VECTRA

Sechs wichtige Angriffsvektoren gegen Ihr Rechenzentrum und Ihre Private Cloud

Segmentierung allein genügt nicht

Die Sicherheit von Rechenzentren und virtualisierten Workloads folgt dem Konzept herkömmlicher Campus-Netzwerksicherheit. Ausgehend von einem Netzwerk-Perimeter wurden zunächst Firewall-ähnliche Funktionen entwickelt, die Segmentierung umsetzen und Regeln für den Daten-Traffic im virtuellen Rechenzentrum erzwingen sollten.

Dazu wurden einfach herkömmliche Firewalls in virtuelle Maschinen umgewandelt. Später wechselten die Hersteller zu agentenbasierten Segmentierungsmodellen, die stärker in die Virtualisierungsplattform integriert wurden. Beide Ansätze konzentrieren sich in erster Linie auf die Durchsetzung von Richtlinien im Cloud-Rechenzentrum.

Mit der Erstellung und Durchsetzung von Richtlinien allein lassen sich jedoch keine Cyber-Angreifer fassen. Am Perimeter werden die Firewall-Funktionen durch verschiedene Technologien zur Bedrohungserkennung und -abwehr (z. B. IDS/IPS, Malware-Schutz und Webfilter) ergänzt.

Diese Technologien wurden – ähnlich wie die Firewalls – einfach in virtuelle Maschinen portiert, um die Sicherheitsarchitektur von Campus-Netzwerken nachzubilden.

Allerdings sind Cloud-Rechenzentren ganz anders aufgebaut als der Perimeter, zudem erreichen die Cyber-Bedrohungen das Cloud-Rechenzentrum häufig in späteren Angriffsphasen als am Perimeter. Das heißt auch, dass die Bedrohungsarten und Angriffstechniken höchst unterschiedlich sind.

Konkret: Bedrohungsschutz am Perimeter konzentriert sich vor allem darauf, die initiale Kompromittierung oder Infektion (z. B. Exploits und Malware) zu erkennen. Die Cyber-Sicherheitsmaßnahmen für Cloud-Rechenzentren müssen auf Angreifer ausgerichtet sein, die den Perimeter bereits überwunden haben und sich in fortgeschritteneren Angriffsphasen befinden.

Dazu gehören die Spionage (Internal Reconnaissance) oder die Bewegung innerhalb des Netzwerks (Lateral Movement) und die Exfiltration von Daten.

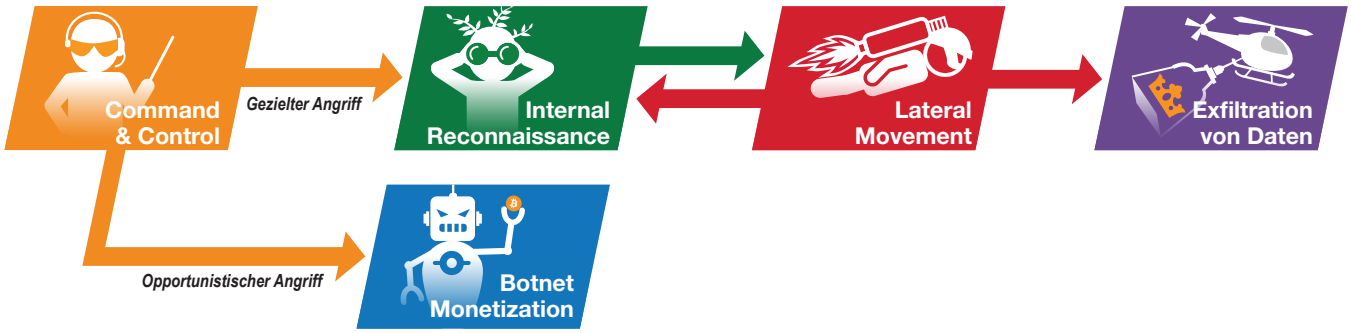
Daher ist ein neuer Cyber-Sicherheitsansatz notwendig, der sich auf die Prozesse innerhalb des Netzwerks konzentriert. Dieser Ansatz muss KI-Erkennungsmodelle nutzen, die auf maschinellem Lernen und Verhaltensanalysen basieren, um Angreifer aufzudecken, die innerhalb des Netzwerks eine Vertrauensstellung eingenommen haben.

