RAPID7

EXECUTIVE BRIEF

DEN BESCHLEUNIGTEN CYBERANGRIFFSZYKLUS ENTSCHLÜSSELN

Ein CISO-Briefing zum Rapid7 Global Threat Landscape Report 2026

Aus Sicht der Führungskräfte: Geschwindigkeit ist kein Vorteil mehr

Die Sicherheit ist im Jahr 2025 nicht daran gescheitert, dass Verteidiger zu langsam waren. Sie ist gescheitert, weil Geschwindigkeit kein entscheidender Differenzierungsfaktor mehr ist.

Das bestimmende Merkmal der diesjährigen Bedrohungsdaten ist die Beschleunigung. Angreifer setzen nicht auf radikal neue Techniken, sondern führen bekannte Vorgehensweisen schneller, in größerem Umfang und mit strengerer operativer Disziplin aus. Automatisierung, künstliche Intelligenz (KI) und die Industrialisierung des cyberkriminellen Ökosystems haben die Zeitspanne zwischen Gefährdung und Auswirkung verkürzt. Was früher Wochen dauerte, dauert heute nur noch Tage – manchmal sogar nur Minuten.

Für CISOs bedeutet dies eine Verlagerung des Betriebsmodells. Die zentrale Frage lautet nicht mehr, wie schnell Sie reagieren können, sondern wie gut Sie Ihre Gefährdung reduzieren können, bevor Angreifer diese ausnutzen.

1. DAS VORHERSAGEFENSTER IST KOLLABIERT

Die folgenreichste Veränderung im Jahr 2025 war die, dass das Vorhersagefenster kollabiert ist. Die bestätigte Ausnutzung von neu bekannt gewordenen **CVSS 7-10-Schwachstellen stieg um 105 %** im Jahresvergleich, von **71 im Jahr 2024 auf 146 im Jahr 2025.** Innerhalb von vier Jahren stieg die Zahl der ausgenutzten Schwachstellen von 7 im Jahr 2022 auf 146 im Jahr 2025, und die Ausnutzungsrate im Verhältnis zur Zahl der gemeldeten Schwachstellen stieg von weniger als 0,1 % auf 0,8 %.

Auch das Timing hat sich verdichtet. Der Medianwert der Zeit von der Veröffentlichung bis zur Aufnahme in die CISA Known Exploited Vulnerabilities (KEV) fiel von 8,5 Tagen auf 5,0 Tage und der Mittelwert von 61,0 Tagen auf 28,5 Tage. Die Kategorie „hochriskant, aber noch nicht ausgenutzt“ ist inzwischen weitgehend verschwunden. Im Jahr 2024 wiesen 338 Schwachstellen eine EPSS-Bewertung (Exploit Prediction Scoring System) ≥ 0,7 auf, ohne dass eine Ausnutzung bestätigt wurde; im Jahr 2025 waren es nur noch 65. Innerhalb des Emerging Threat Response-Datensatzes sank die Zahl der Schwachstellen mit hohem Risiko, die aber noch nicht ausgenutzt wurden, von **15 auf 1**, während die Zahl der bestätigten Ausnutzungen von 5 auf 22 stieg.

Sicherheitslücken mit schwerwiegenden Folgen sind mittlerweile operative Gegebenheiten und keine Wahrscheinlichkeiten mehr. Herkömmliche Priorisierungszyklen sind nicht auf die Zeitpläne der Angreifer abgestimmt. Im Jahr 2025 waren die SOCs nicht durch das Volumen überfordert, sondern durch die schnelle Entwicklung überholt.

0,0625 in

2. ANGREIFER NUTZEN UNGESCHÜTZTE SCHWACHSTELLEN ZU IHREM VORTEIL

Die meisten Angriffe im Jahr 2025 gingen auf vermeidbare Gefährdungen zurück, nicht auf neuartige Zero-Day-Exploits. Gültige Konten **ohne Multi-Faktor-Authentifizierung machten 43,9 % der Incidents aus**. Die Ausnutzung von Schwachstellen machte 24,6 % aus, und exponierte Services 7,0 %.

Die Aktivitäten auf den illegalen Marktplätzen spiegeln dasselbe Muster wider. **Zugriffe über das Remote Desktop Protocol machten 21,2 % der Angebote aus, VPN-Zugänge 12,8 % und RDWeb 11,2 %**. Befugnisse auf Domänenebene wurden häufig angeboten, und der Zugriff wurde routinemäßig gebündelt und verkauft. In nur sechs Monaten listete DarkForums 221 Zugangsangebote und RAMP 208. Der durchschnittliche vermutete Umsatz der betroffenen Unternehmen lag bei über 3,2 Milliarden US-Dollar, bei einem durchschnittlichen Grundpreis von 113.275 US-Dollar pro Angebot. Broker für Erstzugriffe haben die Gefährdung industrialisiert. Sie sammeln Zugangsdaten, validieren den Zugriff und verkaufen ihn als Ware, wie es auch legitime Unternehmen tun würden.

