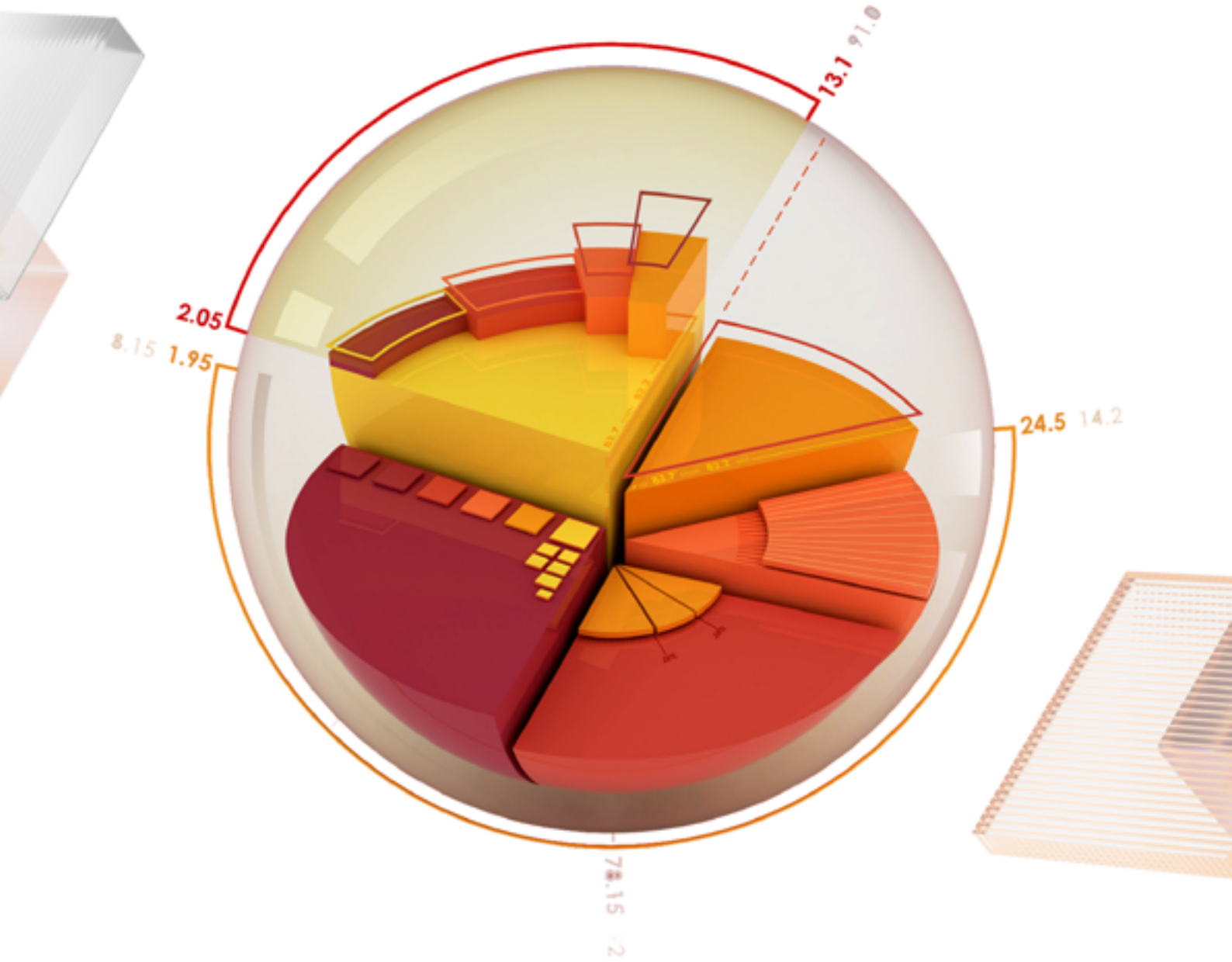
SONICWALL

2025 CYBER THREAT REPORT

WARUM SCHNELLES HANDELN UND STARKE VERBÜNDETE ESSENZIELL IM KAMPF GEGEN CYBERKRIMINELLE SIND



Nachricht von CEO Bob VanKirk

Wir alle haben es mit einer extrem dynamischen und immer komplexeren Bedrohungslandschaft zu tun. Während unsere Gegenspieler ihre Methoden permanent weiterentwickeln, vertrauen uns immer mehr Kunden den Schutz ihrer Netzwerke an. Zu Beginn des neuen Jahres möchte ich erst einmal betonen, wie wichtig unsere Partner in unserem gemeinsamen Kampf gegen Cyberbedrohungen sind. Sie machen eine sichere Zukunft für alle erst möglich. Durch den Schutz von Systemen und Netzwerken tragen wir zur Sicherheit von Einzelpersonen und Unternehmen bei, sodass sie ohne Angst vor Cyberangriffen erfolgreich handeln können. Das gelingt uns, indem wir alle gemeinsam an einem Strang ziehen. Darauf sind wir besonders stolz.

Bedrohungsakteure entwickeln ihre Angriffe konstant weiter und gehen immer raffinierter vor. Daher stand noch nie so viel auf dem Spiel. Unsere Daten zeigen, dass Angreifer so schnell zuschlagen wie nie zuvor: Die Mehrheit der Hacker greift Schwachstellen bereits innerhalb von nur zwei Tagen nach Veröffentlichung des Exploits an. Diese enorme Geschwindigkeit macht allen Organisationen zu schaffen, wobei insbesondere kleine und mittlere Unternehmen (KMUs) oft kaum Schritt halten können.

Im Jahr 2024 haben alarmierende Trends den dringenden Bedarf an proaktiven Verteidigungsstrategien verdeutlicht: Cyberattacken entwickeln sich weiter und werden immer vielfältiger. Kritische Netzwerkangriffe hätten zu mindestens 68 Ausfalltagen führen und somit möglicherweise 19 % des Umsatzes gefährden können.

Mit über 198 Millionen amerikanischen Patienten, die von Ransomware betroffen waren, sah sich der Gesundheitssektor in den Vereinigten Staaten (USA) beispiellosen Herausforderungen gegenüber. Die Angriffe erfolgten häufig erschreckend schnell. Unseren Daten zufolge hatten wir es mit 210.258 bisher unbekannten Malware-Varianten zu tun – im Schnitt 637 neue Bedrohungen täglich. Dies legt nahe, dass Bedrohungsakteure ständig neue Varianten hervorbringen. Die Geschwindigkeit der Angriffe ist dabei mit großer Wahrscheinlichkeit auf die schnelle Bereitstellung und Weiterentwicklung KI-basierter Tools zurückzuführen, die ihre Erfolgschancen erhöhen.

Vor diesem Hintergrund sollte KMUs, aber auch großen Unternehmen immer bewusst sein, dass sie im Kampf gegen Cyberkriminelle nicht alleine sind. Den besten Schutz bietet eine enge Partnerschaft mit Managed-Service-Providern (MSPs) und Managed-Security-Service-Providern (MSSPs). MSPs und MSSPs sollten sich wiederum mit Anbietern zusammentun, die Security-Operations-Center(SOC)-Services und ein 24/7/365-Monitoring für einen umfassenden Schutz bieten.

Ich freue mich, Ihnen heute den jährlich erscheinenden SonicWall Threat Report 2025 zu präsentieren. Darin nehmen wir die Entwicklungen des letzten Jahres in der Cyberbedrohungslandschaft unter die Lupe. Mit diesem Bericht möchten wir Ihnen einen besseren Einblick in die Sicherheitslandschaft vermitteln. Er ist zudem Ausdruck unseres Engagements – und zugleich ein wertvolles Instrument, um Ihnen, unseren Partnern, und unseren Kunden einen besseren Schutz und hilfreiche Anknüpfungspunkte bei Beratungsgesprächen zum heutigen Stellenwert von Sicherheit zu bieten.

Der diesjährige Report liefert nicht nur besorgniserregende Statistiken, sondern vor allem auch aussagekräftige Erkenntnisse, die Ihnen helfen, effektive Verteidigungsstrategien zu entwickeln und umzusetzen. Darüber hinaus haben wir wertvolle Perspektiven unserer 24/7-SOC-Analysten, Markteinblicke führender Cybersecurity-Versicherer und sogar von KI generierte Sichtweisen integriert.

Ich möchte allen unseren Partnern und Kunden ans Herz legen, diesen Bericht als strategisches Instrument in Gesprächen mit Stakeholdern und Kunden einzusetzen. Die darin enthaltenen Informationen helfen Ihnen dabei, ihren Kunden zu erklären, wie wichtig solide Cybersicherheitsmaßnahmen sind und welche Schritte erforderlich sind, um aktuelle Bedrohungen abzuwehren. Je enger wir zusammenarbeiten, desto erfolgreicher können wir Cyberbedrohungen bekämpfen und desto schneller können wir mit den Entwicklungen einer zunehmend dynamischen Bedrohungslandschaft Schritt halten. Ihr Feedback hat uns enorm dabei geholfen, unsere Aktivitäten und Maßnahmen zu verbessern. Natürlich werden wir Sie auch künftig mit allen nötigen Ressourcen unterstützen, die Sie für einen effektiven Schutz Ihrer Umgebungen benötigen.

Im Namen des gesamten SonicWall-Teams – einschließlich unserer engagierten Bedrohungsexperten von Capture Labs – ist es mir eine große Freude, diesen wichtigen Einblick in die neuesten Cybersecurity-Entwicklungen mit Ihnen zu teilen und Ihnen aufzuzeigen, wie wir gemeinsam diesen Herausforderungen entgegentreten können.

Bob VanKirk
President und CEO
SonicWall

BEDROHUNGSLANDSCHAFT

48 STUNDEN

In 61 % der Fälle nutzten Hacker neuen Exploit-Code innerhalb von 48 Stunden.

2024 wurden Organisationen vor 68 potenziellen Ausfalltagen bewahrt.

68 TAGE

6 Mrd.

Unsere Sensoren fingen das dritte Jahr in Folge mehr als 6 Milliarden kritische Netzwerkangriffe ab.

RANSOMWARE

Die Zahl der Ransomware-Angriffe stieg in Nordamerika moderat (+8 %) und in Lateinamerika explosionsweise (+259 %).

▲259 %

850.700 $

Durchschnittliche Kosten bei Ransomware: 2024 lag die durchschnittliche Ransomware-Lösegeldzahlung bei 850.700 USD, wobei die Gesamtkosten (einschließlich für Ausfallzeiten und Wiederherstellung) mit über 4,91 Millionen USD zu Buche schlugen.

MALWARE

▲8 %

Malware nahm um 8 % im Jahresvergleich zu, mit einem massiven Anstieg von 92 % allein im Mai.

IoT- UND VERSCHLÜSSELTE ANGRIFFE

IoT-Angriffe (+124 %) und verschlüsselte Bedrohungen (+93 %) stiegen weiterhin weltweit.

▲124 %

SECURITY-OPERATIONS-CENTER (SOC)

85 %

Identitätsdiebstahl, Cloud-Angriffe und kompromittierte Zugangsdaten machten 85 % der Warnmeldungen aus, die ein Eingreifen erforderten.