Dieser nach innen gerichtete Ansatz zur Angriffserkennung ist im Cloud-Rechenzentrum noch wichtiger. Lange bevor Angreifer einen virtuellen Workload erreichen, haben sie bereits den Perimeter, ein Endgerät und gestohlene Administrator-anmeldedaten kompromittiert.

Statt Exploits oder Payloads direkt gegen Rechenzentrum-Ressourcen einzusetzen, nutzen Cyber-Angreifer viel häufiger ihre erlangte Vertrauensposition, um auf wichtige Daten zuzugreifen oder sie zu beschädigen.

Der bisherige Ansatz, der für die Absicherung von Cloud-Rechenzentren die Campus-Sicherheit imitiert, hat zu einem Cyber-Sicherheitsvakuum im Rechenzentrum selbst geführt. Während viel Arbeit in die native Richtliniendurchsetzung und Segmentierung des virtualisierten Netzwerks gesteckt wurde, spielte die Bedrohungserkennung hier eine untergeordnete Rolle.

Schlimmer noch: Herkömmliche Modelle für Perimeter-Eindringungsschutz sind nicht darauf ausgelegt, die heutigen ausgefeilten Angriffe auf Rechenzentren zu erkennen. Daher ist ein neues Modell notwendig, das Cyber-Sicherheit in die native virtualisierte Umgebung des Cloud-Rechenzentrums integriert.



Phasen eines Cyber-Angriffs innerhalb der Kill Chain.

Native Integration in virtualisierte Umgebung

Cyber-Sicherheitsfunktionen für Rechenzentren müssen nicht nur fortgeschrittenere Angriffsphasen erkennen, sondern zudem auch nativ in die Virtualisierungsplattform integriert sein. Laut einer Analyse von Cloud-Rechenzentren bleiben 80 % des Traffics innerhalb des Rechenzentrums. Das heißt, dass sich die Sicherheitslösung in der virtuellen Plattform befinden muss, um alle potenziellen Bedrohungen erkennen zu können.

Es genügt jedoch nicht, die Lösung einfach nur in die Virtualisierungsplattform zu integrieren: Da die virtuelle Umgebung dynamisch, höchst flexibel und stets im Fluss ist, ist sie ein attraktives Ziel.

Entwickler können schnell neue Anwendungen bereitstellen. Wenn sich die Anforderungen ändern, können diese Anwendungen einfach an andere Stellen – eventuell sogar auf komplett andere physische Hosts – verlagert werden.

Jede Sicherheitslösung, die nach Angreiferverhalten und Angriffsverläufen sucht, muss den Kontext einbeziehen und all diese Veränderungen der virtuellen Umgebung erfassen können. Daher genügt es nicht, sie einfach als einen weiteren Host in der virtuellen Umgebung einzurichten, der Sicherheit als Anwendung ausführt.

Stattdessen muss die Sicherheitslösung über nativen Überblick und Kontext für die virtualisierte Plattform verfügen. Sie darf also nicht nur eine Figur auf dem virtuellen Schachbrett sein, sondern muss alle Akteure im Spiel kennen sowie diese Kontextinformationen dauerhaft besitzen. Andernfalls ist eine Erstellung von Verhaltensmodellen unmöglich.

Einheitlicher Überblick für alle Teams

Eine Sicherheitslösung hat nicht nur die Aufgabe, aktive Angriffe zu erkennen, sondern benötigt auch einen einheitlichen Überblick über die Rechenzentrum-Sicherheit, der alle Operations-Teams abdeckt. Cloud-Rechenzentren werden prinzipbedingt von mehreren Teams mit jeweils eigenen Prioritäten und Zeitplänen gepflegt und genutzt.

