SOPHOS
Cybersecurity evolved.

Minimieren Sie das Risiko von Supply-Chain-Angriffen: Best-Practice-Richtlinien

Im Dezember 2020 sorgte der Cybervorfall beim IT-Management-Unternehmen SolarWinds weltweit für Schlagzeilen und rückte auch Supply-Chain-Angriffe ins Rampenlicht. Dabei handelt es sich keineswegs um ein neues Phänomen. In einer von Sophos in Auftrag gegebenen Studie aus dem Jahr 2020 gaben 9 % der befragten 5.000 IT-Manager aus 26 Ländern an, dass Ransomware über vertrauenswürdige Drittanbieter ins Unternehmensnetzwerk eingeschleust wurde[1].

Worum handelt es sich bei Supply-Chain-Angriffen genau und wie laufen sie ab? Und wichtiger noch: Wie können Sie Ihr Unternehmen vor den Auswirkungen eines Supply-Chain-Angriffs schützen?

In unserem Whitepaper finden Sie Antworten auf diese Fragen.

1 The State of Ransomware 2020 – Sophos, 2020

Sophos-Whitepaper. April 2021

Was genau ist ein Supply-Chain-Angriff?

Viele Unternehmen lagern bestimmte Geschäftsprozesse (z. B. die Verwaltung ihrer IT-Infrastruktur) vollständig oder teilweise an externe Anbieter aus. Natürlich bringt es durchaus geschäftliche Vorteile für Unternehmen, Drittanbietern den Zugriff auf ihr Netzwerk zu gewähren (z. B. werden so interne Ressourcen freigesetzt). Doch dieser Schritt birgt auch Sicherheitsrisiken, da Unternehmen dadurch anfälliger für Supply-Chain-Angriffe sind.

Angriffe auf die Lieferkette zielen nicht direkt auf Ihr Unternehmen ab. Vielmehr fassen Cyberkriminelle in Ihrer Umgebung Fuß, indem sie den Zugang zu Ihrem Netzwerk nutzen, den Sie vertrauenswürdigen Drittanbietern gewährt haben. Ist Ihr Netzwerk erst kompromittiert, können die Angreifer zahlreiche schädigende Aktivitäten durchführen.

Auch wenn nur ein einziger Drittanbieter mit Ihrem Netzwerk verbunden ist, ist Ihr Unternehmen bereits anfällig für Supply-Chain-Angriffe. Im Schnitt gewähren kleine und mittelständische Unternehmen eigenen Angaben zufolge jedoch mindestens drei Drittanbietern Zugriff auf ihr Netzwerk[2]. Die Absicherung verbundener Drittanbieter stellt die IT vor enorme Herausforderungen und erhöht zudem die Arbeitsbelastung der IT-Teams. Hinzu kommt, dass Angriffe auf die Lieferkette bekanntermaßen schwer zu erkennen, geschweige denn abzuwehren sind, da sie von jedem Teil der Lieferkette ausgehen können.

Arten von Drittanbietern

Am häufigsten können sich Professional-Service- und IT-Serviceanbieter mit dem Netzwerk eines Unternehmens verbinden.

Professional Services

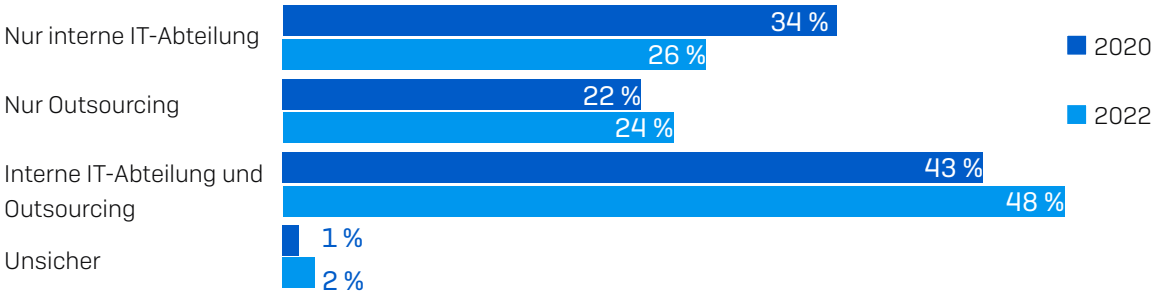
Unternehmen lassen bestimmte Geschäftsbereiche (oder Teile davon) häufig von Professional-Service-Anbietern verwalten, wenn sie intern nicht über die erforderliche Expertise verfügen. Ein Beispiel: Ein Wirtschaftsprüfungsunternehmen muss (über Software) auf sensible Finanzdaten zugreifen, um dem Kunden die gewünschten Analysen und Ergebnisse zu liefern. Wie Sie sich sicher vorstellen können, kann ein erfolgreicher Cyberangriff auf ein solches Unternehmen verheerende Folgen für seine Kunden nach sich ziehen.

