Incident Response in der Cloud

Infrastruktur in der Cloud bietet durch die Erreichbarkeit im Internet besonders viel Angriffsfläche. Schon eine Fehlkonfiguration kann für einen Datenabfluss reichen. Um das Ausmaß eines Angriffs zu beurteilen, müssen alle nötigen Logs verfügbar sein.

Von Tabea Nordieker

Mit der Migration der Unternehmensinfrastruktur in die Cloud setzen auch die Angreifer ihre Hebel direkt dort an [1]. Denn im Vergleich zu einer On-Premises-Infrastruktur bietet die Cloud per Design eine große Angriffsfläche, da die Ressourcen remote über das Internet erreichbar sein sollen. Somit sind die Berechtigungsverwaltung und das Zugriffsmanagement zentrale Komponenten des Absicherns von Cloud-Umgebungen. Bereits eine Fehlkonfiguration kann zu großem Schaden führen: Angreifer durchsuchen das Internet aktiv nach veröffentlichten API-Schlüsseln oder öffentlich zugänglichen S3-Buckets.

Die Angriffsszenarien sind altbekannte Phänomene wie Ransomware, Datenabfluss oder kompromittierte Benutzer. Was in der Cloud neu ist, ist der Missbrauch von Ressourcen, was einen nicht zu unterschätzenden finanziellen Schaden mit sich bringt. Die Kosten von Cloud-Diensten orientieren sich an der übertragenen Datenmenge oder den verwendeten Ressourcen. Angreifer können durch schädliche Aktivitäten die monatlichen Rechnungen erheblich in die Höhe treiben.

Angriff auf die Cloud

Die Herangehensweise einer forensischen Analyse in der Cloud weist gegenüber on Premises grundlegende Unterschiede auf [2]. Dieser Artikel fokussiert sich auf die Cloud-Umgebungen von Microsoft und Amazon. Die beschriebenen Konzepte sind in ähnlicher Form auch bei anderen Cloud-Anbietern anzutreffen. Ein fiktives, realitätsnahes Szenario zeigt mögliche Angriffsvektoren, die veranschaulichen, wie Incident Response in der Cloud abläuft.

Angenommen, ein Mitarbeitender eines Unternehmens erhält eine Phishing-E-Mail, die auf eine vermeintliche Microsoft-365-Loginseite (M365) verweist. Die Person gibt auf der Loginseite ihre Zugangsdaten ein, die Angreifer im Hintergrund mitlesen. Das kann auch funktionieren, wenn eine Multi-Faktor-Authentisierung (MFA) eingerichtet wurde, da die Kriminellen die gestohlenen Logindaten im Hintergrund direkt an Microsoft weiterleiten und M365 somit eine legitime MFA-Abfrage auslöst (siehe ix.de/z5jk).

Der Angreifer hat nun Zugriff auf die Dienste von M365, beispielsweise Exchange Online und SharePoint. Im Postfach des kompromittierten Benutzers richtet er eine Weiterleitungsregel ein, sodass er alle empfangenen und versendeten E-Mails mitlesen kann. Diese Informationen lassen sich für spätere Business-E-Mail-Compromise-Angriffe verwenden.

Kurze Zeit später erreicht eine Lösegeldforderung einen IT-Administrator des Unternehmens. Darin behauptet der Angreifer, sensible Projektdaten gestohlen zu haben, und droht mit deren Veröffentlichung, wenn nicht ein Lösegeld in Bitcoins gezahlt wird. Eine erste Überprüfung durch den IT-Mitarbeitenden ergibt, dass gewisse Projektdaten gelöscht wurden und nicht mehr auf SharePoint verfügbar sind.

