SOPHOS

So stoppen Sie aktive Angreifer: Neueste Erkenntnisse aus der Cybersecurity-Praxis

Wichtige Fakten für IT-Führungskräfte und Business Leader basierend auf der Analyse von 232 schwerwiegenden Cybervorfällen, die vom Sophos X-Ops Incident-Response-Team behoben wurden

Sophos-Whitepaper. Dezember 2023

Über diesen Guide

Hintergrund

In diesem Guide stellen wir Ihnen die wichtigsten Erkenntnisse aus der Analyse von 232 Cyberangriffen vor, die vom Sophos X-Ops Incident-Response-Team in 2022 und im ersten Halbjahr 2023 abgewehrt wurden. Dabei kombinieren wir die Ergebnisse aus den drei Sophos Active Adversary Reports aus dem Jahr 2023, um einen einzigartigen Einblick in die Taktiken, Techniken und Verfahren zu bieten, die aktuell von professionellen Cyberkriminellen eingesetzt werden.

Weitere Einzelheiten hierzu finden Sie unter:

- Active Adversary Report für Business Leader 2023
- Active Adversary Report für Tech Leader 2023
- Active Adversary Report für IT-Security-Experten 2023

Das Sophos X-Ops Incident-Response-Team

Sophos Rapid Response ist ein engagiertes Team von Response-Experten, die sich darauf spezialisiert haben, aktive Cyberangriffe abzuwehren und weiteren Schäden vorzubeugen. Jedes Unternehmen und jede Organisation, egal ob Sophos-Kunde oder nicht, kann bei einem akuten Angriff die Unterstützung unserer Experten anfordern.

Das Team steht rund um die Uhr zur Verfügung und besteht aus 50 Spezialisten für digitale Forensik sowie 35 Bereitstellungsexperten, die im Bedarfsfall gezielte Abwehrmaßnahmen ergreifen.

Außerdem wird Sophos Rapid Response von über 150 Analysten aus dem Security Operations Center (SOC) der Sophos Managed Detection and Response (MDR) Services unterstützt. Diese Analysten überwachen und schützen tagtäglich proaktiv Tausende von Kundenumgebungen und liefern aktuelle Einblicke darüber, welche Angreifer und Bedrohungen sie dort beobachten und stoppen. Weitere Unterstützung erhält das Team von unseren 400 Malware-Analysten aus den SophosLabs, die Experten im Entpacken, Analysieren und Blockieren von schädlichem Code sind.

Das Ziel der Sophos-Response-Experten besteht darin, akute Bedrohungen schnell zu erkennen, einzudämmen und zu beseitigen und Angreifer aus der Umgebung zu entfernen, um weitere Schäden zu verhindern.

Analyse von 232 Incident-Response-Fällen

Diese Studie umfasst 232 Cybervorfälle aus dem Jahr 2022 und dem ersten Halbjahr 2023, die von Sophos-Response-Experten in 35 Ländern und 25 Branchen behoben wurden.

83 % der Vorfälle ereigneten sich in Unternehmen/Organisationen mit weniger als 1.000 Mitarbeitern. Diese breit angelegte Analyse spiegelt das Verhalten von Angreifern in all seinen Facetten wider und liefert somit wertvolle Einblicke in die aktuelle Bedrohungslandschaft.

In der Analyse berücksichtigte Länder

Aktive Angreifer

Da sich dieser Report speziell mit Angriffen befasst, die von aktiven Angreifern ausgeführt werden, ist es wichtig, zu verstehen, wer diese Angreifer sind und wie sie vorgehen.

Wer sind aktive Angreifer?

Aktive Angreifer sind versierte Cyberkriminelle, die häufig umfassende Software- und Netzwerkkenntnisse besitzen. Sie sind meistens hochbezahlt und oft Teil eines professionellen Cybercrime-Netzwerks.

Wie gehen aktive Angreifer vor?

Aktive Angreifer infiltrieren die Systeme von Unternehmen und Organisationen, sorgen dafür, dass sie unerkannt bleiben und passen ihre Techniken kontinuierlich an. Mittels manuellem Hacking und KI-basierten Methoden umgehen sie präventive Sicherheitskontrollen und führen ihre Angriffe effektiv aus. Die kontinuierliche Anpassung ist dabei der Schlüssel zum Erfolg. Die Angreifer starten einen Angriff, sie sehen, was passiert, und reagieren entsprechend. Wenn sie beim ersten Mal nicht erfolgreich sind, greifen sie auf andere Methoden zurück, bis sie ihr Ziel erreicht haben.

Wer ist betroffen?

Die Annahme, dass aktive Angreifer nur größere Unternehmen und Organisationen ins Visier nehmen, ist falsch – von kleinen und mittleren Unternehmen bis hin zu Global Playern – alle sind gleichermaßen gefährdet. 24 % der IT-Führungskräfte in Unternehmen/Organisationen mit 100–250 Mitarbeitern haben im vergangenen Jahr einen Angriff mit einem aktiven Angreifer erlebt[1].

