Lieferketten im Fadenkreuz: Fünf Abwehrmethoden für die nächste große Cyberattacke

Die SolarWinds-Attacke war keine Ausnahme

In weniger als einem Jahr wurden Unternehmen weltweit Opfer mehrerer gravierender Angriffe. Diverse Microsoft Exchange Server-Exploits und Ransomwareangriffe auf Kaseya VSA und zahlreiche weitere Unternehmen sind nur einige Beispiele. Hackergruppen wie die mutmaßlichen Kaseya VSA-Angreifer REvil nutzen aus, dass Kryptowährungen an Wert gewinnen, und nehmen bei ihren neueren Ransomwarekampagnen ein breiteres Spektrum sekundärer Ziele ins Visier. Da Cyberattacken inzwischen regelmäßig Schlagzeilen machen, sollten sich Unternehmen so schnell wie möglich um einen effektiven Schutz ihrer Netzwerke kümmern.

In diesem Whitepaper geben wir Empfehlungen und Tipps, wie Sie Schwachstellen und das Bedrohungsrisiko in Unternehmensumgebungen verringern und Lieferketten besser schützen können.

Einleitung

Die digitale Transformation hat dazu geführt, dass Unternehmen mit zahlreichen Technologie- und Softwareanbietern arbeiten, ihre Lieferketten ausbauen, um die Produktivität zu steigern, und neue Technologien implementieren, um das Wachstum und die Effizienz zu fördern. Cyberkriminelle sehen das Vertrauensverhältnis zwischen Unternehmen und deren Zulieferern als potenzielles Einfallstor: Sie greifen zunehmend Softwarelieferketten an, um sich von dort aus Zugriff auf das Unternehmensnetzwerk zu verschaffen. Mitunter verschaffen Angreifer sich sogar Zugang zum digitalen Signiervorgang eines Anbieters, um die Abwehrmaßnahmen der Opfer zu umgehen.

Die Bedrohung für die Softwarelieferkette wird zusätzlich durch die aktuellen Herausforderungen verschärft, denen Sicherheitsteams gegenüberstehen. Ein Beispiel ist die regelrechte Flut an unzusammenhängenden Sicherheitsalarmen, in denen die zur Auswahl geeigneter Gegenmaßnahmen erforderlichen Kontextinformationen fehlen. Aus diesem Grund ist es so wichtig, dass Unternehmen Tools für die Bedrohungserkennung und -abwehr mit integrierten Funktionen für das maschinelle Lernen implementieren, die gezielt nach schädlichen Verhaltensweisen suchen und dabei auch vertrauenswürdige Anbieter nicht außer Acht lassen.

Des Weiteren sollte ein Zero-Trust-Framework für die Netzwerkarchitektur ausgearbeitet werden, damit Unternehmen von traditionellen Sicherheitsfunktionen am Netzwerkrand zu einem auf kontinuierlichen Prüfungen basierenden Modell wechseln können.

Unsere Branche muss die Angriffe versierter Hacker kontern

Im März 2020 versendete SolarWinds ein planmäßiges Softwareupdate, in das Hacker unbemerkt Malware eingeschleust hatten, an 33.000 Orion®-Kunden im privaten und öffentlichen Sektor. Etwa 18.000 davon installierten das Update, das daraufhin Probleme in mehreren Abteilungen des Pentagon, dem US-amerikanischen Außenministerium, Energieministerium, Ministerium für Innere Sicherheit, Finanzministerium, der National Nuclear Security Administration und bei mehreren Anbietern von Cybersicherheitslösungen verursachte. Die Nachwirkungen sind bis heute zu spüren, da Unternehmen und US-amerikanische Behörden immer noch mit Post-Mortem-Analysen beschäftigt sind.

Diese Angriffe unter Ausnutzung von SolarWinds verdeutlichen die Ausmaße, die ein komplexer Angriff auf eine Lieferkette annehmen kann. Da Unternehmen die SolarWinds-Software und -Server zur Verwaltung von zahlreichen Netzwerken, Systemen und IT-Infrastrukturen nutzen, konnten sich die Angreifer einen unglaublich weitreichenden Zugriff verschaffen. Allgemeinen Schätzungen zufolge blieb der Angriff etwa zehn Monate lang unbemerkt.

SolarWinds gab bekannt, dass ein Angreifer Schadcode in ein korrekt signiertes SolarWinds-Softwareupdate eingeschleust hatte. Nachdem das Update installiert wurde, agierte der Schadcode äußerst vorsichtig und im Verborgenen. Bei diesem Angriff war die Malware SUNBURST etwa zwei Wochen lang inaktiv und sandte erst dann ein ping an eine Subdomain von avsvmcloud[.]com – dem Command-and-Control-Server (C2) für die Backdoor –, um weitere Befehle und zusätzliche Schadcodes zu erhalten. Einige der größten und modernsten Unternehmen und Behörden der USA entdeckten SUNBURST auf ihren Produktionsservern, wodurch vertrauliche Daten in Gefahr gerieten.

Ein interessanter Aspekt dieses Angriffs ist die Frage, wie die Hacker sich so lange unbemerkt in der Infrastruktur aufhalten und dabei die nächsten Unternehmen in der Kette infizieren konnten, wobei der meiste Datenverkehr legitim wirkte. Tatsächlich stuften 72 von 72 Lösungen für die Malwareerkennung die avsvmcloud[.]com-Domain als harmlos ein.

