Spuren kompromittierter E-Mail-Konten analysieren

Spuren kompromittierter E-Mail-Konten analysieren

Nachdem der erste Teil des Playbooks zu gekaperten E-Mail-Accounts zeigte, wie man die Logs mithilfe von Microsofts zentraler Logfunktion einsammelt, erklärt der zweite Teil, wie man sie auf verdächtige Vorgänge auswertet und welche Rückschlüsse sich daraus ziehen lassen.
Nachdem der erste Teil des Playbooks zu gekaperten E-Mail-Accounts zeigte, wie man die Logs mithilfe von Microsofts zentraler Logfunktion einsammelt, erklärt der zweite Teil, wie man sie auf verdächtige Vorgänge auswertet und welche Rückschlüsse sich daraus ziehen lassen.

- Beim ersten Anzeichen verdächtiger Aktivität rund um E-Mail-Accounts sollte man IT-forensische Untersuchungen anstoßen, um zu verstehen, was genau passiert ist.

Ausgangspunkt der Analyse sind die gesammelten Logdaten und Artefakte.

- Aussagekräftig im Hinblick auf Eindringlinge ins Firmennetz sind unter anderem fehlgeschlagene Anmeldevorgänge, eingerichtete Mailweiterleitungen oder neu vergebene Berechtigungen. Solche Hinweise sollten sorgfältig untersucht werden.
- Die Ursachenforschung und eine Nachbereitung sind das A und O nach der Bewältigung von Sicherheitsvorfällen. Daraus abgeleitete technische Maßnahmen sowie die Sensibilisierung von Mitarbeitenden sollen künftige Angriffe zumindest erschweren.

Die umfassendste Datenquelle zur Analyse von Unregelmäßigkeiten oder Verdachtsmomenten für einen Sicherheitsvorfall bietet Microsofts zentrale Logfunktion Unified Audit Log (UAL). Hier werden Benutzer- und Administratoraktivitäten auch unabhängig vom Einsatz zusätzlicher Produkte wie Microsoft Sentinel oder Microsoft Defender for Identity aufgezeichnet (wie die Logdaten im Detail gesichert werden, beschreibt [1]). Die nachfolgenden Schritte zeigen, wie man bei der Analyse vorgeht und die Logdaten sinnvoll durchsuchen kann.

Schritt 4: Untersuchen der Anmeldeaktivitäten

Jedes Mal, wenn sich ein Benutzer bei seinem Konto anmeldet, wird ein Ereignis im UAL erstellt. Dieses Ereignis enthält wichtige Informationen, etwa die Quell-IP-Adresse, die sich unter anderem für eine geografische Suche verwenden lässt. Die Ergebnisse lassen sich mit den erwarteten geografischen Standorten eines Unternehmens und seiner Nutzer vergleichen. Wenn zum Beispiel ein Unternehmen in Deutschland ansässig ist und keine Niederlassung in Asien hat oder das VPN des Unternehmens nicht zu einer IP-Adresse in Asien auflöst, würde

man keine Ereignisse aus Asien erwarten. Daher wären Anmeldungen aus Asien in diesem Fall verdächtig.

Natürlich kann es auch sein, dass ein Mitarbeiter sich im Urlaub in Asien befindet und sein Firmenhandy dabeihat, dennoch erfordern diese Ausreißer Aufmerksamkeit. Verdächtige Anmeldungen kann man durch die Suche nach bestimmten Schlüsselwörtern im UAL entdecken. Neben der IP-Adresse liefern auch die Uhrzeit sowie Informationen zum verwendeten Gerät (UserAgent: Betriebssystem, Browser et cetera) gute Anhaltspunkte. Ob das verwendete Gerät dem Unternehmen bekannt ist und von der IT verwaltet wird oder nicht, lässt sich ebenfalls den Ereignissen entnehmen. Für die Suche nach verdächtigen Anmeldeereignissen kann man folgende Schlüsselwörter verwenden:

