Forensik und Logging im Azure AD

Ransomware-Angriffe verdanken ihren Erfolg in der Regel einem kompromittierten Active Directory – so weit, so bekannt. Vergessen wird allerdings häufig der Anteil, den das Azure Active Directory daran hat. Um Datenspuren hier zu analysieren und Vorfälle auszuwerten, bedarf es spezieller Kenntnisse.

Von Fabian Murer

Die meisten der heutigen großen Cyberangriffe, beispielsweise durch einen Verschlüsselungstrojaner (engl. Ransomware), erfolgen durch eine Kompromittierung des Active Directory (AD). Was dabei jedoch häufig nicht bedacht wird, etwa bei präventiven Sicherheitsmaßnahmen oder auch der Analyse solcher Angriffe, ist die Tatsache, dass immer mehr Unternehmen ihr Active Directory zusätzlich zu der On-Premises-Instanz auch in die Cloud mit dem Azure Active Directory (AAD) synchronisieren. Oder vielleicht sogar ausschließlich das AAD verwenden.

Untersuchungen solcher Vorfälle zeigen, dass die Synchronisation häufig in Vergessenheit gerät. Ein Angreifer, der administrative Berechtigungen in der höchsten Ebene des AD erlangen konnte, kann sich jedoch ebenfalls im AAD einnisten, wenn AD und AAD miteinander verknüpft sind. Eine fehlende Analyse des AAD kann zur Folge haben, dass eine Hintertür über die Cloud unentdeckt und trotz beendeter Vorfallsbehandlung (Incident Handling, auch Incident Response) bestehen bleibt.

In diesem Artikel werden einige grundlegende Methoden vorgestellt, die es einem erlauben, bei einem Cybervorfall auch das Azure Active Directory auf etwaige verdächtige Aktivitäten zu überprüfen. Dabei wird sowohl das AAD als auch das stark damit verknüpfte und beliebte Microsoft 365 berücksichtigt.

Die richtigen Berechtigungen

Um eine mögliche Kompromittierung eines Azure AD beziehungsweise Azure Tenants zu untersuchen, benötigt ein Analyst oder Incident Responder entsprechende Berechtigungen, da Ressourcen wie Audit- oder Sign-in-Logs in der Regel für Standardbenutzer nicht sichtbar sind. Man will jedoch einem Analysten, insbesondere wenn es sich um einen externen Spezialisten handelt, nicht einfach die Rolle des „Global Administrator“ und somit die volle Kontrolle über den Azure Tenant geben. Für die IT-forensische Untersuchung eines Sicherheitsvorfalls in einem Azure Tenant eignen sich zwei Rollen besonders.

Die erste ist die des Security Reader (siehe ix.de/zhbc). Benutzer mit dieser Rolle haben globalen Lesezugriff auf alle sicherheitsrelevanten Funktionen im Azure Tenant. Diese umfassen unter anderem Informationen aus dem Microsoft 365 Security Center, dem Azure Active Directory (AAD), der Identity Protection, dem Privileged Identity Management und dem Microsoft 365 Security & Compliance Center. Diese Rolle ist bereits für viele Aktivitäten eines Analysten ausreichend.

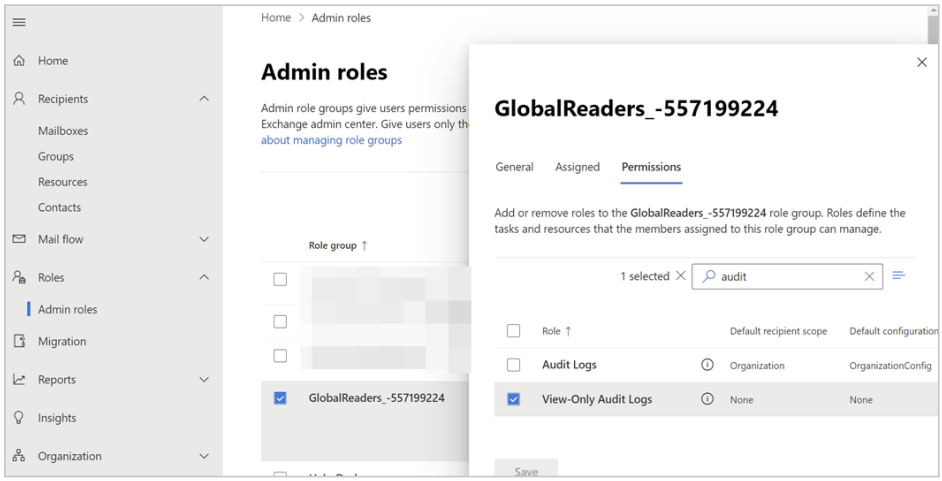
In den meisten IT-forensischen Analysen sind jedoch auch Informationen rund um die Infrastruktur und ihre Einstellungen relevant. Viele dieser Einstellungen lassen sich mit der Rolle des Security Reader jedoch nicht anschauen. Hierzu eignet sich die zweite Rolle des Global Reader (siehe ix.de/zhbc), die alle