33 % der gemeldeten Cybersecurity-Versicherungsfälle sind auf BEC-Vorfälle zurückzuführen – im letzten Jahr waren es noch 9 %.

33 %

RTDMI™

637

NEUE VARIANTEN

PRO TAG

SonicWall identifizierte 210.258 bisher unbekannte Malware-Varianten – 637 pro Tag.

Ransomware-Angriffe erreichten 2024 neue Höhen

2024 machten Ransomware-Angriffe Organisationen rund um den Globus weiterhin das Leben schwer und untermauerten somit ihren Ruf, eine der kostspieligsten Bedrohungen für die Cybersicherheit zu sein. Letztes Jahr gab es signifikante Fortschritte bei den Ransomware-Attacken, wobei die Angreifer oft auf Double Extortion – also doppelte Erpressung – setzten. Besonders in Amerika stieg die Zahl der Angriffe massiv: um 259 % in LATAM bzw. 8 % in NOAM. Und während sicherlich alle Branchen von Ransomware betroffen waren, hatte der Healthcare-Bereich besonders unter schwerwiegenden Angriffen und katastrophalen Folgen zu leiden.

Double und Triple Extortion gehört mittlerweile zur Tagesordnung

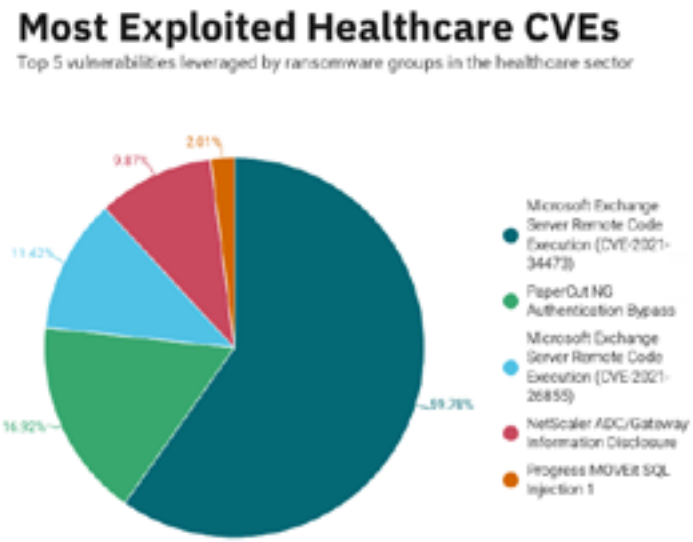
Nicht nur die Vorfälle mit Double Extortion stiegen das ganze Jahr über, auch Triple Extortion nahm zu, ganz besonders im Gesundheitswesen. Bei dieser Taktik werden nicht nur höchstkritische Daten einer Organisation verschlüsselt, sondern die Angreifer drohen auch damit, sensible Informationen zu veröffentlichen, wenn die Forderungen nicht erfüllt werden. So wird der Druck auf die Opfer, das Lösegeld zu zahlen, weiter erhöht, da die Cyberkriminellen sie gleich in mehrfacher Hinsicht mit ihren Daten erpressen. Im Gesundheitswesen gehen die Täter mit Triple Extortion sogar so weit, direkt die Patienten zu kontaktieren und mit der Veröffentlichung ihrer Daten zu drohen, wenn kein Lösegeld gezahlt wird. Durch die immer raffinierteren Ransomware-Tools – etwa durch den Einsatz von KI und Ransomware as a Service (RaaS) – sind diese Mehrfrontenangriffe nun auch für Kleinkriminelle einfacher möglich.

Healthcare und Ransomware: eine ungesunde Beziehung

Im Gesundheitssektor gab es 2024 den bisher größten Anstieg der Ransomware-Aktivitäten: Mehr als **198 Millionen** Amerikaner waren betroffen. Besonders hervorzuheben ist der Angriff auf Change Healthcare, mit über 100 Millionen Betroffenen einer der größten Vorfälle in der Geschichte.

In **95 %** aller Sicherheitsvorfälle im Gesundheitswesen war Ransomware involviert, was sie mit Abstand zur größten Bedrohung für diesen Sektor macht. Hochkarätige Ransomware-Gruppen wie LockBit und BlackCat (ehemals ALPHV) nutzten Ransomware-as-a-Service(RaaS)-Modelle, um weitreichende Angriffe auszuführen und über kritische Schwachstellen in Systeme einzudringen. Durch RaaS-Modelle steht zuverlässigere Ransomware-Software jetzt auch für kleinere, weniger versierte Gruppen zur Verfügung. Folgende Schwachstellen wurden mit am häufigsten ausgenutzt:

- Schwachstellen im Microsoft Exchange Server, wie ProxyShell und ProxyLogon, die 60 % der im Gesundheitswesen ausgenutzten Sicherheitslücken ausmachten
- Die MOVEit-SQL-Injection-Schwachstelle (CVE-2023-34362), die für zahlreiche Vorfälle verantwortlich war, etwa für den Angriff auf CareSource mit über 3 Millionen betroffenen Patienten



Operative Herausforderungen

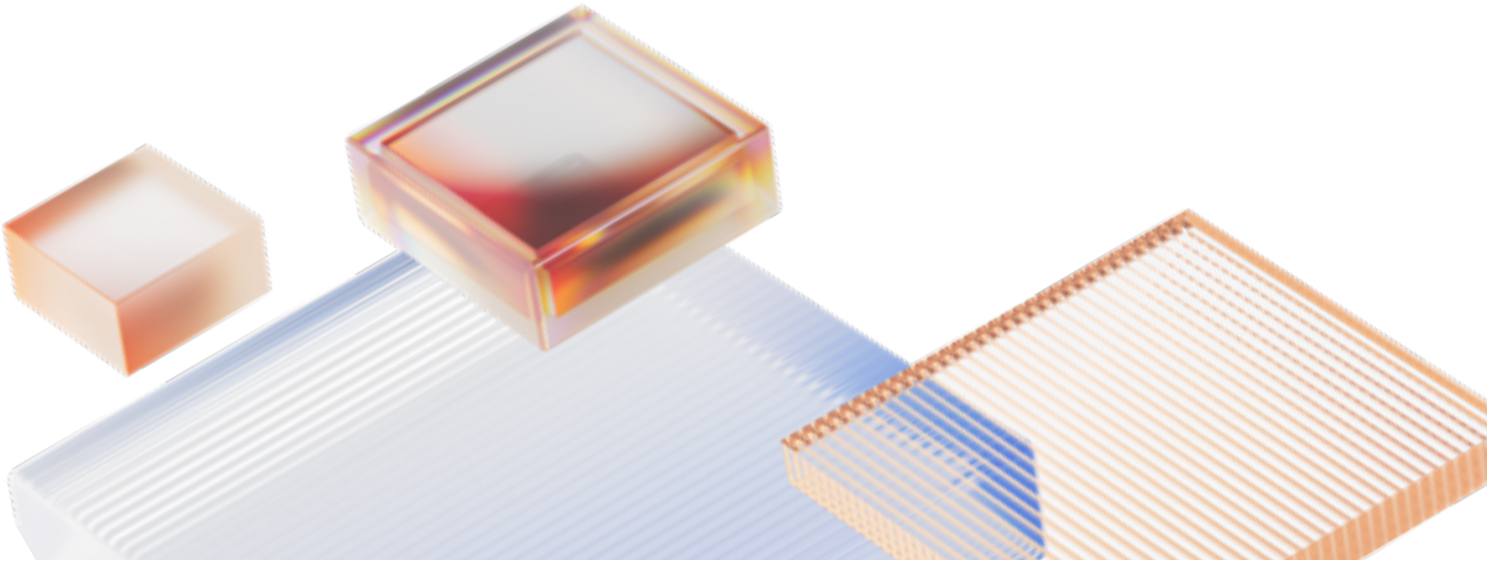
Healthcare-Organisationen waren nicht nur extrem von Ransomware-Angriffen betroffen: Sie waren auch mit am wenigsten auf die Folgen vorbereitet. Die Zeit, die zur Wiederherstellung der normalen Abläufe benötigt wird, spiegelt die zunehmende Komplexität der Ransomware-Vorfälle in allen Bereichen wider. Insbesondere im Gesundheitswesen arbeiten viele Organisationen noch mit veralteten Systemen. Viele von ihnen schieben wichtige Patches viel zu lange auf, was sie besonders anfällig für kritische Schwachstellen macht. All das führt uns eines deutlich vor Augen: Gesundheitsdienstleister sind unzureichend gerüstet – sowohl um ausgeklügelte Bedrohungen abzuwehren als auch um sich von den Folgen zu erholen. Aus diesem Grund steigen die Gesamtkosten eines durchschnittlichen Angriffs auf mehr als das Fünffache der durchschnittlichen Lösegeldzahlung, nämlich auf 4,91 Millionen USD.

DAS SAGT UNSER SOC

Unser Managed-Security-Services(MSS)-Team verzeichnete gegen Ende 2024 bis Anfang 2025 einen 25%igen Anstieg der Ransomware-Vorfälle in einem Zeitraum von 30 Tagen. Die aktivsten Gruppen waren dabei Fog, Akira und SafePay.

DAS SAGEN CYBERVERSICHERER

2024 betrug die durchschnittliche Lösegeldzahlung für Ransomware 850.700 USD – doch diese Zahl erfasst bei Weitem nicht das gesamte Ausmaß des Schadens. Auch die Wiederherstellungskosten sind signifikant gestiegen, sodass die Gesamtkosten eines durchschnittlichen Angriffs mehr als das Fünffache der durchschnittlichen Zahlung erreichen: 4,91 Millionen USD.



Deutlicher Anstieg bei Business-E-Mail-Compromise(BEC)-Angriffen

Im vergangenen Jahr gab es einen gewaltigen Anstieg der Business-E-Mail-Compromise(BEC)-Angriffe, die mittlerweile zu den häufigsten Cyberbedrohungen gehören. BEC-Angriffe setzen in der Regel auf Täuschung und Identitätsbetrug: zwei Methoden, die bei richtiger Ausführung sehr schwer zu erkennen sind. Fast ein Drittel aller gemeldeten Cybervorfälle waren BEC-Angriffe – ein dramatischer Anstieg gegenüber den 9 % im Jahr 2023.

Man-in-the-Middle-Angriffe und Diebstahl von Anmeldedaten: wichtige Elemente von BEC

Man-in-the-Middle(MitM)-Angriffe spielten eine wichtige Rolle bei den BEC-Vorfällen. Dabei nutzten Bedrohungsakteure kompromittierte E-Mail-Adressen (die sie typischerweise durch den Diebstahl von Anmeldedaten abgriffen) oder andere kompromittierte Kommunikationskanäle, um Nachrichten abzufangen oder sogar die interne Kommunikation zu manipulieren. Genau das macht diese Angriffe so hinterhältig und gefährlich: Sie verändern die Wahrnehmung der Wirklichkeit. So glaubt ein Mitarbeiter vielleicht, dass er mit einem Kollegen kommuniziert, während er in Wahrheit unternehmensinterne Informationen an einen Cyberkriminellen weitergibt.