Schlüsselwort	**Bedeutung des Logeintrags**
MailboxLogin	Hinweis auf einen erfolgreichen Log-in-Vorgang
UserLoggedIn	Hinweis auf einen erfolgreichen Log-in-Vorgang
UserLoginFailed	Hinweis auf einen fehlgeschlagenen Log-in-Vorgang
IdsLocked	Hinweis auf einen Brute-Force-Angriff. Der Account wurde gesperrt, da zur viele fehlgeschlagene Anmeldeversuche unternommen wurden.
UserKey=“Not Available“	Hinweis auf einen Brute-Force-Angriff. Die Anmeldung ist fehlgeschlagen, da der Benutzeraccount nicht existiert.

Neben Ereignissen rund um das Log-in können auch Fehlermeldungen zur Multi-Faktor-Authentisierung (MFA) Indikatoren für mögliche schädliche Aktivitäten sein. Ein Angreifer könnte das Passwort eines Anwenders ausgespäht haben, um dann an der MFA-Abfrage zu scheitern. UAL-Einträge mit den folgenden Schlüsselwörtern sollten näher untersucht

werden:

Schlüsselwort	Bedeutung des Logeintrags
UserStrongAuthClientAuthNRequired	Der Benutzer wird zur Bestätigung einer MFA-Abfrage aufgefordert.
UserStrongAuthClientAuthNRequiredInterrupt	fehlgeschlagene MFA-Abfrage

Schritt 5: Untersuchen von Weiterleitungsregeln

Nachdem ein Angreifer einen Benutzeraccount kompromittiert hat, erstellt er häufig Weiterleitungsregeln, um eingehende E-Mails an ein externes Postfach zu schicken. Auf diese Weise kann er die Aktivitäten eines Opfers kontinuierlich überwachen, ohne sich aktiv in das Konto einzuloggen. Selbst wenn das Passwort eines kompromittierten Kontos zurückgesetzt wird, kann der Angreifer weiterhin E-Mails mitlesen.

Ebenfalls beliebt ist der Einsatz von Weiterleitungsregeln zum automatisierten Löschen von E-Mails, um Spuren, die auf Unregelmäßigkeiten hinweisen, zu verwischen. Auch können Weiterleitungsregeln dazu dienen, Spuren vor dem Anwender zu verstecken, indem E-Mails automatisch als gelesen markiert und in einen anderen Ordner (zum Beispiel in den Junk- oder den RSS-Ordner) verschoben werden.

Einem Angreifer bieten sich in einer Microsoft-365-Umgebung gleich mehrere Möglichkeiten, E-Mails an ein externes Postfach umzuleiten. Er kann zunächst einmal Inbox-Regeln anlegen, um E-Mails auszuleiten. Verfügt das Konto zudem über administrative Berechtigungen, ist auch eine Ausleitung über die globalen Postfacheinstellungen oder Exchange-Transportregeln möglich.

Aktive Inbox-Regeln lassen sich mit der Exchange-Management-Shell auffinden, falls sie nicht bereits mittels des im ersten Artikel vorgestellten Tools Hawk extrahiert wurden:

```
Get-InboxRule -Mailbox | ? {$_.forwardto -or $_.forwardasattachmentto -or $_.redirectto}
```

Auch aktive Mailbox-Weiterleitungen kann die Exchange-Management-Shell anzeigen:

```
Get-Mailbox <identity> | Format-List ForwardingSMTPAddress,DeliverToMailboxandForward
```

Der Powershell-Befehl Get-TransportRule liefert eine Übersicht über alle bestehenden Weiterleitungsregeln.

