Angriffe auf Microsoft 365 aufspüren

Mit zunehmendem mobilen Arbeiten rückt die Microsoft-Cloud in den Fokus von Angreifern. Bereits ein einziger kompromittierter Benutzer im Azure Active Directory gewährt Zugriff auf alle genutzten Microsoft-Dienste. Threat Hunting ermöglicht es, Anzeichen einer Kompromittierung frühzeitig aufzudecken und weiteren Schaden zu verhindern.

Von Tabea Nordieker

Cloud-Dienste ermöglichen einen Zugriff auf Firmendaten und -ressourcen von überall auf der Welt aus. Das Cloud-Office-Paket Microsoft 365 (M365) mit Exchange Online, Microsoft Teams und SharePoint ist daher ein viel genutztes Produkt im Firmenalltag.

Da diese Ressourcen von überall aus zugänglich sein sollen, ist die Benutzer- und Zugriffsverwaltung das Herzstück jeder Cloud. Sie stellt sicher, dass nur berechtigte Benutzer, Systeme und Applikationen auf die Daten zugreifen können. M365 nutzt dazu das Azure Active Directory (AAD). Wenn ein AAD-Konto kompromittiert wird, bedeutet das aber auch, dass der Angreifer Zugriff auf alle M365-Dienste und die zugehörigen Daten erlangt hat.

Das Benutzerkonto im Visier

Erfahrungsgemäß nutzen Angreifer jede Gelegenheit, die sich ihnen bietet, für ihre Zwecke aus. So wie man das lokale Netzwerk und seine Systeme absichern sollte, muss man zwingend die Dienste in der Cloud schützen – mit demselben Schutzlevel. Wie man das AAD härten kann, um Angriffe darauf zu verhindern oder zumindest zu minimieren, zeigt [1]. Aber selbst wenn alle Sicherheitsmaßnahmen umgesetzt wurden, bleibt ein zentraler Angriffspunkt bestehen: das Benutzerkonto.

Die drei häufigsten Vorgehensweisen, an diese Zugangsinformationen zu gelangen, sind Phishing-, Brute-Force- und Passwort-Spraying-Angriffe [2]. Bei einem Brute-Force-Angriff versucht der Angreifer durch Ausprobieren das Passwort zu erraten. Solche Angriffe sind deutlich in den Sign-in-Logdateien des AAD-Portals erkennbar. Besonders verdächtig sind mehrere fehlgeschlagene Anmeldeversuche in kürzester Zeit. Wenn darauf eine erfolgreiche Anmeldung folgt, die von einer unbekannten IP-Adresse ausgeht, wurde der Benutzer mit hoher Wahrscheinlichkeit kompromittiert. Hinweise auf eine nicht legitime Anmeldung können eine IP-Adresse sein, die aus einer anderen Region stammt als der Arbeitsort des betroffenen Benutzers, oder eine plötzliche Veränderung der IP-Adresse im Vergleich zu den letzten Tagen und Wochen.

Die Tabelle „Auszug aus den Sign-in-Logs des Azure-Portals“ zeigt einen Ausschnitt aus den Sign-in-Logs des Azure-Portals mit einer Reihe fehlgeschlagener Anmeldungen aus den Niederlanden innerhalb weniger Sekunden (siehe Einträge 1 bis 8). Die Log-in-Versuche fanden im Sekundentakt statt, wobei der Status jeweils fehlgeschlagen ist. In der „Failure Reason“ ist ersichtlich, dass die Zugangsdaten nicht die richtigen sind. Dieser Angriff zog sich über mehrere Tage hin, bis schließlich mit derselben IP-Adresse aus den Niederlanden ein erfolgreicher Log-in erfolgte (Eintrag 9).

Zugangsdaten – Lieblingsbeute der Hacker

Ein Passwort-Spraying-Angriff ist eine besondere Art eines Brute-Force-Angriffs. Dabei versucht ein Angreifer nicht nur das Passwort eines einzelnen Users zu erraten, sondern probiert die gängigsten Passwörter parallel bei mehreren Benutzerinnen und Benutzern durch. In der Regel verhindert dieses Vorgehen eine Sperrung des Benutzers. Ein Passwort-Spraying-Angriff verläuft unauffälliger als ein Brute-Force-Angriff, ist aber dennoch in den Logdaten erkennbar.

