Sicherheit im digitalen Zeitalter – was bedeutet das wirklich?

Trotz der zahlreichen Vorteile und Vorzüge, die Cloud-Netzwerke für Unternehmen mit sich bringen, ist die Sicherheit in der Cloud ein ständiges Sorgenkind. Die Häufigkeit und Raffinesse böswilliger Angriffe auf die Cybersicherheit nehmen ständig zu; die besten Cloud-Unternehmen müssen stets darauf bedacht sein, nicht nur den neuesten Sicherheitsstandards zu entsprechen, sondern den sich ständig verändernden Bedrohungen immer einen Schritt voraus zu sein.

Was also brauchen Sie wirklich, um die Cloudelemente Ihres Unternehmens im digitalen Zeitalter vor Bedrohungen zu schützen? Zunächst einmal muss das Sicherheits-Ökosystem als Ganzes betrachtet werden. Eine skalierbare und einfach zu handhabende Netzwerksegmentierung ist dabei die Voraussetzung, um den Überblick über alle Anwendungen, Benutzer und Geräte zu behalten.

Wir bei Extreme nehmen die Bedrohungen für Verfügbarkeit, Integrität und Vertraulichkeit der Informationen unserer Kunden ernst. Ganz gleich, ob es sich um das Einbinden von Gast-oder Firmengeräten, die Überwachung von IoT-Geräten oder die Kontext-sensitive Durchsetzung von Richtlinien handelt – die Sicherheit und Verfügbarkeit unserer Sicherheitslösungen basieren auf automatischen Aktionen, die überwiegend vom Netzwerk selbst durchgeführt werden. Darüber hinaus bietet das Extreme Netzwerkmanagement offene Schnittstellen zur Interaktion Sicherheitssystemen und-komponenten anderer Anbieter. Das Resultat einer umfangreichen Technologiepartnerschaft mit Herstellern von Sicherheitslösungen ist dabei ein integriertes, ganzheitliches Sicherheits-Ökosystem. Diese Integrationen können so einfach sein wie die Übergabe von Inventardaten per API bis hin zur komplexen Workfloweinbindungen ins Extreme Management Center oder ExtremeCloud IQ.

Netzwerklösungen von Extreme werden in horizontale (typischerweise finden Sie solche in jeder Netzwerk-Implementierung) oder spezialisierte Kategorien (in bestimmten vertikalen Bereichen wie Gesundheitswesen, Einzelhandel, Bildung usw. zu finden) eingeteilt.

Im Folgenden finden Sie einige der integralen Sicherheitselemente, durch die sich unsere Cloud-Lösung von anderen abhebt:

ISO/IEC 27001-Zertifizierung

Extreme Networks ist der erste und einzige große Anbieter von Cloud-verwalteten Netzwerken, der entsprechend des globalen Standards für die Verpflichtung zu Best Practices und Kontrollen für Informationssicherheits-Managementsysteme zertifiziert ist. Die ExtremeCloud IQ Cloud-Plattform von Extreme Networks wurde von der International Standards Organization (ISO) nach ISO/IEC 27001 zertifiziert und gewährleistet ein Höchstmaß an Sicherheit für Informationssysteme und Datenschutz, Management und Compliance. Unsere Mitbewerber

behaupten zwar, durch ihre Hosting-Anbieter SOC2-konform zu sein, aber es gibt keine Anbieter mit SOC2 auf ihrer eigenen Cloud-Management-Plattform. Als einziger Anbieter geht Extreme Networks über diesen grundlegenden Anspruch hinaus und erreicht damit- zusätzlich zum Grundschutz von Amazon Web Services, Google Cloud Platform und Microsoft Azure, die vollständige End-to-End-Zertifizierung gemäß ISO27001. Regelmässige Prüfungen stellen dabei sicher, dass dieser Standard auch in einem hochdynamischen Konstrukt, konsequent eingehalten wird.

Cloud Services

Unsere Cloud Services werden in den Rechenzentren von Amazon AWS (Amazon Web Services), Microsoft Azure und Google gehostet und nutzen deren inhärenten Sicherheits- und Compliance-Funktionen auf der Data Center Ebene.

Doch auch der Managementverkehr zwischen der Kundeninfrastruktur und dem cloudbasierten Management wird bei der Übertragung ins Regionale Rechenzentrum (RDC) verschlüsselt.

Die eigentlichen Nutzdaten aus LAN und WLAN des Kunden werden zu keiner Zeit in Richtung der ExtremeCloud IQ Public Cloud-Instanz des Kunden weitergeleitet.

Rollen-basierte Zugriffskontrolle

Innerhalb von ExtremeCloud IQ können Sie mit Hilfe der Rollen-basierten Zugriffskontrolle verschiedene Benutzerrichtlinien erstellen, die auf Geräte und Personen mit unterschiedlichen Aufgaben im Unternehmen basieren. Diese Rollen beinhalten einen einzigartigen Satz von Regeln für den Zugriff auf Technologie und Ressourcen.

WPA3 und darüber hinaus

Die APs von Extreme unterstützen und bieten das höchste Maß an Sicherheit, das auf den Client-Geräten verfügbar ist. So kann Extreme die neuesten Sicherheitsstandards bieten, gleichzeitig aber auch Legacy-Technologien unterstützen und eine sinnvolle Isolierung zwischen Gruppen unterschiedlicher Sicherheitsstandars gewährleisten.