Des Weiteren kann man im UAL potenzielle Angreiferaktivitäten im Zusammenhang mit Weiterleitungsregeln analysieren. Hier lassen sich auch Regeln nachvollziehen, die der Angreifer schon wieder gelöscht hat. Folgende Schlüsselwörter führen zu den relevanten Logeinträgen:

Schlüsselwort	**Bedeutung des Logeintrags**
New-InboxRule	Anlegen einer neuen Weiterleitungsregel (Inbox-Ebene)
New-TransportRule	Anlegen einer neuen Transportregel (Mail Flow Rule)
Set-Mailbox	Änderungen an den Einstellungen einer Mailbox; kann zum Einrichten einer Weiterleitung auf Mailbox-Ebene verwendet werden
Set-InboxRule	Änderung an einer bestehenden Weiterleitungsregel (Inbox-Ebene)
Set-TransportRule	Änderung an einer bestehenden Transportregel (Mail Flow Rule)

Schlüsselwort	Bedeutung des Logeintrags
DeliverToMailboxAndForward	Hinweis darauf, dass eine E-Mail an eine andere Mailbox weitergeleitet wurde
ForwardingSMTPAddress	Hinweis auf eine erfolgte Weiterleitung einer E-Mail
ForwardingAddress	Hinweis auf eine erfolgte Weiterleitung einer E-Mail
SentTo	Hinweis darauf, wohin eine E-Mail gesendet beziehungsweise weitergeleitet wurde
BlindCopyTo	Hinweis darauf, wohin eine E-Mail gesendet beziehungsweise weitergeleitet wurde
ForwardTo	Hinweis darauf, wohin eine E-Mail gesendet beziehungsweise weitergeleitet wurde

Schritt 6: Persistent Access – Hintertüren entdecken

Im nächsten Schritt gilt es zu prüfen, ob der Angreifer Hintertüren eingerichtet hat. Das würde ihm auch im Fall einer Entdeckung noch Zugriff auf die erbeuteten Konten gewähren. Hier gibt es im Wesentlichen drei beliebte Techniken: App-Kennwörter, das Einrichten schädlicher OAuth-Applikationen und die Manipulation von Berechtigungen.

App-Kennwörter dienen eigentlich der Absicherung von Netzwerkprotokollen, die Microsofts „Modern Authentication“ nicht unterstützen. Um die Sicherheit eines Kontos nicht durch die Verwendung des Kennwortes über ein Protokoll, das nicht dem aktuellen Sicherheitsstand entspricht, zu gefährden, bietet Microsoft die Möglichkeit, ein spezifisches Kennwort einzurichten. Es gilt nur für dieses Protokoll.

Wird es kompromittiert, erhält der Angreifer nur Zugriff zu einem einzelnen Protokoll, zum Beispiel IMAP oder POP, nicht aber zum gesamten Nutzerkonto. Doch Angreifer können diese Funktion auch missbrauchen, damit sie über ein selbst eingerichtetes App-Kennwort auch nach Änderung des Kennworts im Azure AD noch Zugriff auf die Mails eines Nutzers haben und gegebenenfalls auch weiterhin illegitime Mails verschicken können.

Zur Prüfung auf App-Passwörter sollten Administratoren zum einen im Azure AD die für den jeweiligen Benutzeraccount hinterlegten Authentifizierungsmethoden sichten und zum anderen im Kontext des Kontos selbst die Liste der App-Kennwörter abrufen (siehe ix.de/z2y8).

Anwendungen als Hintertür missbrauchen

Auch Enterprise-Applikationen, die sich mittels OAuth authentifizieren, können als Hintertür zu einem kompromittierten Konto genutzt werden. Berechtigt der Angreifer eine von ihm kontrollierte Enterprise-Applikation zum Zugriff auf das übernommene Konto, erlaubt er damit der Applikation, Aktionen im Kontext des Benutzers durchzuführen.

So ist über diese Applikation auch nach Änderung des Kennworts ein Zugriff mit den gewährten Berechtigungen möglich. Um zu prüfen, ob im Rahmen eines Angriffs Enterprise-Applikationen Berechtigungen erhielten – Microsoft spricht in diesem Zusammenhang von „Illicit Consent Attacks“ –, gibt es mehrere Möglichkeiten.