Da SolarWinds so eine wichtige Rolle bei der IT-Automatisierung spielt, konnten die Hacker die strategische Position und die Verbindungen der Lösung nutzen, um sich nahezu auf alle Bereiche der Kundenumgebungen Zugriff zu verschaffen. Dazu manipulierten sie die SAML-Infrastruktur und verwendeten modifizierte SAML-Zertifikate, um sich weiter auszubreiten und sensible Daten in E-Mails abzurufen. Eine Methode zur Bedrohungserkennung war allerdings erfolgreich: Sie basierte auf der Identifizierung von Verhaltensanomalien oder Techniken, die häufig von bekannter Malware und Exploitkits genutzt wurden. Genau so ging Cortex XDR vor.

„Angreifer haben kürzlich versucht, Cobalt Strike auf einen unserer SolarWinds-IT-Server herunterzuladen. Cortex XDR hat diesen Versuch mithilfe unseres Moduls zur verhaltensbasierten Bedrohungserkennung sofort blockiert und das SOC konnte daraufhin den Server isolieren, den Vorfall untersuchen und die Infrastruktur absichern. Außerdem haben wir eine Reihe von Gefahrenindikatoren in die kundeneigenen Palo Alto Networks-Produkte eingebunden.“

Nikesh Arora, CEO, Palo Alto Networks

Am 17. Dezember 2020 gab Nikesh Arora, CEO von Palo Alto Networks, bekannt, dass die interne Cortex XDR dank ihres Moduls zur verhaltensbasierten Bedrohungserkennung eine DNS-Anfrage des SolarWinds Orion-Servers blockiert hatte. Daraufhin konnte das SOC-Team von Palo Alto Networks den Server isolieren und eine Untersuchung starten. Es kam zu dem Schluss, dass dank Cortex XDR der Angriff erfolglos verlief, keine Daten kompromittiert wurden und die Infrastruktur weiterhin sicher war.

Die Funktionen zur Verhinderung, Erkennung und Abwehr von Bedrohungen sowie der Einsatz von maschinellem Lernen und KI für die automatische Integration von Endpunkt-, Netzwerk- und Cloud-Daten ermöglichten die Abwehr dieses beispiellosen Angriffs.

Die Anzahl und das Ausmaß von Angriffen auf Lieferketten steigen weiter an. Cybersicherheitsteams sehen sich staatlich gesponserten Hackergruppen gegenüber, die finanziell extrem gut aufgestellt sind und zielgerichtet und diszipliniert arbeiten. Sie verschaffen sich Zugriff auf die Umgebungen der Opfer, sorgen für langfristige Persistenz und verfolgen diverse Ziele, unter anderem den Diebstahl von Daten. Derartig komplexe Kampagnen lassen sich nur mit neuen Methoden und Technologien abwehren und gleichzeitig müssen die Unternehmen den Hackern stets einen Schritt voraus sein. Doch die gehen jeden Tag hartnäckiger und forscher vor und planen immer raffiniertere Angriffe, bei denen sie die Möglichkeiten der Cloud und der Automatisierung für ihre Zwecke ausnutzen. Diesen Methoden sind ältere Technologien und Risikomanagementansätze einfach nicht gewachsen.

Unternehmen müssen sich jetzt auf die nächste große Attacke vorbereiten

An dieser Stelle muss daran erinnert werden, dass die zu große Abhängigkeit vieler Security Operations Center (SOCs) von menschlichen Eingriffen und einer ganzen Palette voneinander isolierter Sicherheitslösungen schon vor dem SolarWinds-Angriff bekannt war. Analysten standen unter enormem Druck und konnten die Flut an Alarmen aus den zahlreichen bereitgestellten Produkten kaum bewältigen. Die meisten Unternehmen setzen immer noch auf die manuelle Prüfung von Hinweisen auf potenzielle Angriffe, obwohl jede Woche Dutzende Sicherheitslösungen Zehntausende Alarme ausgeben, die alle äußerst wichtig erscheinen. Bei der manuellen Untersuchung und Abwehr von Bedrohungen müssen zahlreiche Kontextinformationen (Angaben zu Endpunkt, Benutzer und Zeit der mutmaßlichen Angriffsaktivitäten) gesucht und eine Vorfallsanalyse (Ereignisse im Zusammenhang mit dem Hostnamen und der IP-Adresse, dem Datenverkehr, der Domain, der genutzten Anwendungen usw.) durchgeführt werden. Da dies in der Regel sehr zeitaufwendig ist, bleiben die Auswertungen unvollständig und die Sicherheitsmaßnahmen sind nicht effizient.

> Laut einer 2019 durchgeführten Umfrage unter CISOs mussten mehr als 41 Prozent der Befragten jeden Tag auf über 10.000 und einige (eigenen Angaben zufolge) sogar auf mehr als 500.000 Alarme reagieren.
>
> Aus demselben Bericht geht hervor, dass sich lediglich 24 Prozent der untersuchten Alarme als tatsächliche Bedrohung erwiesen, während es 2018 noch 34 Prozent waren. Darüber hinaus sei der Anteil der erfolgreich abgewehrten realen Bedrohungen zwischen 2018 und 2019 von 51 auf 43 Prozent gesunken.[1]

Viele Unternehmen setzen zudem veraltete Sicherheitslösungen wie alte Antivirenprodukte, EDR-Lösungen (Endpoint Detection and Response) und andere Sicherheitstechnologien ein, sodass die Risiken sogar noch größer sind. Völlig überfordert von der Menge an irrelevanten Daten ändern viele Analysten die Einstellungen der Sensoren oder ignorieren bestimmte Alarme, wodurch natürlich das Risiko steigt. Viele Alarme werden als False Positives eingestuft, da der Kontext fehlt und somit eine intensivere Untersuchung unnötig erscheint. Doch in Zusammenhang mit anderen Ergebnissen aus weiteren Datenquellen können diese Informationen entscheidend dazu beitragen, die schädlichen Folgen und Absichten hinter scheinbar harmlosen Aktivitäten zu erkennen.

