoren erreichen Sie über die Redaktion. Wir reichen Ihre Anfragen gerne an die Autoren weiter.

Manuskripteinsendungen: Für eingesandte Manuskripte wird keine Haftung übernommen. Sie müssen frei sein von Rechten Dritter. Mit der Einsendung erteilt der Verfasser die Genehmigung zum kostenlosen weiteren Abdruck in allen Publikationen des Verlages. Für die mit Namen oder Signatur des Verfassers gekennzeichneten Beiträge haftet der Verlag nicht. Die in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Übersetzung, Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen nur mit schriftlicher Genehmigung des Verlages. Für Fehler im Text, in Schaltbildern, Skizzen, Listings und dergleichen, die zum Nichtfunktionieren oder eventuell zur Beschädigung von Bauelementen oder Programmteilen führen, übernimmt der Verlag keine Haftung. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Ferner werden Warennamen ohne Gewährleistung in freier Verwendung benutzt.

Layout: IT Verlag für Informationstechnik GmbH
Fotos: Wenn nicht anders angegeben: shutterstock.com

Beteiligungsverhältnisse nach § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: 100% des Gesellschafter-kapitals hält Ulrich Parthier, Sauerlach.

CYBER-PROFILING

WENN ANGREIFER MEHR ÜBER UNTERNEHMEN WISSEN ALS SIE SELBST

Cyberangriffe beginnen selten mit einer auffälligen Aktion wie dem Starten einer Schadsoftware oder dem Ausnutzen einer Zero-Day-Schwachstelle. Meist läuft die entscheidende Phase unbemerkt im Hintergrund ab: das Sammeln, Prüfen und Kombinieren von Informationen über ein Zielunternehmen. Dieses Cyber-Profilung ist die leise Vorbereitung, bei der ein Angreifer ein umfassendes Bild der potenziellen Angriffsfläche erstellt. Je genauer dieses digitale Unternehmensprofil ist, desto zielgerichteter und schneller lassen sich die nächsten Schritte planen.

Was dabei entsteht, ist eine Art „digitaler Zwilling“ des Unternehmens – allerdings aus der Sicht eines potenziellen Angreifers. Für den Aufbau nutzen Kriminelle alles, was sie in die Finger bekommen: offen zugängliche Unternehmensinformationen, Daten aus alten Sicherheitsvorfällen, Einträge in Datenbanken, Forenbeiträge und nicht zuletzt Ergebnisse aus gezielten technischen Scans. Mit Tools wie Shodan oder Censys durchsuchen sie zudem das Internet nach exponierten Systemen, offenen Ports und Konfigurationen, die einen Einstieg ermöglichen könnten.

Der Marktplatz im Untergrund

Einige dieser Informationen werden dabei im Dark Net gehandelt, die sich andere Cyberkriminelle wiederum zusammensuchen können – natürlich gegen entsprechendes Entgelt. Dabei herrscht auf diesen organisierten Marktplätzen Arbeitsteilung: Initial Access Broker sind auf den Verkauf kompromittierter Zugänge spezialisiert – häufig zu VPN-, RDP- oder Webmail-Systemen. Damit der Käufer den Wert einschätzen kann, liefern sie oft Details wie Serverstandort, Systemrolle oder sogar Screenshots des Zugriffs.

Betreiber von sogenannten Stealer-Logs setzen auf Schadsoftware wie RedLine, Raccoon oder Lumma, die Zugangsdaten, Cookies und Session-Tokens direkt von



infizierten Endpunkten abgreifen. Andere Akteure, die man als Leak-Kombinatoren kennt, bündeln alte und neue Datenlecks, reichern sie mit Kontextinformationen wie Abteilungszugehörigkeit oder Funktion im Unternehmen an und schaffen damit hochgradig präzise Datensätze – ideal für zielgerichtete Phishing-Angriffe oder Business Email Compromise (kurz: BEC). Selbst Escrow-Dienste haben ihren festen Platz in dieser Schattenwirtschaft, indem sie Transaktionen absichern und Zahlungen erst freigeben, wenn der Käufer den Erhalt und die Funktionalität der Daten bestätigt.

Der Markt dafür ist lukrativ. Aktuelle Kaspersky-Analysen zeigen, dass die Preise für Zugänge und Informationen im Dark Web stark variieren und von der Art sowie der Qualität der angebotenen Daten abhängen.

Initial Access zu Unternehmensnetzwerken, etwa über kompromittierte RDP- oder VPN-Zugänge, wird bereits ab rund 2.000 US-Dollar gehandelt, kann bei besonders privilegierten oder strategisch wertvollen Zielsystemen jedoch bis zu 50.000 US-Dollar erreichen ^[1]. Für Google-Play-Loader oder App-Install-Kampagnen zahlen Käufer zwischen 2.000 und 20.000 US-Dollar, während vollständige Google-Play-Entwicklerkonten in der Regel zwischen 60 und 200 US-Dollar kosten ^[2]. Deutlich günstiger sind Stealer-Logs, die oft schon ab 5 US-Dollar pro Datensatz verfügbar sind und dennoch Zugang zu einer Vielzahl sensibler Online-Konten enthalten können ^[3].

Wie aus einem Cyber-Profil ein Angriff wird

Ist das Profil vollständig, beginnt der zweite Teil des Angriffs. Zunächst wird geprüft, ob die ermittelten Zugänge noch gültig und die Systeme erreichbar sind. Funktioniert der Login, folgt der eigentliche Einstieg – sei es per direkter Anmeldung, über eine bekannte Schwachstelle oder durch das Ausnutzen einer noch aktiven Session.

Von hier aus arbeiten sich Angreifer oft systematisch weiter vor: Lateral Movement und Privilege Escalation sind Standard, um aus einem einzelnen Nutzerkonto schrittweise Zugriff auf weitere Systeme oder ganze Netzwerke zu erhalten. In manchen Fällen reichen Stealer-Logs in Kombination mit öffentlich zugänglichen Informationen, um innerhalb weniger Stunden vollständigen Zugriff zu erlangen. In anderen Szenarien müssen Angreifer zusätzliche Werkzeuge wie Shodan einsetzen oder Exploits ausführen, um ihre Reichweite auszubauen.

Die Monetarisierung dieser Aktivitäten ist flexibel und marktorientiert. Sie reicht von Ransomware-Angriffen, bei denen Systeme verschlüsselt und anschließend Lösegeld gefordert wird, über den gezielten Diebstahl und Weiterverkauf sensibler Kundendaten bis hin zur Übergabe des erlangten Zugangs an andere Gruppen im Darknet, die diesen für eigene Operationen nutzen. Jede dieser Optionen ist Teil eines eingespielten Wertschöpfungsprozesses, der im Untergrund seit Jahren perfektioniert wird.

Perspektivwechsel: Vom Opfer zum Ermittler. External Attack Surface Management (EASM) hilft die Angriffsfläche von Unternehmen zu reduzieren (Bildquelle: Kaspersky)



Perspektivwechsel: Vom Opfer zum Ermittler – oder: wie man sich davor schützt

Unternehmen können diesem Ablauf nicht vollständig entgehen – Cyber-Profiling lässt sich in einer vernetzten Welt kaum verhindern. Wohl aber lässt sich der eigene Wissensstand so erweitern, dass man selbst früher als der Angreifer erkennt, welche Informationen im Umlauf sind. Dieser Perspektivwechsel, das eigene Unternehmen durch die Augen eines Angreifers zu betrachten, macht sichtbar, welche Dienste offen erreichbar sind, ob kompromittierte Anmeldedaten im Umlauf sind, ob gefälschte Social-Media-Profile oder Phishing-Domains aktiv sind und ob Hinweise auf geplante Angriffe existieren.

Die kontinuierliche Überwachung von OSINT-Quellen, Untergrundforen und Darknet-Marktplätzen, ergänzt durch technische Oberflächenanalysen, liefert ein realistisches Bild der eigenen Angriffsfläche. Dieses sogenannte External Attack Surface Management (EASM) ermöglicht die Reduzierung der eigenen Angriffsfläche.

Takedown-Maßnahmen können gefälschte Profile, Domains oder betrügerische Apps aus dem Verkehr ziehen, bevor sie Schaden anrichten. Threat-Intelligence-Lösungen wie Kaspersky Digital Footprint Intelligence ^[4] bieten genau diesen Blick von außen: Sie identifizieren exponierte Systeme, kompromittierte Daten und gefälschte Online-Präsenzen – und ermöglichen es, Gegenmaßnahmen einzuleiten, bevor aus einem digitalen Profil ein realer Angriff wird.

**MEHR
WERT**



[1]



<https://www.kaspersky.com/about/press-releases/cybercriminals-sell-access-to-companies-via-the-dark-web-from-2000>

[2]



<https://securelist.com/google-play-threats-on-the-dark-web/109452/>

[3]



<https://www.kaspersky.com/about/press-releases/data-stealing-malware-infections-increased-seven-fold-since-2020-kaspersky-experts-say>

[4]



<https://dfi.kaspersky.com/de>



Sören Kohls
Head of Channel DACH
Kaspersky
www.kaspersky.com

MEHRSCICHTIGE SICHERHEIT FÜR KRITIS

ABWEHRSTRATEGIEN GEGEN RANSOMWARE UND ANDERE BEDROHUNGEN

Ob Ransomware oder andere Cyberbedrohungen: Angriffe entwickeln sich rasant weiter und erfolgen immer gezielter und professioneller. Moderne Sicherheitstechnologien setzen daher auf Erkennung und Abwehr, bevor es zu einer Infektion kommt. Längst geht es Angreifern nicht mehr nur um schnelle Erpressung, sondern um systematische Störungen gesellschaftlicher Kernfunktionen. Besonders im Fokus: Kritische Infrastrukturen.

Ob Angriffe auf Energie- und Versorgungsnetze, Verkehrssysteme, staatliche Einrichtungen oder den Finanzsektor – erfolgreiche Attacken auf KRITIS können immense wirtschaftliche Schäden verursachen und die öffentliche Sicherheit ernsthaft gefährden. Laut der European Union Agency for Cybersecurity (ENISA) hinken insbesondere Verwaltung, Gesundheitswesen, Gasversorgung und ICT-Services in ihrer Sicherheitsarchitektur hinterher. Um dieser Bedrohungslage zu begegnen, brauchen KRITIS-Betreiber einen robusten, mehrschichtigen Sicherheitsansatz, der ihre Cyberresilienz nachhaltig stärkt.

Die aktuelle Bedrohungslandschaft für kritische Infrastrukturen

Kritische Infrastrukturen geraten verstärkt ins Visier, sei es durch staatlich unterstützte Hackergruppen, die Spionage betreiben oder Dienste sabotieren, oder durch Cyberkriminelle, die auf Lösegeldzahlungen spekulieren. Angriffe erfolgen gezielt mit Techniken wie dateibasierter Malware, Botnetzen, Zero-Day-Exploits oder Advanced Persistent Threats (APTs). Viele starten in IT-Netzwerken, verlagern sich jedoch zunehmend auf die Operational Technology (OT), um massive Betriebsstörungen auszulösen.



ANGESICHTS DER WACHSENDEN VERNETZUNG VON IT- UND OT-SYSTEMEN MÜSSEN WIR DIE SICHERHEIT UNSERER KRITISCHEN INFRASTRUKTUREN NEU DENKEN. NUR MIT EINER MEHRSCHTIGEN SICHERHEITSSTRATEGIE KÖNNEN WIR RANSOMWARE- UND SUPPLY-CHAIN-ANGRIFFE EFFEKTIV VERHINDERN.

Holger Fischer, Director Sales EMEA Central, OPSWAT

Besonders kritisch ist der Datenaustausch zwischen IT- und OT-Systemen: Die zunehmende Vernetzung eröffnet neue Angriffsflächen. Während IT-Systeme durch etablierte Schutzmechanismen wie Firewalls, Virens Scanner und E-Mail-Security gesichert sind, wurden OT-Systeme – etwa industrielle Steuerungen oder Produktionsanlagen – oft vernachlässigt. Sie sind häufig veraltet, schwer wartbar und nicht für moderne Bedrohungen ausgelegt. Ohne klare Segmentierung oder sichere Schnittstellen können Angreifer gezielt von IT in OT eindringen, mit gravierenden Folgen für Verfügbarkeit und Sicherheit.

Security-Herausforderungen für KRITIS-Betreiber

Sicherheitsteams stehen vor zahlreichen Herausforderungen, die ihre Fähigkeit einschränken, Bedrohungen gegen KRITIS-Betreiber wirksam abzuwehren. Oft arbeiten sie unter engen finanziellen und personellen Vorgaben und ohne ausreichende Unterstützung der Geschäftsleitung. Zwischen geplanten Maßnahmen und bewilligten Ressourcen klappt häufig eine Lücke, sodass Teams sich auf die dringendsten Risiken beschränken und auf neue Angriffstaktiken nur unzureichend vorbereitet sind. Hinzu kommt, dass die Konvergenz von IT und OT neue Anforderungen schafft: Sicherheitsteams müssen zunehmend Systeme schützen, mit denen sie bislang kaum Erfahrung haben.

