SONICWALL

2024 Halbjahres-Update für den Cyber Threat Report

RELEVANTE INFORMATIONEN ZU DEN VERÄNDERTEN BEDROHUNGEN

EINLEITUNG

NACHRICHT VOM CEO

In dieser dynamischen Bedrohungslandschaft vertrauen unsere Kunden mehr denn je darauf, dass wir ihre sensiblen Daten, Systeme und Abläufe vor den immer ausgeklügelteren Cybergefahren schützen. Angefangen bei Ransomware-Angriffen über Malware bis hin zu Cryptojacking: Unsere Gegenspieler entwickeln ihre Methoden unermüdlich weiter, sodass wir ständig wachsam sein und proaktiv vorgehen müssen.

In diesem Sinne freue ich mich, das Halbjahres-Update für den SonicWall Cyber Threat Report 2024 vorstellen zu dürfen. Wir möchten damit unsere Partnerschaft und unsere gemeinsamen Anstrengungen weiter stärken. In diesem Update beleuchten wir nicht nur, wie sich die Bedrohungslandschaft verändert hat, sondern auch, was wir unternehmen, um unsere Partner und Kunden kontinuierlich zu unterstützen. Bedrohungsakteure entwickeln immer effizientere und ausgeklügeltere Taktiken. Die Malware-Zahl ist im Vergleich zum Vorjahreszeitraum um 30 % gestiegen und wir haben deutliche Zunahmen bei IoT-Malware (+107 %) und verschlüsselten Bedrohungen (+92 %). Dies führt uns eines vor Augen: Cyberkriminelle haben auf der ganzen Welt ihre Methoden weiterentwickelt.

Dieser Report bietet Partnern, MSPs, MSSPs und Kunden aussagekräftige Informationen, die ihnen helfen, Abwehrstrategien zur Bekämpfung alter und neuer Bedrohungen zu entwickeln und umzusetzen. Das ist der Hauptgrund, warum wir den SonicWall Cyber Threat Report weiterhin veröffentlichen. Und dieses Jahr haben wir unsere Bedrohungsdaten in einen belastbaren finanziellen Kontext gestellt, der für jede Organisation nachvollziehbar sein sollte.

Um unsere Leser noch besser aufzuklären und zu informieren, haben wir zudem neue Perspektiven hinzugefügt. Diese umfassen das Feedback unserer 24/7/365-SOC-Analysten (SOC = Security-Operations-Center), Markteinblicke eines renommierten Cybersecurity-Versicherungsanbieters sowie Beiträge einiger unserer Partner.

Unsere Partner tun sicher gut daran, diese Ausgabe für Beratungsgespräche über die Dienstleistungen und Produkte zu nutzen, die unsere Kunden für den Schutz ihrer Marken und Unternehmen benötigen.

Ich bin mir sicher, dass dieser Report dazu beitragen wird, unsere gemeinsame Mission, die Umgebungen unserer Kunden effektiv zu schützen, weiter zu stärken. Ihr Feedback und Ihre Beiträge waren dabei entscheidend für unsere Vorgehensweise und die Ausrichtung des Reports – und das werden sie auch künftig sein.

Im Namen unseres erstklassigen globalen Sicherheitspartnernetzwerks und des gesamten SonicWall-Teams, einschließlich der Bedrohungsexperten von Capture Labs, freuen wir uns, Ihnen mit dem Halbjahres-Update für den SonicWall Cyber Threat Report 2024 einen exklusiven Einblick in die jüngsten Entwicklungen der Cybersicherheitslandschaft bieten zu können.

Bob VanKirk
President und CEO
SonicWall

Executive Summary

BEDROHUNGSLANDSCHAFT

125 %

Laut unseren Sensoren kam es im Laufe einer 40-Stunden-Arbeitswoche insgesamt zu ganzen 50 Stunden kritischer Angriffe. Sie haben richtig gelesen: Eine durchschnittliche Firewall stand in einer 40-Stunden-Arbeitswoche zu 125 % der Zeit unter Beschuss.

In den ersten fünf Monaten des Jahres 2024 wurden Organisationen weltweit vor 46 potenziellen Ausfalltagen bewahrt.

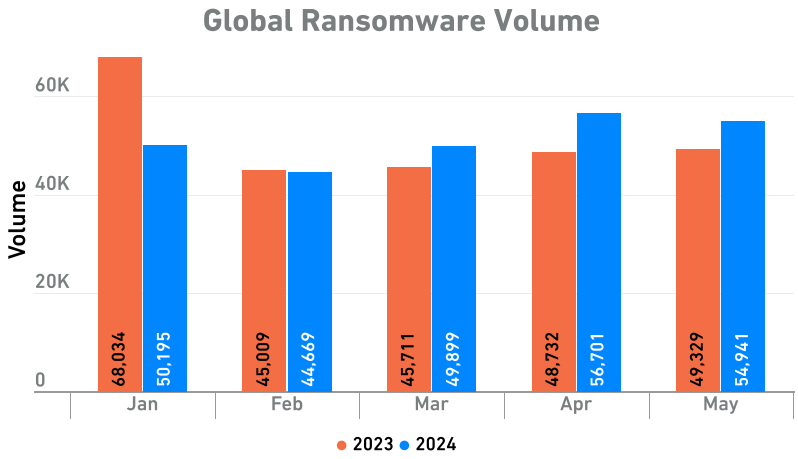
46 TAGE

12,6 %

Mindestens 12,6 % aller Umsätze sind Cyberbedrohungen ohne angemessenen Schutz ausgesetzt. Für ein Unternehmen mit einem Umsatz von 10 Millionen USD wären das 1,2 Millionen USD.

RANSOMWARE

Während die Ransomware-Zahl in der Region Amerikas steigt (NOAM: 15 %, LATAM: 51 %), drückt EMEA das globale Volumen mit einem Rückgang von 49 % nach unten; das deutet darauf hin, dass die verbesserten Cybersecurity- und Strafverfolgungsmaßnahmen Wirkung zeigen.



MALWARE

▲30 %

Malware hat von März bis Mai zugenommen, mit einem massiven Anstieg von 92 % allein im Mai.

15 %

15 % aller Malware nutzt Software-Packing als primäre MITRE-TTP.

IoT-MALWARE

Angegriffene IoT-Geräte standen durchschnittlich 52,8 Stunden unter Beschuss.

▲107 %

VERSCHLÜSSELTE BEDROHUNGEN

▲92 %

Verschlüsselte Bedrohungen nahmen um 92 % zu. Das zeigt: Cyberkriminelle gehen immer raffinierter vor und nutzen nach wie vor zunehmend TLS-verschlüsselte Übertragungswege, um Malware und andere Bedrohungen über das Netzwerk zu verbreiten.

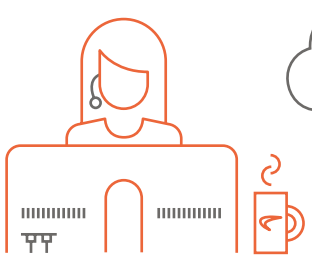
„Das Halbjahres-Update für den SonicWall Cyber Threat Report 2024 beleuchtet aktuelle Trends und bietet unseren Partnern, MSPs, MSSPs und Kunden aussagekräftige Informationen, um Abwehrstrategien zur Bekämpfung alter und neuer Bedrohungen zu entwickeln und umzusetzen."

BOB VANKIRK, PRESIDENT UND CEO VON SONICWALL

SOC

83 % der Sicherheitswarnungen, die unser Managed-Services-Team erhielt, bezogen sich auf Cloud-Apps und kompromittierte Anmeldedaten.

83 %



RTDMI™

526

— NEUE VARIANTEN —

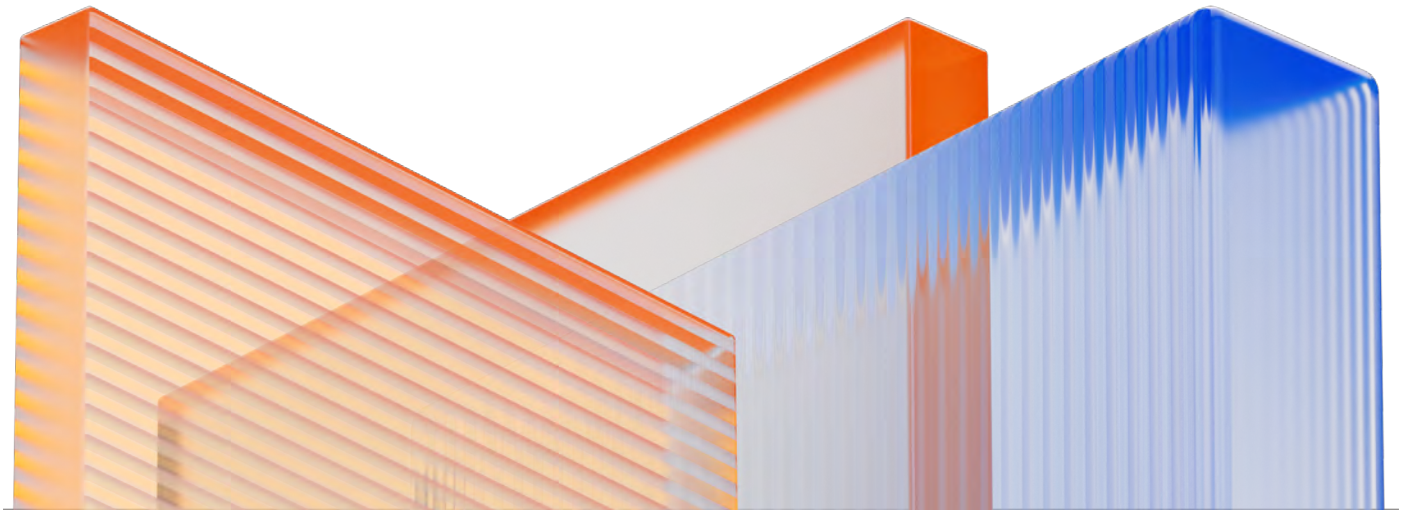
PRO TAG

SonicWall Capture Advanced Threat Protection (ATP) mit Real-Time Deep Memory Inspection (RTDMI ™) erfasste 78.923 neue Varianten.

