HANDLUNGSEMPFEHLUNG

Datacenter & Netzwerk – sicher und stabil gegen moderne Bedrohungen

ORBIT IT-SOLUTIONS

Unsere 7 Handlungsempfehlungen für Ihre Security Roadmap

… kurzfristig

1 Härtung von Server- und Storage-Systemen:

Setzen Sie bewährte Best-Practices zur Härtung Ihrer Server- und Storage-Infrastruktur konsequent um. So reduzieren Sie potenzielle Angriffsflächen und schützen Ihre zentralen Systeme vor unbefugtem Zugriff.

2 Backup-Überprüfung:

Analysieren Sie Ihre aktuelle Backupstrategie. Prüfen Sie, ob die Wiederherstellungsgeschwindigkeit und die sichere Aufbewahrung Ihrer Daten den aktuellen Anforderungen entsprechen. Nur so stellen Sie sicher, dass im Ernstfall ein zuverlässiges Recovery möglich ist.

3 DDoS-Schutz, WAAP-Integration:

Implementieren Sie effektive Schutzmechanismen gegen DDoS-Angriffe sowohl auf Netzwerk- als auch auf Applikationsebene. Das gewährleistet eine hohe Verfügbarkeit Ihrer Dienste – auch bei gezielten Angriffen.

4 Next-Generation-Firewalls:

Setzen Sie moderne Firewalls mit intelligenter Bedrohungserkennung ein, um Anomalien frühzeitig zu erkennen und automatisiert auf Sicherheitsvorfälle zu reagieren.

… mittelfristig

5 Zero-Trust-Netzwerkarchitektur:

Entwickeln Sie Ihr Netzwerk hin zu einer Zero-Trust-Architektur und setzen Sie das Prinzip der minimalen Rechtevergabe (Least Privilege) konsequent um. Das verhindert unautorisierte Zugriffe und begrenzt potenzielle Schäden.

6 Disaster-Recovery-Strategien:

Erarbeiten Sie lückenlose Notfallhandbücher, führen Sie regelmäßige Wiederherstellungstests durch und setzen Sie auf automatisierte Orchestrierung, um im Ernstfall schnell und strukturiert reagieren zu können.

7 Network Access Control:

Integrieren Sie Lösungen zur Überprüfung und Kontrolle aller Geräte, die auf Ihr Netzwerk zugreifen. Dadurch erhalten nur autorisierte und sichere Endgeräte Zugriff.

ORBIT Gesellschaft für Applikations- und Informationssysteme mbH | mailing@orbit.de | www.orbit.de