paloalto NETWORKS

PRISMA BY PALO ALTO NETWORKS

Prisma Access Cloud SWG

Schutz vor modernen webbasierten Bedrohungen

INHALT

In den letzten Jahren hat sich das Arbeitsleben drastisch verändert. Die meisten Unternehmen haben hybride Arbeitsmodelle eingeführt, sodass die Mitarbeiter standortunabhängig arbeiten können. Einige haben sogar ihre physischen Standorte vollständig aufgegeben und setzen ganz auf die Arbeit im Homeoffice. Viele Unternehmen nutzen zudem Software-as-a-Service(SaaS)-Tools, um die Produktivität der mobilen Mitarbeiter zu gewährleisten oder sogar zu steigern.

Von diesem neuen Modell profitieren sowohl die Mitarbeiter als auch die Unternehmen – aber leider auch die Cyberkriminellen.

Durch die zunehmende Verbreitung der hybriden Arbeitsplätze und SaaS-Anwendungen müssen Unternehmen den Internetzugriff für ihre Mitarbeiter noch besser schützen, und zwar unabhängig von deren Standort. Denn da die Beschäftigten inzwischen nahezu überall und mit jedem Gerät auf das Internet zugreifen können, ist die Angriffsfläche erheblich gewachsen. Angreifern mit komplexen und ausgefeilten Techniken, die die herkömmlichen Sicherheitslösungen unterwandern können, bieten sich dadurch zahlreiche Einfallstore.

Zum Schutz vor diesen modernen webbasierten Bedrohungen ist daher eine neue Websicherheitsstrategie notwendig. Die bisherigen Methoden reichen nicht mehr aus, um neue und unbekannte Bedrohungen abzuwehren. Unternehmen benötigen eine Lösung, die den Angreifern und ihren modernen Techniken gewachsen ist.

3 Gründe

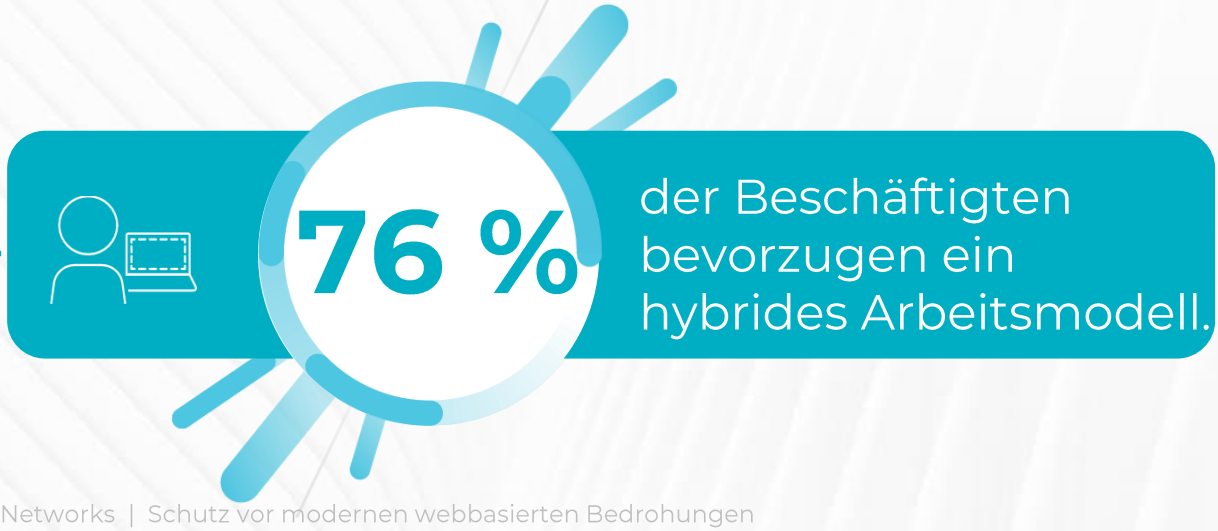
für das rasante Wachstum der Angriffsfläche im Internet

1 Wir nutzen das Internet mehr als je zuvor

Es ist kein Geheimnis, dass das Internet und die dort gehosteten Anwendungen entscheidend zu unserer Produktivität beitragen. Wir rufen jeden Tag diverse Websites auf verschiedenen Geräten auf – sowohl bei der Arbeit als auch in der Freizeit. Dieser umfassende Webzugriff steigert zwar unsere Produktivität, hat aber auch zu einer deutlich größeren Angriffsfläche geführt, die Cyberkriminelle für ihre Zwecke ausnutzen.