Der Verzeichnisdienst Entra ID als Teil der Microsoft Cloud wird im Unternehmen nicht nur für die Authentisierung bei M365 verwendet, sondern kann auch für die Zugangsberechtigung zu den Amazon Web Services (AWS) genutzt werden. Der Angreifer erstellt dadurch eine eigene VM in AWS, mit der er Data-Mining betreibt. Ein Blick in die AWS-Flow-Logs (Firewall der Cloud) zeigt zusätzlich einen erheblichen Ausschlag in

iX-TRACT

- Nutzt man Cloud-Anbieter, sollte man sichergehen, dass alle relevanten Logs gesammelt werden.
- Da man Berechtigungen auf verschiedenen Ebenen vergibt, ist es entscheidend, das jeweilige Cloud-Schema zu kennen, um die Analyse an den richtigen Ausgangspunkten anzusetzen.
- Fehlende Sichtbarkeit kann dazu führen, dass Spuren eines Angriffs nicht entdeckt werden.
- Hat ein Angreifer ein Benutzerkonto oder eine Ressource kompromittiert, muss das Incident-Response-Team identifizieren, welche Berechtigungen und Rollen mit dieser Entität verknüpft sind, um den Angriff korrekt einschätzen und eindämmen zu können.

der Datenübertragung. Ein API-Schlüssel wurde gestohlen, der Zugriff auf einen S3-Bucket (Datenspeicher in der AWS-Cloud) erlaubt, wodurch es zum Datenabfluss kam.

An diesem Punkt ruft man das Incident-Response-Team, um den Vorfall zu untersuchen. Die zentrale Aufgabe: herausfinden, woher der Angriff erfolgte, welche Konten und Ressourcen kompromittiert wurden und die damit verbundenen Berechtigungen. Außerdem gilt es festzustellen, welche Auswirkungen der Angriff auf die Organisation hat, etwa Änderungen an der Konfiguration, das Erstellen von neuen Ressourcen und Datenabflüsse. Ein detailliertes Bild zu Taktiken und Techniken der Cloud-Angriffe zeigt die Cloud-Matrix MITRE ATT&CK (siehe ix.de/z5jk).

Die Cloud verstehen

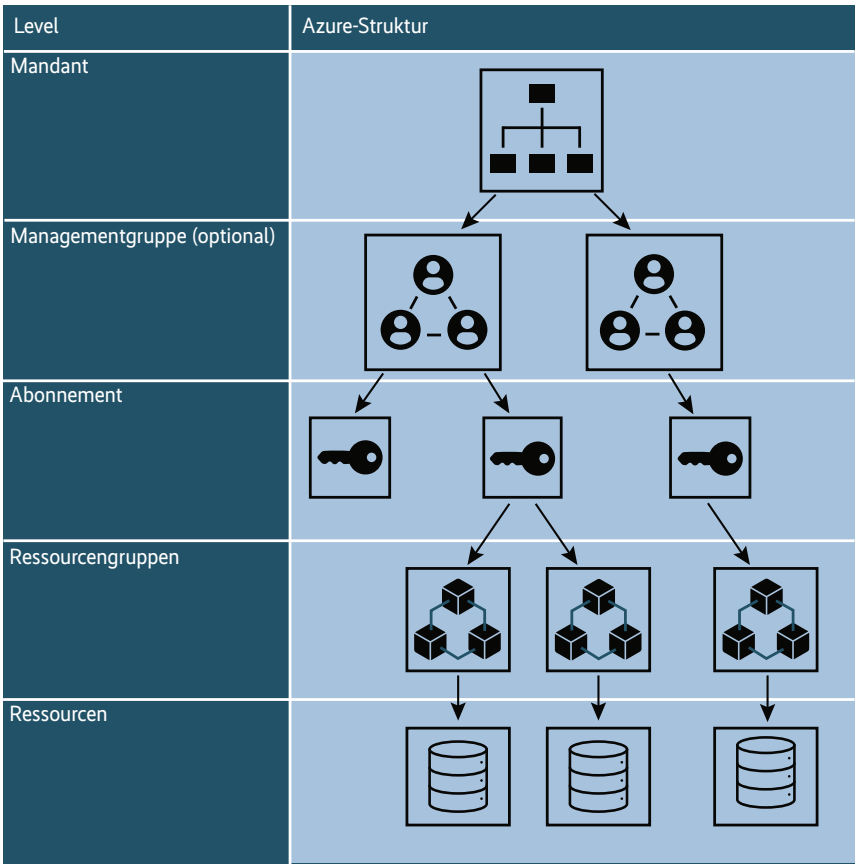
Auch wenn sich der Cloud-Aufbau der einzelnen Anbieter in vielen Punkten gleicht, hat jeder Anbieter Besonderheiten, die es bei der forensischen Analyse zu beachten gilt [3]. Insbesondere die Vergabe von Berechtigungen und das Sammeln von Logdateien sind ausschlaggebend für den Erfolg einer Untersuchung. Abbildung 1 und 2 zeigen die Aufbauschemata von Azure und AWS.