Vendor-E-Mail-Compromise (VEC) auf dem Vormarsch

Laut Abnormal Security stiegen VEC-Angriffe in der ersten Jahreshälfte 2024 um 68 % in der Baubranche und im Maschinenbau sowie um 70 % im Einzelhandel und in der Konsumgüterindustrie. Ein VEC-Angriff ähnelt einem BEC-Angriff sehr: Bei VEC-Attacken geben sich die Angreifer als Anbieter aus oder stehlen deren Zugangsdaten, um die vertrauensvolle Beziehung zwischen dem Anbieter und seinen zahlreichen Kunden auszunutzen und nicht nur ein, sondern gleich mehrere Unternehmen zu bestehlen. Gelingt es einem Angreifer, sich in die Systeme eines Anbieters einzuschleichen, kann er wichtige Informationen wie Zahlungspläne, Identitäten von Entscheidungsträgern, Finanzprozesse und vieles mehr erlangen. Sobald die Angreifer genügend Informationen gesammelt haben, schlagen sie zu. Sie können etwa Rechnungen fälschen, unter einem erfundenen Vorwand Großkunden zu einer dringenden Zahlung bewegen oder die gewonnenen Daten für andere kriminelle Zwecke nutzen.

DAS SAGEN CYBERVERSICHERER

Die BEC-Kosten übersteigen das Budget der CISA. 2024 lag der weltweite Schaden durch BEC-Angriffe bei über 2,95 Milliarden USD. Zum Vergleich: Das sind 150 Mio. USD mehr als das gesamte Budget der Cybersecurity and Infrastructure Security Agency (CISA), das 2024 2,8 Milliarden USD betrug.

DAS SAGT UNSER SOC

Ein branchenführendes Beratungsunternehmen berichtete kürzlich von einem BEC-Angriff auf eine seiner ranghohen Führungskräfte. Das Opfer erhielt eine E-Mail von einem vertrauenswürdigen Account, der jedoch gehackt worden war. Diese Mail enthielt einen OneDrive-Link, der die Person auf eine gefälschte Microsoft-Log-in-Seite weiterleitete, um deren Zugangsdaten zu stehlen. Nach der Kompromittierung gelangte der Angreifer in das E-Mail-Programm dieser Führungskraft und teilte deren Kontaktliste über einen externen Dateifreigabedienst, um seine betrügerischen Aktivitäten auszubauen.

Angreifer schlagen immer schneller zu

Eine Analyse der größten Schwachstellen, die *in the wild* ausgenutzt wurden, zeigt, dass die meisten Angriffe innerhalb von 48 Stunden nach der Bekanntgabe eines Proof of Concept (PoC) starten. Dieser Trend wird von der Threat Analysis Group von Google bestätigt, der zufolge viele Sicherheitslücken nur wenige Tage nach Veröffentlichung ausgenutzt werden.

Die Angriffe zielen regelmäßig auf Schwachstellen in Microsoft Exchange, IoT-Geräten und Drittanbietersoftware wie MOVEit ab. Fortschrittliche Ransomware-as-a-Service(RaaS)-Angebote machen es heute deutlich einfacher, diese Schwachstellen auszunutzen. Gruppen wie LockBit und BlackCat sind bekannt für ihre schnelle Reaktion auf neue Sicherheitslücken.

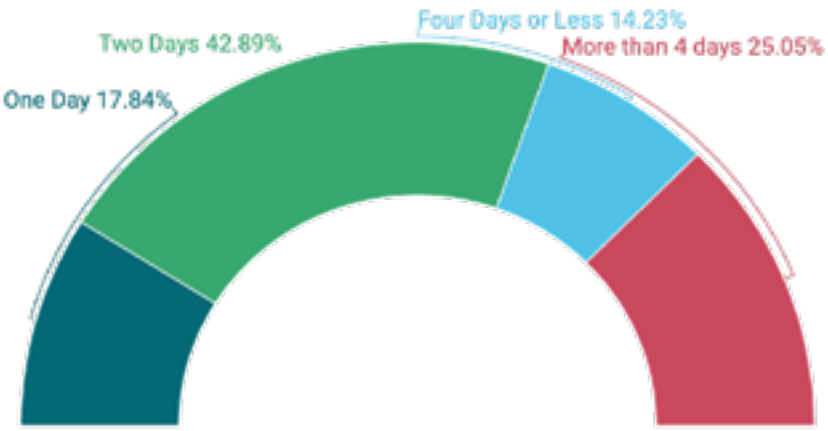
LockBit nutzte beispielsweise CVE-2024-27198 (Umgehung des Authentifizierungsschritts im TeamCity-Tool von JetBrains) in kürzester Zeit aus und startete innerhalb von 24 Stunden nach Bekanntgabe der Schwachstelle einige Ransomware-Angriffe. Ebenso nutzte die Cl0p-Ransomware-Gang eine kritische Schwachstelle in einem anderen Dateitransferdienst, um 66 Unternehmen zu hacken und innerhalb von nur 48 Stunden nach PoC-Veröffentlichung Lösegeldforderungen zu stellen.

„Als MSP erleben wir an vorderster Front, wie schnell sich Cyberbedrohungen entwickeln. Die Geschwindigkeit, mit der Angreifer öffentlich verfügbaren schädlichen Code nutzen – oft innerhalb von ein bis vier Tagen – zeigt, wie dringend proaktive Sicherheitsmaßnahmen sind. Die Zeiten, in denen Schwachstellen erst nach mehreren Wochen gepatcht wurden, sind vorbei. Angreifer haben ihre Reaktionszeiten auf wenige Stunden reduziert. Daher brauchen Unternehmen einen MSP, der proaktiv neue Bedrohungen überwacht, erkennt und abwehrt, bevor es zu kostspieligen Sicherheitsvorfällen kommt."

– SONICWALL-PARTNER FARZAD VAHID, FORNIDA

Zeit, die Angreifer für Exploit brauchen

Wie schnell Hacker Exploit-Code nutzen



Living-off-the-Land-Binaries (LOLBins): ein ernst zu nehmendes Problem

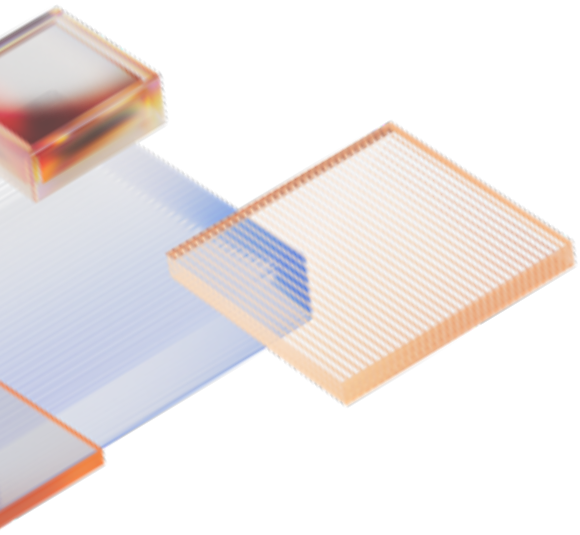
Binärdateien bzw. Binaries sind Programme, die bereits in Ihrem Betriebssystem integriert sind und legitime, nützliche Funktionen erfüllen, um Ihren Computer am Laufen zu halten. Living-off-the-Land-Binaries (LOLBins) steht für eine Methode, diese vorhandenen Programme für schädliche Aktivitäten zu nutzen. Stellen Sie sich vor, Sie möchten zu Hause etwas reparieren. In den meisten Fällen werden Sie Werkzeuge verwenden, die Sie bereits daheim haben, anstatt neue zu kaufen. Cyberkriminelle verfahren bei ihren Angriffen oft nach demselben Schema: Sie nutzen Tools und Programme, die bereits in Ihrem System vorhanden sind, statt eigene Hacking-Software einzusetzen. Wenn ein Angreifer eines dieser scheinbar harmlosen Tools (Binärdateien) für kriminelle Zwecke missbraucht, kann dies die Sicherheitssoftware täuschen, da diese Programme eigentlich tagtäglich auf Ihrem Computer laufen sollten. Das Blockieren oder Deaktivieren dieser Tools würde höchstwahrscheinlich die Funktionalität Ihres Betriebssystems beeinträchtigen.

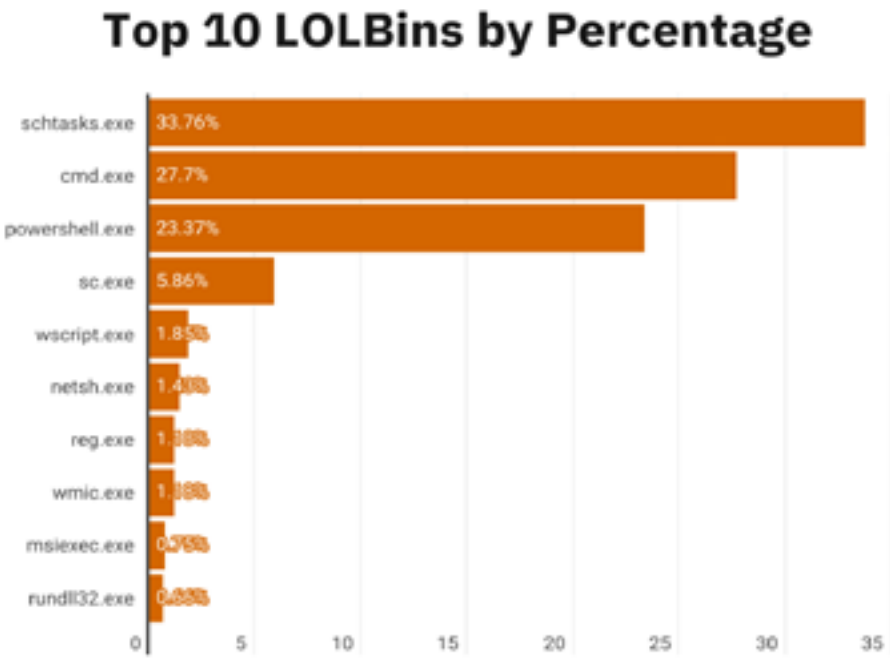
Angreifer nutzen diese Tools für Lateral Movement und die Ausweitung von Berechtigungen innerhalb kompromittierter Netzwerke. So verwenden LockBit und damit verbundene Gruppen laut CISA häufig Tools wie PowerShell und Batch-Scripts, um Umgebungen auszukundschaften, Zugangsdaten in Erfahrung zu bringen und Berechtigungen auszuweiten. Ebenso berichtet Sygnia, dass BlackCat (ALPHV) Beobachtungen zufolge PowerShell-Techniken und Tools wie schtasks nutzte, um sich seitlich im Netzwerk auszubreiten und Windows Defender zu deaktivieren.

Die Nutzung von LOLBins fügt sich in den breiteren Trend ein, vertrauenswürdige Infrastrukturen für bösartige Zwecke auszunutzen – ein Phänomen, das auch bei dateiloser Malware zu beobachten ist, die einen regelrechten Höhenflug erlebt. Die Bedrohungsexperten von SonicWall fanden heraus, dass schtasks.exe, cmd.exe und powershell.exe mit mehr als 80 % aller identifizierten Fälle die am häufigsten ausgenutzten LOLBins ausmachten.