Administratoren können die Berechtigungen über das Azure-Active-Directory-Portal über den Menüpunkt „Nutzer“ und Auswahl des betroffenen Nutzerkontos prüfen. Eine globale Liste zeigt im Azure AD der Unterpunkt Enterprise-Applikationen. Wer lieber mit PowerShell arbeitet, kann das Skript AzureADPSPermissions.ps1 (siehe ix.de/z2y8) verwenden, um sämtliche OAuth-Berechtigungen eines Tenant in eine CSV-

Datei zu exportieren und anschließend zu überprüfen.

Das Hinzufügen von Enterprise-Applikationen beziehungsweise das Erteilen von Berechtigungen für sie im Analysezeitraum wird im UAL erfasst. Das Werkzeug Hawk extrahiert die Artefakte automatisch (Azure_Application_Audit.csv und Consent_Grant.csv).

Eine Variante zum Phishing mittels OAuth-Applikationen ist das sogenannte Device-Code-Phishing, mit dem sich Office-365-Konten übernehmen lassen. Details zu dieser Angriffstechnik sowie Hinweise zur Detektion und Aufklärung finden sich in einem Artikel des Sicherheitsforschers Nestori Syynimaa (siehe ix.de/z2y8).

Schlüsselwort	Bedeutung des Logeintrags
Add 0Auth2PermissionGrant	Einer Enterprise-Applikation wurden Berechtigungen erteilt.
Consent to application	Einer Enterprise-Applikation wurden Berechtigungen durch einen Admin erteilt.
Add app role Assignment grant to use	Ein Benutzer wurde einer Applikation hinzugefügt.

Hat ein Angreifer mehrere Konten eines Unternehmens kompromittiert, kann er sie dazu missbrauchen, Hintertüren einzurichten, indem er den anderen kompromittierten Konten Zugriff auf eine Mailbox gibt. Solange die Verteidiger nicht sämtliche betroffenen Konten identifizieren, behält der Angreifer weiter Zugriff.

Ereignisse im Zusammenhang mit Berechtigungsänderungen lassen sich durch die Suche nach den folgenden Schlüsselwörtern im UAL ausfindig machen:

Schlüsselwort	Bedeutung des Logeintrags
Add-MailboxPermission	Neue Berechtigungen auf ein Postfach wurden vergeben.

Schlüsselwort	Bedeutung des Logeintrags
Add-MailboxFolderPermission	Neue Berechtigungen auf einen Order in einem Postfach wurden vergeben.
Add-RecipientPermission	Hinweis darauf, dass einem Benutzer die „Senden als“-Berechtigung zugewiesen wurde.
Set-MailboxFolderPermission	Bestehende Berechtigungen eines Ordners in einem Postfach wurden geändert.

Hat ein Angreifer sogar ein Konto mit administrativen Berechtigungen gekapert, kann er zudem eigene neue Benutzerkonten anlegen, die dann als Hintertür dienen. Auch das hinterlässt Spuren im UAL.

Schlüsselwort	Bedeutung des Logeintrags
Added user	Ein neuer Benutzer wurde angelegt.

Schritt 7: Datenexfiltration analysieren

Bestätigt es sich, dass jemand Unbefugtes Zugriff auf das Unternehmensnetzwerk hatte, stellt sich in erster Linie die Kernfrage: Worauf hat der Angreifer zugegriffen? Dem zugrunde liegt oft die (späte) Erkenntnis über Art und Umfang der Informationen, die mit einem Benutzerkonto prinzipiell erreichbar wären, verbunden mit dem Wunsch, dieses Worst-Case-Szenario irgendwie einzugrenzen.

Hier zunächst die schlechte Nachricht vorweg: Es ist in der Praxis selten möglich, einen Negativbeweis zu führen, also festzustellen, was die Angreifer nicht mitgenommen haben. Die Aussagekraft der Artefakte ist meist begrenzt, da schlicht nicht alles protokolliert wird. In der Regel muss bei einer gesicherten Kompromittierung eines Kontos unterstellt werden, dass der Angreifer alle erreichbaren Inhalte ausgespäht hat. Das hat erhebliche Konsequenzen beispielsweise für die

datenschutzrechtliche Bewertung eines Vorfalls.