iX-TRACT

- Wie die Angriffe selbst verschieben sich auch deren IT-forensische Untersuchungen immer häufiger in die Cloud. Da das On-Premises Active Directory oftmals mit dem Azure Active Directory verknüpft ist, sollte man letzteres in die Analyse von Cyberangriffen grundsätzlich einbeziehen.
- Die Sicherheitsdienste im Azure Tenant führen von Hause aus im Hintergrund bereits erste Analysen und Auswertungen durch. Ihren Warnhinweisen etwa zu Anmeldungen aus fremden Ländern ist zwingend nachzugehen. Auch sollten weitere Aspekte manuell überprüft werden.
- Mithilfe der Unified Audit Logs aus Microsoft 365 lassen sich Angriffe wie Business-E-Mail-Compromises schnell identifizieren.

Einstellungen und Informationen eines Azure Tenants lesen darf. Diese Rolle ist das Pendant zum Global Administrator, jedoch nur mit Lese- und ohne Schreibzugriff. So können keine administrativen Aktionen ausgeführt und Einstellungen verändert werden. Diese Rolle ist daher besonders für die Planung, für Audits oder für Untersuchungen im Rahmen eines Sicherheitsvorfalles geeignet.

Für die Durchsuchung der Unified Audit Logs (UAL) von Microsoft 365 reicht je nach Einstellung die Security-Reader- oder auch die Global-Reader-Rolle nicht aus. Grund dafür ist, dass die benötigten Berechtigungen innerhalb von Microsoft 365 durch Exchange Online definiert werden, da die für die Durchsuchung dieser Logs verwendeten Befehle aus dem Exchange-Online-Umfeld stammen.



Die Leseberechtigung für die UAL muss je nach Rolle händisch erteilt werden (Abb. 1).

Nur schauen, nicht anfassen

Im Exchange Admin Center (siehe ix.de/zhbc) kann man die Berechtigungen des Security und des Global Reader überprüfen. Es sollte die Rolle View-Only Audit Logs zugewiesen sein (siehe Abbildung 1). Diese Rolle ist standardmäßig nur den Gruppen „Compliance Management“ und „Organisation Management“ zugewiesen und muss deshalb in der Regel manuell ergänzt werden.

Eine Studie der Anti-Phishing Working Group (APWG) hat gezeigt, dass Dienste wie Webmail oder allgemein Software as a Service (SaaS) mit rund 30 Prozent Anteil das mit Abstand größte Ziel für Phishingangriffe sind (siehe ix.de/zhbc). Microsoft ist in diesem Bereich mit Azure sowie mit Microsoft 365 sehr stark vertreten und wird von vielen Unternehmen verwendet. Hinzu kommt, dass durch die große Interkonnektivität zwischen den Microsoft-Diensten mit einem kompromittierten Benutzerkonto gleich der Zugang zu verschiedensten Diensten kompromittiert ist.

Wird also ein Mitarbeiter eines Unternehmens Opfer eines Phishingangriffes, dessen Ziel es ist, an die Zugangsdaten des AD-Kontos zu gelangen, wird der Angreifer mit großer Wahrscheinlichkeit versuchen, diese Zugangsdaten auch an den häufig verwendeten Cloud-Diensten von Microsoft auszuprobieren. Glücklicherweise werden im AAD Tenant alle Anmeldungen protokolliert, ob sie erfolgreich sind oder nicht. Sie werden mindestens sieben Tage gespeichert, je nach Lizenzmodell bis zu 30 Tage. Diese protokollierten Anmeldungen lassen sich im Azure-Portal (siehe ix.de/zhbc) unter dem Dienst „Azure Active Directory“ unter „Sign-in logs“ leicht durchsuchen und filtern.