2 Durch das mobile Arbeiten sind Mitarbeiter anfälliger

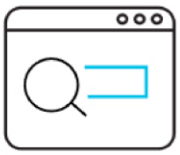
Unter Arbeit verstehen wir meist keinen physischen Ort mehr, sondern eine Tätigkeit. Dadurch können Mitarbeiter auch zu Hause, an öffentlichen Orten wie Cafés oder an anderen Orten mit einer WLAN-Verbindung arbeiten. Doch das mobile Arbeiten hat nicht nur Vorteile, sondern birgt auch Risiken. Mobile Mitarbeiter nutzen Heimnetze oder öffentliche Netzwerke für ihre Aufgaben – auch dann, wenn sensible Unternehmensdaten involviert sind. In der Vergangenheit haben Unternehmen Technologien wie VPNs (Virtual Private Networks) und ältere ZTNA 1.0-Sicherheitslösungen genutzt, um Remotebenutzer zu schützen, aber diese Methoden sind nicht flexibel genug und weisen zu viele Einschränkungen auf. Der Nachteil des flexiblen Modells ist, dass mobile Mitarbeiter unter Umständen Bedrohungen ausgesetzt sind, die in einem privaten und sicheren Büronetzwerk blockiert werden würden.



3 Cyberkriminelle sind technisch immer versierter

Angreifer kennen sich inzwischen gut mit den Techniken herkömmlicher Sicherheitslösungen aus und passen ihre Aktivitäten entsprechend an oder entwickeln neue Methoden. Auch Verschleierungstechniken wie Cloaking, mehrstufige Angriffe und einmalige Links kommen immer häufiger zum Einsatz, um neue und bisher unbekannte Bedrohungen zu verbreiten und die Sicherheitslösungen zu umgehen.

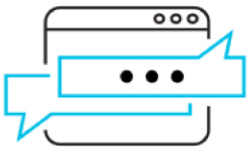
Eine Internetminute
im Jahr 2022



5,7 Mio.
Google-Suchanfragen

856
Minuten Webinare über Zoom

6 Mio.
Personen tätigten Onlinekäufe



148.000
gesendete Slack-Nachrichten

Wichtige webbasierte Bedrohungen

Bei diesen neuen Arbeitsmodellen finden viele sensible Arbeitsschritte und auch die vertrauliche Zusammenarbeit im Internet statt.

Für die Unternehmenskommunikation werden überwiegend E-Mails, Zoom oder Slack genutzt. Geschäftliche SaaS-Anwendungen wie Google Workspace oder Microsoft 365 kommen bei der Zusammenarbeit und Freigabe vertraulicher Dokumente in den Unternehmen zum Einsatz. Mitarbeiter verwenden gegebenenfalls auch nicht autorisierte Anwendungen wie Trello, Asana, Dropbox oder Evernote, um ihre Produktivität zu steigern. Angreifer nutzen diese Abhängigkeit von Web- und Unternehmensanwendungen aus, um sensible Daten zu stehlen. Damit droht den Opfern unter Umständen ein erheblicher Schaden.

Es gibt zahlreiche webbasierte Bedrohungsarten, aber einige wie Phishing, Ransomware und Malware gehören zu den bevorzugten Angriffstypen von Cyberkriminellen. Phishingangriffe sind besonders beliebt, da der Aufwand für die Erstellung und Durchführung einer Kampagne relativ gering ist. Ransomwareangriffe sind äußerst profitabel und Malware legt die Grundlage für verschiedene weitere Schritte, die dann unter anderem die finanzielle Bereicherung oder den Datendiebstahl ermöglichen.

Phishing

Eine zunehmende Gefahr für Unternehmen

Phishing ist eine Social-Engineering-Taktik, bei der ein Angreifer gefälschte Kommunikation wie E-Mail, SMS, Nachrichten in sozialen Medien oder Anrufe nutzt, um einen Benutzer dazu zu verleiten, Malware auf ein Gerät herunterzuladen oder sensible Informationen wie personenbezogene, Anmelde- oder Finanzdaten herauszugeben. Phishing ist zwar keine neue Methode, sondern schon seit Jahrzehnten im Einsatz, aber nach wie vor eine der am weitesten verbreiteten und gefährlichsten Arten von Cyberkriminalität.

Da ein Großteil der Kommunikation heutzutage online stattfindet, werden insbesondere E-Mails für Phishing-kampagnen ausgenutzt. Studien zufolge wurden **96 % der Phishing-angriffe im Jahr 2021 über E-Mails gestartet.** Cyberkriminelle gehen dabei meist nicht gezielt vor, sondern versenden zahllose E-Mails mit schädlichen Links und hoffen, dass mindestens einer aktiviert wird.

5 gängige Arten
von Phishingangriffen

Spear-Phishing

Bei Spear-Phishingangriffen wird eine personalisierte E-Mail, die häufig einen Link oder einen Anhang mit Malware enthält, gezielt an ein Opfer gesendet. Klickt diese Person darauf, wird die Malware auf ihr Gerät geladen und die Angreifer haben Zugriff auf persönliche Informationen.

Whaling

Beim Whaling werden gezielt Führungskräfte in Unternehmen kontaktiert, um sensible Informationen wie Anmelde- oder Finanzdaten zu stehlen oder Malware auf dem Gerät des Opfers zu installieren.

Smishing

Diese Phishingvariante nutzt SMS mit gefälschten Anhängen oder schädlichen Links, damit die Benutzer auf ihren Mobilgeräten darauf klicken.