IT-Serviceanbieter

Bei IT-Serviceanbietern handelt es sich um externe Unternehmen, die mit dem Betrieb der IT-Infrastruktur und/oder der IT-Security eines Unternehmens betraut werden. Sie werden häufig auch als Managed Service Provider (MSPs) oder Managed Security Service Provider (MSSPs) bezeichnet.

Da IT-Serviceanbieter Zugang zu vielen unterschiedlichen Unternehmen haben, sind sie ein besonders attraktives Ziel für Supply-Chain-Angriffe. Prognosen zufolge wird der Anteil der Unternehmen, die ihre IT-Security auslagern, bis 2022 auf 72 % steigen[3]: Die Sicherheitslage dieser Drittanbieter spielt also eine zentrale Rolle für Ihre eigene IT-Security.

Wie wird IT-Sicherheit im Unternehmen umgesetzt? Aktuell und in 2022



2,3 Cybersecurity: The Human Challenge, Sophos, 2020

Arten von Supply-Chain-Angriffen

Supply-Chain-Angriffe unterscheiden sich zwar in der Art und Weise, wie sie durchgeführt werden, aber die Grundprinzipien und Ziele sind oft die gleichen: Angreifer versuchen, vertrauenswürdige Drittanbieter zu infiltrieren, um deren Zugang für ihre Zwecke zu missbrauchen und Malware einzuschleusen, geistiges Eigentum zu stehlen oder die interne Kommunikation auszuspionieren.

Phishing-Angriffe

Phishing-E-Mails gehören zu den häufigsten Angriffsmethoden bei Supply-Chain-Angriffen. Angreifer zielen mit Phishing-E-Mails auf vertrauenswürdige Dritte ab, um deren Netzwerke zu kompromittieren und sich Zugang zu ihnen zu verschaffen. Sie nutzen diese als Sprungbrett, um in die Systeme der Kunden einzudringen.

Kompromittierte Software-Updates

Bei ausgeklügelteren Supply-Chain-Angriffen infiltrieren Hacker die Infrastruktur eines Softwareunternehmens bzw. Distributors und schleusen Schadcode in Software-Update-Pakete ein. Betroffene Drittanbieter verteilen diese Updates an ihre Kunden und infizieren sie dabei unwissentlich. Auch hier können die Folgen verheerend sein, besonders wenn das betroffene Unternehmen ein großes Kundenportfolio besitzt. Der SolarWinds-Vorfall im Dezember 2020 ist ein perfektes Beispiel für diese Art von Angriffen.

Case Study zu Supply-Chain-Angriffen: SolarWinds

Ende 2020 wurde bekannt, dass die Lieferkette des IT-Management-Unternehmens SolarWinds kompromittiert wurde. Dieser Vorfall sorgte weltweit für Schlagzeilen und rückte die Anfälligkeit von Lieferketten ins Rampenlicht. Schätzungen zufolge sind über 18.000 Kunden des Unternehmens betroffen.

