IT-SICHERHEITS-ANALYSE

Im Rahmen der Analyse soll dem Unternehmen die Möglichkeit gegeben werden, den eigenen Stand der IT-Sicherheit besser einzuschätzen und Bereiche mit Verbesserungspotential zu erkennen.

Darüber hinaus sollen die Ergebnisse dazu dienen, dem Versicherer eine Risikoeinordnung des zukünftigen Kunden zu ermöglichen.

ABLAUF

Die Analyse findet in Form eines ausführlichen Interviews mit den jeweiligen Fachleuten des Unternehmens statt. Der Zeitbedarf liegt bei ca. 2-3 Stunden.

Im Rahmen des Interviews werden wir uns zunächst gemeinsam einen Überblick hinsichtlich der Netzwerkstruktur verschaffen und dann einen Fragenkatalog auf Grundlage aktueller IT-Sicherheits- und Datenschutzstandards (ISO27000, DSGVO, BSI Grundschutz) abarbeiten. Die Fragen ergeben sich dabei aus den folgenden Themenbereichen:

- Organisation der IT-Sicherheit (Verantwortliche, Richtlinien, Notfallpläne, etc.)
- Management externer Dienstleister (SLAs, Auftragsdatenverarbeitung, etc.)
- Mitarbeitende (Schulung Awareness)
- Inventarisierung (Soft-/Hardware)
- Physische Sicherheit (Serverräume, Datenverteiler, etc.)
- Umgang mit Daten (Klassifizierung von Daten, Datenschutz, Löschung von Daten)
- Identitätsmanagement (Rechtekonzept, Passwortrichtlinie, Ablauf von Benutzerkonten, etc.)
- Netzwerksicherheit (Segmentierung, NAC, Gästenetz)
- Absicherung der IT-Systeme (IDS, IPS, DLP, Antivirus, Endpoint Security etc.)
- Schwachstellenmanagement (Patchmanagement, Altsysteme, Schwachstellenscans)

VORBEREITUNG

Um einen möglichst reibungslosen Ablauf zu gewährleisten sollten die folgen Unterlagen im Vorfeld bereitgestellt werden:

- Grafische Übersicht Netzwerkstruktur (Netzwerksegmentierung, Netzwerkübergänge etc.)
- Vorhandene Leitlinien und Richtlinien
- Organigramm der Verantwortlichkeiten
- Übersicht über externe Dienstleister bzw. Abhängigkeiten

NW Assekuranz
Global Insurance Broking

OPTIONEN FÜR DAS WEITERE VORGEHEN

SCHWACHSTELLENSCAN

- Naturgemäß kann eine Analyse in Form eines Interviews nur in begrenztem Umfang den realen Stand der IT- bzw. Netzwerksicherheit einer Infrastruktur abbilden.
- Angreifer dringen heute i. d. R. per Social Engineering in Unternehmensnetze ein und nutzen dann Schwachstellen im Unternehmensnetzwerk aus, um sich auszubreiten.
- Sogenannte Penetration-Tests von außen sind zur Identifizierung solcher Lücken nicht zielführend.
- Um hier weitere Klarheit zu gewinnen, bieten wir die Durchführung eines Schwachstellenscans an. Hierzu wird ein Appliance im Unternehmensnetz platziert, die über einen längeren Zeitraum (ca. zwei Wochen) Schwachstellen-scans aller erreichbaren Geräte durchführt. Ziel ist es, alle Sicherheitslücken im IT-Netzwerk aufzuspüren, bevor ein Angreifer die Lücke ausnutzen kann.

RESTART NACH EINEM CYBERANGRIFF

- Nach einem Cyberangriff ist der Faktor Zeit i. d. R. das entscheidende Element zur Schadensbegrenzung.
- Je besser die Vorbereitung ist, desto schneller ist das Unternehmen wieder arbeitsfähig.
- Gerne unterstützen wir auch bei der Ausarbeitung eines tragfähigen Konzeptes zum Wiederanlauf der IT-Infrastruktur nach einem Cyber-Vorfall.

KONTAKT

T: +49 (0)421 989607-332
cyber@nw-assekuranz.de
www.nw-assekuranz.de

Nordwest Assekuranzmakler GmbH & Co. KG
Herrlichkeit 5 – 6
28199 Bremen

NW Assekuranz
Global Insurance Broking