Vishing

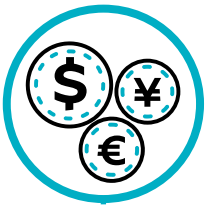
Vishing ist die Kurzform von „Voice Phishing“ und bezeichnet Phishingangriffe per Telefonanruf. Dabei geben sich die Angreifer häufig als Bank oder Behörde aus, um auf diese Weise Zugriff auf Daten der Opfer zu erhalten.

Angler Phishing

Diese Phishingvariante ist auf Benutzer sozialer Medien ausgerichtet. Angreifer geben sich als Kundendienst eines legitimen Unternehmens aus und kontaktieren unzufriedene Kunden, um ihre personenbezogenen Daten oder Anmeldedaten zu stehlen.

Risiken von Phishingangriffen

Phishingangriffe können in Unternehmen großen Schaden anrichten. Meist werden in diesem Zusammenhang die finanziellen Verluste genannt, aber diese sind nicht das einzige Problem.



Finanzielle Verluste

Phishingangriffe sind in der Regel mit finanziellen Verlusten verbunden, die aber verschiedene Gründe haben können. So können Angreifer beispielsweise ein Unternehmen oder einen Mitarbeiter dazu bringen, Geldbeträge an ein externes Konto zu überweisen. Unter Umständen fallen aber auch hohe Geldstrafen wegen Complianceverstößen in Bezug auf Verordnungen wie HIPAA, PCI und PIPEDA oder erhebliche Kosten für die Untersuchung des Vorfalls und die Entschädigung der Betroffenen an.

Datenverlust

Nach einem erfolgreichen Phishingangriff haben Cyberkriminelle unter Umständen Zugriff auf diverse sensible Daten. Dazu gehören Anmeldedaten, personenbezogene Daten wie Adressen und Telefonnummern, Unternehmensdaten, medizinische Informationen oder Bankdaten.

Imageschaden

Unternehmen ist häufig daran gelegen, dass ein Phishingangriff auf ihre Systeme nicht öffentlich bekannt wird, um das Vertrauen der Kunden und Investoren nicht zu verlieren. Das gilt insbesondere für Unternehmen, die sensible Kundendaten verwalten.

Störungen des Geschäftsbetriebs

Phishingangriffe, bei denen Geräte mit Malware infiziert werden, können Ausfallzeiten oder erhebliche Störungen bei der Bereitstellung von Services verursachen und dadurch die Produktivität des betroffenen Unternehmens beeinträchtigen.

Malware-Infektionen

Bei einem erfolgreichen Phishingangriff werden Unternehmensgeräte häufig mit Malware infiziert, was dann zu Störungen des Geschäftsbetriebs, Datendiebstahl, Ausfallzeiten im Netzwerk und anderen Problemen führt.

Ransomware

Ransomware ist eine Form von Malware und kann bei Phishingangriffen verheerenden Schaden anrichten, einschließlich finanzieller Verluste und Datenpannen. Dabei verschlüsseln die Angreifer sensible Daten und fordern für die Herausgabe des Entschlüsselungsschlüssels zur Wiederherstellung der Informationen ein Lösegeld.

$14,8 Mio.

durchschnittliche Kosten eines Phishingangriffs im Jahr 2021

$4,24 Mio.

durchschnittliche Kosten einer Datenpanne im Jahr 2021

50 Tage

durchschnittlicher Verlust infolge eines Malwareangriffs für Unternehmen

Starke Zunahme

an Ransomwareangriffen

Ransomware ist eine Form von Malware, mit der Angreifer den Zugriff auf wertvolle Dateien, Daten oder Informationen auf einem Gerät sperren. Sie verschlüsseln diese Dateien und fordern dann für die Herausgabe des Schlüssels für die Entschlüsselung ein hohes Lösegeld von ihren Opfern.

Ransomwareangriffe haben in der letzten Zeit häufig Schlagzeilen gemacht und dieser Trend scheint sich auch weiterhin fortzusetzen. **2021 gab es über 623 Millionen Ransomware-angriffe – 105 % mehr als im Vorjahr.** Dieser große Anstieg ist vor allem auf Ransomware-as-a-Service (RaaS) zurückzuführen. Mit diesem Angebot stehen Tools für Ransomwareangriffe allen Interessierten zur Verfügung, sodass auch technisch weniger versierte Angreifer den Einstieg in diese Sparte wagen und die Anzahl und die Häufigkeit der Angriffe entsprechend zunimmt.

Was ist Ransomware-as-a-Service?