In vielen KRITIS-Organisationen sind SCADA-Systeme für Fernzugriff und Telemetrie direkt mit Standard-IT-Netzwerken verbunden – eine Ausweitung der Angriffsfläche, die spezielles Fachwissen erfordert. Fehlendes IT- und OT-Know-how führt

zu Lücken beim Verständnis, wie sich IT-Bedrohungen auf OT-Systeme auswirken. Zugleich erschwert der Mangel an qualifiziertem Personal den sicheren Betrieb komplexer hybrider Umgebungen mit Cloud-Speicher, Open-Source-Tools und vernetzten Plattformen.

Angesichts dieser Hürden und der zunehmenden Raffinesse von Cyberangriffen ist die Einführung mehrschichtiger Sicherheitsstrategien wie dem Defense-in-Depth-Ansatz unerlässlich.

Mehrschichtige Sicherheit: Defense-in-Depth-Ansatz für KRITIS

Defence-in-Depth ist ein mehrschichtiges Sicherheitskonzept, das Abhängigkeiten von einzelnen Schwachstellen minimiert und so Erkennung, Reaktion und Neutralisierung von Bedrohungen verbessert. Ziel ist der Schutz kritischer Ressourcen und der Erhalt eines unterbrechungsfreien Betriebs.

Die **Netzwerksicherheit** bildet die erste Verteidigungslinie: Firewalls, Gateways, Datendioden und Netzwerksegmentierung regulieren den Datenverkehr, isolieren Bedrohungen und verhindern unbefugten Zugriff oder Datenexfiltration. Speziell in OT- und ICS-Umgebungen schützen hardwarebasierte, unidirektionale Datendioden vor Schadsoftware aus unsicheren Netzen, ohne den notwendigen Informationsfluss zu behindern.

Beim Thema **Datensicherheit** gilt es zu verhindern, dass in Dateien versteckte Malware sensible Systeme erreicht. **Multiscanning** mit bis zu 30 parallel arbeitenden Malware-Engines in der OPSWAT **MetaDefender Core-Plattform** erkennt bekannte Schadsoftware mit außergewöhnlich hoher Erfolgsquote, während **Sandbox-Analysen** und **Threat Intelligence** unbekannte Angriffe aufdecken. **Deep Content Disarm & Reconstruction (CDR)** bereinigt Dateien gründlich, indem es potenziell schädliche Bestandteile - unabhängig von ihrer Bekanntheit - entfernt und die Inhalte auf Basis sicherer Elemente neu aufbaut, ehe sie in isolierten Tresoren gespeichert werden. So ist ihre Integrität sichergestellt, bevor sie in geschützte Netzwerke gelangen.

Für den sicheren Datentransfer in und aus kritischen Netzwerken sorgen beispielsweise der MetaDefender Kiosk und MetaDefender Managed File Transfer:



Bildquelle: OPSWAT

Sie bieten kontrollierte, isolierte Schnittstellen, die Datenströme überwachen und nur gründlich geprüfte Inhalte passieren lassen.

Ergänzend schützt die **Endpunktsicherheit** Laptops, Desktops und andere Geräte durch die Kombination mehrerer Erkennungsmodule, Verhaltensanalysen und aktueller Threat-Feeds – auch gegen Zero-Day-Bedrohungen. **E-Mail-Schutz** blockiert Phishing-Versuche sowie schädliche Anhänge oder Links und trägt so zur Gesamtresilienz bei.

Gemeinsam bilden diese Sicherheitsschichten innerhalb der OPSWAT MetaDefender Core-Plattform ein geschlossenes, robustes Abwehrsystem, das KRITIS-Betreiber wirksam gegen zunehmend komplexe Cyberangriffe absichert.

OPSWAT | www.opswat.com

**GUT ZU
WISSEN**



OPSWAT.

RANSOMWARE IN IHRE SCHRANKEN WEISEN

DEFINITION, ANGRIFFSPHASEN UND TIPPS ZUR PRÄVENTION

Ransomware-Angriffe haben sich im Jahr 2025 mehr als verdoppelt und stellen damit für 92 Prozent der Branchen eine der größten Bedrohungen dar. Auch die Zahl der aktiven Ransomware-Banden ist im letzten Jahr sprunghaft angestiegen. Derzeit sind 65 Gruppen aktiv, wobei die aktivsten unter ihnen ihre Opferzahl im Vergleich zum Vorjahr um mehr als 200 Prozent gesteigert haben.

Kay Ernst von Zero Networks gibt einen Überblick zum Thema und erläutert den Effekt von Mikrosegmentierung auf die Ausbreitung von Ransomware.

Ransomware ist eine Art von Schadcode, der Dateien oder Systeme verschlüsselt und somit unzugänglich macht, bis ein Lösegeld gezahlt wird. Angreifer verlangen oft Zahlungen in Kryptowährungen, um die Rückverfolgung zu erschweren. Das „Double Extortion“-Modell, also der doppelten Erpressung mit Ransomware macht sie besonders gefährlich: Zusätzlich zur Sperrung von Dateien exfiltrieren viele Ransomware-Varianten Daten und drohen mit deren Veröffentlichung oder Verkauf, wenn das Lösegeld nicht gezahlt wird.

Warum sind Ransomware-Angriffe so schwer zu stoppen?

Da das Ransomware-Geschäft so profitabel ist, können Cyberkriminelle talentiert Top-Kräfte einstellen, um Zero-Day-Lücken zu finden, maßgeschneiderte Tools (die schwerer zu erkennen sind) zu entwickeln und fortschrittliche Ausweichtechniken wie Hypervisor Jackpotting und die Umgehung von EDRs zu erforschen.



Mit anderen Worten: Ransomware-Banden verfügen über Ressourcen und Fähigkeiten, die früher nur Nationalstaaten vorbehalten waren, sodass ihre Opfer militärische Abwehrmaßnahmen benötigen, um sich angemessen zu schützen. Ransomware-Angriffe sind in der Regel hochentwickelt; sie nutzen oft legitime Netzwerkfunktionen aus, was es unglaublich schwierig macht, Ransomware zu erkennen, bevor es zu spät ist.

Wie funktioniert Ransomware?

Es gibt zwar verschiedene Arten von Ransomware, aber in den meisten Fällen werden Dateien oder Systeme nach einer Phase der heimlichen Bewegung durch das Netzwerk verschlüsselt. Obwohl Ransomware-Angriffe viele Formen annehmen können, folgen sie im Allgemeinen dem gleichen Ablauf.

Ransomware-Angriffe erfolgen in der Regel in sechs Phasen:

- #1 Aufklärung:** Die Angreifer untersuchen das Netzwerk, identifizieren wertvolle Ressourcen und suchen nach Schwachstellen.
- #2 Infektion:** Sie verschaffen sich ersten Zugriff – häufig über Phishing-E-Mails, Exploit-Kits oder kompromittierte Anmeldedaten.
- #3 Eskalation:** Die Angreifer bewegen sich lateral durch das Netzwerk und erweitern ihre Berechtigungen, um an sensible Systeme zu gelangen.
- #4 Scannen:** Die Malware listet Dateien und Systeme auf, um Ziele für die Verschlüsselung zu identifizieren.
- #5 Verschlüsselung:** Nach der Identifizierung der Ziele setzen die Angreifer Ransomware ein, um Dateien oder Systeme zu verschlüsseln, oft begleitet von der Löschung von Backups oder Schattenkopien.
- #6 Lösegeld:** Die Angreifer verlangen eine Zahlung für die Herausgabe des Entschlüsselungscodes; oft werden diese Forderungen mit der Drohung verbunden, die Daten zu veröffentlichen.

Arten von Ransomware

Angrifer verwenden bei Ransomware-Angriffen verschiedene Techniken und Monetarisierungsstrategien, darunter:

- **Verschlüsselnde Ransomware:** Diese häufigste Kategorie von Ransomware verschlüsselt Dateien, sodass Angreifer Lösegeld für die Entschlüsselung verlangen können.
- **Scareware:** Durch die Anzeige gefälschter Warnmeldungen oder Popups täuscht Scareware den Benutzern vor, dass ihr System infiziert ist, um Geld zu erpressen.
- **Screen Lockers:** Diese Bildschirmsperren verhindern, dass Benutzer auf ihren Bildschirm zugreifen können, bis ein Lösegeld gezahlt wird.
- **DDoS-Erpressung:** Distributed-Denial-of-Service-Angriffe (DDoS) werden angedroht oder ausgeführt, sofern keine Zahlung erfolgt.
- **Ransomware-as-a-Service (RaaS):** Bei diesem immer beliebter werdenden Geschäftsmodell verkaufen oder vermieten Entwickler Ransomware-Kits an andere Kriminelle.

Wie sich Ransomware-Angriffe verhindern lassen

Ransomware-Angriffe sind raffiniert, komplex und gut koordiniert. Das bedeutet, dass Unternehmen einen starken Schutz gegen jede Form von Angriff einrichten und akzeptieren müssen, dass es zu Sicherheitsverletzungen kommen wird. Die besten Strategien zur Ransomware-Prävention behandeln Ransomware als unvermeidbar – und nehmen ihr dann ihre Fähigkeit zur Verbreitung. Eine umfassende Ransomware-Abwehr sollte proaktive Sicherheitskontrollen und Maßnahmen zur Optimierung der Wiederherstellung umfassen.



Proaktive Sicherheitskontrollen

Da Ransomware-Angriffe so oft unentdeckt bleiben, bieten präventive Kontrollen den besten Schutz:

- **Mikrosegmentierung:** Ransomware-Angriffe benötigen Netzwerkzugriff, um sich zu verbreiten. Dies gilt sowohl für die frühen Phasen eines Angriffs, in denen das interne Netzwerk gescannt wird, als auch für die späteren Phasen, in denen Schwachstellen in exponierten Diensten ausgenutzt oder kompromittierte Anmeldedaten verwendet werden, um sich zu verbreiten. Ein segmentiertes Netzwerk schneidet Angreifer ab, sodass sie fast nichts tun können, um sich zu verbreiten.
- **MFA:** Anmeldedaten gehören zu den am häufigsten verwendeten „Waffen“ von Angreifern, die sie oft nur allzu leicht stehlen oder knacken können. Durch den Schutz privilegierter Zugriffe mit MFA können Verteidiger das Risiko erheblich begrenzen.
- **Deaktivieren unnötiger Ports und Dienste:** Das Abschalten ungenutzter Fernzugriffsprotokolle (wie RDP und SMB) und die Durchsetzung strenger Zugriffskontrollen schränken die Angriffswege ein und reduzieren die Angriffsfläche für Ransomware.
- **Robuste Perimeter-Abwehr:** Lösungen wie Next-Generation-Firewalls (NGFW) und granulare Zugriffskontrollen minimieren Bedrohungen durch eine verstärkte Absicherung des Nord-Süd-Datenverkehrs.

Maßnahmen zur Optimierung der Wiederherstellung

Die vollständige Verhinderung von Ransomware ist zwar ideal, aber ebenso wichtig ist die Vorbereitung auf die Wiederherstellung. Bewährte Verfahren zur Optimierung der Wiederherstellung sind Backup-Systeme sowie kontinuierliche Überwachung und Reaktion. Das bedeutet: Regelmäßige, verschlüsselte Backups in einer vom Hauptnetzwerk getrennten Umgebung vereinfachen die Wiederherstellung für den Fall, dass Ransomware wichtige Daten verschlüsselt.

Unternehmen sollten zudem auf verdächtige Aktivitäten im Netzwerk achten und darauf reagieren, um aufkommende Bedrohungen frühzeitig zu erkennen. Zu beachten ist hierbei: Endpoint Detection and Response (EDR)-Systeme allein können laterale Bewegungen nicht blockieren und vor Ransomware schützen.

Sobald die Ransomware verbreitet ist, sind deren Entfernung und die Wiederherstellung verschlüsselter Daten von entscheidender Bedeutung. Schnelligkeit ist wichtig, aber Vorsicht auch. Zu schnelles Handeln ohne klare Strategie kann zu einer erneuten Infektion oder zu einer Beeinträchtigung der Wiederherstellungsmaßnahmen führen. Der erste Schritt zur Eindämmung von Ransomware besteht darin, die Reichweite der Infektion zu begrenzen. Betroffene Systeme gilt es vom Netzwerk zu trennen, um zu verhindern, dass die Malware andere Ressourcen scannt, verschlüsselt oder auf andere Ressourcen überspringt. Wenn bereits eine Netzwerksegmentierung vorhanden ist, lassen sich infizierte Bereiche gezielter isolieren und so die Auswirkungen auf das gesamte Unternehmen reduzieren.