Häufigkeit der ausgenutzten LOLBins

Die Grafik zeigt, wie häufig bestimmte Binärdateien ausgenutzt werden. Schtasks.exe wurde in 34 % der identifizierten LOLBin-Fälle von Angreifern genutzt, um Aufgaben zu Persistenzzwecken oder für die Ausführung bösartiger Scripts zu planen. Cmd.exe machte 28 % der Fälle aus und wurde oft im Rahmen breiter angelegter dateiloser Angriffe für die Ausführung von Befehlen genutzt. Mit einem Anteil von 23 % erwies sich Powershell.exe als äußerst vielseitig und ermöglichte anspruchsvolle Techniken wie Prozessinjektion und Datendiebstahl. Schon das Halbjahres-Update für den SonicWall Threat Report 2024 zeigte, dass 90 % der häufigsten Malware-Familien in irgendeiner Form PowerShell nutzten. Weitere Binärdateien – darunter sc.exe, wscript.exe und netsh.exe – wiesen zwar niedrigere, aber dennoch besorgniserregende Nutzungsraten auf, was auf ihren Einsatz in speziellen oder zielgerichteten Angriffsszenarien hinweist.





Häufige Einsatzszenarien bei Cyberangriffen

LOLBins sind ein fester Bestandteil dateiloser Malware-Kampagnen. Angreifer nutzen hier native Systemtools, um keine herkömmlichen Artefakte zu hinterlassen und so eine Erkennung durch konventionelle signaturbasierte Lösungen zu vermeiden. Hier ein paar Beispiele:

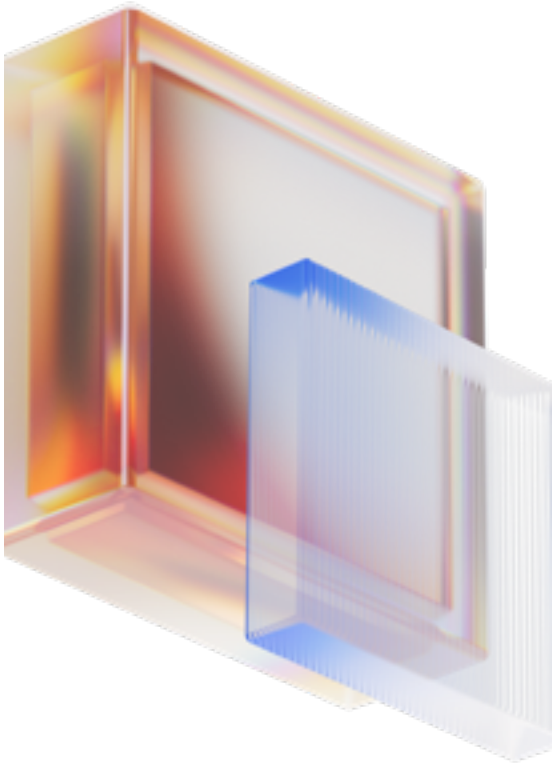
- **wscript.exe**: wird häufig missbraucht, um bösartige Scripts in Phishing-Kampagnen auszuführen, wodurch Angreifer VBScript-Payloads unauffällig starten können
- **cmd.exe**: wird von sehr vielen Bedrohungsakteuren genutzt, um Befehle direkt in gehackten Systemen auszuführen, und dient oft als Einstieg für umfangreichere Command-and-Control-Operationen
- **rundll32.exe**: Dieses Tool gehörte einst zu den am weitesten verbreiteten LOLBins. Obwohl es zunehmend durch effektivere Methoden für dateilose Malware verdrängt wird – die Nutzungsrate liegt nur noch bei 0,66 % –, ist es nach wie vor problemlos in der Lage, bösartige DLLs zu laden und eine Erkennung durch Sandboxen zu umgehen.

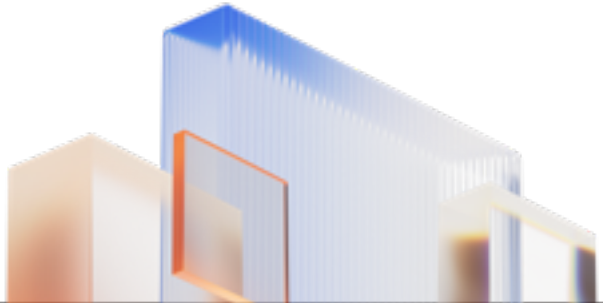
DAS SAGT UNSER SOC

In einer Kindertagesstätte beobachtete unser Managed-Security-Services(MSS)-Team, wie Angreifer einen Check-in-Kiosk als Einfallspforte nutzten. Über diesen Kiosk – ein ungepatchtes Windows-Gerät mit direktem Internetzugang – konnten sie sich mithilfe vorhandener Binärdateien seitlich im Netzwerk ausbreiten. Durch das Einbetten eines versteckten Objekts in den Gruppenrichtlinien-Editor konnten sie schließlich Persistenz herstellen.

DAS SAGT DIE KI

Cyberkriminelle werden mit hoher Wahrscheinlichkeit weiter auf LOLBins setzen, da sie mithilfe vertrauenswürdiger Systemtools wie PowerShell, cmd.exe und schtasks.exe unerkannt ihr Unwesen treiben können. Mit der zunehmenden Verbreitung von dateiloser Malware und Zero-Trust-Modellen werden Angreifer ihre Taktiken weiter verfeinern, um Sicherheitsvorkehrungen zu umgehen. Erweiterte Funktionen für Threat-Hunting und Verhaltensüberwachung sind essenziell, um diesem Trend entgegenzuwirken. – Open AI, 2/5/25, v4.0



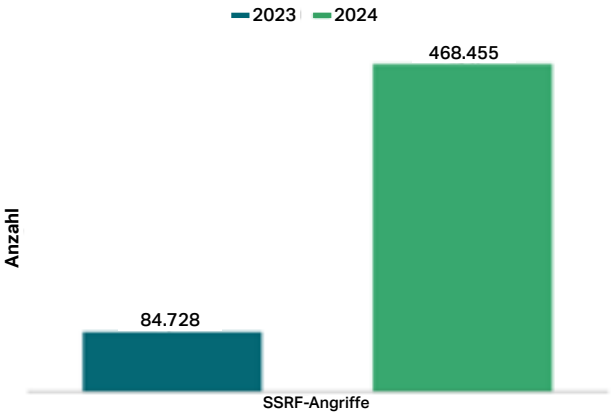


KI-Automatisierungstools senken die Einstiegshürde und erhöhen die Angriffskomplexität

Server-Side-Request-Forgery(SSRF)-Angriffe gehören seit Langem zu den Lieblingswerkzeugen von Cyberkriminellen. Bei dieser Angriffsmethode bringt ein Bedrohungsakteur im Grunde den Server dazu, eine Anfrage an potenziell sensible interne Dienste innerhalb einer Organisation zu stellen. In manchen Fällen können sie sogar den Server dazu zwingen, auf beliebige externe Dienste zuzugreifen. Dies kann dazu führen, dass vertrauliche Daten wie z. B. Anmeldedaten nach außen gelangen. Früher waren für einen SSRF-Angriff umfangreiche Kenntnisse für das Identifizieren von Schwachstellen, für das Erstellen von Payloads sowie im Umgang mit komplexen Serverkonfigurationen erforderlich. Doch mit dem Aufkommen KI-gestützter Tools – insbesondere solcher, die natürliche Sprachverarbeitung (NLP) und generative Modelle nutzen – ist die technische Einstiegshürde erheblich gesunken. Hier ein paar Beispiele, wie KI-Tools solche Angriffe erleichtern:

- **Aufspüren ungepatchter Systeme**: KI-basierte Schwachstellenscanner können veraltete Systeme mit ungepatchten SSRF-Sicherheitslücken selbst in großen, komplexen Infrastrukturen identifizieren.
- **Automatisierung von Exploit-Ketten**: Mithilfe der KI lassen sich SSRF-Angriffe besser mit anderen Schwachstellen verknüpfen und automatisierte Workflows für die Ausweitung von Berechtigungen und Lateral Movement erstellen.
- **Umgehung von Erkennungsmechanismen**: Mittels KI lassen sich Verschleierungstechniken verbessern, sodass es für Sicherheitslösungen schwieriger ist, SSRF-Payloads zu erkennen.

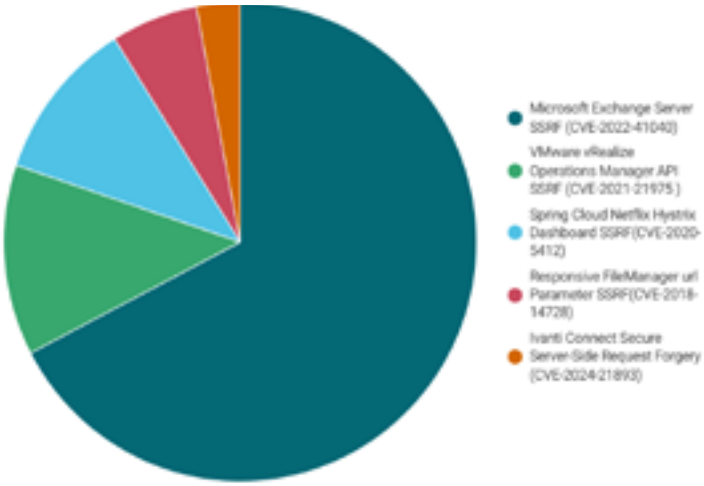
SSRF-Angriffe im Vergleich zum Vorjahr



2024 wurden SSRF-Angriffe zu einem kritischen Problem für die Cybersicherheit, da sie gegenüber 2023 um besorgniserregende 452 % zulegten. Weil SSRF-Angriffe zunehmend mit anderen Methoden wie Privilegienausweitung und Command-Injection-Schwachstellen kombiniert werden, können sie inzwischen einen weitaus höheren Schaden anrichten. Das bietet Bedrohungsakteuren die Möglichkeit, eine breitere Auswahl an Zielsystemen ins Fadenkreuz zu nehmen und tiefer einzudringen.

KI haucht älteren Bedrohungen neues Leben ein

Die 5 größten SSRF-Schwachstellen im Jahr 2024



Einige der am häufigsten ausgenutzten SSRF-Schwachstellen waren keineswegs neu. Cyberkriminelle haben mithilfe von KI-Tools einfach ältere Sicherheitslücken angegriffen, die in vielen Systemen nicht mehr gepatcht werden. Ein paar Beispiele:

- **SSRF-Angriff auf die API des vRealize Operations Manager von VMware (CVE-2021-21975)**: Diese Schwachstelle ermöglicht es Angreifern, über die API des vRealize Operations Manager auf interne Dienste zuzugreifen, was zur Offenlegung sensibler Daten führen kann.
- **SSRF-Angriff auf Microsoft-Exchange-Server (CVE-2022-41040)**: Ein schwerwiegender Fehler erlaubt es Angreifern, Microsoft-Exchange-Server auszunutzen. Dies ermöglicht es, die Authentifizierung zu umgehen und möglicherweise Remote-Code auszuführen.