Aktive Angreifer nehmen nur selten ein bestimmtes Unternehmen oder eine bestimmte Organisation ins Visier. Vielmehr suchen sie gezielt nach Sicherheitslücken in der Cyberabwehr und schlagen zu, sobald sie fündig geworden sind.

1 Cybersecurity-Report 2023: Der Business Impact von Cyberangriffen, Sophos – Befragung von 3.000 IT-Entscheidern aus 14 Ländern

Schritt 1: Erstes Zugriffsereignis

Wir sehen uns zunächst an, wie Angreifer sich Zugang verschaffen.

Angriffsvektoren entwickeln sich weiter

Im Jahr 2022 waren ausgenutzte Schwachstellen mit 37 % die häufigste Angriffsursache, gefolgt von kompromittierten Zugangsdaten mit 30 %.

Diese Ergebnisse decken sich weitestgehend mit den Daten aus unserem Ransomware-Report 2023: Dort waren 36 % der Ransomware-Angriffe im Vorjahr auf ausgenutzte Schwachstellen und 29 % auf kompromittierte Zugangsdaten zurückzuführen.

Bei genauerer Betrachtung der vom Sophos Incident-Response-Team im Jahr 2022 behobenen Angriffe fällt auf, dass bei mehr als der Hälfte (55 %) der Angriffe, die mit Schwachstellen begannen, nur zwei Schwachstellen ausgenutzt wurden: ProxyShell und Log4Shell – für beide waren zum Zeitpunkt der Kompromittierung bereits Patches verfügbar.

In der ersten Jahreshälfte 2023 waren dann kompromittierte Zugangsdaten die häufigste Ursache. Sie kamen bei der Hälfte der vom Team behobenen Vorfälle zum Einsatz. Ausgenutzte Schwachstellen wurden in knapp einem Viertel (23 %) der Fälle als Zugangsmethode verwendet.

Es ist jedoch noch zu früh, um daraus eindeutig auf eine veränderte Taktik der Angreifer zu schließen. Denkbar wäre auch, dass in der ersten Hälfte des Jahres 2023 nicht so viele leicht ausnutzbare Schwachstellen verfügbar waren oder dass die Initial Access Broker Überbestände hatten, die sie günstig abtreten wollten. Sicher ist jedoch, dass kompromittierte Zugangsdaten, die mittels Phishing-Angriffen oder Datenschutzverletzungen erlangt werden, im Darkweb jederzeit leicht zu erwerben sind.

Angriffsursache

	2022	1. Hj. 2023
Ausgenutzte Schwachstellen	**37 %**	**23 %**
Kompromittierte Zugangsdaten	**30 %**	**50 %**

Quelle: Active Adversary Report für Business Leader, 2023, Sophos (n = 152); Active Adversary Report für Tech Leader, 2023, Sophos (n = 80)

Eine fehlende mehrstufige Authentifizierung (MFA) bietet Angreifern ein willkommenes Einfallstor

In vielen Unternehmen/Organisationen ist keine mehrstufige Authentifizierung (MFA) vorhanden. Dies macht es Angreifern leichter, kompromittierte Zugangsdaten zu missbrauchen. Bei weit über einem Drittel (39 %) der in der ersten Jahreshälfte 2023 behobenen Vorfälle wurde festgestellt, dass keine MFA implementiert war.

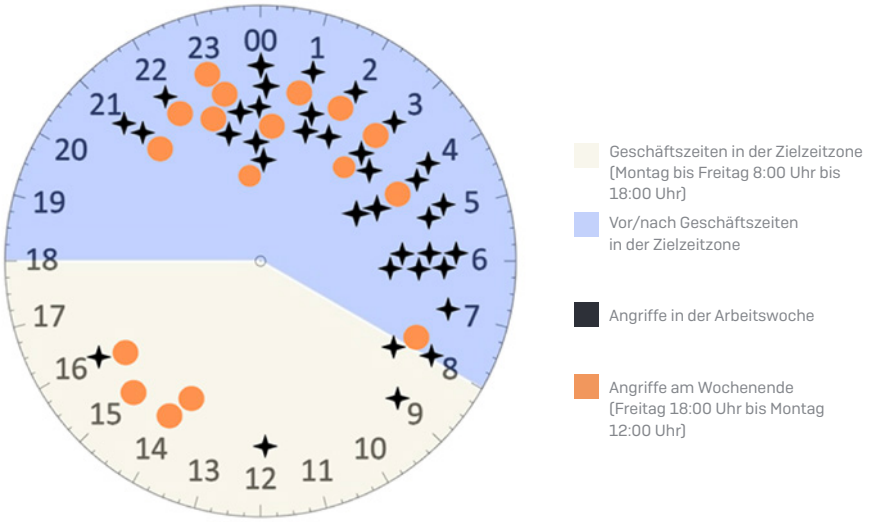
MFA ist keine komplett neuartige, ungetestete Technologie. Im Gegenteil: Sie ist ausgereift und leicht verfügbar. Es gibt daher keinen guten Grund, auf diese zusätzliche Sicherheitsvorkehrung zu verzichten. Wenn Sie keine MFA aktiviert haben, machen Sie es Angreifern unglaublich einfach, Ihr Unternehmen oder Ihre Organisation zu infiltrieren.