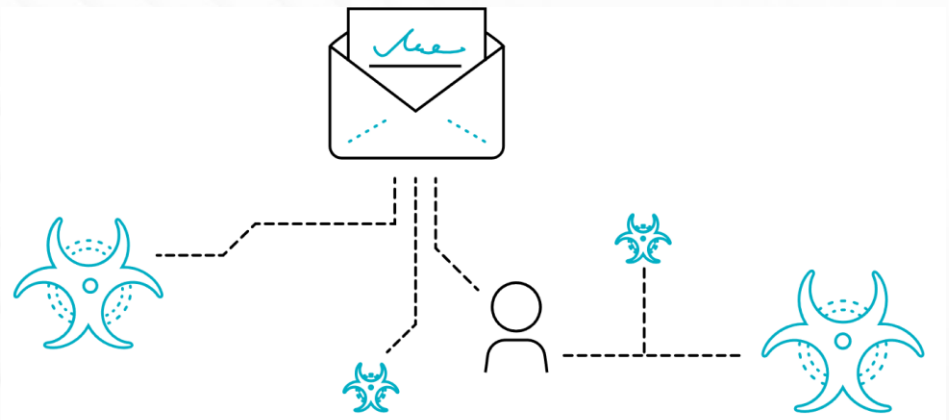
Ransomware-as-a-Service (RaaS) ist ein Geschäftsmodell unter Cyberkriminellen. Damit stehen Tools für Ransomwareangriffe allen Interessierten zur Verfügung, sodass auch technisch weniger versierte Angreifer den Einstieg in diese Sparte wagen können. Die Anbieter verlangen monatliche Nutzungsgebühren und erhalten zudem einen Prozentsatz des gezahlten Lösegelds.

Auf welchem Weg wird Ransomware am häufigsten verbreitet?

Phishing-E-Mails

Angreifer setzen für die Verbreitung von Ransomware bevorzugt auf Phishing-E-Mails, da diese in der Masse der täglichen Kommunikation weniger auffallen.

Inzwischen werden etwa **333,2 Milliarden E-Mails pro Tag gesendet, das sind 3,5 Millionen E-Mails pro Sekunde.** Da die meisten Benutzer E-Mails verwenden, ist es viel leichter, sie auf diesem Weg dazu zu bringen, auf einen schädlichen Link zu klicken und dadurch Ransomware auf ihr Gerät herunterzuladen. Von den 333,2 Milliarden E-Mails, die pro Tag versendet werden, **sind 3,4 Milliarden Phishing-E-Mails.** Das bedeutet, eine von 100 E-Mails ist eine Phishing-E-Mail. Je nachdem, wie viele E-Mail-Adressen oder Abonnements Sie haben, erhalten Sie unter Umständen jeden Tag mehrere Phishing-E-Mails.



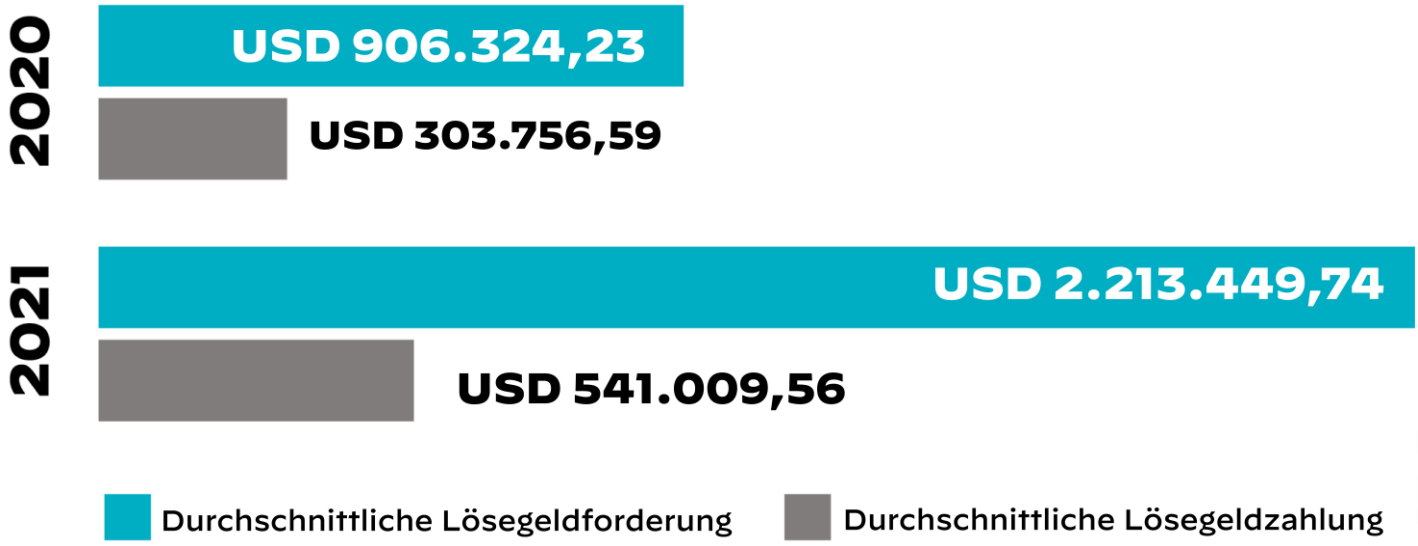
78 % der Unternehmen

erhielten 2021 eine Phishing-E-Mail mit Ransomware oder einem Link zu einem Ransomwaredownload.

Konsequenzen von Ransomwareangriffen

Mit zunehmender Anzahl an Ransomwareangriffen sind auch die verursachten Kosten stark gestiegen.