Phishingangriffe verleiten einen Benutzer dazu, seine Zugangsdaten auf ei-

iX-TRACT

- Microsoft 365 rückt als beliebte Cloud-Umgebung in den Fokus der Angreifer.
- Das Azure Active Direcory ist für das Nutzermanagement verantwortlich. Ein kompromittierter Benutzer bedeutet für einen Angreifer Zugriff auf alle M365-Dienste.
- Mit einem Threat Hunting hält man proaktiv nach Angriffen auf die Cloud Ausschau. Dabei wird nach Spuren bekannter Angriffsszenarien gesucht.

Auszug aus den Sign-in-Logs des Azure-Portals

Referenz	Date (UTC)	User	Ressource	IP Address	Location	Status	Failure Reason
1	2022-10-09 07:47:18	User A	Office 365 Exchange Online	185.222.58.60	Amsterdam, Noord-Holland, NL	Failure	Error validating credentials due to invalid username or password.
2	2022-10-09 07:47:19	User A	Office 365 Exchange Online	185.222.58.60	Amsterdam, Noord-Holland, NL	Failure	Error validating credentials due to invalid username or password.
3	2022-10-09 07:47:19	User A	Office 365 Exchange Online	185.222.58.60	Amsterdam, Noord-Holland, NL	Failure	Error validating credentials due to invalid username or password.
4	2022-10-09 07:47:20	User A	Office 365 Exchange Online	185.222.58.60	Amsterdam, Noord-Holland, NL	Failure	Error validating credentials due to invalid username or password.
5	2022-10-09 07:47:21	User A	Office 365 Exchange Online	185.222.58.60	Amsterdam, Noord-Holland, NL	Failure	Error validating credentials due to invalid username or password.
6	2022-10-09 07:47:21	User A	Office 365 Exchange Online	185.222.58.60	Amsterdam, Noord-Holland, NL	Failure	Error validating credentials due to invalid username or password.
7	2022-10-09 07:47:29	User A	Office 365 Exchange Online	185.222.58.60	Amsterdam, Noord-Holland, NL	Failure	Error validating credentials due to invalid username or password.
8	2022-10-09 07:47:29	User A	Office 365 Exchange Online	185.222.58.60	Amsterdam, Noord-Holland, NL	Failure	Error validating credentials due to invalid username or password.
	[...]						
9	2022-10-10 10:38:10	User A	Office 365 Exchange Online	185.222.58.60	Amsterdam, Noord-Holland, NL	Success	Other.

ner gefälschten Webseite des Angreifers einzugeben, der so an das Passwort gelangt. Eine Anmeldung mit durch Phishing erlangten Log-in-Daten ist nicht anhand fehlgeschlagener Anmeldeversuche erkennbar. Diese Hinweise liefern andere Artefakte in den Logdateien – zum Beispiel die Region, aus der die Anmeldung erfolgte, die verwendete Applikation oder der genutzte Browser.

Wenn plötzlich Anmeldungen aus einem anderen Land auftreten, die nicht durch Reisetätigkeiten zu erklären sind, sollte man prüfen, ob die Ursache möglicherweise die Nutzung eines Virtual Private Networks (VPN) sein kann. Auch dokumentieren die Sign-in-Logs, von welchem Gerät aus sich der Benutzer anmeldet. Plötzliche Wechsel des Betriebssystems oder des verwendeten Browsers können ebenso verdächtig sein wie Versionssprünge von neu nach alt.

Wenn die Anmeldung beim Dienst Exchange Online erfolgt, kann die verwendete Applikation ein weiterer Hinweis sein. Dies ist in den Sign-in-Logs der Tabelle „Sign-in-Logs von Exchange Online“ ersichtlich. Hier handelt es sich erneut um einen Brute-Force-Angriff, der in diesem Fall von verschiedenen IP-Adressen aus erfolgt. Geschwärzt sind die IP-Adressen, über die sich der legitime Benutzer anmeldete. Dazwischen befinden sich erfolgreiche Anmeldungen des Benutzers, zwischen denen erfolgreiche Anmeldungen von Angreifern aus Mexiko und der Ukraine zu sehen sind (Eintrag 9 und 10). Ein solcher räumlicher Wechsel innerhalb einer knappen Stunde ist ein gutes Beispiel eines „Impossible Travel“. In der Spalte „Client App“ ist ersichtlich, dass der legitime Benutzer sich über den Webservice anmeldet (Eintrag 7, 8, 11, 12), der Angreifer hingegen nutzt das Protokoll IMAP.

