SOPHOS
Cybersecurity delivered.

Lessons Learned aus echten Cyberangriffen

7 Tipps, mit denen Sie Ihr Unternehmen besser schützen

„Wahnsinn ist, immer wieder das Gleiche zu tun und andere Ergebnisse zu erwarten." - Albert Einstein

Doch wir können aus unseren Fehlern lernen und dafür sorgen, dass wir sie in Zukunft nicht wiederholen. Dies gilt für alle Lebensbereiche – auch für die Cybersicherheit.

Rob Collins, Specialist Systems Engineer für Sophos Managed Detection and Response und Rapid Response, hat in diesem Whitepaper die sieben wichtigsten Erkenntnisse von Unternehmen zusammengefasst, die von Cyberangriffen betroffen waren. Aus diesen Erkenntnissen abgeleitet werden sieben Tipps, mit denen Sie Ihr Unternehmen besser schützen können und so vermeiden, selbst Opfer eines Angriffs zu werden. Dabei sind die meisten dieser Vorschläge ganz ohne die Anschaffung von Tools umsetzbar.

Sophos-Whitepaper. August 2022

Inhaltsverzeichnis

Tipp #1:
Erzwingen Sie MFA für Ihre Systemadministration und Sicherheitskonsolen 3

Tipp #2:
Blockieren Sie Remote Desktop Protocol (RDP) für externe Verbindungen 4

Tipp #3:
Schützen Sie alle Endpoints 5

Tipp #4:
Verhindern Sie, dass Bedrohungsakteure Ihre Passwörter erhalten (und verwenden) 7

Tipp #5:
Bearbeiten Sie Admin-Tools lieber mit dem Skalpell statt mit dem Vorschlaghammer 10

Tipp #6:
Seien Sie immer einen Schritt voraus 12

Tipp #7:
Planen Sie im Vorfeld für den Ernstfall 14

Wie Sophos helfen kann 17

Tipp #1: Erzwingen Sie MFA für Ihre Systemadministration und Sicherheitskonsolen

Die Multi-Faktor-Authentifizierung (MFA) ist eine Sicherheitsmaßnahme, die zwei oder mehr Identitätsnachweise erfordert, um dem jeweiligen Benutzer Zugang zu gewähren. Mit anderen Worten: Sie brauchen mehr als nur ein Passwort, um Zugriff auf das gewünschte System oder die Anwendung zu erhalten. Ein einmaliger Zugangscode, eine Gesichtserkennung oder ein Fingerabdruck können ebenfalls als zusätzliche Sicherheitskontrolle erforderlich sein.

Jeder Administrator kennt die Vorteile von MFA für den Zugriff auf Geschäftsanwendungen. So sind unsere Office365- und Salesforce-Daten auch dann geschützt, wenn ein Angreifer an einen Benutzernamen und ein Passwort kommt, diese errät, kauft oder durch wahlloses Ausprobieren (Brute Force) herausfindet.

Doch mit der Verlagerung in die Cloud sind auch die Anmeldekonsolen für diese Anwendungen dem Internet ausgesetzt. Damit wandert die Systemverwaltung und -sicherheit ebenfalls in die Cloud und erfordert MFA.

MITRE ATT&CK-Verfahren T1078 („Valid Accounts") beschreibt, wie Bedrohungsakteure gültige Konten verwenden, um sich erstmalig Zugang zum Netzwerk zu verschaffen, Schutzmaßnahmen zu umgehen, Persistenz zu erlangen und ihre Privilegien zu erweitern.

Diese Taktiken ermöglichen es, verschiedene Abwehrmaßnahmen zu umgehen, darunter Virenschutz, Anwendungskontrolle, Firewalls, Systeme zur Erkennung und Verhinderung von Bedrohungen und Systemzugangskontrollen. Doch es ist sehr schwer, zwischen berechtigtem Zugriff und unbefugter Nutzung zu unterscheiden.

Der Zugriff über gültige Konten gehört zu den fünf häufigsten Techniken für den Erstzugriff (https://attack.mitre.org/tactics/TA0001/), wie aus dem 2021 Active Adversary Playbook von Sophos hervorgeht. Sogar Admin-Tools, wie beispielsweise Solarwinds, Webroot, Kaseya und Connectwise, werden zur Verbreitung schädlicher Payloads verwendet.

Was passiert, wenn ein Angreifer Zugang zu einer Sicherheitskonsole erhält? In dem folgenden Beispiel hat der Bedrohungsakteur einfach seine eigene Richtlinie geschrieben und alle Sicherheitseinstellungen deaktiviert.

Threat Protection (2)

Name	Status
YOUR FILES HAS BEEN STOLEN	✔ Enforced
Base Policy - Threat Protection	✔ Enforced

Selbst lokale Sicherheitsverwaltungssysteme sollten nach Möglichkeit MFA verwenden – andernfalls ist es für einen Angreifer noch leichter, seine Malware einzusetzen, wenn er Ihre Sicherheitslösungen zuvor einfach ausschalten kann. Wenn Sie ein VPN für den Zugriff auf Ihr Netzwerk verwenden, empfehlen wir dringend, MFA auch für dieses zu aktivieren.

Damit sorgen Sie in dreifacher Hinsicht für mehr Schutz, denn MFA

- minimiert das Risiko unbefugter Zugriffe.
- generiert Warnmeldungen bei Zugriffsversuchen und ermöglicht es dem Administrator, künftige Zugriffsversuche nach Bedarf zu blockieren
- verhindert die gemeinsame Nutzung von Konten und ermöglicht genaue Audit-Verläufe, sodass das Verhalten einem bestimmten Benutzer zugeordnet werden kann

Dabei nimmt die Aktivierung von MFA lediglich etwas Zeit in Anspruch. Sie haben schon mehrfach die auffälligen Hinweise „MFA aktivieren" auf Ihren Konsolen ignoriert? Dann sollten Sie keine Zeit mehr verstreichen lassen, um dieser Aufforderung nachzukommen. Wenn Ihr Sicherheitsanbieter keine MFA-Optionen anbietet, ist es an der Zeit zu fragen: Warum nicht?

Tipp #2: Blockieren Sie Remote Desktop Protocol (RDP) für externe Verbindungen

Das Remote Desktop Protocol (auch bekannt als Terminal Services oder Remotedesktopdienst) ermöglicht es, eine Verbindung zu einem anderen entfernten Computer herzustellen und so die gleiche Benutzererfahrung zu bieten, als wäre man physisch anwesend.

Unserem Active Adversary Playbook 2021 zufolge wurde Microsofts integriertes RDP bei 32 % der Angriffe verwendet, um über das Internet auf die Systeme eines Unternehmens zuzugreifen – diese Art des Angriffs ist somit die häufigste Methode für Erstzugriffsversuche.

Im Gegensatz zu einigen anderen Fernzugriffstools erfordert RDP in der Regel nicht mehr als einen Benutzernamen und ein Passwort, wobei der Benutzername häufig offengelegt wird (damit man sich beim nächsten Mal leichter anmelden kann). Teilweise ist sogar ein Zugriff ohne jegliche Anmeldeinformationen möglich.

Missbrauch von RDP fällt unter unterschiedliche MITRE ATT&CK-Techniken, die gängigste ist T1133 (Externe Remote-Dienste). Weitere MITRE ATT&CK-Techniken, bei denen RDP eine Rolle spielt, sind:

- T1563 – RDP Hijacking (Zugang und Kontrolle über IT-Systeme durch Angreifer als vermeintlich legitime Nutzer)
- T1021 – Lateral Movement using RDP (Laterale Bewegung per RDP)
- T1572 – Tunneling over RDP (Tunnelzugriff über RDP)
- T1573 – Command and Control over RDP (Kontrolle über RDP)
- T1078 – Using Valid Accounts with RDP (Verwendung gültiger Konten per RDP)
- T1049 – System Network Connections Discovery (System zur Erkennung der Netzwerkverbindungen)
- T1071 – Application Layer Protocol (Protokoll auf Anwendungsebene)

Sobald sich ein Bedrohungsakteur erfolgreich in eine RDP-Sitzung eingeloggt hat, ist es so gut wie unmöglich ihn aufzuhalten, nicht einmal das Rechenzentrum mit den höchsten physischen Sicherheitsstandards der Welt wäre dazu in der Lage.