Die durchschnittliche Lösegeldforderung nach einem Ransomwareangriff lag 2021 bei **$2,2 Millionen und damit 144 % höher als noch 2020. Die durchschnittliche Lösegeldzahlung betrug $541.000 – 78 % mehr als noch im Vorjahr.** Aufgrund der großen Anzahl und der potenziellen schweren Schäden stellen Ransomwareangriffe eine gravierende Bedrohung für Unternehmen dar.



Vergleich der durchschnittlichen Lösegeldforderungen und der durchschnittlichen Lösegeldzahlungen 2020 und 2021 (Daten aus Incident-Response-Einsätzen von Unit 42)

Malware

Eine universelle Bedrohung

Malware ist schädliche Software und das bevorzugte Mittel von Angreifern, um Systeme und Netzwerke zu infiltrieren.

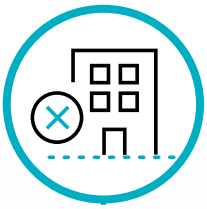
Gelingt es einem Angreifer, Malware auf dem Gerät eines Opfers zu installieren, kann er einen **Command-and-Control-Kanal einrichten und sich per Fernzugriff Kontrolle über das Gerät verschaffen**, Malware an andere ahnungslose Benutzer verbreiten, Anmeldedaten abrufen, das lokale Netzwerk des Benutzers ausspähen, weitere Angriffsschritte wie das Stehlen sensibler Daten oder das Implementieren eines Bots ausführen oder sogar von diesem Netzwerk aus einen Angriff auf andere Unternehmen starten. Es gibt zahlreiche Möglichkeiten, Malware zu verbreiten, aber Phishing ist seit der Zunahme an hybriden Arbeitsplätzen eine der beliebtesten Methoden.

Was ist Command-and-Control?

Command-and-Control (C2) ist eine Technik, mit der Angreifer über das Netzwerk mit infizierten Geräten kommunizieren und weitere Befehle übermitteln, zum Beispiel zum Herunterladen weiterer Malware, Erstellen von Botnets oder Ausschleusen von Daten.

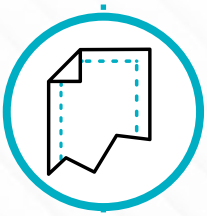
Konsequenzen von Malwareangriffen

Ein erfolgreicher Malwareangriff kann die Sicherheitsinfrastruktur eines Netzwerks erheblich beschädigen und diverse Sicherheitsprobleme verursachen. Außerdem ist der Zeit- und Kostenaufwand zur Behebung der Probleme sehr hoch. Zu den typischen Konsequenzen von Malwareangriffen gehören unter anderem:



Störungen des Geschäftsbetriebs

Malware kann den Netzwerkbetrieb stören oder lahmlegen, den Geschäftsbetrieb beeinträchtigen und in einigen Fällen die Bereitstellung von Services verhindern. Das kann die Produktivität eines Unternehmens mindern und zu schweren Verlusten führen.



Datenverlust

Unternehmen, denen bei einem Malwareangriff Daten gestohlen werden, müssen mit ernsten Konsequenzen wie Klagen, Verlust des Kundenvertrauens und Imageschäden rechnen.

Imageschaden

Opfer von Malwareangriffen müssen finanzielle Verluste durch die Störung des Geschäftsbetriebs, aber auch durch Kundenabwanderung, Wiederherstellung der Daten, Untersuchungen, Rechtskosten, Strafgebühren und Abwicklungskosten befürchten.

Probleme herkömmlicher Sicherheitslösungen

Aufgrund der zunehmenden Gefahr eines Phishing-, Ransomware- oder Malwareangriffs stehen Unternehmen unter enormem Druck, ihre Ressourcen angemessen zu schützen. Doch die herkömmlichen Sicherheitslösungen sind den neuen Methoden der Angreifer nicht gewachsen.

Cyberkriminelle sind technisch immer versierter

Entscheidend zum Erfolg moderner webbasierter Bedrohungen trägt die zunehmende **Kompetenz der Angreifer** bei. Cyberkriminelle haben im Laufe der Zeit ihre Techniken weiterentwickelt und können inzwischen herkömmliche Sicherheitslösungen umgehen und Abwehrmaßnahmen unterwandern.

- Dazu nutzen sie diverse Verschleierungstechniken wie Cloaking und Reverse-Proxys für Man-in-the-Middle-Angriffe sowie legitime SaaS-Plattformen.
- Mithilfe von Phishingkits und Cloud-Infrastrukturen können sie so innerhalb weniger Minuten Tausende Phishing-URLs generieren.
- Außerdem nutzen sie neue und bisher unbekannte Bedrohungen, die von herkömmlichen Sicherheitslösungen nicht erkannt werden, um jegliche Abwehrmaßnahmen problemlos zu umgehen.

5 gängige
Verschleierungstechniken

Neue und unbekannte URLs

Herkömmliche Webcrawler können neue und unbekannte schädliche URLs nicht schnell genug erkennen, sodass die Angreifer Abwehrmaßnahmen relativ problemlos umgehen können.

Cloaking zum Verbergen schädlicher Inhalte

Da Webcrawler den Netzwerkverkehr nicht in Echtzeit analysieren, verbergen Angreifer einfach ihre Absichten und leiten Netzwerkscanner auf eine harmlose Website oder eine leere Seite, bevor sie dann ihre echte schädliche Website freischalten.