Was die einzelnen Clouds eint, sind die grundlegenden Komponenten, auf denen ihre Funktionen basieren:

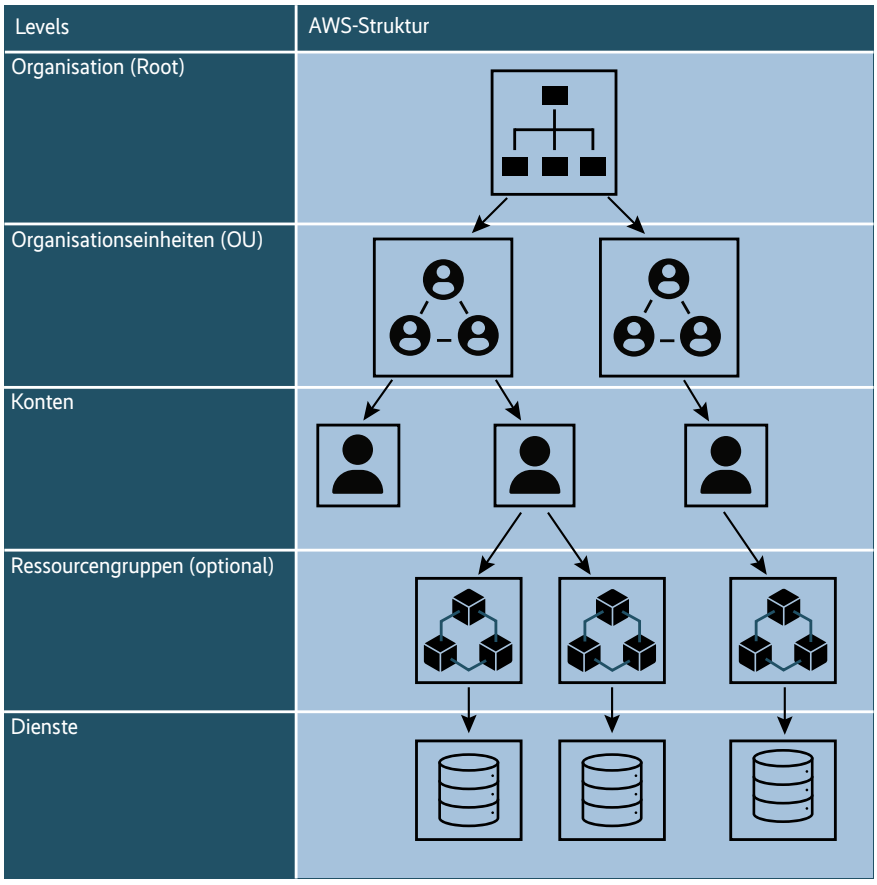
- Identity and Access Management (IAM) für die Rollen- und Rechtevergabe;
- Compute (VMs und Serverless-Funktionen);
- Networking für den internen und externen Netzwerkverkehr mit Funktionen, die einer Firewall oder einem VPN gleichkommen;
- Storage (Datenspeicher);
- Analytics für die Loganalyse innerhalb der Cloud.