Damit die SOCs effizient arbeiten können, müssen veraltete, isolierte Sicherheitstools durch integrierte Lösungen mit zuverlässigen Analysen, maschinellem Lernen und automatisierten Erkennungsfunktionen ersetzt werden, um die Reaktionszeiten zu verkürzen und die Genauigkeit zu verbessern. Durch die Integration der richtigen Tools mit relevanten und konsolidierten Daten können Unternehmen schneller reagieren, sich dank detaillierter Kontextinformationen einen umfassenden Überblick über die Vorfälle verschaffen und letztendlich effizientere Untersuchungen durchführen.

Wie soll es also weitergehen? Wie können sich Unternehmen und Organisationen auf den nächsten Angriff auf Lieferketten und die sich ständig verändernden Bedrohungen vorbereiten, die ihnen in Zukunft drohen?

Erwägen Sie die folgenden fünf Maßnahmen – von Cyberrisikobewertungen bis zur Entwicklung einer weiter gefassten Security-Operations-Strategie – und deren mögliche Auswirkungen auf bestimmte Aktivitäten in Ihrem Unternehmen.

1. *Anticipating the Unknowns*, Cisco, März 2019, https://ebooks.cisco.com/story/anticipating-unknowns/page/6/6.

1. Ermittlung der Angriffsfläche

Wenn Mitarbeiter, Partner und Anbieter außerhalb des Unternehmensnetzwerks arbeiten, sind die internen Systeme anfälliger für Angriffe und Datendiebstahl. Abhilfe schaffen unter anderem Penetrationstests, Schwachstellenscans und eine neue Technologie – das Angriffsflächenmanagement (Attack Surface Management, ASM).

Überblick über das Angriffsflächenmanagement

Laut dem SANS Technology Institute ist das Angriffsflächenmanagement …

> „… eine neue Kategorie von Lösungen, die Unternehmen durch die Vermittlung der Außenperspektive der eigenen Angriffsfläche unterstützen. Die Angriffsfläche eines Unternehmens besteht aus allen über das Internet zugänglichen und für Angreifer erkennbaren Assets (Hardware, Software, SaaS und Cloud). Ihre Angriffsfläche besteht also aus allen externen Assets, die ein Angreifer finden, angreifen und ausnutzen könnte, um Ihre Umgebung zu infiltrieren."[2]

Das SANS Technology Institute nennt einige gängige Anwendungsszenarien für ASM-Lösungen, darunter:

- Identifizierung von Einfallstoren und Transparenzlücken
- Erfassung unbekannter Assets und der Schatten-IT
- Risikomanagement rund um die Angriffsfläche
- Risikobasierte Priorisierung von Sicherheitslücken
- Bewertung der Risiken durch Fusionen, Firmenübernahmen und Tochtergesellschaften

Unabhängig davon, ob Unternehmen sich für ASM-Lösungen entscheiden oder lieber Penetrationstests oder Schwachstellenscans durchführen, müssen die produktbezogenen und operativen Anforderungen geklärt werden, zum Beispiel in Bezug auf die Funktionalität, die Funktionen, die Eigenschaften und Evaluierungskriterien, um die jeweils beste Lösung zu finden.

2. Größtmögliche Prävention

Trotz zahlreicher verfügbarer Sicherheitslösungen gibt es immer noch Cyberattacken, die zudem immer komplexer werden (und offenbar besser finanziert sind).

Allerdings werden bei vielen großen Angriffen relativ einfache Angriffsvektoren eingesetzt, zum Beispiel eingebettete Malware, Phishing-E-Mails und die Ausweitung von Zugriffsrechten. Daher sollten Technologien und Best Practices für eine umfassende Prävention genutzt werden, damit Sie sich auf die kritischen Punkte konzentrieren können.

Grundlagen für die Prävention

- Investieren Sie in den Schutz Ihrer Endpunkte. EPPs (Endpoint Protection Platforms) nutzen verschiedene Präventionstechniken, zum Beispiel statische Analysen zur Evaluierung potenzieller Malware durch die Untersuchung von Dateien, heuristische Regeln zur Blockierung von Exploits und Verhaltensanalysen zur Evaluierung der Schädlichkeit der Dateien je nach Funktion.
- Egal, ob sie in einer Entwicklungs-, QA- oder Produktionsumgebung bereitgestellt wird, Sie benötigen in jedem Fall eine integrierte Sicherheitslösung, mit der Sie Daten zu Schwachstellen an bereits vorhandene Tools, wie Bugtracker, senden und die Fehlerbehebung beschleunigen können.
- Verwenden Sie starke Passwörter. Schon ein Passwort mit mindestens zehn Stellen trägt entscheidend zu einer größeren Sicherheit bei. Ändern Sie Ihr Passwort zwei- bis dreimal im Jahr, selbst wenn Sie nicht gezielt dazu aufgefordert werden.
- Sorgen Sie dafür, dass Ihre Sicherheitssoftware auf dem neuesten Stand ist. Installieren Sie regelmäßig Patches.
- Beschränken Sie den Netzwerkzugriff auf vertrauenswürdige Hosts und Netzwerke. Beschränken Sie den Internetzugriff auf die erforderlichen Netzwerkdienste. Sofern nicht unbedingt nötig, implementieren Sie keine Systeme, die direkt vom Internet aus zugänglich sind. Falls Remotezugriff erforderlich ist, sollten Sie VPN, SSH oder andere sichere Zugriffsmethoden verwenden.
- Phishingangriffe und sonstige E-Mail-basierte Bedrohungen lassen sich am besten abwehren, wenn Ihre Mitarbeiter über die aktuellen Best Practices und Richtlinien informiert sind, wie das Löschen verdächtiger Anhänge.
- Verwenden Sie die Multifaktor-Authentifizierung (MFA), sofern möglich.
- Konfigurieren Sie Ihre Spamfilter für den höchsten Schutz.