CRYPTOJACKING

▼60 %

Nach einem Rekordjahr fiel die Cryptojacking-Zahl um 60 %. Die meisten Regionen der Welt verzeichneten einen Rückgang, mit Ausnahme von Indien, wo Cryptojacking um erschreckende 409 % nach oben schoss.



Eine neue Art, Bedrohungen zu messen

Auch der SonicWall Threat Report kommt langsam in die Jahre. Für uns ist dies der richtige Zeitpunkt, die Art und Weise, wie wir Daten messen und erfassen, auf den Prüfstand zu stellen. Nur so können wir uns an die dynamische Bedrohungslandschaft anpassen. Mit den neuen Bedrohungen vergrößern sich die Angriffsflächen, und auch die Komplexität der Daten nimmt zu. Herkömmliche Messgrößen können unscharf werden und zu mangelhaften Interpretationen führen. Durch die kontinuierliche Verfeinerung unserer Analysemethoden können wir die Nuancen sich verändernder Bedrohungen besser erfassen, die Auswirkungen von Anomalien reduzieren und genauere, zeitnähere und aussagekräftigere Erkenntnisse gewährleisten. Wir geben heute bekannt, dass wir künftig unsere Daten auf eine neue Art und Weise präsentieren werden. Statt wie bisher die sogenannte HITS-Metrik zu nutzen, wenden wir in Zukunft die neue TICKS-Bedrohungsmetrik an. Wir sind davon überzeugt, dass diese unseren Partnern und Kunden aussagekräftigere Erkenntnisse liefert.

Die Umstellung auf die TICKS-Metrik für die Meldung von Telemetriedaten soll Genauigkeit und Verlässlichkeit verbessern und eine präzisere Messung der Firewall-Aktivität ermöglichen. **TICKS gibt die Anzahl der Stunden an, die eine Firewall einer bestimmten Bedrohung ausgesetzt ist.**

Die absolute Anzahl der HITS kann je nachdem, wie die Signatur geschrieben ist, schwanken. Dies hängt nicht von der tatsächlichen Bedrohung, sondern eher von der Erkennungstechnologie ab.

TICKS normalisiert die „Erkennungsereignisse“ oder Treffer auf einen logischen Wert (wahr/falsch) für jede Bedrohung entsprechend unserer standardmäßigen Zeiteinheit, die in Stunden angegeben wird.

Anstatt die Gesamtzahl der Ereignisse zu zählen, erfasst die TICKS-Metrik die Stunden, in denen eine Firewall unter Beschuss ist, wobei nur Stunden mit mindestens einem Treffer gezählt werden. Auf diese Weise werden die Daten normalisiert und die Anfälligkeit für Ausreißer verringert. Der Fokus liegt auf der Dauer der Angriffe und nicht auf ihrer Intensität, wodurch anhaltende Bedrohungen besser hervorgehoben werden. Dieser Ansatz reduziert die Auswirkungen gelegentlicher Angriffsspitzen und hebt anhaltende Bedrohungen hervor, die sofortige Aufmerksamkeit erfordern. Er verbessert die Genauigkeit und Zuverlässigkeit bei der Einschätzung von Cybersicherheitsbedrohungen und optimiert Entscheidungen und Strategien zum Schutz von Netzwerken und Systemen.

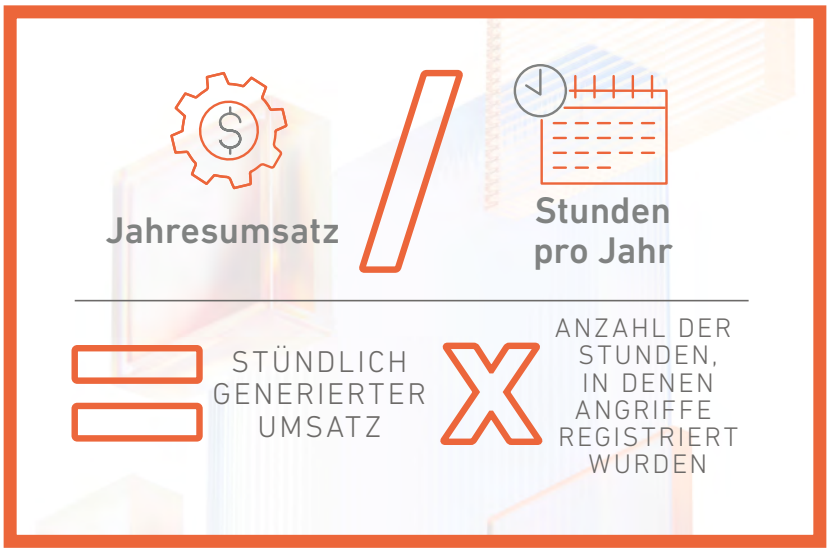
Durch die kontinuierliche Entwicklung unserer Methodik profitieren wir zudem von Fortschritten in den Bereichen Data-Science und Datentechnologie. Auf diese Weise verbessern wir unsere Fähigkeit, Muster zu erkennen, Trends vorherzusagen und fundierte Entscheidungen zu treffen. Letzten Endes ist es unerlässlich, neueste Erkenntnisse in den Bereichen Datenanalyse und Messmethodik zu nutzen, um robuste Sicherheitsmaßnahmen umzusetzen, die Performance zu optimieren und Innovationen voranzutreiben.

Methodik

Wie bereits erwähnt, haben wir unsere Metriken so weiterentwickelt, dass wir einen ungefähren Dollarbetrag für den Unternehmensumsatz angeben können, der von unseren Produkten vor bösartigen Angriffen geschützt wurde. Um den Umsatz pro Stunde zu ermitteln, haben wir den Jahresumsatz durch die Anzahl der Stunden pro Jahr geteilt.

In dieser Formel teilen wir den Jahresumsatz durch die Anzahl der Stunden pro Jahr, um den stündlichen Umsatz zu erhalten. Mithilfe unserer neu eingeführten TICKS-Daten multiplizieren wir diese Zahl mit der Anzahl der Stunden, in denen unsere Sensoren kritische Angriffe registriert haben.

Die endgültige Zahl entspricht dem Gesamtumsatz, der mindestens durch diese bekannten Angriffe gefährdet wurde. Nicht enthalten sind eventuelle Zusatzkosten für die Reparatur oder den Ersatz infizierter Systeme, die Behebung der Schwachstelle, die Quarantäne der kompromittierten Hard- und Software usw.



Was sind die neuesten Trends?

Unser Halbjahres-Update zum Threat Report bietet Partnern einen Überblick über die neuesten Sicherheitstrends aus der ersten Jahreshälfte. Damit können sie das Verhalten von Bedrohungsakteuren besser nachvollziehen und ihre Sicherheitsmaßnahmen optimieren.

Supply-Chain-Attacken auf dem Vormarsch

Supply-Chain-Attacken werden immer raffinierter und effektiver und sind mittlerweile zu einer großen Bedrohung für die Cybersicherheit geworden. Diese Angriffe profitieren davon, dass moderne Unternehmen stark vernetzt sind, und zielen auf Schwachstellen in Drittanbieter-Software und -Services ab, um größere Netzwerke zu kompromittieren. In der ersten Jahreshälfte 2024 gab es zahlreiche Vorfälle, die für großes Aufsehen sorgten, wie etwa die Umgehung des Authentifizierungsschritts im TeamCity-Tool von JetBrains. Dies zeigt, wie weit verbreitet diese Angriffe sind und welche schwerwiegenden Folgen sie haben können.

Analysen von SonicWall belegen, dass ältere Schwachstellen nach wie vor ein signifikantes Risiko darstellen, ganz besonders für KMUs mit begrenzten Ressourcen. Wie bereits berichtet, standen bis Ende 2023 drei der fünf häufigsten Angriffe im Zusammenhang mit Lieferketten. Dabei waren mehr als 50 % der Kunden von Schwachstellen in der Lieferkette betroffen, einschließlich älterer Probleme wie Log4j und Heartbleed.