Das AAD verfügt über Mechanismen, um solche Auffälligkeiten in den Anmeldungen darzustellen. Im Bereich Risky Sign-ins oder Risky Users des Azure-

Sign-in-Logs von Exchange Online

Referenz	Date (UTC)	IP Address	Location	Status	Failure Reason	Client App
1	2022-10-10T07:25:11Z	112.165.87.176	Gyeongsan, Gyeongsangbuk-Do, KR	Failure	The account is locked, you've tried to sign in too many times with an incorrect user ID or password.	IMAP
2	2022-10-10T07:25:16Z	112.165.87.176	Gyeongsan, Gyeongsangbuk-Do, KR	Failure	The account is locked, you've tried to sign in too many times with an incorrect user ID or password.	IMAP
3	2022-10-10T07:25:23Z	77.38.238.41	Riga, Riga, LV	Failure	The account is locked, you've tried to sign in too many times with an incorrect user ID or password.	IMAP
4	2022-10-10T07:25:25Z	77.38.238.41	Riga, Riga, LV	Failure	The account is locked, you've tried to sign in too many times with an incorrect user ID or password.	IMAP
5	2022-10-10T07:42:56Z	196.0.118.106	Kampala, Kampala, UG	Failure	The account is locked, you've tried to sign in too many times with an incorrect user ID or password.	IMAP
6	2022-10-10T07:42:56Z	196.0.118.106	Kampala, Kampala, UG	Failure	The account is locked, you've tried to sign in too many times with an incorrect user ID or password.	IMAP
7	2022-10-10T08:19:56Z	[redacted]	Geneve, Geneve, CH	Success	Other.	Exchange Web Services
8	2022-10-10T09:02:09Z		Geneve, Geneve, CH	Success	Other.	Exchange Active-Sync
9	2022-10-10T10:38:10Z	91.235.225.76	Vitryanka, Chernivets'ka Oblast', UA	Success	Other.	IMAP
10	2022-10-10T10:43:31Z	187.190.28.230	Mexico City, Distrito Federal, MX	Success	Other.	IMAP
11	2022-10-10T11:30:56Z	[redacted]	Zuerich, Zuerich, CH	Success	Other.	Exchange Web Services
12	2022-10-10T14:24:27Z		Zuerich, Zuerich, CH	Success	Other.	Browser

Erfolgreicher Angriff trotz MFA

Referenz	Date (UTC)	IP Address	Location	Status	Failure Reason	Multifactor Authentication Result	Conditional Access
1	2022-10-12 12:56:05	197.210.55.219	Lagos, Lagos, NG	Success	Other.	MFA requirement satisfied by claim in the token	Success
2	2022-10-12 12:55:38	197.210.55.219	Lagos, Lagos, NG	Success	Other.	MFA requirement satisfied by claim in the token	Success
3	2022-10-12 12:55:38	197.210.55.219	Lagos, Lagos, NG	Success	Other.	MFA requirement satisfied by claim in the token	Success
4	2022-10-12 12:55:38	197.210.55.219	Lagos, Lagos, NG	Success	Other.	MFA requirement satisfied by claim in the token	Success
5	2022-10-12 12:50:37	197.210.55.219	Lagos, Lagos, NG	Interrupted	Strong Authentication is required.	User needs to perform multi-factor authentication. There could be multiple things requiring multi-factor, e. g. Conditional Access policies, per-user enforcement, requested by client, among others.	Failure
6	2022-10-12 12:32:22	197.210.55.219	Lagos, Lagos, NG	Interrupted	Strong Authentication is required.	User needs to perform multi-factor authentication. There could be multiple things requiring multi-factor, e. g. Conditional Access policies, per-user enforcement, requested by client, among others.	Failure
7	2022-10-12 08:53:28	197.210.55.219	Lagos, Lagos, NG	Interrupted	Strong Authentication is required.	User needs to perform multi-factor authentication. There could be multiple things requiring multi-factor, e. g. Conditional Access policies, per-user enforcement, requested by client, among others.	Failure

Portals werden beispielsweise basierend auf der Geolokalisierung, der verwendeten IP-Adresse oder dem verwendeten Browser ungewöhnliche Anmeldungen dokumentiert (siehe dazu auch Microsoft Learn „What is risk?“, ix.de/z99w). Um von diesen Sicherheitsvorkehrungen zu profitieren, muss man regelmäßig in das Azure-Portal schauen oder idealerweise die Informationen an ein im Unternehmen eingesetztes SIEM (Security Information and Event Management) weiterleiten.

