Penetration Testing

Schutz und Sicherheit durch die gezielte Identifikation von Sicherheitslücken und Fehlkonfigurationen

In den Medien vergeht kaum ein Tag, an dem nicht über gezielte, erfolgreiche Hackerangriffe auf Industrie und Handel oder auf Kommunen und Versorger sowie die damit verbundenen Herausforderungen berichtet wird.

Der Schutz von Netzwerken, Computer-Systemen und sensiblen Daten hat für alle Unternehmen höchste Priorität. Es ist Zeit zu Handeln!

Bei vielen dieser Angriffe werden sensible Kundendaten oder kritische Informationen entwendet, wichtige IT-Systeme werden manipuliert oder verschlüsselt, hohe Geldsummen werden gefordert.

Einen wesentlichen Baustein in diesem Kontext bilden Penetrationstests. Denn sie tragen durch eine umfassende Sicherheitsprüfung von IT-Systemen und Netzwerken dazu bei, Schwachstellen nicht nur zu identifizieren, sondern sie tragen dazu bei, diese auch erfolgreich zu schließen.

Ein Penetrationstest umfasst neben dem Erkennen von Sicherheitslücken auch die Überprüfung bereits implementierter Schutzmaßnahmen

Mit einem professionellen Penetrationstest simulieren wir einen tatsächlichen Angriff auf die Infrastruktur unserer Kunden. Dabei können Kunden zwischen verschiedenen Ausprägungen wie z.B. dem Blackbox Penetrationstest (keine Offenlegung von Login-Daten oder Systeminformationen) oder dem Whitebox Penetrationstesting (Offenlegung von Systeminformationen und Login) wählen. Auch Mischformen sind denkbar.

Härtung der Widerstandsfähigkeit der Systeme

Unsere Cyber Security Consultants führen Penetrationstest nach Stand der Technik, etwa dem OWASP Standard, und nach Empfehlungen des BSI durch. Selbstverständlich werden alle Prüfschritte protokolliert und in Abschlussberichten als Nachweis gegenüber Dritten dokumentiert. Im Rahmen eines Abschlussgesprächs werden nach erfolgter Durchführung dann die Ergebnisse und Erkenntnisse vorgestellt. Außerdem erhalten unsere Kunden mit dem ausführlichen Bericht über mögliche Findings auch einen empfohlenen Maßnahmenkatalog zur Härtung der IT-Infrastruktur.

IHRE VORTEILE

- Sicherheitslücken identifizieren
- Sicherheitslücken schließen
- Messbarkeit der Informationssicherheit
- Schutzmaßnahmen ausbauen und Widerstandsfähigkeit erhöhen
- Sicherheitsprozesse implementieren
- Erhöhung des Security-Levels
- Angepasstes Reporting für ISMS
- Entwicklung von Grundlagen der IT-Strategie

OEDIV SecuSys GmbH
Brückenweg 5 | 18146 Rostock | **www.secusys.de**

Info@secusys.de

+49 381 37573-0