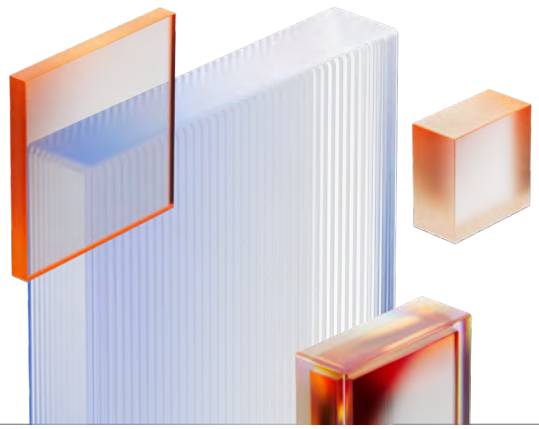
Warum Supply-Chain-Attacken so komplex sind

Bei einem Supply-Chain-Angriff wird ein Unternehmensnetzwerk über Schwachstellen bei Drittanbietern oder Partnern infiltriert. Bedrohungsakteure nutzen Schwachstellen in Software-Updates, Bibliotheken oder vernetzten Systemen aus und verschaffen sich so einen unerlaubten Zugriff auf sensible Daten oder Systeme. Diese Methode ist besonders effektiv, da sie herkömmliche Sicherheitsmaßnahmen umgeht, die sich auf direkte Angriffe fokussieren, und die Erkennung und Prävention von Bedrohungen erschwert.

Der Vorfall mit dem TeamCity-Tool von JetBrains

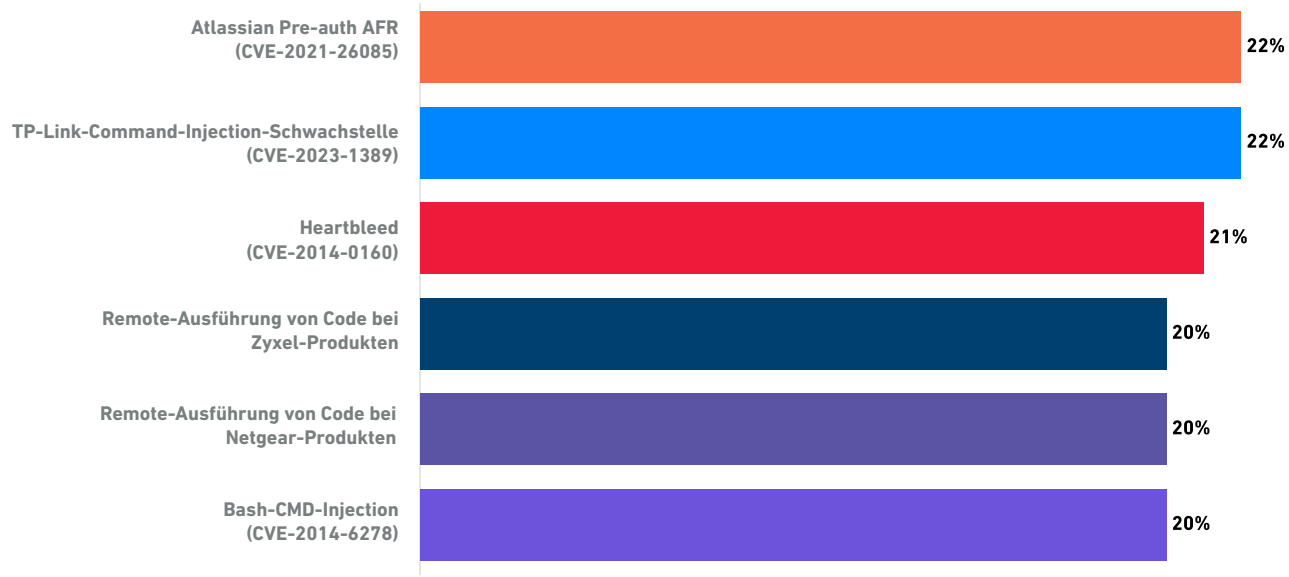
Im März 2024 nutzten Cyberkriminelle Schwachstellen in TeamCity, einem beliebten CI-/CD-Tool von JetBrains, aus. Unseren Untersuchungen zufolge konnten die Angreifer die Authentifizierungsmechanismen umgehen, indem sie eine 404-Antwort ausgaben und den JSP-Abfrageparameter manipulierten. Dadurch erlangten sie möglicherweise die vollständige Kontrolle über die betroffenen Systeme. Die US-Behörde für Cybersicherheit und Infrastruktursicherheit (CISA) nahm die JetBrains-Schwachstelle (CVE-2024-27198) umgehend in ihren Katalog der bekannten ausgenutzten Schwachstellen auf.

Laut unseren Telemetriedaten nahmen Bedrohungsakteure, die diese Schwachstelle ausnutzten, 16 % all unserer Kunden ins Visier – dies zeigt, wie einfach die Schwachstelle sich ausnutzen ließ und wie nützlich sie für Bedrohungsakteure war. 83 % dieser Angriffe erfolgten im März, gefolgt von einem beträchtlichen Rückgang in den darauffolgenden Monaten. Hier wird deutlich, wie kritisch unverzügliches Patching ist, da Angreifer häufig in dem Zeitfenster agieren, das Organisationen zur Implementierung von Patches benötigen.



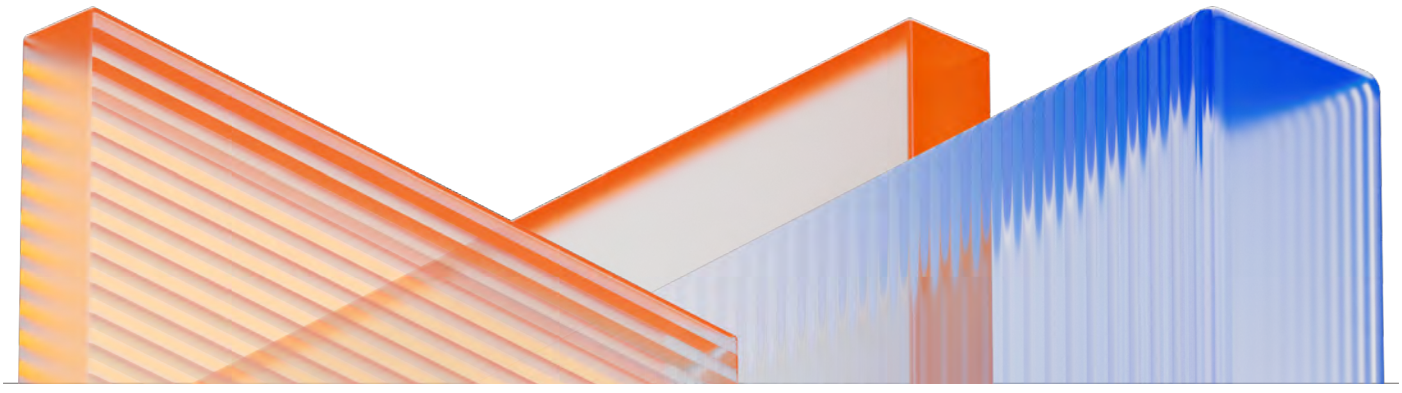
Nachdem die Ausnutzung der JetBrains-TeamCity-Schwachstelle gemeldet wurde, setzten Bedrohungsakteure die Ransomware Jasmin und den Kryptominer XMRig ein, was zu schwerwiegenden Datenschutzverletzungen, hohem Ressourcenverbrauch und Betriebsunterbrechungen führte. Obwohl SonicWall einen 60%igen Rückgang bei Cryptomining-Angriffen in der ersten Jahreshälfte 2024 beobachtete, zeigt die Ausnutzung dieser spezifischen Schwachstellen, wie allgegenwärtig die Cryptojacking-Gefahr noch ist.

Die 5 häufigsten Netzwerkangriffe im Jahr 2024



DAS SAGT UNSER SOC

Um Supply-Chain-Schwachstellen zu verhindern, muss man gründlich vorgehen – Sie müssen alle Einzelheiten Ihrer Drittanbieter-Software und -Services kennen, damit Sie ein starkes Sicherheitskonzept umsetzen können. Robuste Patch-Management-Protokolle helfen Ihnen, Ihr Risiko für ältere Schwachstellen wie Log4j und Heartbleed, die immer noch ausgenutzt werden, zu senken. Branchenberichte ergaben, dass Organisationen im Durchschnitt 55 Tage brauchen, um 50 % der kritischen Schwachstellen zu patchen. MSPs bieten automatisiertes Patching und professionelle Sicherheitstests, um Ihnen Zugang zu fortschrittlichen Sicherheitsmaßnahmen zu verschaffen – ohne hohe Kosten und interne Ressourcen.



Der Vormarsch von Business-E-Mail-Compromise (BEC) aus Sicht einer Cyberversicherung

In den letzten Jahren haben sich Cyberbedrohungen grundlegend weiterentwickelt, wobei Business-E-Mail-Compromise(BEC)-Angriffe in den Vordergrund gerückt sind. Unserem Versicherungspartner zufolge kommen heute auf einen Ransomware-Vorfall im Durchschnitt zehn BEC-Ereignisse – und alles deutet darauf hin, dass dieser Trend wachsen wird. Auch falsche Konfigurationen in Microsoft Office 365 (O365), besonders auf der Active-Directory-Ebene, tragen zur Zunahme der BEC-Vorfälle bei.