Mehrstufige Angriffe und CAPTCHAs

Angreifer verbergen ihre Aktivitäten hinter diversen harmlosen Schritten, zum Beispiel einem CAPTCHA, damit Webcrawler die schädlichen Inhalte nicht erkennen.

Dynamische Links und Phishingkits

Mithilfe von Phishingkits und Automatisierungstools ist es jetzt einfacher und günstiger als je zuvor, große Mengen an neuen und bisher unbekannten URLs zu erstellen. Auf diese Weise können Angreifer schädliche URL schon nach wenigen Minuten oder sogar Sekunden austauschen, sodass Sicherheitslösungen die Nachverfolgung erschwert wird.

Manipulierte Websites und SaaS-Plattformen

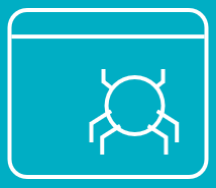
Angreifer können legitime Websites oder SaaS-Plattformen manipulieren und für Phishingangriffe ausnutzen, damit herkömmliche Funktionen zur Bedrohungserkennung sie als harmlos einstufen.

Unzulänglichkeiten herkömmlicher Sicherheitslösungen

bei modernen Angriffsmethoden

Viele Unternehmen setzen noch auf ältere Methoden wie Daten aus Webcrawlern, um moderne komplexe und gut getarnte Bedrohungen abzuwehren, und fallen dadurch leicht web-basierten Bedrohungen wie Phishingangriffen zum Opfer.

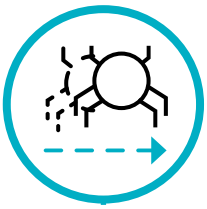
Diese älteren Methoden sind den neuen und unbekannten Bedrohungen nicht gewachsen. 2021 wurden **56 Millionen neue schädliche Webseiten** erstellt, daher ist es kaum verwunderlich, dass **93 % der Unternehmen 2021 Opfer eines Phishingangriffs** wurden. Nachfolgend finden Sie einige Gründe, weshalb herkömmliche Websicherheitslösungen Schwierigkeiten haben, mit modernen Bedrohungen Schritt zu halten.



Was ist ein Webcrawler?

Ein Webcrawler ist eine Art Bot, der das World Wide Web durchsucht, Websites indexiert und eine Liste aller Webseiten erstellt, die dann in die Suchergebnisse aufgenommen werden können.

Auf der nächsten Seite sind drei Gründe aufgeführt, weshalb herkömmliche Websicherheitslösungen Schwierigkeiten haben, mit modernen Bedrohungen Schritt zu halten.



Webcrawler sind zu langsam

Die Suchvorgänge und Analysen von Webcrawlern sind für die schnellen und gut getarnten modernen Bedrohungen einfach zu langsam. Angreifer nutzen Automatisierungstools und Verschleierungstechniken, um schnell zahlreiche neue Webseiten zu erstellen und herkömmliche Abwehrmaßnahmen zu umgehen. Gelangen diese Bedrohungen ins Netzwerk, weil Unternehmen sie nicht abwehren konnten, drohen gravierende Schäden.

Herkömmliche URL-Filterdatenbanken können nicht skaliert werden

Herkömmliche Websicherheitslösungen haben sich überwiegend auf URL-Filterdatenbanken verlassen, in denen die von den Webcrawlern erfassten Daten gespeichert werden, um den Zugriff auf schädliche Websites, einschließlich Phishingwebsites, zu verhindern. Doch da die Webcrawler so langsam sind, enthalten die Datenbanken veraltete Informationen und eignen sich nicht, um neue und gut getarnte Bedrohungen in Echtzeit abzuwehren.

Ein Großteil des Netzwerkverkehrs ist verschlüsselt

Da ein Großteil des Netzwerkverkehrs heutzutage verschlüsselt ist, können Angreifer ihre schädlichen Aktivitäten relativ einfach verbergen. Obwohl für 99 % der Chrome-Browsersitzungen HTTPS verwendet wird, bieten die meisten Websicherheitslösungen keine SSL/TLS-Entschlüsselung, da für die Entschlüsselung, Analyse und erneute Verschlüsselung des Datenverkehrs eine hohe Rechenleistung erforderlich ist. Ohne die richtige Technologie kann es dann zu erheblichen Leistungseinbußen im Netzwerk kommen. Da Unternehmen ihren Datenverkehr nicht entschlüsseln, werden sie leicht Opfer von Phishingangriffen und anderen Bedrohungen. **83 % der Phishingwebsites nutzen inzwischen SSL-Verschlüsselung, um schädliche Aktivitäten vor Netzwerkscannern zu verbergen.**

Die besten Methoden zur Erfassung getarnter und unbekannter Bedrohungen

Bei der Suche nach der besten Websicherheitslösung für Ihr Unternehmen sollten Sie unbedingt darauf achten, dass der gewählte Anbieter geeignete Tools und Methoden zur Abwehr moderner Bedrohungen bietet.

Was ist der „Patient Zero“?

