"T.I.S.P. Community Meeting 2020"

Berlin, 03.-04.11.2020

Penetration Testing und Incident Response in der Cloud

Inés Atug, HiSolutions AG

$Whoami

Name:
Inés Atug

Position:
Senior Expert

E-Mail:
atug@hisolutions.com

Fachliche Schwerpunkt

- Beratung zu Cloud-Security
- Beratung zu Informationssicherheit nach ISO 27001 und IT-Grundschutz
- Durchführung von Analysen im Security- und Risikomanagement
- Beratung zu KRITIS / Durchführung KRITIS Prüfungen

Zertifikate

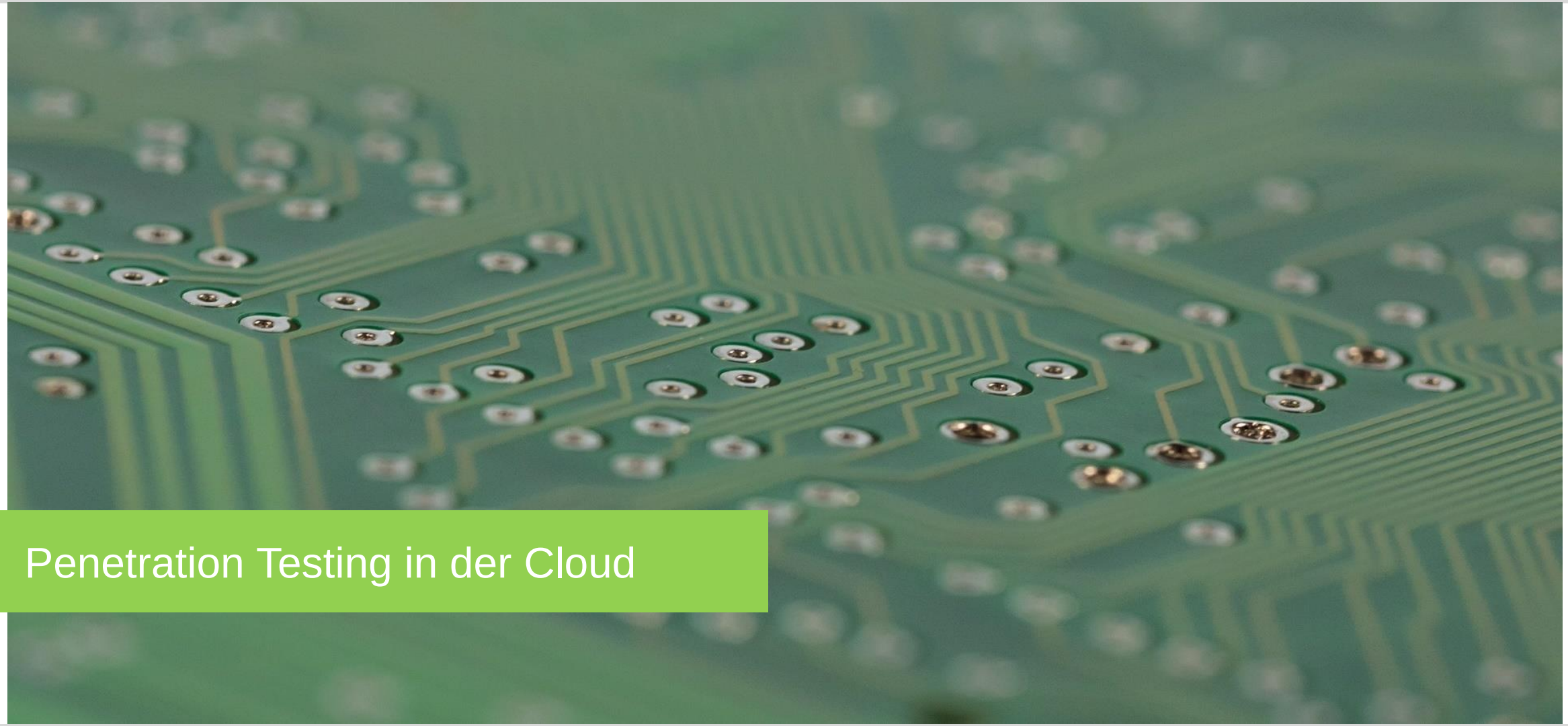
- GPEN (GIAC Penetration Tester)
- IT-Grundschutz Praktiker
- Datenschutzbeauftragte (TÜV)
- PRINCE2® Foundation
- Spezielle Prüfverfahrens-Kompetenz für § 8a BSIG

Publikationen (Auswahl)

- Ebenen der Vertraulichkeit in der Cloud, kes 2/2020
- Schlüsselmanagement in der Cloud, kes 1/2020
- Detektion und Reaktion in der Cloud, kes 2/2019
- IT-Grundschutz Konformität in Office 365 innerhalb der Microsoft Cloud Deutschland, Microsoft 12/2017
- IT-Grundschutz Konformität in Dynamics 365 innerhalb der Microsoft Cloud Deutschland, Microsoft 12/2017

Ausbildung / Studium

- MSc in Applied IT Security
- Postgraduate Certificate in Mathematics
- BSc (hons) Mathematics
- Bankkauffrau (IHK)



Penetration Testing in der Cloud

Webseite lässt Kunden Kryptocoins schürfen

- Im Februar 2018 wurde bekannt, dass die Webseite der LA Times seit fast einem Monat einen schadhaften Code implementiert hatte, der mittels der Rechenressourcen der Kunden, die diese Webseite aufrufen, Kryptocoins schürfte.