Angreifer schlagen gezielt außerhalb der Geschäftszeiten zu

Eine weitere wichtige Erkenntnis ist, dass Angreifer Unternehmen und Organisationen aktiv ins Visier nehmen, wenn eine höhere Wahrscheinlichkeit besteht, unerkannt zu bleiben (bei dieser Analyse haben wir uns auf Ransomware-Angriffe konzentriert, da sie die zuverlässigsten und objektivsten Indikatoren liefern).

43 % aller Ransomware-Angriffe wurden in der Zeitzone des Opfers an einem Freitag oder Samstag gestartet. Cyberkriminelle wählen absichtlich diese Tage, damit sie am Wochenende daran arbeiten können – wenn IT-Abteilungen voraussichtlich weniger aktiv Sicherheitswarnmeldungen überwachen und darauf reagieren.

Tatsächlich geht aus unseren Daten hervor, dass 9 von 10 Angriffen (91 %) außerhalb der normalen Geschäftszeiten in der Zeitzone des Opfers beginnen (d. h. nicht Montag bis Freitag zwischen 8:00 und 18:00 Uhr).



Zu welcher Tageszeit Ransomware-Angreifer zuschlagen

Die 24-Stunden-Uhr oben zeigt die Uhrzeit des Angriffs in der Zeitzone des Opfers an. Die orangefarbenen Punkte sind Angriffe am Wochenende (Freitag 18:00 Uhr bis Montag 12:00 Uhr) und die schwarzen Kreuze sind Angriffe an Wochentagen. Aus dem Schaubild geht klar hervor, dass die Angriffe besonders häufig zwischen 23:00 Uhr und 6:00 Uhr beginnen – Angreifer arbeiten also ganz bewusst nachts.

Wie viele Personen überwachen Ihr Netzwerk und reagieren für Sie außerhalb der normalen Geschäftszeiten aktiv auf Warnmeldungen und verdächtige Aktivitäten? Damit meinen wir keine Personen, die bei Bedarf angerufen werden können, sondern echte Analysten, die verdächtige Aktivitäten aktiv aufspüren und analysieren. Wenn Sie kein Personal haben, das Nächte, Wochenenden und Feiertage abdeckt, sollten Sie dringend Ihre Abwehrmaßnahmen überdenken.

Schritt 2: Interne Aktivität

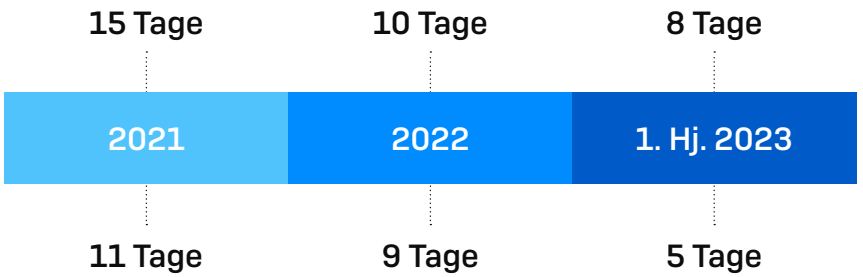
Wie gehen Angreifer vor, sobald sie in Ihr Netzwerk gelangt sind – und wie lange brauchen sie dafür?

Angreifer werden immer schneller

Sobald Angreifer in Ihr Netzwerk eingedrungen sind, bewegen sie sich schnell. In den letzten zweieinhalb Jahren haben Angreifer ihr Tempo beschleunigt. Dies ist teilweise auf Verbesserungen bei den Abwehrfunktionen zurückzuführen, die wiederum schnellere Angriffe erforderlich gemacht haben. Außerdem werden Angreifer immer versierter – je mehr Angriffe sie ausführen, desto schneller werden sie.

Die Verweildauer ist die Zeit, die ein Angreifer in Ihrer Umgebung verbringt, bevor er erkannt wird. Bei erfolgreichen Cyberangriffen bleiben Angreifer in der Regel bis zu dem Zeitpunkt unentdeckt, an dem sie ihren Angriff starten, z. B. wenn sie ihre Ransomware in Umlauf bringen und mit der Verschlüsselung von Dateien beginnen. Daher bedeutet eine kürzere Verweildauer eine insgesamt schnellere Ausführung von Angriffen. Die Verweildauer ist zudem der Zeitraum, innerhalb dessen Sie einen aktiven Angreifer erkennen und beseitigen können, bevor er sein Ziel erreicht.

Durchschnittliche Verweildauer: alle Vorfälle



Durchschnittliche Verweildauer: Ransomware-Vorfälle

Im Schaubild haben wir die durchschnittliche Verweildauer von Cybervorfällen allgemein (oben) der durchschnittlichen Verweildauer von Ransomware-Vorfällen (unten) gegenübergestellt.