Doch es gibt eine einfache Lösung – setzen Sie RDP keinen externen Risiken aus. Leiten Sie den Port TCP:3389 auf Ihrer Firewall nicht einfach weiter. Und glauben Sie nicht, dass die Verwendung eines anderen Ports hilft – Sie sind sichtbar, zwölftausend RDPs auf Port 3388!

Die Option erscheint verlockend, aber Shodan.IO (eine Suchmaschine für das Internet der Dinge) zeigt, dass über 3,3 Millionen RDP-Ports 3389 weltweit ansprechbar und leicht zu finden sind. Warum ist RDP eigentlich so beliebt? Zugriff über RDP zu erlauben, ist eine schnelle und einfache Möglichkeit, Systeme remote zu verwalten. So kann beispielsweise ein Managed Service Provider (MSP) den Server eines Kunden problemlos betreuen oder ein Zahnarzt von zu Hause aus auf sein Praxissystem zugreifen.

Wenn der Fernzugriff auf RDP oder Terminal Services erforderlich ist, sollte er nur über eine sichere VPN-Verbindung (mit MFA) zum Unternehmensnetzwerk oder über ein vertrauenswürdiges Remote Access Gateway erfolgen.

Tipp #3: Schützen Sie alle Endpoints

In Teilen der IT-Welt herrscht die Meinung vor, dass für einige Systeme keine Endpoint-Sicherheit erforderlich sei. Diese Einschätzung ist häufig für solche Geräte anzutreffen, die isoliert und nicht mit dem Internet verbunden sind oder keine wichtigen Daten oder Programme enthalten, wie etwa Entwicklungssysteme. So manches Unternehmen lässt sogar seine Endpoint-Schutz-Lizenzen auslaufen, in dem Glauben, dass diese ohnehin keinen zusätzlichen Nutzen bringen.

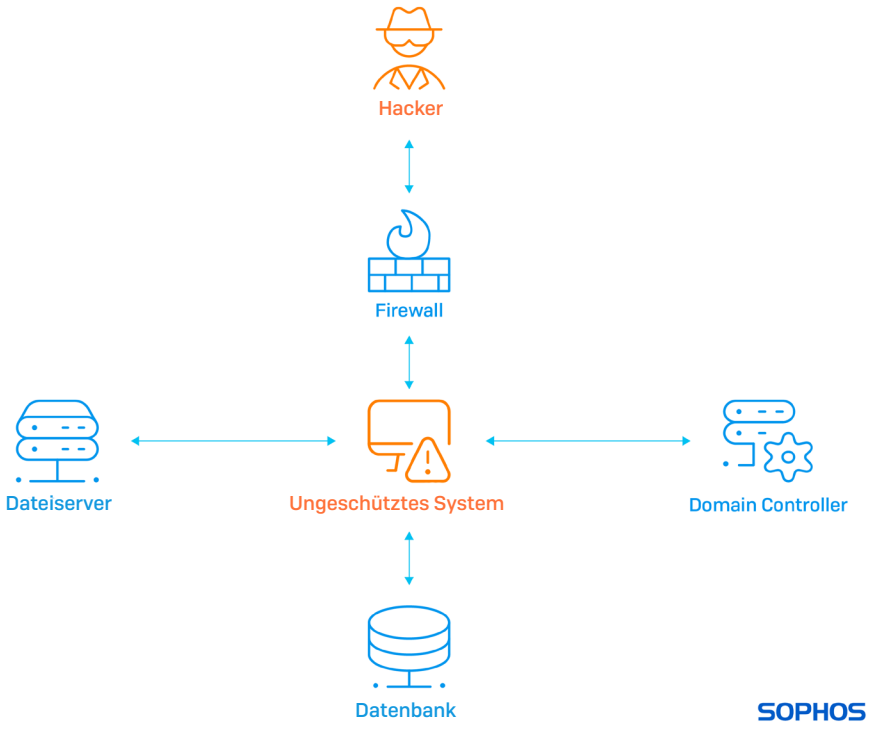
Diese Denkweise rührt daher, dass die Endpoint-Security seit langem (jedenfalls in der Welt der IT) darauf ausgelegt ist, das Eindringen von Malware zu verhindern. Wenn es sich also um ein isoliertes oder unwichtiges System handelt, es leicht wiederhergestellt werden kann oder man „immer höchste Vorsicht walten lässt", wird ein Schutz oft als nicht erforderlich angesehen.

Auch werden Nutzer-Workstations/Laptops oftmals für weniger wichtig erachtet als Server und daher nur letztere geschützt. Tatsächlich trafen laut unserem Sophos Active Adversary Playbook 2021 **54 % der Angriffe ungeschützte Systeme**.

Sowohl der Endpoint-Schutz als auch die Art und Weise von Angriffen haben sich in letzter Zeit drastisch verändert. Cyberkriminelle gehen mit ausgeklügelten Taktiken vor, bei denen sie die Verwaltungstools ihres Opfers verwenden (z. B PowerShell) sowie Skriptumgebungen (z. B JavaScript), Systemeinstellungen (z. B geplante Aufgaben und Gruppenrichtlinien), Netzwerkdienste (z. B SMB und Admin Shares und WMI) und gängige Anwendungen (wie TeamViewer, AnyDesk oder ScreenConnect). So vermeiden sie, dass sie Malware einsetzen müssen, um ihre Ziele zu erreichen. Was früher als Techniken von Staaten und Advanced Persistent Threats (APT) angesehen wurde, wird heute selbst von solchen Bedrohungsakteuren eingesetzt, die nicht unbedingt zu den versiertesten zählen.

Doch die Zielsetzung der Angreifer bleibt unverändert – sie wollen Geld verdienen. Dies kann durch den Einsatz von Ransomware (oft nach Datenexfiltration und Löschung von Sicherungskopien, um Lösegeldzahlungen zu erzwingen), durch das Schürfen von Kryptowährungen, die Beschaffung von personenbezogenen Daten zum Verkauf oder durch Industriespionage geschehen.

Als Reaktion darauf hat sich der Endpoint-Schutz weiterentwickelt. So werden schädliche Aktivitäten jetzt erkannt und abgewehrt. Moderne Endpoint-Security bietet zudem umfassende Transparenz, Kontext und Tools zum Aufspüren von Bedrohungen. Und diese fortschrittliche Entwicklung sollte man nutzen, um sich zu schützen. **Denn ungeschützte Systeme sind blinde Flecken**.



Ein ungeschütztes System mit Internetzugang kann zum verborgenen Einfallstor für den Zugriff auf Ihre internen kritischen Daten und Anwendungen werden.

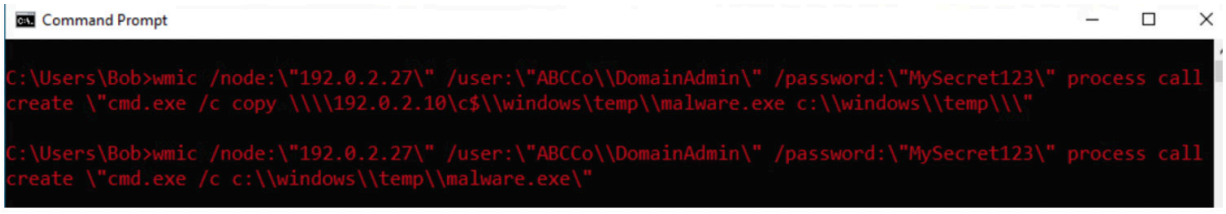
Systeme ohne direkten Internetzugang benötigen Schutz

Doch wie können Bedrohungsakteure ein ungeschütztes System angreifen, das keinen direkten Internetzugang hat?