Bei BEC-Angriffen kommen primär Social-Engineering-Taktiken zum Einsatz: So nutzen 70 % der gemeldeten Vorfälle irgendeine Art von Social Engineering. Im Rahmen dieser ausgeklügelten Angriffe werden Einzelpersonen oft so manipuliert, dass sie Geld überweisen oder sensible Informationen teilen. Zum Beispiel gab es einen Fall, bei dem Angreifer eine begrenzte Kontrolle über das E-Mail-Konto ihres Opfers erlangt haben. Anschließend konnten sie betrügerische Rechnungsanfragen versenden und Antworten auf einen RSS-Feed umleiten. Diese Taktik erweckt den Eindruck, dass das Opfer die Kontrolle über sein E-Mail-Konto hat. Der Angreifer antwortet währenddessen per E-Mail auf Verifizierungsanfragen und versichert den Kunden fälschlicherweise, dass die Überweisung sicher sei. Dadurch wurden Summen in Millionenhöhe auf betrügerische Konten überwiesen, ohne dass eine realistische Möglichkeit einer Rückforderung bestand.

In einem anderen Fall wurde ein Anbieter kompromittiert, was einen Man-in-the-Middle(MITM)-Angriff zur Folge hatte. Bei diesem Angriff blieb die Kommunikation zwischen dem Anbieter und dem Kunden zwar bestehen, der Bedrohungsakteur war jedoch in der Lage, die Überweisungsanweisungen zu ändern. Folglich überwiesen die Kunden beträchtliche Summen – manchmal in Millionenhöhe – auf das falsche Konto, weil sie von einer ordnungsgemäßen Transaktion ausgingen.

Im Versicherungsbereich stellen solche Vorfälle ein Problem dar. Normalerweise sehen Versicherungspolicen vor, dass Änderungen an Überweisungsaufträgen immer überprüft werden. Dieser Schritt wird jedoch häufig vernachlässigt, wenn die Kommunikation legitim erscheint. Trotz robuster E-Mail-Filtering-Services und Security-Stacks sind diese Angriffe aufgrund der Authentizität der kompromittierten Kommunikationskanäle oft erfolgreich.

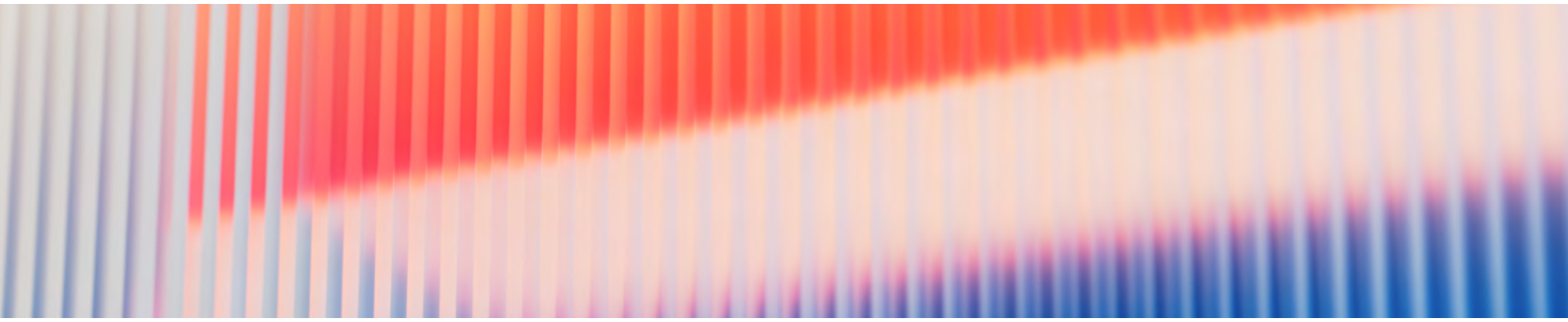
DAS SAGT EIN VERSICHERER

Unserem Versicherungspartner zufolge kommen heute auf einen Ransomware-Vorfall im Durchschnitt zehn BEC-Ereignisse.

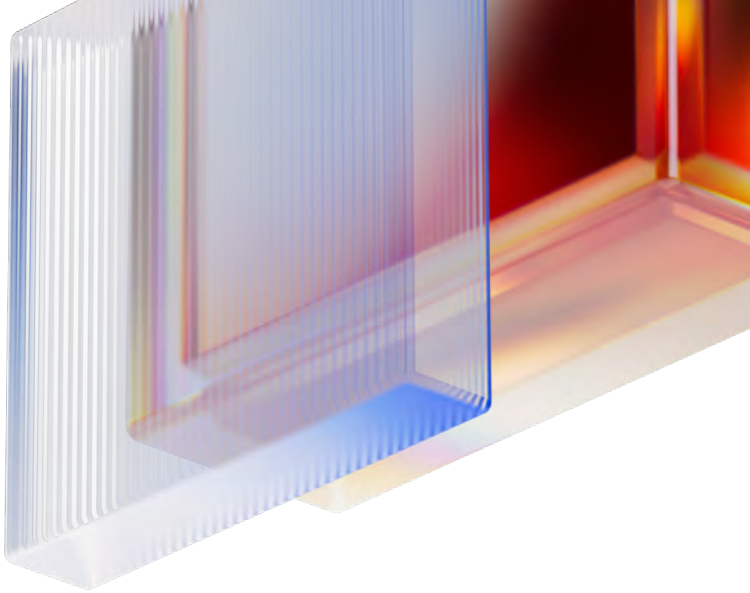
PARTNEREINBLICKE

„Die Bedrohungslandschaft stellt Organisationen und ihre Sicherheitsteams vor komplexe Herausforderungen. Die meisten Cybersecurity-Vorfälle sind zu einem gewissen Grad auf menschliches Versagen zurückzuführen. Letzten Endes gibt es zwei Möglichkeiten, dagegen vorzugehen: Möglichkeiten reduzieren und Nutzer sensibilisieren. Je weniger Möglichkeiten es für Fehler gibt, desto weniger werden Nutzer auf die Probe gestellt. Und je besser Mitarbeiter trainiert sind, desto unwahrscheinlicher machen sie einen Fehler – selbst wenn die Möglichkeit dazu besteht."

STEVEN HUANG – COO, Fornida
SonicWall-Partner



Hacker nehmen leichtere Schwachstellen in Microsoft-Produkten ins Visier



Zu Beginn des Jahres publizierte SonicWall einen Überblick über die Patches und Schwachstellen, die Microsoft 2023 veröffentlicht hat. Die Untersuchung zeigte, dass trotz der beträchtlichen Anzahl von Schwachstellen nicht alle Sicherheitslücken gleich behandelt werden sollten. Allein 2023 hat Microsoft mehr als 900 Schwachstellen gepatcht. Doch die eigentliche Sorge liegt darin, wie Angreifer diese Sicherheitslücken ausnutzen.

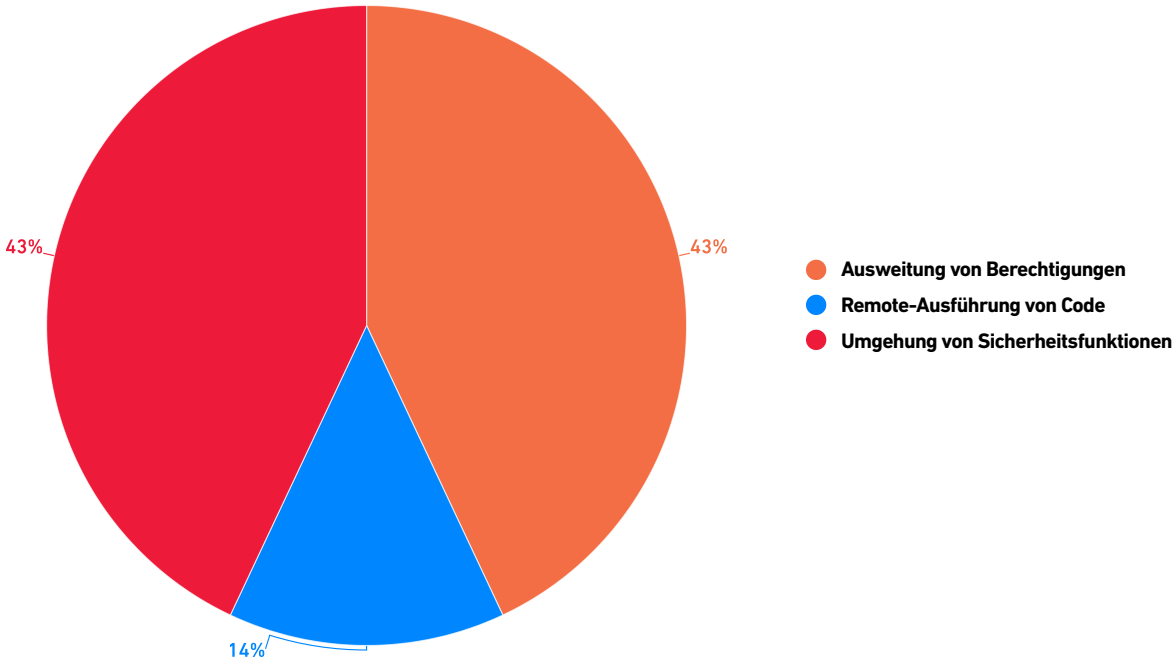
Unter den von Microsoft gepatchten Anfälligkeiten entfallen 36 % auf die Remote-Ausführung von Code (Remote Code Execution, RCE). Obwohl RCE-Schwachstellen einen erheblichen Anteil an der Gesamtzahl der Sicherheitslücken ausmachen, wurden sie 2023 nur in 5 % der Fälle ausgenutzt; dagegen wurden Anfälligkeiten, die auf die Ausweitung von Berechtigungen abzielen (Elevation of Privilege), in 52 % der Fälle ausgebeutet.