- Im Jahr 2021 betrug die Verweildauer 15 Tage für Vorfälle allgemein und 11 Tage für Ransomware.
- 2022 verkürzte sich die Verweildauer für Vorfälle allgemein auf 10 Tage und für Ransomware auf 9 Tage.
- In der ersten Jahreshälfte 2023 fiel die Verweildauer noch kürzer aus: acht Tage für Vorfälle allgemein und nur fünf Tage für Ransomware.

In Anbetracht dieser Entwicklung und der Erkenntnis, dass Angreifer immer häufiger nach Feierabend zuschlagen, stehen Unternehmen und Organisationen, die über keine 24/7-Sicherheitsabdeckung verfügen, einer immer weiter wachsenden Herausforderung gegenüber. Wenn ein Angreifer seinen Ransomware-Angriff am Freitagabend um 21:00 Uhr startet, Sie die verdächtigen Aktivitäten und Warnmeldungen aber erst am Montagmorgen um 9:00 Uhr bemerken, haben Sie bereits eine wichtige Chance vertan, den Angreifer zu erkennen und ihn aus Ihrer Umgebung zu entfernen.

Quelle: Active Adversary Playbook 2022, Sophos (n = 144); Active Adversary Report für Business Leader, 2023, Sophos (n = 152); Active Adversary Report für Tech Leader, 2023, Sophos (n = 80)

Die Verweildauer variiert je nach Angriffstyp

Die Abbildung rechts zeigt die Verweildauer verschiedener beliebter Angriffstypen. Wir sind bereits auf die Zahlen für Ransomware eingegangen. Darüber hinaus sind vor allem die folgenden Angriffsmethoden erwähnenswert:

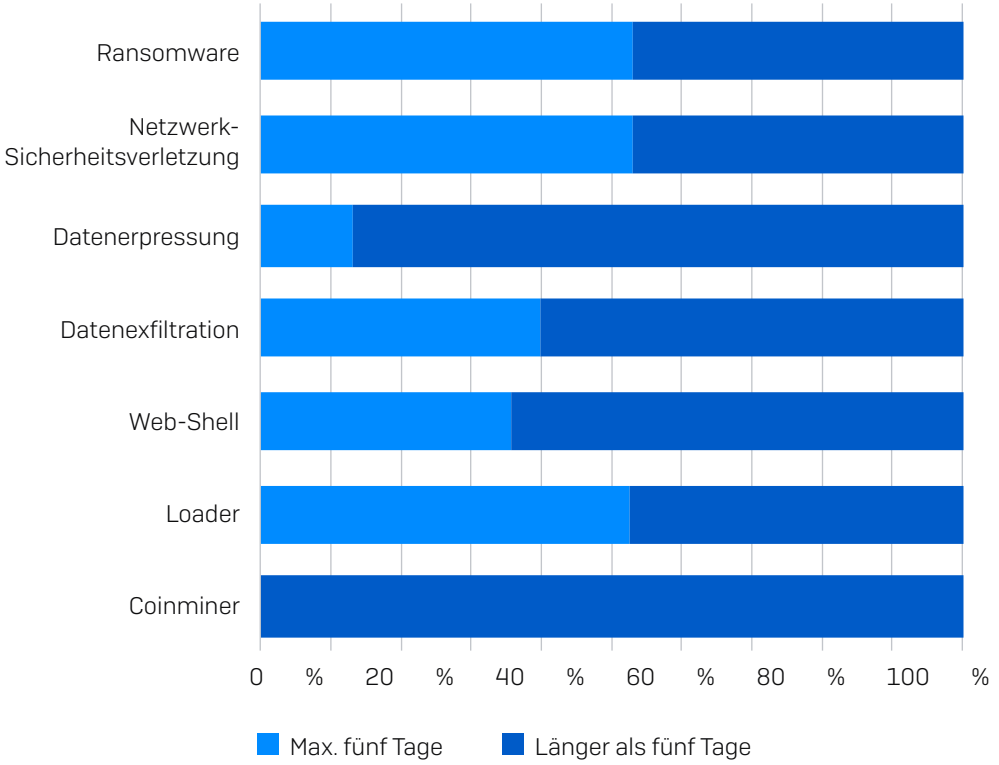
Coinminer haben eine sehr lange Verweildauer, sind aber auch auf eine langfrisitige Ausführung ausgelegt. Coinminer nisten sich auf Servern ein und schürfen über Monate hinweg langsam aber stetig Cent-Beträge.

Datenerpressung: Die meisten, aber nicht alle Angriffe dieses Typs fielen in die Kategorie „langsamere" Angriffe. Bei einem Erpressungsangriff verblieben die Angreifer länger im Netzwerk als in Fällen, in denen Daten einfach exfiltriert, aber keine Erpressung durchgeführt wurde.

Da es bei diesen Angriffen keine Verschlüsselungskomponente gibt, können die Angreifer vermutlich unauffälliger und demzufolge langsamer und gezielter agieren.