- **SSRF-Angriff auf das Hystrix-Dashboard von Spring Cloud Netflix (CVE-2020-5412)**: Über eine Schwachstelle im Hystrix-Dashboard verschafften sich Angreifer Zugang zu internen Diensten und veröffentlichten sensible Informationen.

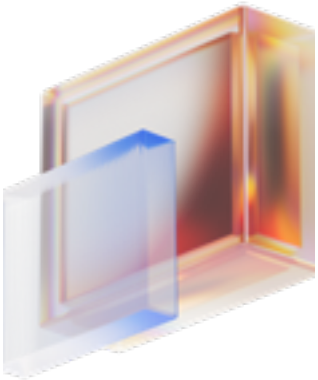
Dass diese älteren SSRF-Schwachstellen immer noch ausgenutzt werden, verdeutlicht, wie hoch die anhaltenden Risiken eines nachlässigen Patch-Managements sind. Vor allem zeigt das Wiederaufleben alter Sicherheitslücken durch KI eines: Organisationen sollten ihr Augenmerk nicht nur auf neue Bedrohungen richten, sondern sich auch weiterhin um diese älteren Schwachstellen kümmern.

Business-E-Mail-Compromise

Vor dem Siegeszug generativer KI benötigten Cyberkriminelle spezielle Fähigkeiten: Zum Beispiel mussten sie den Schreibstil eines Unternehmens nachahmen, hochgradig kontextualisierte Phishingmails erstellen und wissen, wie sie bei der Ausführung ihrer Angriffe herkömmliche Sicherheitssysteme umgehen können, ohne den Alarm auszulösen. KI-Tools können nun all diese Aufgaben auf hohem Niveau übernehmen. Das bedeutet: Theoretisch kann jetzt jeder Bedrohungsakteur, der einen KI-Prompt formulieren kann, einen solchen Angriff durchführen.

Die Rolle generativer KI in der Sicherheit von Open-Source-Software (OSS)

Generative KI bietet den Vorteil, dass sie das Coding beschleunigen und die Zugänglichkeit erhöhen kann. Allerdings kann sie bei unzureichender Validierung Schwachstellen verursachen. Angreifer können dieselben KI-Tools, die zur Beschleunigung des Coding-Prozesses verwendet werden, für bösartige Absichten nutzen, etwa um Schwachstellen in Unternehmenssystemen zu identifizieren und auszunutzen. Aus diesem Grund sind sogar noch strengere Prozesse für die Prüfung und Validierung von Code gefragt.

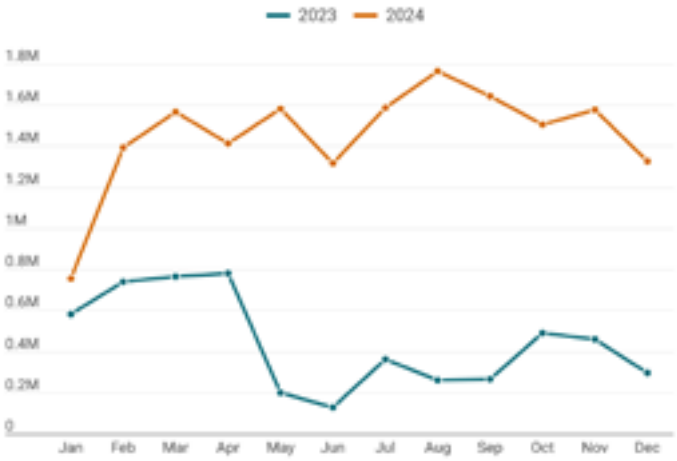


„Wir beobachten ständig, wie KI die Cyberbedrohungslandschaft umkrempelt und es für Angreifer einfacher macht, ältere Schwachstellen auszunutzen, ausgeklügelte Angriffe zu automatisieren und herkömmliche Abwehrmaßnahmen zu umgehen. Der rasante Anstieg KI-gestützter SSRF- und BEC-Angriffe zeigt, dass Unternehmen sich keine reaktiven Sicherheitsstrategien mehr leisten können. Organisationen brauchen einen proaktiven Sicherheitspartner, der Bedrohungen in Echtzeit erkennt und abwehrt, einen solideren Schutz vor KI-gestützten Angriffen bietet und die Einhaltung veränderter Sicherheitsvorgaben gewährleistet, um neuen Risiken stets einen Schritt voraus zu sein."

– SONICWALL-PARTNER LUIS ALVAREZ, PRESIDENT & CEO, ALVAREZ TECHNOLOGIES

Das Internet of Things (IoT) breitet sich immer weiter aus – und mit ihm die Bedrohungen

Cyberkriminelle richteten ihre IoT-Angriffe zunehmend auf IP-Kameras. Allein 2024 verhinderte SonicWall mehr als 17 Millionen Angriffe auf IP-Kameras, wobei die monatlichen Angriffszahlen zwischen 750.000 und 1,8 Millionen schwankten. Kriminelle nutzen zunehmend die oft schwachen Sicherheitsvorkehrungen vernetzter Geräte aus – insbesondere jener, die in staatlichen Einrichtungen und kritischen Infrastrukturen eingesetzt werden. Diese Geräte sind anfällig für störende Aktivitäten wie die Manipulation von Überwachungssystemen und Distributed-Denial-of-Service(DDoS)-Angriffe. IP-Kameras sind häufig in sensiblen Bereichen wie staatlichen Einrichtungen und sogar Wahllokalen zu finden, was darauf hindeutet, dass der Anstieg zumindest teilweise auf die weltweit in 2024 erfolgten Wahlen zurückzuführen ist. Eine der alarmierendsten IoT-Bedrohungen ist die Command-Injection-Schwachstelle von Hikvision-IP-Kameras (CVE-2021-36260), die es Angreifern ermöglicht, Befehle direkt im Kamerasystem einzugeben und so die vollständige Kontrolle über das Gerät zu übernehmen.



IoT-Botnet

Der IoT-Botnet Reaper nutzt Sicherheitslücken in IoT-Geräten aus, um die volle Kontrolle zu übernehmen und dann groß angelegte Angriffe zu starten. Während andere Botnets auf Mängel wie schlechte Passwörter angewiesen sind, nutzt Reaper gezielt Schwachstellen aus, wodurch das Bedrohungslevel für IoT-Hardware steigt.

Diese Trends markieren den Wechsel von opportunistischen Angriffen zu einem zielgerichteten Vorgehen, das darauf ausgelegt ist, Überwachungsmechanismen zu überlisten, kritische Dienste zu stören oder Spionage zu ermöglichen.

Open-Source-Software (OSS)

Open-Source-Software (OSS) hat die Softwareentwicklung revolutioniert und besonders für IoT-Geräte einen hohen Grad an Innovation und Kosteneffizienz ermöglicht. Sie hat allerdings einen großen Nachteil: Wenn Tausende IoT-Geräte alle dieselbe OSS nutzen, kann eine einzige Schwachstelle verheerende Folgen haben. Laut unseren Recherchen gibt es drei OSS-Projekte, die häufiger als andere ausgenutzt werden. Alle drei kommen auch in IoT-Geräten zum Einsatz.

- **PHP**: Schwachstellen wie CVE-2017-9841, CVE-2018-20062 und CVE-2024-4577 ermöglichen die Ausführung von beliebigem Code und bergen somit erhebliche Risiken.
- **Apache**: Bekannte Schwachstellen wie Log4j CVE-2021-44228 erleichtern die Remote-Ausführung von Code und begünstigen Datenlecks.
- **OpenSSL**: Bugs wie Heartbleed (CVE-2014-0160) ermöglichen die Offenlegung sensibler Daten, weshalb sie nach wie vor gerne von Hackern ausgenutzt werden.

DAS SAGT DIE KI

IoT-Angriffe werden weiter zunehmen, da mehr und mehr vernetzte Geräte mit schwacher Sicherheit in kritischen Bereichen zum Einsatz kommen. Immer mehr Bedrohungsakteure ersetzen opportunistische Exploits zugunsten zielgerichteter Angriffe. Dabei nutzen sie Botnets wie Reaper und Schwachstellen in IP-Kameras und OSS-Komponenten. Ohne stärkere Sicherheitsframeworks, Patch-Management und Bedrohungsüberwachung werden IoT-Geräte die primären Ziele von Cyberkriminellen bleiben. – OpenAI, 2/5/24, v4

Zunehmende Vielfalt bei Angriffstypen: Cyberkriminelle werden kreativ

Cyberangriffe werden immer vielfältiger, da Cyberkriminelle neue Taktiken entwickeln und bewährte Strategien verfeinern, um Schwachstellen auszunutzen. Die Kosten eines Cyberangriffs steigen – und sie sind nicht nur finanzieller Natur. Ein Cyberangriff kann langfristige Reputationsschäden verursachen und langfristige Folgen haben.

Strela-Stealer-Strategien nehmen parallel zu anderer Malware zu

Erstmals im November 2022 entdeckt, hat sich Strela Stealer inzwischen zu den hartnäckigsten und gefährlichsten Bedrohungen in Europa entwickelt. SonicWall Capture Labs verzeichnete im Jahr 2024 durchgehend Aktivitäten, wobei folgende Monate besonders hervortraten:

- **Juli und Dezember**: Grund für den Anstieg waren hier möglicherweise die Urlaubs- und Ferienzeiten, in denen generell weniger Mitarbeiter im Büro sind und weniger Ressourcen zur Verfügung stehen.
- **Oktober**: In diesem Monat startet in vielen Unternehmen das Finanzreporting. Weil dadurch mehr sensible Informationen ausgetauscht werden, ist dies ein idealer Zeitpunkt für Angreifer.

Anfangs übertrugen Bedrohungsakteure Strela Stealer über JavaScript-Dateien in E-Mail-Anhängen, um E-Mail-Zugangsdaten von Plattformen wie Microsoft Outlook und Mozilla Thunderbird zu erlangen. Im Jahr 2024 wurde die Malware durch den Einsatz besserer Verschleierungstechniken weiter verfeinert, wobei sie bestimmte Regionen ins Visier nimmt. Während Russland verschont bleibt, stehen – vermutlich aus geopolitischen Gründen – Länder wie Deutschland, Spanien, Polen und Italien weit oben auf der Angriffsliste. Strela Stealer nutzt verschiedene Methoden, um unerkannt zu bleiben. Unter anderen prüft die Malware die Spracheinstellungen und die Tastaturbelegung des Systems, um festzustellen, ob sich das Gerät in einem Zielgebiet befindet. Dies zeigt, dass Cyberkriminelle nicht nur ihre Tools verbessern, sondern auch strategischer vorgehen.

„Cyberkriminelle gehen immer strategischer vor. Sie kombinieren neue Angriffsmethoden mit bewährten Taktiken, um Schwachstellen gezielt auszunutzen. Die Kosten von Cyberangriffen sind nicht nur finanzieller Natur: Sie können das Image eines Unternehmens dauerhaft schädigen und den Geschäftsbetrieb lahmlegen. Unternehmen brauchen einen Sicherheitspartner, der neuen Bedrohungen immer einen Schritt voraus ist und durch proaktiven Schutz, Echtzeitüberwachung und strategische Abwehrmaßnahmen ihre wertvollsten Ressourcen schützt."