Bis Mitte 2024 wurden 434 Microsoft-Schwachstellen gemeldet und gepatcht, also ähnlich viele wie im Vorjahr. Interessant ist, dass zwar knapp 40 % der gemeldeten Sicherheitslücken als RCE eingestuft waren, aber nur eine einzige RCE-Schwachstelle ausgenutzt wurde. Bei 86 % der ausgenutzten Microsoft-Schwachstellen handelt es sich um Sicherheitslücken zur Umgehung von Sicherheitsfunktionen oder zur Ausweitung von Berechtigungen. Dies zeigt, wie wichtig es ist, diese Kategorien im Rahmen von Cybersicherheitsstrategien zu priorisieren, auch wenn sie zahlenmäßig weniger kritisch erscheinen.

DAS SAGT UNSER SOC

Um eine robuste Sicherheit zu gewährleisten, sollten Organisationen einen ausgewogenen Ansatz verfolgen und sich sowohl mit den weitverbreiteten RCEs als auch mit den häufiger ausgenutzten Elevation-of-Privilege-Schwachstellen befassen. Automatisches Patching, das häufig von MSPs eingesetzt wird, ermöglicht die Anwendung von Software-Updates, ohne dass der Benutzer eingreifen muss. Dieser Ansatz stellt sicher, dass Schwachstellen umgehend behoben werden. Dadurch wird das Zeitfenster für potenzielle Angriffe verkleinert, unabhängig davon, wie gravierend sie eingeschätzt werden. Das Ergebnis ist eine höhere Sicherheit.

Ausgenutzte Microsoft-Schwachstellen



Die Bedrohung entschlüsseln

Android-Geräte geraten immer häufiger ins Visier von Bedrohungsakteuren, insbesondere durch RATs – dabei meinen wir nicht die käsefressenden Nager, sondern Remote-Access-Trojaner. Diese RATs tarnen sich als legitime Anwendungen, um Berechtigungen zu erhalten. Anschließend stellen sie eine Verbindung zu Command-and-Control-Servern her, um Anmeldedaten zu stehlen und die Multi-Faktor-Authentifizierung (MFA) zu umgehen. Nennenswerte RATs wie Anubis, AhMyth und Cerberus, die in diesem Jahr in großem Umfang von Bedrohungsakteuren eingesetzt wurden, haben sich so weiterentwickelt, dass sie die MFA umgehen. Im April haben wir über verschiedene Kampagnen berichtet, bei denen RATs die Icons beliebter Apps nutzten, um User dazu zu verleiten, Berechtigungen zu erteilen. Auf diese Weise konnten sie Zwei-Faktor-Authentifizierungscodes über Zugangsdienste abfangen und sich einen unberechtigten Zugriff auf sensible Informationen verschaffen.

Malware-Upgrades

Anubis, ein Banking-Trojaner, kann mittlerweile MFA-Mechanismen umgehen, indem er SMS-Nachrichten mit Einmalpasswörtern (OTPs) abfängt. Das macht ihn zu einer erheblichen Bedrohung im Google Play Store.

AhMyth, ein RAT aus 2017, der immer noch im Einsatz ist, zielt durch infizierte Apps in verschiedenen Stores auf Android-Geräte ab, führt Keylogging durch, macht Screenshots und fängt MFA-OTPs ab.

Cerberus, eine Schadsoftware, die seit mindestens 2019 im Umlauf ist, wird als Malware as a Service (MaaS) betrieben und umfasst Funktionen wie SMS-Kontrolle, Keylogging und Audioaufzeichnung. Dadurch kann sie OTPs abfangen und die MFA für nicht autorisierte Transaktionen umgehen.

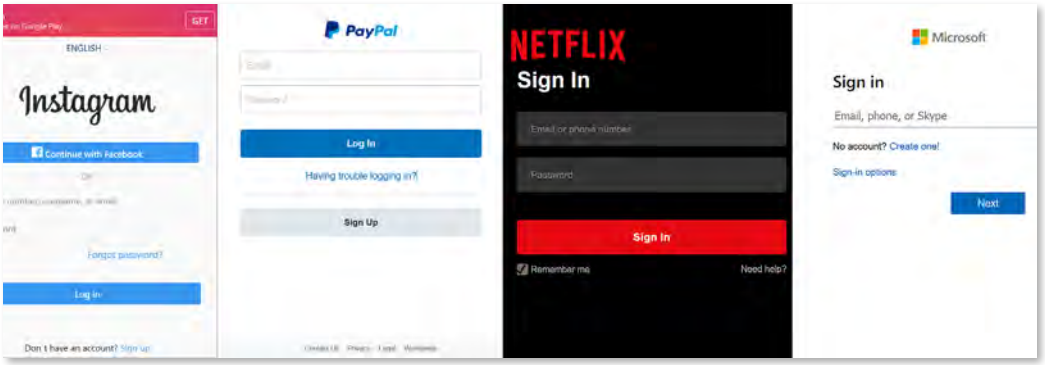


Abbildung 1: Reale Beispiele betrügerischer mobiler Log-in-Seiten

DAS SAGT UNSER SOC

Aus SOC-Perspektive werden standortbezogene Warnmeldungen durch Zugriffsversuche von ungewöhnlichen geografischen Standorten ausgelöst, die auf potenzielle Sicherheitsbedrohungen hinweisen. So würde etwa ein Zugriffsversuch von Russland aus eine Warnung auslösen, wenn sich ein User sonst immer von New York aus anmeldet. Diese Warnungen sind entscheidend für die Verbesserung der MFA-Sicherheit, da sie den SOC-Analysten helfen, unautorisierte Zugriffsversuche zu identifizieren und zu unterbinden, insbesondere solche, bei denen Anmeldedaten kompromittiert oder Standortdaten durch Malware manipuliert wurden. Unser Managed-Services-Team hat bereits mehr als 7.400 standortbezogene Warnmeldungen erhalten. Damit ist es sehr wahrscheinlich, dass die 2023 verzeichneten Warnmeldungen um 10 % übertroffen werden.

DAS SAGT EIN VERSICHERER

Viele Angreifer suchen ständig nach Möglichkeiten, die MFA zu umgehen. Dabei gibt es immer noch zahlreiche Organisationen, die MFA gar nicht einsetzen. Dies vereinfacht die Durchführung von Angriffen ungemein. In vielen Fällen zahlen die meisten Versicherungsgesellschaften *nicht* für Schäden, wenn die MFA bei betroffenen E-Mails, E-Mail-Systemen oder Servern nicht aktiviert ist. Der Einsatz von MFA ist wie das Anlegen eines Cybersicherheitsgurts: Er verhindert keinen Autounfall, ist aber ein Schlüsselelement für den Schutz Ihres Unternehmens und stellt sicher, dass Sie bei Ihrer Versicherungsgesellschaft in der bestmöglichen Position sind.

PowerShell: ein zweischneidiges Schwert – von mehr als 90 % der Malware-Familien ausgenutzt

Das Framework PowerShell hat sich bei Entwicklern und Systemadministratoren aufgrund seiner leistungsstarken Scripting-Funktionen, seiner Objektorientierung und seiner umfangreichen Schnittstelle für die Kommunikation mit dem Betriebssystem Windows zu einem beliebten Werkzeug entwickelt. Dank der engen Integration mit Windows können Benutzer eine Vielzahl von Aufgaben automatisieren, was es zu einem wertvollen Tool für legitime Zwecke macht.

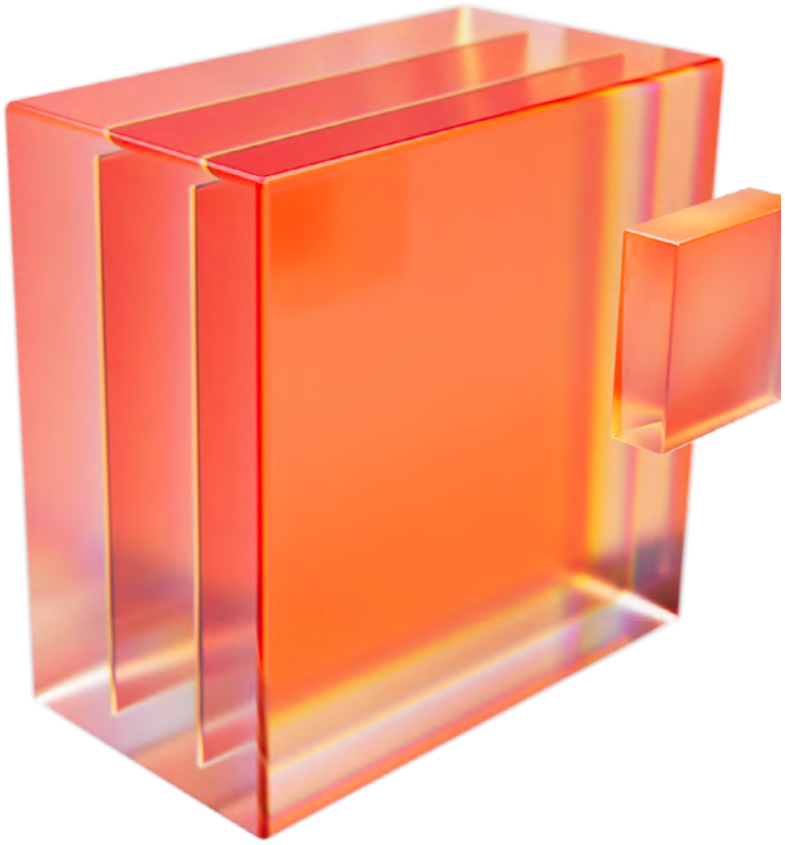
Leider sind es genau diese benutzerfreundlichen Features, die PowerShell zu einem attraktiven Werkzeug für Cyberkriminelle machen. Über 90 % der häufigsten Malware-Familien nutzen PowerShell, 73 % davon, um zusätzliche Malware herunterzuladen oder unentdeckt zu bleiben. Im Grunde machen sich alle Malware-Familien PowerShell zunutze. Bekannte Malware-Familien wie AgentTesla, GuLoader, AsyncRAT, DBatLoader und LokiBot setzen PowerShell-Skripts in großem Umfang ein, um eine Vielzahl bösartiger Aufgaben auszuführen.