Da man in der Cloud nur Ressourcen zur Verfügung gestellt bekommt und keinen Zugriff auf die Cloud-Infrastruktur an sich hat, ist man beim Logging vom Cloud-Anbieter abhängig. Dies zeigt sich einerseits in den gesammelten Logdaten selbst, aber auch daran, ob diese standardmäßig aktiviert sind, wie lange die Aufbewahrungszeit beträgt und mit welchen Kosten die Protokollierung verbunden ist. Die Tabelle „Logdateien von Microsoft und AWS“ zeigt die für eine forensische Analyse eines Sicherheitsvorfalls relevanten Logdateien der beiden Anbieter Microsoft und Amazon.

Eine ebenfalls nicht zu unterschätzende Informationsquelle sind die Ab-



Schematischer Aufbau der Azure-Cloud (Abb. 1).



Schematischer Aufbau der AWS-Cloud (Abb. 2).

Logdateien von Microsoft und AWS

Cloud	Logdatei	Logebene	Aufbewahrungszeit	Standardmäßig aktiv?
Azure	Sign-in-Logs	Tenant	30 Tage	ja
Azure	Auditlogs	Tenant	30 Tage	ja
Azure	Activity-Logs	Subscription	90 Tage	ja
Azure	Network-Security-Group-Flow-Logs	Ressource (Network Security Group)	1 Jahr	nein
Azure	Storage-Account-Logs	Ressource (Storage-Account)	individuell	nein[1]
M365	Unified-Audit-Logs	Tenant	180 Tage (E3)/1 Jahr (E5)	ja
AWS	CloudTrail	Organisation	90 Tage	ja
AWS	VPC-Flow-Logs	Service (VPC-/Subnet-/Network-Interface)	individuell	nein[2]
AWS	Route-53-Logs	Service (VPC)	individuell	nein[3]
AWS	Load-Balancer-Logs	Service (VPC)	individuell	nein[4]
AWS	Server-Access-Log	Service (S3-Bucket)	individuell	nein[5]

[1] können im Network Watcher des Azure Portals aktiviert werden; [2] können durch das Erstellen eines Flow-Logs erstellt werden; [3] können in der Route-53-Konsole erstellt werden; [4] können in der EC2-Konsole erstellt werden; [5] können in der S3-Konsole aktiviert werden; für [2] und [5] siehe ix.de/z5jk.

rechnungsdaten. Die zusätzliche Nutzung von Ressourcen, beispielsweise in einem Crypto-Mining-Fall, kann zu erheblichen Kosten führen. Auch Datenexfiltrationen schlagen sich in der Rechnung nieder, denn Exporte aus der Cloud heraus und Datenübertragungen zwischen Cloud-Regionen verursachen Kosten. Ein möglicher Schutz vor solchem finanziellen Schaden ist die Konfiguration von Limits und Quotas.

Berechtigungen für die Analyse

Um in der Cloud eine Analyse durchführen zu können, ist ein Analysebenutzer mit den entsprechenden Berechtigungen notwendig. Es empfiehlt sich, diesen Analysebenutzer möglichst hoch in der Hierarchie anzusiedeln (siehe Abbildung 1 und 2), da man sonst wichtige Informationen übersehen kann.

Beispielsweise sieht ein Benutzer mit Berechtigungen auf ein Azure-Abonnement nur Elemente, die sich im selben Abonnement befinden. Führt das Incident-Response-Team nun eine Analyse im Verzeichnisdienst Entra ID durch und hat nur einen Benutzer innerhalb des Abonnements und nicht auf Ebene der Managementgruppe oder des Mandanten, erhält es kein umfassendes Bild.