Entwickler konzentrieren sich meist auf die schnelle Erstellung von Anwendungen, während das Virtualisierungs-Team diese so schnell wie möglich bereitstellen und unterstützen möchte. Daher ist das Security-Team nicht immer über die Änderungen in der virtuellen Umgebung informiert.

Die kritischen Angriffsvektoren

Rechenzentren und die darin enthaltenen Informationen sind das primäre Ziel der Angreifer. Doch sofern der Angreifer nicht das Glück hat, eine über das Internet zugängliche Schwachstelle zu finden, sind für die Kompromittierung von Rechenzentren erheblicher Aufwand und umfangreiche Planungen erforderlich.

Daher sind Cyber-Angreifer, die es auf Rechenzentren abgesehen haben, meist geduldig. Sie nutzen ausgereifte Prozesse, die sich auf Persistenz konzentrieren und möglichst unterhalb des Radars der Security-Teams ablaufen.

In diesem Abschnitt erläutern wir die kritischen Angriffsvektoren und Techniken, die von Cyber-Angreifern gegen Rechenzentren eingesetzt werden.

Missbrauch des Administratorzugangs

Administratoren verfügen über besonders umfangreiche Zugriffsrechte für das Rechenzentrum und sind daher das wichtigste Ziel der Angreifer. Die administrativen Protokolle können Angreifern Backdoor-Zugriff auf das Rechenzentrum ermöglichen, ohne dass eine Anwendungsschwachstelle direkt ausgenutzt werden muss. Mithilfe gängiger Admin-Tools wie SSH, Telnet oder RDP können sich Angreifer problemlos in den regulären Admin-Traffic einschleusen.

Da in diesen Angriffsphasen keine Payloads, sondern zulässige Protokolle verwendet werden, sind zur Erkennung von Cyber-Bedrohungen verhaltensbasierte Modelle besonders wichtig. Die Verhaltensmodelle sollten möglichst mit dem tatsächlichen Netzwerk-Traffic abgeglichen werden, da die Logs für die genutzten Protokolle häufig nicht zur Verfügung stehen.

Schließung der lokalen Authentifizierungslücke

Zusätzlich zu den Standardpfaden, die von Administratoren verwendet werden, setzen viele Rechenzentren auf lokale Authentifizierungsoptionen für Notfallsituationen. Wenn zum Beispiel ein Domain-Controller oder eine andere Authentifizierungsinfrastruktur ausfällt, müssen die Administratoren weiterhin in der Lage sein, das Rechenzentrum zu verwalten.

In diesen Fällen setzen Administratoren für den Zugriff auf die zu verwaltenden Hosts und Workloads auf lokale Authentifizierung. Diese lokalen Authentifizierungsoptionen werden jedoch nicht protokolliert. Zudem werden aus Bequemlichkeit häufig die gleichen Anmeldeinformationen für Hosts und Workloads verwendet.

Damit erweisen sich diese eigentlich unverzichtbaren Authentifizierungskanäle als schwerwiegendes Sicherheitsrisiko für das Rechenzentrum. Wenn Angreifer durch die Kompromittierung eines Administrators an dessen Anmeldedaten gelangen, erhalten sie unbemerkt Zugriff auf das Rechenzentrum, ohne befürchten zu müssen, dass ihre Aktivitäten protokolliert werden.

Hardware-Hintertür in die Verwaltung

Lokale Authentifizierung ist ein Beispiel für eine Hintertür, mit der Administratoren – und Angreifer – auf ein Rechenzentrum zugreifen können. Es gibt jedoch noch weitere Möglichkeiten, die den gleichen Ansatz nutzen und auf die zugrunde liegende Hardware ausdehnen.

Obwohl Virtualisierung heute nicht mehr aus dem Rechenzentrum wegzudenken ist, müssen die virtualisierten Umgebungen immer noch auf physischer Hardware ausgeführt werden. Virtuelle Laufwerke benötigen physische Festplatten, die wiederum in physischen Servern laufen.