„Patient Zero“ bezeichnet die erste Person oder das erste System, die Opfer einer bisher unbekannten Cyberattacke werden. Wenn das Unternehmen über einen Sicherheitsvorfall informiert wird, muss dieses Gerät schnellstmöglich isoliert werden, um eine Ausbreitung zu verhindern.

5 wichtige Funktionen
für moderne Websicherheit

Daten und Bedrohungserkennung

Für moderne Websicherheit müssen die Erkennungsfunktionen auf riesigen Mengen an Bedrohungsdaten basieren. Damit werden Modelle für das maschinelle Lernen trainiert, die dann potenzielle Bedrohungen präzise analysieren und zuverlässig erkennen können – ganz ohne Interventionen von Analysten oder Umwandlung von Rohdaten (Feature Engineering).

Analyse des Datenverkehrs in Echtzeit

Datenverkehr muss inline analysiert werden, damit schädliche Inhalte sofort erfasst werden, wenn sie in das Netzwerk gelangen. Auf diese Weise können auch neue und unbekannte Bedrohungen aufgedeckt werden, da die Verschleierungs-techniken bei der Echtzeitanalyse nicht funktionieren.

Durchsetzung in Echtzeit

Die Bedrohungen müssen nicht nur erfasst werden, sobald sie ins Netzwerk gelangen, sondern auch sofort gestoppt werden, um eine Erstinfektion zu verhindern. Eine Sicherheitslösung muss den Datenverkehr zur Analyse in die Cloud leiten und dann in Echtzeit eine Einschätzung empfangen können.

Cloud-Analysen und hohe Rechenleistung

Modelle für das maschinelle Lernen können in Millisekunden Ergebnisse ermitteln und eine Einschätzung in Echtzeit bereit-stellen, um Erstinfektionen zu verhindern, doch dafür ist eine sehr hohe Rechenleistung erforderlich.

URL-Datenbanken mit unmittelbaren Updates

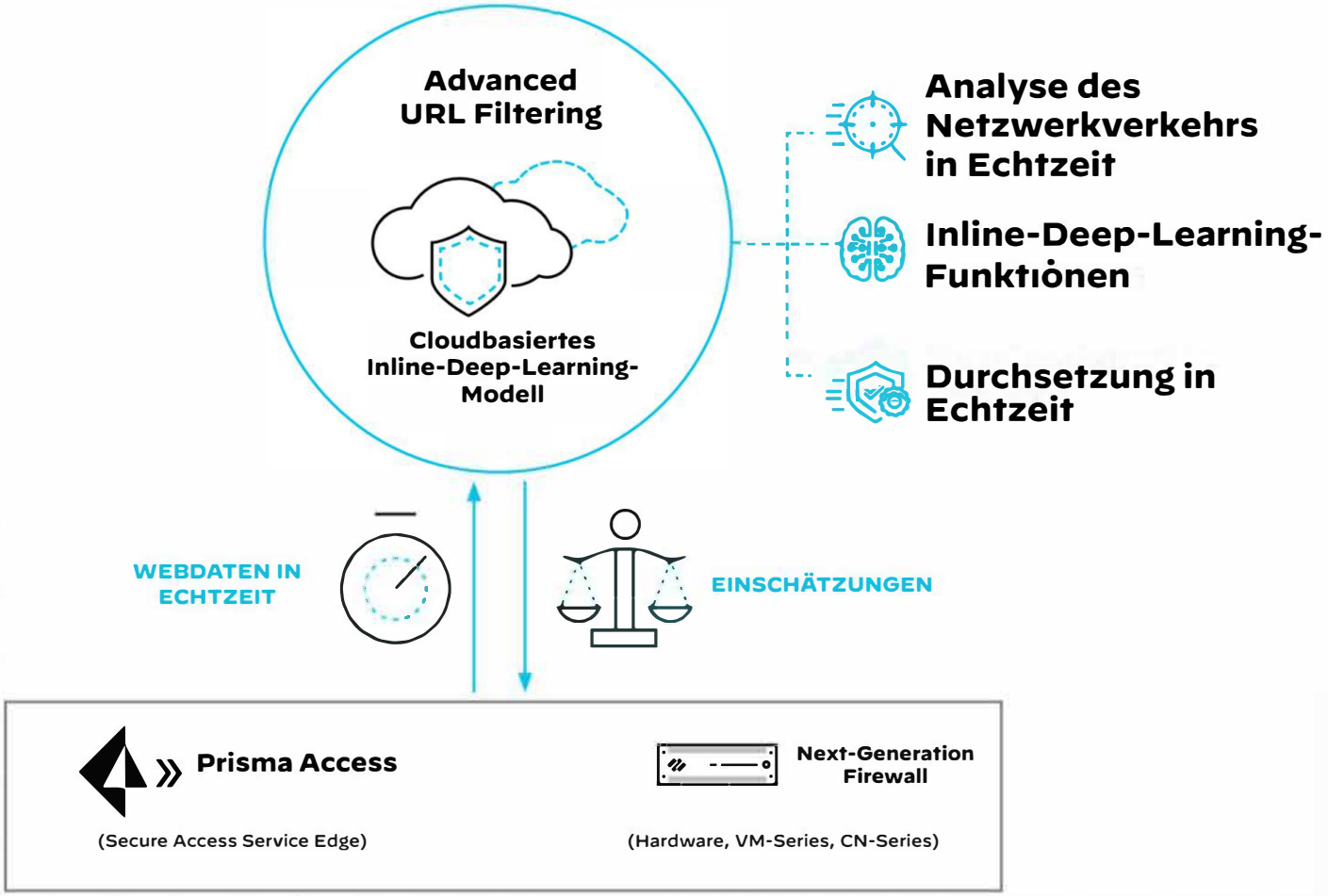
Zur Verbesserung der Websicherheit ist ein neuer Ansatz erforderlich. Statische Datenbanken sind nur ein Teil der Lösung. Letztendlich ist ein cloudbasierter Service notwendig, der mithilfe von Modellen für das maschinelle Lernen Einschätzungen von Daten in Echtzeit vornehmen und dadurch auch komplexe und neue Angriffstechniken abwehren kann.