In der Regel starten Cyberkriminelle ihren Angriff von einem System aus, das über einen Command-and-Control-Kanal auf Port 443 (schwer zu identifizierender, anomaler, verschlüsselter Datenverkehr) mit einem Trojaner oder Stager als Vermittler verbunden ist. Ob es sich dabei um ein Server- oder ein Benutzersystem handelt, ist unerheblich – sie alle verfügen über ähnliche Kernfunktionen. Der Angreifer kann dann auf dieselbe Weise auf Ihre Systeme zugreifen wie Sie selbst.

Hier eine Liste der Techniken, die für einen Angriff auf ein System per LAN zur Verfügung stehen (Links zu MITRE ATT&CK):

- T1047 - Windows Management Instrumentation (Windows-Verwaltungsinstrumentierung)
- 1 - Remote Desktop Protocol
- 2 - Administration Shares
- 3 - Distributed Component Object Model
- 4 – Secure Shell (SSH)
- 6 - Windows Remote Management
- 5 – VNC, ScreenConnect, TeamViewer oder andere Remote-Verwaltungstools von Drittanbietern



Einfache Befehle zur Verwendung von WMI, um Malware auf ein anderes Gerät umzuleiten und auszuführen

Angesichts der vielen Möglichkeiten, die Cyberkriminellen zur Verfügung stehen, ist es daher wichtig, **Endpoint-Schutz *für alle Systeme einzurichten, auch für solche ohne direkten Internetzugang***. Während die Aktivität auf dem zwischengeschalteten System harmlos aussehen mag (z. B. Herstellen einer RDP-Verbindung), können die Folgen auf dem ungeschützten System katastrophal sein.

Wenn Sie Ihre blinden Flecken mittels Endpoint-Schutz beseitigen, haben Angreifer weniger Möglichkeiten, sich zu verstecken. Das ist wichtig, denn wenn sich Angreifer in einem System verstecken, können sie tage-, wochen- oder sogar monatelang unentdeckt bleiben und im Stillen Informationen über die Umgebung, Benutzer, Netzwerke, Anwendungen und Daten sammeln. Sie finden Ihre End-of-Life-Systeme, Linux-Server, Hypervisoren sowie vernachlässigte und ungepatchte Anwendungen und graben dann so lange weiter, bis sie für den endgültigen Angriff bereit sind.

In den meisten Fällen besteht ihr Standardverfahren darin, die Endpoint-Sicherheit zu deaktivieren (was sie tun können, weil sie erhöhte oder sogar Systemrechte erhalten haben), Backups zu exfiltrieren und dann zu löschen und die Ransomware-as-a-Service ihrer Wahl einzusetzen.

Vor kurzem wurde das Sophos Rapid-Response-Team bei einem Sicherheitsvorfall zu Hilfe gerufen, bei dem ein ungeschütztes System involviert war. Ein Paradebeispiel, das zeigt, warum – im Nachhinein betrachtet – ein umfassender Endpoint-Schutz sinnvoll gewesen wäre.

Tipp #4: Verhindern Sie, dass Bedrohungsakteure Ihre Passwörter erhalten (und verwenden)

Laut dem Sophos Active Adversary Playbook 2021 gehört die Verwendung gültiger Konten (über einen Benutzernamen und ein Kennwort) zu den fünf häufigsten Techniken für den Erstzugriff bei Sicherheitsverletzungen (MITRE ATT&CK-Technik T1078). Gültige Anmeldeinformationen spielen in der Phase des Erstzugriffs eine wichtige Rolle. Außerdem können sie natürlich auch während der gesamten Angriffskette verwendet werden, einschließlich Persistenz, Ausweitung von Berechtigungen und Umgehung der Verteidigung.

Eine besondere Herausforderung

Wie eingangs erwähnt, ist es für IT-Sicherheitsexperten äußerst schwierig, zwischen berechtigtem Zugriff und unbefugter Nutzung zu unterscheiden. Zudem kann ein gültiges Konto innerhalb eines Unternehmens unterschiedliche Berechtigungsstufen haben (vom einfachen Benutzer bis hin zu Domänen-Administratorrechten) und Anmeldedaten können auf viele verschiedene Arten erlangt werden.

Eine weitere Komplikation besteht darin, dass im Unternehmen möglicherweise Testkonten, Dienstkonten für den nicht-menschlichen Zugriff, APIs, Konten für Dritte für den Zugriff auf Ihre Systeme (z. B. einen ausgelagerten Helpdesk) oder Geräte mit fest codierten Anmeldedaten eingerichtet sind.

Viele Menschen nutzen ihre Unternehmensanmeldedaten auch für private Online-Dienste und die meisten verwenden hierbei eine E-Mail-Adresse anstelle des Benutzernamens, was die Bedrohungslage noch einmal verstärkt. Auch die Wiederverwendung von Passwörtern ist leider immer noch weit verbreitet. Ein einziges durch Kriminelle gekapertes Passwort kann so der Schlüssel zu vielen weiteren Türen sein. Ein weiterer fataler Vorteil für die Cyberkriminellen: Im Zuge der COVID-19-Pandemie gingen Unternehmen schnell dazu über, den Fernzugriff für alle zuzulassen, was die Angriffsfläche für die unbefugte Nutzung von VPN und Fernzugriffstools noch vergrößerte.

Wie kommen die kriminellen Eindringlinge an unsere Anmeldedaten?

Die Liste der Möglichkeiten, um Anmeldedaten unbefugt zu erlangen ist tatsächlich umfangreich, deshalb hier nur der Blick auf einige der wichtigsten. Das Ziel der Hacker besteht darin, die höchste Berechtigungsstufe zu erlangen, die sie zur Zielerreichung benötigen (z. B. Deaktivieren von Sicherheitsfunktionen, Exfiltrieren von Daten, Löschen von Backups und Bereitstellen von Ransomware). Da sie nicht erwarten, Domänen-Administratorkonten über einen Phishing-E-Mail-Angriff zu erhalten, beginnen sie mit einfacheren Zielen und arbeiten sich nach oben.

Externe Methoden wie Phishing (T1598), Brute-Force (T1110), Social Engineering (so könnte sich ganz einfach jemand als Mitarbeiter eines vertrauenswürdigen IT-Anbieters ausgeben und um die Einrichtung eines Kontos bitten – T1593.1) und SQL Injection (T1190) werden manchmal in Compilations of Many Breaches (COMB) zusammengefasst und im Darkweb gegen eine Gebühr oder sogar kostenlos zur Verfügung gestellt.

Die Hacker versuchen, die erhaltenen Anmeldeinformationen mit Ihren externen Zugriffsmethoden abzugleichen (RDP – siehe Tipp #2, VPN, FTP, Terminal Services, CPanel, Fernzugriffstools wie TeamViewer, Cloud Services wie O365 oder Sicherheitskonsolen). Hierzu wenden sie die sogenannte Credential-Stuffing-Methode an, um herauszufinden, was funktioniert. Da von den Benutzern nicht erwartet werden kann, dass sie sich mehr als ein paar Passwörter merken, werden Anmeldeinformationen häufig wiederverwendet, und Benutzernamen können oft aus E-Mail-Adressformaten abgeleitet werden. Aus diesem Grund ist die Multi-Faktor-Authentifizierung (MFA/2FA) für alle externen und internen Zugriffe wichtig (siehe Tipp#1). Sobald ein Satz von Anmeldeinformationen erfolgreich mit einer Fernzugriffsmethode verknüpft wurde, kann der Bedrohungsakteur zu einem gültigen Benutzer werden und sich in Ihrem Unternehmen verstecken.

Mit gültigen Anmeldedaten kann sich ein Bedrohungsakteur wie jeder andere Mitarbeiter unauffällig im Netzwerk bewegen.