MFA-Fatigue-Angriffe mit App verhindern

Mit Multi-Faktor-Authentisierung (MFA) lassen sich solche Angriffe effektiv verhindern. Sie erfordert zusätzlich zum Passwort einen weiteren Faktor für eine erfolgreiche Anmeldung. Leider versuchen Angreifer verstärkt, MFA zu umgehen, beispielsweise durch einen MFA-Fatigue-Angriff. So nennt man es, wenn ein Benutzer mit MFA-Anfragen überhäuft wird, in der Hoffnung, dass er irgendwann ausreichend genervt oder verzweifelt ist und eine dieser Anfragen akzeptiert. Dieses Risiko lässt sich mit dem Einsatz einer Authenticator-App minimieren, indem anstelle von Push-Nachrichten die Codeeingabe aus der Authenticator-App vorgeschrieben wird. Microsoft hat hierzu einen lesenswerten Beitrag veröffentlicht (siehe ix.de/z99w). Diese Methode wird seit Neustem standardmäßig in AAD-Instanzen umgesetzt.

Ein MFA-Fatigue-Angriff ist in den Sign-in-Logs aus dem Azure-Portal ersichtlich (siehe Tabelle „Erfolgreicher Angriff trotz MFA“). Dabei kann in den Logdateien klar unterschieden werden, wann ein Passwort kompromittiert wurde (Eintrag 5, 6, 7), aber MFA nicht erfolgreich war (Status: Interrupted, Conditional Access: Failure), und wann der Zugriff auf das Benutzerkonto erfolgte (Eintrag 4) (Status: Success, Conditional Access: Success).

Gelingt es einem Angreifer, an die Zugangsdaten zu kommen, kann er auf alle verfügbaren Microsoft-Cloud-Dienste zugreifen. Eingeschränkt ist er nur durch die Berechtigungen des Benutzers.

Vorbereitungen zur Jagd

Wie erfolgreich ein Angreifer ist oder, besser gesagt, wie groß der durch ihn angerichtete Schaden ist, hängt unter anderem davon ab, wie lange er sich unbemerkt in der kompromittierten Umgebung bewegen kann. Genau an diesem Punkt setzt Threat Hunting an. Es handelt sich um eine Analyse ohne konkreten Anhaltspunkt, um unentdeckte Sicherheitsrisiken aufzuspüren, in diesem Fall in der Microsoft-Cloud. Dabei orientiert man sich an gängigen Angriffsszenarien, um Spuren möglicher verdächtiger Aktivitäten identifizieren zu können. Diese Art von Analyse hat einen präventiven Charakter, um die Sicherheit in der Cloud-Umgebung zu erhöhen und den Schaden zu minimieren, falls es bereits zu einer Kompromittierung gekommen ist.

Im Artikel „Forensik und Logging im Azure AD“ [3] wurden bereits erste Analysemöglichkeiten dargestellt, allerdings haben sich in der Zwischenzeit das Wissen und die Werkzeuge weiterentwickelt. Geblieben ist die Tatsache, dass alle relevanten Logs aus den unterschiedlichen Diensten zentral in den Unified Audit Logs (UAL) gespeichert werden. Bis ein Event allerdings in den UAL erscheint, kann es bis zu 24 Stunden dauern. Das muss bei einer Analyse berücksichtigt werden, denn falls die UAL direkt nach einer Kompromittierung exportiert werden, kann es sein, dass Informationen zu den Aktivitäten eines Angreifers noch nicht in den Logs stehen. Wie viele Events in den UAL gespeichert werden, ist von der M365-Lizenz abhängig.

Um die UAL für eine spätere Analyse exportieren zu können, ist ein Benutzerkonto mit globalen Leseberechtigungen im AAD erforderlich. Für einen vollumfänglichen Lesezugriff auf alle für eine Analyse relevanten Logs hat sich das folgende Vorgehen als zielführend herausgestellt:

- Im AAD einen neuen Benutzer erstellen, der nur für die Analyse genutzt wird. Es muss sich um einen Benutzer im AAD des Kunden (also im AAD des zu analysierenden und zu schützenden Systems) handeln. Ein Gastbenutzer kann zu Problemen mit den Berechtigungen führen.
- Dem Analyse-Benutzer die Rollen „Global Reader“ und „Security Reader“ zuweisen.

Aufbewahrungszeiten von Logs

Azure-Portal (siehe ix.de/z99w): Innerhalb des Webportals sind die Einträge der letzten 30 Tage einsehbar.

Unified Audit Logs: Mit einer E3-Lizenz können die Logdaten 90 Tage analysiert werden, mit einer E5-Lizenz sogar ein ganzes Jahr.

Advanced Hunting in M365 Defender: Mit diesem Tool können Rohdaten bis zu 30 Tage zurück inspiziert werden.

- Im Exchange-Online-Admin-Portal (siehe ix.de/z99w) eine neue Rolle erstellen.
- Dieser Rolle die Berechtigung „View-Only Audit Logs“ hinzufügen.
- Dem zuvor erstellten Analyse-Benutzer zusätzlich diese neue Rolle zuweisen.