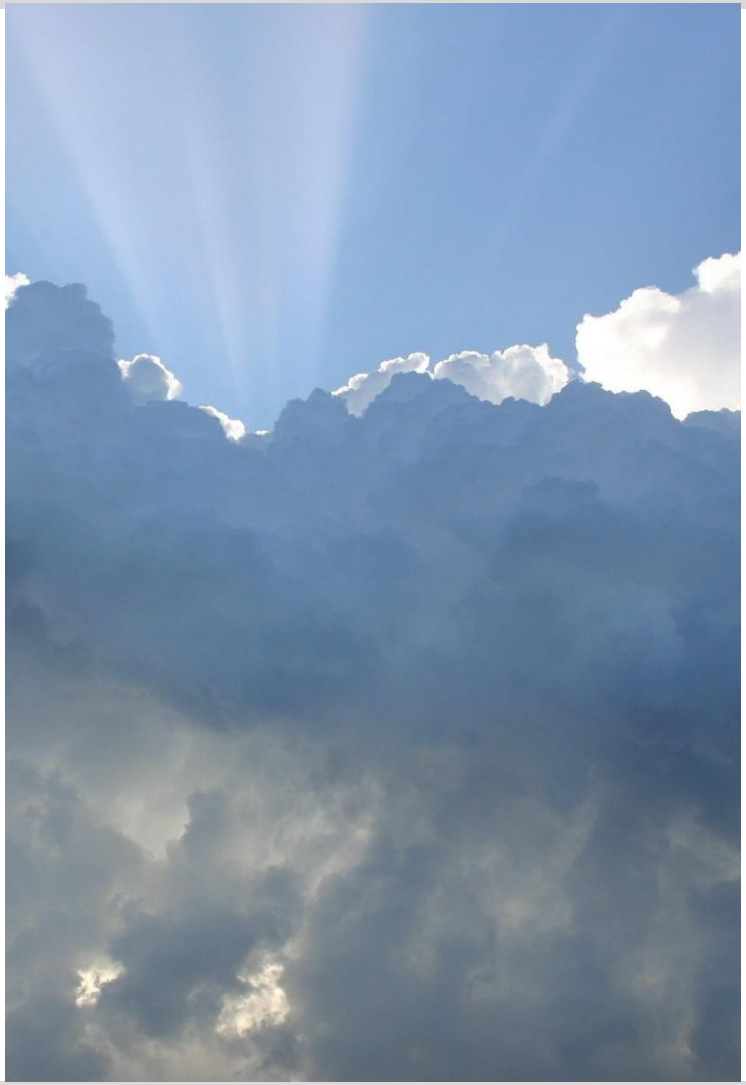
- **Ursache:**
  - S3 Bucket erlaubte lesenden und schreibenden Zugriff
  - Die Angreifer platzierten ein JavaScript im Programmcode einer dort abgelegten interaktiven Karte

- **Folgen / Auswirkungen:**
  - Nicht bekannt

Was ist Cloud aus der Sicht eines Pentester?

- „It‘s all the same, but different“
  - Das Vorgehen ändert sich nicht, aber die Methoden: Interne Informationssammlung mittels externer Methoden: APIs und CLI Werkzeuge
  - Die Cloud-Dienste unterscheiden sich in den Eigenschaften; z.B. auf Lambda kann nicht öffentlich zugegriffen werden ohne API Gateway, während Google Functions öffentlich sind und nicht hinter eine Firewall gebracht werden können.

- Es gibt drei verschiedene Ebenen für die Penetration Tests
  - „Auf der Cloud-Umgebung“:
    - Pentesting von virtuellen Systemen („Lift and Shift“)
    - Pentesting von Webanwendungen (ohne die darunterliegende Infrastruktur)
  - „In der Cloud-Umgebung“:
    - Pentesting der internen Konfiguration, z.B. des PaaS-Dienstes oder des SDN
  - „Absicherung der Cloud-Umgebung“:
    - Überprüfung der Berechtigungen und anderen Einstellungen



Modell der geteilten Verantwortung

- Die Sicherheit von Daten und Anwendungen, die in der Cloud verarbeitet werden, liegt in der Verantwortung des Cloud-Kunden und des Cloud-Anbieters.

- Der Cloud-Anbieter trägt die Verantwortung für die „Sicherheit der Cloud selbst“, d.h. die Cloud-Infrastruktur. Dies umfasst den Schutz von Hardware, Software, Netzwerk und den Betrieb von Cloud-Diensten.