Die gute Nachricht ist, dass auch Microsoft das erkannt hat. Konten, die mit einer E5-Lizenz ausgestattet sind, verfügen über eine „erweiterte Überwachung“. Diese Funktion protokolliert unter anderem Zugriffe auf einzelne E-Mails, was die Chance auf den seltenen Negativbeweis zumindest für die Inhalte des Postfachs deutlich verbessert.

Im UAL finden sich dann Einträge der Art MailItemsAccessed. Diese haben unter anderem ein Attribut MailAccessType, das zwischen Bind und Sync unterscheidet.

Operation	Bedeutung des Logeintrags
MailItemsAccessed	Hinweis auf den erfolgten Zugriff auf Inhalte eines Postfachs

Bind-Einträge werden erzeugt, wenn eine einzelne E-Mail abgerufen wird. Die ID der Nachricht steht dann im Attribut InternetMessageId. Die Protokollierung unterliegt jedoch einer wichtigen Einschränkung: Werden innerhalb von 24 Stunden mehr als 1000 Zugriffe dokumentiert, wird die Protokollierung für Bind-Ereignisse für 24 Stunden ausgesetzt (Throttle).

Zuerst sollte also geprüft werden, ob das UAL Einträge des Typs MailItemsAccessed für die zu untersuchende Mailbox enthält. Anschließend gilt es auszuschließen, dass ein Throttling stattgefunden hat. Dazu schaut man, ob es bei den MailItemsAccessed-Ereignissen welche gibt, die beim Attribut IsThrottled den Wert True vermerkt haben. Im Idealfall gibt es keinen solchen Eintrag.

Welche Sitzung gehört zu wem?

Der nächste Schritt besteht darin, die zum Angreifer gehörenden Sitzungen zu ermitteln. Dafür gleicht man die MailItemsAccessed-Vorgänge im UAL mit den Informationen des Angreifers (verdächtige Log-in-Aktivitäten, IP-Adressen, Zeitstempel, Art des Zugriffs) und den Informationen über den

legitimen Anwender ab. Die Einträge haben mitunter mehrere Session-IDs und IP-Adressen für ein Benutzerkonto. Anhand der in den vorangegangenen Schritten ermittelten Kompromittierungsindikatoren lässt sich feststellen, welche Sitzungen wahrscheinlich legitim oder gültig sind. Einige Sitzungen haben möglicherweise keine Session-ID, weil für die Anmeldung eine alte (Legacy-)Authentifizierung verwendet wurde. Die verdächtigen MailItemsAccessed-Einträge werden dann weiter analysiert.

Sync-Einträge entstehen immer dann, wenn ein E-Mail-Client, beispielsweise Outlook, ein Postfach synchronisiert und dabei Inhalte auf einen lokalen Computer herunterlädt. Hierbei entsteht kein Logeintrag pro Element, sondern pro Ordner des Postfachs. Finden sich im UAL MailItemsAccessed-Einträge mit dem MailAccessType Sync, die dem Angreifer zugeordnet werden, so muss man davon ausgehen, dass alle E-Mails im synchronisierten Ordner kompromittiert wurden.

Zuletzt bleiben die Bind-Vorgänge, die dem Angreifer zugeordnet werden. Diese enthalten eine InternetMessageID. Um damit auf die eigentlichen Nachrichten schließen zu können, ist es notwendig, das Message Trace Log mit den IDs abzugleichen. Leider reicht das Message Trace Log nicht so weit zurück wie die Einträge im UAL, sondern lediglich zehn Tage. Auch lässt sich die InternetMessageID nicht als Suchparameter im Rahmen einer Suche nach Beweismitteln (E-Discovery) verwenden.