3. DIE AUSNUTZUNG KONZENTRIERT SICH AUF ZUVERLÄSSIGE SCHWACHSTELLENKLASSEN

Obwohl die Gesamtzahl der hochkritischen und kritischen CVEs im Jahresvergleich moderat von etwa 16.200 auf 18.100 anstieg, verteilte sich die Ausnutzung nicht gleichmäßig. Sie konzentrierte sich auf eine kleine Gruppe zuverlässiger Schwachstellenklassen.

CWE-502 (Deserialisierung) war im Jahr 2025 die am häufigsten ausgenutzte Ursache, wobei Authentifizierungsumgehung und Speicherbeschädigung ebenfalls durchgängig vertreten waren. Hochkarätige Ransomware-Kampagnen zielten auf Deserialisierungsfehler und Authentifizierungsumgehung in Dateiübertragungssystemen, Kollaborationsplattformen und Edge-Geräten ab.

Im Gegensatz dazu spielten häufig auftretende Sicherheitslücken wie Cross-Site-Scripting und SQL Injection bei bestätigten Angriffen eine weitaus geringere Rolle. Angreifer priorisieren Zuverlässigkeit, Zugriff vor der Authentifizierung und skalierbare Remote-Code-Ausführung.

Dies unterstreicht für Schwachstellenmanagement-Programme die Notwendigkeit, Prioritäten auf der Grundlage der Ausnutzbarkeit, der Rolle der Ressource und des Gefährdungskontexts zu setzen, anstatt sich auf reine CVE-Zahlen zu stützen.

4. RANSOMWARE HAT SICH ZU EINER GESCHWINDIGKEITSOPTIMIERTEN ZUGANGSÖKONOMIE ENTWICKELT

Ransomware war auch 2025 das dominierende operative Ergebnis und **machte 42 % der Rapid7-MDR-Untersuchungen aus**. Die Anzahl der Leak-Beiträge stieg von 6.034 im Jahr 2024 auf 8.835 im Jahr 2025 und damit um **46,4 %.** Die Anzahl der aktiven Ransomware-Gruppen wuchs von 102 auf 140, wobei auch die durchschnittliche Anzahl der Beiträge pro Gruppe zunahm.

Qilin führte die Liste der Leak-Beiträge mit 1.029 Einträgen an, gefolgt von Akira und Cl0p. Modelle der doppelten Erpressung und Ransomware-as-a-Service dominierten dabei. Der Datendiebstahl erfolgte häufig vor der Verschlüsselung, was auf „Smash-and-Grab"-Erpressungstaktiken hindeutet, die darauf abzielen, den Druck schnell zu maximieren.

Bemerkenswert ist, dass Ransomware-Incidents überwiegend über vorhersehbare Wege zustande kamen, wie beispielsweise kompromittierte Zugangsdaten, ungeschützte VPN- oder RDP-Services und nicht gepatchte Edge-Infrastruktur. Hierbei handelt es sich nicht lediglich um ein Ransomware-Problem, sondern um die Monetarisierungsphase ungeschützter Schwachstellen.

5. EINGEBETTETER ZUGRIFF DEFINIERT DAS STRATEGISCHE RISIKO, NICHT PERIMETERVERLETZUNGEN

Der klassische Unternehmensperimeter ist verschwunden. Angreifer zielen auf Identitätssysteme, Cloud-Steuerungsebenen, Kollaborationsplattformen und die Infrastruktur am Netzwerkrand ab. In diesen Umgebungen verschwimmt die Grenze zwischen legitimen und böswilligen Aktivitäten, was die Erkennung und Eindämmung erschwert.

Staatsnahe Akteure positionieren sich vorzeitig in Telekommunikations-, Cloud-Umgebungen und Infrastrukturen, um langfristig präsent zu bleiben. Kriminelle Akteure nutzen dieselben Angriffsflächen zur Monetarisierung. Zu den im Jahr 2025 beobachteten Beispielen zählen „Operational Relay Box"-Netzwerke, die aus kompromittierten SOHO-Routern aufgebaut wurden, der Missbrauch von Kollaborationsplattformen für Command-and-Control-Zwecke, die Ausnutzung von GraphQL-APIs sowie spezielle Malware wie FrostyGoop, die auf industrielle Steuerungssysteme abzielt.

KI als Beschleunigungsebene und zugleich als Angriffsfläche

KI hat bestehende Angreifer-Playbooks verstärkt statt neue Kategorien zu schaffen – und damit die Zeit vom Erstzugriff bis zur Wirkung erheblich verkürzt. Dies wurde deutlich daran, dass Angreifer generative KI einsetzten, um Phishing und Aufklärung zu skalieren, Skripte zu verfeinern und Ransomware-Angriffe zu beschleunigen.

Gleichzeitig geriet auch die KI-Infrastruktur ins Visier, was zeigt, dass bekannte Schwachstellen inzwischen in dynamischen KI-Ökosystemen auftreten. In unseren Daten fanden sich unter anderem unsichere Deserialisierung in Model-Servern, offengelegte Tokens in selbst betriebenen Plattformen, Injektionsrisiken in Orchestrierungs-Frameworks sowie Supply-Chain-Angriffe wie das manipulierte Paket „postmark-mcp“.