- Der Cloud-Kunde trägt die Verantwortung für die „Sicherheit in der Cloud“, d.h. Dienstkonfiguration und –verwaltung, Verwaltung der Gastbetriebssysteme von virtuellen Maschinen etc.

Penetrationstests auf Software-as-a-Service

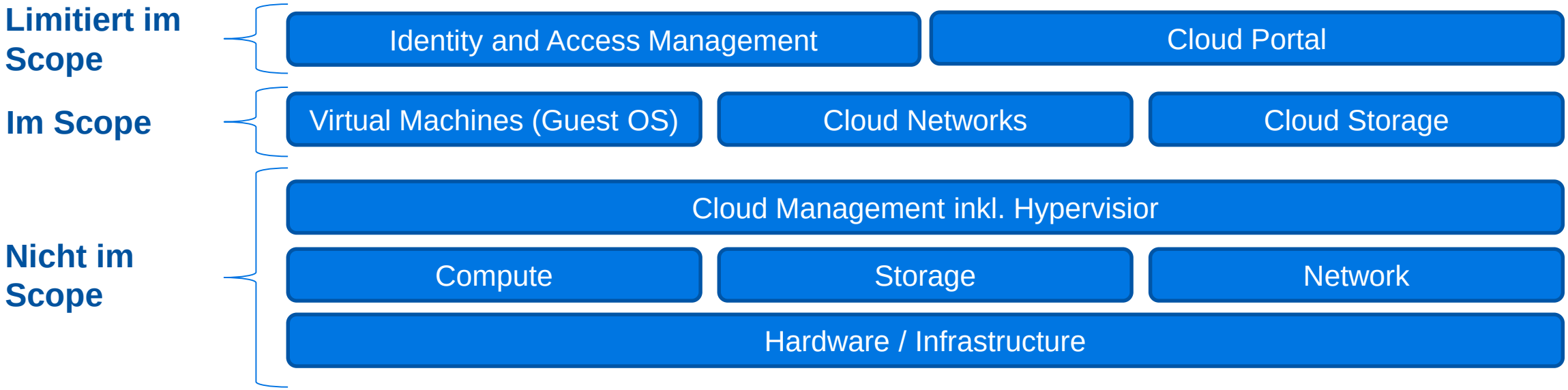
- Penetrationstests in Software as a Service sind restriktiv.
- Ziel des Angreifers:
  - Administratorkonto und/oder Benutzerkonto
    - Zugriff auf Daten
    - Zugriff auf Funktionen (z.B. E-Mail)
  - Datenabgriff

Penetrationstests auf Platform-as-a-Service

- Platform as a Service bietet Anwendungen, um die Anwendungsentwicklung zu erleichtern.
- Penetrationstests fokussieren sich auf die Anwendung
  - Kunden-Container sind im Scope
  - Host oder andere Container sind nicht im Scope
    → Container Escape sind nicht im Penetrationstest-Scope

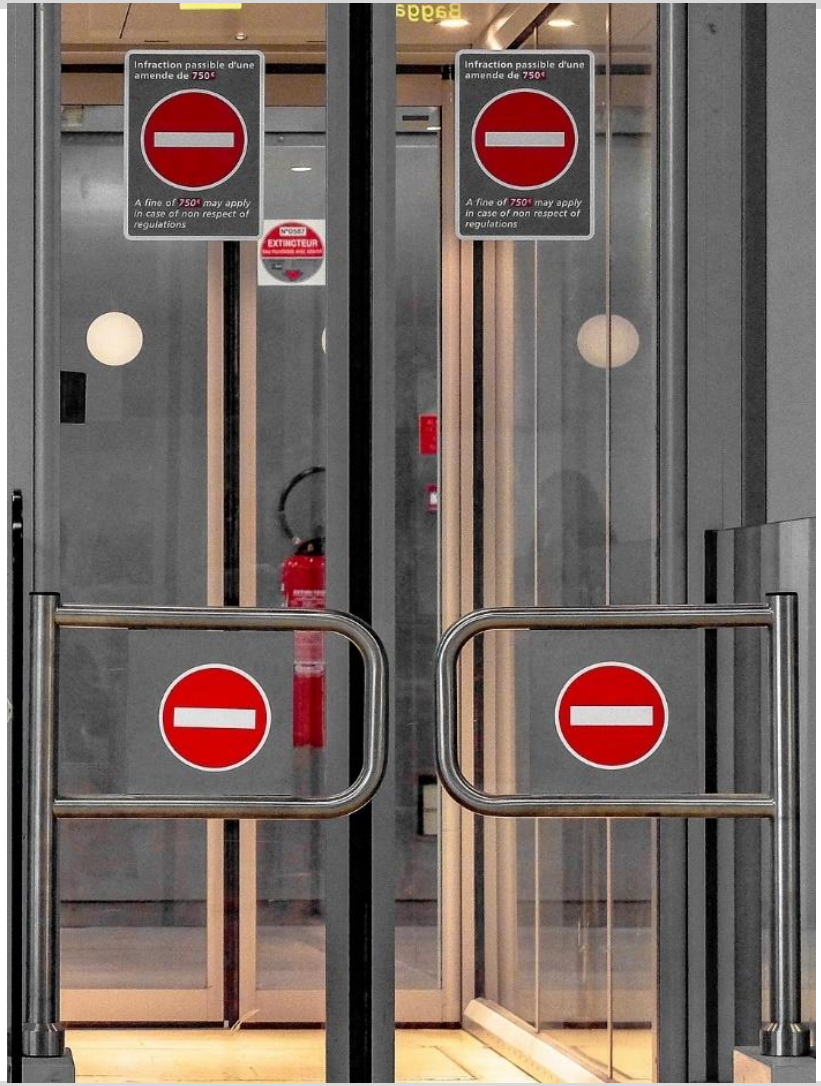
Penetrationstests auf Infrastructure-as-a-Service