Bevor wir auf die Methoden der Rechteausweitung eingehen, ist es wichtig zu wissen, dass es auch andere Zugriffsmethoden gibt, die keine Anmeldedaten erfordern. So wurden Exploits (T1212) oder Standardkennwörter (T1078.1) in VPN-Konzentratoren, Exchange, Firewalls/Routern, Webser und SQL-Injection bereits genutzt, um Fuß zu fassen. Drive-by-Downloads können ebenfalls dazu verwendet werden, eine Hintertür einzurichten (T1189). Wenn man erst einmal im Netzwerk ist, haben einfache Benutzerkonten immer noch genügend Zugriffsrechte, um verschiedene Erkundungstechniken anzuwenden und einen Weg zu finden, um zu einem Zugang mit erweiterten Rechten zu wechseln oder Konten zu erstellen, um Zugriffsrechte zu erhalten.

Cyberkriminelle vermeiden weitestgehend den Einsatz von Tools, die verdächtig sind und entdeckt werden könnten, also versuchen sie es womöglich über diese Wege:

- Informationen über das System und die Umgebung mit einfachen Befehlen wie „whoami“ und „ipconfig“ ermitteln (T1016)
- Das Gerät, auf dem man sich befindet (und alle zugeordneten Laufwerke) nach Dateien mit „Passwörtern“ im Namen oder Inhalt durchsuchen (T1552.1)
- LDAP durchsuchen, um zu sehen, welche anderen Konten interessant sein könnten (T1087.2)
- Durchsuchen der Windows-Registrierung nach gespeicherten Anmeldeinformationen (T1552.2)
- Durchsuchen von Web-Cookies nach gespeicherten Anmeldeinformationen (T1539)
- Ein PowerShell-basiertes Befehls- und Steuerungstool ablegen, damit der Angreifer wieder zurückkehren kann, selbst wenn Sie ein Kennwort ändern oder einen Patch für Ihre Sicherheitslücke installieren (T1059.1)
- Herausfinden, welche Programme installiert sind – Fernzugriffstools und Admin-Tools wie PSExec und PSKill können sehr nützlich sein, wenn sie bereits vorhanden sind (T1592.2)

Zudem könnten Cyberkriminelle zur Installation und/oder Verwendung von „potenziell unerwünschten Programmen“ übergehen. Die oben erwähnten PSExec und PSKill sind offizielle Microsoft-Admin-Tools, werden aber auch in vielen anderen Bereichen eingesetzt. IOBit, GMER, Process Hacker, AutoIT, Nircmd, Port-Scanner und Packet-Sniffer wurden bei den von Sophos bearbeiteten Angriffen eingesetzt. Das Ziel dieser Tools ist es, alle Endpoint-Sicherheitslösungen lahmzulegen, damit ein Bedrohungsakteur zum nächsten Schritt übergehen kann, bei dem dann Tools eingesetzt werden, die wahrscheinlich einen Alarm der IT-Sicherheitssysteme auslösen würden.

Zu den beliebten Tools zum Auffinden von Konten mit höheren Berechtigungen gehören Mimikatz, IcedID, PowerSploit und Cobalt Strike. Trickbot war früher ein alter Favorit. Sie ermöglichen es den Hackern, die Angaben, die Netzwerke

zur Authentifizierung von Benutzern verwenden (z. B. Kerberos), genau zu erfassen, zu deuten, zu exportieren und zu manipulieren. Die Daten sind zwar bis zu einem gewissen Grad verschlüsselt, aber das hat sich für geschickte Hacker nur als unbedeutendes Hindernis erwiesen, das sich schnell aus dem Weg räumen ließ. Der verschlüsselte Token, der das gültige Konto repräsentiert, kann oft über das Netz weitergegeben und akzeptiert werden, bekannt als Pass-the-Hash (T1550.2) und Pass-the-Ticket (T1550.3). Umfangreiche Tabellen mit Passwörtern und deren verschlüsselten Versionen werden verwendet, um ein verschlüsseltes Passwort schnell mit der Klartextversion abzugleichen (T1110.2). Keylogging-Tools können eingesetzt werden, um die Tastaturanschläge auf einem Gerät aufzuzeichnen, wenn sich jemand das nächste Mal anmeldet. Es wurden bestimmte Sicherheitslücken gefunden, die den Zugriff auf Anmeldedaten auch ohne Administrationsrechte ermöglichen, z. B. HiveNightmare/SeriousSam und PrintNightmare. Doch damit nicht genug: Es gibt zudem leicht erhältliche Toolkits wie LaZagne, die alles für die Cyberkriminellen erledigen und sogar Passwörter abrufen, die in Browsern, Instant-Messaging-Software, Datenbanken, Spielen, E-Mails und WiFi gespeichert sind.

Gültige Anmeldeinformationen als Einfallstor

Gültige Anmeldedaten, insbesondere mit Administrationsrechten, haben einige wichtige Vorteile für die Angreifer. Sie können unternehmensweit verwendet werden, um Gruppenrichtlinien zu ändern (T1484.1), Sicherheitstools zu deaktivieren (T1562.1), Konten zu löschen und neue zu erstellen. Daten können exfiltriert und dann verkauft, zu Erpressungszwecken oder zur Industriespionage verwendet werden. Sie können für Imitations- und Kompromittierungsangriffe auf geschäftliche E-Mails mit einem hohen Maß an Authentizität verwendet werden. In den meisten Fällen werden sie Ransomware-as-a-Service verbreiten und ausführen. Und wenn das nicht gelingt, können Angreifer auch einfach das gültige Konto verwenden, um BitLocker zu aktivieren (oder den Schlüssel zu verschieben).

Wie Sie Ihr Unternehmen schützen können

Das Problem ist ernst und die Folgen real. Doch die gute Nachricht ist: Die passenden Lösungen sind bereits vorhanden. Diese müssen nur von den Mitarbeitern, Prozessen und Technologien entsprechend umgesetzt werden. Bei der Schulung der Mitarbeiter in Sachen Cybersicherheit geht es in der Regel um folgende Inhalte:

- Erkennen von Phishing-E-Mails
- Keine Wiederverwendung von Passwörtern – Passwortmanagement-Tools
- Keine Arbeitspasswörter für persönliche Konten
- Anforderungen an die Komplexität von Passwörtern
- Vermeiden dubioser Websites

Was Sie in Bezug auf Verfahren und Technologien beachten sollten

- Die Multi-Faktor-Authentifizierung sollte so weit wie möglich eingesetzt werden.
- Die externe Angriffsfläche sollte so klein wie möglich sein und auf dem neuesten Stand gehalten werden
- Reduzieren Sie die Anzahl der Konten auf höchster Ebene auf ein Minimum. Acht Domänenadministratoren sind zu viel…
- Beschränken Sie die Nutzung lokaler Administrationsrechte
- Dienstkontenhygiene – Entfernen Sie nicht genutzte Dienst- und Testkonten
- Kontrollieren und überwachen Sie die Verwendung von leistungsstarken Admin-Tools und potenziell unerwünschten Programmen
- Überwachen Sie unerwartete Anmeldeereignisse (z. B. nach Ort und Zeit)

Tipp #5: Bearbeiten Sie Admin-Tools lieber mit dem Skalpell statt mit dem Vorschlaghammer

Wie im Sophos Active Adversary Playbook 2021 beschrieben, greifen Hacker gerne auf Tools zurück, die auch von IT-Administratoren und Sicherheitsexperten verwendet werden, um so die automatische Erkennung verdächtiger Aktionen zu erschweren. Viele dieser Tools werden von Sicherheitsprodukten als „Potenziell unerwünschte Anwendungen", kurz PUAs oder auch Risk Ware bzw. Risk Tools erkannt, sind aber von IT-Teams teilweise für den täglichen Gebrauch unerlässlich. Um die passenden Abwehrmaßnahmen zu treffen, sollten daher zwei zentrale Fragen beantwortet werden: (1) Müssen alle meine Anwender berechtigt sein, diese Dienstprogramme zu nutzen? (2) Müssen diese Dienstprogramme auf jedem Gerät ausgeführt werden können?

PUA – was ist das?