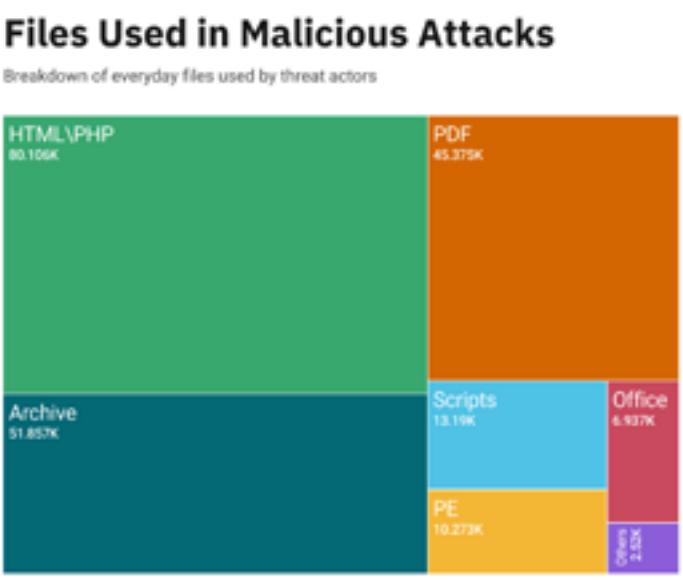
– SONICWALL-PARTNER JOSH SKEENS, CEO, LOGICALLY

DAS SAGT DIE KI

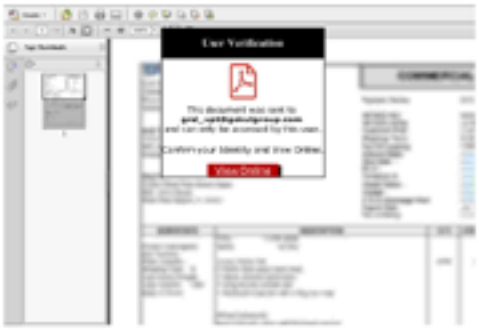
2024 stiegen die durchschnittlichen Kosten eines Sicherheitsvorfalls weltweit auf 4,88 Millionen USD – ein Anstieg von 10 % im Vergleich zum Vorjahr und die höchste jährliche Steigerung seit der Pandemie.
– OpenAI, 1/29/25, v4.0

Die versteckten Risiken im Alltag: PDFs, HTML-Phishing und gefälschte mobile Apps

Dateibasierte Angriffe haben deutlich zugenommen, allen voran schädliche PDFs und HTML-Phishing-Dateien. Laut den von SonicWall erhobenen Daten waren 38 % der identifizierten bösartigen Dateien HTML-basiert, dicht gefolgt von PDFs mit 22 %.



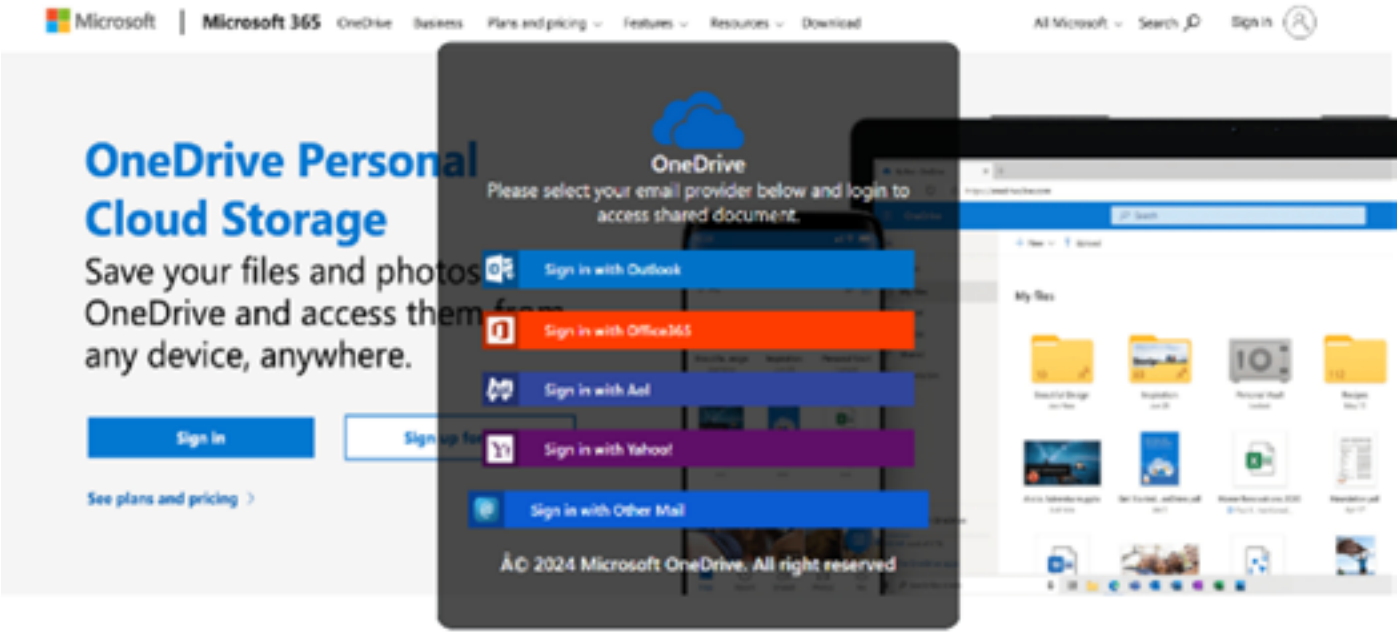
Angreifer nutzen diese Dateitypen, weil sie Sicherheitsmechanismen leicht umgehen und sich den Faktor Mensch zunutze machen können, um sensible Informationen wie Zugangsdaten zu stehlen. Bedrohungsakteure leiten Opfer über QR-Codes, die in bösartigen PDFs eingebettet sind, zu Phishing-Seiten weiter. Sobald das Opfer den QR-Code scannt, gelangt es auf eine scheinbar legitime Log-in-Seite. In Wahrheit werden die eingegebenen Informationen an die Angreifer übermittelt und für ihre kriminellen Zwecke verwendet. Dieser Angriff ist oft nur der erste Schritt. Sobald die Angreifer Zugriff auf die gestohlenen Zugangsdaten haben, setzen sie in der Regel weitere Taktiken wie BEC, Wirtschaftsspionage und Datendiebstahl ein.



HTML-Phishing-Angriffe nahmen um 10 % zu und entwickelten sich somit zu einer der beliebtesten Methoden zur Kompromittierung von Anmeldedaten. Hier einige der Techniken, die Hacker für HTML-Phishing nutzen:

- **Formularbasiertes Phishing**: HTML-Phishing-Seiten füllen oft die E-Mail-Adresse des Opfers automatisch aus, um authentisch zu wirken und den Benutzer zur Eingabe seines Passworts zu verleiten.
- **Übermittlung von Code über Archive**: HTML-Dateien werden häufig in ZIP- oder RAR-Archiven übermittelt, um Sicherheitsvorkehrungen zu umgehen und die Neugier der Benutzer zu wecken.

Hier ein paar Beispiele aus der Praxis:



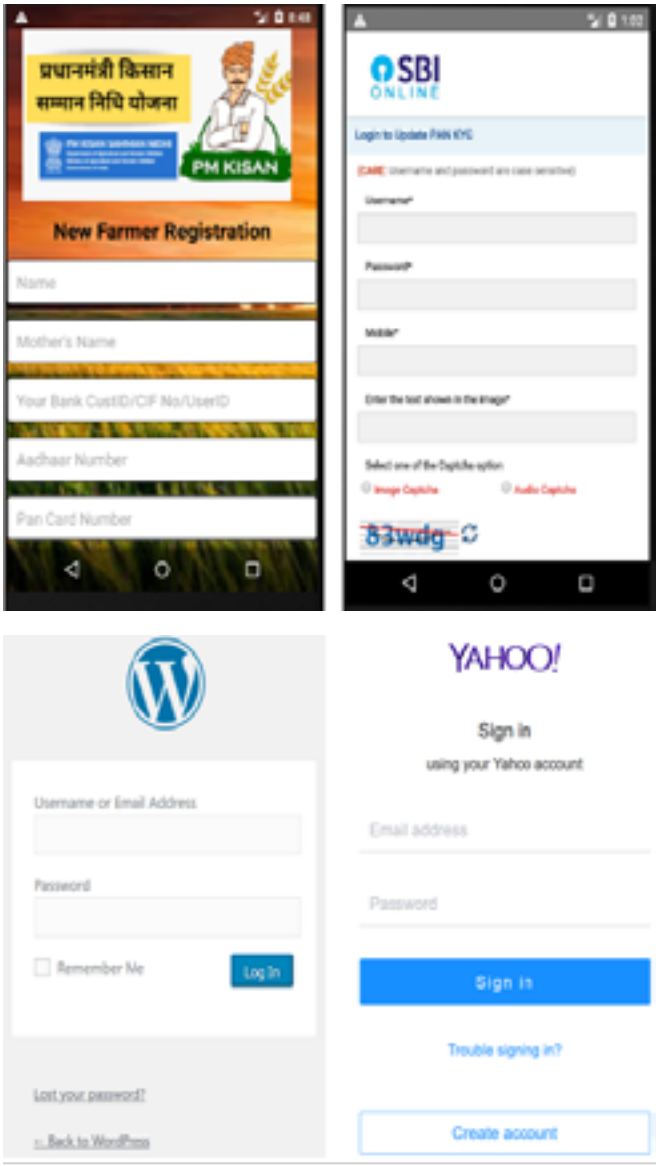
Gewöhnliche Dateien, ungewöhnliche Bedrohungen

ZIP- und RAR-Dateien mit schädlichen Payloads sind mittlerweile auch eine gängige Methode, um E-Mail-Filter zu umgehen. Hierbei werden Ransomware, Trojaner oder Remote-Access-Tools (RATs) an ahnungslose Opfer übertragen. Solche Methoden wurden in jüngster Zeit bei einigen der größten Angriffe eingesetzt, etwa beim Bumblebee-Malware-Loader. Dieser verschickte Phishingmails mit ZIP-Archiven, die bösartige LNK-Dateien enthielten, um nicht erkannt zu werden.

Die zunehmende Nutzung von HTML-, PDF- und anderen dateibasierten Angriffen ist ein ausgezeichnetes Beispiel für die wachsende Vielfalt und – man muss es so sagen – Kreativität, die Hacker bei der Entwicklung dieser neuen Angriffsmethoden an den Tag legen. Die Attacken richten sich an verschiedene Branchen und Unternehmen jeder Größe. Schädliche Payloads in scheinbar gewöhnlichen oder häufig genutzten Dateien zu verpacken, macht es wesentlich schwieriger für herkömmliche Sicherheitsmethoden, diese Angriffe aufzuspüren, bevor sie Schaden anrichten können.

