Datenklau im Rechenzentrum

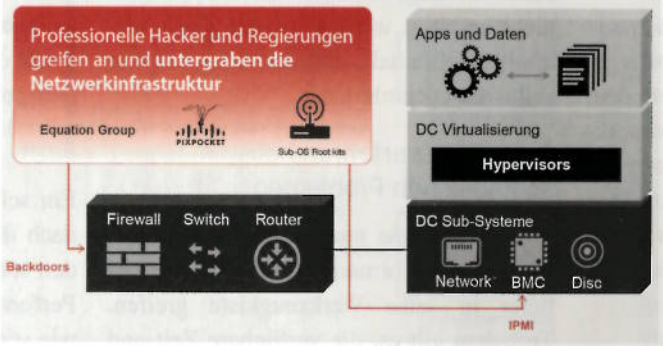
Schwachstelle Admin-Zugriff

Die Sicherheitsmaßnahmen im RZ sind noch nicht ausgereift. Angreifer von außen sowie Insider bedienen sich Methoden, die Sicherheitsteams nicht wahrnehmen oder auf die sie nur unzureichend vorbereitet sind. Auch administrative Fernzugriffe über Verfahren wie IPMI (Intelligent Platform Management Interface) sind oft unzureichend gesichert. Neue Sicherheitsstrategien und -lösungen sind gefragt, um Schwachpunkte im RZ zu identifizieren und hochentwickelte Angriffe aufzudecken.

Die meisten Unternehmen setzen in Sachen Datacenter Security immer noch auf traditionelle Maßnahmen der Perimetersicherheit wie Firewalls, IDS/IPS, Anti-Malware-Lösungen oder Web Filtering. Doch laut dem Gartner-Report „Network Security Architectures for Virtualized Data Centers" vom August 2015 mangelt es „perimeterzentrischer Sicherheit und zonenbasierten Firewall-Infrastrukturen beispielsweise an Überblick und Kontrolle über Ost-West-Rechenzentrums-Traffic, was rund 80 Prozent des gesamten Datacenter-Netzwerk-Traffics ausmacht." Laterale Bewegungen der Angreifer sowie das Ausbreiten von Malware ließen sich damit nicht kontrollieren, so die Analysten.

Im virtualisierten Rechenzentrum konzentrieren sich IT-Organisationen auf Firewall-Sicherheitsmechanismen, um Richtlinien für den Datenverkehr durchzusetzen. Dazu zählt zum Beispiel die einfache Portierung traditioneller Firewalls, damit diese als virtuelle Maschinen (VMs) agieren. Hinzu kommen agentenbasierte Segmentierungsmodelle, die eng in die Virtualisierungssoftware integriert sind.

Solche Sicherheitsansätze reichen jedoch nicht aus, um das RZ umfassend zu schützen. So sind Angriffe heute deutlich besser getarnt und professioneller als noch vor einigen Jahren. Herkömmliche Sicherheitslösungen können viele der neuen Methoden schlichtweg nicht erkennen. Ein Beispiel: Angreifer versuchen vermehrt, die physische RZ-Infrastruktur zu beeinflussen und zu kontrollieren. Sie agieren im Verborgenen, „unter dem Radar" traditioneller Sicherheitslösungen, die sich auf VM-Workloads und den Datenverkehr innerhalb der Hypervisoren konzentrieren. Immer mehr Kriminelle greifen aber die Switches, Router und Firewalls sowie physischen Hosts an, die das Rechenzentrum ausmachen. IT-Umgebungen benötigen deshalb einen neuen, verlässlicheren Sicherheitsansatz.



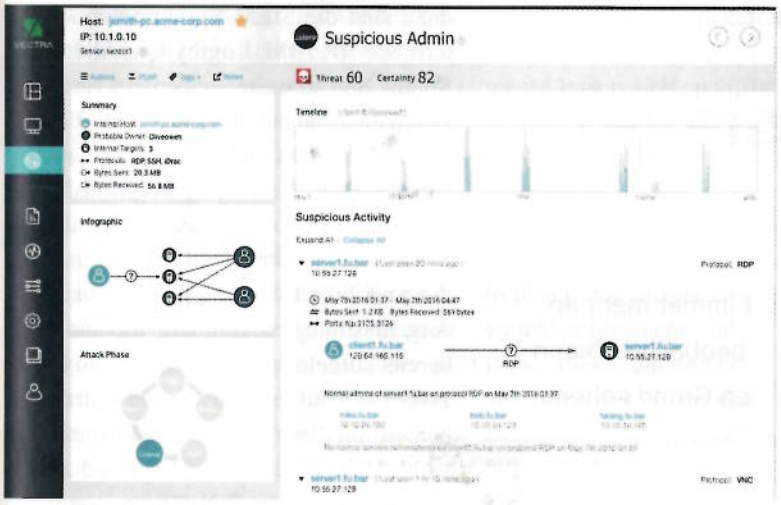
Angreifer kommen gerne über Hintertüren ins Rechenzentrum, zum Beispiel über Fernzugriffe per IPMI. Bild: Vectra Networks

Um neue Strategien entwickeln zu können, muss eine IT-Organisation die Angriffsmethoden kennen, die Angreifer vermehrt einsetzen, um Rechenzentren zu kompromittieren – und die oft übersehen werden. Zu den beliebten Hintertüren gehören beispielsweise die Protokolle für den Fernzugriff des Administrators. Ein Hacker, der über gestohlene Administratorenrechte und Zugangsdaten verfügt, hat in den meisten Unternehmen umfassenden Zugriff auf Systeme und Daten, sodass er immensen Schaden anrichten kann.