KI muss daher als privilegierte Infrastruktur verwaltet werden. Ordnungsgemäß gepflegte Bestandsverzeichnisse, Zugriffskontrolle, Segmentierung und Token-Monitoring sind unerlässlich. Gleichzeitig werden KI-gestützte Sicherheitsmaßnahmen zunehmend notwendig, um mit der Geschwindigkeit der Angreifer Schritt zu halten.

Branchen- und regionalspezifische Ausrichtung

Auf Nordamerika entfielen 82 % der beobachteten Vorfälle, wobei rund 70 % der Leak-Posts aus den Vereinigten Staaten stammten. Am häufigsten wurden die Branchen Fertigung, Unternehmensdienstleistungen und Einzelhandel ins Visier genommen, wobei auch das Gesundheitswesen und der öffentliche Sektor stark betroffen waren.

Diese Sektoren kombinieren sensible Daten, finanzielle Liquidität und Lieferketten-Hebelwirkung, was sie sowohl für Erpressung als auch für strategische Vorpositionierung attraktiv macht.

Strategische Leitlinien für 2026

Die Daten verdeutlichen ein strukturelles Missverhältnis zwischen der Geschwindigkeit der Angreifer und traditionellen Verteidigungsprozessen. Um diese Lücke zu schließen, ist ein Umdenken hin zu präventiver Sicherheit als Betriebsmodell erforderlich.

Im Jahr 2026 empfehlen wir, dass CISOs:

- Priorisierung der kontinuierlichen Sichtbarkeit von Assets und Identitäten
- Konsistente Multi-Faktor-Authentifizierung erzwingen
- Absicherung der Edge-Infrastruktur
- Betrachtung von SaaS und KI als produktionskritische Systeme
- Erweiterung von Erkennungs- und Abwehr-Workflows durch Automatisierung und KI zur Beschleunigung der Untersuchungszeiträume

Einige Schwachstellen werden ausgenutzt werden; zum jetzigen Zeitpunkt ist dies ein natürlicher Teil des Zyklus. Daher sollte die Resilienzplanung dies berücksichtigen. Unveränderliche Backups, getestete Wiederherstellung, das Zurücksetzen von Anmeldedaten und einstudierte Incident-Response-Prozesse sind wesentliche Schutzmaßnahmen.

Fazit

Die Bedrohungslandschaft des Jahres 2026 ist durch Beschleunigung geprägt. Exploits erfolgen schneller, initialer Zugriff ist zur Ware geworden und Ransomware ist industrialisiert.

Die zentralen Schwachstellen sind jedoch nicht neu. Schwache Zugangsdaten, exponierte Services und ungepatchte Edge-Systeme bleiben weiterhin häufig genutzte Angriffsvektoren. Was jedoch neu ist, ist die Geschwindigkeit, mit der diese Schwachstellen identifiziert, gebündelt und ausgenutzt werden.

Für CISOs liegt der Wettbewerbsvorteil heute in einem klaren Überblick über die Gefährdungslage. Die Unternehmen, die ihre Angriffsfläche kontinuierlich im Blick behalten und Risiken bereits vor einer Ausnutzung minimieren, sind am besten gerüstet, um dem beschleunigten Zyklus von Cyberangriffen standzuhalten.

BERICHT HERUNTERLADEN

ÜBER RAPID7

Rapid7, Inc. (NASDAQ: RPD) ist ein weltweit führender Anbieter von KI-gestützten Managed Cybersecurity Operations, der Unternehmen dabei unterstützt, ihre Cyber-Resilienz zu verbessern.Die offene und erweiterbare Rapid7 Command Platform integriert Sicherheitsdaten und ergänzt diese mit KI, Threat Intelligence und 25 Jahren Erfahrung und Innovation, um Risiken zu reduzieren und Angreifer zu stoppen. Als anerkannter Marktführer im Bereich präventiver Managed Detection and Response (MDR) vereint Rapid7 die Erkennung und Abwehr von Sicherheitsrisiken und transformiert damit die Cybersicherheitsmaßnahmen von mehr als 11.500 Kunden weltweit. Weitere Informationen finden Sie auf unserer Website. Besuchen Sie außerdem unseren Blog oder folgen Sie uns auf LinkedIn oder X.

RAPID7

SICHERN SIE IHRE

Cloud | Anwendungen | Infrastruktur | Netzwerk | Daten

BESCHLEUNIGUNG MIT

Command-Plattform | Exposure Management | Angriffsflächen-Management | Schwachstellen-Management | Cloudnativer Anwendungsschutz | Anwendungssicherheit | Next-Gen SIEM | Threat Intelligence | MDR-Services | Incident-Response-Services | MVM-Services

SICHERHEIT, UM ANGREIFERN EINEN SCHRITT VORAUS ZU SEIN

Testen Sie unsere Sicherheitsplattform risikofrei – starten Sie Ihre Testversion auf **rapid7.com**