Die erstellten Benutzer und Rollen sollten gut dokumentiert werden, sodass sie nach Abschluss der Analyse wieder gelöscht werden können.

Daten exportieren und untersuchen

Mit diesem Analyse-Benutzer sind alle Voraussetzungen geschaffen, die Logdateien zu exportieren und anschließend zu analysieren. Die Logs können auch direkt über die verschiedenen Produktportale heruntergeladen werden. Allerdings ist das nicht zu empfehlen, da die Gefahr besteht, nicht alle Events zu exportieren. Beispielsweise werden über das Microsoft-Compliance-Portal jeweils nur 50 000 Elemente pro Export heruntergeladen. Um solche Einschränkungen zu umgehen, kann man die Audit- und Sign-in-Logs mit einem PowerShell-Skript aus dem AAD exportieren (siehe Listing).

Für den Export der UAL bietet sich das Tool „Microsft 365 Extractor Suite“ an (siehe ix.de/z99w). Es ermöglicht einen kompletten Export der UAL oder durch das Setzen von Filtern nur der Protokolldateien eines bestimmten Benutzers, eines bestimmten Dienstes oder eines definierten Zeitraums. Abbildung 1 zeigt eine Übersicht aller Logquellen, die für diesen Tenant im Zeitraum vom 9. bis 13. April 2023 verfügbar waren, sowie die Anzahl der Einträge jeder Logdatei.

Die exportierten Logdateien kann man anschließend beispielsweise in einer vom SANS-Institut speziell dafür entwickelten virtuellen Maschine (VM) namens SOF-ELK (siehe ix.de/z99w) analysieren. Die exportierten Logs werden durch vorgefertigte Parser in die Datenbank eingelesen. Diese JSON-Objekte lassen sich anschließend in der Benutzeroberfläche gezielt mit Filtern und Suchen analysieren. Im Folgenden werden Suchparameter referenziert, die in der SOF-ELK oder in den entsprechenden Feldern anderer Analyseumgebungen eingesetzt werden können.

Um effizient nach Angriffsspuren zu suchen, hilft es, sich in die Rolle eines Angreifers zu versetzen. Nur wer die gängigen Angriffsmethoden kennt, kann gezielt nach daraus resultierenden Spuren in den Logdateien suchen. Eine Kompromittierung der Microsoft-Cloud-Umgebung kann unterschiedliche Auswirkungen haben: Einerseits können Angreifer Informationen ausspähen, die für weitere Angriffe nützlich sein können, andererseits können sie direkt Daten aus der Microsoft-Cloud abgreifen.

Um ans Ziel zu gelangen, können Angreifer Benutzerkonten manipulieren und so weitere Berechtigungen erlangen. Auch versuchen sie mit verschiedenen Ablenkungsmanövern, ihre eigentlichen bösartigen Aktionen zu verschleiern oder einen persistenten Zugriff einzurichten. Besonders der Zugriff auf ein E-Mail-Konto eröffnet viele Möglichkeiten, weitere Angriffe wie Phishing-Kampagnen oder Business E-Mail Compromise (BEC; [4]) durchzuführen.

Änderung der Zugriffsberechtigungen

Wenn ein Benutzer kompromittiert wurde, hat der Angreifer Zugriff auf dessen Konto bei den verschiedenen Onlinediensten. Das kann er ausnutzen, um mit den zugehörigen Berechtigungen die Benutzerkonten zu manipulieren: Er kann neue Benutzer oder Gruppen erstellen und Benutzer zu Gruppen hinzufügen oder entfernen. Dadurch kann der Angreifer einerseits versuchen, sich mehr Privilegien zu verschaffen, andererseits kann er das Vorgehen auch als Persistenzmechanismus einsetzen. Überdies kann er neue Applikationen oder Geräte im AAD hinterlegen oder deren Berechtigungen ausweiten.

All diese Aktivitäten lassen sich in den UAL nachvollziehen. Hier eine Auswahl interessanter Einträge:

- Operations: „Add user.“
- Operations: „Update user.“
- Operations: „Add member to group.“

Lässt sich der Zeitpunkt, wann ein Benutzer kompromittiert wurde, klar definieren, lohnt es sich, alle Aktivitäten dieses Benutzers im relevanten Zeitraum in den UAL zu filtern und sich einen Überblick zu verschaffen.