Gefälschte Android-Apps: wie Hacker Vertrauen und Berechtigungen für mobilen Betrug ausnutzen

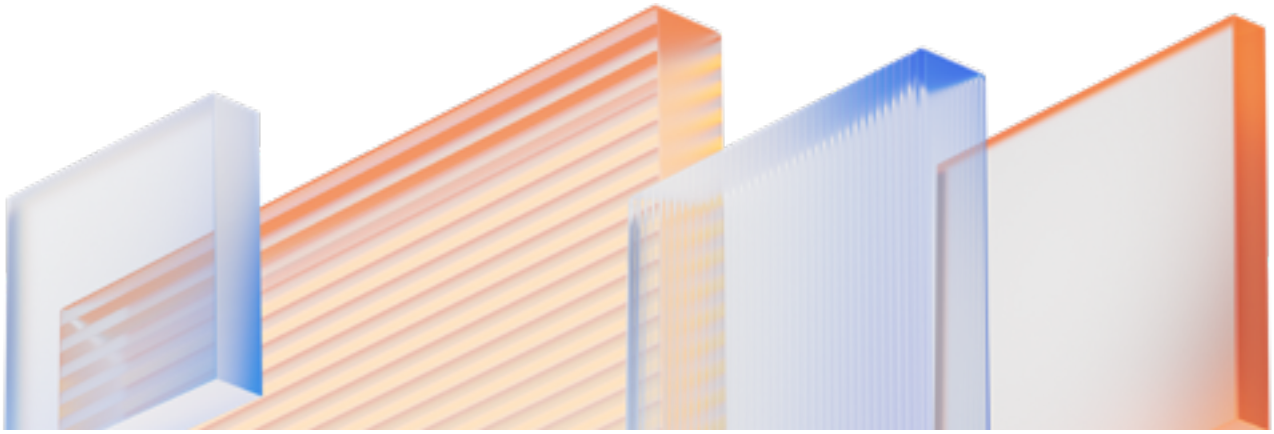
Gefakte Android-Apps haben sich zu einer weiteren ernst zu nehmenden Cyberbedrohung entwickelt, allen voran in der Region Asien-Pazifik (APAC), wo die Fälle von mobilem Betrug insgesamt stark angestiegen sind. Bedrohungsakteure in dieser Region nutzen die hohe Verbreitung von Android-Smartphones aus und machen sich den Umstand zunutze, dass generell ein tief verwurzeltes, kulturbedingtes Vertrauen in Autoritätspersonen besteht. Diese Apps fordern Berechtigungen vom Gerät an, die für ihre Funktion nicht wirklich erforderlich sind, wie etwa das Empfangen und Lesen von Textnachrichten. Dadurch können Angreifer Einmalpasswörter (OTPs) abfangen und Benutzerkonten kapern. Häufig geben sich die Apps als legitime Finanz- oder Regierungsdienste aus. Berücksichtigt man die Tatsache, dass sie oft auf Opfer mit geringerer digitaler Kompetenz abzielen, wird deutlich, warum es Angreifern so leicht gelingt, ihnen sensible Informationen zu entlocken.



Herausforderungen für eine effektive Sicherheitsstrategie

Es ist extrem wichtig, dass Security-Partner, MSPs und MSSPs die Herausforderungen bei der Umsetzung guter Cybersicherheitspraktiken verstehen. Fakt ist: Die sich ständig wandelnde Bedrohungslandschaft erfordert einen proaktiven, mehrschichtigen Cybersecurity-Ansatz. Gefragt sind hier vor allem Echtzeitüberwachung, eine schnelle Implementierung von Patches, Zero-Trust-Sicherheitsmodelle und eine kontinuierliche Sensibilisierung und Schulung von Nutzern. Wenn wir alle an einem Strang ziehen, können wir diese Herausforderungen überwinden und so ein sichereres Umfeld für alle schaffen.

1. **Schnelle Ausnutzung von Schwachstellen**: Nie zuvor haben sich Angreifer Sicherheitslücken so schnell zunutze gemacht wie jetzt. Nach Veröffentlichung einer Demo mit entsprechender Anleitung brauchten Hacker in 75 % der Fälle lediglich vier Tage oder weniger, um Schwachstellen auszunutzen. Diese atemberaubende Geschwindigkeit setzt Sicherheitsteams enorm unter Druck, Schwachstellen zügig zu identifizieren und zu beheben.
2. **Steigende Kosten im Zusammenhang mit Ransomware und Wiederherstellung**: Ransomware-Angriffe bleiben eine der verheerendsten Cyberbedrohungen. So waren allein im US-Gesundheitssektor über 198 Millionen Menschen von Sicherheitsverletzungen betroffen. Die Wiederherstellungskosten pro Vorfall lagen bei mehr als 4,91 Millionen USD – ein deutliches Warnsignal, wie gefährlich fehlende Back-up-Lösungen und Wiederherstellungspläne sein können.
3. **Menschliches Versagen**: Individuelle Fehler einzelner Personen wirken sich erheblich auf das gesamte Cybersecurity-Konzept aus. Diese Fehltritte können das Risiko von Datenpannen oder unbefugtem Zugriff unabsichtlich erhöhen.
4. **Deutlicher Anstieg bei Business-E-Mail-Compromise(BEC)-Angriffen**: BEC-Angriffe haben deutlich zugenommen und machen inzwischen ein Drittel aller gemeldeten Cyberversicherungsansprüche aus. Weil Angreifer ausgeklügelte KI-gestützte Techniken nutzen, ist diese Betrugsmasche schwerer zu erkennen.
5. **Erweiterte Angriffsfläche durch IoT-Geräte**: Mit der steigenden Zahl internetfähiger Geräte entstehen neue Sicherheitsherausforderungen, da Angreifer schwache Konfigurationen dieser Geräte gezielt ausnutzen.
6. **Zunehmende Komplexität KI-gestützter Cyberangriffe**: Cyberkriminelle setzen für ihre Angriffe zunehmend auf KI, sodass KI-gestützte Bedrohungen wie Server-Side-Request-Forgery(SSRF)-Attacken deutlich gestiegen sind.
7. **Dateibasierte Angriffsmethoden und automatisierte Bedrohungen**: Phishing-Angriffe, insbesondere auf Basis schädlicher PDF- und HTML-Dateien, sind auf dem Vormarsch. Oft enthalten diese trügerische Links und QR-Codes, was die Erkennung erheblich erschwert.



Strategische Maßnahmen zur Stärkung Ihrer Cybersicherheit

Die Bedrohungslandschaft verändert sich so rasant wie nie zuvor, und kein Unternehmen ist davor gefeit. Die gute Nachricht ist, dass sich viele der in diesem Report beschriebenen Angriffe mit einem guten Cybersicherheitskonzept verhindern lassen. Mit proaktiven Maßnahmen können Sie Ihre Sicherheitsstrategie erheblich stärken. Hier ein paar Beispiele:

Implementieren Sie ein echtzeitbasiertes Patch-Management – ein schlechtes Patch-Management macht Organisationen besonders anfällig für Cyberangriffe. Durch kontinuierliche Überprüfungen und zeitnahes Patching können Ransomware-Infektionen, Sicherheitsvorfälle und Systemkompromittierungen verhindert werden, bevor Angreifer bekannte Schwachstellen ausnutzen können.

Wählen Sie ein Zero-Trust-Sicherheitsmodell – Hacker nutzen KI und Automatisierung, um in Netzwerke einzudringen. Sicherheitsteams müssen strenge Zugriffskontrollen durchsetzen, dürfen niemals implizit vertrauen und sollten jede Zugriffsanfrage prüfen.

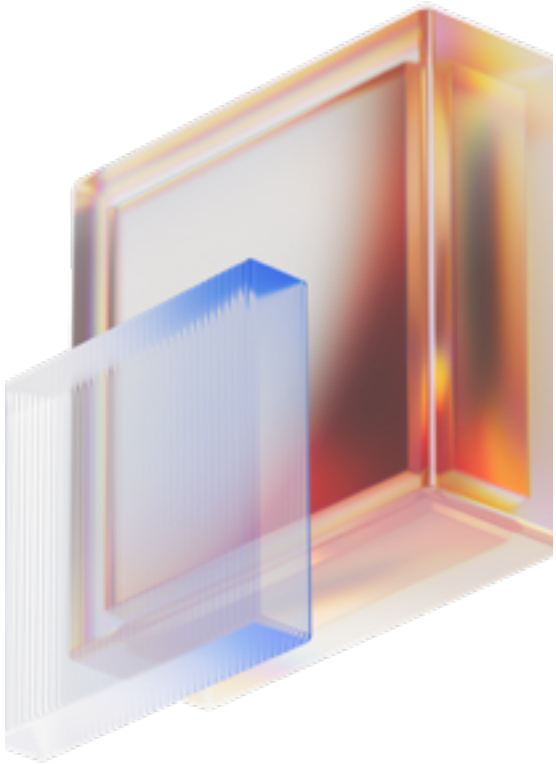
Setzen Sie auf 24/7-SOC-Services für einen Bedrohungsschutz in Echtzeit – MSPs/MSSPs sollten mit Sicherheitsanbietern zusammenarbeiten, die SOC-Services und 24/7/365-Monitoring bieten, da Cyberangriffe sich rasant entwickeln und Angreifer Schwachstellen innerhalb weniger Stunden nach Bekanntwerden ausnutzen. Eine kontinuierliche Überwachung ermöglicht es, Bedrohungen in Echtzeit zu erkennen, schnell auf Vorfälle zu reagieren und Ausfallzeiten zu minimieren – und so Kunden vor kostspieligen Sicherheitsvorfällen und Betriebsunterbrechungen zu schützen.

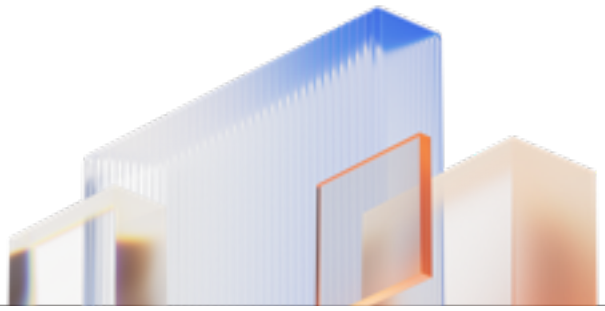
Bereiten Sie Ihre Kunden besser auf Ransomware vor – Organisationen müssen auf katastrophale Ransomware-Vorfälle vorbereitet sein. Daher sollten sie Lösungen für regelmäßige Back-ups, Netzwerksegmentierung und Endpoint Detection and Response (EDR) implementieren.

Stärken Sie die IoT-Sicherheit – IoT-Angriffe nahmen 2024 um ganze 124 % zu. Vermeiden Sie einfache Passwörter, führen Sie Firmware-Updates durch und schränken Sie den Netzwerkzugriff ein, um IoT-Geräte zu schützen.

Überwachen Sie Cloud-Umgebungen und SaaS-Anwendungen – 78 % der Sicherheitsmeldungen waren auf cloudbasierte Bedrohungen zurückzuführen. Setzen Sie auf Multi-Faktor-Authentifizierung (MFA), CASB-Lösungen und Least-Privilege-Zugriffsregeln.

