VECTRA
SECURITY THAT THINKS

WHITE PAPER

Bedrohungserkennung und Response in Cloud-Umgebungen

INHALTSVERZEICHNIS

Vectra® protects business by detecting and stopping cyberattacks.

As a leader in network detection and response (NDR), Vectra® AI protects your data, systems and infrastructure. Vectra AI enables your SOC team to quickly discover and respond to would-be attackers —before they act.

Vectra AI rapidly identifies suspicious behavior and activity on your extended network, whether on-premises or in the cloud. Vectra will find it, flag it, and alert security personnel so they can respond immediately.

Vectra AI is *Security that thinks®*. It uses artificial intelligence to improve detection and response over time, eliminating false positives so you can focus on real threats.

Preventing a compromise is increasingly difficult but detecting the behaviors that occur – from command and control to data exfiltration – is not.

HIGHLIGHTS

- Attackers have two avenues of attack to compromise cloud resources; accessing systems inside the enterprise network perimeter, or by compromising credentials from an administrator account that has remote administrative capabilities or has CSP administrative access.
- According to a survey conducted by the Cloud Security Alliance, top concerns were related to managing credentials and methods of compromising those credentials to gain access to cloud environments for malicious intent.
- In the APT10 Operation Cloud Hopper attack, the method of initial intrusion and the attack behaviors within those cloud environments were the same behaviors found in private cloud and physical data centers.
- Properly assigning user access rights and managing the use of API tokens help reduce instances of shared credentials so cloud tenants can focus on how those credentials are used.
- When visibility is available in the cloud infrastructure, it is much easier to detect attacker behaviors in compromised systems and services that are clearly operating outside of expected specifications.

Unterschiede zur Erkennung von Bedrohungen in herkömmlichen Umgebungen

Cloud-Umgebungen ändern fundamentale Annahmen dazu, wie Bedrohungserkennung und Response funktionieren muss.

Da Cloud-Workloads äußerst dynamisch sind und innerhalb von Sekunden aktiviert und deaktiviert werden können, sind sie grundsätzlich unsicher. Wenn es während der Aufbauphase zu Systemkonfigurationsfehlern kommt, können sich diese Fehler verschärfen bzw. verstärken, sobald sie per Automatisierung für viele Workloads repliziert werden. Die mit dem Cloud Service Provider (CSP) geteilte Verantwortung führt zu potenziellen Lücken in der Bedrohungserkennung innerhalb des Angriffsablaufs. Der Trend in der Cloud geht in Richtung Datenzugriff per API, sodass herkömmliche Ansätze zur Überwachung von Traffic nicht mehr wirksam sind.

Zu den Herausforderungen bei der Bedrohungserkennung und Response kommt erschwerend hinzu, dass Unternehmen mit dem Innovationstempo in der Cloud nicht Schritt halten können. Gleichzeitig konzentrieren sich Unternehmen durch den wachsenden Wettbewerbsdruck stärker auf die Bereitstellung von Funktionen und lagern nicht grundlegende Funktionen des Geschäftsmodells aus – häufig auf Kosten der IT-Sicherheit.

Aufgrund der rasanten Zunahme bei Cloud-Services ist das Konzept eines Perimeters hinfällig, sodass Perimeter-Kontrollen ins Leere laufen. Eine Zunahme bei neuer Infrastruktur und Bereitstellungstools ermöglicht neue Umgebungen mit neuen Sicherheitsmodellen – und neuen Angriffsflächen.

> An explosion of cloud services means the concept of a perimeter is gone and using perimeter controls becomes futile.

Die von CSPs angebotenen Tools sind komplex und für einige Unternehmensmandanten immer noch neu, was zu versehentlichen Fehlkonfigurationen führen kann. Und schließlich wird der bestehende Fachkräftemangel in der IT-Sicherheit durch die vielen neuen Funktionen und Services weiter verschärft.