Die (Risky) Sign-in Logs

Vermutet man einen Phishingangriff, lässt sich anhand der Logs schnell ermitteln, welcher Benutzer sich wann an welcher Applikation von wo angemeldet hat. Filtert man nun beispielsweise nach dem verdächtigen Benutzerkonto und schaut sich an, von wo sich der Benutzer in den letzten Tagen rund um den Zeitpunkt des vermuteten Phishingangriffs angemeldet hat, ist oft ziemlich schnell ersichtlich, ob und welche Anmeldungen potenziell bösartiger Natur sind. So sticht beispielsweise eine Anmeldung aus Singapur deutlich aus den sonstigen Anmeldungen aus Zürich heraus (siehe Abbildung 2), besonders wenn mehrere Versuche nur wenige Minuten nacheinander erfolgen. Spätestens die Nachfrage beim Benutzer, wo er sich gerade aufhält, kann letzte Zweifel beseitigen.

In einem großen, weltweit tätigen Unternehmen mit mehreren Tausend Mitarbeitenden ist die Frage, ob eine Anmeldung aus Singapur oder China legitim ist oder nicht, schwer zu beantworten. Es sei denn, man hat schon einen Verdacht.

Glücklicherweise verwendet Microsoft unter Azure jedoch diverse automatisierte Überwachungssysteme, die im Hintergrund solche Aktivitäten überwachen und analysieren. Diese Sicherheitstools erkennen verdächtige Anmeldungen oft bereits automatisch und fassen sie in einer separaten Übersicht, den „Risky Sign-ins“, zusammen. Diese riskanten Anmeldungen sind im Azure-Portal unter dem Dienst Sicherheit zu finden.

Im Beispiel von oben hat Azure eine weitere verdächtige Aktivität identifiziert und angezeigt. Dabei werden diese Anmeldungen in verschiedene Kategorien eingeteilt. So wird die Anmeldung aus Singapur als „Atypical Travel“, also atypische Reise, eingestuft. Darunter versteht Azure zwei Anmeldungen des gleichen Benutzers aus verschiedenen Ländern, wovon sich mindestens einer der Orte von den typischen Anmeldeor-

2/12/2022, 3:17:33 PM		Microsoft Teams Web Client	Success	Singapore, Central Singapore, SG	Success
2/12/2022, 3:17:31 PM		Microsoft Teams Web Client	Interrupted	Singapore, Central Singapore, SG	Success
2/12/2022, 3:17:02 PM		Microsoft Teams Web Client	Interrupted	Singapore, Central Singapore, SG	Failure
2/12/2022, 3:06:06 PM		Azure Portal	Success	Zuerich, Zuerich, CH	Success
2/12/2022, 3:06:03 PM		Azure Portal	Interrupted	Zuerich, Zuerich, CH	Success
2/12/2022, 3:05:52 PM		Azure Portal	Interrupted	Zuerich, Zuerich, CH	Failure
2/11/2022, 4:48:42 PM		Microsoft Stream Portal	Success	Zuerich, Zuerich, CH	Success
2/11/2022, 3:43:50 PM		Microsoft Stream Portal	Success	Zuerich, Zuerich, CH	Success

Die Logs offenbaren eine verdächtige Anmeldung aus Singapur (Abb. 2).

Weitere verdächtige Anmeldungen konnten über das Betriebssystem und den User Agent identifiziert werden (Abb. 3).

ten des entsprechenden Benutzers unterscheidet.

Ein Filter für alle Fälle

Hat man nun verdächtige Anmeldungen eines Benutzerkontos identifiziert, möchte man auch herausfinden, was während dieser Anmeldungen passiert ist und was der mögliche Angreifer mit den Zugangsdaten angestellt hat. Dazu kann man sich noch einmal die Anmeldeprotokolle anschauen und beispielsweise nur nach der verdächtigen Quelle filtern, indem man über „Add filters“ einen Filter für die identifizierte IP-Adresse oder den entsprechenden Standort einstellt.

Das Ganze kann nun einerseits auf die Anmeldeprotokolle des betroffenen Benutzers angewendet werden, um beispielsweise herauszufinden, welche Applikationen der Angreifer verwendet hat. Alternativ kann der Filter über alle Anmeldeprotokolle gelegt werden. So kann man etwa erkennen, ob sich neben dem bereits bekannten kompromittierten Benutzer noch weitere Benutzer von dieser Quelle angemeldet haben. Das würde darauf hindeuten, dass diese Benutzerkonten ebenfalls kompromittiert sind und entsprechend behandelt werden müssen.

Ein weiterer nützlicher Indikator können auch der eingesetzte Browser oder das verwendete Betriebssystem sein. Damit diese Spalten angezeigt werden, müssen über „Columns“ die beiden Spalten „Operating System“ und „Device Browser“ angewählt werden. Diese beiden Artefakte können deswegen aussagekräftig sein, weil sich das Betriebssystem sowie der verwendete Browser eines legitimen Benutzers in der Regel nicht stark ändern. Korreliert man das zusätzlich mit der üblicherweise verwendeten IP-Adresse respektive dem Anmeldeort, so stechen Ausreißer besonders heraus und können nachverfolgt werden.