Außerdem ist es wichtig, dem Analysebenutzer die relevanten Rollen zu geben. Diese unterscheiden sich je nach Cloud-Anbieter, zentral sind jedoch Rollen, die die Logdateien ansehen dürfen. Grundsätzlich reichen in den meisten Fällen globale Leseberechtigungen, da man während einer Analyse keine Veränderungen an der Konfiguration vornehmen sollte.

Incident-Response-Prozess in der Cloud

Der Incident-Response-Prozess für Cloud-Umgebungen lässt sich in sechs Schritten zusammenfassen:

1. Verschaffen eines Überblicks über die Authentisierung und Konfiguration: Welche Cloud-Anbieter sind im Einsatz? Welche Dienste werden genutzt? Was für Lizenzierungen sind vorhanden? Wie sind die Services und Ressourcen miteinander verknüpft?
2. Sammeln der relevanten Logs und Konfigurationsinformationen und deren Export.
3. Identifikation des Zugangs der Angreifer: Wurde ein Benutzer kompromittiert? Ist ein API-Schlüssel gestohlen worden? Liegt eine Fehlkonfiguration vor [4]?
4. Feststellen, welches Ausmaß der Vorfall hat. Welche Rechte und Rollen besitzt die kompromittierte Ressource? Welche Aktivitäten können dem Angriff zugeschrieben werden?
5. Eindämmung des Vorfalls durch Deaktivierung der kompromittierten Benutzer, Blockierung des Zugangs der Angreifer und Isolation der infizierten Ressourcen.
6. Tiefer gehende Analyse, um Aktivitäten, Persistenzen und Datenzugriffe der Angreifer zu identifizieren.

Mit fortschreitender Analyse und neu gewonnenen Erkenntnissen ist dieser Prozess iterativ zu wiederholen.

Protokoll einer Analyse

Beim Beispiel in diesem Artikel stellt sich also die Frage, ob die M365-Logs Anmeldungen des Angreifers anzeigen. Ausgangspunkt bleibt der kompromittierte User, nach dessen Anmeldungen man die Sign-in-Logs durchsucht. Dabei filtert man bekannte IPs und Geolocation heraus. Eine Hilfestellung bietet Microsoft mit den Risky-User- und Risky-Sign-in-Listen im Entra-ID-Portal. Die Sign-in-Logs geben zusätzlich Auskunft, wie die Anmeldung erfolgt ist (Ressource, Client-App) und wie der Benutzer validiert wurde (Passwort, MFA, Access-Token). Stellt man eine Kompromittierung eines Benutzers fest, sind folgende Sofortmaßnahmen umzusetzen:

- Passwort zurücksetzen.
- Sitzung schließen.
- Token widerrufen.

Außerdem muss man sicherstellen, dass der Angreifer keine neuen Geräte zur Multi-Faktor-Authentisierung hinzugefügt hat.

Im nächsten Schritt folgt das Prüfen, welche Veränderungen der Angreifer im Postfach des kompromittierten Benutzers durchgeführt hat. Eine Möglichkeit ist die Suche nach erstellten E-Mail-Weiterleitungsregeln:

```
operation: Set-Mailbox AND ↵
  (parameters.ForwardingSMTPAddress:↵
    * OR parameters.DeliverToMailbox↵
 AndForward:* OR ForwardingAddress:*)
```

Des Weiteren sollte geprüft werden, ob der Angreifer neue Inbox Rules hinzugefügt oder bestehende Regeln verändert hat [5]:

```
Operation: (new-inboxrule or set-↵
       inboxrule or UpdateInboxRules)
```

Weitere interessante Operationen in den Unified-Audit-Logs (UAL) bezüglich

Exchange Online zeigt die Tabelle „Exchange-Operationen in den Unified Audit Logs (UAL) von Azure“.