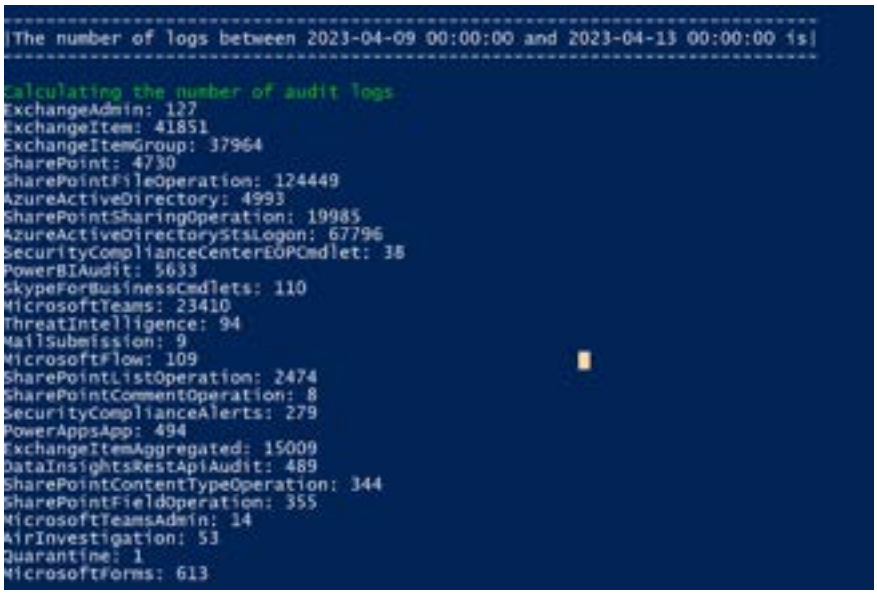
Hat ein Angreifer Zugriff auf ein Exchange-Online-Konto, sieht er alle darin befindlichen Informationen wie gesendete und erhaltene E-Mails, Kalendereinladungen und Kontakte. Mit diesen Informationen kann er weitere mögliche Opfer identifizieren oder in aktive Kommunikationen eingreifen.

Manipulation des E-Mail-Postfachs

Durch das Einrichten neuer oder das Ändern bestehender Weiterleitungsregeln kann er sicherstellen, dass er auch

Listing: Logs aus dem AAD exportieren

```
Connect-AzureAD$SignInLogs = Get-AzureADAuditSignInLogs -All $trueforeach ↵
                ($a in $SignInLogs) {$a | ConvertTo-Json -Compress | tee -a .\↵
          SignInLogs_full.json}$AuditLogs = Get-AzureADAuditDirectoryLogs -All↵
     $trueforeach ($a in $AuditLogs) {$a | ConvertTo-Json -Compress | tee -a .\↵
                                                          AuditLogs_full.json}
```



Beispiele von Logquellen der UAL eines Tenant in einem bestimmten Zeitraum (Abb. 1).

ohne oder bei geänderten Zugangsdaten weiterhin über den aktuellen E-Mail-Verkehr informiert bleibt. Dies ist ein typisches Szenario für einen Business E-Mail Compromise, bei dem ein Angreifer E-Mails mit Rechnungen und Zahlungsanweisungen abfängt und die Kontodaten des Empfängers manipuliert. Adressen, an die E-Mails in einem Postfach weitergeleitet werden, sind im Feld „parameters.ForwardingSmtpAddress.keyword“ zu sehen.

Eine andere Möglichkeit, den E-Mail-Verkehr zu beeinflussen, bietet das Erstellen von Transportregeln. Mit ihnen kann ein Angreifer beispielsweise festlegen, dass von jeder Mail eine Blindkopie (BlindCopyTo, bcc:) an ihn versendet wird. Diese Manipulation lässt sich mit folgenden Suchparametern identifizieren:

- Operations: „New-TransportRule“
- Operations: „Set-TransportRule“

Angreifer missbrauchen Assistenzfunktionen

An zusätzliche Informationen können Angreifer auch über das Einrichten einer Postfachdelegierung gelangen. Diesen zusätzlichen Zugriff auf ein Mailkonto kann man mit der Suche „Operations: ‚Add-MailboxPermission‘“ aufdecken. Wenn Regeln zum Senden einer E-Mail über ein anderes Postfach eingerichtet wurden, lässt sich das mit der Suche „Operations: ‚Add-RecipientPermission‘ AND parameters.AccessRights: ‚SendAs‘“ herausfinden.

