Moderne Rechenzentren benötigen heute einen neuen Sicherheitsansatz

→ Virtualisierung, Cloud und Software-Defined Networking (SDN) definieren Rechenzentren neu.

→ Workloads, Anwendungen und Daten befinden sich heute überall, in Multi-Cloud-Umgebungen.

→ Benutzer arbeiten außerhalb der Unternehmensumgebung, sind zunehmend mobil und greifen mit den verschiedensten Geräten auf Ressourcen zu.

→ Die heutigen Rechenzentren sind unglaublich komplex, und Unternehmen müssen ihren Sicherheitsansatz überdenken.

Security-Teams verbringen **76 %** ihrer Zeit mit dem Schutz des Rechenzentrums mit folgenden prozentualen Anteilen:*

- **47 %** Server
- **20 %** Kundendaten
- **24 %** Endpunkte

57 % sagen, dass der Schutz von Daten in der Public-Cloud die größte Herausforderung ist***

Nur **38 %** haben ihr Rechenzentrum segmentiert*

Sicherheitsverantwortliche bestätigen, dass fehlendes Personal ein Problem für die Sicherheit darstellt:***

25 % der Entscheidungsträger für globale Sicherheit sagen, dass Personalmangel eine große Herausforderung ist und sie nur schwer Mitarbeiter mit den erforderlichen Kompetenzen finden. Das Personalproblem verstärkt sich zusätzlich, wenn zu viele nicht integrierte Lösungen verwaltet werden müssen.

Wie werden Daten gestohlen? Über Mitarbeiter****

81 % der Sicherheitsverletzungen durch Hacking nutzten gestohlene oder schwache Passwörter

86 % der schädlichen Payloads werden über E-Mails **73 %** und das Internet **13 %** übermittelt

Datenquelle:
*Cisco Annual Cybersecurity Report 2017
**Cisco Annual Cybersecurity Report 2018
***Zero Trust eXtended (ZTX) Ecosystem von Chase Cunningham, Forrester
****Verizon Data Breach Investigation Executive Summary and Full Report 2017

Moderne Rechenzentren haben 3 wichtige Sicherheitsanforderungen

Transparenz

Behalten Sie den Überblick mit vollständiger Transparenz in Bezug auf Benutzer, Geräte, Netzwerke, Anwendungen, Workloads und Prozesse.

Segmentierung

Verhindern von lateraler Ost-West-Bewegung von Angreifern im Netzwerk durch Mikro-Segmentierung und Whitelists für Anwendungen

Schutz vor Bedrohungen

Schnellere Erkennung von Sicherheitsverletzungen mit mehrschichtigen Bedrohungssensoren zur schnellen Erkennung, Blockierung und Reaktion, um Datendiebstahl und Betriebsunterbrechungen zu verhindern

Es ist Zeit für einen neuen Ansatz in Bezug auf die Sicherung Ihrer Daten, Anwendungen und dynamischen Workloads.

Ein Ansatz mit innovativen Technologien und einer integrierten Architektur für moderne Rechenzentren. Ihre Vorteile:

Kontext, um bei der Übertragung von Anwendungen und Mikro-Anwendungen im Rechenzentrum zu erkennen, ob Datenverkehr schädlich ist oder nicht

Dynamische, flexible Kontrollen für die Konsolidierung und Automatisierung von Netzwerk-, Sicherheits- und Anwendungsrichtlinien

Mehrschichtige Erkennung und Eindämmung von Sicherheitsrisiken, damit mehr Bedrohungen blockiert und Bedrohungen, die Ihr Rechenzentrum erreicht haben, schneller eingedämmt werden

Cisco schützt Daten, Anwendungen und Workloads und sorgt in Ihrem Unternehmen für mehr Sicherheit und Produktivität

Schnellere Bedrohungserkennung durch umfassende Transparenz in Bezug auf alle Benutzer und den Netzwerkverkehr im Unternehmen, in der Cloud und im Rechenzentrum

Reduzierte Angriffsfläche durch Kontrollen, die nicht autorisierte Benutzer und komplexe Bedrohungen daran hindern, **sich lateral in Ihrem Rechenzentrum zu bewegen**

Schnelles Erkennen, Blockieren und Reagieren auf Sicherheitsverletzungen und Betriebsunterbrechungen

Cisco hat innovative neue Technologien entwickelt, die zusammenarbeiten, um moderne Rechenzentren zu schützen.

Mehr Infos

C05-740358-00 04/18