Auch diese physischen Server verfügen über eigene Verwaltungsebenen, mit denen Lights-Out- und Out-of-Band-Management umgesetzt wird. Die Verwaltungsebenen wiederum nutzen eigene Management-Protokolle, Energieversorgung, Prozessoren und Speichersysteme, sodass Administratoren selbst bei abgeschaltetem Hauptserver noch Laufwerke bereitstellen und Re-Imaging durchführen können.

Dabei kommen häufig Protokolle wie Intelligent Platform Management Interface (IPMI) zum Einsatz. Auch wenn viele Hardware-Anbieter eigene IPMI-Varianten wie Dell iDRAC oder HPE Integrated Lights-Out (ILO) nutzen, basieren diese alle auf IPMI und bieten den gleichen Funktionsumfang.

Diese Funktionen stehen unabhängig von der Datenebene des Servers zur Verfügung. Effektiv befinden sich diese Protokolle unterhalb der Virtualisierungsebenen, unterhalb aller Host-Betriebssysteme und selbst unterhalb des BIOS auf dem Mainboard.

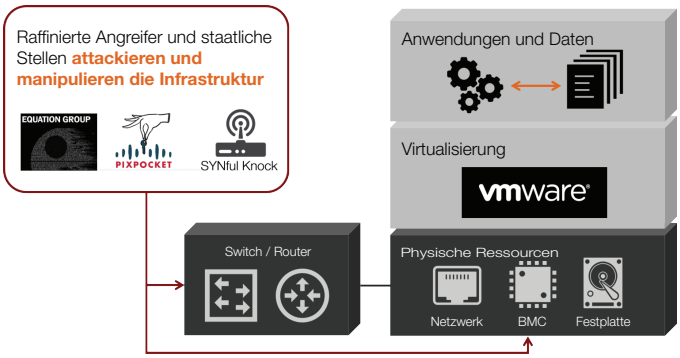
IPMI und verwandte Protokolle haben gut dokumentierte Sicherheitsschwachstellen, die häufig nur langsam durch Aktualisierungen und Bugfixes behoben werden. Die Kombination aus IPMI-Schwachstellen und großem Funktionsumfang macht diese Protokolle zu einer beliebten Angriffsfläche für Angreifer, die die Sicherheitsmaßnahmen des Rechenzentrums unterlaufen wollen.

Raffinierte Angreifer zielen tief

Leider beschränken sich die Hardware-Probleme im Rechenzentrum nicht auf IPMI. Raffinierte Angreifer (einschließlich staatlicher Stellen) nehmen zunehmend physische Server, Router, Switches und selbst Firewalls ins Visier.

Tools wie Synful Knock haben demonstriert, wie Angreifer unterhalb des Betriebssystems ansetzen können, um die vollständige Kontrolle über einen Router zu übernehmen und anschließend Angriffe auf andere Systeme und Router im gleichen Netzwerk zu starten.

Im Grunde genommen sind diese Tools nichts anderes als Rootkits, die sich unterhalb des Betriebssystems einnisten und daher eine Erkennung mit herkömmlichen Mitteln äußerst schwierig machen.



Angriffe auf Rechenzentren konzentrieren sich auf die zugrunde liegende physische Infrastruktur.

Die Offenlegung von Angriffstools der Equation Group gibt eine Vorstellung vom Bedrohungsarsenal und den Techniken, die staatlichen Angreifern zur Verfügung stehen. Dazu gehören verschiedenste Techniken und Tools, mit denen Software und Firmware in verschiedenste Firewalls und Sicherheits-Appliances implantiert werden.

Diese Techniken erlauben Angreifern das Infizieren just der Geräte, die den Schutz des Netzwerks gewährleisten sollen, sowie den Missbrauch dieser Geräte zur Durchführung von Angriffen auf das Netzwerk. Auch hier gibt die strategische Ausrichtung dieser Geräte den Angreifern die Möglichkeit, Traffic zu überwachen und umzuleiten sowie Angriffe aus einer Vertrauensstellung heraus zu starten.