Im obigen Beispiel wurde bei der Anmeldung aus Singapur der Firefox-Browser auf einem Linux-System verwendet, dagegen stammen die legitimen Anmeldungen aus Zürich von einem Edge-Browser unter Windows. Filtert man nun die Protokolle dieses Benutzeraccounts nach dem Firefox-Browser, tauchen weitere auffällige Anmeldungen aus Kolumbien auf (Abbildung 3). Auf diese Weise lassen sich durch geschicktes Kombinieren von Filtern und bekannten Informationen über das Verhalten der Benutzer verdächtige Aktivitäten identifizieren.

Die Azure Active Directory Audit Logs

Im fiktiven Beispiel haben die ersten Untersuchungen gezeigt, dass sich die Angreifer über die erbeuteten Zugangsdaten an verschiedenen Microsoft-Azure-Diensten angemeldet haben, unter anderem auch am Azure-Portal selbst. Je nach den Berechtigungen dieses Benutzers kann der Angreifer mit direktem Zugang zum Portal verschiedene weitere Angriffe starten.

Bei Cybervorfällen, in denen das ganze (A)AD kompromittiert wird, die Angreifer also die Kontrolle über einen Domänenadministrator besitzen, wird oft beobachtet, dass sie sich einfach ein neues Konto mit administrativen Rechten erstellen, um sich auf diese Weise einen zusätzlichen Zugriff (Persistenz) zum Unternehmen zu verschaffen. In der Cloud sind ebenfalls oft zusätzlich erstellte virtuelle Maschinen zu sehen, mit denen Kriminelle Kryptowährungen schürfen.

Um solche Manipulationen am Azure Tenant zu identifizieren, lohnt sich ein Blick in die Audit Logs des Azure Active Directory. Sie protokollieren alle Änderungen, die im Azure Tenant vorgenommen werden – zum Beispiel an Benutzerkonten, an Gruppenrechten oder Anpassungen an Applikationen im Azure Tenant. Mit den Audit Logs lassen sich folgende Fragen beantworten:

- Welche Benutzer wurden vor Kurzem erstellt?
- Welche Benutzer haben vor Kurzem ihr Passwort geändert?
- Wurde ein Benutzer einer neuen Gruppe hinzugefügt?

Analog zu den zuvor gesehenen Anmeldeprotokollen des AAD lassen sich die Audit Logs im Azure Portal unter dem Dienst Azure Active Directory finden und durchsuchen. Die Aktivitäten eines Benutzers sind in der Spalte „Activity“ aufgelistet. Mit einem entsprechenden Filter kann man so die Auditprotokolle nach speziellen Aktionen durchsuchen. Im folgenden Beispiel (Abbildung 4) lässt sich etwa anhand der Aktivität „Add user“ und „Invite external user“ feststellen, dass ein externes Gastkonto für die E-Mail-Adresse „gormaxdon@gmail.com“ angelegt wurde. Die darauffolgende Aktion „Add member to role“ deutet darauf hin, dass ein Benutzer einer neuen Rolle zugewiesen wurde. Wählt man den entsprechenden Eintrag aus, erhält man zusätzliche Informationen, die zeigen, dass der

Eine Analyse der Audit Logs enthüllt, in welchen Schritten sich ein Angreifer einen Benutzeraccount mit allen Rechten angelegt hat (Abb. 4).

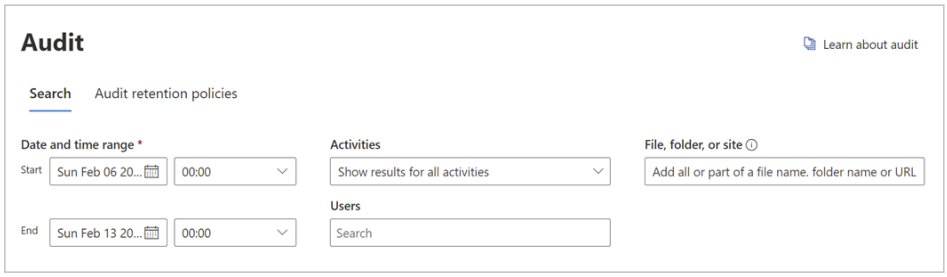
eben erstellte Gastbenutzer der Gruppe „Global Administrators“ hinzugefügt wurde. Gleich danach wurde die Einladung angenommen („Redeem external user invite“) und der Angreifer hat sich erfolgreich einen zweiten Zugang zum Azure Tenant verschafft.