Kontext-basiertes Networking

Durch Kontext-basiertes Networking können Sie Benutzer, Geräte und Anwendungen identifizieren und deren Zugriff je nach dem Nutzen für Ihr Netzwerk und Ihr Unternehmen entweder priorisieren oder einschränken. Auf diese Weise können Sie die Performance eines Gast-oder BYOD-Geräts gegenüber einem Unternehmensgerät einschränken, Shadow IT oder illegale Streamingdienste blockieren und gleichzeitig die Servicequalität legitimer Sprach-oder Videoanwendungen erweitern. Dieser Rollen-basierte Zugriff und das Kontext-basierte Networking müssen nicht unbedingt auf der SSID-Ebene erfolgen. Benutzerprofile sind eine hervorragende Möglichkeit, Benutzer unter dem Dach einer einzigen SSID auf verschiedene Segmente zu verteilen. Die Zuweisung von Nutzern und Endsystemen zu entsprechenden Zugriffsregelwerken lässt sich anhand von Gruppenzugehörigkeit, aber auch Lokation, Uhrzeit sowie anderen Charakteristiken flexibel zuweisen.

PPSK

Private Pre-Shared Keys (PPSK), schließen die Lücke zwischen dem komplexen 802.1X und der traditionellen, im professionellen Umfeld schwer zu handhabenden, PSK-Lösung.

PPSK stellt eine ausgezeichnete Lösung für Gastnetzwerke oder für Geräte dar, die 802.1X nicht unterstützen. Aber auch in in Fällen, in denen 802.1X einfach zu schwer zu implementieren und zu überwachen ist, wird PPSK zum Mittel der Wahl. Unterstützen zahlreiche IoT-Geräte keine Zertifikatsbasierte Authentisierung, erfordert der Sicherheitsanspruch trotzdem eine saubere Separierung in unterschiedlichen, logischen Netzsegmenten. Mit PPSK erlaubt erhält jedem Benutzer bzw. Client einen individuellen Schlüssel.

Private Client Groups

Private Client Groups (PCG) bieten eine sichere und einfache Möglichkeit Endsysteme in logischen Gruppen zu organisieren. Vor allem für PPSK Szenarien bietet sich damit die Möglichkeit den Sicherheitsbedarf besonderer Anwendungen wie z.B. Klimasensoren, Zugangskontrollen oder Drucker durch den Einsatz von Microsegmentierung bzw. Zugriffsregelwerken präzise anpassen.

Aber auch RADIUS-basierte Authentisierungsszenarien lassen sich durch den Einsatz von Private Client Groups einfacher handhaben.

Layer 2-7 DPI

Die Deep Packet Inspection auf Layer 2-7 ermöglicht Ihnen einen vollständigen Überblick darüber, wer welche Anwendungen wann in Ihrem Netzwerk nutzt und wieviel Bandbreite dabei konsumiert wird.

Cloud-verwaltete Network Access Control (NAC)

Eine Option für zusätzliche Sicherheit in Cloud-Netzwerken ist ExtremeCloud A3 – eine innovative, Cloud-verwaltete Lösung zur Netzwerkzugriffskontrolle (NAC). Sie sichert, verwaltet und kontrolliert alle Geräte in Ihrem Netzwerk und bietet umfassende Funktionen für das Geräte-Onboarding, die Gastverwaltung, eine automatische Gerätebereitstellung, die Erstellung von Geräteprofilen und die Zugriffskontrolle. A3 ist Herstellerunabhängig und kann in der Netzwerkzugriffskontrolle (NAC) aller großen Anbieter eingesetzt werden.

Einige zusätzliche Maßnahmen, mit denen Extreme unsere Cloud-basierten Anwendungen absichert:

- Firewalling, um den ein-und ausgehenden Datenverkehr zu kontrollieren und zu schützen
- Erkennung von Bedrohungen mit kontinuierlicher Überwachung auf böswilliges und unbefugtes Verhalten, einschließlich unbefugten Systemzugriffs und Brute-Force-Angriffen
- DDoS-Angriffsvermeidung und Flusskontrolle mit branchenführenden Tools
- Staging aller ExtremeCloud IQ-Releases und Patches mit kontinuierlichem Penetration-Scanning auf Sicherheitslücken in Anwendungen, um Probleme vor dem eigentlichen Einsatz in der Produktion zu vermeiden
- OS-Härtungsprozesse nach Industriestandard für die Bereitstellung der Produktionsserver
- Tägliche Backups der Daten des Produktionsnetzwerks und Speicherung der Backups in verschlüsseltem Zustand
- Sicherung des Zugriffs auf die zugrundeliegende Computer-Infrastruktur mit Funktionen wie VPC, NAT, TLS-Verschlüsselung, Reporting-Tools und automatisiertem Passwortschutz
- Strikte Beschränkung des Zugriffs auf die AWS-Cloud-Infrastruktur auf eine kleine Anzahl von designierten Extreme Networks DevOps-Ingenieuren
- Überwachung und Verfolgung der Aktivitäten des DevOps-Personals in der AWS-Umgebung mit einem Server/Anwendungs-Audit-Trail

Dank Extreme können Administratoren sicherstellen, dass ihre Netzwerke nicht missbräuchlich genutzt oder infiltriert werden. Sollte dies dennoch der Fall sein, lassen sich Bedrohungen schneller als bisher identifizieren lokalisieren und durch die zentrale Anpassung von Sicherheitsrichtlinien effektiv bekämpfen.

Extreme networks

http://www.extremenetworks.com/contact