Am schwerwiegendsten ist dabei die Einführung zahlreicher neuer Zugriffs- und Verwaltungsfunktionen, die die Variabilität deutlich erhöhen und erhebliche Risiken für Cloud-Bereitstellungen mit sich bringen. Es ist schwierig, Administratoraktionen zu verwalten, zu überwachen und zu überprüfen, wenn diese Anwender von innerhalb oder außerhalb der Unternehmensumgebung auf Cloud- Ressourcen zugreifen können.

Ohne eine durchdachte Strategie zur Rechteverwaltung, die strikt getrennte Rollen für den Administratorzugriff ausschließlich von zulässigen Stellen erlaubt, können die entsprechenden Anmeldedaten und Berechtigungen in Unternehmen missbraucht werden.

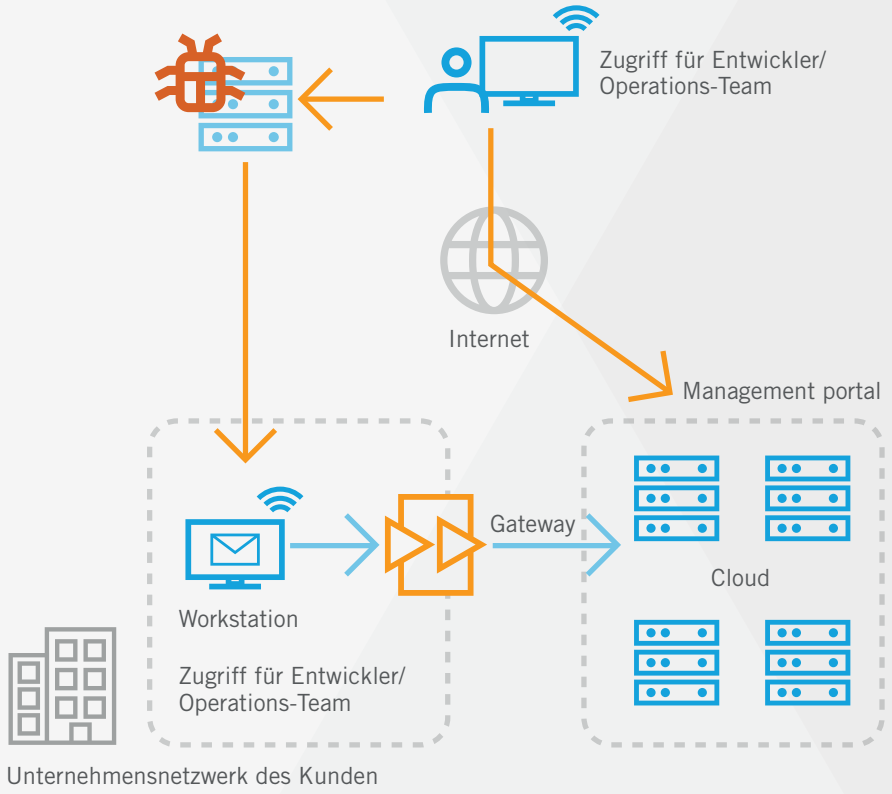
Bislang erforderte der Zugriff auf einen Server die Authentifizierung beim Perimeter, und die Überwachung (und Verfolgung) des Administratorzugriffs konnte im privaten Netzwerk implementiert werden. Der Zugriff auf die Cloud-Management-Systeme erfolgt jedoch per Weboberfläche oder API über das öffentliche Internet. Ohne angemessenen Schutz könnte der Unternehmensmandant damit seine „Schätze“ – seine wichtigsten Informationen – angreifbar machen.

Angriffsablauf in der Cloud

Für die Kompromittierung von Cloud-Ressourcen stehen Angreifern zwei wichtige Einfallstore zur Verfügung. Das erste nutzt herkömmliche Methoden, wozu auch der Zugriff auf Systeme innerhalb des Netzwerk-Perimeters des Unternehmens gehört. Anschließend folgen Reconnaissance und Rechteerweiterung für ein Administratorkonto, das Zugriff auf Cloud-Ressourcen hat.