Datenexfiltration ist eine Variante der Datenerpressung (alle Erpressungen beinhalten eine Form der Exfiltration, aber nicht alle Exfiltrationen beinhalten Erpressung), die aus ähnlichen Gründen eine längere Angriffsdauer umfasst. („Datenexfiltration" umfasst in unserer Analyse Fälle, in denen Daten das betroffene Netzwerk nachweislich verlassen haben, aber keine weiteren Informationen darüber vorliegen, wie der Angreifer mit diesen Daten weiter verfahren ist.)

Verweildauer nach Angriffstyp, 2022–1. Hj. 23



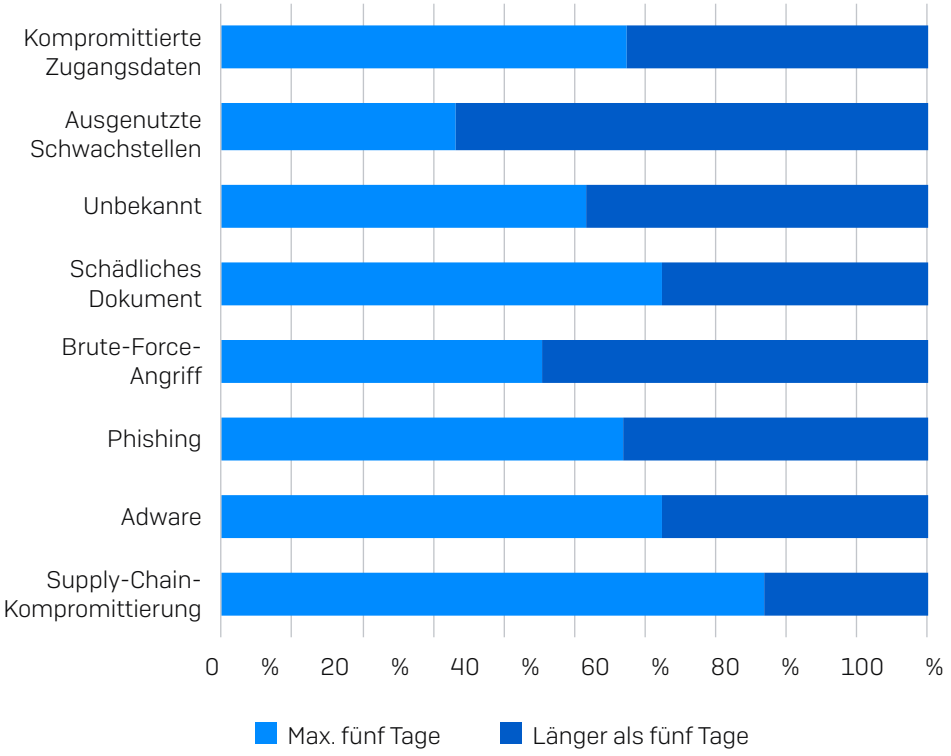
Die Verweildauer variiert je nach Ursache

Wir haben bereits gesehen, dass die häufigsten Ursachen von Angriffen kompromittierte Zugangsdaten und ausgenutzte Schwachstellen waren. Aber wie variiert die Verweildauer je nach Ursache?

In der Regel bewegten sich Angriffe, die mit kompromittierten Zugangsdaten begannen, schneller als Angriffe, deren Ursache eine ausgenutzte Schwachstelle war. Mehr als die Hälfte der Angriffe, die mit kompromittierten Zugangsdaten begannen, hatten eine Verweildauer von maximal fünf Tagen, verglichen mit einem Drittel der Angriffe, die mit einer ausgenutzten Schwachstelle begannen.

Ein bemerkenswerter Ausreißer sind in diesem Fall Supply-Chain-Angriffe, bei denen mehr als drei Viertel eine Verweildauer von weniger als fünf Tagen hatten. Supply-Chain-Kompromittierungen sind die „Fertiggerichte" der Bedrohungswelt: Alle Zutaten werden zur Verfügung gestellt und sind einsatzbereit – es geht nur noch um die Ausführung.

Verweildauer nach Ursache, 2022–1. Hj. 23



Angreifer stürzen sich auf Active Directory

Die Ergebnisse der Vorfallanalysen legen nahe, dass Angreifer, sobald sie in ein Unternehmensnetzwerk eingedrungen sind, alles daran setzen, mittels lateraler Bewegung so schnell wie möglich auf Active Directory(AD)-Server zu gelangen. Tatsächlich betrug die durchschnittliche Zeit bis zum Erreichen von AD für Angriffe in der ersten Jahreshälfte 2023 nur 0,68 Tage – etwa 16 Stunden.

Durchschnittliche Zeit bis zum Erreichen von Active Directory für Angriffe im 1. Halbjahr 2023

Quelle: Active Adversary Report für Tech Leader, 2023, Sophos (n = 80)

Diese Ergebnisse in Kombination mit den bereits erwähnten Daten zum Angriffszeitpunkt machen deutlich, dass AD sich außerhalb der Geschäftszeiten leicht kompromittieren lässt.

