



Ihr Partner, wenn es um
IT-Sicherheit und Datenschutz geht

Vulnerability Management Best Practices

Optionen nach Schwachstellen-Identifizierung:

- Patch installieren, sofern Fix vorhanden
- Monitoring, um Anfälligkeit zu reduzieren, sofern (noch) KEIN Fix vorhanden
- Risiko akzeptieren

Vulnerability Management Best Practices

Prozesse eines Vulnerability-Management-Programms:

1. Asset Management
2. Vulnerability-Identification
3. Vulnerability-Remediation (Patch-Management)
4. Erfolgs-Messung von Vulnerability-Management-Programm
5. KVP

Vulnerability Management Best Practices

1. Asset Management

- Risiko-Reduzierung durch Environment Visibility
- Know your Assets
 - OS
 - Applikation
 - Netzwerk
- ...um die Fähigkeit zu erlangen
 - Schwachstellen zu identifizieren
 - Schwachstellen zu priorisieren
 - Schwachstellen zu patchen (Patch-Management)
 - Reporting von Schwachstellen in Systemen und darauf laufender Software

Vulnerability Management Best Practices

2. Vulnerability-Identification

- Identifizierung der Schwachstellen (Schwachstellen-Scanner, Endpoint-Agents, Pentests usw.)
- Problem: Zeitlimit, Ressourcen, ständiger Wandel
→ daher unrealistisch, Schwachstellen (sofort) zu patchen, wann welche gefunden wurden
- Kritischer Aspekt in Vulnerability Management:
→ Priorisierung der Schwachstellen
→ ...aufgrund „whats actually exploited in the wild“
(Severity, CVSS Score, Malware/Exploit Exposure, Schwachstellen-Alter)
→ ... aufgrund Asset Kritikalität

Vulnerability Management Best Practices

3. Vulnerability-Remediation

- Identifizierung und Priorisierung von Schwachstellen ist wichtig
- Risiko-Reduzierung durch Problem-Behandlung
- Patch Management

Vulnerability Management Best Practices

3. Vulnerability-Remediation

- Patch Management
 - strategischer Prozess (kosteneffizient und sicherheitsfokussiert)
 - kein Bug-fixing ohne Berücksichtigung von Business-Impact
 - Abschätzen der Optionen (Bug-fixing, Risiko reduzieren, Risiko akzeptieren)
 - Test-Umgebung / Lab
 - Disaster Recovery

Vulnerability Management Best Practices

3. Vulnerability-Remediation

- Patch Management-Prozess
 - Asset Inventory (quartalsweise oder auf monatlicher Basis, um Visibility über OS, Applikationen, Netzwerkequipment, IoT usw. zu erhalten)
 - Standardisierung der Systeme und OS (beschleunigt den Patch-Prozess und gestaltet diesen effektiver)
 - Dokumentation der Security-Controls (entscheidend für Risikobehandlung und Business Impact)
 - Abgleich der Schwachstellen mit Inventory (Unterstützung bei Abschätzung über Business Impact)
 - Risiko-Klassifizierung und -Priorisierung
 - Testing / Lab / Validierung
 - Patch-Rollout
 - Progress-Tracking (Sicherstellung, dass Schwachstellen gefixt wurden)

Vulnerability Management Best Practices

4. Erfolgsmessung Vulnerability-Management-Programm

- Value add?
- RoI
- Executive Summary
- Trends

Vulnerability Management Best Practices

5. KVP

- Plan B (falls etwas schief geht)
- Dokumentation / Ticketing
- Lessons Learned

Vulnerability Management Best Practices



Sie haben Fragen?
Wir haben die Antworten!

hello@snapsec.at

+43-720-51-37-07

VORBEREITET ZU SEIN IST EINFACH, WENN MAN EINEN GUTEN PLAN HAT!

www.snapsec.at