Die zweite Variante verkürzt den Prozess und kompromittiert direkt die Anmeldedaten eines Administratorkontos, das Verwaltungsberechtigungen oder CSP-Administratorzugriff besitzt.

Diese Variabilität bei Administratorzugriffsmodellen bedeutet, dass sich die Angriffsfläche bei neuen Sicherheitsbedrohungen ändert, da der Zugriff über unregulierte Endgeräte zur Verwaltung von Cloud-Services erfolgt. Nicht verwaltete Geräte, die für die Entwicklung und Verwaltung der Infrastruktur genutzt werden, gefährden Unternehmen durch Bedrohungsvektoren wie Webnutzung und E-Mails.



Attackers have two avenues of attack to compromise cloud resources.

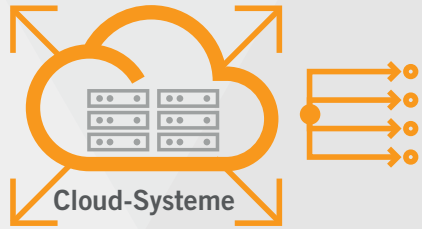
Cyberattack Lifecycle

NETZWERK

Initiale Infektion
Command & Control
Internal Reconnaissance
Lateral Movement
Exfiltration von Daten

Cloud

Diebstahl der Domain-Admin-Anmeldedaten
Zugriff auf das Steuerungskonto des Cloud Providers
Erkundung des Netzwerks
Freie Bewegung im Netzwerk
Ausführung beliebiger Aktivitäten



Sobald Angreifer die Kontrolle über das Konto erlangt haben, können sie z. B. neue Konten erstellen.

Wenn das Administrator-Hauptkonto kompromittiert ist, muss der Angreifer keine Berechtigungen mehr eskalieren oder den Zugriff auf das Unternehmensnetzwerk aufrechterhalten, da das Administratorkonto all diese Möglichkeiten bietet – und viele weitere mehr. Wie können Unternehmen durch ausreichende Überwachung den Missbrauch von CSP-Administratorrechten verhindern?

Dazu müssen Unternehmen überprüfen, wie die Systemadministration und Eigentümerschaft des Cloud-Kontos geregelt sind.

1. Wie viele Personen verwalten das Hauptkonto?
2. Wie sind Kennwörter und Authentifizierungen implementiert?
3. Wer überprüft die Sicherheit dieses wichtigen Kontos?

Wer übernimmt die Verantwortung, wenn ein Sicherheitsproblem auftritt – der CSP oder das Cloud-Mandanten-Unternehmen? Auch wenn dies vom jeweiligen Kontext abhängig zu sein scheint, möchten einige CSPs diese Verantwortung zum Mandantenunternehmen schieben.

Die wichtigste Frage ist jedoch: Wie kontrolliert ein Unternehmen das Vorhandensein und den Missbrauch von Administratoranmeldedaten? Es liegt in der Verantwortung des Mandanten, das Administratorkonto abzusichern.

Die CSPs kommunizieren sehr deutlich, wie wichtig das ist und dass es die Aufgabe des Mandanten ist. Zudem weisen sie nachdrücklich auf die Folgen von schwachem oder fehlendem Schutz hin. Wenn Cloud-Mandanten-Unternehmen der Überblick über die Backend-Management-Infrastruktur beim CSP fehlt, müssen sie den Missbrauch des CSP-Zugriffs auf ihre eigenen Umgebungen erkennen können.

