ALTERSOLUTIONS DEUTSCHLAND

Cyber Security

Network Penetration Testing

Network Penetration Testing (intern/extern)

Die Relevanz eines sicheren und stabilen IT-Netzwerks wird aufgrund der stetig steigenden Maße von Cyber Attacken immer wichtiger. Cyber Kriminelle haben es nicht selten auf wichtige Produktionslinien oder zentrale IT-Systeme abgesehen, deren Stillstand bzw. Ausfall immensen Schaden anrichten kann. Der ungeplante Stopp von Produktionseinrichtungen kann zu immensen finanziellen Belastungen führen; der Ausfall von relevanten IT-Systemen kann - je nach Umfeld, bspw. im Gesundheitswesen – sogar eine Gefahr für Leib und Leben bedeuten. Um eine möglichst hohe Ausfallsicherheit zu erlangen und das eigene Sicherheitsniveau zu optimieren, bedarf es einer Vielzahl von Präventivmaßnahmen in Bezug auf die betrieblichen Abläufe, die IT-Sicherheit sowie die begleitenden IT-Prozesse. Eine zentrale Maßnahme ist die Durchleuchtung des gesamten Unternehmensnetzwerks auf Schwachstellen mittels des Network Penentration Testing.

Wir unterstützen

Unsere Leistungen und Vorgehensweisen im Bereich des internen und externen Network Penetration Testing
Wir unterstützen unsere Kunden mit der Simulation zweier Angriffsvektoren:

Externes Penetration Testing: Hierbei simulieren wir eine reale Cyber Attacke, indem wir vergleichbare Tools, Methoden und Vorgehensweisen nutzen, um von außen in die IT-Systeme unserer Kunden einzudringen, die auch von Cyber Kriminellen angewandt werden (u.a. gemäß standardisierter Methodik OWASP). Unser Ziel besteht darin, die Schwachstellen in IT-Systemen im Voraus zu identifizieren und zielgerichtete Handlungsempfehlungen auszusprechen, um das Risiko eines realen Angriffs zu minimieren. Im Rahmen eines externen Network Penetrationstests versuchen wir den Zugang zu so vielen kritischen Systemen wie möglich zu erlangen.

I**nternes Penetration Testing**: Bei einem internen Network Penetrationtest simulieren wir den unternehmensinternen Angriff (etwa durch einen IT-Mitarbeiter, IT-Administrator oder Geschäftspartner mit entsprechender Motivation). Auch bei dieser Testing Methoden setzen wir auf vergleichbare Tools, Methoden und Vorgehensweisen, die Cyber Kriminelle nutzen (u.a. gemäß standardisierter Methodik OWASP). Darüber hinaus besteht die Option, unsere Tests zu vertiefen und auszubreiten und unsere Experten mit immer mehr „internem Wissen“ auszustatten.

Unsere Network Penetrationtests bieten wir in den Verfahren Black-Box-, Grey-Box- und/oder White-Box-Testing an. Dabei wird jeder unserer Penetrationtests nach den folgenden methodischen Schritten umgesetzt:

- ***Aufklärung & Untersuchung***: Sammlung von Informationen und Identifikation sensibler Daten zur Anwendung
- ***Scan & Aufzählung***: manuelles und automatisiertes Scannen der Anwendung hinsichtlich Schwachstellen
- ***Angriff & Ausnutzung***: Durchführung kontrollierter Angriffe auf die Anwendung
- ***Zugriff & Dokumentation***: Zugriff auf sensible Daten der Applikation und Dokumentation unseres Handelns
- ***Report & Präsentation***: Erstellung und Vorstellung des Ergebnis-Reports für Management und Techniker

Ihr Mehrwert

Mehr Sicherheit für Ihre IT-Netzwerke

- Umfassende Aufdeckung von Schwachstellen mittels manueller und automatisierter Verfahren
- Objektive Bewertung der spezifischen Wirksamkeit vorhandener IT-Schutzmaßnahmen
- Erarbeitung individueller Handlungsempfehlung zu technischen, organisatorischen und prozessualen IT-Schutzmaßnahmen
- Explizite Steigerung des Sicherheitsniveaus von Systemen und Applikationen
- Kosteneinsparung aufgrund der präventiven Wirkung von Penentrationstests