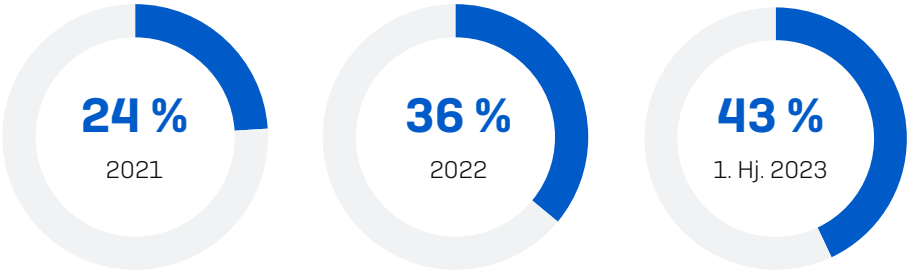
Für einen Angreifer gibt es viele operative Gründe, sich auf Active Directory zu konzentrieren. Hat ein Angreifer erst einmal auf einem AD-Server Fuß gefasst, baut er seinen Spielraum erheblich aus. Denn ein AD-Server ist in der Regel die leistungsfähigste und privilegierteste Ressource in einem Netzwerk. Er ist in der Lage, Identitäten und Richtlinien im gesamten Unternehmen zu kontrollieren. Angreifer können privilegierte Konten ausnutzen, neue Konten erstellen oder legitime Konten deaktivieren.

Auch AD-Server können sie dazu missbrauchen, Malware von einer vertrauenswürdigen Quelle zu verbreiten. Und wenn die Angreifer ungestörten Zugriff auf eine AD-Umgebung haben, stellen sie oft fest, dass die Server nur mit Microsoft Defender oder gar nicht geschützt sind.

Die Deaktivierung des Schutzes ist mittlerweile Standard

In den letzten Jahren sind Angreifer sehr geschickt darin geworden, Cybersecurity-Software zu deaktivieren: Mittlerweile beobachten wir bei fast der Hälfte der von Sophos-Response-Experten bekämpften Angriffe eine solche Deaktivierung.

Prozentualer Anteil von Kompromittierungen, bei denen Angreifer den Schutz deaktivieren



Quelle: Active Adversary Playbook 2022, Sophos (n = 144); Active Adversary Report für Business Leader, 2023, Sophos (n = 152); Active Adversary Report für Tech Leader, 2023, Sophos (n = 80)

Ausnutzung legitimer IT-Tools (Living off the Land)

Angreifer nutzen häufig legitime IT-Tools aus, um Schutztechnologien zu überlisten. In der folgenden Tabelle sind die am häufigsten ausgenutzten legitimen IT-Tools (fachsprachlich auch als „Living-off-the-Land"-Binärdateien bezeichnet) aufgeführt.

Top 10 „Living-off-the-Land"-Binärdateien (LOLBins), die im Rahmen der Analyse beobachtet wurden

RANG	MAX. 5 TAGE	MEHR ALS 5 TAGE	RANG
1	RDP	RDP	1
2	PowerShell	PowerShell	2
3	PsExec	cmd.exe	3
4	cmd.exe	PsExec	4
5	Taskplaner	Net.exe	5
6	net.exe	Taskplaner	6
7	rundll32.exe	rundll32.exe	7
8	ping.exe	WMI	8
9	reg.exe	ping.exe	9
10	vssadmin.exe	whoami.exe	10

Wir unterscheiden hier zwischen schnellen Angriffen (maximal fünf Tage) und langsameren Angriffen (mehr als fünf Tage). Remote Desktop Protocol (RDP) ist das sowohl bei schnellen als auch langsameren Angriffen am häufigsten missbrauchte IT-Tool, dicht gefolgt von PowerShell.

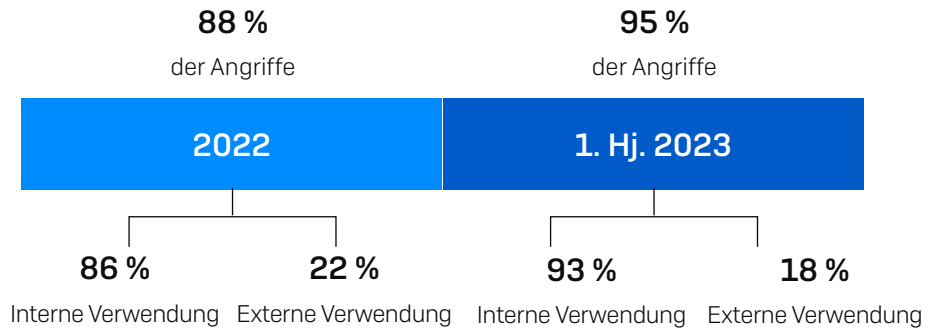
Zudem tauchen acht Tools auf beiden Seiten der Tabelle auf, und wenn wir die Liste auf die Top 20 Binärdateien erweitern, erscheinen 90 % sowohl auf der schnellen als auch auf der langsamen Liste.