- Penetrationstests in Infrastructure as a Service sind am wenigsten restriktiv.
- Es darf alles oberhalb der Virtualisierung getestet werden.



Was ist erlaubt? Was nicht?

- AWS:
  - https://aws.amazon.com/de/security/penetration-testing/
  - Es gibt Dienste, deren Test ist **prinzipiell erlaubt**, z.B. Amazon EC2 Instances, NAT Gateways und Elastic Load Balancers, Amazon RDS, Amazon CloudFront, Amazon Aurora …
  - Es gibt **verbotene Aktivitäten**, z.B. DNS Zone Walking über gehostete Amazon Route 53-Zonen, (D)DoS, Port-Flodding etc.
- Azure:
  - https://docs.microsoft.com/en-us/azure/security/fundamentals/pen-testing
  - https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement?rtc=1
  - Auch wenn keine Voranmeldung mehr notwendig ist, verpflichtet sich der Kunde darauf die Pentest-Regeln (Rules of Engagement) von Microsoft einzuhalten.
  - Es sind Tests, die andere Cloud-Kunden betreffen können, Zugriff auf fremde Daten und (D)DoS verboten



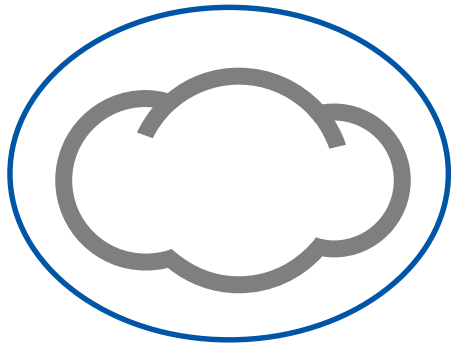
Entwickler lädt AWS Schlüssel auf GitHub hoch

- Im September 2014 hat ein Wordpress Entwickler versehentlich seinen AWS Zugangsschlüssel in GitHub abgespeichert.

- **Ursache:**
  AWS Zugangsdaten waren in einer Backupdaten enthalten gewesen.

- **Folgen / Auswirkungen:**
  - Der AWS Schlüssel war erst 5 Minuten auf GitHub und schon konnte ein Bot sie finden und 140 Server für Kryptomining starten.
  - Die neuen Instanzen waren schwer zu finden und erst mit der Hilfe von AWS konnte das Konto bereinigt werden.

Das Vorgehen beim Cloud Pentest

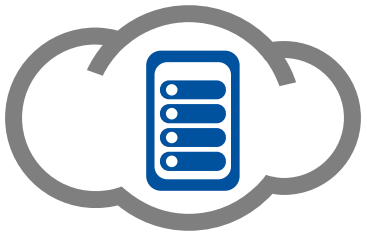


Absicherung der Cloud-Umgebung

- Konfig. Review
- Pentest

In der Cloud-Umgebung

- Konfig. Review
- Pentest



Auf der Cloud-Umgebung

- Konfig. Review
- Pentest

Angreifer schürfen Kryptocoins auf ungeschütztem AWS Account

- Im Januar 2018 wurde durch Sicherheitsforscher entdeckt, dass Teslas AWS Account zum Kryptocoins schürfen genutzt wurde.

- **Ursache:**
  Eine Kubernetes Konsole war offen zugängig und hierrüber konnten die Angreifer AWS Zugangsdaten auslesen und ihren Angriff ausweiten.

- **Folgen / Auswirkungen:**
  - Die Angreifer installierten eine Kryptomining-Software in Teslas AWS Account und nutzten Ressourcen, für die Tesla bezahlte.
  - Laut Tesla waren keine Kundendaten betroffen.

MILLIONENBEUTE

Hacker kapern Tesla-Cloud für Krypto-Mining

Hacker haben eine Sicherheitslücke bei Tesla ausgenutzt, um Krypto-Währung zu schürfen. Die Beute soll mehrere Millionen Dollar betragen.