Nach einem Ransomware-Angriff müssen nicht nur Daten „wiederhergestellt“ werden – auch alle Anmeldedaten, Geheimnisse, API-Schlüssel und privaten Schlüssel sind möglicherweise kompromittiert und müssen neu generiert werden, um einen erneuten Angriff zu verhindern.

Ransomware unmittelbar blockieren

Geschwindigkeit, Tarnung und Raffinesse sind die größten Waffen von Ransomware. Da sie sich innerhalb eines Netzwerks so schnell und oft unentdeckt verbreitet, können herkömmliche Sicherheitslösungen einfach nicht Schritt halten. Entscheidend ist eine Lösung, die laterale Bewegungen unmöglich macht.

Durch die Kombination von Mikrosegmentierung und granularen identitätsbasierten Zugriffskontrollen können Unternehmen Ransomware-Angriffe stoppen, bevor sie sich ausbreiten, und so sicherstellen, dass Angreifer niemals Berechtigungen eskalieren oder kritische Systeme erreichen können. Selbst wenn Anmeldedaten kompromittiert werden, sorgt eine Just-in-Time-MFA auf Netzwerkebene dafür, dass diese Anmeldedaten nicht verwendet werden können.

Mit anderen Worten: Wenn Ransomware die Perimeter-Sicherheit durchbricht, bleibt sie an Ort und Stelle und kann sich nicht über den ursprünglichen Eintrittspunkt hinausbewegen. Der beste Schutz vor Ransomware ist nicht reaktiv, sondern integriert.

Kay Ernst, Zero Networks
www.zeronetworks.com

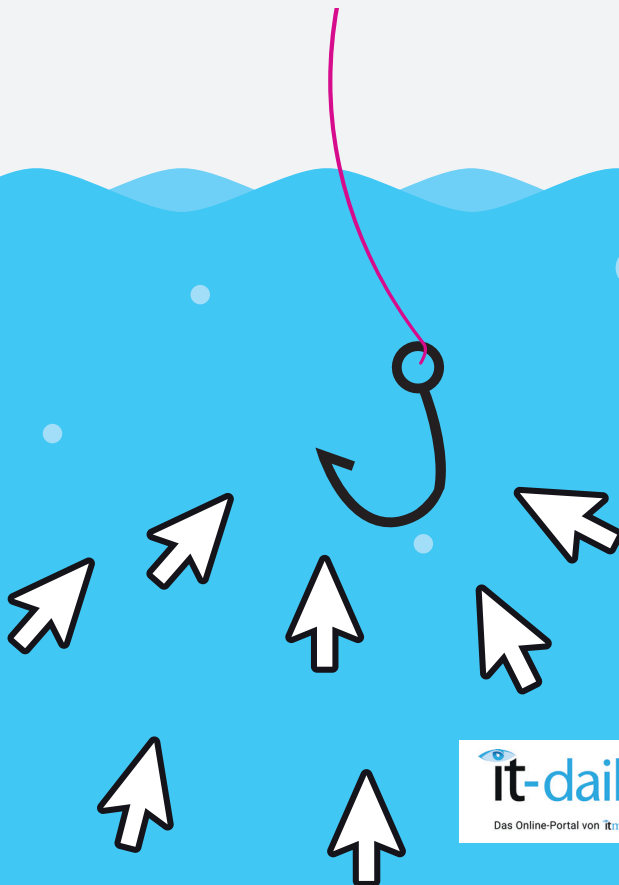
Phi·shing

/ˈfɪʃɪŋ/

Substantiv, Neutrum [das]

englisch phishing, zu: fishing = das Fischen;
die ph-Schreibung als häufig gebrauchte Verfremdung im Hackerjargon für f wohl nach
englisch-amerikanisch phreaking = das Hacken (zu: freak, Freak).

Beschaffung persönlicher Daten anderer Personen (Passwort, Kreditkartennummer o. Ä.)
mit gefälschten E-Mails oder Websites.





RANSOMWARE BLEIBT HOCHRISIKO

3 GRÜNDE FÜR DIE WACHSENDE GEFAHR

Ransomware ist ein einträgliches Geschäft. So wurden allein im Jahr 2023 weltweit 1 Milliarde Euro an Lösegeld bezahlt. Schlimmer als diese Zahlungen ist jedoch die Spur der Verwüstung, die Ransomware-Angriffe in der Unternehmenslandschaft nach sich ziehen. Nach Bitkom-Angaben beliefen sich allein in Deutschland alle Schäden durch Cyberangriffe im Jahr 2024 auf ~178,6 Mrd. Euro. Davon geht natürlich ein immenser Teil auf das Konto von Ransomware.

Und die Forderungen der Erpresser werden immer höher, wie auch die Zahl an Ransomware-Attacken weiter nach oben geht. Ransomware ist heute im Security-Bereich die größte Bedrohung für die Existenz eines Unternehmens. Und das hat gute Gründe.

#1 Industrialisierung der Ransomware:

Um profitabler zu werden, schreitet die Industrialisierung (auch Ransomware-as-a-Service (RaaS) genannt) stark voran und ist mittlerweile Realität. War Ransomware früher oft ein Einzelprogramm, ist es heute ein Geschäftsmodell. Anbieter entwickeln Verschlüsselungs-Malware und vermieten sie an Kriminelle, die dann als Affiliates die Angriffe ausführen. Dies hat Ransomware zu einem quasi Massenmarkt gemacht.

Ein Beispiel hierfür ist Gruppe ShadowSyndicate, die als Affiliate für verschiedene Ransomware-Familien agiert. Im Jahr 2024 begann ShadowSyndicate, die Ransomware von RansomHub zu nutzen, einer neuen RaaS-Plattform, die nach der Zerschlagung von ALPHV/BlackCat und LockBit entstanden ist. ShadowSyndicate führte Angriffe durch, bei denen sie RansomHub-Ransomware einsetzten, um Daten zu verschlüsseln und zu exfiltrieren.

#2 Doppelte Erpressung:

Die Erpresser erhöhen den Druck. Denn im Gegensatz zu früher sperren Angreifer nicht mehr nur das System, sondern sie exfiltrieren die Daten und drohen darüber hinaus jetzt auch, diese zu veröffentlichen, wenn kein Lösegeld gezahlt wird. Oft wird den Opfern mit Countdowns auf Seiten im Darkweb gedroht, wann ihr Daten freigegeben werden. Diese Double-Extortion kombiniert Verschlüsselung mit Datenleaks und bringt vielfach höhere Summen.

#3 Unknackbare Verschlüsselung:

Um den Druck auf ihre Opfer zu maximieren, verschlüsseln die Angreifer die Daten mit einem AES/RSA-Verschlüsselungsverfahren: Jede Datei wird zunächst mit einem symmetrischen AES-Schlüssel verschlüsselt, anschließend wird dieser AES-Schlüssel mit einem asymmetrischen RSA-Schlüssel geschützt und in der Datei abgelegt. Nur der Angreifer besitzt den für jedes Opfer individuellen RSA-Privatschlüssel, sodass nur er die Daten wieder freigeben kann.

Wie kommen die Angreifer rein?

Ransomware findet fast immer über eine erste Schwachstelle Zugang ins Netzwerk. Die häufigsten Einfallstore sind:

- **Phishing und Social Engineering:** Gefälschte E-Mails und manipulierte Webseiten sind der Hauptvektor. Mitarbeiter erhalten scheinbar seriöse Nachrichten mit versteckten Schad-Links oder -Anhängen. Bitkom fand, dass 26% aller Unternehmen von Phishing berichteten.
- **Fernzugriffe (RDP/VPN):** Offene oder schwach abgesicherte Remote-Desktop-Verbindungen sind ein beliebter Einstieg. Ohne VPN und Zwei-Faktor-Ab-sicherung kann RDP leicht geknackt oder mit Brute-Force überwältigt werden.
- **Software-Schwachstellen und Zero-Day-Exploits:** Ungepatchte Programme (Betriebssysteme, Server-Software, SMB, Exchange, Browser usw.) bieten Attacken Tore. Besonders gefährlich sind Zero-Day-Lücken, für die es noch keinen Patch gibt. Kriminelle nutzen solche Lücken aus, um sich unbemerkt im Netzwerk umzuschauen und Ransomware auszulösen.
- **Lieferketten-Angriffe:** Über Partner und Dienstleister können Täter indirekt ins Ziel-Netzwerk gelangen. Bei sogenannten Supply-Chain-Angriffen knacken die Täter zunächst Zulieferer oder IT-Dienstleister und nutzen deren Vertrauens-stellungen (VPN-Zugänge, Wartungs-Accounts etc.), um ins eigentliche Ziel einzudringen.
- **Kompromittierte Zugangsdaten:** Zugangsdaten (Passwörter, SSH-Keys) werden auf Darknet-Marktplätzen gehandelt. Das Eindringen mit gekauften Credentials eröffnet Angreifern direkt Administratorrechte. In vielen Fällen gehen RDP- oder Admin-Logins über genau solche gehackten Konten.

Abwehrstrategien für Ransomware

Die Strategie, um Ransomware-Angriffe abzuwehren, beginnt mit Sicherheitsstandards und Frameworks (z. B. NIST Cybersecurity Framework, ISO27001/IT-Grundschutz).

Wenn diese Rahmen gesetzt sind, empfiehlt sich die weitere Abwehrstrategie auf zwei Säulen zu stellen.

#1 Technische Schutzmaßnahmen

Technische Schutzmaßnahmen zielen darauf ab, Angriffe frühzeitig zu erkennen oder ihre Ausbreitung zu verhindern:

- **Endpoint Security (AV/EDR/XDR):** Auf Endgeräten sollte moderne Sicherheitssoftware mit Verhaltensanalyse laufen. Cloud-basierte Lösungen und Intrusion-Prevention-Module erhöhen den Schutz.
- **NextGen-Firewalls (NGFW):** Moderne Firewalls, die neben klassischer Paketfilterung auch Funktionen wie Deep Packet Inspection, Intrusion Prevention und Applikationskontrolle bieten, um Netzwerke effektiv vor komplexen Bedrohungen zu schützen.
- **Netzwerksegmentierung:** Trennung von Netzbereichen (z.B. Büro, Produktion, Server) verhindert Schadcode-Ausbreitung. Laut BSI lässt sich damit in 80–90% der Fälle größere Ausbreitung verhindern.
- **Multi-Faktor-Authentifizierung (MFA):** Absicherung von Admin- und Fernzugängen durch MFA schützt vor Missbrauch kompromittierter Passwörter.
- **Monitoring & Logging:** Zentralisiertes Monitoring (SIEM/NDR) erkennt auffälliges Verhalten (z.B. Massenzugriffe, Datenabflüsse). Tools wie IDS/IPS, Firewalls und Log-Auswertung (z.B. mit Splunk) alarmieren bei Vorfällen.
- **Sicherheitsstandards:** Umsetzung nach Frameworks wie NIST, ISO 27001 oder IT-Grundschutz stärkt die Resilienz. Das BSI bietet praxisnahe Leitfäden für IT-Härtung und Überwachung.

#2 Organisatorische Schutzmaßnahmen

Neben Technik hilft vor allem Vorbereitung auf den Ernstfall:

- **Awareness-Trainings:** Regelmäßige Schulungen sensibilisieren Mitarbeiter für Phishing, Social Engineering und sicheres Verhalten. Simulationen („Phishing-Tests“) schärfen das Bewusstsein. Ein engagiertes Sicherheitsbewusstsein auf allen Ebenen verringert Infektionsrisiken erheblich.
- **Notfall- und Incident-Response-Plan:** Ein strukturierter IT-Notfallplan ist essentiell. Darin muss beschrieben sein, welche kritischen Systeme im Ernstfall priorisiert wiederhergestellt werden und wer welche Rolle hat. Hier ist es wichtig, dass alle beteiligten Personen wissen, was zu tun ist und dass dieser Plan immer erreichbar abgelegt ist, also nicht (nur) auf dem Server. In Deutschland verfügen erstaunlicherweise nur etwa 40% der Unternehmen über einen solchen Plan – 60% wären im Cyber-Notfall unvorbereitet.
- **Backup- und Wiederanlaufkonzept:** Backups sind die wichtigste Vorsorge: Sie ermöglichen Wiederherstellung ohne Lösegeldzahlung. Wichtig sind auch regelmäßige Tests der Wiederherstellung. Eine zentrale Datenspeicherung (z.B. Netzlaufwerke mit restriktiven Zugriffsrechten) kann verhindern, dass Benutzerdateien verschlüsselt werden können.
- **Incident-Response-Prozesse:** Jenseits des Plans benötigt es klare Abläufe zur Entdeckung und Meldung. Die Meldekette wie auch Kommunikationswege müssen feststehen (z.B. auch externe Experten und Behörden wie CERT-Bund informieren). Bei jedem Vorfall sollte ein IT-Sicherheitsbeauftragter und ein Krisenteam sofort aktiviert werden. Regelmäßige Übungen und Nachbesprechungen verbessern die Reaktion kontinuierlich.