Was genau ist eine potenziell unerwünschte Anwendung (PUA), und wie können Sie solche Anwendungen sicher verwenden? Mit den Admin-Tools, die mit einem Betriebssystem wie z. B. PowerShell gebündelt sind, können Geräte in einem Netzwerk automatisiert und verwaltet werden. Darüber hinaus gibt es zusätzliche Tools von Drittanbietern, die häufig zur Erweiterung von Funktionen wie Port-Scanning, Paketerfassung, Skripting, Überwachung, Sicherheitstools, Komprimierung und Archivierung, Verschlüsselung, Debugging, Penetrationstests, Netzwerkverwaltung und Fernzugriff verwendet werden. Die meisten dieser Anwendungen laufen mit System- oder Root-Zugriff.

Sofern diese Anwendungen intern von Ihrem eigenen IT-Team installiert und genutzt werden, sind sie nützliche Werkzeuge. Geschieht dies aber durch andere Anwender, gelten sie als PUAs und werden von seriösen Endpoint-Sicherheitslösungen oft als solche gekennzeichnet. Um diese Tools ungehindert nutzen zu können, fügen viele Administratoren die von ihnen verwendeten Tools einfach zu einer globalen Ausschluss- oder Zulassungsliste in ihrer Sicherheitskonfiguration hinzu. Leider ermöglicht diese Methode auch die Installation und Verwendung der Tools durch Unbefugte, oft ohne jegliche Überwachung, Warnungen oder Benachrichtigungen.

Kritische PUAs

Hier sind einige der gängigsten PUAs und ihre Funktionen, die Angreifer gerne nutzen:

- **PSExec** – „...ein leichtgewichtiger Telnet-Ersatz, der es dem Nutzer ermöglicht, Prozesse auf anderen Systemen auszuführen, komplett mit voller Interaktivität für Konsolenanwendungen und ohne manuell Client-Software installieren zu müssen. Zu den leistungsfähigsten Anwendungen gehören das Starten interaktiver Kommandozeilen (Command Prompts) auf entfernten Systemen und remotefähiger Programme wie IpConfig, die ansonsten nicht in der Lage sind, Informationen über entfernte Systeme anzuzeigen."
- **PSKill** – kann „Prozesse auf entfernten Systemen beenden, sogar ohne vorheriger Client-Installation auf dem Zielcomputer."
- **Process Hacker** – ein Tool zur Ressourcenüberwachung, das oft verwendet wird, um Sicherheits- und Log-Software zu beenden.
- **Anydesk/TeamViewer/RDPWrap** – oder jedes andere Tool, das für den Fernzugriff, insbesondere via Internet, entwickelt wurde, kann von einem Angreifer verwendet werden.
- **GMER** – als Anti-Rootkit-Tool entwickelt nutzen Bedrohungsakteure es, um Sicherheitsprozesse auszuhebeln.
- **7Zip/GZip/WinRar** – diese Komprimierungstools nutzen Angreifer, um Daten zu kombinieren, zu verkleinern und zu exfiltrieren. In der Regel zu Erpressungszwecken.
- **Nirsoft tools** – eine Sammlung von Tools zur Passwort-Wiederherstellung, Deinstallation von Software plus: Möglichkeit, Befehlszeilentools ohne Anzeige einer Benutzeroberfläche auszuführen.
- **IOBit** – bringt leistungsstarke Deinstallationsfunktionen mit und wird häufig zum Entfernen von Sicherheitssoftware verwendet.
- **ProcDump** – ein Debugging-Tool, das den Speicher auf die Festplatte auslagern kann. Es ermöglicht Angreifern, speicherinterne Informationen wie Anmeldedaten offenzulegen.

Wie setzen Cyberkriminelle PUAs ein?

Die Konfiguration von Sicherheitsrichtlinien, die PUAs zulassen, sollte deshalb mit Bedacht erfolgen. Denn ein solcher Freifahrtschein ist für die Cyberkriminellen Gold wert und zudem besteht keinerlei Einblick in Verwendung, Absicht und Kontext des Tools.

Wurde ein Tool ausgeschlossen, kann ein Bedrohungsakteur dennoch versuchen, es zu installieren und zu nutzen, selbst wenn es noch nicht auf einem bestimmten Gerät installiert ist. Die als „Living off the land" bekannte Angriffstechnik setzt allerdings voraus, dass Angreifer bereits vorhandene Funktionen und Tools nutzen, um eine Entdeckung so lange wie möglich zu vermeiden. Sie ermöglichen den Akteuren eine ganze Reihe von Dingen: Auskundschaften, Zugriff auf Anmeldedaten, Berechtigungserweiterungen, Umgehung von Verteidigungsmaßnahmen, Persistenz, laterales Bewegen im Netzwerk, Sammeln und Exfiltration von Daten – ohne dass auch nur ein einziges Warnsignal ausgelöst wird.

Sobald der Gegner bereit ist, die letzte Phase seiner Attacke auszurollen (zum Beispiel Ransomware), ist es schon zu spät: Die Sicherheitstools des Unternehmens sind bereits deaktiviert (durch PSKill oder IOBit), ein hohes Maß an Zugriffsrechten wurde erlangt (durch GMER oder ProcDump), Daten liegen schon im Dark Web (in 7Zip-Dateien) und die Malware ist bereits auf wichtigen Systemen (oder schlimmer, auf Domain Level File Shares wie SYSVOL oder NETLOGON) zur Ausführung vorbereitet (durch PSExec). Je mehr PUAs die Angreifer finden können, desto größer ist ihr Aktionsradius.

Wie können Sie PUAs im Unternehmen zulassen?

Im ersten Schritt gilt es, die aktuellen globalen Ausnahmen im Unternehmen zu überprüfen: Sind sie notwendig? Wird ein Grund für die Ausnahme genannt – oder war sie „schon immer da"? Verantwortliche sollten nachforschen, warum die Sicherheitslösung die PUA zunächst einmal erkannt hat – könnte sie bereits böswillig genutzt werden? Müssen die Ausschlüsse wirklich für ALLE Server und Endgeräte gelten? Ist das Admin-Tool immer noch erforderlich, oder lässt es sich auf eine integrierte Funktion ausweichen? Ist mehr als ein Tool nötig, um das gleiche Ergebnis zu erzielen?

Sophos empfiehlt, PUAs nur streng kontrolliert zuzulassen: nur für bestimmte Anwendungen, bestimmte Geräte, bestimmte Zeiten und bestimmte Anwender. Dies kann über eine Richtlinie mit der erforderlichen Ausnahme erreicht werden, die bei Bedarf auch wieder rückgängig gemacht wird. Jede entdeckte, unerwartete Nutzung von PUAs sollte untersucht werden, da sie ein Hinweis darauf sein kann, dass sich Cyberkriminelle bereits Zugang zu den Systemen verschafft haben.

Tipp #6: Seien Sie immer einen Schritt voraus

Die Welt der Cybersicherheit entwickelt sich mit unglaublicher Dynamik und ist mit einer riesigen, weltweit ausgetragenen Schachpartie zu vergleichen. Auch hier geht es um Züge, Gegenzüge und einer ständig wechselnden Anzahl von Spielern. Wenn Sie in Ihrem Unternehmen irgendeine Art von Informationstechnologie verwenden, dann haben Sie keine andere Wahl, als das Spiel mitzuspielen. Aber das Spiel wird nicht automatisch zu Ihren Gunsten entschieden. Ihre Angreifer sind rund um die Uhr aktiv. Sie können überall auf der Welt sein, verstecken ihre Züge und suchen ständig nach Schwachstellen in Ihrer Verteidigungslinie; und sie werden sogar versuchen, Ihre eigenen Figuren gegen Sie einzusetzen.

In der Praxis bedeutet dies, dass Ihre Cyberabwehr ebenfalls rund um die Uhr einsatzbereit sein muss. Sie müssen Ihre Schwachstellen finden und sie beseitigen, bevor ein Gegner sie findet. Und Sie müssen sich auch darüber im Klaren sein, was der Gegner unternehmen könnte, wenn er eine Schwachstelle findet.