PowerShell hat viel unternommen, um zu verhindern, dass heruntergeladene Skripts mit eingeschränkten Ausführungsrichtlinien ausgeführt werden. Leider haben Angreifer Wege gefunden, diese Einschränkungen zu umgehen: Sie rufen Skripts etwa lokal auf oder nutzen Befehlszeilenargumente, um bösartigen Code auszuführen.

Kürzlich erschienene Berichte deuten auf eine drastische Zunahme der PowerShell-basierten Angriffe. Die Zahl der Bedrohungen, die PowerShell nutzen, ist bis Ende 2020 um 208 % gestiegen und erreichte einen Höhepunkt, als fast alle Malware-Familien PowerShell verwendeten. Dieser Anstieg ist auf die zunehmende Verwendung von PowerShell für verschiedenste Angriffe zurückzuführen, darunter Prozessinjektion und Techniken zur Ausweitung von Berechtigungen. Auch bei dateilosen Malware-Angriffen wird PowerShell häufiger eingesetzt: So gibt es zahlreiche Kampagnen, die Payloads über PowerShell-Skripts übertragen, die in Spam-E-Mails oder Makros für Office-Dokumente eingebettet sind.

DAS SAGT UNSER SOC

Unsere Managed-Services-Mitarbeiter sind mit den Risiken von PowerShell vertraut. Bei einem Vorfall im Jahr 2024 wurden mehrere Geräte durch das Tool Mimikatz kompromittiert, das Cyberkriminelle häufig zum Stehlen von Anmeldeinformationen einsetzen. Die Untersuchungen ergaben, dass auf mehreren Rechnern ein verschlüsseltes PowerShell-Skript ausgeführt wurde. Dieses Skript war für das Herunterladen von Mimikatz und die Ausführung anderer bösartiger PowerShell-Befehle verantwortlich. Leider war die Sicherheitsrichtlinie zu diesem Zeitpunkt so eingestellt, dass solche Skripts nicht blockiert wurden, sondern nur eine Warnung ausgegeben wurde. Dadurch konnten sich die bösartigen Aktivitäten ausbreiten und Probleme verursachen. Zur Implementierung und internen Verbreitung dieser schädlichen Skripts nutzten die Angreifer einen kompromittierten ungeschützten Computer im Netzwerk. Dieser Vorfall macht deutlich, wie wichtig eine robuste Sicherheitskonfiguration und das proaktive Reagieren auf Sicherheitswarnungen sind, um die missbräuchliche Verwendung von PowerShell für Cyberangriffe zu verhindern.



Steigende Risiken von IoT-Angriffen

In der IoT-Sicherheitslandschaft hat sich im Laufe von 2024 einiges getan. Besonders hervorzuheben ist eine deutliche Zunahme von Angriffen auf IoT-Geräte. Unsere Daten ergeben für die erste Jahreshälfte 2024 einen dramatischen Anstieg der IoT-Angriffe von 107 % gegenüber dem Vorjahr. Diese Zunahme zeigt, dass Cyberkriminelle öfter auf IoT-Geräte abzielen – wahrscheinlich weil IoT-Geräte in der Regel leichtere Ziele abgeben. Oft fehlen diesen Geräten robuste Sicherheitsmechanismen, während die Angriffsflächen von Mainstream-Systemen wie Microsoft Windows besser geschützt werden.

Die TP-Link-Command-Injection-Schwachstelle (CVE-2023-1389) hat sich unter den zahlreichen Schwachstellen, die von Cyberkriminellen ausgenutzt werden, als eine der größten Bedrohungen herausgestellt. Diese Sicherheitslücke ist einer der Hauptgründe für den drastischen Anstieg der Angriffe im Jahr 2024, wobei im Mai eine besonders hohe Zunahme verzeichnet wurde. Sie ist die zweithäufigste Angriffsart und betrifft 21,25 % der kleinen und mittleren Unternehmen (KMUs). Die Ausnutzung dieser Schwachstelle war ein wesentlicher Grund dafür, dass die berüchtigte Mirai-Malware sich so schnell verbreiten konnte. Diese Malware kapert IoT-Geräte, um Botnets zu bilden, die groß angelegte Distributed-Denial-of-Service(DDoS)-Angriffe durchführen können. Unser Team berichtete bereits über den Anstieg der Aktivitäten und darüber, was die von den Bedrohungsakteuren ausgenutzten Schwachstellen gemeinsam haben. Obwohl diese Sicherheitslücke bereits seit 2023 existiert, haben Angreifer erst vor Kurzem damit begonnen, sie in großem Stil auszunutzen. Dies entspricht dem allgemeinen Trend der Kriminellen, ältere Schwachstellen ins Visier zu nehmen.

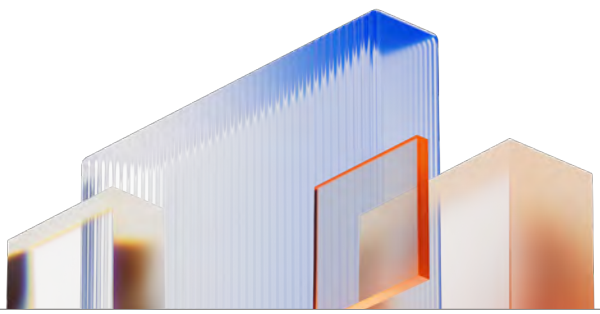
Eine weitere kritische Schwachstelle, die zurzeit ausgenutzt wird, zielt auf die Remote-Ausführung von Code in Zyxel-Produkten ab. Diese Sicherheitslücke, die 20,5 % der kleinen Unternehmen betrifft, steht 2024 an vierter Stelle der häufigsten Angriffe und erleichtert auch die Verbreitung von Mirai. Dies zeigt ganz klar, wie invasiv diese Malware ist.

Die Auswirkungen von IoT-Angriffen

Der Vormarsch von IoT-Angriffen bereitet Cybersicherheitsbeauftragten weltweit große Sorgen. Vorfälle wie die Volt-Typhoon-Botnet-Attacke und der koordinierte Angriff auf den dänischen Energiesektor verdeutlichen die wachsende Bedrohung. Bei der Volt-Typhoon-Attacke kompromittierte eine vom chinesischen Staat geförderte Hackergruppe Hunderte von SOHO-Routern in den USA und baute ein Botnet auf, das weitere Hackeraktivitäten gegen kritische Infrastrukturen verschleierte. Die kompromittierten Router – hauptsächlich von Cisco und NetGear – waren veraltet und wurden nicht mehr unterstützt, was sie besonders anfällig machte.

Im Mai 2023 kam es zu einem weiteren koordinierten Cyberangriff, der sich gegen 22 Energieunternehmen in Dänemark richtete. Hacker nutzten mehrere Schwachstellen in Zyxel-Firewalls aus, übernahmen die Kontrolle über die Systeme und führten Befehle aus. Dieser Angriff – der bisher größte auf kritische Infrastrukturen in Dänemark – führt uns klar vor Augen: Angreifer sind in der Lage, die Energieversorgung zu stören und kompromittierte Geräte für DDoS-Angriffe zu nutzen.

Diese Vorfälle entsprechen den Trends, die wir in der ersten Jahreshälfte 2024 beobachtet haben: Deutlich mehr Angreifer nehmen IoT-Geräte ins Visier und nutzen sie für ihre Zwecke. Da IoT-Geräte häufig Teil kritischer Infrastrukturen sind, können erfolgreiche Angriffe sehr lukrativ für Cyberkriminelle sein.



Phishing-Taktiken: wie HTML, KI und QR-Codes die Cybersicherheit neu definieren

Phishing-Taktiken haben sich enorm weiterentwickelt. Sie nutzen heute fortschrittliche Technologien und werden immer raffinierter. HTML-Phishing ist nach wie vor eine weitverbreitete und effektive Methode, um Anmeldedaten zu stehlen. Unseren Daten zufolge gab es zwischen dem vierten Quartal 2023 und dem ersten Halbjahr 2024 durchschnittlich mehr als 1.200 neue Bedrohungen pro Monat. Die Angreifer versuchen in der Regel, das Opfer mithilfe von Panikmache zur Eingabe seiner Zugangsdaten zu bewegen, um wichtige Dokumente einsehen zu können; manchmal wird die E-Mail-Adresse vorausgefüllt und nur das Passwort abgefragt. Sobald der User das Passwort eingibt, werden die Anmeldedaten an einen bösartigen Server weitergeleitet. Gleichzeitig findet eine Umleitung auf eine legitime Website statt, um keinen Verdacht zu erregen. Diese HTML-Dateien werden häufig mit Techniken wie iFrame-Umleitung und JavaScript getarnt, um nicht entdeckt zu werden.