Praxisbewährte Maßnahmen zur Risikominimierung

In großen Umgebungen kommen umfassende Security-Suites zum Einsatz. Moderne EDR/XDR-Systeme wie CrowdStrike Falcon, SentinelOne oder Microsoft Defender for Endpoint bieten automatisierte Bedrohungserkennung. Advanced Firewalls und Sandboxing (z.B. von Palo Alto, Check Point, Fortinet) blockieren Ransom-

ware-Angriffe. SIEM-Plattformen (Splunk, QRadar, Elastic) sowie Managed Detection & Response (MDR) ergänzen die Abwehr. Für Backups und Recovery sind spezialisierte Lösungen empfehlenswert (z.B. Veeam, Acronis, Rubrik), die Schutz gegen Manipulation und Backdoor-Verschlüsselung bieten. Auch dedizierte Phishing-Simulationen oder Awareness-Trainings großer Anbieter (z.B. KnowBe4, Proofpoint) können die Mitarbeitersicherheit professionalisieren.

Fazit

Ransomware-Angriffe sind die größte Gefahr für Unternehmen. Die Lösegeld-Forderungen steigen und das Vorgehen der Erpresser wird immer rabiater.

Hierzu haben sich die Angreifer auf neue Wege spezialisiert, indem sie

- Ransomware industrialisieren und als Service anbieten,
- durch Datenklau und Veröffentlichungs-Drohung den Druck auf die Opfer erhöhen,
- die Verschlüsselung unknackbar machen.

All dies macht Ransomware zu so einer großen Bedrohung. Sind die Täter einmal im System, gibt es kaum mehr Möglichkeiten und der Reparaturschaden ist existenzgefährdend.

Das Einzige, was Unternehmen machen können, ist mit Regeln, Frameworks sowie mit technischen und organisatorischen Schutzmaßnahmen dafür sorgen, dass niemand in das eigene System kommt. Und das so schnell wie möglich, denn je länger mit Schutzmaßnahmen gewartet wird, desto schwieriger ist es diese überhaupt wieder aufzuholen. Dabei können Beratungs- und Integrationshäuser helfen.



Philip Huisgen
Managing Director
DATAKOM GmbH
www.datakom.de

INSIDER- BEDROHUNGEN

TECHNISCHE SCHUTZARCHITEKTUREN GEGEN INSIDER-BEDROHUNGEN

Während die Bedrohungslandschaft durch Insider-Angriffe dramatisch zunimmt und die Gefahren durch externe Angriffe (Ransomware-Attacken) parallel bestehen bleiben, stehen IT-Verantwortliche vor der Herausforderung, konkrete technische Lösungen zu implementieren. Dieser Leitfaden konzentriert sich auf die praktische Umsetzung bewährter Sicherheitstechnologien und deren Integration in bestehende IT-Infrastrukturen.

Denn: Insider-Bedrohungen sind die unterschätzte Gefahr für Unternehmen. Während die meisten Diskussionen über IT-Sicherheit sich auf externe Cyberangriffe konzentrieren, zeigen aktuelle Studien ein alarmierendes Bild: 83% der Organisationen berichteten 2024 über mindestens einen Insider-Angriff und zwischen 2023 und 2024 gab es einen 28%igen Anstieg bei datenbasierten Sicherheitsvorfällen durch Insider. Diese Zahlen verdeutlichen, dass die Bedrohung von innen nicht nur real, sondern auch zunehmend ist.

Böswillig oder nicht – der Schaden zählt

Insider-Bedrohungen umfassen sowohl böswillige Handlungen als auch unbeabsichtigte Sicherheitsverletzungen durch Mitarbeiter, Auftragnehmer oder Geschäftspartner mit legitimen Zugriffsrechten. Diese Akteure haben bereits Vertrauen und Zugang zu kritischen Systemen, was sie besonders gefährlich macht. Die Angriffsvektoren von innen sind vielfältig: Datendiebstahl durch unzufriedene Mitarbeiter, Sabotage von Systemen bei Kündigung, unbeabsichtigte Datenlecks durch Fahrlässigkeit, Missbrauch von Privilegien für persönliche Vorteile, oder die Kompromittierung von Mitarbeiterkonten durch Social Engineering.

Externe Cyberangriffe nutzen hingegen andere Vektoren: Phishing-Kampagnen zur Credential-Beschaffung, Malware-Infektionen über E-Mail-Anhänge oder Downloads, Ransomware-Angriffe auf ungeschützte Systeme, DDoS-Attacken zur Systemüberlastung, SQL-Injection und andere Web-Anwendungsangriffe, Zero-Day-Exploits in Software-Schwachstellen, oder Advanced Persistent Threats (APTs) für langfristige Infiltration. Egal, ob intern oder extern. Die Gefahr der Verschlüsselung besteht durch beide Varianten.

ANGRIFFSVEKTOREN AUF UNTERNEHMEN

EXTERNE ANGRIFFE

- Phishing & Social Engineering
- Malware & Ransomware
- DDoS-Attacken
- Web-Anwendungsangriffe (SQL Injection, XSS)
- Zero-Day-Exploits
- Advanced Persistent Threats
- Netzwerk-Infiltration
- Supply Chain Attacks
- Man-in-the-Middle
- Brute-Force-Angriffe
- IoT-Gerätekompromittierung

UNTERNEHMEN
IT-Systeme
Daten & Assets

INSIDER-BEDROHUNGEN

- Böswilliger Datendiebstahl
- System-Sabotage
- Unbeabsichtigte Datenlecks
- Missbrauch von Privilegien
- Credential-Weitergabe
- Kompromittierte Accounts
- Unsichere Datenträger
- Shadow IT & Cloud Services
- Verletzung von Richtlinien
- Auftragnehmer-Risiken
- Post-Employment-Zugriff

Die Grafik veranschaulicht die duale Bedrohungslandschaft moderner Unternehmen. Während externe Angriffe oft spektakulärer und medienwirksamer sind, zeigen die aktuellen Statistiken, dass Insider-Bedrohungen ein ebenso kritisches, wenn nicht sogar größeres Risiko darstellen. Eine effektive IT-Sicherheitsstrategie muss beide Dimensionen gleichwertig berücksichtigen und entsprechende Schutzmaßnahmen implementieren. Der Schlüssel liegt in der Erkenntnis, dass Sicherheit nicht nur eine technische, sondern auch eine organisatorische und kulturelle Herausforderung ist. Während Firewalls und Antivirensoftware externe Bedrohungen abwehren können, erfordern Insider-Bedrohungen ein tieferes Verständnis menschlicher Motivationen und Verhaltensweisen sowie entsprechende präventive Maßnahmen.

Ganzheitlicher Ansatz gefragt

Daher müssen IT-Sicherheitsverantwortliche das Thema neu denken. Zu den zu berücksichtigenden Aspekten gehören:

#1 Network Access Control: Intelligente Zugangssteuerung implementieren

Network Access Control-Systeme bilden das technische Fundament für die Kontrolle interner Bedrohungen. Die moderne NAC-Implementierung geht weit über einfache MAC-Adress-Filterung hinaus und nutzt dynamische Profiling-Mechanismen zur Geräteerkennung. Diese Systeme analysieren kontinuierlich Netzwerktraffic-Muster, DHCP-Fingerprinting und Protokoll-Anomalien, um unbekannte oder kompromittierte Geräte zu identifizieren.

Die Implementierung erfolgt typischerweise in drei Phasen: Zunächst wird ein umfassendes Asset-Discovery durchgeführt, das alle Netzwerkgeräte erfasst und kategorisiert. In der zweiten Phase werden Policy-Engines konfiguriert, die Zugriffsregeln basierend auf Gerätetyp, Benutzeridentität und Compliance-Status definieren. Die finale Phase umfasst die Einrichtung automatisierter Remediation-Workflows, die nicht-konforme Geräte automatisch isolieren oder in spezialisierte Quarantäne-VLANs verschieben.

Moderne NAC-Lösungen integrieren Machine Learning-Algorithmen zur Verhaltensanalyse auf Netzwerkebene. Diese können ungewöhnliche Kommunikationsmuster zwischen internen Systemen erkennen, die auf laterale Bewegungen oder Datenexfiltration hindeuten. Die Integration mit SIEM-Systemen ermöglicht korrelierte Threat Intelligence, die sowohl Netzwerk- als auch Anwendungsebene umfasst.

#2 Zero Trust Network Access: Granulare Anwendungssicherheit

ZTNA-Architekturen revolutionieren den traditionellen VPN-Ansatz durch applikations-spezifische Zugriffskontrollen. Im Gegensatz zu herkömmlichen Netzwerk-VPNs, die breiten Zugang zu Netzwerksegmenten gewähren, erstellen ZTNA-Lösungen verschlüsselte Mikro-Tunnel direkt zu einzelnen Anwendungen oder Services. Die technische Implementierung basiert auf Software-Defined Perimetern, die dynamische Verschlüsselungs-Gateways vor kritischen Anwendungen positionieren. Diese Gate-

ways führen kontinuierliche Risikobewertungen durch, die Faktoren wie Geräte-Posture, Benutzerverhalten, geografische Anomalien und zeitbasierte Zugriffsmuster berücksichtigen. Adaptive Authentifizierungsmechanismen können zusätzliche Verifikationsschritte auslösen, wenn Risikoschwellenwerte überschritten werden.

Ein wesentlicher Vorteil von ZTNA liegt in der Implementierung von Just-in-Time-Zugriff für privilegierte Operationen. Anstatt permanente administrative Rechte zu gewähren, werden diese temporär und aufgabenspezifisch zugewiesen. Automatische Session-Recordings und Keystroke-Logging für privilegierte Sitzungen ermöglichen umfassende forensische Analysen bei verdächtigen Aktivitäten.

#3 Mikrosegmentierung: Isolation auf Workload-Ebene

Moderne Netzwerksegmentierung geht über traditionelle VLAN-Strukturen hinaus und implementiert Mikrosegmentierung bis auf die Workload-Ebene. Diese Technologie nutzt Software-Defined Networking-Prinzipien, um granulare Sicherheitsrichtlinien zwischen einzelnen Anwendungskomponenten durchzusetzen. Die Implementierung erfolgt durch Host-basierte Firewall-Agents oder Hypervisor-integrierte Filtering-Mechanismen, die East-West-Traffic innerhalb des Datenzentrums kontrollieren. Application Dependency Mapping-Tools analysieren zunächst normale Kommunikationsflüsse zwischen Systemen, um Baseline-Policies zu definieren. Machine Learning-Algorithmen optimieren diese Policies kontinuierlich und identifizieren Anomalien in der Inter-System-Kommunikation.

Container-Umgebungen erfordern spezialisierte Mikrosegmentierung durch Service Mesh-Architekturen. Diese implementieren mTLS-Verschlüsselung für alle Service-zu-Service-Kommunikation und nutzen Certificate-basierte Identitäten für granulare Zugriffskontrolle. Istio oder Linkerd als Service Mesh-Plattformen ermöglichen Policy-Enforcement auf Layer 7, wodurch HTTP-Header, URL-Pfade und API-Endpunkte in Sicherheitsentscheidungen einbezogen werden können.

#4 Data Loss Prevention: Intelligente Content-Analyse

Moderne DLP-Systeme nutzen fortschrittliche Content Analysis-Engines, die weit über einfache Keyword-Matching hinausgehen. Natural Language Processing und

Machine Learning-Modelle analysieren Dokumentkontext, semantische Beziehungen und Datenklassifizierungen, um sensible Informationen auch in verschleierte oder transformierten Formaten zu erkennen.

Die technische Implementierung umfasst mehrere Analyse-Schichten: Structured Data Matching für Datenbank-ähnliche Inhalte, Statistical Analysis für die Erkennung von Kreditkartennummern oder Sozialversicherungsnummern, und Conceptual Analysis für die Identifikation geschäftskritischer Informationen basierend auf Kontext und Semantik. Network-basierte DLP-Agents analysieren Datenströme in Echtzeit und können verdächtige Übertragungen blockieren oder in Quarantäne versetzen. Endpoint-DLP-Lösungen integrieren sich tief in Betriebssysteme, um Datenzugriffe auf Prozessebene zu überwachen. Cloud Access Security Broker integrieren DLP-Funktionalitäten für SaaS-Anwendungen und überwachen Daten-Uploads in Cloud-Services.