Angreifer versuchen üblicherweise, ihre Aktivitäten zu verschleiern. Bei der Manipulation von Mailkonten funktioniert das, indem sie Postfachregeln erstellen oder bestehende verändern. So erreichen sie beispielsweise, dass von ihnen selbst versendete E-Mails direkt in den Ordner „gelöscht“ verschoben werden und dem regulären Benutzer nicht auffallen. Solche Aktivitäten sind mit den folgenden Suchparametern zu identifizieren:

Angreifer versuchen zwar, ihre Manipulationen zu verschleiern, aber die Logs bringen es an den Tag, hier zum Beispiel durch den gesetzten Parameter einer Inbox-Regel (Abb. 2).

- Operations: „New-InboxRule“
- Operations: „Set-InboxRule“

Im Feld „Name“ ist die Aktivität ersichtlich, beispielsweise „MoveToFolder“, wenn eine E-Mail in einen Ordner verschoben werden soll (siehe Abbildung 2). Der Name des entsprechenden Ordners wird dann im Feld „Value“ dokumentiert.

E-Mail missbräuchlich einsetzen

Kann sich ein Angreifer mit kompromittierten Zugangsdaten beim Dienst Exchange Online anmelden, hat er Zugriff auf ein legitimes E-Mail-Postfach, das er für weitere Angriffe verwenden kann. Das erhöht die Chancen, dass der Empfänger auf die Nachricht reagiert, da er den Absender eventuell kennt. So lässt sich vom kompromittierten E-Mail-Konto aus eine Phishingkampagne starten, um beispielsweise an weitere Zugangsdaten zu gelangen oder zusätzliche Systeme zu kompromittieren.

Wenn die Zahl der gesendeten Mails über dem konfigurierten Tageslimit liegt, kann das im Portal des Windows Defender Alarm auslösen. Eine solche Phishingkampagne ist in Abbildung 3 ersichtlich. In diesem Beispiel wurden an manchen Tagen über 5000 E-Mails von einem kompromittierten Benutzerkonto aus versandt.

Im Windows Defender kann man im Bereich „E-Mail & Collaboration“ den E-Mail-Versand überprüfen (Abb. 3).

Datenexfiltration de luxe

In der Microsoft-Cloud sind viele Informationen zu finden – zum einen über die Benutzer, Geräte und verwendeten Applikationen, zum anderen die Nutzerdaten, die in den verschiedenen Diensten entstehen. Ein Angreifer kann den erlangten Zugang zur Microsoft-Cloud nutzen, um Informationen zu sammeln. Das kann beispielsweise mit der Microsoft-Graph-API (siehe ix.de/z99w) erfolgen. Über sie kann man mit gezielten Abfragen auf die umfangreichen Daten der Microsoft-365-Plattform zugreifen.

Diese Informationen können entweder für einen weiteren Angriff nützlich sein oder das Opfer wird mit der Androhung ihrer Veröffentlichung erpresst. Daten können auf diversen Wegen abfließen, etwa durch das Einrichten von Weiterleitungsregeln in Exchange Online oder durch direktes Herunterladen aus den Diensten OneDrive oder SharePoint. Der File-Download ist in den UAL mit der Suche „Operations: ‚FileDownloaded‘“ erkennbar. Mit der Darstellung der Dateiexporte auf einer zeitlichen Achse können Unregelmäßigkeiten und Peaks schnell visuell identifiziert werden.

Zugriff trotz Passwortwechsel

Wenn ein Angreifer Zugangsdaten eines Benutzers erlangen konnte, läuft er immer Gefahr, dass der Benutzer das Passwort zurücksetzt und der Angreifer damit seinen Zugang verliert. Ein Ziel des Angreifers ist es daher, sich einen persistenten Zugang einzurichten, der es ihm ermöglicht, unabhängig vom Benutzer auf die Cloud-Umgebung zuzugreifen. Eine Form von Persistenz können die schon erwähnten Weiterleitungsregeln und Delegierungen in Exchange Online sein.

Wenn die Zwei-Faktor-Authentisierung (2FA) aktiviert ist, kann sie umgangen werden, indem der Angreifer ein eigenes 2FA-Gerät hinzufügt. Das setzt voraus, dass er Zugriff zu einem kompromittierten Benutzer hat. Änderungen an den Einstellungen zu 2FA werden mit dem Nutzer „fim_password_service@support.onmicrosoft.com“ ausgeführt, entsprechend schnell lassen sich damit neu hinzugefügte Geräte identifizieren. Das Bei-

Mit dem Hinzufügen eines eigenen Geräts kann ein Angreifer versuchen, die Zwei-Faktor-Authentisierung zu umgehen. Das bleibt aber nicht unbemerkt, wenn man gezielt danach sucht (Abb. 4).

spiel in Abbildung 4 zeigt, wie ein Gerät mit dem Namen „InvisibleHuman“ zur Authentisierung erstellt wurde.