Führen Sie regelmäßige Cybersecurity-Sensibilisierungstrainings durch – menschliches Versagen ist und bleibt ein wesentlicher Risikofaktor. Durch regelmäßige Schulungen zu den Themen Phishing, Social Engineering und Passworthygiene lässt sich das Risiko erheblich verringern.





Die wichtigsten Punkte

Das sagt unser SOC

- Ransomware-Angriffe stiegen Ende 2024 um ganze 25 %, insbesondere aufgrund aggressiver Aktivitäten der Gruppen Fog, Akira und SafePay.
- Ein führendes Beratungsunternehmen wurde Opfer eines BEC-Angriffs, bei dem ein gehackter vertrauenswürdiger Account einer Führungskraft Anmeldedaten entlockte. Daraufhin verbreitete der Angreifer seine betrügerischen Aktivitäten über die Kontaktliste dieser Führungskraft.
- Cyberkriminelle hackten einen ungepatchten, mit dem Internet verbundenen Check-in-Kiosk in einer Kindertagesstätte, um sich im Netzwerk auszubreiten und über den Gruppenrichtlinien-Editor Persistenz herzustellen.

Das sagt die KI

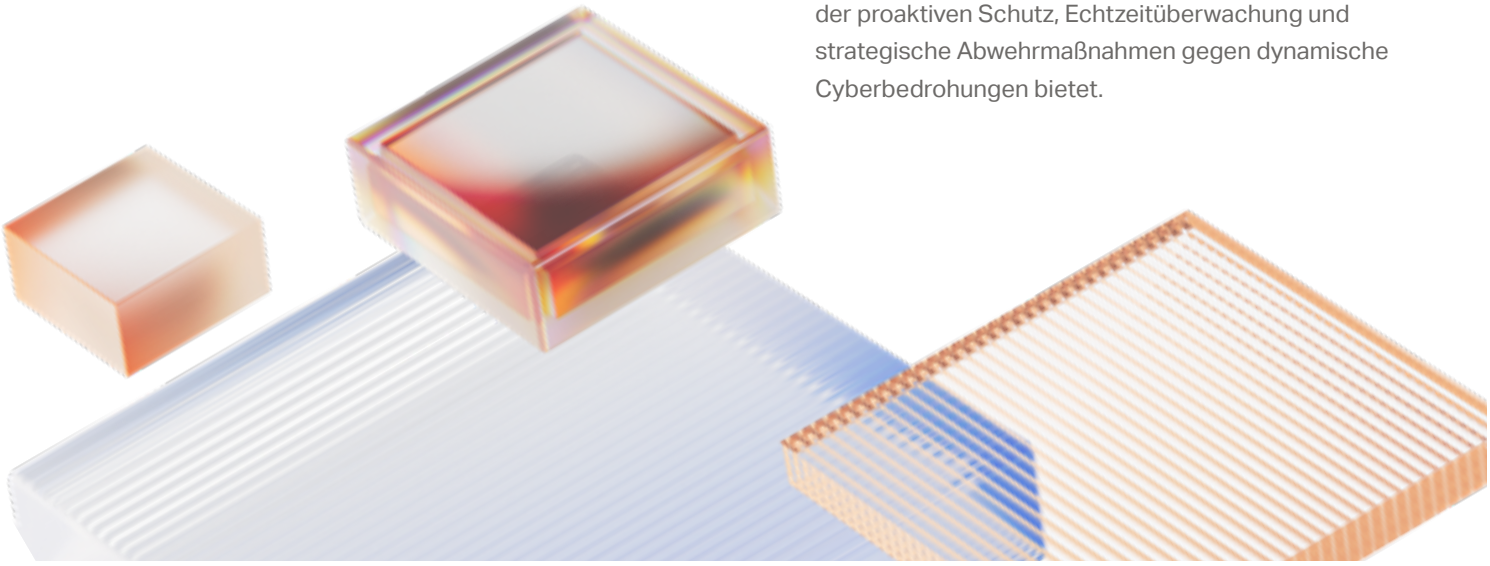
- Angreifer missbrauchen zunehmend vertrauenswürdige Systemtools wie PowerShell und cmd.exe, um unerkannt zu bleiben. Erweiterte Funktionen für Threat-Hunting und Verhaltensüberwachung sind essenziell, um dem LOLBin-Trend entgegenzuwirken.
- IoT-Geräte mit schwacher Sicherheit überfluten gerade kritische Sektoren. Die Zahl gezielter Angriffe mittels Botnets wie Reaper wird stark ansteigen, was den dringenden Bedarf an stärkeren Sicherheitsframeworks und proaktivem Monitoring unterstreicht.
- 2024 stiegen die durchschnittlichen Kosten eines Sicherheitsvorfalls weltweit auf 4,88 Millionen USD – die höchste jährliche Steigerung seit der Pandemie.

Das sagen Cyberversicherer

- Die Gesamtkosten eines Ransomware-Angriffs lagen im Schnitt bei 4,91 Millionen USD – fünfmal mehr als die durchschnittliche Lösegeldzahlung in Höhe von 850.700 USD. Grund sind die deutlich gestiegenen Kosten für die Wiederherstellung.
- Der weltweite Schaden durch BEC-Angriffe lag bei über 2,95 Milliarden USD – und übertraf somit das Jahresbudget der CISA in Höhe von 2,8 Milliarden USD um 150 Millionen USD.

Das sagen unsere Partner

- Da Cyberkriminelle Schwachstellen innerhalb weniger Tage ins Fadenkreuz nehmen, brauchen Unternehmen einen MSP, der proaktiv Bedrohungen überwacht, erkennt und abwehrt, bevor es zu kostspieligen Sicherheitsvorfällen kommt.
- KI-gestützte Angriffe wie SSRF und BEC nehmen rasant zu. Um neuen Risiken einen Schritt voraus zu sein, ist eine proaktive Erkennung und Abwehr von Bedrohungen in Echtzeit gefragt.
- Unternehmen brauchen einen Sicherheitspartner, der proaktiven Schutz, Echtzeitüberwachung und strategische Abwehrmaßnahmen gegen dynamische Cyberbedrohungen bietet.



SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, Kalifornien 95035, USA

www.sonicwall.com

© 2025 SonicWall Inc.

SonicWall ist eine Marke oder eingetragene Marke von SonicWall Inc. und/oder deren Tochtergesellschaften in den USA und/oder anderen Ländern. Alle anderen Marken und eingetragenen Marken sind Eigentum der jeweiligen Inhaber. Die Informationen in diesem Dokument werden in Verbindung mit den Produkten von SonicWall Inc. und/oder deren Tochtergesellschaften bereitgestellt. Sie erhalten durch dieses Dokument oder in Verbindung mit dem Verkauf von SonicWall-Produkten keine Lizenz (weder ausdrücklich noch stillschweigend, durch Rechtsverwirkung oder anderweitig) für geistige Eigentumsrechte.

SONICWALL UND/ODER TOCHTERGESELLSCHAFTEN VON SONICWALL ÜBERNEHMEN KEINE HAFTUNG UND KEINERLEI AUSDRÜCKLICHE, STILLSCHWEIGENDE ODER GESETZLICHE GEWÄHRLEISTUNG FÜR DIE ANGEBOTENEN PRODUKTE, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG FÜR DIE HANDELSÜBLICHKEIT, DIE VERWENDUNGSFÄHIGKEIT FÜR EINEN BESTIMMTEN ZWECK UND DIE NICHTVERLETZUNG VON RECHTEN DRITTER, SOWEIT SIE NICHT IN DEN BESTIMMUNGEN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT NIEDERGELEGT SIND. IN KEINEM FALL HAFTEN SONICWALL UND/ODER SEINE TOCHTERGESELLSCHAFTEN FÜR DIREKTE UND INDIREKTE SCHÄDEN, FOLGESCHÄDEN, STRAFSCHADENSERSATZ, BESONDERE SCHÄDEN ODER BEILÄUFIG ENTSTANDENE SCHÄDEN (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SCHÄDEN FÜR GEWINNVERLUSTE, GESCHÄFTSUNTERBRECHUNGEN ODER INFORMATIONSVERLUSTE), DIE SICH AUS DER VERWENDUNG ODER DER UNMÖGLICHKEIT DER VERWENDUNG DIESES DOKUMENTES ERGEBEN, SELBST WENN SONICWALL UND/ODER SEINE TOCHTERGESELLSCHAFTEN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDEN.

SonicWall und/oder dessen Tochtergesellschaften übernehmen keine Gewährleistungen in Bezug auf die Genauigkeit oder Vollständigkeit dieses Dokuments und behalten sich das Recht vor, Spezifikationen und Produktbeschreibungen jederzeit ohne Vorankündigung zu ändern. SonicWall Inc. und/oder Tochtergesellschaften von SonicWall Inc. übernehmen keinerlei Verpflichtung, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

Als Best Practice optimiert SonicWall regelmäßig seine Methoden zur Datenerfassung, Analyse und Berichterstattung. Dazu gehören Verbesserungen der Datenbereinigung, Änderungen an Datenquellen und die Konsolidierung von Bedrohungsfeeds. In früheren Berichten veröffentlichte Zahlen wurden möglicherweise für verschiedene Zeiträume, Regionen oder Branchen angepasst.

Die in diesem Dokument enthaltenen Materialien und Informationen, einschließlich, aber nicht beschränkt auf Texte, Grafiken, Fotografien, Illustrationen, Symbole, Bilder, Logos, Downloads, Daten und Datensammlungen, gehören SonicWall oder dem ursprünglichen Ersteller und sind durch geltende Gesetze geschützt, einschließlich, aber nicht beschränkt auf US-spezifische und internationale Urheberrechte und Vorschriften.

Wir könnten den SonicWall Threat Report nicht ohne den unermüdlichen Einsatz des Capture-Labs-Teams realisieren.

Über SonicWall

Mit über 30 Jahren Erfahrung gilt der Cybersecurity-Pionier SonicWall als ein führendes Partner-first-Unternehmen auf dem Markt. SonicWall setzt auf eine echtzeitbasierte Erstellung, Skalierung und Verwaltung von Sicherheitssystemen über cloudbasierte, hybride und traditionelle Umgebungen hinweg. Zunehmend mobil und cloudbasiert arbeitende Nutzer profitieren so von einem nahtlosen Schutz vor schwer zu fassenden Cyberbedrohungen, die Netzwerke über zahllose Angriffspunkte befallen. Mit seinem eigenen Threat-Research-Center kann SonicWall sämtlichen Organisationen weltweit – ob großen Unternehmen, Behörden oder KMUs – schnell und kostengünstig maßgeschneiderte Sicherheitslösungen zur Verfügung stellen. Besuchen Sie uns unter www.sonicwall.de oder folgen Sie uns auf Twitter, LinkedIn, Facebook und Instagram, wenn Sie weitere Informationen wünschen.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA

Als Best Practice optimiert SonicWall regelmäßig seine Methoden zur Datenerfassung, Analyse und Berichterstattung. Dazu gehören Verbesserungen der Datenbereinigung, Änderungen an Datenquellen und die Konsolidierung von Bedrohungsfeeds. In früheren Berichten veröffentlichte Zahlen wurden möglicherweise für verschiedene Zeiträume, Regionen oder Branchen angepasst.