



## Penetration-Testing

### IT-Sicherheitslücken im Unternehmen finden

#### Was ist ein Pen-Test?

Bei einem Penetrationstest untersuchen und bewerten Experten die Sicherheit Ihrer IT-Systeme. Dabei wird die Unternehmens-IT durch einen simulierten Hackerangriff auf Schwächen wie zum Beispiel technische Fehler oder bekannte Sicherheitslücken geprüft.

#### Was bringt der Pen-Test?

Die Ergebnisse zeigen auf, wie anfällig Ihre IT-Systeme sind, wie wahrscheinlich ein Angriff auf die IT-Infrastruktur ist und wie Sie sich vor potentiellen Angriffen schützen können.

#### Was wird getestet?

Es gibt verschiedene Varianten des Pen-Tests. Bei **externen** Tests werden sämtliche Komponenten, die über eine Internetverbindung erreichbar sind, untersucht. Hierzu gehören Server, die dazugehörige Infrastruktur und die verwendete Software. Bei **internen** Tests wird das interne Firmennetzwerk geprüft, so zum Beispiel Kommunikationswege und Zugangsbeschränkungen. Das Reaktionsverhalten der Mitarbeiter:innen gehört ebenfalls dazu.

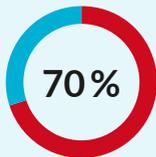
## Pen-Tests: Eine wirksame Waffe gegen Hackerangriffe

Mit Hilfe eines Pen-Test werden versteckte Schwachstellen der Unternehmens-IT erkannt, bevor Hacker:innen sie finden. So verhindern Unternehmen aber nicht nur Systemausfälle und sparen Reparaturkosten – sie finden auch heraus, wo sie ihr Budget für IT-Sicherheit am effektivsten einsetzen können.

## Angriffsziel deutsche Wirtschaft

 **223 Mrd. €**

Gesamtschaden im Jahr 2021 durch digitale Angriffe in Deutschland



der Unternehmen sind durch digitale Angriffe zu Schaden gekommen



Unternehmen waren 2021 Ziel von digitalen Angriffen

n = 1067 befragte Führungskräfte von deutschen Unternehmen

Quelle: [Bitkom Research 2021: Angriffsziel deutsche Wirtschaft.](#)

## Und so läuft der Pen-Test ab:

### 1. Bedarfsanalyse

Der Dienstleister bespricht mit Ihnen Ziel und Umfang des Penetrationstests.

### 2. Informationssammlung

Alle Informationen, die aus der Sicht eines Angreifers relevant sind, werden erhoben.

### 3. Identifikation von Schwachstellen

Mögliche Schwachstellen werden anschließend durch gezielte Tests aufgedeckt.

### 4. Schwachstellen reporten

Gefundene Schwachstellen werden bewusst gehackt, um sie realitätsnah zu dokumentieren und einzuordnen.

### 5. Berichterstellung

Die Ergebnisse des Pen-Tests werden zusammengefasst und individuelle Handlungsempfehlungen abgeleitet

Eine Liste zertifizierter Pen-Test-Anbieter finden Sie unter [bsi.de](#) über die Suche, Stichwort „IT-Sicherheitsdienstleister Penetrationstest“.

Mehr Flyer & Infos zu Digitalthemen: [digitalzentrum.berlin](#)

#### Impressum

Verleger: Der Mittelstand, BVMW e. V. | Potsdamer Straße 7, 10785 Berlin

Vereinsregister Berlin Charlottenburg Nr. 19361 Nz, | USt.-ID-Nr. DE 230883382

Text & Redaktion: Alexander Krug, Marie Landsberg | Design: [simpelplus.de](#) | Stand: März 2022

Gefördert durch:



Bundesministerium  
für Wirtschaft  
und Klimaschutz

Mittelstand-  
Digital 

aufgrund eines Beschlusses  
des Deutschen Bundestages