2. Pierre Lidome, „The SANS Guide to Evaluating Attack Surface Management", SANS Institute, 26. Oktober 2020, https://www.sans.org/reading-room/whitepapers/analyst/guide-evaluating-attack-surface-management-39905.

Viele Sicherheitsvorfälle werden durch eine Kombination aus menschlichen Fehlern, nicht gepatchten Systemen und der Hartnäckigkeit der modernen Angreifer ermöglicht, die auch eine Art digitale Transformation durchlaufen haben und diese zu ihrem Vorteil nutzen.

Fall Sie vermuten, einem Angriff zum Opfer gefallen zu sein, sollten Sie wie folgt vorgehen:

- Wenn nur wenige Systeme betroffen sind, trennen Sie diese sofort (physisch) von dem internen Netzwerk, um eine Ausbreitung zu verhindern. Falls dies nicht möglich ist oder zu viele Systeme infiziert wurden und Sie keine starken Ausgangsfilter für die Firewall und Proxyserver implementiert haben, sperren Sie sofort den gesamten ausgehenden Datenverkehr an externe Netzwerke.
- Implementieren Sie Filter auf internen Routern, Firewalls und sonstigen Netzwerkgeräten, um die infizierten Bereiche zu isolieren und den Netzwerkverkehr zu überwachen. Auf diese Weise können Sie feststellen, ob Sie den Angriff eingegrenzt haben oder ob er sich weiter ausbreitet und welche Hosts betroffen sind.
- Überwachen Sie den gesamten Netzwerkverkehr, um mehrschichtige Angriffe zu erkennen.
- Prüfen Sie die entsprechenden Logdateien, um festzustellen, wann das erste System infiziert wurde und welcher Angriffsvektor zum Einsatz kam.
- Ermitteln Sie unbedingt, ob ein infiziertes System eine Website aufgerufen hat und ob Daten ausgeschleust und offengelegt wurden.

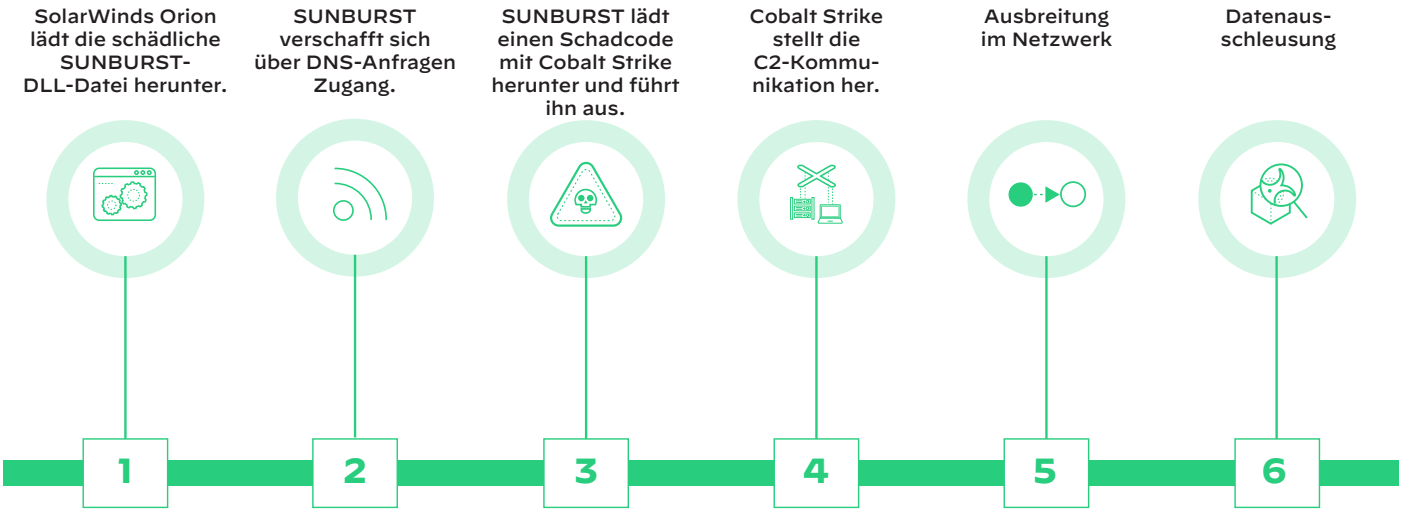

Abbildung 1: Der SolarStorm-Angriff wurde von Cortex XDR in der dritten Phase blockiert.