#5 Endpoint Detection and Response: Verhaltensbasierte Anomalieerkennung

EDR-Lösungen implementieren fortschrittliche Telemetrie-Sammlung auf Endpoint-Ebene, die Prozess-Ausführung, Dateisystem-Änderungen, Registry-Modifikationen und Netzwerk-Verbindungen kontinuierlich überwacht. Diese granularen Daten werden durch maschinelle Lernmodelle analysiert, um verdächtige Aktivitätsmuster zu identifizieren. Die technische Architektur basiert auf Lightweight-Sensoren, die minimale Systemressourcen verbrauchen, aber umfassende Visibility bieten. Kernel-Level-Hooking ermöglicht die Überwachung von System Calls und API-Aufrufen, während User-Mode-Komponenten Anwendungsverhalten analysieren.

Cloud-basierte Analytics-Engines korrelieren Endpoint-Telemetrie mit Threat Intelligence-Feeds und identifizieren Advanced Persistent Threats.

Behavioral Analytics-Engines erstellen Baseline-Profil für normale Benutzeraktivitäten und erkennen Abweichungen, die auf Account-Kompromittierung oder böswillige Insider hindeuten könnten. File Integrity Monitoring überwacht kritische Systemdateien und Konfigurationen auf unbefugte Änderungen, während Process Hollowing Detection und Memory Forensics-Techniken Advanced Malware identifizieren.

#6 User and Entity Behavior Analytics: KI-gestützte Anomalieerkennung

UEBA-Plattformen implementieren unüberwachte Machine Learning-Algorithmen, die normale Verhaltensmuster für Benutzer und Entitäten etablieren. Diese Systeme analysieren diverse Datenquellen: Active Directory-Logs, VPN-Verbindungen, E-Mail-Metadaten, Anwendungszugriffe und Dateisystem-Aktivitäten.

Die technische Implementierung nutzt statistisches Clustering und Anomalie-Detection-Algorithmen wie Isolation Forests oder One-Class SVMs. Diese identifizieren Ausreißer in multidimensionalen Verhaltensräumen und können subtile Veränderungen in Benutzermustern erkennen, die manuellen Analysen entgehen würden.

Risk Scoring-Engines gewichten verschiedene Anomalien und erstellen zusammengesetzte Risiko-Scores für Benutzer und Entitäten. Peer Group Analysis vergleicht Benutzerverhalten mit ähnlichen Rollen oder Abteilungen, um kontextuelle Anomalien zu identifizieren. Temporal Analysis erkennt ungewöhnliche Zugriffsmuster außerhalb normaler Arbeitszeiten oder in untypischen Sequenzen.

#7 Privileged Access Management: Technische Implementierungsstrategien

Moderne PAM-Architekturen implementieren Vault-basierte Credential-Verwaltung mit automatischer Passwort-Rotation und Session-Isolation. Diese Systeme nutzen HSM-Integration für kryptographische Schlüsselverwaltung und bieten API-basierte Integration für DevOps-Workflows.

Just-in-Time Access-Implementierungen nutzen Workflow-Engines für automatisierte Genehmigungsprozesse und temporäre Rechtezuweisung. Session-Proxy-Technologien ermöglichen privilegierte Zugriffe ohne Credential-Weitergabe und implementieren granulare Kommando-Filterung basierend auf Risikobewertungen.

Für Cloud-Umgebungen integrieren PAM-Lösungen mit nativen IAM-Services und implementieren Cloud Service Provider-spezifische Assume Role-Mechanismen. Container-Orchestrierungs-Plattformen erfordern spezialisierte Secret Management-Integration mit Kubernetes Secrets oder HashiCorp Vault.

#8 Security Information and Event Management: Korrelations-Engines

Moderne SIEM-Architekturen implementieren Stream Processing-Engines, die Millionen von Events pro Sekunde in Echtzeit verarbeiten können. Apache Kafka oder ähnliche Messaging-Plattformen puffern Event-Streams, während Complex Event Processing-Engines Korrelationsregeln in Echtzeit ausführen.

Machine Learning-basierte Anomalie-Detection ergänzt regelbasierte Korrelation durch unüberwachtes Lernen von Event-Mustern. Time Series Analysis identifiziert zeitbasierte Anomalien in Event-Volumina oder -Mustern, während Graph Analytics verdächtige Beziehungsmuster zwischen Entitäten aufdecken.

Threat Hunting-Plattformen integrieren sich mit SIEM-Daten und ermöglichen proaktive Suche nach Indicators of Compromise. Integration mit Threat Intelligence-Feeds ermöglicht automatische IOC-Matching und Context-Enrichment für Security Events.

#9 Integration und Orchestrierung: SOAR-Implementierung

Security Orchestration, Automation and Response-Plattformen automatisieren wiederkehrende Sicherheitsaufgaben und orchestrieren komplexe Incident Response-Workflows. Diese Systeme integrieren diverse Sicherheitstools über standardisierte APIs und implementieren Playbooks für häufige Sicherheitsszenarien.

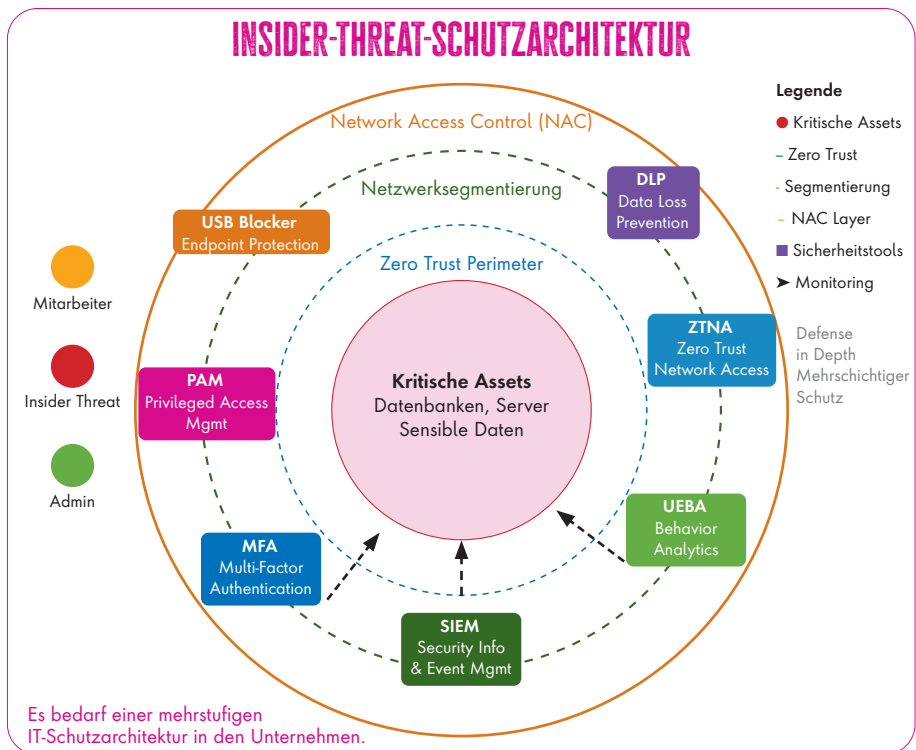
Automated Threat Response nutzt vordefinierte Workflows zur sofortigen Eindämmung identifizierter Bedrohungen. Account-Isolation, Netzwerk-Quarantäne und Forensic Data Collection können automatisch ausgelöst werden, um Schadensbegrenzung zu gewährleisten.

Case Management-Systeme integrieren mit ITSM-Plattformen und ermöglichen strukturierte Incident-Bearbeitung mit Audit-Trails und Eskalations-Mechanismen. Threat Intelligence-Integration ermöglicht automatische IOC-Extraktion und Sharing mit externen Partnern oder Threat Intelligence-Plattformen.

#10 Implementierungsstrategie: Phasen-basierter Rollout

Die erfolgreiche Implementierung technischer Insider-Threat-Schutzmaßnahmen erfordert einen strukturierten, phasierten Ansatz. Die initiale Bewertungsphase umfasst Asset Discovery, Risikobewertung und Baseline-Etablierung für normale Systemaktivitäten.

Phase 1 konzentriert sich auf grundlegende Kontrollen: NAC-Implementierung, grundlegende SIEM-Integration und Endpoint-Monitoring. Phase 2 erweitert um UEBA-Deployment, DLP-Rollout und erweiterte SOAR-Integration. Die finale Phase implementiert fortgeschrittene Technologien wie Mikrosegmentierung und KI-basierte Threat Detection. Erfolgsmessung erfolgt durch KPIs wie Mean Time to Detection, False Positive Rates und automatisierte Response-Zeiten. Kontinuierliche Optimierung nutzt Feedback-Loops zur Verbesserung von Detection-Accuracy und Operational Efficiency.



Fazit: Technische Exzellenz als Grundlage

Die technische Implementierung effektiver Insider-Threat-Schutzmaßnahmen erfordert durchdachte Architekturentscheidungen und sorgfältige Integration verschiedener Sicherheitstechnologien. Erfolgreiche Deployments zeichnen sich durch granulare Kontrollmechanismen, intelligente Automatisierung und umfassende Monitoring-Capabilities aus.

Die kontinuierliche Evolution der Bedrohungslandschaft macht adaptive Sicherheitsarchitekturen erforderlich, die maschinelles Lernen und künstliche Intelligenz nutzen, um sich entwickelnden Angriffstechniken einen Schritt voraus zu bleiben. Nur durch die konsequente Implementierung dieser technischen Fundamente können Organisationen effektiven Schutz vor den komplexen Herausforderungen interner Bedrohungen gewährleisten.

Ulrich Parthier



RANSOMWARE VERSTEHEN UND BEKÄMPFEN

Jetzt herunterladen!

itsecurity eBook



SCAN ME

BYE, BYE,
RANSOMWARE!

CYBERSTORAGE

Schutz dank fragmentierter Daten.
Colomo ist ein Beispiel für solche eine Lösung
der neuen Generation, die Daten unhackbar
machen soll, um Datendiebstahl und
exfiltration zu verhindern.

MODERNES BACKUP

Erkennen, schützen, wiederherstellen,
so lautet hier die heilige Dreifaltigkeit.
Dortüberhinaus gibt es neue Produkte für
Block Storage und eine Garantie, die
Unternehmensdaten nach einem Ransomware-
Angriff wiederherzustellen.

EDR-LÖSUNGEN

Ransomware-Bereinigungsfunktionen sichern Dateien,
um sicherzustellen, dass sie im Falle einer Ransomware-
Verschlüsselung nicht beschädigt werden oder verloren
gehen. Jedes Mal, wenn ein Ransomware-Angriff erkannt
wird, blockieren sie alle Prozesse, die an dem Angriff
beteiligt sind, und starten den Sanierungsprozess.

WWW.IT-DAILY.NET

it-daily.net

Das Online-Portal von ITmanagement & ITsecurity

RANSOMWARE: WER STILLSTEHT, VERLIERT

KEIN PARDON

Die Anzahl erfolgreicher Cyberangriffe geht erneut durch die Decke, so Bitkom. Demnach ist der Anteil der betroffenen Unternehmen im Jahr 2024 von 72 auf 81% gestiegen. Bei etwa einem Drittel (31%) davon richtete Ransomware den größten Schaden an (2023: 23%).

Was begünstigt den Erfolg von Ransomware-Angriffen?

Wer über die Anmeldedaten von Personen aus einem Unternehmen verfügt, kann sich in der Regel ganz einfach im System anmelden und sich frei bewegen – sofern keine zusätzlichen Sicherheitsmechanismen wie Multifaktor-Authentifizierung oder eingeschränkte Zugriffsprivilegien aktiv sind. Für ein zusätzliches „Taschengeld“ verkaufen viele Betrüger die Anmeldedaten im Dark Web, was zum Wachstum des Ransomware-Marktes beiträgt (Initial Access Broker).

Bekannt als Ransomware-as-a-Service-Modell bieten kriminelle Gruppen und Einzelgänger darüber hinaus sowohl ihre Dienste als auch ihre Tools gegen Zahlung im Dark Web an. Damit können sogar Cyber-Crime-Laien ohne nennenswerte Hacking Skills Unternehmen erpressen. Ein weiteres rentables Geschäftsmodell bildet Double Extortion – also die doppelte Erpressung: zunächst durch Datenverschlüsselung und anschließend durch Veröffentlichung oder Verkauf der Daten an Höchstbietende.

And last, but not least: Cyberkriminellen steht – wie allen anderen auch – die Welt zu neuen Technologien offen. Mithilfe von KI steigern sie zum Beispiel die Erfolgsrate ihrer Phishing-Kampagnen, indem sie damit unter anderem die Inhalte glaubwürdiger gestalten.

Wo hakt es in IT-Abteilungen?

Es gibt verschiedene Faktoren, die es Cyberkriminellen unter günstigen Umständen besonders leicht machen, Unternehmen Ransomware unterzujubeln und sich dadurch sensible Daten unter den Nagel zu reißen. Diese Schwachstellen erklären, wieso Angriffe so häufig und erfolgreich sind und warum Unternehmen lange unter den Folgen von Ransomware-Attacken leiden müssen.