Prisma Access Cloud SWG

Advanced URL Filtering

Prisma Access Cloud SWG nutzt Advanced URL Filtering von Palo Alto Networks, um unbekannte und komplexe webbasierte Bedrohungen in Echtzeit abzuwehren.

Dank unserer Inline-Deep-Learning-Technologie ist Advanced URL Filtering die branchenweit einzigartige Websicherheitslösung, die moderne Bedrohungen in Echtzeit abwehren und damit die Infektion des „Patient Zero“ verhindern kann. Sie **wehrt 40 % mehr Bedrohungen** als herkömmliche Webfilterungsdatenbanken ab.



Was ist Deep Learning?

Deep Learning ist eine Form von maschinellem Lernen mit mehrschichtigen, künstlichen neuronalen Netzwerken, die nicht speziell von Datenanalysten zusammengestellt werden müssen, und kann aus den beobachteten Sicherheitsereignissen lernen.

Analyse des Netzwerkverkehrs in Echtzeit

Analysiert den Datenverkehr am Netzwerkrand in Echtzeit, statt sich auf nachträgliche Analysen zu verlassen, und kann daher Bedrohungen unmittelbar abwehren.

Erkennung getarnter Bedrohungen

Analysiert den Netzwerkverkehr in Echtzeit (und nicht nur die Daten von Webcrawlern) und kann daher mehr getarnte und gezielte Angriffe aufdecken.

Zuverlässiger Schutz

Wehrt bekannte und unbekannte getarnte, webbasierte Bedrohungen in Echtzeit ab und verhindert so die Erstinfektion.

40 %

besserer Schutz vor Bedrohungen als herkömmliche Webfilterungsdatenbanken

88 %

der schädlichen URLs mindestens 48 Stunden vor anderen Anbietern abgewehrt

11,5 Mio.

schädliche URLs pro Tag erkannt

Bessere Websicherheit mit paloalto NETWORKS

Prisma Access Cloud SWG mit Advanced URL Filtering stoppt nicht nur die bestens getarnten und komplexesten Cyberattacken, sondern strafft auch die Prozesse und verbessert die Benutzererfahrung. Filialen, Homeoffices und mobile Mitarbeiter können unabhängig von ihrem Standort sichere Verbindungen zum Internet und zu allen geschäftskritischen Apps herstellen – und zwar mit derselben zuverlässigen Sicherheit wie im Hauptsitz.

Prisma Access Cloud SWG

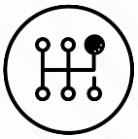
KI- und ML-gestützte Internet- und SaaS-Sicherheit

Zur Website

Cloud SWG und Webproxy-Appliances im Vergleich

Beide Lösungen im direkten Vergleich

Infografik herunterladen



Ultimativer SASE-Test

Erleben Sie unsere Lösung in Aktion

Jetzt anmelden

Modernize Your SWG with SASE (Modernisierung des SWG mit SASE)

Ein Whitepaper der ESG

Herunterladen

QUELLEN:

- 90 % der 2021 gemeldeten Sicherheitsvorfälle sind auf Phishing zurückzuführen.
- Die gesamte Weltbevölkerung sendet 197,6 Millionen E-Mails, gibt $1,6 Millionen bei Online-käufen aus und lädt fast 415.000 Apps herunter.
- Mitarbeiter nutzen im Durchschnitt 75 % ihres Arbeitstags einen Webbrowser.
- Die durchschnittlichen Kosten eines Phishingangriffs beliefen sich auf $14,8 Millionen.
- 93 % der Unternehmen wurden 2021 Opfer eines Phishingangriffs.
- 83 % der Phishingwebsites nutzen SSL-Verschlüsselung.
- 90 % der Phishingkits beinhalten Verschleierungsfunktionen.
- Pro Tag werden 3,4 Milliarden Phishing-E-Mails gesendet.

www.paloaltonetworks.de

Oval Tower, De Entrée 99–197
1101 HE Amsterdam, Niederlande

Zentrale: +31 20 888 1883
Vertrieb: +800 7239771
Support: +31 20 808 4600