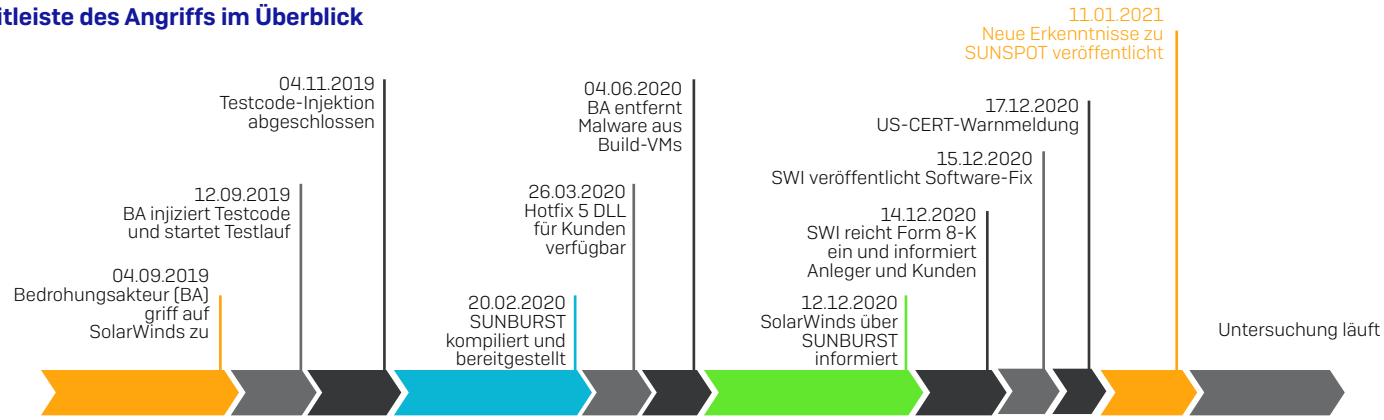
Wir möchten an dieser Stelle darauf hinweisen, dass die Untersuchungen zum SolarWinds-Angriff zum Zeitpunkt der Veröffentlichung unseres Whitepapers (April 2021) noch nicht abgeschlossen sind.

Wie gingen die Angreifer vor?

Kurz gesagt: Den Cyberkriminellen gelang es, Schadcode in SolarWinds Plattform Orion einzuschleusen – ein Tool zur Überwachung und Steuerung der Infrastruktur. Dieser Schadcode wurde dann unwissentlich über ein Standard-Software-Update an die Kunden von SolarWinds verteilt. Berichten zufolge installierten rund 18.000 Kunden (darunter auch Fortune-500-Unternehmen und US-Regierungsbehörden) das Update – und waren somit angreifbar.

Besorgniserregend ist, dass SolarWinds bereits im September 2019 Anzeichen verdächtiger Aktivitäten bemerkte, wie aus unserer Zeitleiste unten hervorgeht. Dies deutet auf einen kalkulierten Angriff hin. Außerdem ist davon auszugehen, dass die Hacker große Vorsicht walten ließen, um möglichst wenige Alarme auszulösen. Unsere umfassende Analyse darüber, wie die Malware-Variante Sunburst Abwehrmaßnahmen umgehen konnte, können Sie in den Sophos-News nachlesen.

Zeitleiste des Angriffs im Überblick



Änderungen sämtlicher Ereignis- und Datumsangaben sind bis zum Abschluss der SolarWinds-Untersuchung vorbehalten – https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

Wie hat sich der Angriff ausgewirkt?

Der unter dem Namen „Sunburst" bekannte Angriff ermöglichte Cyberkriminellen umfassenden Zugang zu Informationssystemen von staatlichen Einrichtungen und Unternehmen. Schon jetzt hat der Angriff zu Datendiebstahl bislang unbekannten Ausmaßes geführt. Außerdem wird befürchtet, dass die Angreifer noch unentdeckte Hintertüren in Unternehmensnetzwerke einbauen konnten.

Das globale Ausmaß des Angriffs hat deutlich gemacht, wie unvorbereitet viele Unternehmen sind, wenn es um die Abwehr von Angriffen auf die Lieferkette geht.

Poison Packages

Eine bislang weniger verbreitete Art von Supply-Chain-Angriffen, die sich jedoch in Zukunft vermutlich häufen wird, sind Poison Packages („vergiftete Pakete"). Mit der zunehmenden Nutzung der Clouds, Docker und agilen Entwicklungsmethoden kommen auch immer häufiger Standardkomponenten zum Einsatz, die den Entwicklungszyklus verkürzen. Vor diesem Hintergrund manipulieren Cyberkriminelle jetzt gängige Container, Librarys oder sonstige Ressourcen – in der Hoffnung, dass kompromittierte Pakete in Ihr Endprodukt integriert werden.

Tipps zur Abwehr von Supply-Chain-Angriffen

Supply-Chain-Angriffe sind komplex und vielschichtig und lassen sich mit Technologie allein nicht stoppen. Mit unseren Best-Practice-Richtlinien minimieren Sie jedoch die mit Supply-Chain-Angriffen einhergehenden Risiken.