#1 Die Bereitschaft, nachzugeben

Über die Hälfte der Unternehmen haben sich laut einer aktuellen Studie gegen die allgemein bekannten Handlungsempfehlungen entschieden und das verlangte Lösegeld mit der Aussicht gezahlt, den Wiederherstellungsprozess zu beschleunigen. Allerdings haben sie es mit Kriminellen zu tun, die nicht immer ihr Wort halten. 26%, die sich auf die Forderungen eingelassen haben, erhielten ihre Daten nicht zurück. Somit gibt es keine Garantie, dass Angreifer die verschlüsselten Systeme und Daten wieder freigeben, geschweige denn darauf verzichten, ihre Ausbeute im Dark Web zu Geld zu machen.

#2 Alleiniges Vertrauen in die Basics

Wenn es um Cybersicherheit geht, setzen sehr viele Unternehmen auf diese vier Top-Maßnahmen: regelmäßige Updates, Backups sensibler Daten, vorgeschriebene Passworthygiene sowie Anwendungskontrollen. Robustere Mechanismen wie Identity- und Access-Management sucht man hier vergeblich. So hilfreich die aufgezählten Maßnahmen auch sind – die steigende Anzahl von Ransomware-Opfern beweist, dass sie allein nicht ausreichen, um sich wirksam gegen Phishing-Angriffe und Datendiebstahl zu schützen.

#3 Ein verschobener Fokus

Auch wenn es in vielen Unternehmen an fortschrittlicheren Sicherheitsmaßnahmen fehlt, sind die meisten von ihnen (90%) zumindest teilweise auf den Ernstfall vorbereitet. Dieser Anteil verfügt nach eigenen Aussagen nämlich über Incident-Response- und Backup-Pläne. Allerdings zeigen die Umfrageergebnisse auch hier, dass die Konzepte mit hoher Wahrscheinlichkeit ihre Lücken haben. Denn 75% der Unternehmen benötigten im Schnitt zwei Wochen, um sich von einem Ransomware-Angriff zu erholen und ihre Ressourcen wiederherzustellen. Lediglich 18% schafften das innerhalb von 24 Stunden.

Prävention statt Reaktion

So lange es Sicherheitslücken gibt und Opfer bereitwillig das Lösegeld zahlen bleibt die Bedrohung bestehen. Gleichzeitig vergrößert sich aufgrund technologischer Innovationen die Angriffsfläche in Unternehmen, was Cyberkriminellen in die Karten spielt und den Schutz vor Datendiebstahl verkompliziert. Das macht eine präventive, proaktive und mehrschichtige Abwehrstrategie unerlässlich, die grundlegende und fortschrittliche Sicherheitsmaßnahmen sowie Incident-Response- und Recovery-Pläne miteinander verbindet.

Dazu gehören zum einen die wichtigen Basics wie risikobasiertes Patching, regelmäßige Backups, Anwendungskontrollen, aber auch Security-Awareness-Schulungen für alle Mitarbeitenden. Zum anderen spielt das Thema Access- und Identity-Management eine essenzielle Rolle. In diesem Kontext bilden Privileged Access Management, Least Privilege, Governance und Zero Trust den Hauptbestandteil einer robusten Sicherheitsstrategie. Denn nur wer ganz genau weiß, welche Mitarbeitenden und Geräte sich im Netzwerk befinden und ihnen nur ein Mindestmaß an Privilegien zuschreibt, kann das Risiko durch ungewollte Dritte minimieren.

Der Einsatz von KI-Technologien kann die Ransomware-Abwehr zusätzlich stärken. Dabei geht es vor allem darum, potenzielle Bedrohungen und aktive Angriffe so schnell wie möglich aufzudecken. Dafür eignet sich ein KI-gestütztes Sicherheitssystem besonders gut, da es Unmengen an Daten durchgehend analysieren und Ausschau nach verdächtigen Mustern und Abweichungen halten kann (Indicators of Compromise). Neben Bedrohungsdaten kann es auch nach Verhaltensauffälligkeiten, unerwartet überprivilegierten Identitäten und nach verdächtigen Inhalten in E-Mail – sowohl im Text als auch im Anhang – suchen. Künftig wird zudem das Thema Agentic AI im Security-Bereich zunehmend an Bedeutung gewinnen, da ein solches System autonom Aufgaben wie Threat Hunting und Intelligent Policy Authorization übernehmen kann und somit bereits stark unterbesetzte und unterbudgetierte IT-Teams noch mehr entlastet.



Andreas Müller
Vice President Enterprise Sales
Central and Eastern Europe
Delinea
www.delinea.com/de

Cyberkriminelle überall da tut Hilfe not

Who're you
gonna call?

Securitybusters!

Mehr Infos dazu im Printmagazin

The logo for 'itsecurity' features a stylized eye icon to the left of the word 'itsecurity' in a lowercase, sans-serif font.

und online auf www.it-daily.net

RANSOMWARE-SCHUTZ

GANZHEITLICHE ABWEHR, SCHNELLE REAKTION, SICHERE WIEDERHERSTELLUNG

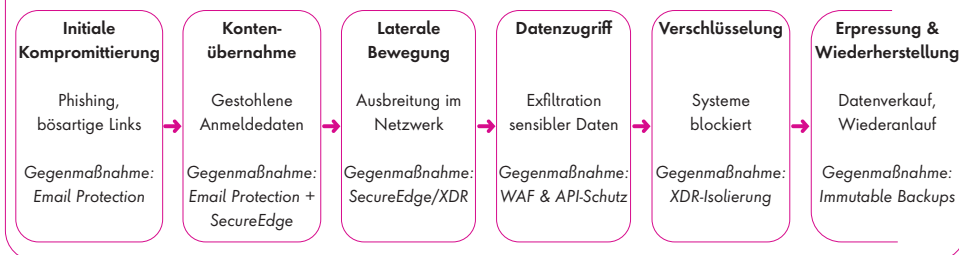
Ransomware trifft Unternehmen aller Größen – oft mehrfach. Barracuda kombiniert AI-gestützten E-Mail-Schutz, Web- und API-Absicherung, Zero-Trust-Zugriff, unveränderliche Backups und 24/7 Managed XDR zu einer integrierten Plattform, die Angriffe früh stoppt, Vorfälle schneller beendet und Daten zuverlässig wiederherstellt.

Warum Ransomware-Resilienz heute mehr ist als nur Prävention

Ransomware-Gruppen setzen längst nicht mehr nur auf Verschlüsselung. Vor der Erpressung erfolgen häufig Datendiebstahl, das Einschleusen zusätzlicher Schadsoftware, laterale Bewegungen im Netzwerk und das Löschen von Schattenkopien und Backups – oft verbunden mit zusätzlichem Druck, etwa durch Drohungen, gestohlene Daten zu veröffentlichen.

Aktuelle Barracuda-Erkenntnisse zeigen: 57% der Unternehmen erlebten in den vergangenen 12 Monaten einen erfolgreichen Ransomware-Angriff; knapp ein Drittel der Betroffenen wurde sogar mehrfach attackiert. 32% zahlten ein Lösegeld, doch 41% erhielten nicht alle Daten zurück. Das unterstreicht, wie wichtig integriertes Erkennen, Reagieren und Wiederherstellen ist – also echte Resilienz statt reiner Abwehr.

ANATOMIE EINES RANSOMWARE-ANGRIFFS & BARRACUDA-GEGENMASSNAHMEN



Der erste Schutzwall: AI-gestützter E-Mail-Schutz und schnelle Post-Delivery-Response

E-Mail bleibt das Einfallstor Nummer eins für Phishing, Malware und Kontenübernahmen. Barracuda Email Protection nutzt KI, URL- und Anhangsanalyse, Reputations-Checks und Schutz vor Impersonation, um Ransomware-Kampagnen zu blockieren, bevor sie Benutzer erreichen. Gelangt eine schädliche Nachricht dennoch durch, automatisiert Incident Response die Nachbearbeitung – verdächtige Mails werden in Minuten aus allen betroffenen Postfächern entfernt, und Angriffsketten werden frühzeitig unterbrochen. Bemerkenswert: 71% der Unternehmen mit E-Mail-Breach wurden auch Opfer von Ransomware – ein klarer Auftrag, E-Mail-Sicherheit als Kernmaßnahme zu priorisieren.

Anwendungen und APIs absichern: WAF, Bot-Mitigation und WAAP

Moderne Angriffe zielen zunehmend auf Web-Apps und APIs. Die Barracuda Web Application Firewall und die Cloud-basierten WAAP-Dienste schützen vor OWASP-Top-10-Risiken, Zero-Day-Exploits, Datenabfluss und L7-DDoS. API-Protection deckt REST/JSON, XML und auch GraphQL ab – einschließlich Erkennung automatisierter Bot-Angriffe. So werden Exfiltration und Ransomware-Vorstufen an der Applikationsschicht gestoppt, bevor sie in Erpressungsszenarien münden.

Zero-Trust-Zugriff statt VPN-Blindspots: Barracuda SecureEdge (ZTNA/SASE)

Klassische VPNs bieten oft zu groben Zugriff. Mit Barracuda SecureEdge lassen sich Zero-Trust-Zugriffsrichtlinien, Gerätezustand und Sicherheitsinspektion durchsetzen – in der Cloud, in der Niederlassung oder am Endgerät. Das erschwert laterale Bewegungen und begrenzt die Angriffsfläche, selbst wenn Zugangsdaten kompromittiert wurden. Integrierte SD-WAN- und Firewall-as-a-Service-Funktionen unterstützen konsistentes Policy-Enforcement und Sichtbarkeit.

Datenwiederherstellung, die hält, was sie verspricht: Immutable Backups & Cloud-to-Cloud Backup

Zahlen nützt wenig, wenn der Schlüssel nicht funktioniert – robuste, unveränderliche Backups sind daher Pflicht. Barracuda Backup und Cloud-to-Cloud Backup für Microsoft 365 speichern Daten nach dem Write-Once-Prinzip, verhindern

direkten Zugriff und schützen auch vor API-Manipulation. So bleiben Wiederherstellungen möglich, selbst wenn Angreifer Schattenkopien löschen oder Backups ins Visier nehmen. Unterstützt werden Exchange, SharePoint, OneDrive, Teams, OneNote und Entra ID – mit granularer Suche und schneller Wiederherstellung.

24/7 Erkennung und Reaktion: Managed XDR mit globalem SOC

Wenn jede Minute zählt, liefert Barracuda Managed XDR rund um die Uhr Telemetrie-Korrelation über E-Mail, Endpunkte, Netzwerke, Cloud und Identitäten – gemappt an MITRE ATT&CK. Das globale SOC verkürzt die Zeit bis zur Eindämmung drastisch und unterstützt dich bei Triage, Forensik und Wiederanlauf. Offene Integrationen ermöglichen die Nutzung bestehender Tools, während ein zentrales Dashboard Transparenz schafft.

Integrierte Plattform statt Tool-Wildwuchs

Die Datenlage ist eindeutig: Fragmentierte Sicherheitslandschaften mit vielen, schlecht integrierten Einzellösungen begünstigen erfolgreiche Ransomware-Angriffe. BarracudaONE bündelt Schutz für E-Mail, Daten, Anwendungen und Netzwerke in einer AI-gestützten Plattform mit zentralem Dashboard – inklusive 24/7 Managed XDR. Das reduziert Lücken, vereinfacht den Betrieb und stärkt die Cyber-Resilienz messbar.

Fazit: Prävention, Erkennung, Reaktion und Recovery – als geschlossener Kreislauf

Wirksamer Ransomware-Schutz entsteht erst im Zusammenspiel: E-Mail-Prävention und schnelle Post-Delivery-Response, WAAP/WAF für Apps und APIs, Zero-Trust-Zugriff gegen laterale Bewegung, unveränderliche Backups für belastbare Wiederherstellung sowie 24/7 XDR für rasche Eindämmung.

Genau diese Klammer setzt Barracuda – integriert, skalierbar und für Organisationen jeder Größe. Die aktuelle Forschung zeigt: Wer segmentiert, konfiguriert, trainiert, Backups testet und integrierte Sicherheit einsetzt, reduziert Risiko und Folgeschäden deutlich.

Ulrich Parthier

SPOT AN FÜR STARKE IT-LÖSUNGEN



Die besten IT-Lösungen | Die innovativsten Anbieter | Alles auf einen Blick!

UNSERE PREMIUMANBIETER



Hier könnte Ihr Logo platziert sein!
Jetzt buchen.