Hauke Gierow

21.02.2018 - 13:26 Uhr • 2 Kommentare • 2 x geteilt

Welche Werkzeuge können unterstützen?

- Alt bekannte Werkzeuge, wie nmap, masscan, Burp, Metaspoit …
- Neue Werkzeuge wie:
  - LazyS3 – AWS S3 Buckets auffinden
  - MicroBurst – Tool-Sammlung für einen Azure Pentest
  - Pacu – Post Exploitation AWS Toolkit

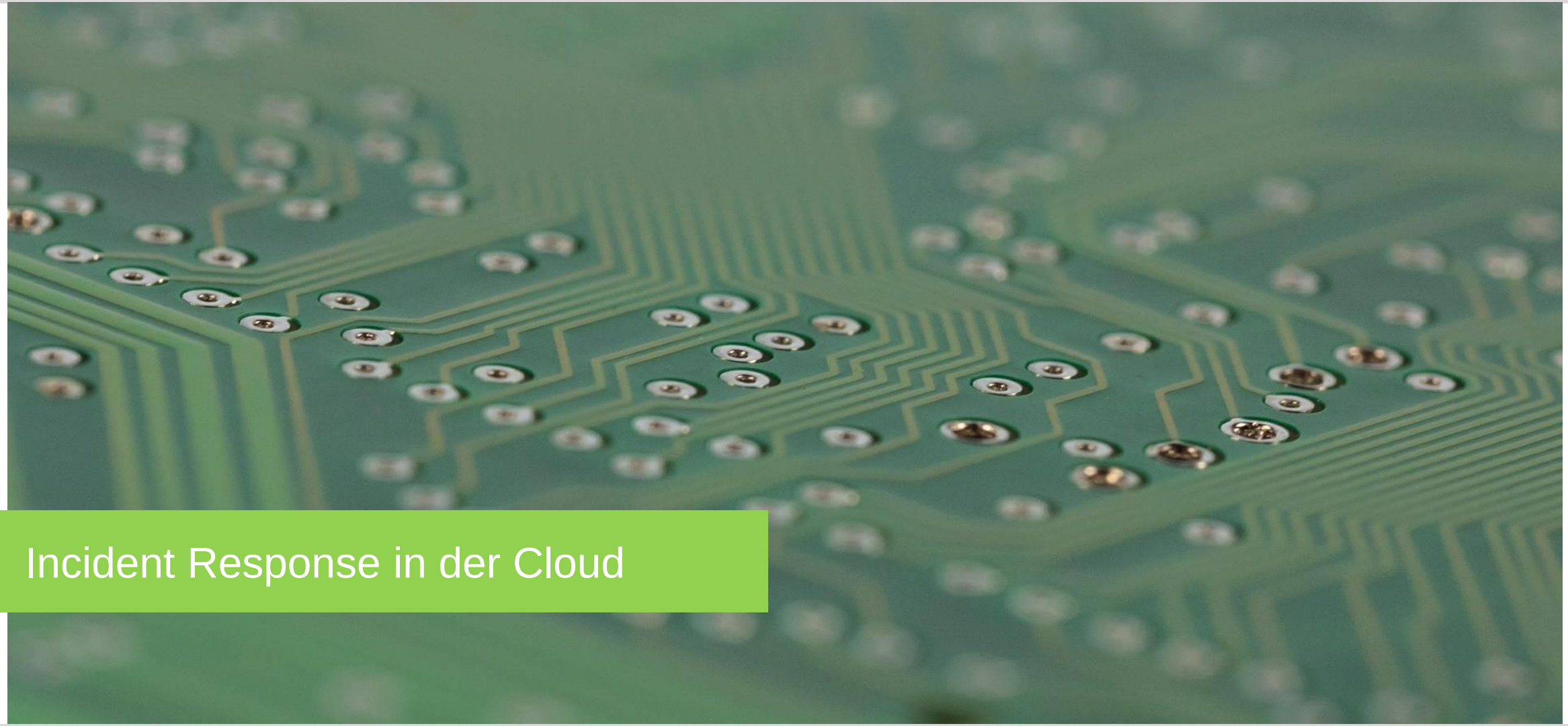
Weitergehende Quellen

- Übersicht AWS Werkzeuge
  https://github.com/toniblyx/my-arsenal-of-aws-security-tools
- Cloud Penetration Testing Playbook, 2019-12-07
  https://cloudsecurityalliance.org/artifacts/cloud-penetration-testing-playbook/

Fazit und Ausblick

„It‘s the same, but different“

Penetrationstests unterscheiden sich je nach Servicemodell, Betriebsmodell und Cloud Provider



Incident Response in der Cloud

Was ist Cloud aus der Sicht eines Incident Responder?

