Retrospektive - Folge 1:
Warum Admins ihre Lieblings-Tools lieber mit dem Skalpell statt mit dem Vorschlaghammer bearbeitet sollten

Was können wir aus den Fallbeispielen, in denen Unternehmen Opfer von Cyberangriffen werden, lernen? In einer mehrteiligen Artikelserie reisen die Sophos-Experten zurück in die Zukunft und widmen sich verschiedenen spezifischen Aspekten der IT-Sicherheit, um Empfehlungen abzuleiten, die für jeden umsetzbar sind.

Wie im Sophos Active Adversary Playbook 2021 beschrieben, greifen Angreifer gerne auf Tools zurück, die von IT-Administratoren und Sicherheitsexperten verwendet werden, um so die Erkennung verdächtiger Aktionen zu erschweren. Viele dieser Tools werden von Sicherheitsprodukten als „Potenziell Unerwünschte Anwendungen“, kurz PUA (oder auch RiskWare bzw., RiskTool) erkannt, sind aber von IT-Teams für den täglichen Gebrauch unerlässlich. Für den Umgang damit müssen sich Administratoren hinsichtlich der IT-Policy des Unternehmens zwei zentralen Fragen stellen: Müssen alle Anwender in der Lage sein, diese Dienstprogramme zu nutzen und müssen diese Dienstprogramme auf jedem Gerät ausgeführt werden können?

Was sind PUAs?
PUAs sind Admin-Tools, die mit einem Betriebssystem gebündelt sind (z.B. PowerShell) und bieten Möglichkeiten zur Automatisierung und Verwaltung von Geräten in einem Netzwerk. 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.

Warum die Ausschlussliste der IT problematisch ist
Sofern Admin-Tools intern vom eigenen IT-Team installiert und verwendet werden, sind diese Anwendungen nützliche Werkzeuge. Geschieht dies aber durch andere Anwender, gelten sie als PUAs und werden von seriösen Sicherheitslösungen für Endgeräte oft als solche gekennzeichnet. Um ihnen die ungehinderte Nutzung dieser Tools zu ermöglichen, fügen viele Administratoren die von ihnen verwendeten Tools einfach zu einer globalen Ausschluss- oder Zulassungsliste in ihrer Endpunktsicherheitskonfiguration hinzu. Leider ermöglicht diese Methode auch die Installation und Verwendung der Tools durch Unbefugte, oft ohne jegliche Überwachung, Warnungen oder Benachrichtigungen.

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 es den Akteuren, die Entdeckung, Zugriff auf Anmeldedaten, Berechtigungserweiterungen, Umgehung von Verteidigungsmaßnahmen, Persistenz, seitliche

Bewegungen im Netzwerk, Sammeln und die Exfiltration durchzuführen, ohne dass auch nur eine einzige rote Fahne geschwenkt wird.

Zulassen von PUAs im Unternehmen nur im kontrollierten Modus
Im ersten Schritt gilt es, die aktuellen globalen Ausnahmen im Unternehmen zu überprüfen:

- Sind sie notwendig?
- Wird ein Grund für den Ausschluss genannt – oder war er „schon immer da“? Verantwortliche sollten nachforschen, warum das 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?

Auf Basis zahlreicher Fallbeispiele empfiehlt Sophos, PUAs nur auf einer sehr kontrollierten Basis zuzulassen: bestimmte Anwendung, spezifische Maschinen, genaue Zeiten und ausgewählte Benutzer. Dies kann über eine Richtlinie mit dem erforderlichen Ausschluss erreicht werden, die bei Bedarf auch wieder entfernt wird. Jede entdeckte Nutzung von PUAs, die nicht erwartet wird, sollte untersucht werden, da sie ein Hinweis darauf sein kann, dass sich ein Cyberkrimineller bereits Zugang zu den Systemen verschafft hat.

Der komplette Artikel mit PUA-Beispielen steht als Download bereit unter:
https://news.sophos.com/de-de/2021/09/09/warum-admin-ihre-lieblings-tools-lieber-mit-dem-skalpell-statt-mit-dem-vorschlaghammer-bearbeitet-sollten/

Weitere Beiträge der Serie „Sicherheit in der Retrospektive“, wie beispielsweis zu den Themen „Passwort-Sicherheit“ und „Endpoint-Schutz“, werden in den nächsten Wochen auf dem Sophos-LinkedIn-Kanal veröffentlicht.

Neu: Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de