Wie im Beispiel beschrieben, hat ein Angreifer durch einen kompromittierten Benutzer ebenfalls Zugriff auf SharePoint und OneDrive. Die folgende Auswahl an Operationen erlaubt eine Analyse, auf welche Dokumente zugegriffen wurde, und ob es eventuell zu Veränderungen oder gar einem Datenabfluss kam:

- FileAccessed
- FileModified
- FileRenamed
- FileRecycled
- FileDeleted
- FileDownloaded

Eine weitere Möglichkeit, Daten aus einem SharePoint zu entwenden, ist das Teilen von Ordnern und Dateien mit externen Benutzern. Die Einrichtung einer Freigabe in SharePoint ist ebenfalls in den UAL ersichtlich, die entsprechenden Operationen zeigt die Tabelle „SharePoint-Operationen in den UAL von Azure“. Das Erstellen von Freigaben birgt auch das Risiko einer Fehlkonfiguration. Wird ein Link mit bestimmten Personen geteilt, geschieht dies in einer E-Mail. Das ist ebenfalls in den Exchange-Logs ersichtlich.

Wenn der Azure-Verzeichnisdienst Entra ID wie im Beispiel für die Authentifizierung in anderen Clouds verwendet wird, sollte man die Active Directory Federation Services (ADFS) Sign-in Logs analysieren. Gibt es auch hier eine verdächtige Anmeldung durch den kompromittierten Benutzer, muss man die Analyse ausweiten – im Beispiel auf die CloudTrail-Logs von AWS.

Exchange-Operationen in den Unified-Audit-Logs (UAL) von Azure

Operation	Beschreibung
MailItemAccessed	Eine E-Mail wurde geöffnet.[1]
Add-MailboxPermission	Es wurden Änderungen an den Berechtigungen des Postfachs vorgenommen.
MoveToDeletedItems	Eine Nachricht wurde in den Ordner Deleted verschoben.
SoftDelete	Eine Nachricht wurde aus dem Ordner Deleted gelöscht.
HardDelete	Eine Nachricht wurde aus dem Ordner Recoverable Items entfernt und damit unwiederbringlich gelöscht.

[1] Hier unterscheidet man zwischen Sync- und Bind-Aktivitäten; Sync beschreibt die Synchronisation eines Postfachordners via Outlook, Bind den Aufruf einer einzelnen E-Mail via OWA, IMAP oder POP3.

SharePoint-Operationen in den UAL von Azure

Operation	Bemerkung
SharedLinkCreated	Ein Freigabelink wurde erstellt.
AnonymousLinkCreated	Die Datei wurde ohne Restriktionen mit allen geteilt, die den Link besitzen.
SecureLinkCreated	Die Datei wurde nur mit Mitgliedern einer dedizierten Gruppe geteilt.
SecureLinkUsed	Der zugesandte Link wurde genutzt, um auf eine Datei zuzugreifen.
SharedLinkDisabled	Der Freigabelink wurde deaktiviert.

Angriffe zum Missbrauch von Cloud-Ressourcen

Angriffe in der Cloud können auf die verarbeiteten Daten und auf die verfügbaren Ressourcen abzielen. Letztere nutzen Angreifer, indem sie eigene VMs erstellen, die sie für zukünftige Angriffe oder Crypto-Mining verwenden. Um die Logeinträge in AWS interpretieren zu können, ist das Verständnis des Amazon Resource Name (ARN) zentral. Dies ist eine globale Kennzeichnung, die jede Ressource und jede Identität in der AWS-Cloud eindeutig identifiziert. Der Aufbau eines ARN ist wie folgt:

```
arn:partition:service:region:↵
              account-id:resource-id
arn:partition:service:region:↵
 account-id:resource-type/resource-id
arn:partition:service:region:↵
 account-id:resource-type:resource-id
```

In den Logeinträgen beschreibt das Feld `EventSource`, welcher Dienst den Logeintrag generiert hat und welche Ressourcen betroffen sind:

- ec2.amazonaws.com – Themen rund um Computing und VM;
- s3.amazonaws.com – alle Aktivitäten rund um S3-Buckets;
- signin.amazonaws.com – Einträge zu Logins;
- iam.amazonaws.com – Informationen zu Rechten, Rollen und Authentisierungsmethoden.