Microsoft 365 Unified Audit Logs (UAL)

Microsoft 365 (vormals Office 365) ist bei vielen kleinen und großen Unternehmen nicht mehr wegzudenken. Zahlreiche beliebte Applikationen wie Microsoft Teams oder Exchange Online sind ein Teil davon. Was wenige wissen: Das Benutzermanagement dieser Anwendungen ist verknüpft mit dem Azure Active Directory. Spricht man von IT-forensischen Untersuchungen im AAD, spielt Microsoft 365 dabei ebenfalls eine zentrale und wichtige Rolle. Die folgenden Abschnitte zeigen, wie sich mithilfe der von Microsoft 365 generierten Protokolle verschiedene Angriffe auf die Dienste entdecken lassen.

Wie viele andere Applikationen und Systeme von Microsoft protokolliert auch Microsoft 365 alles rund um das Produkt sehr ausführlich. In der Welt von Microsoft 365 spricht man von den „Unified Audit Logs“ (UAL). Sie protokollieren verschiedenste Aktivitäten von Benutzern und Administratoren in allen Microsoft-365-Diensten und -Produkten. Microsoft 365 unterscheidet noch zwischen den „Basic Audit Logs“ und den „Advanced Audit Logs“. Erstere sind für alle mit entsprechender Lizenz standardmäßig aktiviert (Details zu den Lizenzen siehe ix.de/zhbc). Die Protokolle werden für 90 Tage gespeichert und können sowohl über das Webinterface als auch über PowerShell-Befehle und die API durchsucht werden.

Die Advanced Audit Logs können länger gespeichert werden und erlauben es, zusätzliche Richtlinien zu definieren. Sie sind ab der E5-Lizenz enthalten. Generell



Die Unified Audit Logs lassen sich über das Microsoft 365 Compliance Center komfortabel nach Auffälligkeiten durchsuchen (Abb. 5).

lassen sich die UAL, wie die anderen Protokolle im Azure Tenant, auch an zentrale Log-Sammelstellen weiterleiten. Um festzustellen, ob sie im eigenen Tenant aktiviert sind, kann folgender Befehl in einer Exchange Online PowerShell ausgeführt werden:

```
Get-AdminAuditLogConfig | FL ↵
      UnifiedAuditLogIngestionEnabled
```

Durchsuchen der Unified Audit Logs

Die UAL lassen sich auf verschiedene Arten durchsuchen. Um sie lesen zu können, sind Berechtigungen wie die des genannten Global Reader erforderlich. Die einfachste Methode, die UAL auszuwerten, ist im Microsoft 365 Compliance Center in der Spalte Audit zu finden (siehe Abbildung 5). Dort kann man nach Zeit, Benutzer oder Aktivitäten filtern und so gezielt nach Aktivitäten wie dem Einrichten einer neuen Mailbox („Created Mailbox Item“) oder einer erfolgreichen Anmeldung („User Logged In“) suchen (mehr Beispiele siehe ix.de/zhbc). Es kann allerdings je nach Ereignis zwischen 30 Minuten und 24 Stunden dauern, bis der entsprechende Audit-Protokoll-Eintrag in den Ergebnissen einer Suche angezeigt wird.

Alternativ lassen sich die UAL auch über den PowerShell-Befehl `Search-UnifiedAuditLog` durchsuchen (Beispiele siehe ix.de/zhbc). Er muss dabei ebenfalls in einer Exchange Online PowerShell ausgeführt werden. Mit dem folgenden Befehl lassen sich beispielsweise alle erfolgreichen Anmeldungen anzeigen:

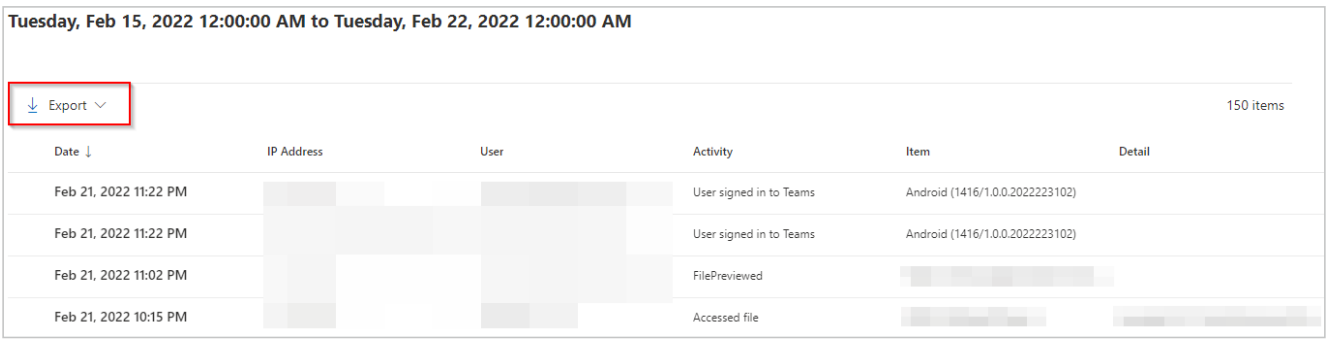
```
Search-UnifiedAuditLog ↵
                -StartDate 2022-01-01 ↵
    -EndDate 2022-01-31 -Operations ↵
                          UserLoggedIn
```

UAL: Erst exportieren, dann analysieren

Für eine effiziente Analyse der Unified Audit Logs eignen sich weder die Weboberfläche noch die PowerShell-Befehle. Um die UAL mit weiteren Tools zu untersuchen, kann man sie mit einfachen Mitteln exportieren. Variante 1 funktioniert über die Weboberfläche im Microsoft 365 Compliance Center. Hat man zunächst eine Suche durchgeführt, lassen sich die angezeigten Resultate über die Funktion „Export/Download all results“ im CSV-Format herunterladen (Abbildung 6).

Über diese Methode lassen sich allerdings nur 50 000 Einträge auf einmal herunterladen. Für mehr muss die Zeitspanne angepasst werden und die Resultate müssen auf mehrere Dateien verteilt werden. Es empfiehlt sich daher, den Export kurz zu überprüfen, bevor man mit der Analyse beginnt.

Eine Alternative bietet das PowerShell-Skript Office365_Extractor.ps1 des Incident-Response-Teams der Wirtschaftsprüfer- und Beratungsgesellschaft PwC (Abbildung 7). Mit seiner Hilfe las-



Über die Weboberfläche lassen sich die UAL zur detaillierteren Analyse herunterladen (Abb. 6).

Der Office 365 Extractor erlaubt das Exportieren vieler Datensätze über einen langen Zeitraum hinweg (Abb. 7).

sen sich die UAL über einen längeren Zeitraum hinweg und mit mehr als 50 000 Einträgen herunterladen. Um das Skript auszuführen, braucht man

- einen Microsoft-365-Account mit Berechtigungen, die UAL zu lesen (zum Beispiel Global Reader);
- das PowerShellGet-Modul;
- das Exchange-Online-Modul.

Zum Installieren der beiden Module sind in einer administrativen PowerShell die folgenden Befehle auszuführen:

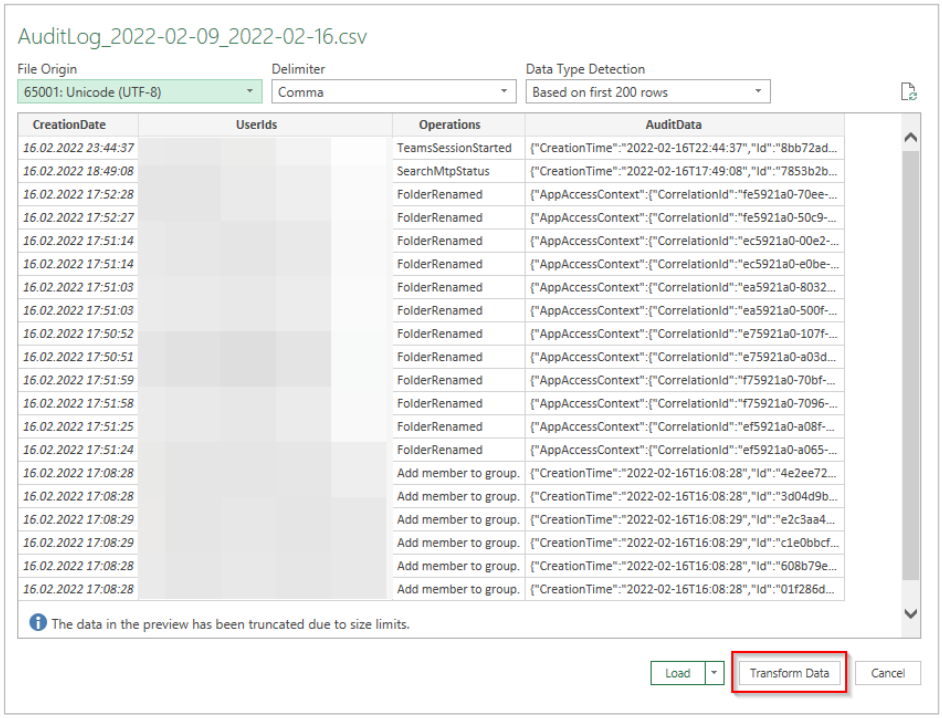
```
Install-Module PowerShellGet
Install-Module -Name ↵
                ExchangeOnlineManagement
```