Mit Cortex XDR sparen Sie Zeit und Geld, da Sie keine eigene globale Sicherheitsinfrastruktur für Ihre Endpunkte aufbauen müssen. Dank der einfachen Bereitstellung, die weder Serverlizenzen und Datenbanken noch andere Infrastrukturkomponenten voraussetzt, können Unternehmen ihre Endpunkte schnell schützen.

3. Umfassende Transparenz

Mithilfe von Unternehmenstransparenz und einem einheitlichen Ansatz für die Daten in der gesamten Lieferkette können Sie sich einen umfassenden Überblick über die Anwendungen und Infrastruktur verschaffen. Das kann auch Telemetriedaten von Endpunkten, Netzwerken und Cloud-Umgebungen einschließen. Zudem müssen die Daten aus den verschiedenen Quellen zusammengeführt und Beziehungen zwischen den unterschiedlichen Ereignissen erkannt werden, um anhand des Kontexts zu ermitteln, ob ein bestimmtes Verhalten verdächtig ist.

Telemetrie- und Forensikdaten in Kombination mit Algorithmen für das maschinelle Lernen ermöglichen einen detaillierten Überblick über den Angriffsverlauf und eine eingehende Analyse während der Ersteinschätzung und Verifizierung eines Alarms. So lassen sich Untersuchung und Reaktion vereinfachen und beschleunigen.

Bei dem SolarWinds-Angriff konnte die interne Cortex XDR von Palo Alto Networks dank des Moduls zur verhaltensbasierten Bedrohungserkennung verhindern, dass Cobalt Strike auf einen der SolarWinds-IT-Server heruntergeladen wurde, obwohl der nicht autorisierte Schadcode bereits in die Software des Anbieters eingebettet worden war (siehe Abbildung 1).

Haben Unternehmen einen umfassenden Überblick, können sie auch komplexe Angriffe wie den auf SolarWinds erkennen und in allen Phasen des Angriffsverlaufs abwehren (selbst wenn der Host bereits infiziert wurde). Sollten die Angreifer allerdings schon die Präventionsmaßnahmen umgangen haben, müssen Sie deren weitere Aktivitäten erkennen können.

4. Schnelle Reaktion

Die Hacker verschafften sich vermutlich im Januar 2019 Zugriff auf ein SolarWinds-System, doch der Zugang zur Infrastruktur wurde schon seit dem 13. Oktober 2017 im Exploit Cybercrime-Forum im Dark Web zum Verkauf angeboten. Das verdeutlicht, wie groß der finanzielle Anreiz ist, APT-Kampagnen durchzuführen.

Im März 2021 meldeten sowohl Microsoft als auch FireEye neue Gefahrenindikatoren, wie Backdoors und weitere eingeschleuste Malware für den persistenten Zugang zu den betroffenen Netzwerken. Laut Microsoft hatten sie …

> „… diese neuen Angriffstools und -funktionen in einigen infizierten Kundennetzwerken entdeckt und festgestellt, dass sie von August bis September 2020 genutzt wurden. Weitere Analysen haben ergeben, dass sie sich eventuell schon im Juni 2020 auf den betroffenen Systemen befunden haben. Diese Tools gehören zu einer neuen Malwarevariante, die bisher nur von dieser Gruppe verwendet wurde. Sie wurden speziell für bestimmte Netzwerke entwickelt und scheinen erst implementiert zu werden, nachdem sich der Angreifer mithilfe von gestohlenen Anmeldedaten oder der SolarWinds-Binärdatei Zugriff verschafft und mit TEARDROP und anderen Befehlen und Tastatureingaben im Netzwerk ausgebreitet hat.“[3]

Nachdem sich ein Hacker Zugang zu einem Netzwerk verschafft hat, muss er die Erkennungsfunktionen umgehen und für Persistenz sorgen, um seine Ziele zu erreichen. SolarStorm, die Hackergruppe hinter dem Angriff auf SolarWinds, nutzte gestohlene Anmeldedaten, um auf Cloud-Services zuzugreifen, und manipulierte Identitäten, um über VPNs und Remote Access Tools in Netzwerke einzudringen und sich dort festzusetzen.

Die wichtigsten Ziele sind daher die Verkürzung der Verweildauer (also die schnellere Erkennung von Angriffen) und die Verhinderung der darauf folgenden Ausbreitung im Netzwerk, um einen Angriff einzudämmen, abzuwehren und die Umgebung wiederherzustellen. Abgesehen von der potenziellen Rufschädigung, den Geldbußen für die Missachtung der Compliancevorgaben und dem Verlust kritischer Unternehmensdaten drohen auch größere finanzielle Belastungen, je länger der Sicherheitsvorfall unerkannt bleibt.

In ihrem Bericht „Quantifying the Value of Time in Cyber-Threat Detection and Response“ merkte die Aberdeen Group an, dass bei einer Verweildauer von maximal sieben Tagen die Auswirkungen um 77 Prozent reduziert werden. Wird der Angriff schon nach einem Tag erkannt und blockiert, verringern sich die Auswirkungen sogar um 96 Prozent (siehe Abbildung 2).[4]

