RWT

Cyber Security Checks

Risiko- und Schwachstellenanalyse · Risikoeinschätzung und Handlungsempfehlungen · Mitarbeiter Awareness

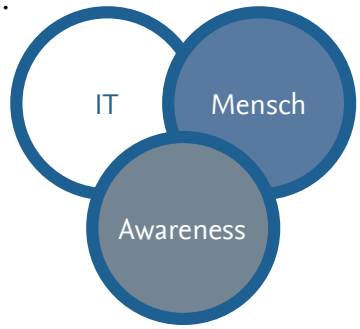
RWT – *besser beraten*

Global presence through Crowe

RWT

Cyber Security erfordert eine Betrachtung sämtlicher für eine maximale Sicherheit relevanter Rahmenbedingungen im Unternehmen:

- technisch
- organisatorisch
- infrastrukturell
- physisch
- personell



Die in unseren Cyber Security Checks geplanten Maßnahmen zur Cyber Sicherheit umfassen, für ein nachhaltiges Sicherheitsbewusstsein, alle Ebenen der Unternehmensstruktur. Die Umsetzung erfolgt in Anlehnung an die BSI/ISO27001 Standards:

- Netzwerkpenetrationstests
- Datenschutz- und DSGVO-Audit-Services (DSGVO)
- Netzwerkinfrastruktur-Audits
- Penetrationstests für Web-Applikationen
- ISO-Consulting und ISO-Audit
- Beratung für Netzwerksicherheits-Audits
- Business Continuity Management
- Identitäts- und Zugriffsmanagementdienste (IAMS)
- IT/Datenschutz Schulung und Sensibilisierung
- Digital Forensic und Incident Response
- Managed Security Services

Unser Vorgehen

Wir ermitteln den IST-Zustand durch Check des First-View Sicherheitslevel und führen einen Zertifizierungscheck (BSI/ISO) durch. Danach definieren wir den SOLL-Zustand und klären welchen Level an Sicherheit Sie mit welchem Aufwand und Budget erreichen wollen. Bei Bedarf unterstützen wir Ihre Cyber-Security-Strategie durch Implementierung eines Netzwerk-Monitorings (NSM), unterstützt von einem IDS (Intrusion Detection System) und einem IPS (Intrusion Prevention System).

Bei einer ersten Risikobewertung identifizieren wir die möglichen Angriffsvektoren und skizzieren den Schaden im Eintrittsfall.

Auf technischer Ebene ermitteln wir die Patchkultur und klassifizieren den aktuellen Patchlevel.

Sicherheitsrisiken bewerten wir sukzessive nach Ihrer Priorisierung in der Risikobewertung und listen Handlungsoptionen auf.

Grundsätzlich führen wir auch Penetrationstests der IT-Infrastruktur und der im Unternehmen eingesetzten Applikationen durch. Denn gerade die Internet-faced Web-Applikationen liegen bei Hackern im Focus als Eintrittstor zum Unternehmensnetzwerk.

Parallel zu den technischen Maßnahmen legen wir ein Augenmerk auf die physische Gebäudesicherheit. Die „physische“ Schwachstelle für das Eindringen in ein Firmengebäude stellt nicht der Pförtner oder geschulte Empfangsmitarbeiter dar, sondern der freundliche Mitarbeiter, welcher dem scheinbaren Lieferanten oder vermeintlichen Kollegen die Tür aufhält. Die Angreifer werden besonders kreativ wenn sie an einer soliden Netzwerktechnik scheitern.

Aus dem IST-Zustand ergeben sich die technischen und organisatorischen Prüfungselemente. Diese sind von elementarer Bedeutung da der IST-Zustand einmalig ermittelt und mit den Zwischenstufen bis zum angestrebten SOLL-Zustand verglichen wird.

Der IST-Zustand dient zudem als Grundlage für einen Awareness-Maßnahmenplan. Hierbei stellen Mitarbeiterschulungen nur eine Maßnahme dar. Die Mitarbeiter-Awareness muss im ständigen Fokus und mit regelmäßiger Überprüfung im Unternehmen implementiert sein. Das Bewusstsein für IT-Sicherheit und Datenschutz wird mit Webinaren, CBTs oder eTrainings in den Regelbetrieb integriert. Unterstützt wird der Maßnahmenplan mit unregelmäßigen Phishing- und Spear-Phising-Kampagnen.

