Net at Work
Building IT-Excellence.

SECURITY
ASSESSMENT

Net at Work Security Assessment

Erhöhen Sie mit konkreten Maßnahmen das Sicherheitslevel Ihrer Umgebung.

Im Security Assessment identifizieren wir Schwachstellen und Sicherheitslücken in Ihrem Unternehmen. Wir geben Ihnen eine Übersicht über die notwendigen Schritte zur Erhöhung des Security Reifegrades.

Schwachstellen & Sicherheitslücken erkennen

Wir stellen Ihre Umgebung mithilfe eines maschinellen Scans auf den Prüfstand und decken Schwachstellen sowie Sicherheitslücken auf.

Individuelle und umfangreiche Bewertung

Wir fokussieren uns dabei nicht nur auf technische Konfigurationen sondern auch auf den Datenbestand sowie organisatorische Prozesse und Regelungen.

Konkrete Schritte zur Erhöhung des Reifegrads

Nach der Prüfung erhalten Sie die Ergebnisse und wir präsentieren Ihnen die notwendigen Schritte zur Erhöhung des Reifegrads.

Das Security Assessment dient zur Einordnung des Security Reifegrades Ihres Unternehmens. Dabei werden sowohl technische Konfigurationen als auch der Datenbestand und organisatorische Prozesse und Regelungen bewertet.

Zur Identifizierung von Schwachstellen und Sicherheitslücken führen wir einen maschinellen Scan durch, der folgende Punkte betrachtet:

On-Premises Endpoints
- Server
- Clients
- Netzwerkgeräte

On-Premises-Services
- Active Directory
- Email DNS Spoofing Protection
- SharePoint
- FileServer

Cloud Services
- Entra ID
- Azure
- Microsoft 365 Dienste
- Intune
- Google Workspace

Ablauf des Security Assessments

Das Security Assessment beginnt mit einem Kick-Off-Call, in dem wir das Tool für den Scan Ihrer Umgebung installieren und konfigurieren. Darüber hinaus erhalten Sie von uns einen Fragebogen für die Erhebung der Ist-Situation. Mit Hilfe dieses Fragebogens sammeln wir Informationen zur Organisation und zu Prozessen im Bereich IT-Sicherheit, um eine Einordnung in das Reifegrad-Modell vornehmen zu können. Die Fragen richten sich nach den CIS Controls und decken unter anderem die Bereiche „Access Control Management“ und „Security Awareness and Skill Training“ ab. Beim Thema „Access Control Management“ geht es um die Organisation der Berechtigungsvergabe in Ihrer Umgebung und den Einsatz von Multi-Faktor-Authentifizierung. Im Bereich „Security Awareness and Skill Training“ geht es beispielsweise um etablierte Prozesse zur Mitarbeiter-Sensibilisierung.

Anschließend läuft der Scan etwa drei bis vier Wochen, ehe wir den Report finalisieren und präsentieren. Wir geben Ihnen bei der Auswertung der Ergebnisse konkrete Maßnahmen an die Hand, mit denen Sie den Security Reifegrad in Ihrem Unternehmen erhöhen. Die Bewertung und Priorisierung nehmen wir nach allgemeinen Best Practices vor. Dabei fließen auch die folgenden Faktoren ein: Empfehlungen vom Center for Internet Security (CIS), Prinzipen der Zero Trust Sicherheitsarchitektur (ZTA) und Schlüsselaktivitäten gegen Rapid Cyberattacks.

Vorgehen im Detail

Tag 1

- Technischer Kick-Off-Call
- Übermittlung des Fragebogens
- Einrichtung des Scans

Tag 2

- Download des Rohberichts
- Finalisierung des Reports
- Präsentation des Reports

Tag 3

- Präsentation der Ergebnisse
- konkrete Maßnahmen zur Erhöhung des Security-Reifegrades

3 Wochen

- maschineller Scan
- Faktenerhebung

Net at Work Security Assessment

- ✓ Schwachstellen und Sicherheitslücken erkennen
- ✓ Individuelle und umfang-reiche Bewertung
- ✓ Konkrete Schritte zur Erhöhung des Reifegrads

Jetzt Angebot anfragen!