1. Wechseln Sie von reaktiver zu proaktiver Cybersecurity

SolarWinds hat viele Unternehmen weltweit wachgerüttelt. Doch wenn ein Angriff bekannt wird, ist es häufig schon zu spät: Bis Cyberkriminelle ihre Payloads einschleusen, haben sie möglicherweise bereits kritische Daten gestohlen und greifen seit Tagen auf Ihr Netzwerk zu. So ist ein neuer Ansatz gefragt: Gehen Sie davon aus, dass Sie immer kompromittiert sind, und spüren Sie Bedrohungen proaktiv auf, bevor es zu spät ist. Technologien und Services, auf die wir später noch eingehen, können Sie dabei unterstützen.

2. Achten Sie auf frühe Anzeichen einer Kompromittierung

Unser „Sophos Managed Threat Response (MTR)"-Team beobachtet immer wieder die beiden folgenden Ereignisse als erste Anzeichen einer Kompromittierung: Zum einen die Nutzung von Zugangsdaten für den Remote-Zugriff oder administrative Aufgaben außerhalb der Geschäftszeiten und zum anderen den Missbrauch von Systemadministrations-Tools, um Netzwerke auszuspionieren und Daten zu stehlen.

Wenn Hacker über legitime Konten und Ihre Unternehmens-Tools über einen längeren Zeitraum im System verbleiben, spricht man häufig von „Living off the Land" (LOL). Solche Verhaltensweisen zu erkennen, erfordert kontinuierliches Monitoring und fundiertes Cybersecurity-Know-how. Geschulte Sicherheitsanalysten können Sie vor einem Angriff warnen, bevor ernsthafter Schaden entsteht. Sie sollten daher entweder in erforderliche Technologien und Schulungen für die Überwachung dieser Indikatoren investieren oder einen Managed Detection and Response (MDR)-Dienstleister mit dem Monitoring Ihrer Systeme beauftragen.

3. Überprüfen Sie Ihre Lieferkette

Nehmen Sie sich die Zeit, eine Liste aller Unternehmen zu erstellen, mit denen Sie in Verbindung stehen: Wahrscheinlich sind es mehr, als Sie denken. So ermitteln Sie schnell Schwachstellen (z. B. für Angriffe besonders anfälliger Lieferanten) und können weitere Maßnahmen zur Risikominimierung ergreifen. Sie können davon ausgehen, dass Sie unter anderem mit folgenden Drittanbietern verbunden sind:

- **IT-Serviceanbieter**
  - MSPs/MSSPs
  - Cloud-Anbieter
- **Professional Services**
  - Finanzen
  - Rechtsdienstleister
  - Security
  - Hausmeisterdienste
- **Zulieferer**
  - Materialien/Rohstoffe
  - Dienstleistungen
  - Arbeitskräfte
  - Logistik

Nach der Bestandsaufnahme können Sie den Netzwerkzugriff von Drittanbietern sowie ihren Zugang zu Unternehmensdaten prüfen. Beschränken Sie den Zugriff für Drittanbieter auf die notwendigen Funktionen und Daten. Beginnen Sie mit den Anbietern, die den umfangreichsten Zugriff auf nicht unbedingt erforderliche Bereiche besitzen, und arbeiten Sie sich nach unten vor.

4. Prüfen Sie den Sicherheitsstatus Ihrer Drittanbieter und Geschäftspartner

Dabei können Sie auf unterschiedliche Weise vorgehen. Bei großen Service-Anbietern, Cloud-Service-Providern und Zahlungsabwicklern empfiehlt es sich jedoch, die Zertifizierungen und Audits der jeweiligen Anbieter zu prüfen.

So sind Zahlungsabwickler etwa an PCI DSS gebunden. Wenn Ihr Anbieter PCI DSS Level 1 oder 2 einhalten muss, fordern Sie einen Compliance-Bericht (Report on Compliance, RoC) an, der von der Aufsichtsbehörde QSA/ISA ausgestellt wird. Überprüfen Sie diese RoCs vierteljährlich, um sicherzustellen, dass sie Ihre Erwartungen erfüllen.

Eine weitere gängige Zertifizierung zur Bestätigung von Audits ist SOC 2/2+/3 für Cloud-Service-Provider. SOC-Audits bewerten Sicherheitskontrollen und Risikominimierungs-Maßnahmen. Sie decken fünf Trust-Service-Prinzipien ab: Datenschutz, Sicherheit, Verfügbarkeit, Verarbeitungsintegrität und Vertraulichkeit.