Ihre Ansprechpartner:



Kerstin Fraenzke
Head of Media Consulting
Tel. +49 8104 6494 19
fraenzke@it-verlag.de



Karen Reetz-Resch
Media Consulting
Tel. +49 8121 9775 94
reetz@it-verlag.de



Marion Mann
Media Consulting
Tel. +49 152 363 412 55
mann@it-verlag.de

it-daily.net/it-spotlight

RANSOMWARE- ABWEHR

MEHRSTUFIGE VERTEIDIGUNGSSTRATEGIEN ERFORDERLICH

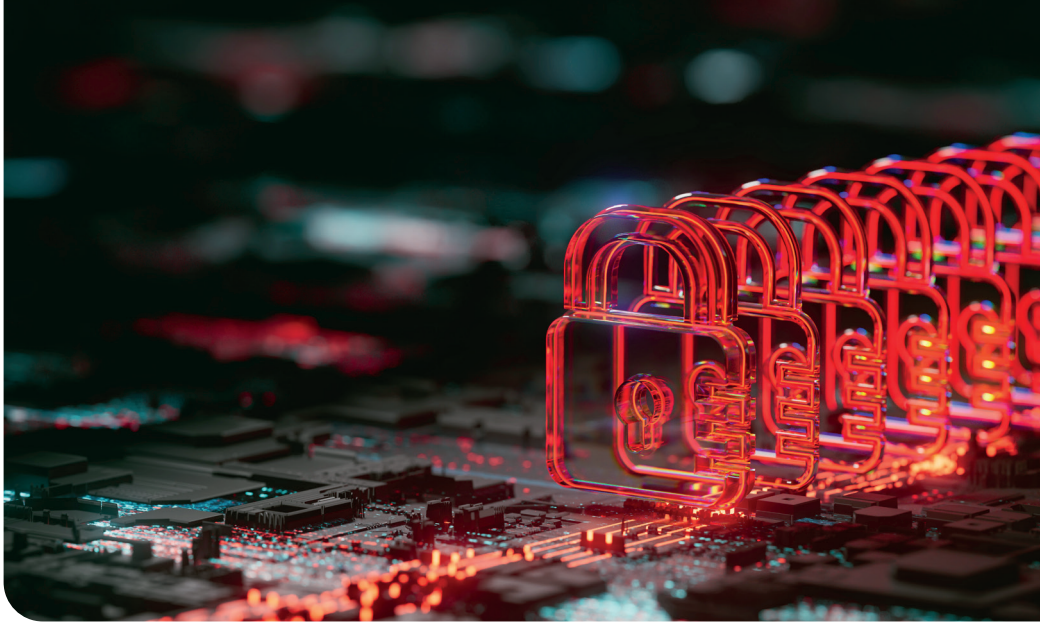
Ein ganzheitlicher Ansatz mit innovativen Cyberstorage-Technologien hilft gegen die wachsende Cyber-Bedrohung.

Die Bedrohung durch Ransomware hat in den letzten Jahren exponentiell zugenommen und entwickelt sich zu einer der kritischsten Herausforderungen für Unternehmen aller Größenordnungen. Während frühere Angriffe hauptsächlich automatisiert erfolgten, dominieren heute von Menschen gesteuerte, gezielte Attacken die Bedrohungslandschaft. Diese sophisticated „Human-Operated Ransomware“ kann wochenlang unentdeckt in Netzwerken verweilen, bevor der eigentliche Verschlüsselungsangriff erfolgt. Laut aktuellen Studien werden bis 2025 mindestens 75% aller Unternehmen mit einem oder mehreren Ransomware-Angriffen konfrontiert sein. Die durchschnittlichen Kosten für Wiederherstellung und Ausfallzeiten können dabei das Zehnfache des geforderten Lösegelds betragen.

Die Evolution der Ransomware-Bedrohung

Die moderne Ransomware-Landschaft zeichnet sich durch mehrere charakteristische Entwicklungen aus, die traditionelle Sicherheitsansätze vor neue Herausforderungen stellen. Angreifer haben ihre Taktiken von der einfachen Datenverschlüsselung zu komplexen, mehrstufigen Erpressungsstrategien weiterentwickelt. Die sogenannte "Double Extortion" kombiniert Datenverschlüsselung mit Datendiebstahl - Angreifer drohen nicht nur mit der Vernichtung der Daten, sondern auch mit deren Veröffentlichung. Einige Gruppen gehen sogar noch weiter zur „Triple Extortion“, bei der zusätzlich Kunden, Partner oder Behörden direkt kontaktiert werden.

Der typische Angriffsverlauf beginnt oft mit kompromittierten Anmeldedaten oder Phishing-Attacken. Angreifer verschaffen sich zunächst Zugang zu einem einzelnen



System und bewegen sich dann lateral durch das Netzwerk, sammeln Informationen über kritische Systeme und Daten, eskalieren ihre Privilegien und deaktivieren Sicherheitssysteme einschließlich Backup-Lösungen. Erst nach dieser gründlichen Vorbereitung erfolgt die finale Verschlüsselung.

Strategische Grundpfeiler

Ein effektiver Schutz gegen Ransomware erfordert eine durchdachte Strategie, die sich auf vier zentrale Phasen konzentriert: Prävention, Erkennung, Datenschutz und Wiederherstellung. Diese Strategie muss sowohl technische als auch organisatorische Aspekte berücksichtigen und eine Balance zwischen Benutzerfreundlichkeit und Sicherheit schaffen.

Der präventive Schutzwall

Die erste Verteidigungslinie gegen Ransomware besteht in der Verhinderung des initialen Eindringens. Hier spielen mehrere Faktoren zusammen, die synergistisch wirken müssen. Ein robustes Asset-Management bildet die Grundlage, denn nur was bekannt ist, kann auch geschützt werden. Besondere Aufmerksamkeit verdienen dabei Legacy-Systeme, die oft übersehen werden, aber kritische Schwachstellen darstellen.

Das Vulnerability Management muss risikobasiert und kontinuierlich erfolgen. Threat Intelligence sollte dabei helfen, Prioritäten zu setzen - Schwachstellen, die

aktiv von Ransomware-Gruppen ausgenutzt werden, erfordern sofortige Aufmerksamkeit. Penetrationstests und Breach-and-Attack-Simulationen decken Lücken auf, die automatisierte Scans übersehen.

Ein kritischer Aspekt ist das Identity and Access Management. Die Entfernung lokaler Administratorrechte für normale Benutzer und die Implementierung einer starken Authentifizierung für privilegierte Konten reduzieren das Risiko einer Kompromittierung erheblich. Dark Web Monitoring Services können frühzeitig vor kompromittierten Zugangsdaten warnen.

Die Erkennungsschicht

Auch die beste Prävention kann nicht alle Angriffe verhindern. Daher ist die frühzeitige Erkennung von eindringenden Angreifern entscheidend. Moderne EDR-Lösungen (Endpoint Detection and Response) können verdächtige Aktivitäten identifizieren, bevor die eigentliche Ransomware aktiviert wird. Network Detection and Response (NDR) Systeme überwachen den Netzwerkverkehr auf Anomalien und Command-and-Control-Kommunikation.

Verhaltensbasierte Analyse spielt hier eine Schlüsselrolle. Anstatt nur nach bekannten Signaturen zu suchen, werden Verhaltensmuster analysiert. Plötzliche Änderungen in Datenzugriffsmustern, ungewöhnliche Netzwerkkommunikation oder die massenhafte Umbenennung von Dateien können frühe Indikatoren für einen laufenden Angriff sein.

SIEM-Systeme können verschiedene Datenquellen korrelieren und ein ganzheitliches Bild der Sicherheitslage liefern. Besonders wichtig ist es, auch auf das zu achten, was "nicht passiert" - wenn Backup-Zeitpläne geändert oder Sicherheitstools deaktiviert werden, sollten sofort Alarme ausgelöst werden.

Cyberstorage: Die neue Dimension der Datensicherheit

Eine revolutionäre Entwicklung in der Ransomware-Abwehr stellt das Konzept des Cyberstorage dar. Diese innovative Technologie wurde von Gartner als neue Kategorie im Hype Cycle 2022 Innovation Trigger Section eingeführt und repräsentiert einen fundamentalen Paradigmenwechsel von der traditionellen Perimeter-Verteidigung hin zu einem datenorientierten Sicherheitsansatz.

DIE VIER VERTEIDIGUNGSLINIEN GEGEN RANSOMWARE

#1 Perimeter & Zugang

Secure Email Gateways, Web Gateways, Firewalls, VPN mit MFA

Ziel: Eindringen verhindern

#2 Endpunkt & Netzwerk

EDR, EPP, Netzwerksegmentierung, Zero-Trust-Architektur

Ziel: Ausbreitung stoppen

#3 Traditioneller Datenschutz

Immutable Backups, 3-2-1-1-Regel, Offline-Kopien

Ziel: Wiederherstellung ermöglichen

#4 Cyberstorage (NEU)

Datenfragmentierung, Multicloud-Verteilung, Selbstheilung

Ziel: Daten auch bei Exfiltration wertlos machen

Was ist Cyberstorage?

Cyberstorage ist zwischen der Netzwerkinfrastruktur und dem Speichersystem angesiedelt und bietet Unternehmen eine Sicherheit, bei der die Daten im Vordergrund stehen. Im Gegensatz zu herkömmlichen Sicherheitslösungen, die versuchen, Angreifer fernzuhalten, geht Cyberstorage davon aus, dass Angriffe erfolgreich sein werden, und konzentriert sich darauf, die Daten selbst zu schützen.

Der Kern des Cyberstorage-Konzepts liegt in der Datenfragmentierung. Dabei werden Dateien in mehrere Fragmente aufgeteilt und über verschiedene, geografisch und physisch getrennte Speicherorte verteilt - einen sogenannten "Datenhafen" (Data Harbour). Kein einzelner Speicherort enthält dabei alle Fragmente, die zur vollständigen Wiederherstellung einer Datei erforderlich sind.

Fragmentierte Daten als ultimativer Ransomware-Schutz

Die Fragmentierung von Daten bietet mehrere kritische Vorteile gegen moderne Ransomware-Bedrohungen:

- **Schutz vor Double und Triple Extortion:** Bei traditionellen Ransomware-Angriffen mit doppelter Erpressung werden zunächst Kopien der Daten gestohlen oder exfiltriert, bevor sie verschlüsselt werden. Mit fragmentierten Daten sind alle exfiltrierten Daten von Natur aus unvollständig und für den Angreifer völlig nutzlos - selbst wenn sie erfolgreich gestohlen werden.
- **Eliminierung des Single Point of Failure:** Während verschlüsselte Daten immer noch an einem einzigen Ort gespeichert sind und theoretisch mit einem einzigen Schlüssel entschlüsselt werden können, eliminiert die Fragmentierung diesen zentralen Angriffspunkt vollständig. Jedes Fragment ist zusätzlich mit einem anderen Schlüssel verschlüsselt.
- **Wertlose Darknet-Daten:** Selbst wenn Angreifer Fragmente erfolgreich exfiltrieren und im Darknet zum Verkauf anbieten, sind diese Fragmente einzeln vollkommen wertlos. Ohne Zugang zu allen Fragmenten und den entsprechenden Entschlüsselungsschlüsseln können Käufer im Darknet nichts mit den gestohlenen Daten anfangen.

Technische Umsetzung des Cyberstorage-Konzepts

Moderne Cyberstorage-Lösungen arbeiten mit einem mehrstufigen Ansatz:

- ❶ **Automatische Fragmentierung:** Dateien werden automatisch in mehrere Fragmente aufgeteilt, wobei jedes Fragment einzeln verschlüsselt wird.
- ❷ **Multicloud-Verteilung:** Die Fragmente werden über verschiedene Cloud-Anbieter und geografische Standorte verteilt, um maximale Ausfallsicherheit zu gewährleisten.
- ❸ **Selbstheilende Systeme:** Wenn ein Speicherort kompromittiert oder nicht verfügbar ist, können die Daten automatisch aus anderen verfügbaren Fragmenten rekonstruiert werden.
- ❹ **Transparente Benutzerexperience:** Trotz der komplexen Backend-Technologie bleibt die Benutzererfahrung transparent, und Änderungen der Latenz sind in der Regel nicht bemerkbar.