Patching

Das regelmäßige Patchen von Betriebssystemen und Anwendungen ist zweifelsohne wichtig. Die allerhöchste Priorität sollte jedoch das Patchen Ihrer von außen zugänglichen Systeme haben: Laut dem Sophos Active Adversary Playbook 2021 ist die Ausnutzung von öffentlich zugänglichen Anwendungen eine der fünf häufigsten Techniken für einen Erstzugriff. Zu den bekanntesten aktuellen Beispielen gehören die Microsoft-Exchange-Schwachstellen ProxyLogon (auch bekannt als Hafnium) und ProxyShell sowie eine Confluence-Schwachstelle, die innerhalb kürzester Zeit ausgenutzt wurde. Auch VPN-Lösungen mehrerer großer Anbieter und WordPress, die Anwendung hinter vielen Websites, sind immer wieder beliebte Angriffsziele.

Nur durch eine gründliche Erfassung Ihrer öffentlich zugänglichen Systeme sind Sie daher in der Lage, diese Systeme auf Schwachstellen zu überwachen und sie so schnell wie möglich zu patchen. Warten Sie nicht erst auf Nachrichten über die Ausnutzung einer Sicherheitslücke oder darauf, dass ein Anbieter eine CVE-Meldung (Common Vulnerability and Exposure) erstellt, um auf Schwachstellen und Sicherheitsrisiken hinzuweisen. Microsoft stellte im April und Mai 2021 Patches für Exchange Server zur Behebung von ProxyShell-Sicherheitslücken bereit. Allerdings wurden diese Schwachstellen erst am 13. Juli bekannt gegeben, was viele zu der Annahme verleitete, die Patches seien nicht wichtig.

Bedrohungslandschaft

Sich über die neuesten Taktiken, Techniken und Verfahren von Bedrohungsakteuren auf dem Laufenden zu halten ist entscheidend, um bei diesem Spiel die Oberhand zu behalten. So lautet die erste Regel: Kenne deinen Feind. Wenn Sie über eine Meldung erfahren, dass die Zugangsdaten von 500.000 VPN-Benutzern im Dark Web aufgetaucht sind, und Sie die gleiche VPN-Technologie verwenden, sollten Sie das überprüfen. Wenn Sie hören, dass Exchange für die Verbreitung von Ransomware ausgenutzt wird, und Sie einen Exchange-Server betreiben, sollten Sie weitere Untersuchungen durchführen.

Hier einige hilfreiche Informationsquellen:

- https://www.bleepingcomputer.com
- https://us-cert.cisa.gov
- https://www.ncsc.gov.uk/section/keep-up-to-date/reports-advisories
- https://www.cyber.gov.au
- https://news.sophos.com/de-de/
- https://nakedsecurity.sophos.com

Schatten-IT

Es kommt immer wieder vor, dass in bestimmten Geschäftsbereichen die IT umgangen wird, um eine eigene Lösung zu implementieren. Diese sogenannte Schatten-IT entsteht häufig, wenn Abteilungen sich einer Prüfung entziehen oder ein Projekt beschleunigen wollen. Vielleicht hat auch die IT-Abteilung die Anfrage abgelehnt, sodass sie nach einem Workaround suchen. Auch wenn diese Schatten-IT-Lösung nicht verboten wurde, heißt das nicht, dass Sie sie einfach ignorieren können. **Entweder sorgen Sie dafür, dass die Lösung vollständig in eine Silo-Infrastruktur integriert wird oder dafür, dass sie auf andere Weise genau kontrolliert wird**. Die enge Zusammenarbeit mit den Geschäftsbereichen bei der Suche nach erfolgreichen Lösungen trägt dazu bei, Schatten-IT zu verhindern, aber Sie müssen dabei auch auf neue Systeme und Anwendungen achten, die Sie gefährden könnten.

Immer die aktuelle Lage im Blick

Vielleicht sind Sie mit dem derzeitigen Sicherheitsstatus Ihres Unternehmens sehr zufrieden. Aber es braucht nur ein kompromittiertes Konto, eine kleine Firewall-Änderung oder einen Zero-Day-Exploit, um einem Bedrohungsakteur Zugang zu verschaffen. Selbst wenn der Angreifer diesen Zugang während Ihrer Geschäftszeiten findet, wird er abwarten und erst dann zugreifen, wenn Sie nicht auf der Hut sind. Ein kürzlich veröffentlichter Sicherheitshinweis des FBI und der CISA warnte Unternehmen vor einem höheren Angriffsrisiko an Feiertagen und Wochenenden und belegte dies durch bekannte Sicherheitsverletzungen bei Colonial Pipeline, JBS und Kaseya. Wie bereits erwähnt, wurde Confluence als Schwachstelle ausgenutzt, und zwar zu Beginn des Labor-Day-Wochenendes in den USA.

Wir empfehlen Unternehmen, einen Managed Service Provider zu beauftragen, der einen 24/7 Service anbietet und bei Sicherheitsverletzungen sofort eingreifen kann – selbst wenn diese z. B. mitten in der Nacht oder am Wochenende passieren. Ein Experte, der Einblick in die weltweite Lage in puncto IT-Sicherheit hat und entsprechend handelt, um Ihre Sicherheitsrisiken zu minimieren. Achten Sie darauf, dass Sie einen Anbieter wählen, der proaktiv Maßnahmen ergreift, anstatt Sie bei Sicherheitsvorfällen nur zu benachrichtigen.

Tipp #7: Planen Sie im Vorfeld für den Ernstfall

Bisher haben wir uns primär mit dem Thema Prävention befasst, indem wir von anderen Unternehmen gelernt haben, die von Sicherheitsvorfällen betroffen waren. Dieser Abschnitt geht nun darauf ein, welche Maßnahmen Sie ergreifen können, sollten Sie unglückliches Opfer eines Angriffs werden. Wie können Sie den Schaden minimieren und aus den Folgen die passenden Konzepte ableiten? Obwohl es im Folgenden insbesondere um Ransomware geht, gelten viele unserer Empfehlungen auch für andere Arten von Sicherheitsverletzungen, etwa den Befall durch Coinminer und Industriespionage.

Mit einem Plan ist viel gewonnen

Einen Plan für die Reaktion auf einen Vorfall (Incident Response Plan) zu haben, ist wichtig. Damit legen Sie die Maßnahmen fest, die Sie im Falle einer Sicherheitsverletzung oder einem Angriff ergreifen müssen. **Folgende Fragestellungen sind die Grundlage für einen Incident Response Plan:** Wie schwerwiegend ist der Vorfall? Wo befinden sich die kritischen Systeme und wie sind sie zu isolieren? Wie und mit wem soll kommuniziert werden? Wer ist zu kontaktieren und welche Maßnahmen sind zu ergreifen? Was ist mit den Sicherheitskopien? Der Plan sollte einfach und überschaubar sein, damit er in einer Situation mit hohem Druck leicht zu befolgen ist. Und es ist wichtig, dem verantwortlichen Team zu vertrauen, dass es selbstständig denkt und agiert. Das SANS Incident Handler's Handbook und der Incident Response Guide von Sophos enthalten beide ausführliche Abschnitte zur Vorbereitung.

Unverzüglich Hilfe anfordern

Bevor Sie sich bei einem Angriff darum kümmern, Computer und Systeme neu anzulegen oder wiederherzustellen oder gar ein Lösegeld auszuhandeln, sollten Sie **zuallererst professionelle Hilfe anfragen**. Die Reaktion auf Angriffe erfordert spezielle Kenntnisse, und die meisten Unternehmen beschäftigen keine Incident-Response-Spezialisten für einen Vorfall, von dem jeder hofft, dass er nie eintritt.