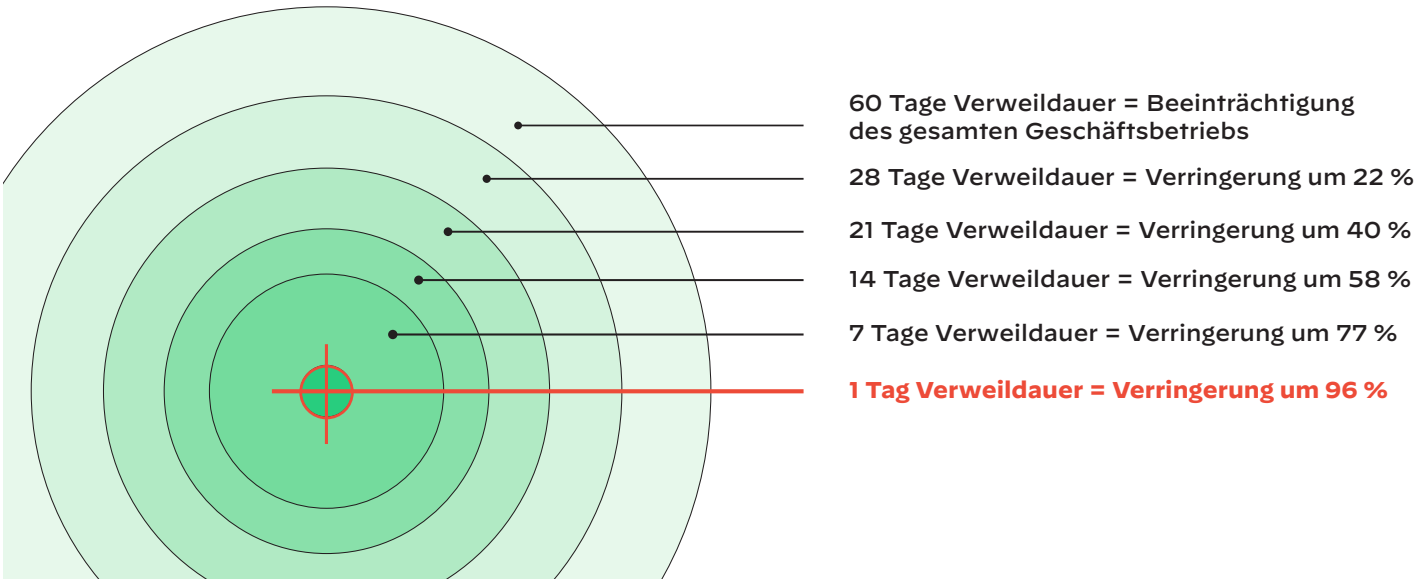

Abbildung 2: „Quantifying the Value of Time in Cyber-Threat Detection and Response“, Aberdeen Group, Februar 2016

3. Ramin Nafisi et al., „GoldMax, GoldFinger, and Sibot: Analyzing NOBELIUM's Layered Persistence“, 4. März 2021, https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/4.
4. Aberdeen Group, „Quantifying the Value of Time in Cyber-Threat Detection and Response“, Februar 2016.

Nicht nur für den Notfall ist es wichtig, zu wissen, wie schnell und wie oft Angreifer potenzielle Angriffsvektoren scannen und identifizieren. Die jüngsten Scanningtechnologien geben Hackern die Möglichkeit, ohne große Probleme Angriffsvektoren zu finden und ungenutzte, unautorisierte oder falsch konfigurierte Assets für Cyberattacken zu missbrauchen.

Im kürzlich erschienenen Cortex Xpanse-Bedrohungsbericht für Angriffsflächen für das Jahr 2021 mit Erkenntnissen von führenden globalen Unternehmen zu ASM-Lösungen von Palo Alto Networks werden die zentralen Ergebnisse aus der Untersuchung der über das Internet zugänglichen Angriffsflächen einiger der weltweit größten Unternehmen zusammengefasst. Von Januar bis März hat das Team Scans von 50 Millionen IP-Adressen der untersuchten 50 Großunternehmen ausgewertet und ermittelt, wie schnell Angreifer unsichere Systeme identifizieren können.

Dabei waren unter anderem folgende Punkte interessant:

- **Cyberkriminelle machen keine Pause.** Im ewigen Katz-und-Maus-Spiel führen Hacker jede Stunde einen Scan durch, wohingegen weltweit agierende Unternehmen zwischen einzelnen Scans oft mehrere Wochen verstreichen lassen.
- **Cyberkriminelle stürzen sich auf neue Sicherheitslücken.** Zwischen Januar und März haben Hacker innerhalb von 15 Minuten nach der Bekanntgabe neuer CVEs (Common Vulnerabilities and Exposures) und bereits in den ersten 5 Minuten nach der Sicherheitsaktualisierung für die Zero-Day-Sicherheitslücke in Microsoft Exchange Server die ersten Scans gestartet.
- **Kritische Sicherheitsprobleme stecken mehrheitlich in der Cloud.** 79 Prozent der gefährlichsten Sicherheitsprobleme wurden in den Cloud-Umgebungen der untersuchten Unternehmen festgestellt. Der vergleichsweise niedrige Anteil von 21 Prozent in On-Premises-Umgebungen bestätigt, dass cloudbasierte Dienste inhärent risikobehaftet sind.

MTTD (Mean Time to Detect) ist die Zeit, die ein Unternehmen benötigt, um einen potenziellen Sicherheitsvorfall aufzudecken.

MTTF (Mean Time to Failure) ist die Zeitspanne, die ein defektes System noch läuft, bevor es ausfällt.

MTTR (Mean Time to Respond) gibt an, wie lange ein Team braucht, um eine identifizierte Bedrohung zu isolieren, einzudämmen und zu beheben.

MTBF (Mean Time between Failures) spiegelt die Zuverlässigkeit und Verfügbarkeit eines Systems wider. Damit wird die Performance eines Systems unter vorab definierten Bedingungen in einem bestimmten Zeitrahmen evaluiert.