Genau wie bei Ihrer eigenen Sicherheit bieten Audits alleine keine Garantie. Sie lassen jedoch darauf schließen, dass Ihre Anbieter die Sicherheit und Einhaltung der Prinzipien ernst nehmen. Fragen Sie außerdem nach Penetration-Test-Reports, Nachweisen zur Einhaltung der Datenschutz-Grundverordnung (DSGVO) sowie Informationen über frühere Schwachstellen oder Datenschutzverletzungen.

5. Überprüfen Sie kontinuierlich die Einhaltung von Sicherheitsvorgaben in Ihrem Unternehmen

Obgleich die Sicherheit Ihrer Drittanbieter für den Schutz vor Supply-Chain-Angriffen entscheidend ist, sollten Sie auch die Einhaltung von Sicherheitsvorgaben in Ihrem Unternehmen nicht außer Acht lassen. Viele Unternehmen ignorieren diesen Bereich, da sie entweder nicht wissen, wo sie ansetzen sollen, oder sich nicht als potenzielles Ziel von Supply-Chain-Angriffen sehen. Ihre Sicherheitsvorgaben können den Unterschied zwischen einem lästigen Problem und einer katastrophalen Datenpanne ausmachen.

Aktivieren Sie die mehrstufige Authentifizierung (MFA)

Am häufigsten werden Unternehmen aufgrund von gestohlenen, jedoch legitimen Zugangsdaten Opfer von Supply-Chain-Angriffen. Nur allzu oft erhalten Drittanbieter Zugangsdaten mit denselben Berechtigungen wie interne Mitarbeiter.

Das heißt: Für sie entfällt eine mehrstufige Authentifizierung. So können Cyberkriminelle nicht nur Zugangsdaten ausnutzen, die durch Phishing-Angriffe gestohlen wurden. Sie profitieren auch von der unbefugten Wiederverwendung von Zugangsdaten durch die Mitarbeiter. Da die meisten Unternehmen mit SSO (Single Sign-On) arbeiten, können die Anmeldedaten missbraucht werden, um auf zahlreiche Systeme zuzugreifen. Dadurch erhöht sich das Angriffsrisiko von innen und außen.

Überprüfen Sie die Zugriffs- und Anwendungsberechtigungen Ihrer Drittanbieter

Ein weiterer häufiger Fehler ist die Bereitstellung uneingeschränkter VPN-, RDP-, oder sonstiger Remote-Access-Technologien für Dritte, um ihnen die Verwaltung von Lösungen zu ermöglichen. Unter uneingeschränktem Zugriff verstehen wir in diesem Zusammenhang den Zugang zum gesamten Netzwerk anstelle einer Segmentierung und sorgfältigen Härtung aller erforderlichen Remote-Access-Tools.

Alle extern genutzten Tools sollten eine mehrstufige Authentifizierung vorschreiben. Zudem sollten sie sich auf einzelne Hosts oder Systeme beschränken. Wenn Sie zusätzlichen Zugriff anbieten möchten, empfehlen wir „Jump Hosts", um Risiken zu minimieren und zusätzliche Überwachung und Protokollierung zu ermöglichen.

Auch wenn Unternehmen alle Anwendungen, die mit dem Softwarezertifikat eines Anbieters signiert sind, standardmäßig zulassen, setzen sie sich dem Risiko von Supply-Chain-Angriffen aus. Wir haben wiederholt beobachtet, dass Zertifikate gestohlen und zum Signieren von Malware missbraucht wurden. Security-Tools sollten alle möglichen Angriffspunkte abdecken.

Behalten Sie Sicherheitsbulletins Ihrer Drittanbieter im Auge

Lesen Sie die Sicherheitsbulletins Ihrer Drittanbieter, um Patches schnell installieren und Abwehrmaßnahmen ergreifen zu können, sobald Schwachstellen entdeckt werden. Auch Schlagzeilen in den Medien sind eine hilfreiche Informationsquelle. Wenn Ihre Drittanbieter im Krisenmodus auf einen Vorfall reagieren, stehen Sie möglicherweise nicht ganz oben auf der Liste der zu benachrichtigenden Kunden. Wenn Sie sich jedoch proaktiv informieren, können Sie den Zugang sperren und prüfen, ob Sie von einem Vorfall betroffen sind.