Können E-Mails nicht mehr über das Message Trace Log zugeordnet werden, bleibt lediglich der Weg, das Postfach selbst zu exportieren und die E-Mails zu durchsuchen. Die ID ist in den Eigenschaften der E-Mails gespeichert. Der Export des Postfachs lässt sich außerdem über die E-Discovery-Funktion realisieren, die auch bereits gelöschte Elemente berücksichtigt (sofern entsprechende Aufbewahrungsrichtlinien konfiguriert sind und die Elemente noch vorgehalten werden).

Rekonstruieren, was geklaut wurde

Wie beschrieben können E-Mails auch über Weiterleitungsregeln abgegriffen werden. Findet man bei einer Untersuchung solche Regeln, kann sowohl das UAL (siehe Schritt 5) wie auch die Logik der Regeln selbst Aufschluss über die betroffenen Inhalte geben. Neben dem Abgleich der Einträge im UAL mit dem Message Trace Log sollte die Mailbox nach den Parametern der Regel(n) durchsucht werden.

Sofern ein Angreifer Zugang zu einem Konto mit administrativen Berechtigungen und der E-Discovery-Suche hatte, kann er auch auf diesem Weg Inhalte gesucht und exportiert haben. Hinweise darauf lassen sich wieder im UAL finden.

Analog zu den E-Mails sind alle weiteren Inhalte zu berücksichtigen, die mit dem kompromittierten Konto für den Angreifer erreichbar waren. Das beinhaltet sowohl in OneDrive geteilte Dateien wie Teams-Nachrichten und SharePoint-Seiten als auch sämtliche nachgelagerten Applikationen, die Azure AD zur Authentifizierung verwenden. Die Analyse ist allerdings oft sehr individuell und würde den Rahmen dieses Artikels sprengen.

Schritt 8: Remediation

Nachdem die Aktivitäten eines Angreifers nachvollzogen wurden, gilt es, alles rückgängig zu machen, also alle gefundenen Weiterleitungsregeln, Enterprise-Applikationen, App-Kennwörter et cetera zu entfernen und die Kennwörter der betroffenen Konten, falls noch nicht geschehen, zurückzusetzen. Auch sollten alle Analysen und eingeleiteten Maßnahmen dokumentiert und mit den zugehörigen Logdateien aufbewahrt werden.

Zeigte die Untersuchung einen unberechtigten Zugriff auf Postfächer, handelt es sich um einen meldepflichtigen Vorfall gemäß der DSGVO. Dementsprechend ist eine Erklärung an den zuständigen Landesdatenschutzbeauftragten verpflichtend. Dabei

gilt es, die gesetzlichen Fristen zu beachten. Binnen 72 Stunden ab dem Zeitpunkt der Kenntnisnahme muss die Meldung erfolgen. Zu diesem Zeitpunkt ist gegebenenfalls noch nicht das gesamte Ausmaß des Vorfalls bekannt. In diesem Fall sollte die Meldung einfach alle bisher gesicherten Informationen enthalten. Die Meldung sollte durch den benannten Datenschutzbeauftragten des betroffenen Unternehmens erfolgen.

Neben den Datenschutzbehörden müssen gegebenenfalls auch die betroffenen Personen informiert werden. Dies ist dann der Fall, wenn besonders heikle personenbezogene Daten gemäß Art 9 DSGVO – also beispielsweise religiöse oder weltanschauliche Überzeugungen oder Gesundheitsdaten – betroffen sind. In diesem Fall sind die betroffenen Personen direkt zu benachrichtigen. Die Prüfung einer solchen Meldepflicht obliegt dem Datenschutzbeauftragten. Gegebenenfalls sollte bei Verdacht auf einen solchen Fall juristischer Beistand hinzugezogen werden.

Schritt 9: Root Cause Analysis – woran liegts?