Endziel: Ihre Daten

Letztlich geht es bei den meisten Angriffen um Datendiebstahl. Daher müssen Security-Teams Angriffe immer identifizieren, noch bevor Datenzugriffe stattfinden können. Das schließt auch die Phase der Datenexfiltration ein.

Je nach Ziel und Kompetenz stehen den Angreifern zahlreiche Möglichkeiten zur Ausleitung der Daten aus dem Rechenzentrum zur Verfügung. Die offensichtlichste Methode ist die massenhafte Übertragung der Daten – entweder direkt über das Internet oder über einen Brückenkopf innerhalb des Campus-Netzwerks.

Geduldigere Angreifer gehen subtiler vor und exfiltrieren die Daten in einer Menge und Geschwindigkeit, die weniger auffällt oder Verdacht erregt. Wiederum andere verschleiern die Datenexfiltration mithilfe verborgener Tunnel in zulässigem Traffic (z. B. Web- oder DNS-Traffic).

Verknüpfung von physischem und virtuellem Kontext

Die Rechenzentren der einzelnen Unternehmen sind höchst individuell. Sie verfügen über einen spezifischen Bestand an Anwendungen und werden auf unterschiedliche Weise genutzt. Am häufigsten anzutreffen sind heute private unternehmenseigene Rechenzentren, die meist im Rahmen größerer Angriffe auf das Unternehmen selbst attackiert werden.

Möglicherweise haben die Angreifer zunächst einen Mitarbeiter-Laptop per Phishing-E-Mail oder Social Engineering kompromittiert. Im nächsten Schritt versuchen sie sich im Netzwerk festzusetzen, indem sie sich vom ursprünglichen Opfer zu anderen Hosts oder Geräten ausbreiten.

Zur Steuerung des laufenden Angriffs platzieren Angreifer Hintertüren und verborgene Tunnel, über die sie aus dem Netzwerk heraus kommunizieren. Im Laufe der Zeit erkunden sie das interne Netzwerk, identifizieren wertvolle Ressourcen und kompromittieren Geräte sowie Anmeldedaten.

Die für einen Angreifer wichtigste gestohlene Ressource sind die Anmeldedaten des Administrators, da sie weitgehende Autonomie im angegriffenen Netzwerk erlauben. Diese Zugangsdaten sind besonders für Angriffe auf Rechenzentren wichtig, da Administratoren häufig die einzigen Personen sind, die in großem Umfang auf Daten zugreifen können.

Wichtig ist hierbei, dass Angriffe bereits stark ausgebaut sind, wenn sie das private Rechenzentrum erreichen. Voraussetzung für die erfolgreiche Eindringung sind verborgener Command-and-Control-Traffic, Reconnaissance, Lateral Movement sowie kompromittierte Anmeldedaten von Administratoren und Anwendern.