Überprüfen Sie Ihre Cybersecurity-Versicherungspolice (falls vorhanden)

Wenn Sie über eine Cybersecurity-Versicherung verfügen, sollten Sie prüfen, ob Drittschäden abgedeckt werden und wie Sie Schäden im Bedarfsfall melden können. Sprechen Sie sich mit Ihren Drittanbietern ab, um zu ermitteln, ob sich Ihr Versicherungsschutz mit der Versicherung Ihrer Anbieter überschneidet.

Technologie und Services

Wie bereits erwähnt, ist die Abwehr von Supply-Chain-Angriffen sehr komplex. Daher geht es vor allem um Risikominimierung und Schadensbegrenzung. Glücklicherweise gibt es Technologien und Services, die Sie hierbei wirksam unterstützen.

Threat Hunting

Wie bereits erwähnt, erfordert die Abwehr von Supply-Chain-Angriffen einen proaktiven Ansatz. Threat Hunting unterstützt Unternehmen bei der proaktiven Suche nach Bedrohungen.

Endpoint Detection and Response (EDR)

EDR-Technologien spielen eine zentrale Rolle beim Threat Hunting. In der Regel werden EDR-Lösungen in Endpoint-Protection-Plattformen integriert. EDR kombiniert kontinuierliches Monitoring in Echtzeit und Endpoint-Daten mit automatisierten Reaktions- und Analysefunktionen. So sind Sicherheitsteams in der Lage, Bedrohungen schnell zu ermitteln und zu beseitigen.

Sophos Intercept X Endpoint bietet Ihnen leistungsstarke EDR-Funktionalität. Sophos EDR ist die erste speziell für Sicherheitsanalysten und IT-Administratoren entwickelte EDR-Lösung. Mit ihr können Sie detaillierte Abfragen erstellen, um Bedrohungen aufzuspüren und Ihre IT Security Operations zu optimieren. Sie erhalten Zugriff auf leistungsstarke, sofort einsatzbereite und individuell anpassbare SQL-Abfragen, die Ihnen Informationen liefern, die Sie für fundierte Entscheidungen benötigen.

Die automatische Bedrohungsidentifizierung in Sophos EDR erkennt und priorisiert verdächtige Aktivitäten automatisch. Außerdem lässt sich Ihr gesamter Endpoint- und Server-Bestand schnell und einfach auf potenzielle Bedrohungen durchsuchen.

Weitere Informationen über Sophos EDR

Managed Detection and Response (MDR) Services

Die verheerendsten Cyberangriffe, wie der SolarWinds-Hack, werden in der Regel zumindest teilweise manuell von Hackern durchgeführt. Und obwohl Technologien, insbesondere EDR und andere Threat-Hunting-Tools, eine zentrale Rolle spielen, sind nach wie vor versierte Cybersecurity-Experten gefragt. Denn nur manuelles Threat Hunting durch Bedrohungsexperten kann manuelle Hacker-Angriffe stoppen. IT-Managern ist dies bekannt: 48 % planen, diese Schutzmaßnahmen bis Ende nächsten Jahres umzusetzen[4].

MDR-Services bieten Threat Hunting durch ein Expertenteam. Sophos Managed Threat Response (MTR), der preisgekrönte MDR-Service von Sophos, bietet mehr als nur Benachrichtigungen bei Bedrohungen: Ihre IT arbeitet mit einem

4 Cybersecurity: The Human Challenge, Sophos, 2020

persönlichen, rund um die Uhr verfügbaren Cybersecurity-Experten-Team zusammen, das in Ihrem Auftrag proaktiv Bedrohungen aufspürt, analysiert und Reaktionsmaßnahmen ergreift.

Unsere Experten übernehmen für Sie folgende Aufgaben:

- Proaktives Aufspüren und Prüfen von potenziellen Bedrohungen und Vorfällen
- Nutzen aller vorliegenden Informationen, um Ausmaß und Schwere von Bedrohungen zu bestimmen
- Anwenden geeigneter Maßnahmen je nach Risikobewertung der Bedrohung
- Einleiten von Maßnahmen zum Stoppen, Eindämmen und Beseitigen von Bedrohungen
- Bereitstellen konkreter Ratschläge, um die Ursache wiederholt auftretender Vorfälle zu bekämpfen

Mehr über Sophos MTR erfahren

Stellen Sie um auf Zero Trust

Wir haben die Überprüfung Ihrer eigenen Sicherheitslage bereits angesprochen – insbesondere die Durchsetzung einer mehrstufigen Authentifizierung sowie die kontinuierliche Prüfung von Zugriffs- und Anwendungsrechten. All dies lässt sich durch die Umstellung auf einen Zero-Trust-Ansatz in der Cybersecurity erreichen.