Wichtigste Cloud-Sicherheitsbedrohungen

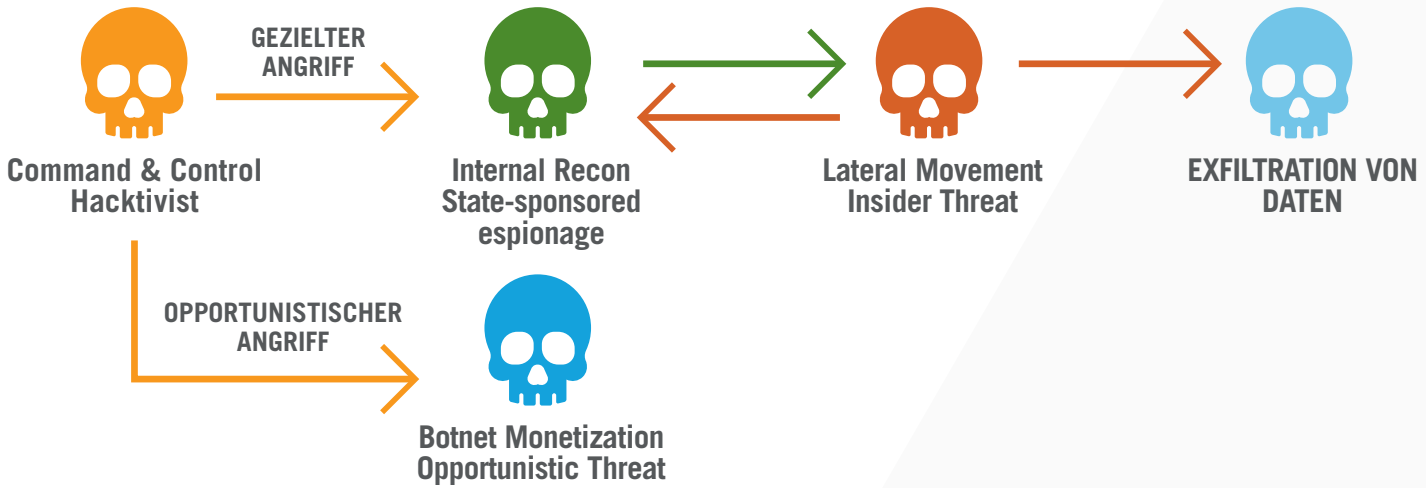
Im Jahr 2017 führte die Cloud Security Alliance (CSA) eine Umfrage durch, um Expertenmeinungen zu den – nach damaliger Ansicht – schwerwiegendsten Sicherheitsproblemen im Cloud Computing zusammenzutragen.

Von den 12 genannten Sorgen bezogen sich fünf auf die Verwaltung von Anmeldedaten sowie auf die Methoden, mit denen diese Daten kompromittiert werden, um böswillige Zugriffe auf Cloud-Umgebungen zu ermöglichen. Diese fünf Probleme wurden genannt (gewichtet nach Schweregrad in der Umfrage):

1. **Unzureichende Verwaltung von Identität, Anmeldedaten und Zugriff:** Keine skalierbaren Systeme zur identitätsbasierten Zugriffsverwaltung, fehlende Mehrfaktor-Authentifizierung, schwache Kennwörter, keine permanente Rotation kryptografischer Schlüssel, Kennwörter und Zertifikate.
2. **Unsichere Schnittstellen und APIs:** Von der Authentifizierung und Zugriffskontrolle bis zur Verschlüsselung und Aktivitätsverwaltung müssen diese Schnittstellen so konzipiert sein, dass sie versehentliche ebenso wie böswillige Versuche zur Richtlinienumgehung verhindern.
3. **Kontoübernahme:** Angreifer können Anwenderaktivitäten und Transaktionen belauschen, Daten manipulieren, gefälschte Informationen ausgeben und Ihre Kunden auf nicht legitime Websites weiterleiten.
4. **Böswillige Insider:** Ein aktueller oder ehemaliger Mitarbeiter, Auftragnehmer oder Geschäftspartner, der autorisierten Zugriff auf Netzwerk, Systeme oder Daten eines Unternehmens hat oder hatte und diesen Zugriff absichtlich erweitert oder missbraucht und so die Vertraulichkeit, Integrität oder Verfügbarkeit der Informationen bzw. Informationssysteme des Unternehmens beeinträchtigt.
5. **Unzureichende Einhaltung der Sorgfaltspflicht (Due Diligence):** Dies kann eine kaum übersehbare Lawine an wirtschaftlichen, finanziellen, technischen, juristischen und Compliancebezogenen Risiken für das Unternehmen nach sich ziehen, die den geschäftlichen Erfolg gefährden.