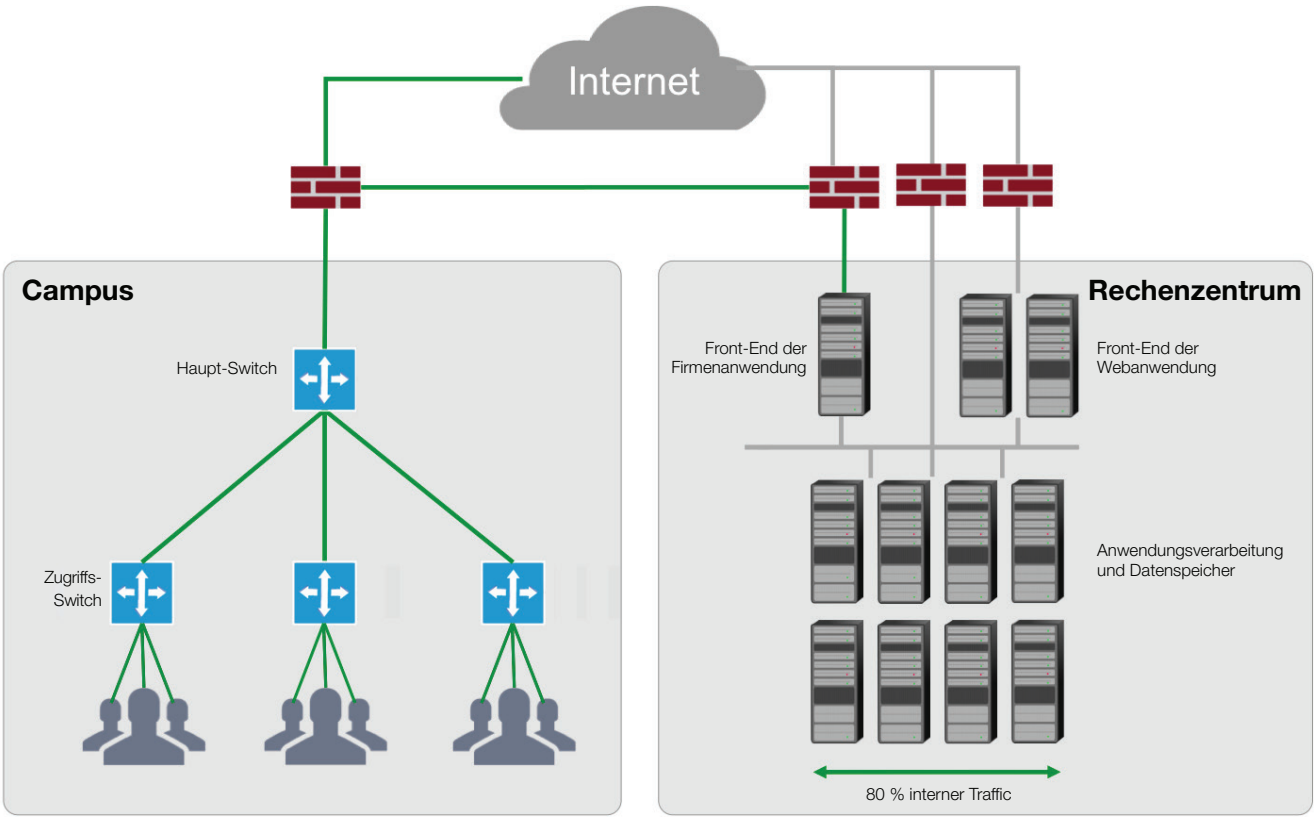
Jede dieser Phasen bietet eine Möglichkeit, den Angriff zu erkennen. Daher müssen Security-Teams so viel Kontext wie möglich erfassen, bevor der Angriff das Rechenzentrum erreicht.

Genau deshalb ist auch ein einheitlicher Cyber-Sicherheitsansatz – vom Campus über Zweigniederlassungen bis zum Rechenzentrum – so wichtig. Cyber-Angriffe sind komplexe und vernetzte Ereignisse. Wenn die Sicherheit des Rechenzentrums isoliert verwaltet wird, profitieren davon nur die Angreifer.

Fazit

Der Bestand an Daten und Anwendungen macht Rechenzentren zum primären Ziel für Cyber-Angreifer. Da sich die Sicherheitsmaßnahmen bislang nur auf den Schutz der virtualisierten Ebenen innerhalb des Rechenzentrums konzentrieren, nehmen Angreifer zunehmend die physische Infrastruktur der Rechenzentren ins Visier.

Für Security-Teams muss deshalb die Möglichkeit, Cyber-Angriffe auf Rechenzentren zu erkennen, an erster Stelle stehen. Dazu stehen verschiedene Methoden bereit, z. B. hochentwickelte Erkennungsmodelle, die Angriffe gegen Anwendungen, Daten und Virtualisierungsebenen in Rechenzentren sowie gegen die zugrunde liegende physische Infrastruktur aufdecken. Damit erhalten Security-Teams die Möglichkeit, kritische Schwachstellen auf jeder Ebene des virtualisierten Rechenzentrums zu schließen.



Zur Erkennung von Cyber-Angriffen ist ein vollständiger Überblick über Campus und Rechenzentrum erforderlich.

VECTRA
Security that thinks®

E-Mail info_dach@vectra.ai **Telefon** +1 408 326 2020
vectra.ai/de