Wenn Sie Anzeichen verdächtiger Aktivitäten mit diesen Tools erkennen, sollten Sie unverzüglich eine Analyse einleiten.

Allgegenwärtigkeit von RDP bei Angriffen

Wie aus der Abbildung unten hervorgeht, verwenden Angreifer gerne RDP. Tatsächlich spielte RDP in der ersten Jahreshälfte 2023 bei ganzen 95 % der Angriffe eine Rolle – ein nochmaliger Anstieg gegenüber 2022, als der Wert bereits bei 88 % lag.

Einsatz von RDP bei Angriffen



Quelle: Active Adversary Report für Business Leader, 2023, Sophos (n = 152); Active Adversary Report für Tech Leader, 2023, Sophos (n = 80)

Viele gehen davon aus, dass RDP von Angreifern vor allem dazu genutzt wird, um sich Zugriff auf Unternehmen und Organisationen zu verschaffen. Tatsächlich verwenden Angreifer RDP jedoch weit häufiger, nachdem sie sich Zugriff verschafft haben, um ihre Angriffe voranzutreiben.

In der ersten Jahreshälfte 2023 wurde RDP bei 93 % der Vorfälle zur internen Fortbewegung und nur bei 18 % der Vorfälle extern verwendet. Im Jahr 2022 betrug der Anteil der internen Verwendung 86 %, der externen Verwendung 22 %.

Die Daten verdeutlichen, dass RDP bei einer Reihe von Vorfällen sowohl für den internen als auch für den externen Zugriff genutzt wurde. Es wird jedoch selten ausschließlich für den externen Zugriff verwendet – sowohl 2022 als auch in der ersten Jahreshälfte 2023 kam dies in nur 2 % der Fälle vor.

Wenn Sie sich also bei Ihrer Suche nach missbräuchlicher RDP-Nutzung nur auf die mögliche Infiltrierung Ihres Unternehmens/Ihrer Organisation von außen konzentrieren, lassen Sie den häufigsten Anwendungsfall der internen Fortbewegung von Angreifern außer Acht.

Vernichten von Beweisen

Um ihre Spuren zu verwischen, vernichten viele aktive Angreifer Beweise für ihre Aktivitäten. In 82 % der Fälle, in denen Telemetrie-Protokolle fehlten, hatten Cyberkriminelle diese deaktiviert oder gelöscht.

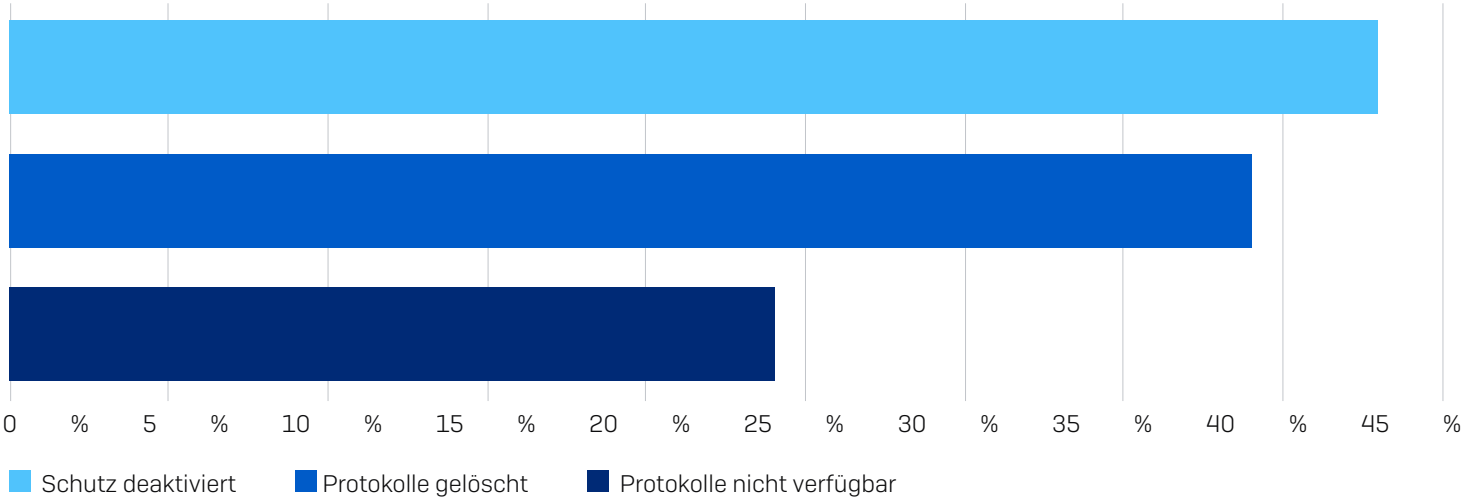
Bei der Reaktion auf eine akute Bedrohung ist Zeit ein entscheidender Faktor: Die Zeit zwischen der Erkennung des ersten Zugriffsereignisses und der vollständigen Beseitigung der Bedrohung sollte so kurz wie möglich sein.