Das Erstellen einer VM hat in den AWS-Logs den Event Name `RunInstances`. Die gleiche Analyse kann für Azure in den Activity-Logs erfolgen. Auch hier kann aus dem Operation Name herausgelesen werden, welcher Ressourcenprovider den Logeintrag generiert hat:

- MICROSOFT.COMPUTE
- MICROSOFT.STORAGE
- MICROSOFT.NETWORK
- MICROSOFT.RESOURCES

Um eine neu erstellte VM in Azure zu identifizieren, sucht man also nach der

Analyseumgebungen

Bei Incident Response in der Cloud muss man entscheiden, in welcher Umgebung man die Analyse durchführen will. Das geht direkt in der Cloud, mit Cloud-eigenen Mitteln oder in einer eigens für diesen Zweck erstellten IR-Umgebung in der Cloud. Außerdem kann man die relevanten Logdateien aus der Cloud exportieren und in einem SIEM oder der dafür entwickelten SOF-ELK untersuchen (siehe ix.de/z5jk). Die Tabelle „Vor- und Nachteile von Analyseumgebungen" stellt die Vor- und Nachteile dieser Verfahren gegenüber.

Vor- und Nachteile von Analyseumgebungen

Analysemethode	Vorteil	Nachteil
Cloud-eigene Mittel	• alles aus einer Hand • Aufbereitung der Logdateien ist optimiert	• Tools müssen oftmals bezahlt werden. • Kompromittierung der Cloud-Umgebung kann auch die Analyse beeinträchtigen.
IR-Umgebung in der Cloud	• getrennte Analyseumgebung • ortsunabhängig und individualisierbar • schneller Zugriff auf Analysedaten • Beweiskette wird durch Zugangsprotokollierung gewahrt	• Überregionaler Austausch verursacht Kosten. Dies kann durch mehrere IR-Umgebungen umgangen werden. • Gefahr der Kompromittierung der IR-Umgebung, wenn die Cloud angegriffen wird.
SIEM	• Korrelation diverser Datenquellen • fortlaufende Logumleitung • Erhöhung der Aufbewahrungszeiten	• Kosten durch Datenexport
SOF-ELK	• Open-Source-Tool • Neben initialen Hardwarekosten fallen keine Kosten an.	• Kosten durch Datenexport • Lückenhafte Analyse, falls Logdateien nicht aktiviert wurden.

Operation `MICROSOFT.COMPUTE/VIRTUALMACHINES/WRITE`. Virtuelle Maschinen kommen mit verschiedenen technischen Spezifikationen daher, für Crypto-Minings nutzen Angreifer VM-Typen, die eine GPU besitzen.

Im Bereich Computing ergeben sich für einen Datenabfluss andere Möglichkeiten als bei E-Mail-Postfächern und Datenablagen wie SharePoint und OneDrive. Es besteht die Gefahr, dass Angreifer einen API-Schlüssel zu einem Speicherkonto (Azure) oder S3-Bucket (AWS) entwenden. Oder sie erstellen einen Snapshot einer ganzen VM und exportieren ihn in einem weiteren Schritt.

Wird ein Schlüssel eines Speicherkontos in Azure angezeigt, ist das mit der Operation `Microsoft.Storage/storageAccounts/listKeys/action` in den Logs ersichtlich. Ein Angreifer braucht die entsprechenden Rechte, um auf ein Speicherkonto zuzugreifen und die hinterlegten Schlüssel auszulesen. Erfahrungsgemäß ist die Firewall eine gute Datenquelle, um Datenabflüsse zu identifizieren. Im Fall von Speicherkonten speichern die Flow-Logs diese Datentransfers jedoch nicht. Man benötigt zusätzliche Speicherkontenlogs, die nicht standardmäßig aufgezeichnet werden. Da diese Logdateien datenintensiv sind, sollte man sie nur für Speicherkonten aktivieren, die sensible Daten enthalten.