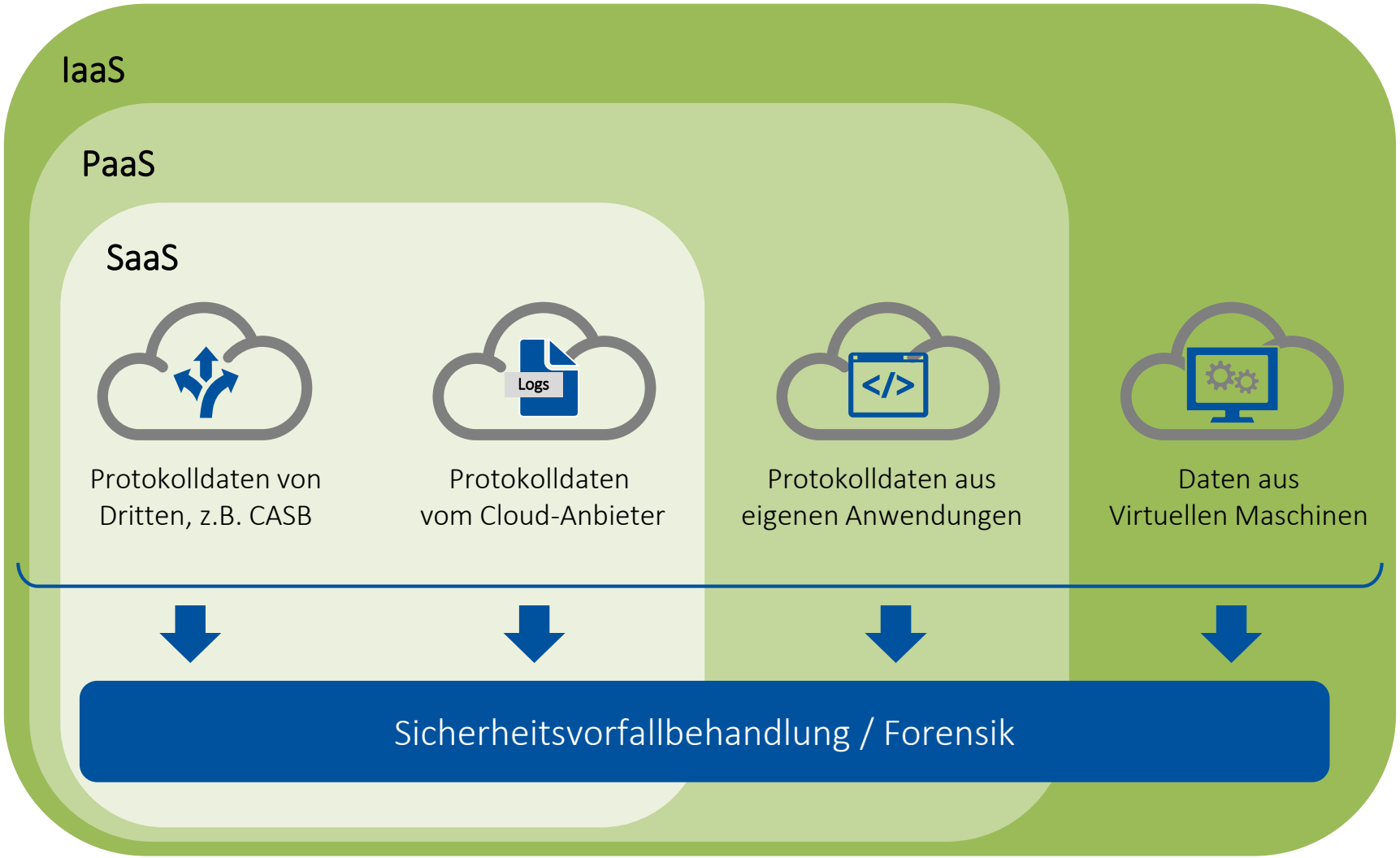
Sofern IR nicht mit einbezogen wurde:

Schwarzes Loch

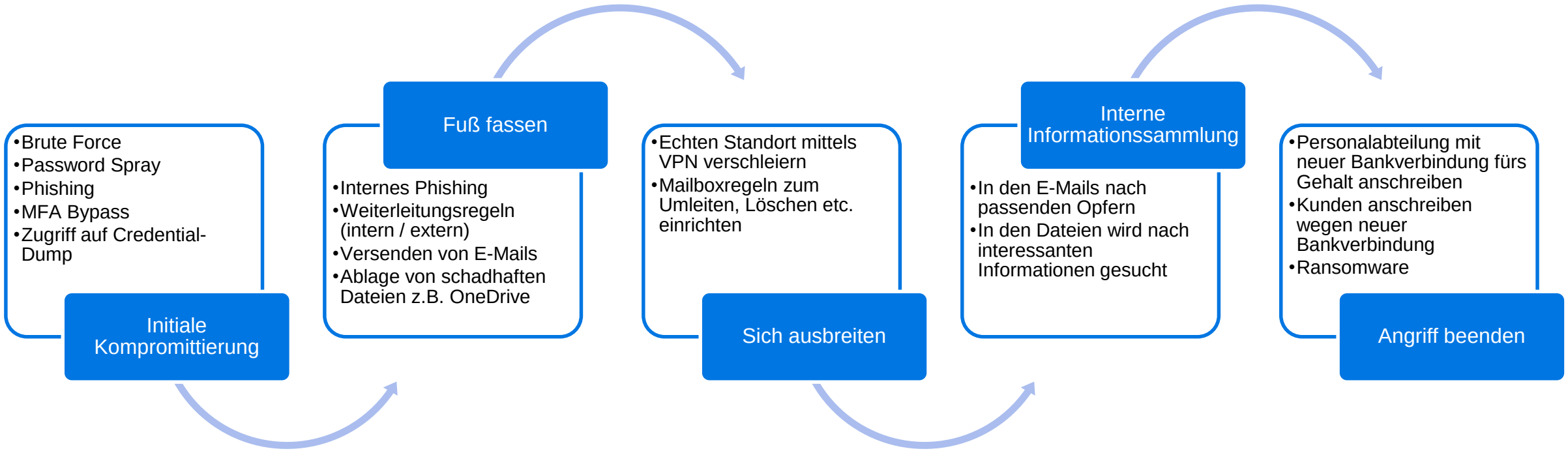
Vorbereitung Incident Response

- Es sollten Kommunikationswege vom und zum Cloud-Anbieter definiert sein.
- Es sollten Benutzerkennungen angelegt werden, die im Falle eines Sicherheitsvorfalls verwendet werden können. Hierbei ist darauf zu achten, dass diese Benutzer nur die benötigten Berechtigungen beinhalten und nicht für das tägliche Arbeiten verwendet werden.
- Das Incident Response Team muss die Informationsquellen kennen.
- Für IaaS / PaaS könnte das Einrichten einer Sicherheitsvorfall-Umgebung sinnvoll sein.

Woher können Informationen kommen?



Office 365 – Mögliche Angriffsmethoden



Ablauf des OAuth-Angriffs

Angreifer erstellt eine App und registriert die App beim Cloud-Provider

From: no-reply@sharepointonline.com
Sent: Friday, September 25, 2020 7:48:02 AM
To: Undisclosed repipients;;
Subject: WICHTIG – Einschnitte im Budget Q4/…

Budget report attached.

Budget report Q4-2020.xlsx

Angreifer erstellt eine Phishing Mail mit einem Link über den die App Berechtigungen gewährt bekommt

From: no-reply@sharepointonline.com
Sent: Friday, September 25, 2020 7:48:02 AM
To: Undisclosed repipients;;
Subject: WICHTIG – Einschnitte im Budget Q4/…

Budget report attached.

Budget report Q4-2020.xlsx

Empfänger klickt auf den Link, und authentifiziert sich am Cloud-Dienst

Permissions required

Budgetmanagement O365

This app would like to:

- Read your mail
- Read and write your mailbox settings

Empfänger wird gebeten Berechtigungen an die App zu übergeben und bestätigt diese

Angreifer hat Zugriff auf die Cloud-Umgebung entsprechend der freigegebenen Berechtigungen

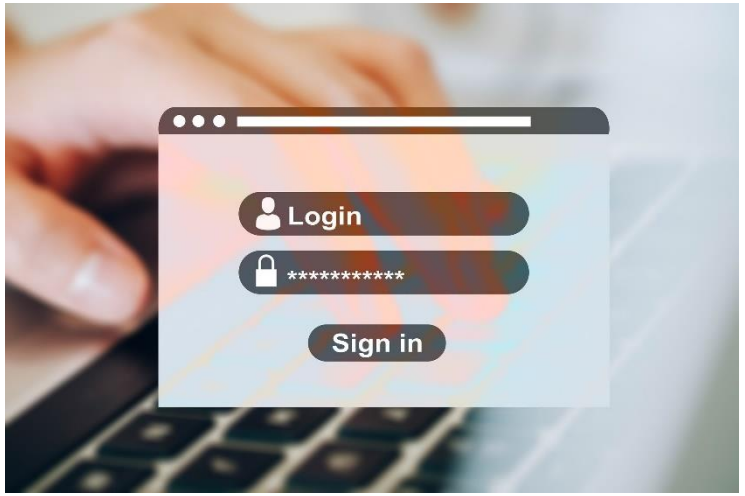
Office 365 – Benötigte Rollen

- Bevor die Untersuchung eines Office 365-Vorfalls möglich ist, sollte ein „Incident Response“-Konto eingerichtet werden. Dieses sollte mindestens mit folgenden Rollen ausgestattet sein:

Exchange Admin Roles
- View-only audit logs
- View-only configuration
- View-only recipients
- Mailbox Search
- Message Tracking

eDiscovery Rights
- eDiscovery Manager role

Azure Active Directory Roles
- Global Reader



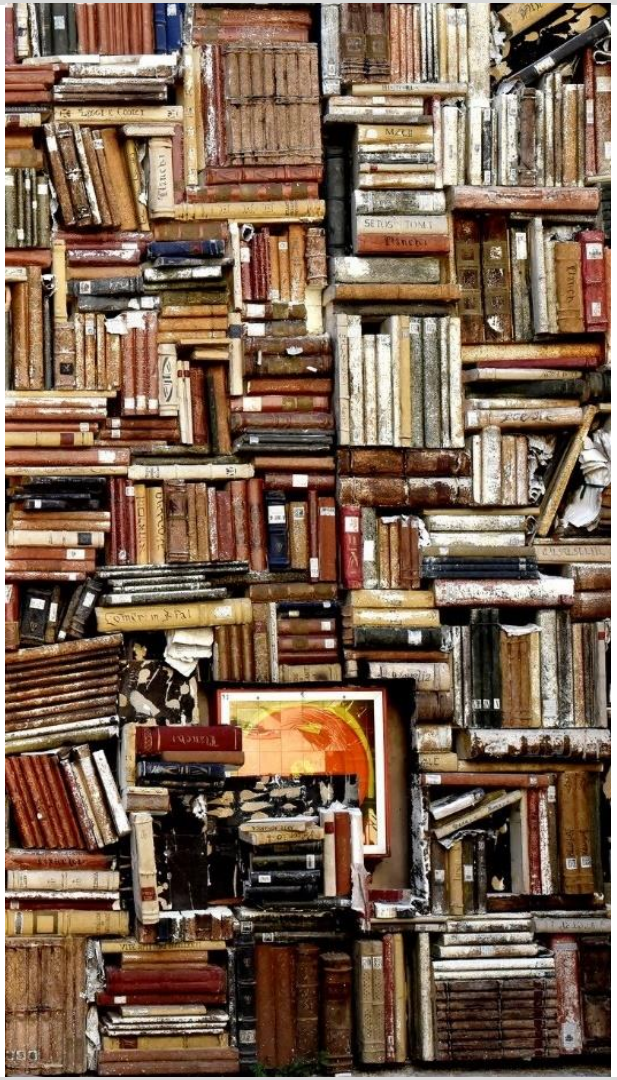
- Es kann sein, dass die Rollen innerhalb eines Incident Response-Falls dann angepasst werden müssen.

Office 365 – Welche Protokolle gibt es?

Protokollname	Portal	PowerShell cmdlet	Limits
Unified Audit Log (UAL)	protection.office.com	Search-UnifiedAuditLog	- Anfrage auf 5.000 Ergebnisse limitiert - Nur 90 Tage aufbewahrt - Bis 24 Std. bis auffindbar
Mailbox Audit Log (MAL)		Search-MailboxAuditLog (eine bestimmte Mailbox)	- Nur 90 Tage aufbewahrt
Administrator Audit Log		Search-AdminAuditLog	- Nur 90 Tage aufbewahrt - Audit Log Search muss aktiviert sein
Azure AD Logs	portal.azure.com	Get-AzureADAudit DirectoryLogs Get-AzureADAudit SignInLogs	- Nur 30 Tage aufbewahrt

Weitere interessante Office 365 Quellen

- Cloud App Security Portal
  - Überprüfen / Verhindern von Oauth-Angriffen
  - E5 Lizenz notwendig
- Message Traces
  - Protokolliert die E-Mails, die von einem Benutzer gesendet und empfangen werden.
  - Mail Flow Informationen beinhalten: subject lines, original client IP addresses, and message sizes.
  - Letzte Tage mittels PowerShell cmdlet: Get-MessageTrace
  - Bis zu 90 Tage mittels PowerShell cmdlet: Get-HistoricalSearch
  - Berichte in Security and Compliance Center erstellbar
- eDiscovery Content Searches
  - Suchergebnisse abhängig davon was indiziert wurde.
  - Nur die aktuellen 1.000 Suchergebnisse werden angezeigt.
  - Kann verwendet werden, um E-Mails von Angreifern zu finden.



Office 365 – Mögliches Vorgehen

Suche nach auffälligen Aktivitäten
- Unified Audit Logs
- Azure AD Logs

Anschließend auf die Benutzer konzentrieren, die als involviert erkannt wurden.
- Unified Audit Log
- Mailbox Audit Log
- Azure AD Logs
- Admin Audit Logs

Aufgrund aufgefundener IP-Adressen wird versucht andere kompromittierte Benutzer zu finden.
- Unified Audit Log

Ausgehende E-Mails analysieren. Bei Phishing auch eingehende E-Mails.
- Message Traces

Vom Angreifer verwendete Domains erkennen
- Content Searches

Weitergehende Quellen

- ENISA, Exploring Cloud Incidents, 2016-06-01
  https://www.enisa.europa.eu/publications/exploring-cloud-incidents
- CSA, Cloud Incident Response Framework – A Quick Guide, 2020-04-21
  https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework-a-quick-guide/

Fazit und Ausblick

„It‘s the same, but different“ – neue und alte Angriffe

Jede Cloud-Umgebung ist anders!

Vorbereitung und Einarbeitung in die eigene Cloud-Umgebung spart Zeit

Vielen Dank für Ihre Aufmerksamkeit!

Gibt es Fragen?