Integration in bestehende Sicherheitsarchitekturen

Cyberstorage ergänzt bestehende Sicherheitsmaßnahmen und bildet eine zusätzliche, kritische Verteidigungsschicht:

- **Backup-Schutz:** Traditionelle Backup-Lösungen sind zunehmend Ziel von Ransomware-Angriffen. Jüngste Untersuchungen zeigen, dass 72% der Unternehmen im Jahr 2021 von Angriffen auf ihre Backup-Repositories betroffen waren. Cyberstorage-Technologien können diese kritische Schwachstelle eliminieren.
- **Compliance-Vorteile:** Die inhärente Fragmentierung und Verschlüsselung vereinfacht die Einhaltung von Datenschutzvorschriften wie GDPR, HIPAA oder PCI-DSS erheblich, da gestohlene Fragmente per Definition unvollständig und nutzlos sind.
- **Proaktive Bedrohungserkennung:** Moderne Cyberstorage-Lösungen integrieren auch erweiterte Analysefunktionen, die Anomalien in Datenzugriffsmustern erkennen und automatisch Gegenmaßnahmen einleiten können.
- **Mehrstufige Verteidigungslinien mit Cyberstorage:** Eine effektive Ransomware-Abwehr erfordert mehrere, sich ergänzende Verteidigungsebenen, die auch dann Schutz bieten, wenn einzelne Maßnahmen versagen. Cyberstorage fügt hier eine völlig neue Dimension hinzu.



Erste Verteidigungslinie: Perimeter und Zugang

Die äußere Verteidigungslinie umfasst alle Maßnahmen, die das Eindringen von Angreifern in die IT-Infrastruktur verhindern sollen. Secure Email Gateways filtern schädliche E-Mails heraus, bevor sie Benutzer erreichen. Secure Web Gateways blockieren den Zugang zu kompromittierten oder bekanntermaßen schädlichen Websites. Web-Isolation-Technologien können verdächtige Inhalte in einer sicheren Sandbox-Umgebung ausführen.

Firewalls der nächsten Generation mit integrierten IPS-Funktionen bilden eine weitere Barriere. Besonders wichtig ist die ordnungsgemäße Konfiguration und regelmäßige Aktualisierung der Regelwerke. VPN-Lösungen müssen sicher konfiguriert sein und sollten Multi-Faktor-Authentifizierung erfordern.

Zweite Verteidigungslinie: Endpunkt- und Netzwerksicherheit

Auf der Endpunktebene bilden moderne EPP-Lösungen (Endpoint Protection Platforms) die Basis. Diese sollten durch EDR-Funktionalitäten erweitert werden, die nicht nur Malware erkennen, sondern auch verdächtige Verhaltensweisen identifizieren können. Die Integration mit SOAR-Plattformen (Security Orchestration, Automation and Response) ermöglicht automatisierte Reaktionen auf Bedrohungen.

Netzwerksegmentierung ist ein oft unterschätzter, aber kritischer Baustein. Durch die Aufteilung des Netzwerks in kleinere Segmente kann die laterale Bewegung von Angreifern erheblich erschwert werden. Zero-Trust-Netzwerkarchitekturen gehen noch einen Schritt weiter und erfordern eine kontinuierliche Verifizierung aller Verbindungen.

Dritte Verteidigungslinie: Traditioneller Daten- und Backup-Schutz

Diese Ebene war traditionell die letzte Chance zur Wiederherstellung nach einem erfolgreichen Angriff. Moderne Backup-Lösungen müssen über spezielle Ransomware-Schutzfunktionen verfügen. Dazu gehören unveränderliche Speicherformate, bei denen einmal geschriebene Daten nicht mehr verändert werden können, sowie die Erkennung von Anomalien in Backup-Prozessen.

Die 3-2-1-Regel hat sich als Best Practice etabliert: drei Kopien der Daten auf zwei verschiedenen Medientypen, wobei eine Kopie offline und eine weitere

unveränderlich gespeichert wird. Cloud-basierte Backup-Lösungen können hier wertvolle Dienste leisten, sofern sie ordnungsgemäß konfiguriert und gegen Angriffe gehärtet sind.

Vierte Verteidigungslinie: Cyberstorage als ultimative Absicherung

Cyberstorage bildet die neue, vierte Verteidigungslinie, die selbst dann Schutz bietet, wenn alle anderen Maßnahmen versagt haben. Diese Schicht operiert nach drei grundlegenden Prinzipien:

- ❶ **Absorption statt Abwehr:** Anstatt Angriffe zu verhindern, werden sie absorbiert, ohne dass verwertbare Daten preisgegeben werden.
- ❷ **Data-First Security:** Der Fokus liegt auf dem Schutz der Daten selbst, nicht auf den Speichermedien oder der Infrastruktur.
- ❸ **Automatische Selbstheilung:** Kompromittierte Fragmente werden automatisch identifiziert und durch gesunde Kopien ersetzt.

Wiederherstellung im Worst-Case-Szenario

Trotz aller Präventionsmaßnahmen und Cyberstorage-Technologien kann ein Ransomware-Angriff erfolgreich sein. In diesem Fall ist eine schnelle und effektive Wiederherstellung entscheidend für das Überleben des Unternehmens.

Sofortmaßnahmen nach der Erkennung

Die ersten Minuten nach der Erkennung eines Ransomware-Angriffs sind kritisch. Ein vorbereitetes Incident Response Team muss sofort aktiviert werden. Die Isolierung betroffener Systeme steht dabei an erster Stelle - moderne EDR-Lösungen bieten oft Funktionen zur automatischen Isolation.

Mit Cyberstorage-Technologien können Unternehmen jedoch einen entscheidenden Vorteil nutzen: Selbst wenn Angreifer erfolgreich in das System eingedrungen sind und Daten exfiltriert haben, bleiben diese Daten aufgrund der Fragmentierung wertlos. Dies verschafft IT-Teams wertvolle Zeit für die Eindämmung, ohne den Druck der drohenden Datenveröffentlichung.

Forensik und Schadensbewertung mit Cyberstorage-Unterstützung

Während die Eindämmung läuft, muss parallel eine gründliche forensische Analyse beginnen. Cyberstorage-Lösungen können hier wertvolle Einblicke liefern, da sie detaillierte Logs über Datenzugriffe und -bewegungen führen. Die automatische Erkennung von Anomalien in den Fragmentierungsmustern kann dabei helfen, den Zeitpunkt der initialen Kompromittierung genauer zu bestimmen.

Ein wesentlicher Vorteil von Cyberstorage liegt darin, dass die Bewertung gestohlener Daten vereinfacht wird: Da alle exfiltrierten Fragmente per Definition unvollständig sind, ist das regulatorische und rechtliche Risiko erheblich reduziert.

Der erweiterte Wiederherstellungsprozess

Die Wiederherstellung mit Cyberstorage-Technologien erfolgt in mehreren Phasen:

- ❶ **Sofortige Datenverfügbarkeit:** Durch die Selbstheilungsfunktionen von Cyberstorage-Systemen können kritische Daten oft sofort wiederhergestellt werden, ohne auf traditionelle Backup-Prozesse warten zu müssen.
- ❷ **Fragmentvalidierung:** Jedes Fragment wird auf Integrität geprüft und kompromittierte Fragmente werden durch gesunde Kopien ersetzt.
- ❸ **Systemrekonstruktion:** Parallel zur Datenwiederherstellung erfolgt die Rekonstruktion der kompromittierten Systeme nach etablierten Verfahren.
- ❹ **Kontinuitätsgewährleistung:** Die fragmentierte Architektur ermöglicht es oft, den Geschäftsbetrieb mit minimalen Unterbrechungen fortzusetzen.

Organisatorische Aspekte und Governance

Technische Maßnahmen allein reichen nicht aus - erfolgreiche Ransomware-Abwehr erfordert auch eine solide organisatorische Grundlage, die das neue Cyberstorage-Paradigma berücksichtigt.

Mitarbeitersensibilisierung für die neue Datenrealität

Mit der Einführung von Cyberstorage-Technologien müssen Mitarbeiter über die neue Datenarchitektur informiert werden. Während die Benutzererfahrung transparent bleibt, ist es wichtig, dass Mitarbeiter verstehen, dass ihre Daten durch innovative Technologien geschützt sind, die selbst bei erfolgreichen Angriffen Schutz bieten.

Notfallplanung mit Cyberstorage-Integration

Ransomware-Response-Pläne müssen überarbeitet werden, um die Möglichkeiten von Cyberstorage-Technologien zu berücksichtigen. Die Tatsache, dass exfiltrierte Daten wertlos sind, verändert die Verhandlungsposition mit Angreifern grundlegend und kann die Entscheidungsfindung bei Lösegeldforderungen beeinflussen.

Regulatorische Anforderungen und Cyberstorage

Die regulatorische Landschaft profitiert erheblich von Cyberstorage-Technologien. Die NIS2-Richtlinie der EU und andere Cybersecurity-Vorschriften fordern robuste Datenschutzmaßnahmen. Cyberstorage geht über diese Anforderungen hinaus, indem es Datenschutz auch bei erfolgreichen Angriffen gewährleistet.

Zukunftsausblick und Emerging Technologies

Die Cyberstorage-Kategorie steht noch am Anfang ihrer Entwicklung. Gartner prognostiziert, dass während heute nur etwa 10% der Unternehmen integrierten Ransomware-Schutz für ihre Daten benötigen, diese Zahl in den nächsten drei Jahren auf 60% ansteigen wird.

KI-gestützte Cyberstorage-Systeme

Künstliche Intelligenz wird die nächste Evolution der Cyberstorage-Technologien antreiben. KI-basierte Systeme können Fragmentierungsmuster optimieren, Anomalien noch präziser erkennen und Selbstheilungsprozesse intelligenter steuern.

Quantum-resistente Fragmentierung

Mit der Entwicklung von Quantencomputern müssen auch Cyberstorage-Technologien quantum-resistente Verschlüsselungsmethoden integrieren. Die Fragmentierung bietet hier jedoch einen inhärenten Vorteil: Selbst wenn Quantencomputer einzelne Fragmente entschlüsseln können, bleibt der Gesamtdatensatz ohne alle Fragmente unbrauchbar.

Erfolgsmessung und kontinuierliche Verbesserung

Die Effektivität von Cyberstorage-Implementierungen erfordert neue Metriken:

- **Data Fragmentation Integrity Rate:** Prozentsatz der erfolgreich fragmentierten und verteilten Daten
- **Self-Healing Response Time:** Zeit bis zur automatischen Wiederherstellung kompromittierter Fragmente
- **Exfiltration Impact Mitigation:** Messung der Wertlosigkeit exfiltrierter Daten durch Fragmentierung

Fazit: Ein paradigmatischer Wandel in der Ransomware-Abwehr

Die Einführung von Cyberstorage-Technologien markiert einen fundamentalen Wandel in der Cybersecurity-Strategie. Während traditionelle Ansätze darauf abzielen, Angreifer fernzuhalten, akzeptiert Cyberstorage die Realität erfolgreicher Angriffe und macht diese durch datenorientierte Schutzmaßnahmen wirkungslos.

Cyberstorage löst dabei ein zentrales Problem moderner Ransomware: die Verwertbarkeit gestohlener Daten. Durch die Fragmentierung werden exfiltrierte Daten grundsätzlich wertlos - sie können weder im Darknet verkauft noch für Erpressungen verwendet werden. Dies gilt selbst für verschlüsselte Daten, da einzelne Fragmente ohne die anderen Teile des Puzzles nutzlos bleiben.

Die mehrstufige Verteidigungsstrategie gegen Ransomware wird durch Cyberstorage um eine kritische vierte Ebene erweitert, die selbst dann Schutz bietet, wenn alle anderen Maßnahmen versagen. Unternehmen, die heute in diese innovative Technologie investieren, positionieren sich nicht nur defensiv gegen aktuelle Bedrohungen, sondern schaffen auch eine zukunftssichere Grundlage für die sich weiterentwickelnde Cyber-Bedrohungslandschaft.

Der Erfolg liegt dabei nicht in der Cyberstorage-Technologie als isolierte „Silver Bullet“-Lösung, sondern in ihrer orchestrierten Integration mit bestehenden Sicherheitsmaßnahmen. Die Kombination aus Prävention, Erkennung, traditionellem

Datenschutz und innovativem Cyberstorage schafft eine Cyber-Resilienz, die auch ausgeklügeltsten Ransomware-Angriffen standhält.

Die Investition in Cyber-Resilienz mit Cyberstorage-Komponenten ist dabei nicht nur ein Kostenfaktor, sondern ein strategischer Wettbewerbsvorteil in einer zunehmend digitalisierten Wirtschaft, in der Daten das wertvollste Gut darstellen - und nun endlich auch entsprechend geschützt werden können.

Ulrich Parthier





Wie schnell kann Ihre Security-Lösung Angriffe entdecken?

>35 % der Cyberangriffe dauern einen Monat und länger*

Kaspersky Next Complete ist EPP, EDR und MDR in einem. Unser Power-Trio bietet:

- Starken Endpoint-Schutz, umfassende Kontrollmechanismen, Schulungsangebote und Patch-Management
- EDR-Funktionen für mehr Transparenz, eine schnelle Untersuchung sowie angeleitete Abwehrmaßnahmen
- 24/7 Managed SOC



kas.pr/complete

kaspersky bring on
the future

*Kaspersky Incident Response Analyst Report 2024

Copyright © 2025 AO Kaspersky Lab. All rights reserved.