Je weiter ein Angreifer in der Angriffskette gelangt ist, desto aufwendiger sind die Bereinigungsmaßnahmen. Fehlende Telemetriedaten machen diesen Prozess noch langwieriger und kostspieliger. Deshalb ist eine vollständige und genaue Protokollierung unerlässlich.

Da Microsoft nun begonnen hat, die Protokollierung für Basislizenzen kostenlos anzubieten (Stand: September 2023), ist es empfehlenswert, diese Vorteile vollständig auszuschöpfen.

Und wie viele andere Datentypen sollten Protokolle ordnungsgemäß gesichert werden, damit sie im Falle forensischer Analysen zur Verfügung stehen.

Ursachen fehlender Telemetrie, 1. Hj. 23



Gründe, warum den Analyse-Experten bei Vorfällen in der ersten Jahreshälfte 2023 keine Telemetriedaten zur Verfügung standen. Da bei einem Angriff mehrere Gründe zutreffen können, ergeben die Prozentsätze in Summe mehr als 100 Prozent.

Wichtige Erkenntnisse für die Cyberabwehr

Basierend auf den Erkenntnissen aus Vorfällen, die von Sophos-Response-Experten behoben wurden, empfehlen wir Ihnen zur Abwehr aktiver Angreifer die folgenden Maßnahmen:

Machen Sie es Angreifern so schwer wie möglich

Wenn Ihre Systeme gut gewartet sind, müssen Angreifer sich besonders anstrengen, um diese zu manipulieren. Das kostet wertvolle Zeit und erhöht die Gefahr, erkannt zu werden. Ausgefallene Techniken wie BYOVD-Angriffe (Bring Your Own Vulnerable Driver) stehen auf der Liste der meisten Angreifer an vierter oder fünfter Stelle – nachdem alles andere versagt hat und sie schwerere Geschütze auffahren müssen.

Robuste, mehrschichtige Abwehrsysteme, die auf automatischem und adaptivem Schutz basieren, nehmen Angreifern den Wind aus den Segeln und sperren Bedrohungsakteure ohne Spezialkenntnisse von vornherein aus.

Schützen Sie alles

Angreifer nutzen jeden Schwachpunkt, den sie finden können, um in Ihre Umgebung einzudringen. Einmal nach innen gelangt, bewegen sie sich fort und starten die nächsten Phasen ihrer Angriffe. Sorgen Sie dafür, dass Ihre gesamte Umgebung geschützt ist – Sie sind nur so stark wie Ihr schwächstes Glied. Außerdem liefern starke Abwehrmechanismen wertvolle Telemetriedaten, mit denen die Bedrohungserkennung und -reaktion beschleunigt werden kann.

Überwachen Sie Ihre Umgebung 24/7

Wenn Sie Ihre Sicherheitsmaßnahmen auf die Geschäftszeiten beschränken, bemerken Sie wichtige Anzeichen für Angriffsaktivitäten erst, wenn es zu spät ist.

Seien Sie jederzeit bereit und reagieren Sie sofort

Ein Notfallplan ist wichtig, aber Sie müssen auch in der Lage sein, umgehend zu handeln. Wenn Sie rechtzeitig reagieren, müssen Sie vielleicht nur ein kleines Problem beheben, anstatt zu einem späteren Zeitpunkt anhand von Backups Ihre gesamte Umgebung wiederherstellen zu müssen. Stellen Sie sicher, dass Sie Reaktionspläne für die häufigsten Angriffstypen haben, die Ihr Unternehmen/Ihre Organisation am ehesten beeinträchtigen könnten. Und spielen Sie die Implementierung dieser Pläne mit Ihren Sicherheitsexperten und anderen Stakeholdern durch, auf die Sie sich im Ernstfall verlassen müssen.

Wie Sophos helfen kann

Sophos X-Ops

Sophos X-Ops bietet kollektives Expertenwissen über die gesamte Angriffsumgebung zur effektiven Abwehr hochkomplexer Bedrohungen. Die vom Team veröffentlichten Materialien bieten Experteneinblicke und -empfehlungen, die IT-Mitarbeiter dabei unterstützen, ihre Unternehmen und Organisationen erfolgreich zu schützen.

Veröffentlichungen des X-Ops-Teams finden Sie unter news.sophos.com/category/threat-research.

Alternativ können Sie X-Ops auf X unter dem Handle @SophosXOps folgen. Das Team verwendet dasselbe Handle auf InfoSec Exchange.

Services und Produkte von Sophos

Sophos bietet eine Reihe branchenführender Lösungen, mit denen aktive Angreifer erkannt und gestoppt werden können. Dazu gehören ein 24/7 Managed Detection and Response Service, Incident Response Support und adaptive Endpoint Protection.

Um mehr zu erfahren, starten Sie eine kostenlose Testversion oder sprechen Sie mit unserem Team.

Weitere Informationen zu Sophos-Lösungen finden Sie unter www.sophos.de

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.

2023-12-15 (WP-NP)

SOPHOS