Analyse eines realen Cloud-Angriffs

Der APT10-Gruppe wurde die taktische Kampagne mit der Bezeichnung „Operation Cloud Hopper“ zugeschrieben, bei der weltweit eine Reihe dauerhafter Angriffe auf Managed CSPs und ihre Kunden durchgeführt wurden. Ziel dieser Angriffe war der Zugriff auf geistiges Eigentum und Kundendaten.



Das US-CERT wies darauf hin, dass Operation Cloud Hopper sich vor allem dadurch auszeichnete, dass die Angreifer nach dem Erlangen des Zugriffs auf einen Managed CSP dessen Cloud- Infrastruktur nutzten, um über das Netzwerk von einem Cloud- Mandanten zum nächsten zu springen (engl. „to hop“). Dabei gelangten die Angreifer an vertrauliche Daten verschiedenster Behörden und Unternehmen in Gesundheitswesen, Fertigung, Finanzsektor und Biotechnologie in mindestens einem Dutzend Ländern.

Angriffsablauf von Cloud Hopper

In Operation Cloud Hopper griffen die Angreifer zunächst auf Phishing-E-Mails zurück, um Konten mit Administrator- Zugriffsrechten für Managed CSPs zu kompromittieren. Phishing-E-Mails sind die häufigste Infektionsmethode bei jeder Art von Angriff und bis heute die einfachste Möglichkeit, initialen Zugriff auf ein Netzwerk zu erlangen. Dabei nutzt der Angreifer eine Malware, die die notwendigen Anmeldedaten abgreift und den direkten Zugriff auf die interne Umgebung des Managed CSPs ermöglicht. Anschließend kann er die vom CSP verwalteten Workloads des Mandanten angreifen oder sich auf andere Weise in seine Infrastruktur einklinken.

Sobald der Zugriff auf die Management-Infrastruktur hergestellt ist, kann der Angreifer innerhalb der vom Kunden verwalteten Infrastruktur mit PowerShell verschiedene Befehlszeilen-Skripts starten. Diese dienen beispielsweise zur Durchführung von Reconnaissance und Erfassung von Informationen für Lateral Movement, um Zugriff auf weitere Systeme zu erlangen.

Die Angreifer nutzten die kompromittierten Anmeldedaten weiter aus, um Sicherheitsbegrenzungen zu überwinden und Cloud Service Provider als Einfallstor für den Zugriff auf Daten zahlreicher Unternehmen zu missbrauchen.