Das Ausnutzen von Hintertüren im Netzwerk ist gut dokumentiert. Bekannte Vorfälle gab es bereits Ende der 1990er-Jahre sowie Anfang und Mitte der 2000er-Jahre. Hinzu gesellen sich nicht zuletzt die Snowden-Enthüllungen 2013. Ein Beispiel aus dem Sommer 2016: Im August behaupteten die sogenannten Shadow Brokers, eine Hackergruppe namens Equation Group gehackt zu haben, die der NSA nahestehen soll. Die Shadow Brokers initiierten eine Auktion angeblicher Exploits der Equation Group, mit denen sich Netzwerke kompromittieren lassen sollen.

Ein gern genutztes Einfallstor für Angreifer ist das Intelligent Platform Management Interface (IPMI), eine von Intel, Hewlett-Packard, NEC und Dell entwickelte Schnittstelle für die Fernwartung von Endgeräten, selbst wenn diese ausgeschaltet sind (das sogenannte „Lights-out-Management", LOM). So untersucht die Shadowserver Foundation im Rahmen eines breit angelegten Projekts öffentlich zugängliche Geräte, die via IPMI Hintertüren für Angriffe öffnen. Ziel des Projekts ist es, ungeschützte und somit angreifbare IPMI-Geräte aufzudecken und die Eigentümer auf die gefundenen Sicherheitslücken hinzuweisen.

Auf die aktuelle IPMI-Abfrage haben 168.887 IP-Adressen geantwortet. Von den 50.683 Hosts, die auf IPMI v1.5 setzen, nutzen 43.112 die NONE-Authenti-



Moderne Abwehrlösungen spüren verdächtiges Anwenderverhalten im Netzwerk auf und erkennen dadurch potenzielle Angriffe.

Bild: Vectra Networks

fizierungsmethode: Um auf diese Geräte zuzugreifen, sind demnach keinerlei Berechtigungsnachweise notwendig – eine Top-Gelegenheit für Cyberkriminelle. Deutschland steht im Ranking der Shadowserver-Gruppe übrigens auf dem zweiten Platz nach den USA mit den meisten öffentlich zugänglichen und somit unsicheren IPMI-Hosts. Hier besteht dringender Handlungsbedarf.

Gesucht ist also ein umfassender Ansatz zur Aufdeckung versteckter Sicherheitslücken in Netzwerkinfrastrukturen. Abhilfe schaffen neue Lösungen, die eng mit der Virtualisierungsplattform verbunden und gleichzeitig in der Lage sind, das Verhalten fortschrittlicher Angreifer ebenso wie Angriffe auf die gesamte IT-Infrastruktur eines Unternehmens aufzudecken – von entfernten Standorten bis zu Rechenzentren oder Private Clouds. Es gilt, Sicherheitslösungen einzusetzen, die versteckte Tunnel finden, den Missbrauch von Administrationsprotokollen und -rechten durch Insider wie auch externe Angreifer aufdecken und zugleich vor Betriebssystem-Rootkits und anderen Angriffen schützen. Nicht vergessen darf man dabei Aspekte wie Remote Access Trojans (RATs) oder Werkzeuge der Verhaltensanalyse, die Angreifer ebenfalls nutzen, um an Daten zu gelangen und Infrastrukturen zu beschädigen.

Aktuelle Sicherheits-Tools zur Angriffsabwehr beinhalten zwei Kernkomponenten: Sensoren und eine Analyse-Engine. Die Sensoren werden in der gesamten RZ-Umgebung verteilt, um so den Überblick über den Netzwerkverkehr zu verbessern. Sie ermöglichen es der Analysekomponente, Data-Science- und Machine-Learning-Prozesse anzustoßen, um die Verhalten der Angreifer aufzudecken und Gegenmaßnahmen in die Wege zu leiten. Virtuelle Sensoren verknüpfen sich dabei mit jedem Vswitch, um den Datenverkehr zu analysieren und Bedrohungen zwischen den Workloads in der virtuellen Umgebung aufzudecken. Unternehmen sollten einen Ansatz wählen, der es ihnen gestattet, umfassende Transparenz und Sicherheit für alle physischen und virtuellen Assets im Unternehmen zu erhalten.

Fazit: Versteckte Zugänge aufdecken

Lange haben sich Überlegungen zur RZ-Sicherheit hauptsächlich mit Themen wie Segmentierung, Zugriffsrichtlinien und Antivirenlösungen beschäftigt, um Einfallstore für Angreifer zu schließen. Hacker haben aber herausgefunden, dass sich der Schlüssel für kriminelle Vorhaben tiefer in den Geräten befindet, die im RZ zum Einsatz kommen. Neue Techniken und Sicherheitsstrategien müssen versteckte Zugänge ebenso aufdecken wie Rootkits und Angriffe, die von gesicherter Infrastruktur ausgehen. Hinzu kommt die Kontrolle unsachgemäßer administrativer Aktivitäten, darunter solcher, die Low-Level-Management-Protokolle wie IPMI nutzen. Nur wer die Gefahren im RZ kennt, kann Angriffe stoppen, ehe sie Schaden anrichten.

Alex Waterman/wg

Alex Waterman ist Senior Director Product Management bei Vectra Networks, www.vectranetworks.com.