Rettung in der Not

Falls während eines Threat Hunting Hinweise auf eine Kompromittierung gefunden wurden, sollte man umgehend eine Reihe von Sofortmaßnahmen umsetzen:

- Das Passwort des kompromittierten Benutzers zurücksetzen und dessen aktive Sessions beenden. Damit kann sichergestellt werden, dass der direkte Zugang zum Benutzerkonto gesperrt ist. Leider zeigt die Erfahrung, dass es eine Weile dauern kann, bis aktive Sessions unterbrochen werden. Daher empfiehlt es sich, den Benutzer nach dem Passwortwechsel für ungefähr eine Stunde komplett zu deaktivieren, sodass in dieser Übergangszeit keine schädlichen Aktionen durchgeführt werden können.
- Falls noch keine Multi-Faktor-Authentisierung eingerichtet wurde, sollte dies umgehend nachgeholt werden. Andernfalls sollten aktive MFA-Geräte darauf überprüft werden, ob eine Manipulation stattfand.
- In einem weiteren Schritt ist zu prüfen, welche Aktivitäten dem kompromittierten Benutzer zugeordnet werden können. Eingerichtete Regeln sollten gelöscht und Benutzermanipulationen rückgängig gemacht werden.
- In den nächsten Tagen sollte der zuvor kompromittierte Benutzer regelmäßig überwacht werden, um sicherzustellen, dass auch wirklich alle Spuren des Angriffs beseitigt wurden.
- Falls ein Angriff einer einzelnen IP oder einer Region zugeordnet werden kann, die im alltäglichen Betrieb nicht verwendet wird, kann man eine Blockierung in Betracht ziehen.

Handelt es sich bei dem kompromittierten Benutzer um einen Administrator, sind die Auswirkungen des Angriffs größer, da Angreifer mit administrativen Rechten mehr Aktionen ausführen können – zum Beispiel neue Benutzer erstellen oder Berechtigungen ändern. Administratorkonten sind deshalb besonders zu schützen [1].

Die Kompromittierung von Benutzerkonten im AAD birgt auch immer die Gefahr, dass reguläre Benutzer aus dem eigenen AAD Tenant ausgesperrt werden. Für solche Fälle kann ein sogenannter Break Glass Account erstellt werden. Hierbei handelt es sich um einen Benutzer mit administrativen Rechten und einem sicheren Passwort, der aber im Normalbetrieb nicht genutzt wird. Das Passwort sollte sicher, aber im Notfall zugänglich aufbewahrt werden.

Fazit

Mit der Verlagerung von Microsoft-Diensten in die Cloud nehmen Angriffe darauf stetig zu. Mit kompromittierten Benutzern im AAD verschaffen sich Angreifer Zugriff zu allen verfügbaren M365-Produkten. In den Sign-in-Logs sind fehlgeschlagene sowie erfolgreiche Anmeldeversuche von Angreifern ersichtlich. Microsoft selbst bietet auch Sicherheitsmeldungen, wenn Unregelmäßigkeiten im Nutzerverhalten identifiziert werden.

Angreifer können kompromittierte Benutzer einsetzen, um ihre Rechte in der Cloud-Umgebung des Unternehmens auszuweiten, Daten abzuziehen oder das legitime Postfach für weitere Angriffe wie Phishingkampagnen zu nutzen. Das kann neben anderen Konsequenzen schnell eine Rufschädigung nach sich ziehen, wenn aus Unternehmenspostfächern schädliche Aktionen ausgeführt werden. Mithilfe von Threat Hunting lassen sich Anzeichen eines kompromittierten Benutzers frühzeitig erkennen, um weiteren Schaden zu verhindern. (ur@ix.de)

Quellen

[1] Frank Ully; Das Netz verstärkt; Azure Active Directory und Azure-Dienste absichern; iX 4/2022, S. 60

[2] Frank Ully; Ins Netz gegangen; Angriffe auf das Azure Active Directory und auf Azure-Dienste; iX 4/2022, S. 50

[3] Fabian Murer; Forensik und Logging im Azure AD; iX 6/2022, S. 112

[4] Jens Lüttgens, Dominik Oepen; E-Mail-Betrug in MS-365-Umgebungen; iX 12/2022, S.102

[5] Die im Text genannten Tools, Artikel und Dokumentationen sind über ix.de/z99w zu finden.

TABEA NORDIEKER

ist als Digital-Forensics- und Incident-Response-Spezialistin bei der Oneconsult AG in Zürich angestellt, wo sie Kunden bei der Behebung von Cybersicherheitsereignissen unterstützt.