5. Einbindung der Zero-Trust-Prinzipien

Das Zero-Trust-Konzept gibt es schon eine Weile, aber es wurde erst 2009 wirklich anerkannt, als Forrester Research das „Zero-Trust-Modell" der Cybersicherheit vorstellte.[5] Es ist sowohl ein Architekturmodell für Netzwerke als auch ein Framework für Sicherheitsrichtlinien.

Ein Zero-Trust-Modell basiert auf der strikten Prüfung und Validierung aller Personen, Geräte oder Organisationen, die versuchen, auf Netzwerkressourcen zuzugreifen. Das vorrangige Ziel ist es, Manipulationen von Daten, Anwendungen und geschäftskritischen Systemen durch Angriffe und Exploits zu verhindern.

Alle Zero-Trust-Prinzipien sollen dabei helfen, die Bedrohungsrisiken zu verringern und den nicht autorisierten Zugriff zu verhindern. Sie wurden speziell entwickelt, um die Sicherheit kritischer Anwendungen und sensibler Daten in Unternehmen zu gewährleisten, und lassen sich ganz einfach in jede Sicherheitsstrategie integrieren. Zu den Prinzipien gehören unter anderem:

- **Least Privilege**: Mit dieser Richtlinie erhalten Endbenutzer nur minimale Zugriffsrechte, d. h. nur jene, die sie für ihre Arbeit benötigen. Dadurch wird die Zahl der Pfade reduziert, über die Angreifer in eine Infrastruktur eindringen, Malware ein- oder Daten ausschleusen können.
- **Mikrosegmentierung**: Das Netzwerk wird in separate Segmente oder in Rechenzentren oder Cloud-Umgebungen in „sichere Zonen" mit eigenen Anmeldedaten unterteilt, um die Workloads zu isolieren. Dadurch wird Eindringlingen zudem die Ausbreitung in internen Netzwerken beschränkt.
- **Multifaktor-Authentifizierung (MFA)**: Dabei müssen sich Einzelpersonen mit mehreren Sicherheitsverfahren authentifizieren. In der Regel handelt es sich um eine Kombination aus etwas, das man kennt (zum Beispiel ein Passwort oder eine PIN), etwas, das man besitzt (wie einen Handsender oder einen Ausweis) und physischen Merkmalen wie biometrischen Daten, der Stimme (bei der Spracherkennung) oder einem Fingerabdruck.

5. John Kindervag et al., „No More Chewy Centers: The Zero Trust Model of Information Security", 23. März 2016, https://www.forrester.com/report/No+More+Chewy+Centers+The+Zero+Trust+Model+Of+Information+Security/-/E-RES56682?objectid=-RES56682.

Für ausgereifte Zero-Trust-Funktionen sollten unter anderem folgende Punkte beachtet werden:

- Überwachen Sie alle Aktivitäten und erfassen Sie alle Daten – nicht nur verdächtige Ereignisse.
- Decken Sie Verhaltensanomalien mithilfe von Analysen und maschinellem Lernen auf.
- Erkennen und blockieren Sie schädliches Verhalten auf dem Endpunkt.
- Segmentieren Sie den Zugriff über eine Hostfirewall.
- Überwachen und beschränken Sie den Zugriff nicht autorisierter USB-Geräte mit den Funktionen zur Gerätekontrolle. Benutzer können dann grundsätzlich keine Speichergeräte mit den Computern verbinden. Ausnahmen sind für autorisierte Geräte und für eine begrenzte Zeit möglich.
- Blockieren Sie schädliche externe Hosts.
- Orchestrieren Sie die Sicherheitsfunktionen. Automatisierung und Orchestrierung können dabei helfen, Lücken in Zero-Trust-Architekturen aufzudecken und automatisch zu beheben oder Workflows zu starten, die die Analysten bei der Behebung unterstützen. Laut des Forrester-Berichts The Zero Trust eXtended (ZTX) Ecosystem sollten Punktlösungen vermieden und stattdessen integrierbare Produkte gewählt werden, die sich zu einem Netzwerk verknüpfen lassen und dadurch eine größere Transparenz und Kontrolle sowie eine zuverlässige Orchestrierung der Sicherheitsmaßnahmen ermöglichen.

Weitere Informationen zu der Zero-Trust-Strategie finden Sie hier:

- National Institute of Standards and Technology: Zero Trust Architecture: NIST Publishes SP 800-207
- The National Cyber Security Centre: Zero trust principles – beta release
- The National Security Agency: Embracing a Zero Trust Security Model
- Forrester Research: Five Steps To A Zero Trust Network* mit Tipps zur Implementierung einer effektiven Zero-Trust-Roadmap:
    1. Identifizieren Sie Ihre sensiblen Daten.
    2. Ermitteln Sie die Datenflüsse dieser sensiblen Informationen.
    3. Erstellen Sie einen Zero-Trust-Mikroperimeter.
    4. Überwachen Sie die Zero-Trust-Umgebung äußerst sorgfältig mithilfe von Sicherheitsanalysen.
    5. Vertrauen Sie auf Sicherheitsautomatisierung und -orchestrierung.

** Der Forrester-Bericht ist für Forrester-Abonnenten verfügbar und kann zudem käuflich erworben werden.*

Keine Geheimwaffe: Cortex XDR

Es gibt bereits eine effiziente Methode, um die oben aufgeführten Prinzipien in jede beliebige Sicherheitsstrategie zu integrieren. Moderne XDR-Plattformen (Extended Detection and Response) erfassen Daten von verschiedenen Quellen – Endpunkten, Servern, Cloud-Workloads und Netzwerken – und korrelieren sie automatisch, sodass Bedrohungen zeitnah erkannt werden und Sicherheitsanalysten schneller reagieren und die Vorfälle besser untersuchen können.

