Sicher?
Sicher!

IT-Sicherheit und Penetration Tests

GRUNDIG
Business Systems

IT-Sicherheit

Cyber-Attacken

Das Internet bietet viele Möglichkeiten, birgt aber auch eine Menge Risiken. Mit zunehmender Vernetzung wird die Angriffsfläche für Cyber-Angriffe immer größer.
Die Zahl der größtenteils automatisierten Cyber-Attacken auf Unternehmen ist in den letzten Jahren enorm gestiegen. Durch unzureichend geschützte Systeme können den Unternehmen Schäden in Millionenhöhe entstehen, werden dabei auch noch sensible Daten ausgespäht, drohen zusätzlich strafrechtliche Konsequenzen.

Wir helfen Ihnen, sich gegen Cyber-Attacken, Industrie-Spionage und Denial of Service-Angriffe effektiv zu schützen!

Penetration-Tests

Die zunehmende Digitalisierung und ein oft unzureichender Schutz der IT bieten der Cyber-Kriminalität immer mehr Möglichkeiten. Mit Hilfe von Penetration Tests betrachten wir Ihre IT-Landschaft aus der Perspektive von Angreifern, um so eventuelle Schwachstellen aufzuspüren und alle Sicherheitslücken zu schließen.

- Penetration Tests der internen Systeme: Überprüfung Ihrer Anwendungen (mobile, Desktop, Web) und deren Anbindungen zur Sicherheit Ihrer Daten.
- Penetration Tests der externen Systeme: Überprüfung Ihrer über das Internet erreichbaren Strukturen (Mailserver, VPNs, Clouds) auf mögliche Eintrittspforten.

Unsere Leistungen

Ein Penetration Test dient dazu, mögliche Schwachstellen Ihrer IT-Systeme zu identifizieren. Im Zuge dieser Tests arbeiten wir mit Mitteln, die reale Angreifer ebenfalls verwenden. Wir testen beispielsweise auf angreifbare Konfigurationen und Härtungen sowie veraltete Software bis hin zum Versuch physisch in Ihr Netzwerk einzudringen. Nach Abschluss der Tests erhalten Sie eine ausführliche Dokumentation mit allen gefunden Schwachstellen sowie ein Konzept mit konkreten Schritten zur Schließung der Schwachstellen.

Zu den Leistungen gehören die Prüfung folgender Komponenten:

- Server
- Mailserver
- Webserver
- WLAN
- Active Directory
- Netzwerkgeräte (NAS/ Switch/Router/Firewall/ IoT- Geräte)
- Software

Social Engineering

Auch menschliches Fehlverhalten oder misslungene Software-Updates können Cyber-Angriffen Tür und Tor öffnen. Die entsprechende Sensibilisierung Ihrer Mitarbeiter minimiert diese Risiken, wie beispielsweise Phishing-Angriffe rechtzeitig zu identifizieren.

Audits

Ihre IT-Struktur entwickelt sich ständig weiter. Änderungen, Erweiterungen, neue Software, Updates – es gibt keinen Ist-Zustand. Deshalb ist eine ständige Überprüfung und Verbesserung Ihrer IT-Security-Landschaft notwendig.

Beratung

Wir geben unser Wissen gerne an Sie weiter und begleiten Sie auf dem Weg zu einer sicheren IT-Infrastruktur. Profitieren Sie von unserem Know-how, zu Ihrer Sicherheit und der Ihres Unternehmens.

HNE 6497/08.2022

it-service.grundig-gbs.com · it-service@grundig-gbs.com
Infoline: +49 (0) 921-898-200