Danach kann das Skript ausgeführt werden. Es bietet viele zusätzliche Auswahlmöglichkeiten, zum Beispiel das Exportieren der UAL eines bestimmten Benutzers. Sein einziges Manko ist, dass es (Stand Redaktionsschluss) keine Multi-Faktor-Authentisierung unterstützt.

Hat man die UAL einmal exportiert, lassen sie sich mit verschiedenen Werkzeugen weiter analysieren. Als einfachste Möglichkeit kann man die exportierten UAL in eine Excel-Datei importieren und dort mit den eigenen Filterfunktionen sortieren. Das Einlesen in Excel kann im CSV-Format erfolgen. Die Daten sind jedoch vorher noch entsprechend zu transformieren, da standardmäßig nur vier Spalten angezeigt werden (Abbildung 8).

Der eigentliche Log-Inhalt wird in der Spalte AuditData im JSON-Format gespeichert. Im Menü kann sie jedoch über Transform/JSON so umgewandelt werden, dass aus den JSON-Feldern Spalten entstehen, die sich filtern lassen.

Eine interessante Möglichkeit ist das Überführen der exportierten Logs in ein SIEM-System (Security Information and Event Management), in dem man sie dann mit gezielten Abfragen durchsuchen kann (siehe [1]).



Nach erfolgter Transformation lassen sich die UAL in Excel überführen und dort weiter nach Auffälligkeiten durchsuchen (Abb. 8).

Der Kompromittierung auf der Spur

Nachdem sich ein Angreifer Zugriff zu einem Azure-Konto verschaffen konnte, beispielsweise durch einen erfolgreichen Phishingangriff, hinterlässt er oft eine

operation	user_name	operation_properties.Actions	parameters.ForwardingSmtpAddress
UpdateInboxRules	[redacted]	ForwardToRecipientsAction, StopProcessingAction	-
UpdateInboxRules	[redacted]	ForwardToRecipientsAction, StopProcessingAction	-
Set-Mailbox	[redacted]	-	smtp:[redacted]

Die Suche nach dem Schlüsselbegriff „Forward“ enttarnt das Umleiten von E-Mails an einen Angreifer (Abb. 9).

Weiterleitungsregel im E-Mail-Postfach des Opfers. Diese Regel konfiguriert er so, dass E-Mails mit vertraulichen Inhalten automatisch an eine von ihm kontrollierte Adresse weitergeleitet werden. Auf diese Weise kann der Angreifer das Opfer ausspionieren. Im sogenannten Business Email Compromise (BEC), einer speziellen Betrugsmasche, fängt der Angreifer beispielsweise Rechnungen ab und manipuliert sie zu seinen Gunsten.

Mithilfe der UAL lässt sich das Hinterlegen einer neuen Weiterleitungsregel mit wenig Aufwand ausfindig machen. Aktivitäten werden in der UAL in der Spalte Operation gespeichert. Für die Suche nach Weiterleitungsregeln in einer Mailbox sind folgende Aktionen besonders interessant:

- New-InboxRule: Eine neue Inbox-Regel wurde über die Outlook-Web-Applikation erstellt.
- Set-InboxRule: Eine bestehende Inbox-Regel wurde über die Outlook-Webapplikation verändert.
- UpdateInboxRules: Eine Inbox-Regel wurde über den Outlook-Client erstellt, modifiziert oder gelöscht.