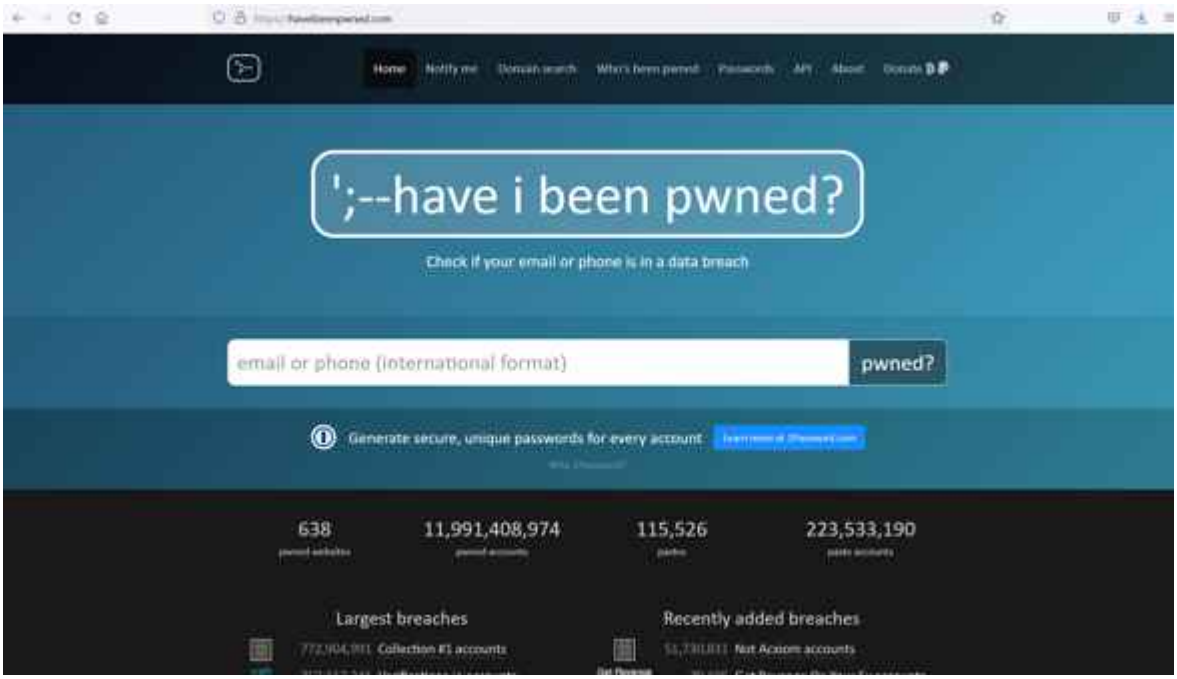
Nachdem aufgeklärt ist, wie ein Angreifer vorgegangen ist und was er genau getan hat, bleibt noch die Frage, wie das passieren konnte. Wie hat er initial Zugang erhalten?

Auch hier ist leider keine pauschale Anleitung möglich, doch die häufigsten Ursachen sind folgende:

- Password Spraying / Brute Force / einfach zu erratende Passwörter: Allen drei Szenarien ist gemeinsam, dass sie in der Regel mit mehrfachem Ausprobieren einhergehen. In den Logs äußert sich dies durch multiple fehlgeschlagene Log-in-Versuche bei einem oder mehreren Konten, ausgehend von derselben IP-Adresse und/oder ähnlichen Parametern wie User-Agent, Protokoll und Zeitpunkt.
- (Spear-)Phishing: Bei einem Phishingangriff erhält das

Opfer eine E-Mail, die einen Link oder einen Anhang enthält, über den die Zugangsdaten abgegriffen werden (funktioniert teilweise auch bei MFA) oder eine Enterprise App via OAuth-Berechtigungsanfrage untergeschoben wird. In dem Fall sind keine gehäuften fehlgeschlagenen Log-in-Versuche zu beobachten. Stattdessen gilt es, die Phishingmail im Postfach oder den aufgerufenen Link ausfindig zu machen.