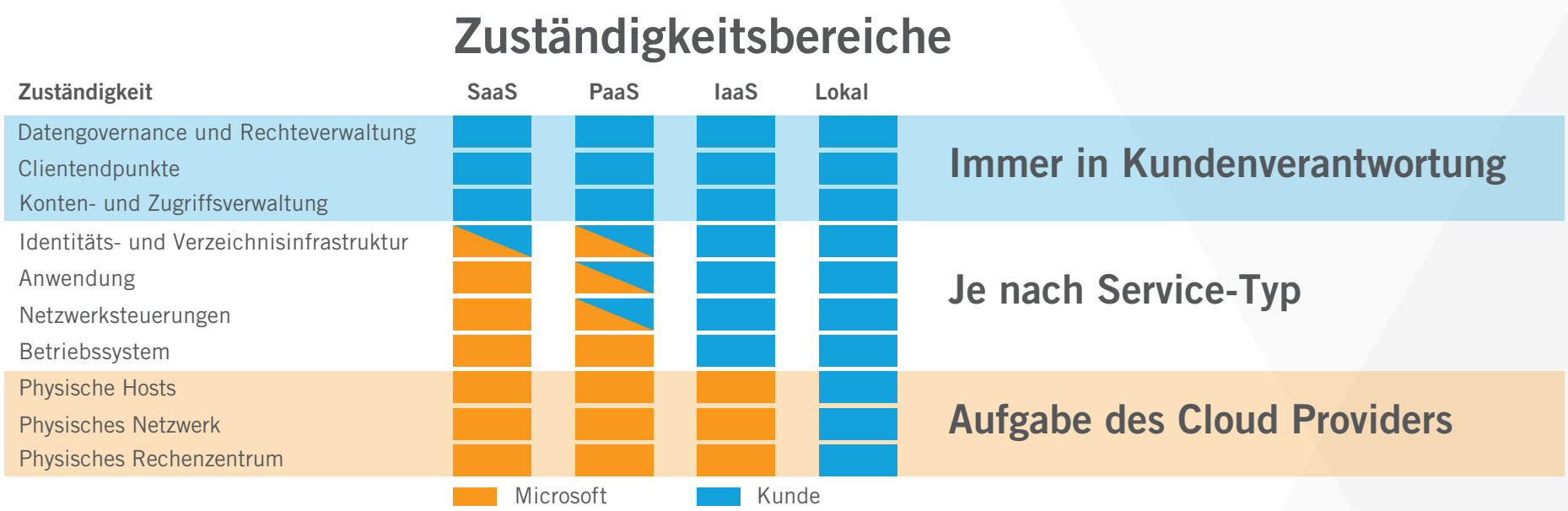
Damit der Zugang zur Cloud-Infrastruktur auch dann gewährleistet war, wenn das Administratorkonto nicht mehr funktionierte, installierten die Angreifer Remote-Zugriffstrojaner für Commandand-Control-Aktivitäten über Websites, die sich als legitime Domains ausgaben.

Zum Einsatz kam dabei standardmäßige Open-Source-Malware wie Poison Ivy und PlugX, die häufig für Angriffe verwendet werden. Viele der mittels Remote-Zugriff kompromittierten Systeme waren nicht geschäftskritisch, sodass das Lateral Movement ungestört erfolgen konnte und eine Entdeckung durch Systemadministratoren vermieden wurde.

Die letzte Stufe bei Operation Cloud Hopper war die Exfiltration von geistigem Eigentum. Diese Daten wurden zusammengetragen, komprimiert, aus der CSP-Infrastruktur exfiltriert und in eine von den Angreifern kontrollierte Infrastruktur übertragen.

Da CSPs in verwalteten Infrastrukturen einen Teil der Aufgaben von Mandanten übernehmen, verringert sich deren Kontrolle und Überblick entsprechend. APT10 profitierte davon und missbrauchte Anmeldedaten sowie Systeme, die sowohl auf CSPals auch auf Unternehmensinfrastrukturen zugreifen konnten.

Da Cloud-Mandanten keine Übersicht und Kontrolle über die eigentliche CSP-Infrastruktur haben, ist es für sie äußerst schwierig, Angreifer zu erkennen sowie zu überwachen, wenn diese zunächst ein System infizieren und dann innerhalb der CSP-Infrastruktur schnell zu einem anderen System wechseln.



Das Microsoft-Modell der gemeinsamen Verantwortung

Die Komplexität von Hybrid-Umgebungen mit CSPs und lokalen Systemen erschwert daher die Lösung von Problemen wie gestohlenen Anmeldedaten oder Lateral Movement von einem Cloud-Mandanten zu einem CSP und dann weiter zu einem zweiten Cloud-Mandanten. Ein sorgloser und unachtsamer Cloud-Mandant kann das Risiko für andere, wesentlich vorsichtigere Cloud-Mandanten erheblich erhöhen.

Modell der geteilten Verantwortung

Die Bedrohungserkennung und Response in Cloud-Umgebungen erfordert ein grundlegendes Verständnis des Modells der gemeinsamen Verantwortung sowie der Auswirkungen, die dieses Modell auf die Sicherheitsverwaltung und -überwachung hat.

Die Sicherheit von Cloud-Services ist eine gemeinschaftliche Arbeit und erfolgt in gemeinsamer Verantwortung von Cloud-Mandanten und dem CSP. Dabei ist der CSP für die Cloud-Plattform und die physische Sicherheit seiner Rechenzentren zuständig.