Die Modellierung von Sicherheitsmaßnahmen gemäß dem ISIS12 Katalog (aus dem BSI-Grundschutzkatalog und ISO/IEC 27001/2 Standard abgeleitet) sollte Ihr langfristiges Gesamtziel sein.

Die hier empfohlenen Maßnahmen, welche durch regelmäßige Revision in der Unternehmenspraxis durchgesetzt werden, münden in einem über alle Unternehmensebenen durchgängig hohen Sicherheitsniveau.

Cyber Security Checks (Beispiele)

Cyber Security *Basis* Check	4.500,00 Euro*
Cyber Security – IST und SOLL Zustandsermittlung / Maßnahmenplanung / Evaluierung • Informationen sammeln, Dokumentationen (IT Assets wie Hardware, Software, Firewall, Network Devices, IP-Adressenpool usw.), Datenschutz,- und Backupkonzepte • Zieldefinition/Abstimmung mit der Leitung IT / IT-Security • Evaluierung/Analyse auf Basis der gesammelten Daten (quantitativ/qualitativ)	2 Manntage
Mitarbeiter Awareness • Sensibilisierung Ihrer Mitarbeiter durch Präsenz- oder Online-Trainings (mögliche Themen: Passwort-Sicherheit, Betrugsversuche durch Phishing Mails, Social Engineering, Datenmanagement und Datenschutz, BYOD in Unternehmen, Sicherheit von mobilen Geräte)	1 Manntag
Basis Schwachstellenanalyse Ihrer IT-Infrastruktur • Schwachstellenanalyse mittels Infrastruktur und APP Penetrationstests (WLAN-Netzwerk Sicherheit / Portscans, Datenbank-Check, Malware und Ransomware Deep Inspection) • Optional: OWASP10 Web-App Scans	1 Manntag

Cyber Security Check *Pro*	10.125,00 Euro*
Cyber Security – IST und SOLL Zustandsermittlung / Maßnahmenplanung / Evaluierung	2 Manntage
Mitarbeiter Awareness	2 Manntage
Basis Infrastruktur und APP Penetrationstests	3 Manntage
Physischer Penetrationstest • Hybride physische Sicherheitsprüfung von Zentrale, Mitarbeiter-Büros, Produktions- und Betriebsstätten im Hinblick auf Verbesserungsmöglichkeiten von Mitarbeitern in der Umsetzung ihrer Sorgfaltspflicht, Barrierechecks der klassischen Objektsicherung wie Schlösser, Fenster, Einbruchsalarme, Sensoren und Kamerasysteme	2 Manntage

Cyber Security Check Pro *Plus*	20.125,00 Euro*
Cyber Security – IST und SOLL Zustandsermittlung / Maßnahmenplanung / Evaluierung	2 Manntage
Mitarbeiter Awareness	2 Manntage
Unfangreiche Infrastruktur und APP Penetrationstests	4 Manntage
Physischer Penetrationstest	2 Manntage
Implementierung eines ISIS12 (Sicherheitsmanagementsystem speziell für KMU), Phase 1: Initialisierung und Overhead • Erstellung von Informationssicherheitszielen und Leitlinien, Mitarbeitersensibilisierung, Ernennung und Schulung von Informationssicherheits- und Datenschutzbeauftragten, Gesamtmaßnahmen- und Projektplanung für Step 3-12 eines ISIS12	8 Manntage

* Preise zzgl. USt

RWT

Kontakt

Rafael Gawenda
Geschäftsführer

T +49 711 319 400 138
rafael.gawenda@rwt-gruppe.de

Dirk Peter
Head of Cyber Security

T +49 711 319 400 144
dirk.peter@rwt-gruppe.de

rwt@rwt-gruppe.de
www.rwt-gruppe.de

Standorte

Reutlingen
Charlottenstraße 45 - 51
72764 Reutlingen
+49 7121 489-201

Stuttgart
Olgastraße 86
70180 Stuttgart
+49 711 319400-00

Albstadt
Schmiechastraße 72
72458 Albstadt
+49 7431 1326-0