- Password Re-use / Leaked Credentials: Oft verwenden Anwender ein Passwort für mehrere Dienste und Konten oder recyceln ein privates Passwort für Firmenzwecke. In dem Fall kann es sein, dass das Kennwort bei einem der anderen Dienste ausgespäht wurde und dann für die Anmeldung am Microsoft-365-Account ausprobiert wird. Auch hier ist nicht unbedingt eine gehäufte Anzahl an Fehlversuchen zu beobachten, sofern nicht zusätzlich MFA aktiviert ist. Um der Ursache in dem Fall näherzukommen, empfiehlt es sich, mit dem Benutzer ein offenes Gespräch zu führen oder die Unternehmens-E-Mail des Anwenders bei seriösen Diensten wie haveibeenpwned.com einzugeben (siehe Abbildung).



Ob ein Passwort geleakt wurde, kann man beispielsweise bei Diensten wie „Have I Been Pwned“ herausfinden. Dieser Dienst

des australischen Sicherheitsforschers Troy Hunt hat einen guten Ruf, da er nicht das Passwort selbst, sondern nur den Benutzernamen abfragt.
Nach der erfolgreichen Bewältigung des potenziellen oder realen Sicherheitsvorfalls sollte immer auch geprüft werden, welche Lektionen man daraus lernen kann und welche Maßnahmen zu ergreifen sind, damit ähnliche Vorfälle in Zukunft seltener oder gar nicht mehr vorkommen. Dabei soll es explizit keine Schuldzuweisungen geben, das Stichwort lautet hier vielmehr „Blameless Post Mortem“.

Awareness-Maßnahmen und Schulungen können gängige Betrugsmuster vermitteln und damit die Anfälligkeit der Mitarbeitenden für solche Angriffe verringern. Klar definierte Prozesse zur Veranlassung von Zahlungen helfen außerdem, bestimmte Arten von finanziellem Betrug zu erschweren. Häufig werden aber im Rahmen der Vorfallsbehandlung vor allem technische Gegebenheiten identifiziert, die die Kompromittierung erleichtert oder die Untersuchung des Vorfalls erschwert haben. So ist es hilfreich, die SPF-, DKIM- oder DMARC-Konfiguration (Sender Policy Framework; DomainKeys Identified Mail; Domain-based Message Authentication, Reporting and Conformance) nachzurüsten, falls sie im Vorfeld des Vorfalls noch nicht aktiv war, die Protokollierung lässt sich verbessern, wenn Logs für die Aufklärung des Angriffs fehlten, oder das Installieren von OAuth-Anwendungen kann für Nutzer des Tenants eingeschränkt werden, falls Angreifer solche Anwendungen als Hintertür installiert haben.

Microsoft gibt im Rahmen einer Referenzarchitektur zahlreiche Hinweise für das Absichern von Microsft-365- und Azure-AD-Umgebungen (siehe ix.de/z2y8), die im Nachgang eines Vorfalls (re-)evaluiert werden und bei Bedarf in das Sicherheitskonzept des Unternehmens integriert werden können. Dedizierte Dienste wie Microsoft Defender for Office, Microsoft Defender for Identity oder Microsoft Defender for Cloud Apps können gegen Angriffe schützen oder bei ihrer Entdeckung und Aufbereitung helfen. Allerdings sind sie häufig nur in den teureren

Lizenzen der Microsoft-Produkte enthalten oder müssen sogar separat lizenziert werden. (ur@ix.de)

1. Quellen
2. Jens Lüttgens, Dominik Oepen; E-Mail-Betrug in MS-365-Umgebungen; iX 12/2022, S. 102
3. Vertiefende Microsoft-Artikel, das erwähnte PowerShell-Skript sowie die Microsoft-Referenzarchitektur sind über ix.de/z2y8 zu finden.

Introducing a new phishing technique for compromising Office 365 accounts

The ongoing global phishing campaings againts Microsoft 365 have used various phishing techniques.
Currently attackers are utilising forged login sites and OAuth app consents. In this blog, I'll introduce a new phishing technique based on Azure AD device code authentication flow.
I'll also provide…