Die Mandanten sind Eigentümer ihrer Cloud-Daten und Identitäten, haben die Verantwortung für deren Schutz und müssen die Sicherheit lokaler Ressourcen sowie der von ihnen kontrollierten Cloud-Komponenten gewährleisten. CSPs stellen Sicherheitskontrollen und -funktionen bereit, um Daten und Anwendungen zu schützen, während die Verantwortung des Mandanten für die Sicherheit vom Cloud-Service-Typ abhängt.

Das Ausmaß und die Verteilung der Kontrolle auf CSP und Cloud-Mandanten variiert mit dem verwendeten Computing-Modell. Das Modell unten für Microsoft Azure verdeutlicht, wie die Verantwortung auf einer Cloud-Plattform verteilt ist.

Zu lokalen Bereitstellungen gehören Rechenzentren, die eine virtualisierte Infrastruktur des Unternehmens nutzen. In diesem Modell ist ein Unternehmen für sämtliche Sicherheitsbereiche von physischen Geräten bis hin zu Daten verantwortlich.

Ein Modell mit virtuellem Rechenzentrum als Infrastructure-asa-Service (IaaS) repliziert vorhandene interne Rechenzentren. In diesem Fall ist die physische Trennung von Hardware nicht möglich und erfordert Hypervisor-Funktionen, um Sicherheitszonen und Remote-Zugriff zu etablieren.

Wenn Unternehmen wählen müssen, ob sie ihre Infrastruktur in einer Private Cloud oder einer Public Cloud verwalten, setzen die meisten auf einen hybriden Ansatz – eine Kombination aus Private und Public Cloud mit gemeinsam genutzten Ressourcen und Distributionskomponenten. Normalerweise ist die kritische Backend-Infrastruktur als Private Cloud ausgeführt, während Zugriff und Distribution als Public Cloud erfolgt.

Sorgen in Bezug auf Sicherheit und Compliance stehen in virtualisierten Rechenzentren und Cloud-Bereitstellungen an erster Stelle. Sicherheitsanforderungen für virtualisierte Rechenzentren und Clouds schreiben die Möglichkeit zur Überwachung virtualisierter Umgebungen vor. Gleichzeitig müssen VM-Hostkapazität und Leistung höchsten Ansprüchen genügen. Zu den Techniken gehören statusbasierte Hypervisor-Firewalls, Netzwerkerkennung und virtualisierungsspezifischer Endgeräteschutz.

In einem Platform-as-a-Service-Modell (PaaS) werden Anwendungen auf vorhandenen ausgelagerten Plattformen installiert und verwaltet. Ein Server kann für exklusiven Zugriff bereitgestellt, aber auch für mehrere Anwendungen genutzt werden.

Da es keinerlei Kontrollen für die vorhandene Hardware gibt, ist es möglich, dass andere Anwender oder der Service Provider an vertrauliche Informationen gelangen. Deshalb müssen bei den Kontrollen für die Daten in den Anwendungen und Datenbanken Verschlüsselung und externe Schlüsselverwaltung implementiert werden, die für virtuelle Umgebungen konzipiert sind.

Bei Software-as-a-Service (SaaS) kommen Drittanbieter-Anwendungen wie Salesforce zum Einsatz, um einen bestimmten Service anzubieten. Daten werden im Backend des Anwendungsanbieters gespeichert, wobei dessen Zugriffskontrollen genutzt werden.

Unternehmensanwendungen unterstützen jetzt Active Directory mit ADFS und SAML zur Kommunikation. Zur Authentifizierung und Zugriffsverwaltung sowie Überwachung müssen Kontrollen bereitgestellt werden, damit gewährleistet ist, dass das Unternehmen die Kontrolle über die Nutzung dieser Anwendungen behält.

Security and compliance concerns are first-order priorities for virtualized data center and cloud deployments.