Cortex® XDR™ von Palo Alto Networks ist die branchenweit erste Extended-Detection-and-Response-Plattform, die Netzwerk-, Endpunkt- und Cloud-Daten nativ integriert, um komplexe Bedrohungen zu stoppen. So können Benutzer Netzwerk-, Endpunkt- und Cloud-Bedrohungen unmittelbar in einer Konsole abwehren.

Nur Cortex XDR kann Sicherheitsteams bei den folgenden Aufgaben unterstützen:

- **Automatische Erkennung verborgener Angriffe** für alle Angriffsvektoren mithilfe von Verhaltensanalysen der Netzwerk-, Endpunkt- und Cloud-Daten. Die Cortex XDR-Technologie ist darauf ausgerichtet, das Verhalten aller Geräte und Benutzer zu erlernen, um es dann mit den Verhaltensweisen anderer Geräte und Benutzer im Netzwerk des jeweiligen Unternehmens zu vergleichen. Anhand dieser Verhaltensprofile können Abweichungen vom bisherigen Verhalten, dem Verhalten von Kollegen oder dem erwarteten Verhalten eines Objekts erkannt werden.
- **Beschleunigung der Untersuchung** durch Zusammenführen von Telemetriedaten und Alarmen mehrerer Endpunkte und zusätzlicher Datenquellen in einem einzigen Sicherheitsvorfall, in dem die Ursache sichtbar wird. Durch diesen umfassenden Überblick über alle Datenquellen werden tote Winkel ausgeleuchtet, die Erkennungsquoten für komplexe Angriffe auf den diversen Datenebenen verbessert und zusätzliche Kontextdaten bereitgestellt, die die Untersuchungen vereinfachen. Außerdem müssen Kunden nicht so viele separate Lösungen für die Bedrohungserkennung und -abwehr verwalten.
- **Fortlaufende Anpassung der Abwehrmaßnahmen** durch Einbindung der Untersuchungsergebnisse zur Abwehr zukünftiger Bedrohungen. Analysten können schnell die Verbreitung von Malware verhindern, Endpunkte isolieren, Malware auf allen Endpunkten in Echtzeit löschen und sogar direkt auf Endpunkte zugreifen und Bedrohungen untersuchen, ohne die Benutzer zu stören.

Zusammenfassung

Angriffe wie bei SolarWinds sind ein deutliches Warnsignal für alle Cybersicherheitsexperten in allen Sektoren und Positionen. Sie zeigen, wie wichtig es ist, fortlaufend für einen umfassenden Schutz der Netzwerke vor persistenten und komplexen Bedrohungen zu sorgen. Während die Branche erst einmal aufatmet, Post-Mortem-Analysen durchführt und potenzielle Schäden des Angriffs behebt, müssen Unternehmen ihre Sicherheitsinfrastrukturen dringend stärken – denn die nächste große Attacke könnte schon morgen beginnen.

Hacker entwickeln bereits Techniken, die bisher unmöglich erschienen, und suchen nach kreativen Methoden, um verborgene Kampagnen durchzuführen und größtmöglichen Schaden anzurichten.

Daher wird es höchste Zeit, das Sicherheitsniveau mithilfe der zahlreichen modernen Sicherheitslösungen und Best Practices zu verbessern. Gehen Sie schrittweise vor und stellen Sie sicher, dass die Sicherheitsteams die richtigen Maßnahmen ergreifen, sich zum Beispiel einen besseren Überblick über die Angriffsfläche verschaffen, eine größtmögliche Prävention anstreben und die Zero-Trust-Prinzipien umsetzen.

Am einfachsten ist dies vermutlich mit einer Next-Generation-Lösung wie XDR, einer logischen Weiterentwicklung bewährter Technologien wie EDR. XDR bietet die erforderliche Transparenz und Kontrolle über die Geschäftskomponenten, da über Integrationen die EDR-Daten mit anderen Telemetriedaten kombiniert werden können.

XDR kann Datenströme für maschinelle Lernverfahren nutzen, die kontinuierlich besser werden, und die koordinierte Erkennung und Abwehr von Bedrohungen unterstützen. Dadurch bietet sie ein enormes Potenzial für eine effektive Abwehr von Hackern – jetzt und in Zukunft.

Sie möchten gern mehr über die neuen Funktionen für die Bedrohungssuche oder die Abwehrmaßnahmen von Cortex XDR erfahren? Dann buchen Sie einfach einen praktischen Workshop mit unseren Experten und/oder fordern Sie eine Cortex XDR-Demo an.

Weitere Ressourcen zu XDR

Laden Sie unser E-Book Ein Leitfaden zu XDR herunter.

Es steht ein Datenblatt zu Cortex XDR zur Verfügung.

Besuchen Sie auch unsere Cyberpedia-Seite: What is XDR?

Informationen zur 3. Runde der MITRE ATT&CK® Evaluations finden Sie in unserem E-Book.

Forrester Research hat uns im Bericht The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2020 als „Leader“ eingestuft. Klicken Sie einfach auf den Link, um den Bericht herunterzuladen.

paloalto NETWORKS

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

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

www.paloaltonetworks.de

cortex_wp_supply-chains-in-the-crosshairs_071221-de