In AWS kann sich ein Angreifer lateral im Netzwerk bewegen, indem er die verfügbaren API-Keys enumeriert. Es existiert eine Vielzahl an API-Aufrufen, die Zugangsdaten ausgeben (siehe ix.de/z5jk). Ein Angreifer kann mit entsprechenden API-Schlüsseln auf S3-Buckets zugreifen und somit Daten exfiltrieren. Von welchen Systemen in kürzester Zeit eine große Menge an Daten abgeflossen ist, ist in den Flow-Logs ersichtlich.

Analyse einer VM in der Cloud

Wenn es zu einer Kompromittierung in der Cloud gekommen ist, kann es notwendig sein, eine dort betriebene VM zu analysieren. Um Kosten durch den Export eines Snapshots zu vermeiden, lohnt es sich, diese Analyse direkt in der Cloud durchzuführen. Die vorbereitenden Schritte für eine solche Analyse in Azure sind:

1. Snapshot erstellen (erzeugt eine identische Kopie der aktuellen VM).
2. Snapshot auf neue Disk kopieren.
3. Erstellen einer Analyse-VM – diese enthält die gängigen Analysetools.
4. Disk mit Snapshot als Datendisk in der Analyse-VM einlesen.
5. Analyse wie gehabt durchführen.

Im Vergleich zur klassischen IT-Forensik muss beachtet werden, dass die eingelesene Datendisk nicht schreibgeschützt ist. Falls diese durch die Analyse verändert oder beschädigt werden sollte, kann man die Vorbereitung ab Schritt 2 jederzeit wiederholen. In AWS unterscheidet sich das Vorgehen nur minimal. Schritt 2 wird nicht benötigt, da man Snapshots direkt einer Analyse-VM hinzufügen kann. Damit nicht jede Untersuchung eine neue Analyse-VM erfordert, lohnt es sich, ein Image der erstellten Analyse-VM in der Azure Compute Gallery oder als Amazon Machine Image (AMI) zu hinterlegen.

Fazit

Wenn ein Unternehmen Infrastruktur in der Cloud betreibt, sollte es sich auf Sicherheitsvorfälle vorbereiten, denn der Angriff auf Cloud-Ressourcen ist heutzutage keine Seltenheit. Zentrale Punkte für eine erfolgreiche Notfallvorsorge sind die Definition einer Analysestrategie (in Cloud oder lokal), eine Übersicht der Konfiguration und der genutzten Dienste und das Sammeln aller benötigten Logdateien. Für letztere muss man je nach Dienst möglicherweise Optionen dazubuchen.

Während der Analyse eines Cloud-Sicherheitsvorfalls benötigt man Sichtbarkeit auf die relevanten Cloud-Bereiche, sodass keine Spuren des Angriffs übersehen werden. Ausgehend von als kompromittiert identifizierten Benutzern oder Ressourcen kann das Ausmaß des Vorfalls bestimmt werden, indem man die mit der Entität verknüpften Rollen und Rechte unter die Lupe nimmt. (pst@ix.de)

Quellen

[1] Frank Ully; Ins Netz gegangen – Angriffe auf das Azure Active Directory und auf Azure-Dienste; iX 4/2022, S. 50
[2] Tabea Nordieker; Angriffe auf Microsoft 365 aufspüren; iX 11/2023, S. 82
[3] Christoph Puppe; Organisationen in der Cloud; iX 9/2022, S. 110
[4] Frank Ully; Überprüfung von Cloud-Umgebungen; iX 1/2024, S. 130
[5] Fabian Murer; Forensik und Logging im Azure AD; iX 6/2022, S. 112
[6] Links und weiterführende Quellen stehen unter ix.de/z5jk

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.