Ein vorausschauender Plan beinhaltet auch die Kontaktdaten von mehreren Incident-Response-Dienstleistern. Von mehreren Dienstleistern deswegen, weil die Kapazitäten der Incident-Response-Spezialisten bei häufigen oder groß angelegten Angriffen sehr schnell an ihre Grenzen stoßen können. Wenn sich der Angriff gegen Server und Endgeräte richtet, z. B. bei einem Ransomware-Vorfall, sollte zunächst der Anbieter für die Endpoint-Sicherheit kontaktiert wenden, wenn dieser einen Incident Response Service anbietet. Er verfügt wahrscheinlich über Telemetriedaten der betroffenen Umgebung und hat Zugang zu vorinstallierten Tools wie EDR/XDR, mit denen er schnell helfen kann. Die meisten Sicherheitsvorfälle resultieren übrigens nicht aus einem Versagen der Sicherheitslösung, sondern aus Fehlern von Menschen oder Prozessen.

Weitere Hilfen, die Sie nach Bedarf in Anspruch nehmen sollten:

- In jedem Fall ist es ratsam, sich an die örtlichen Strafverfolgungsbehörden zu wenden. Mit hoher Wahrscheinlichkeit handelt es bei dem Sicherheitsvorfall um ein Verbrechen, und möglicherweise verfügen die entsprechenden Behörden über hilfreiche Ressourcen.
- Darüber hinaus muss der Vorfall auch der Versicherungsgesellschaft gemeldet werden, sofern Sie über eine Cyberversicherung verfügen.
- Im Falle einer Zusammenarbeit mit einem Technologieanbieter oder Systemintegrator kann dieser möglicherweise bei der Wiederherstellung der Sicherheitskopien helfen.

Isolieren und eindämmen

Hier gibt es keine allgemeingültige Empfehlung, außer dass der Vorfall **so gut wie möglich isoliert und eingedämmt werden sollte**. Dazu gehört auch das Ausschalten der Stromversorgung, das Trennen der Internetverbindung und der Netzwerkkabel, eine softwarebasierte Isolierung, die Anwendung von Deny-All-Firewall-Regeln und das Herunterfahren kritischer Systeme. Sollte ein noch funktionsfähiger Domänencontroller zur Verfügung stehen, gilt es, diesen wenn möglich zu erhalten, indem man den Server herunterfährt und/oder vom Netz trennt. Auch Backups sollten isoliert und vom Netzwerk getrennt sein. Darüber hinaus gilt es, alle mutmaßlich kompromittierten Kennwörter zu ändern und die Konten zurückzusetzen.

Wichtig beim Einsatz von Incident-Response-Diensten, die größtenteils über das Internet erbracht werden, ist die Beratung darüber, wie betroffene Systeme und Verbindungen wieder in Betrieb genommen werden können. Sobald ein Anzeichen von Ransomware bemerkt wird, ist der Angriff in der Regel bereits abgeschlossen. Es ist jedoch wichtig, die Bedrohungsakteure vor Beginn der Wiederherstellungsarbeiten auszuschalten, damit sie nicht erneut zuschlagen können.

Kein Lösegeld zahlen

Zwar klingt die Zahlung des Lösegelds nach einem „einfachen" Ausweg, ermutigt die Kriminellen aber zu weiteren kriminellen Taten. Außerdem sind die Zeiten, in denen das Lösegeld ein paar Hundert Euro für den Entschlüsselungs-Code beträgt längst vorbei: Dem Sophos State of Ransomware Report 2022 zufolge zahlten mittelständische Unternehmen im vergangenen Jahr durchschnittlich 812.360 Euro Lösegeld. Die Angreifer suchen zudem nach kritischen Daten, exfiltrieren diese, um sie im Darknet zu verkaufen, löschen Backups und verschlüsseln dann die Daten. Die Sophos-Studie ergab, dass nur 61 Prozent der verschlüsselten Daten nach einer Lösegeldzahlung wiederhergestellt werden konnten und mehr als ein Drittel der Daten trotz Lösegeldzahlung verloren war.

Ransomware hat, wie jede Software, Fehler und Schwachstellen. Und auch die Cyberkriminellen, die hinter der Schadware stehen, können schlechte Tage haben. Dies kann zwar gelegentlich zum Vorteil des Opfers sein, erschwert jedoch in aller Regel die Entschlüsselung der Daten. Außerdem verschwinden Ransomware-Banden plötzlich und tauchen unter neuem Namen wieder auf. Im schlimmsten Fall haben die Opfer überhaupt keinen Zugang zu einem Entschlüsselungs-Code.

Hinzu kommt, dass die gesetzliche Lage bei Lösegeldzahlungen weltweit unterschiedlich ist. Es ist deshalb ratsam, sich über etwaige Gesetze in dem Land (oder den Ländern) zu informieren, in dem Ihr Unternehmen tätig ist.

Beweise aufbewahren

Allzu oft passiert es, dass Opfer von Attacken hauptsächlich damit beschäftigt sind, ihre Systeme und Dienste so schnell wie möglich wiederherzustellen. Dabei gehen viele Informationen verloren, die dazu beitragen würden, die Ursache zu ermitteln und das Ausmaß der Sicherheitsverletzung zu verstehen. Ein gutes Beispiel ist die Lösegeldforderung: Selbst wenn keine Absicht besteht, zu zahlen oder den Gegner zu kontaktieren, ist die Nachricht der Angreifer aus forensischer Sicht interessant. Diese Nachricht kann einem Incident-Response-Team Aufschluss darüber geben, mit wem sie es zu tun hat und welche Taktiken diese Gruppe üblicherweise anwendet. Sie könnte sogar einen ganz neuen Stamm von Ransomware und die verwendeten Taktiken, Techniken und Verfahren (TTPs) offenbaren.

So bekamen wir vor kurzem zum ersten Mal Einblick in die Lockfile-Nachricht und konnten nachvollziehen, wie die Ransomware Lockbit 2.0 nachahmte, aber eine viel aggressivere Strategie verfolgte. Diese wertvollen Erkenntnisse konnten wir jetzt für jeden nachfolgenden Lockfile-Angriff verwenden, insbesondere im Hinblick auf die frühzeitige Erkennung von Indicators of Breach (IoB). Bewahren Sie die Lösegeldforderung auf – in der Regel handelt es sich um einfache Text- oder HTML-Dokumente, die leicht an anderer Stelle gespeichert werden können.

Ein weiteres interessantes Element zur Analyse ist natürlich die Ransomware oder Malware selbst. Der Industriestandard sieht vor, dass diese in eine Archivdatei mit dem Kennwort "virus" oder "infected" eingefügt und an einem sicheren Ort aufbewahrt werden. Die passwortgeschützte .zip-Datei kann bei Bedarf sicher an Analysten weitergegeben werden. Mit einem Reverse-Engineering kann der Modus Operandi ermittelt werden, was den Einsatzkräften und Ermittlern hilft, die Suche nach dem Schaden einzugrenzen.

Auch die Aufbewahrung der Images von Systemen und virtuellen Maschinen ist wichtig. Um wichtige Beweise im Falle einer Gerichtsverhandlung vorlegen zu können, sollten alle forensischen Beweise verschlüsselt gespeichert und der SHA256-Wert zum Zeitpunkt der Erfassung aufgezeichnet werden. So können Unternehmen auch im Falle einer gerichtlichen Prüfung von Versicherungsansprüchen Beweise vorlegen oder gegenüber einer staatlichen Stelle nachweisen, dass sie nicht gegen Offenlegungsvorschriften verstoßen haben.

Schuldzuordnung und Vergeltung

In vielen Fällen stecken mehrere Gruppen hinter einem Ransomware-Angriff. Gruppe eins verschafft sich möglicherweise den ursprünglichen Zugang. Sie verkauft den Zugang an Gruppe zwei. Gruppe zwei nutzt den Ransomware-as-a-Service von Gruppe drei, um den Angriff auszuführen. Die verschiedenen Gruppen und Gruppenmitglieder sind oft über viele Länder verteilt. Es ist schwierig, den Einbruch einer einzelnen Gruppe zuzuordnen und das Wissen wird zudem im Chaos nach einer Attacke nicht viel helfen. Mit den Informationen aus der Lösegeldforderung und den Gemeinsamkeiten in den Taktiken, Techniken und Verfahren (TTPs) können erfahrene Incident-Response-Experten in der Regel sehr schnell erkennen, mit wem sie es zu tun haben.

