Penetrationstest

Ein Penetrationstest ist ein Sicherheitstest für IT-Systeme und Netzwerkkomponenten im laufenden Betrieb. Wir identifizieren Sicherheitslücken, die bei einem Cyber-Angriff ausgenutzt werden könnten. Der Test wird manuell ausgeführt. Er umfasst alle geschäftlichen Bereiche oder Teilbereiche, die von der IT unterstützt werden und schließt IT-Systeme, Netzwerkkomponenten, Services und Web-Anwendungen mit ein.

Unsere Testmethode folgt dem Paradigma des Ethischen Hackers. Wir nutzen die gleichen technischen Mittel wir ein Hacker. Denn wenn Sie Ihr Unternehmen schützen wollen, müssen sie die Angriffsszenarien der Hacker kennen.

Ergebnis

Als Ergebnis des Penetrationstests erhalten Sie einen Testbericht mit den Testergebnissen.

- Welche Sicherheitslücken hat der Test aufgedeckt?
- Wie hoch ist das Risiko eines Cyber-Angriffs durch diese Lücken?
- Welche Sicherheitslücken sind so risikoreich, dass sie möglichst bald geschlossen werden sollten?

In einem Maßnahmenkatalog werden in dem Bericht die Schritte für eine Korrektur vorgeschlagen. Dabei stehen die Maßnahmen für die risikoreichsten Sicherheitslücken im Ranking ganz oben.

Penetrationstests sind ein sehr gutes Mittel, das Niveau der IT-Sicherheit zu erhöhen.

Garantie

Wir garantieren Ihnen, daß wir alle erhobenen Daten streng vertraulich behandlen. Es werden keine Daten an Dritte weitergegeben oder in irgendeiner Form außerhalb des Penetrationstests verwendet.

Das könnte Sie auch interessieren:

[Was genau ist ein Penetrationstest?]

[Wir bieten einen Penetrationstest speziell für Web-Anwendungen an.]

[Wir bieten einen Penetrationstest speziell für Breitbandrouter an.]