Dieser Befehl durchsucht die UAL nach Änderungen an Inbox-Regeln im Januar 2022:

```
Search-UnifiedAuditLog ↵
              -StartDate 2022-01-01 ↵
    -EndDate 2022-01-31 -Operations ↵
        New-InboxRule,Set-InboxRule,↵
                    UpdateInboxRules
```

Um Weiterleitungsregeln aufzuspüren, müssen diese Resultate noch nach dem Schlüsselwort „Forward“ durchsucht werden (Abbildung 9). Eine weitere Option, alle Weiterleitungsregeln in den Mailboxen der Benutzer zu finden, bietet der Get-Mailbox- Befehl:

```
Get-Mailbox -ResultSize ↵
      Unlimited -Filter "Forwarding↵
     Address-like '*' -or Forwarding↵
     SmtpAddress -like '*'"  Select-↵
      Object Name,ForwardingAddress,↵
                ForwardingSmtpAddress
```

Fazit

Viele Unternehmen verlegen heutzutage ihre Benutzerverwaltung in das Azure Active Directory und verwenden die Dienste von Microsoft 365. Da diese Plattformen in der Regel von überallher erreichbar und nicht von der Unternehmens-Firewall geschützt sind, geben sie ein gutes Ziel für Angreifer ab. Als Folge rückt auch Incident Response in der Cloud immer mehr in den Vordergrund. Aufgrund der standardmäßig umfangreichen Protokollierung in Microsoft-Diensten und -Produkten lassen sich bereits mit einfachen Mitteln erste verdächtige Aktivitäten im Azure Active Directory ausmachen.

Unternehmen, die das Azure Active Directory sowie Microsoft 365 verwenden, sollten sicherstellen, dass die Protokollierung aktiviert ist, sodass im Falle eines Verdachts die für eine Analyse relevanten Informationen zur Verfügung stehen. Darüber hinaus sollten die durch Microsoft automatisiert identifizierten riskanten Benutzer und Anmeldungen regelmäßig überprüft und nachverfolgt werden. (ur@ix.de)

Quellen

[1] Fabian Murer, Gregor Wegberg; Aufgespürt – Angriffsspuren in Windows-Netzen analysieren; iX 1/2022, S. 124

[2] Die im Artikel erwähnten Werkzeuge, Artikel und Dokumente sind über ix.de/ zhbc zu finden.

Fabian Murer

ist Senior Digital-Forensics- und Incident-Response-Spezialist bei der One-consult AG. Er unterstützt Firmen bei der Bewältigung von Cyberattacken und untersucht als IT-Forensiker die Methoden der Angreifer bis auf den letzten Befehl.

iX-Sonderheft „Sicheres Active Directory“

Dieser Artikel ist dem neuen iX-Sonderheft „Sicheres Active Directory“ entnommen. Es beschäftigt sich auf 172 Seiten mit Microsofts Active Directory (AD), dem meistgenutzten Verzeichnisdienst in Unternehmen. Für Kriminelle ist das AD eine Fundgrube an wertvollen Informationen, die dabei helfen, ins Unternehmensnetz vorzudringen, sich dort auszubreiten, Daten zu stehlen oder zu manipulieren und gefährliche Malware wie die verbreiteten Verschlüsselungstrojaner einzuschleusen.

Um das Unternehmensnetz zu schützen, muss man wissen, wie das AD überhaupt funktioniert, was es so angreifbar macht und wie man es auf verschiedenen Ebenen absichert. Versteht man die grundlegenden Konzepte, die Struktur des AD und die eingesetzten Protokolle, kann man nachvollziehen, wie Fehlkonfigurationen, mangelnde Härtung oder zu großzügige Rechtevergabe Angriffe wie Golden Ticket, DCSync, PetitPotam, Pass the Hash und viele mehr ermöglichen. Mit den richtigen Stellschrauben lassen sich solche Angriffe verhindern oder zumindest erschweren. Das iX kompakt behandelt überdies weitere Aspekte zum Absichern eines AD, etwa die richtige Passwortstrategie, die Basisabsicherung nach IT-Grundschutz, neue Sicherheitsansätze wie Zero Trust, forensische Nachvollziehbarkeit von Angriffen und die Unterstützung durch Produkte bei der Prävention und nach etwaigen Angriffen. Eine eigene Rubrik widmet sich dem immer häufiger genutzten Azure AD (AAD), Microsofts cloudbasiertem Identitäts- und Zugriffsverwaltungsdienst. Er wird oft auch in Kombination mit dem lokalen AD im Hybridbetrieb eingesetzt. Das schafft zu den schon bekannten Einfallstoren neue Angriffsmöglichkeiten. Auch hier gilt: Das AAD absichern kann nur, wer es gut kennt.

Das PDF des Sonderhefts zum sofortigen Download kostet 17,99 Euro, die gedruckte Ausgabe für 19,50 Euro lässt sich im heise Shop bestellen (siehe ix.de/zhbc) und ist im gut sortierten Zeitschriftenhandel zu haben. Das Bundle Heft + PDF kostet 25,50 Euro.