

KEINE SCHWACHSTELLE BLEIBT UNENTDECKT

Ausgangssituation

- Ständig neue Bedrohungen, Schwachstellen werden nur sukzessive bekannt
- Maßnahmen für Identifikation und Behebung von Schwachstellen sind aufwendig
 - Regelmäßige Überprüfung mithilfe von Endpoints auf bekannte Schwachstellen
 - Nutzung der Schwachstellenanalyse zur Ergebnis-Korrelation im SIEM
 - Kritikalitätsprüfungen der Schwachstellen
 - Planung von Behebungsaktivitäten und Überwachung der Umsetzung (Patches)
 - Auswertung von Schwachstellen, Eskalation bei unzureichender Umsetzung

Lösungsansatz Vulnerability Management & CERT Service

- Regelmäßige Schwachstellenanalyse
- Unterstützung bei der Behebung

Leistungsumfang Vulnerability Management & CERT Service

- Inbetriebnahme des Endpoints zur Schwachstellenanalyse
- Aufnahme der Applikationen in die Überwachung (Linux & Windows, Server & Clients)
- Unterstützung bei Einbindung ins Netzwerk und Firewall-Freischaltung
- Regelmäßige, zufällig verteilte Scans über die Landschaft
- Wöchentliche Reports über identifizierte und nach Kritikalität kategorisierte Schwachstellen
- Empfehlung eines Zeitfensters bis zum Patch
- Aktives Tracking der identifizierten Schwachstellen
- Eskalation bei nicht gepatchten Schwachstellen
- Servicezeit von 08:00 bis 17:00 Uhr
- Hardware-Austausch vor Ort je nach Kritikalität zwischen vier Stunden und fünf Arbeitstagen



Organisatorische Sicherheitsmerkmale

- Analyse und Aufbereitung durch ständig geschulte Sicherheitsexperten der IS4IT
- Einsatz von renommierten Dienstleistern und Experten im Bereich Schwachstellenerkennung
- Zusammenarbeit mit mehreren international tätigen Cybersicherheitslaboren

Nutzen für den Kunden

- Keine Schwachstelle kann im Unternehmen dauerhaft unentdeckt bleiben
- Zeitgerechte Behebung sichergestellt
- Minimales Risiko, dass bekannte Schwachstellen ausgenutzt werden

MANAGED SERVICES ENTLASTEN IHR TEAM

Ausgangssituation

- Bedrohungslage nimmt ständig zu und wird immer aggressiver
- Neue Regularien und Gesetze (EU-DSGVO, KRITIS etc.)
- Strafen drohen – Bußgelder bis zu 4 % des Umsatzes bzw. bis zu 20 Mio. Euro
- Kronjuwelen des Unternehmens bewerten und schützen
- Security-Analysten und Forensik-Experten sind teuer

Lösungsansatz Managed SOC

- Security-Analysten betreuen mehrere Unternehmen parallel
- Optimale Infrastrukturnutzung □ Mandantenfähigkeit und virtuelle Server

Leistungsumfang Managed SOC

- | | |
|----------------|----------------------------|
| ■ SIEM Service | ■ E-Mail-Service |
| ■ SOAR Service | ■ Vulnerability Management |
| ■ IPPL | ■ Endpoint Service |
| | ■ Network Security Service |



Warum Informationssicherheit mit IS4IT?

- Schneller Return on Investment
- Klare Aufgabentrennung zwischen Betrieb und Sicherheit

Nutzen für den Kunden

- Monatlicher Festpreis, halbjährige Kündigungsfrist,
- Mindestlaufzeit von 12 oder 36 Monaten
- Rechtlich abgesicherte Sicherheitskonzepte und revisionssichere Datenhaltung