Zero Trust fußt auf dem Prinzip: „Nichts und niemandem vertrauen, alles überprüfen". Für Zero Trust gibt es nicht den einen Anbieter, das eine Produkt oder die eine Technologie. Vielmehr ist eine Kombination unterschiedlicher Lösungen erforderlich. Ein erster Schritt in diese Richtung besteht in der Einführung einer Zero-Trust-Network-Access-Lösung (ZTNA).

Wie aus dem Namen hervorgeht, basiert ZTNA auf dem Zero-Trust-Prinzip. ZTNA ermöglicht Benutzern von jedem Standort aus, sicher auf Daten zuzugreifen. Administratoren bietet die Lösung sehr feinstufige Kontrollen.

Bei ZTNA geht es vor allem darum, Benutzer zu verifizieren, und zwar in der Regel mit mehrstufiger Authentifizierung und einem Identitätsanbieter (IdP). Auch der Sicherheitsstatus und die Compliance des Geräts werden kontrolliert. ZTNA stellt sicher, dass das Gerät registriert und ordnungsgemäß geschützt und die Verschlüsselung aktiviert ist. Anhand dieser Informationen werden Benutzerrechte sowie der Zugriff auf wichtige Anwendungen im Netzwerk auf Richtlinienbasis gesteuert. ZTNA ist eine überzeugende Alternative zu Remote Access VPN, da sich der Zugriff auf Daten und Anwendungen gezielt steuern lässt. Dies ist entscheidend, wenn es um den Schutz vor Supply-Chain-Angriffen geht, die über den Zugang von Drittanbietern zu Ihren Systemen verursacht werden.

Sophos ZTNA, unsere neue, in der Cloud bereitgestellte und verwaltete Network-Access-Lösung, befindet sich momentan im Early-Access-Programm (EAP) und ist voraussichtlich Mitte 2021 allgemein verfügbar. ZTNA bietet Schutz für alle Netzwerkanwendungen, die im lokalen Unternehmensnetzwerk, über ein Rechenzentrum oder in der Cloud gehostet werden. Dies umfasst etwa den RDP-Zugriff auf Netzwerkfreigaben oder Anwendungen wie Jira, Wikis, Quellcode-Repositorys, Support- und Ticket-Apps und mehr.

Mehr über Sophos ZTNA erfahren

Fazit

Da Supply-Chain-Angriffe meist sehr komplex sind, ist es praktisch unmöglich, diese zu verhindern. Mit unseren Best-Practice-Richtlinien können Sie das Angriffsrisiko jedoch minimieren und verheerende Schäden vermeiden. Zusammenfassung:

1. Wechseln Sie von reaktiver zu proaktiver Cybersecurity
2. Achten Sie auf frühe Anzeichen einer Kompromittierung
3. Überprüfen Sie Ihre Lieferkette
4. Prüfen Sie den Sicherheitsstatus Ihrer Drittanbieter und Geschäftspartner
5. Überprüfen Sie kontinuierlich die Einhaltung von Sicherheitsvorgaben in Ihrem Unternehmen

Ziehen Sie Technologien und Services, wie EDR, MTR und ZTNA, in Betracht, um Ihre Lieferkette abzusichern.

Die Bedrohungslandschaft hat sich verändert: Supply-Chain-Angriffe können Unternehmen jeder Größe treffen. Wir sind alle potenzielle Ziele: Ergreifen Sie also rechtzeitig Maßnahmen zur Minimierung der Risiken.

Unter www.sophos.de erfahren Sie mehr über die branchenführenden Cybersecurity-Lösungen von Sophos

Sophos bietet branchenführende Cybersecurity-Lösungen für Unternehmen jeder Größe und schützt Kunden in Echtzeit vor komplexen Bedrohungen, wie Malware, Ransomware und Phishing. Bewährte Next-Gen-Funktionen mit der Power von Machine Learning und künstlicher Intelligenz sichern Unternehmensdaten effektiv.

2021-04-14 (SB-NP)

SOPHOS