Fazit

Bei der APT10-Kampagne „Operation Cloud Hopper“ waren die initiale Eindringungsmethode und das Angriffsverhalten innerhalb dieser Cloud-Umgebungen die gleichen Verhaltensweisen, die für Private Clouds und physische Rechenzentren typisch sind.

Der Grund dafür ist, dass alle Angriffe, die auf Datenexfiltration abzielen, einem bestimmten Ablauf folgen müssen. Auch wenn es immer schwieriger wird, Kompromittierungen zu verhindern, lassen sich die dazu genutzten Methoden – von Command-and-Control-Aktivitäten bis hin zur Datenexfiltration – durchaus erkennen. Wichtiger ist jedoch: Wenn ein Angriff innerhalb von Stunden statt Tagen durchgeführt wird, ist die Erkennungsgeschwindigkeit ein kritischer Faktor.

Ein zentraler Punkt des Modells der gemeinsamen Verantwortung ist, dass unabhängig vom genutzten Rechenzentrumsmodell (IaaS, PaaS oder SaaS) das Mandantenunternehmen stets für Daten, Endgeräte, Konten und die Zugriffsverwaltung verantwortlich ist.

Zugriffsverwaltung

CSPs sind dafür verantwortlich, dass ihre eigenen Maßnahmen zur Zugriffsverwaltung und -kontrolle den Zugang zur Cloud- Mandantenumgebungen einschränken. Die Mandanten selbst müssen jedoch davon ausgehen, dass diese Maßnahmen kompromittiert werden können, und sich deshalb auf das Wer, Was, Wann und Wo der Zugriffsverwaltung konzentrieren.

Durch eine ordnungsgemäße Zuweisung von Anwenderzugriffsrechten und Verwaltung der API-Token-Nutzung kann die mehrfache Verwendung derselben Anmeldedaten weitgehend vermieden werden. Cloud-Mandanten können sich also auf die Frage konzentrieren, wie diese Anmeldedaten verwendet werden. Um Lateral Movement zwischen der CSP-Infrastruktur und Cloud- Mandanten zu verhindern, können außerdem Richtlinien für den Ressourcenzugriff implementiert werden.

For more information please contact a service representative at info@vectra.ai.

Erkennung und Response

Die Überwachung von lokalen Umgebungen und der Cloud muss gleichberechtigt erfolgen. Gleichzeitig ist zu klären, wie Daten und Kontext aus beiden Umgebungen korreliert werden, um verwertbare Informationen für Security-Analysten zu gewinnen.

Die Überwachung von Cloud-Ressourcen durch die Cloud- Mandanten ist unverzichtbar, weil auf diese Weise Lateral Movement von der CSP-Infrastruktur zu Mandantenumgebungen und umgekehrt entdeckt werden kann.

Durch die Koordination mit dem CSP – sowie die Koordination des CSP mit Cloud-Mandanten – wird eine umfangreiche Zusammenführung von Informationen ermöglicht, was die Chance einer Entdeckung von Post-Kompromittierungsaktivitäten steigert.

Der Überblick über das Angreiferverhalten ist abhängig von der Implementierung der richtigen Tools, die Cloud-spezifische Daten verarbeiten können.

Security operations

Die Kenntnis und Verwaltung der Infrastruktur im Rahmen der Sorgfaltspflicht sollte die Identifizierung von Systemen und Prozessen ermöglichen, die mit Malware-Implantaten wie bei Operation Cloud Hopper kompromittiert wurden.

Häufig ist es schwierig, Änderungen an Produktionssystemen zu entdecken. Doch wenn der Überblick über die Cloud-Infrastruktur vorhanden ist, lässt sich Angreiferverhalten in kompromittierten Systemen und Services, die klar außerhalb erwarteter Spezifikationen agieren, deutlich leichter aufdecken.

Im Idealfall verfügen die Security-Operations-Teams über handfeste Informationen über zulässige Abläufe in der konkreten Infrastruktur, sodass sich bei Abweichungen vom Normalzustand Malware und ihre Aktivitäten zuverlässiger erkennen lassen.

Email info@vectra.ai vectra.ai