Vom Versuch der Vergeltung, dem so genannten „Hack Back", wird hingegen dringend abgeraten. Er ist in aller Regel illegal und kann die Situation zudem noch verschlimmern.

Die Rolle der Cyberversicherung

Bei einem Cyberangriff, der durch eine Cyberversicherung abgedeckt ist, wird ein Schadensregulierer der Versicherungsgesellschaft zunächst einen externen Rechtsbeistand beauftragen. Dieser organisiert interne und externe Ressourcen und koordiniert die Aktivitäten bis zur Behebung des Vorfalls. Bei einem Ransomware-Angriff umfassen diese Service-Aktivitäten in der Regel Folgendes:

- Festlegung von Rollen und Zuständigkeiten, Ermittlung des Ausmaßes beziehungsweise der Auswirkungen, Festlegung von Kommunikationspräferenzen
- Untersuchung und Analyse der aktiven Bedrohung, Schadensbegrenzung, Identifizierung von Indicators of Compromise (IoC)
- Falls erforderlich, die Ernennung eines Spezialisten, der bei der Handhabung und Verhandlung der Lösegeldforderung berät
- Bei Bedarf die Ernennung eines Spezialisten, der über die Art des Datenzugriffs, der Exfiltration und der Wiederherstellung berät. Ermittlung der kostengünstigsten Methode zur Wiederherstellung der Daten (Lösegeldzahlung, Entschlüsselung, Backups usw.)
- Durchführung von Präventivmaßnahmen, Zugriffseliminierung für die Angreifer, Festlegung eines Zeitplans für den Vorfall
- Erstellung eines Abschlussberichts, der den Status der Umgebung, die Ursachenanalyse, die Art des Angriffs und die identifizierten Taktiken, Techniken und Verfahren der Bedrohungsakteure enthält.

Die meisten Versicherungsgesellschaften verfügen über eine „Anbieterauswahl" von Spezialisten für jede der oben genannten Aktivitäten. Aber es lohnt sich, beim Abschluss einer Versicherung im Voraus zu klären, welche Aktivitäten und welche spezialisierten Anbieter im Falle eines schweren Cyberangriffs abgedeckt sind. Die meisten Cyberversicherungen akzeptieren die Nutzung bereits vorhandener Dienstleister – dennoch sollte die Kompatibilität anderer Anbieter und Dienstleister im Voraus sichergestellt sein. Denn der Austausch zwischen Sicherheitsexperten während eines Vorfalls verursacht sowohl zusätzliche Arbeit als auch ein Sicherheitsrisiko. Beispielsweise verhindert die vorhandene Lösung oft die Eskalation des Angriffs und sollte daher nicht entfernt werden.

Kommunikation

Die Kommunikation wird durch Cyberangriffe oft schwer beeinträchtigt. E-Mail-Systeme sind möglicherweise offline, elektronische Kopien von Versicherungspolicen oder Incident-Response-Pläne sind verschlüsselt und der Angreifer überwacht möglicherweise die Kommunikation. Daher ist es ratsam, eine alternative Kommunikationsmöglichkeit bereitzuhalten, z. B. eine Instant-Messaging-Anwendung. Über einen separaten Kanal können das gesamte Team und alle anderen Beteiligten kommunizieren. Versicherungsdaten, Incident-Response-Pläne und Kontakte zu den Incident-Response-Experten sollten gesondert und in physischer Form aufbewahrt sein.

Training

Die Simulation des Ernstfalls eignet sich hervorragend, um die Reaktion auf eine Datenpanne oder ein Ransomware-Ereignis zu üben. Um die Übung realistischer zu gestalten, sollte diese z. B. um 2 Uhr morgens an einem langen Wochenende stattfinden und die Nutzung des E-Mail-Systems des Unternehmens ausschließen.

Weitere Informationen

Die unten stehenden Artikel erläutern eindrücklich, mit welchen Folgen Sie zu rechnen haben, wenn Sie von einigen der häufigsten Ransomware-Familien betroffen sind. Ein hilfreiches Instrumentarium, das Ihnen die Auswirkungen der jeweiligen Angriffsformen erläutert – jedoch wesentlich „schmerzfreier" als ein erfolgreicher echter Cyberangriff.

- Was Sie erwartet, wenn Sie von der Ransomware REvil betroffen sind
- Was Sie erwartet, wenn Sie von der Ransomware Avaddon betroffen sind
- Was Sie erwartet, wenn Sie von der Ransomware Conti betroffen sind

Wie Sophos helfen kann

Auch wenn viele der Empfehlungen in diesem Bericht keine Anschaffung von Tools erforderlich machen, sind Investitionen in Next-Gen-Cybersecurity-Lösungen ein sicherer Weg, um Ihr Unternehmen vor den modernsten Bedrohungen zu schützen.

24/7/365 Threat Hunting and Response – Sophos Managed Detection and Response (MDR)

Die ausgeklügelsten Cyberangriffe werden von Menschen durchgeführt und erfordern eine entsprechende Reaktion durch ein Expertenteam. Mit dem 24/7 MDR-Service von Sophos ergänzen Sie Ihre mehrschichtige Sicherheitsstrategie um menschliche Expertise. Unser Expertenteam sucht in Ihrem Auftrag proaktiv nach potenziellen Bedrohungen und überprüft diese. Bei entsprechender Genehmigung durch den Auftraggeber ergreifen die Experten Maßnahmen, um Bedrohungen auszuschalten, einzudämmen und unschädlich zu machen, und geben konkrete Ratschläge, um die Ursache wiederholt auftretender Vorfälle zu bekämpfen.
Mehr über Sophos MDR erfahren

Blitzschnelle Reaktion auf Vorfälle – Sophos Rapid Response

Sollte der Ernstfall eingetreten sein, bietet Sophos Rapid Response blitzschnelle Soforthilfe durch ein Expertenteam beim Erkennen und Beseitigen aktiver Bedrohungen. Egal was bei Ihnen vorliegt – eine Infektion, eine Kompromittierung oder ein unbefugter Zugriff, bei dem versucht wird, Ihre Sicherheitskontrollen auszuhebeln: Wir beseitigen das Problem.
Mehr über Sophos Rapid Response erfahren

Abwehr optimieren, Erkennungs- und Reaktionszeiten minimieren - Sophos Endpoint

Der Endpoint-Schutz von Sophos Intercept X nutzt mehrere Verteidigungsebenen, um Cyberattacken im Keim zu ersticken. Anti-Exploit-Technologien stoppen die Taktiken, Techniken und Verfahren der Angreifer, Deep Learning blockiert die Ausführung von Ransomware, und CryptoGuard verhindert unbefugte Datei-Verschlüsselungen bzw. setzt betroffene Dateien in ihren sicheren Ursprungszustand zurück.

Die Extended Detection and Response (XDR)-Funktionen von Sophos ermöglichen Unternehmen, Endpoints, Server, Firewallsysteme und andere Daten vor Angriffen durch frühzeitige Erkennung und Reaktion zu schützen. Sie erhalten die Informationen und kontextbezogenen Einblicke, die Sie benötigen, um schneller und zielgerichteter handeln zu können.
Mehr über Sophos Endpoint erfahren | Mehr über Sophos XDR erfahren

Starker Schutz und höchste Leistung – Sophos Firewall

Mit der Sophos Firewall erhalten Sie eine Fülle von Technologien, die Ihr Unternehmen vor ständig neuen Cyberangriffen schützen. Die Sophos Firewall verfügt über eine der marktweit leistungsstärksten und effektivsten IPS Engines und bietet eine einfache und elegante Lösung zum Lockdown Ihrer RDP-Server.

Mit den flexiblen und einfachen Segmentierungs-Tools (z. B. Zonen und VLANs) der Sophos Firewall sichern Sie Ihr LAN, reduzieren das Risiko lateraler Bewegungen, verringern die Angriffsfläche und minimieren das Risiko und potenzielle Ausmaß einer Ausbreitung.
Mehr über die Sophos Firewall erfahren

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

2022-08-12 DE (PC)