Offensive Security

Die Risiken und Bedrohungen im Bereich der Cyber Security sind vielfältig und reichen von technischen Sicherheitslücken über mangelhaft implementierte Sicherheitsmaßnahmen bis hin zu einfachen Bedienungsfehlern oder Unachtsamkeiten von User:innen. Bei Cyber-Angriffen werden diese Schwachstellen gezielt ausgenutzt. Die Motivation von Cyber-Kriminellen ist dabei sehr vielfältig und reicht von Identitätsbetrug („Fake President Fraud“) über Datendiebstahl bis hin zu Erpressungsfällen („Krypto Locker“).

Unter offensiven Sicherheitsmaßnahmen (Offensive Security) versteht CERTAINITY das präventive Aufdecken von vorhandenen Sicherheitslücken in IT-Systemen, Netzwerken und Anwendungen. Durch proaktiv durchgeführte und simulierte Angriffe erfolgt eine gründliche Untersuchung der Strukturen auf Sicherheitsprobleme und Schwachstellen. Das Expert:innenteam von CERTAINITY nutzt dabei Techniken, Tools und Vorgehensweisen, wie man sie aus tatsächlichen Cyber-Angriffen kennt. Auf Basis der aufgedeckten Sicherheitsprobleme werden individuelle Lösungsempfehlungen erarbeitet, mit denen die IT-Sicherheit einer Organisation nachhaltig erhöht werden kann.

Das OffensivePlus⁺ Angebot von CERTAINITY für KMU gliedert sich in vier Basismodule, die wichtig für die Cyber-Versicherung sind:

Extern

Kontrollierter Cyber-Angriff (Penetrationstest) auf alle Systeme, die über das Internet erreichbar sind. Mit dieser Maßnahme können Sicherheitslücken und Cyber-Risiken identifiziert werden.

Phishing Simulation

Simulation eines Phishing-Angriffs. Ziel ist es, die Sensibilität für Phishing-Risiken zu schärfen und das Sicherheitsbewusstsein der eigenen Mitarbeiter:innen zu stärken.

Intern

Kontrollierter Cyber-Angriff (Penetrationstest) innerhalb des eigenen Netzwerks. Mit dieser Maßnahme können Sicherheitslücken und Cyber-Risiken identifiziert werden.

Active Directory

Überprüfung der Einstellungen und Konfiguration des Active Directory-Verzeichnisdienstes. Neben den lokalen Sicherheitseinstellungen wird auch die Passwortqualität geprüft.

CERTAINITY. Cyber Security Specialists.
reliable. trustworthy. bespoke.

CERTAINITY

Cyber Security Specialists.
Wir unterstützen unsere Kunden dabei, ihre Informationssicherheit nachhaltig zu verbessern und ihr Kerngeschäft abzusichern.

reliable.
Als zuverlässiger Partner sind wir für unsere Kunden da, bis wir die Herausforderungen gemeinsam gelöst haben.

trustworthy.
Wir leben Cyber Security.
Die Informationen von und über unsere Kunden stehen im Zentrum unserer Sicherheitsvorkehrungen.

bespoke.
Wir bieten Beratungsleistungen an, die auf unsere Kunden und ihre jeweilige Situation zugeschnitten sind. Damit schaffen wir echten Mehrwert.

CERTAINITY GmbH
sales@certainity.com

www.certainity.com

Neben dem Basisangebot OffensivePlus⁺ bietet CERTAINITY ein breites Portfolio an individuellen und maßgeschneiderten Beratungsleistungen rund um das Thema Cyber-Sicherheit.

Security Assessment auf Anwendungen

Anwendungen und mobile Apps stellen das Bindeglied zwischen Daten und Benutzer:innen dar. Sie verbinden diese Welten und ermöglichen Benutzer:innen den Umgang mit Daten. Sichere Software-Anwendungen (z. B. ERP, Webshop, ...) sind ein relevanter Faktor für den Unternehmenserfolg und sollten in regelmäßigen Abständen überprüft werden.

Red Team Engagement

Unternehmen mit hohem Security-Reifegrad nutzen Red Team Engagements, um die Wirksamkeit vorhandener Schutzmaßnahmen & Investitionen zu prüfen, und das Blue Team (SOC) zu trainieren. Dabei wird ein Angriff auf allen Ebenen simuliert. Im Gegensatz zu einem reinen Penetrationstest werden Schwachstellen auf allen Ebenen einer Organisation genutzt, um weiter in das Unternehmensnetzwerk vorzudringen.

Haben wir Ihr Interesse geweckt?

Melden Sie sich bei uns unter:

Theresa Mosing
Head of Sales
T +43 664 962 39 32
theresa.mosing@certainity.com

Fabian Mittermair
Head of Offensive Security
T +43 664 883 80 537
fabian.mittermair@certainity.com

Incident Response Hotline

T (D-A-CH): 0800 44 30 555
csirt@certainity.com