iMes IT-Security

IT-Penetrationstest vs. IT-Schwachstellenanalyse

Zentrale Aspekte von Schwachstellenanalyse
und IT-Penetrationstests

Ein nachhaltiges **IT-Sicherheitskonzept** beinhaltet sowohl die **Schwachstellenanalyse** als auch den **IT-Penetrationstest**. Doch in welchen Aspekten unterscheiden sich die **Schwachstellenanalyse** und der **Penetrationstest**?

Technische Security-Analysen und Penetrationstests sind feste Bestandteile einer effektiven IT-Sicherheitsstrategie. Das Ziel hierbei ist es Schwachstellen in den **IT-Netzwerken** und Systemen zu finden bevor Cyber-Kriminelle eventuelle Sicherheitslücken nutzen können. **Schwachstellenanalysen** und **Penetrationstests** werden häufig im selben Atemzug genannt, unterscheiden sich aber in einigen wichtigen Punkten.

Der **iMes Penetrations-test** stellt einen simulierten Eindring-versuch in Computer-netzwerke dar – der **iMes Penetrationstest** deckt Sicherheitslücken und Schwachstellen auf und garantiert so die nachhaltige Sicherheit Ihrer Systeme und Netzwerke.

Zentral Aspekte:

- Schutz von Firmengeheimnissen
- Aufdecken von Sicherheitslücken in Ihrem Computersystem
- Erhöhung der Sicherheit auf technischer und organisatorischer Ebene
- Erarbeitung optimaler Lösungsansätze

IT-Schwachstellenanalyse:

- Nicht klar abgrenzbarer Begriff
- **Schwachstellen-Scans** werden herangezogen, um die technische Sicherheitslage zu bestimmen
- Identifizierung möglicher Angriffspunkte eines Unternehmens
- Schnell, günstiger aber nicht voll verlässlich
- IT-Schwachstellenanalyse als Ausgangspunkt für einen Penetrationstest

IT-Penetrationstest:

- **Penetrationstest** offenbart inwieweit Hacker in die Infrastruktur vordringen können
- Penetrationstest entspricht der Vorgehensweise eines realen **Cyber-Angriffs**
- Identifizierung eventueller tiefgreifender Schwachstellen
- **Schadensanalyse**: in welchem Maße schadet ein **Hacker-Angriff** dem Unternehmen
- **Schwachstellen-Scans** sind immer Teil des **Penetrationstests**

iMes IT-Security

Schwachstellenanalyse vs. Penetrationstest

Zentrale Aspekte von Schwachstellenanalyse
und IT-Penetrationstests

Schwachstellen Scans:

Sog. **Schwachstellen Scans** – auch **Vulnerability Scans** genannt –sind software-gestützte und vollautomatisierte Anwendungen die das System oder Netzwerk auf bereits bekannte Sicherheitslücken testen. Security Analysten setzten durchaus auch Software-Tools ein. Diese sind aber **kein Ersatz** für eine **umfangreiche Sicherheitsprüfung**.

Soll das **IT-System** auf Herz und Nieren getestet werden, ist die Erfahrung eines Security Analysten unerlässlich.

IT-Security u. Industrie 4.0:

Die zunehmende **Vernetzung von Produktionsprozessen**, die Kommunikation von Maschinen über Landesgrenzen hinweg und der damit verbundene Austausch großer Datenmengen erfordern entsprechende **Sicherheitsanforderungen**.

Neben der **Betriebs- und Anlagensicherheit** gewinnt die Sicherheit gegenüber IT-Angriffen enorm an Bedeutung (**IT-Security**). Die Weiterentwicklung zur **Industrie 4.0** ist nicht nur mit Chancen verbunden, sondern auch mit gewissen Risiken – es bedarf einen umfassenden Schutz der hochgradig vernetzten Systemarchitekturen sowie der ausgetauschten Daten und Informationen.