In letzter Zeit haben wir einen wachsenden Trend zum QR-Code-Phishing bzw. „Quishing" beobachtet. Beim Quishing betten Angreifer QR-Codes in Phishingmails ein und fordern die Empfänger auf, diese mit ihrem Smartphone zu scannen. Diese Codes führen typischerweise zu Phishing-URLs, die legitime Log-in-Seiten wie die von Microsoft nachahmen, um Zugangsdaten abzufangen. Branchenberichten zufolge werden Quishing-Angriffe dramatisch zunehmen: von 0,8 % im Jahr 2021 auf 10,8 % aller Phishing-Angriffe im Jahr 2024. Diese Methode ist besonders effektiv, da sie sich die zunehmende Nutzung von Smartphones und QR-Codes zunutze macht. Während QR-Codes früher eher ein Nischendasein fristeten, finden sie sich heute in Kaufhäusern und auf Tischen in Restaurants, wo man damit Speisekarten, Gutscheine und vieles mehr aufrufen kann. Wahrscheinlich hängt die Zunahme dieser Art von Angriffen mit der insgesamt häufigeren Verwendung von QR-Codes zusammen.

Phishing-Angriffe sind außerdem vielschichtiger und komplexer geworden und nutzen verschiedene Kommunikationskanäle, um ihren Erfolg zu steigern. Um Phishing-Angriffe noch effektiver zu machen, setzen Cyberkriminelle zunehmend künstliche Intelligenz (KI) ein. Mithilfe von KI-Tools können sie hochgradig personalisierte Phishing-Nachrichten erstellen, die überzeugender und somit schwerer zu erkennen sind. Angreifer könnten mit einer E-Mail beginnen und dann über Microsoft Teams, Slack oder SMS nachhaken, um den Phishing-Versuch glaubwürdiger zu machen. Dieser Multi-Channel-Ansatz hat sich für Bedrohungsakteure als lukrativ erwiesen, wobei Plattformen wie Microsoft Teams bei einem erheblichen Teil dieser sekundären Angriffe eine Rolle spielen.

Phishing-Taktiken nutzen menschliches Verhalten mittlerweile effektiver aus. Die Phishing-Landschaft 2024 ist von komplexen Herausforderungen geprägt, die hoch entwickelte Erkennungs- und Präventionsmaßnahmen erfordern.

Abbildung 1: Quishing-E-Mail

DAS SAGT UNSER SOC

SOCs achten aktiv auf Konfigurationen, die eine Kompromittierung von Anmeldedaten ermöglichen, beispielsweise wenn MFA deaktiviert wird oder Passwörter unsachgemäß abgerufen werden. Mehr als 800 Warnmeldungen im Zusammenhang mit der Deaktivierung von MFA wurden im Jahr 2023 von unserem SOC bearbeitet. Alarmierend ist, dass wir allein im ersten Halbjahr 2024 bereits mehr als 650 Meldungen zu diesem Thema bearbeitet haben; das deutet darauf hin, dass sich die Zahl der Meldungen im Zusammenhang mit MFA im Jahr 2024 gegenüber dem Vorjahr vermutlich fast verdoppeln wird. Dieser Trend steht in engem Zusammenhang mit der Entwicklung von Phishing-Angriffen, die häufig auf Schwachstellen in der MFA-Implementierung abzielen. Der zunehmende Erfolg dieser Phishing-Strategien zeigt sich in der signifikanten Zunahme MFA-bezogener Warnmeldungen. All das führt uns vor Augen, wie wichtig eine robuste Überwachung ist, um eine Kompromittierung von Zugangsdaten zu verhindern.

DAS SAGT EIN VERSICHERER

Die meisten Ransomware-Angriffe, die einer Versicherung gemeldet werden, gehen auf eine erfolgreiche Phishing-Attacke zurück.

Relevante Informationen zu den veränderten Bedrohungen von heute

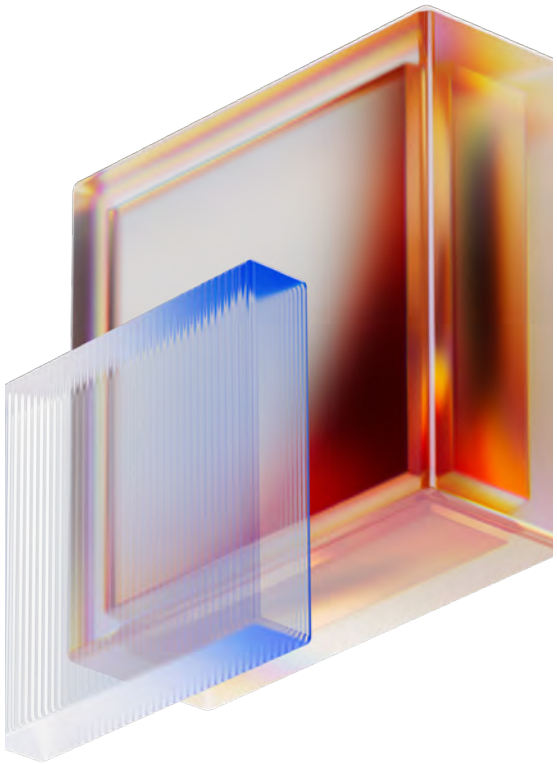
Herausforderungen bei der Entwicklung einer robusten Sicherheitsstrategie meistern

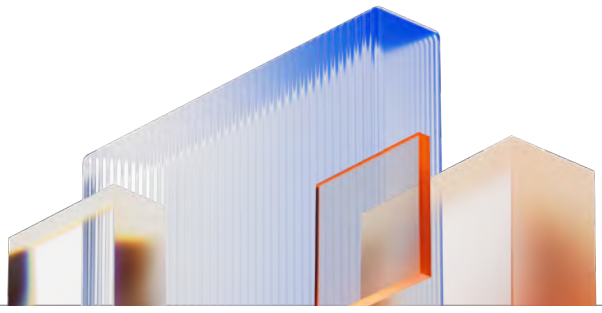
Es ist extrem wichtig zu wissen, welche Schwierigkeiten bei der Entwicklung eines guten Cybersicherheitskonzepts auftreten können. Nur so lassen sich die Hürden erkennen, die möglicherweise die Umsetzung effektiver Sicherheitspraktiken erschweren. Hier einige häufige Herausforderungen:

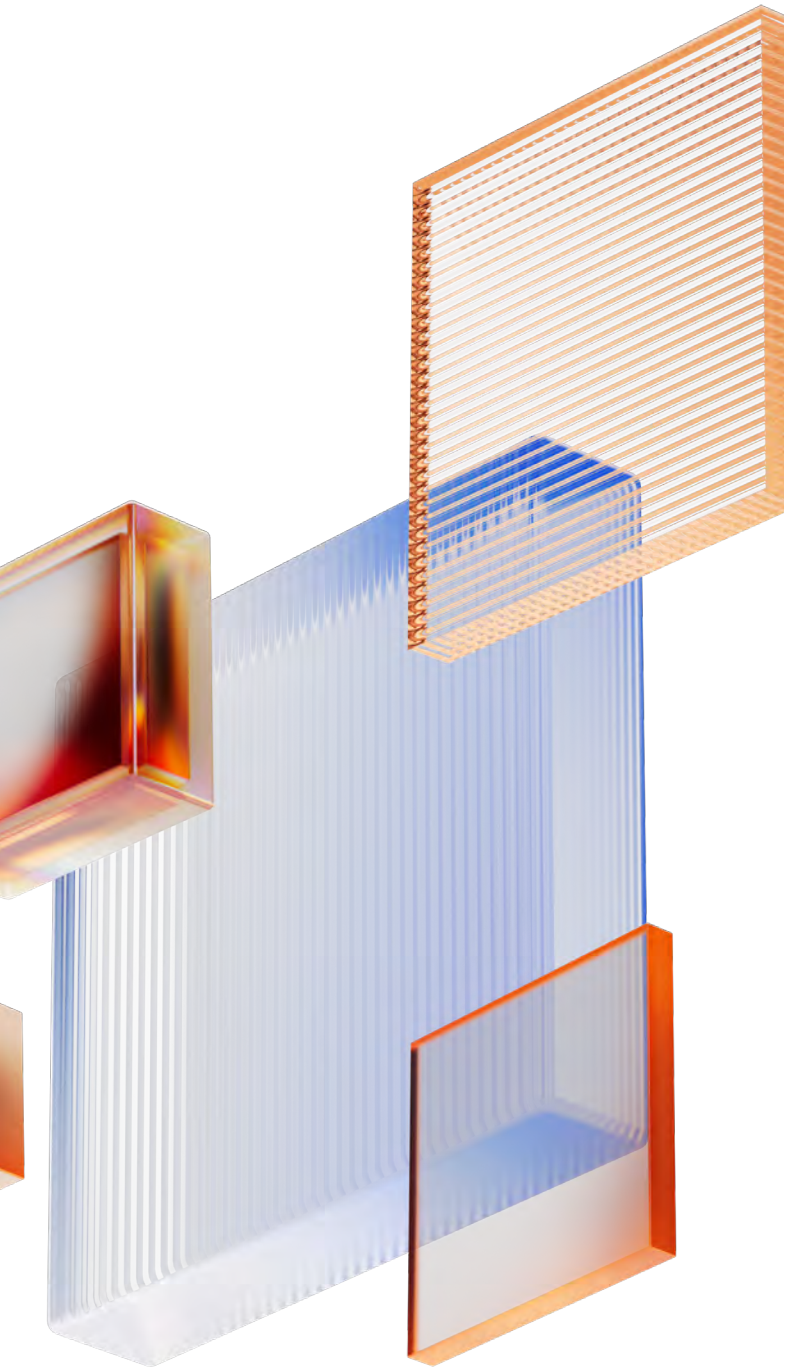
1. **Menschliches Versagen:** Menschliches Versagen stellt eine große Herausforderung für die Cybersicherheit dar, weil es zum versehentlichen Öffnen von Schwachstellen oder zum Missbrauch sensibler Informationen führen kann und damit das Risiko von Datenschutzverletzungen oder unberechtigtem Zugriff erhöht.
2. **Fehlerhaft konfigurierte Sicherheitslösungen:** Falsch konfigurierte Sicherheitslösungen, insbesondere in Cloud-Umgebungen, können kritische Lücken in den Abwehrmechanismen verursachen, was nicht nur Systeme und Netzwerke anfälliger für Cyberbedrohungen macht, sondern auch das Risiko eines unbefugten Zugriffs erhöht.
3. **Blockieren vs. Warnen:** Die Entscheidung, ob eine Blockierungs- oder eine Warnstrategie besser ist, sollte mit Bedacht getroffen werden. Wenn man sich zu sehr auf Warnungen verlässt, kann es passieren, dass Bedrohungen nicht abgewehrt werden. Auf der anderen Seite können zu viele Warnungen Analysten überfordern, was Alert-Fatigue begünstigen und dazu führen kann, dass kritische Sicherheitsvorfälle übersehen werden.
4. **Verzögerungen beim Patching:** Oft kommt es vor, dass Schwachstellen und Malware erkannt werden, Software oder Hardware aber aufgrund verspäteter oder fehlender Updates nicht gepatcht werden. Dadurch bleiben die Geräte anfällig für Angriffe, auch wenn bereits Fixes verfügbar sind.
5. **Standardkonfigurationen:** In vielen Fällen sind Software und Hardware nicht von vornherein für eine optimale Leistung ausgelegt. Sie können ein höheres Maß an Sicherheit erzielen, wenn Sie sich Zeit für das Feintuning Ihrer Hardware nehmen.

DAS SAGT UNSER SOC

Im Jahr 2024 betreute einer unserer MSPs einen Kunden aus der Finanzbranche, der aufgrund einer Sicherheitslücke mit Ransomware infiziert wurde, weil RDP von außen zugänglich war. Diese bekannte Fehlkonfiguration kommt immer noch vor und kann für Unternehmen extrem kostspielig sein.







So stärken Sie Ihr Cybersecurity-Konzept proaktiv

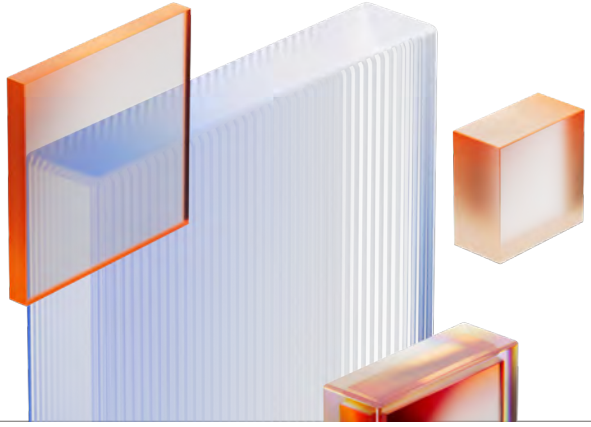
Die moderne Bedrohungslandschaft entwickelt sich unglaublich schnell. Der Siegeszug der KI beschleunigt diesen Prozess. Kein Unternehmen ist davor gefeit. Was sich jedoch nicht geändert hat, ist die Tatsache, dass viele der hier beschriebenen Angriffe und Bedrohungen mit dem richtigen Cybersicherheitskonzept gestoppt werden können. Hier finden Sie ein paar Schritte, mit denen Sie Ihr Cybersecurity-Konzept proaktiv stärken können:

- **Schnelles Patching:** Regelmäßige Patches sind unerlässlich, um Schwachstellen zu beheben und das Risiko zu verringern, böswilligen Akteuren zum Opfer zu fallen, die mit erschreckendem Tempo zuschlagen.
- **Multi-Faktor-Authentifizierung (MFA):** MFA verbessert die Cybersicherheit, da sie zusätzlich zu Passwörtern weitere Verifizierungsschritte vorsieht, was die Zugangskontrolle erheblich verstärkt und unberechtigte Zugriffsversuche vereitelt.
- **Verbesserung der Cloud-Sicherheit:** Da Unternehmen regelmäßig Daten und Prozesse in die Cloud verlagern, sind robuste Sicherheitsmaßnahmen wie Security-Service-Edge (SSE) und Zero-Trust-Network-Architekturen (ZTNAs) erforderlich, um Daten und Anwendungen zu schützen und sich umfassend gegen neue Cyberbedrohungen in Cloud-Umgebungen zu wappnen.
- **Kontinuierliche Überwachung und Reaktion auf Vorfälle:** Der Einsatz von Tools zur Echtzeiterkennung von Bedrohungen und die Entwicklung eines robusten Incident-Response-Plans können zur raschen Bekämpfung und Eindämmung von Cyberangriffen beitragen. Der Einsatz eines Security-Operations-Center (SOC) sollte in Erwägung gezogen werden, um neben der 24/7-Bedrohungserkennung auch eine humanbasierte Ebene hinzuzufügen.
- **Netzwerksegmentierung:** Um die Auswirkungen von Sicherheitsvorfällen und unberechtigten Zugriffen zu begrenzen, sollten Sie Netzwerke in kleinere, sichere Segmente unterteilen.
- **Kontinuierliche Weiterbildung:** Regelmäßige Cybersicherheitsschulungen sind unerlässlich, um Fachkräfte über neue Bedrohungen, Abwehrstrategien und Vorschriften auf dem Laufenden zu halten. So können sie Bedrohungen schnell erkennen und darauf reagieren, um Datenschutzverletzungen und finanzielle Verluste zu vermeiden. Durch kontinuierliches Training fördern Sie eine proaktive Cybersecurity-Kultur und stärken die Resilienz Ihrer Organisation gegenüber neuen Bedrohungen.

Die wichtigsten Erkenntnisse

Die wichtigsten Erkenntnisse für SOCs

- Effektive Patch-Management-Protokolle können dazu beitragen, die Anfälligkeit für ältere Schwachstellen zu reduzieren.
- Automatisiertes Patching steigert die Sicherheit, da Schwachstellen umgehend behoben werden und das Zeitfenster für mögliche Angriffe verkürzt wird.
- Die meisten kritischen Angriffe finden dienstags zwischen 3 und 6 Uhr morgens statt – also außerhalb der normalen Arbeitszeiten.
- Standortbasierte Warnmeldungen sind wichtig, um die MFA-Sicherheit zu verbessern und SOC-Analysten bei der Identifizierung und Unterbindung unbefugter Zugriffsversuche zu unterstützen.
- Sicherheitsrichtlinien sollten so konfiguriert werden, dass sie Bedrohungen blockieren und nicht nur Warnmeldungen ausgeben. So können Sie verhindern, dass sich bösartige Aktivitäten ausbreiten und Probleme verursachen.
- SOCs achten aktiv auf Konfigurationen, die eine Kompromittierung von Anmeldedaten ermöglichen, beispielsweise wenn MFA deaktiviert wird oder Passwörter unsachgemäß abgerufen werden.



Die wichtigsten Erkenntnisse für Versicherer

- Obwohl Ransomware die Schlagzeilen dominiert, sind BEC-Angriffe enorm häufig: Auf einen Ransomware-Vorfall kommen ganze zehn BEC-Attacken.
- Es gibt immer noch zahlreiche Organisationen, die MFA gar nicht einsetzen – das macht es Angreifern besonders einfach.
- In den meisten Fällen zahlen Versicherungsgesellschaften *nicht* für Schäden, wenn die MFA bei betroffenen E-Mails, E-Mail-Systemen oder Servern nicht aktiviert ist.
- Die meisten Ransomware-Angriffe, die einer Versicherung gemeldet werden, gehen auf eine erfolgreiche Phishing-Attacke zurück.

Die wichtigsten Erkenntnisse für Partner

- Die meisten Cybersecurity-Vorfälle sind zu einem gewissen Grad auf menschliches Versagen zurückzuführen.
- Der beste Weg, Fehlverhalten entgegenzuwirken, besteht darin, die Möglichkeiten für Fehler zu reduzieren und die Weiterbildung zu intensivieren.
- Je weniger Möglichkeiten Mitarbeiter haben, Fehler zu begehen, desto eher können häufige Pannen vermieden werden.

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

www.sonicwall.com

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.