SCALTEL

ZERO TRUST

IT-Risk Management

Powered by paloalto NETWORKS

Inhalte

Das IT-Risikomanagement ist ein wichtiger Schritt bei der Initiierung des Zero Trust Prozesses in Unternehmen. IT-Risikomanagement befasst sich mit der Identifizierung, Bewertung und Bewältigung von Risiken, die mit Informationstechnologie und den digitalen Aktivitäten eines Unternehmens verbunden sind. Diese Risiken können die Sicherheit, Verfügbarkeit und Integrität von IT-Systemen, Daten und Prozessen betreffen.

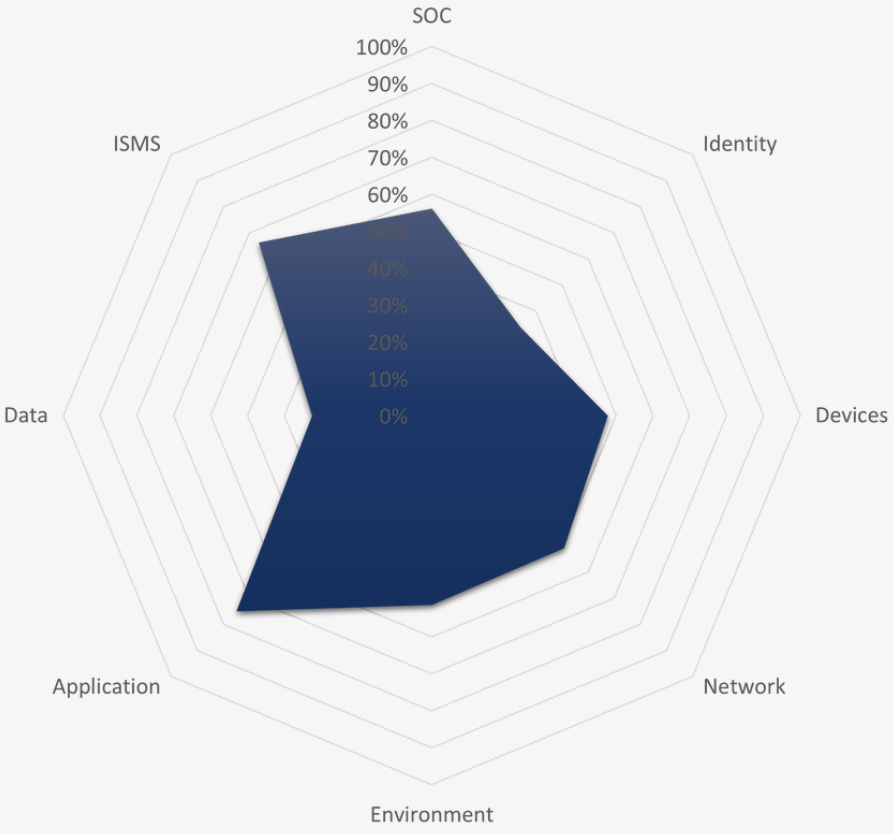
IT-Risk-Management

NIST Cyber Security Framework

IT-RISK-MANAGEMENT

Review Cyber Security Assessment

Die Analysen sämtlicher unserer durchgeführten Cybersecurity-Assessments (CSAs) zeigen, dass in Bezug auf das durchschnittliche Sicherheitsniveau noch erheblicher Optimierungsbedarf besteht. Unsere Ziel ist die Umsetzung und Implementierung einer funktionierenden Zero-Trust-Strategie.



Im Rahmen des IT-Risikomanagements liegt unser besonderes Augenmerk auf dem Sektor der Endgeräte (Devices) sowie auf der risikobasierten Klassifizierung. Es ist erkennbar, dass ein vertieftes Bewusstsein für diese Risikobereiche geschaffen werden muss und gleichzeitig die Kontrollmechanismen zur Risikoreduktion weiter ausgebaut werden müssen.

JOINT CYBERSECURITY ADVISORY

Die laut CISA und NSA zehn häufigsten Security-relevanten Fehlkonfigurationen bei IT-Systemen sind:

1. Default-Einstellungen bei Software oder Applikationen
2. Unzureichende Trennung von User- und Admin-Rechten
3. Unwirksames, internes Netzwerk-Monitoring
4. Keine Netzwerksegmentierung
5. Ungenügendes Patch Management
6. Nicht wirksame Zugangskontrollen
7. Schwache MFA-Methoden
8. Unzureichende Access Control Lists für Netzwerke und Services
9. Schlechte Passwort- beziehungsweise Zugangsdaten-Hygiene
10. Uneingeschränkte Möglichkeiten, Code auszuführen

> **Unter einem Risiko (im engeren Sinne) ist ein eventuelles, hinsichtlich seiner Eintrittswahrscheinlichkeit und Auswirkung bewertetes, zukünftiges Ereignis zu verstehen, das einen negativen Einfluss auf eine Organisation und ihre Handlung hat.**

DETAILGRAD RISIKOBENENNUNG

Um eine Risikobetrachtung durchzuführen, ist es nicht erforderlich, jede einzelne Ransomware zu kennen oder das gesamte Mitre Att&ck Framework vollständig zu durchforsten. Im Allgemeinen genügt es, zwischen dem Initial Access und dem Lateral Movement zu unterscheiden, um einen schnellen Einstieg in die Risiko-Awareness zu ermöglichen.

DETAILGRAD RISIKOKATEGORISIERUNG

Initial Access

Im IT-Risikomanagement bezeichnet "Initial Access" den ersten Punkt, an dem unautorisierte Personen in ein IT-System eindringen können. Es umfasst die Identifizierung, Bewertung und Absicherung dieser potenziellen Schwachstellen.

Lateral Movement

"Lateral Movement" bezieht sich dabei auf die Bewegung von Angreifern innerhalb eines Netzwerks, nachdem sie den Zugang erhalten haben. Es geht darum, Aktivitäten frühzeitig zu erkennen und zu stoppen.

NIST CYBER SECURITY FRAMEWORK

Unser NIST Cyber Security Framework ist unser Leitfaden, um passende Maßnahmen im IT-Risk-Management optimal ein- und durchführen zu können. Ein wichtiger Schritt, um Zero Trust im späteren Schritt erreichen zu können.

NIST Framework

Am Beispiel

Identify

- WIN10 Devices
- Internet Access + E-Mail-Client

Risiko 1: Initial Access
Risiko 2: Lateral Movement

Protect

- XDR Endpoint Security
- Internet-Policy
- Email-Policy
- Patch-Management
- NO-RDP (Makro-Segmentierung)
- Administration nur über Client-Admin-Account
- Mitarbeiter Awareness

Detect

- Security Event Management
- Erkennung Anomalie Verhalten
- Schwachstellen Management
- Segmentierung über interne Firewall
- Meldung Mitarbeiter IT-Hotline

Response

- SOC IR-Team bearbeitet Incident
- Automatische Host-Isolation
- Host ist administrierbar über XDR
- Erkenntnis über Eintrittspunkt und Umfang

Recover

- Löschen der Malware
- Re-Image des Clients
- Einspielen von Backups
- Recovery-Prozess

Powered by paloalto NETWORKS