

# Penetrationstests



## Risiko Sicherheitslücken in IT-Netzwerken



## Penetrationstests

### **Risiko Sicherheitslücken in IT-Netzwerken**

Unbefugter Zugriff auf Systeme und Daten Ihres Unternehmens, Know-how-Abfluss oder Verletzung von gesetzlichen Bestimmungen sind beispielhafte Gefahren, die durch unzureichende Absicherung des internen und externen Netzwerkes entstehen können. Den meisten Unternehmen ist dabei nicht bewusst, welche Schäden hierdurch verursacht werden können.

Um diese Risiken zu reduzieren und ein notwendiges Maß an Sicherheit und Funktionalität zu gewährleisten, kann Ihr Unternehmen bestehende IT-Systeme bezüglich ihrer Sicherheit durch Penetrationstests bewerten lassen.



## Penetrationstests

### Warum Penetrationstests?

- Um zu wissen, wie sicher Ihr Unternehmen ist
- Um das IT-Sicherheitsniveau zu erhöhen
- Um die gesetzlichen Vorschriften und Regelungen zum Schutz von Informationen im Unternehmen einzuhalten

### Was erhalten Sie?

- Eine Einschätzung Ihres Unternehmens und die Darstellung des Gefahrenpotentials des penetrierten Umfeldes aus der Sicht eines Hackers
- Erhöhung der Sicherheit Ihrer technischen Systeme und Infrastruktur
  - Aufzeigen von Schwachstellen und Sicherheitsproblemen
  - Überprüfung von umgesetzten Sicherheitsmaßnahmen
  - Maßnahmenempfehlungen zu gefundenen Schwachstellen
  - Empfehlungen zur Compliance Ihrer IT-Sicherheit
  - Vorschläge für eine regelmäßige IT-Sicherheitsstrategie
- Bestätigung der IT-Sicherheit durch einen externen Dritten

## Bereiche der Penetrationstests

Grundsätzlich werden zwei Test-Methoden innerhalb eines Penetrationstests unterschieden.

### Blackboxtests

Ein Blackboxtest spiegelt einen externen Angriff einer betriebsfremden Person wider. Ziel dieses Tests ist das Aufzeigen von konkreten Sicherheitslücken, die ohne Insiderwissen ausgenutzt werden können.

### Whiteboxtests

Bei einem Whiteboxtest wird der Angriff mit dem Detailwissen eines internen Mitarbeiters simuliert. Ziel dabei ist sowohl das Aufzeigen von potentiellen Schwachstellen als auch die Überprüfung von internen IT-Sicherheitskonzepten.

	Bereiche
<b>Black-box-tests</b>	<ul style="list-style-type: none"><li>• Firewall</li><li>• WLAN</li><li>• Webserver</li></ul>
<b>White-box-tests</b>	<ul style="list-style-type: none"><li>• IT-Infrastrukturen (Router/ Switch)</li><li>• WLAN</li><li>• Datenbanken</li></ul>

### Vorbereitung

- Informationsbasis (Black- oder Whitebox)
- Aggressivität (passiv bis aggressiv)
- Umfang (vollständig bis fokussiert)
- Ausgangspunkt (von innen oder außen)

## **Durchführung**

### **Kick-Off und Informationsbeschaffung**

- Absprache des Durchführungszeitraumes
- Klärung rechtlicher Gegebenheiten
- Definition der einzusetzenden Tools
- Festlegung der Reporting-Strukturen
- Informationsbeschaffung und -auswertung
- Bewertung der Informationen/Risikoanalyse

### **Analysieren und Schwachstellen aufdecken**

- Scanning (z.B.: TCP / UDP Scan)
- Aktive Eindringversuche
- Interpretation der Schwachstellen
- Analyse der Fakten und Abstimmung der weiteren Vorgehensweise

### **Dokumentation und Abschlussgespräch**

- Berichterstellung und -abstimmung
- Dokumentation der Vorgehensweise und Methodiken der durchgeführten Arbeitsschritte
- Dokumentation der gefundenen Schwachstellen
- Risiko-Bewertung der gefundenen Schwachstellen
- Detaillierte Empfehlungen zum weiteren Vorgehen

## Individuell - nicht Standard

IT-Systeme und Verfahren in Unternehmen unterscheiden sich voneinander - Strukturen und technische Organisationen sind ausschlaggebend für Ausprägungen und individuelle Prozesse.

Daher ist es nicht sinnvoll Penetrationstests in einem festen, einheitlichen Schema ablaufen zu lassen. Im Gegenteil. Ein Test sollte möglichst flexibel sein, je nachdem welches Kriterium entscheidend ist. Abhängig von der Perspektive, aus der der Test durchgeführt wird, der Aggressivität und Vorgehensweise des Prüfablaufs, dem Umfang der zu überprüfenden Systeme und der bereitgestellten Informationsbasis führen wir einen individuellen und zielgerichteten Penetrationstest durch.

Neugierig geworden? Lassen Sie sich von uns ein individuelles Angebot erstellen...

**[sales@ibs-hamburg.com](mailto:sales@ibs-hamburg.com)**

Weitere Informationen zu Penetrationstests finden Sie unter **[www.ibs-hamburg.com](http://www.ibs-hamburg.com)**



## **IBS - Das sind wir**

Gegründet am 01. Juli 1979 als *Ingenieurbüro Schreiber* stellt sich das Unternehmen nach vielen Zellteilungen heute dar als *IBS Schreiber GmbH - International Business Services for auditing and consulting*.

### **Mehr Platz für mehr Leistung**

IBS steht für mittlerweile vier Geschäftsbereiche: Von unseren *Prüfseminaren und Fachkonferenzen* über *Revisions- und Beratungsleistungen* und unserer *Prüfsoftware CheckAud®* bis hin zur *Anerkannten Prüfstelle für Datenschutz*.

Unsere Referenzen bilden sich in nahezu jeder Branche bei namhaften Unternehmen ab: Banken, Versicherungen, Forschung, öffentliche Hand, Fertigungsindustrie, Medien, Prüfer und Berater sind nur einige Zweige, die wir zu unseren stetig wachsenden Kundengruppen zählen dürfen.

Aktualität, Lernbereitschaft und Weiterentwicklung sind dabei nicht nur Mittel zum Zweck, sondern definieren sich in unseren Unternehmenswerten als Innovation.

**IBS Schreiber GmbH**

International Business Services  
for auditing and consulting

Zirkusweg 1  
20359 Hamburg

Telefon: +49 (0) 40 / 69 69 85-15

Telefax: +49 (0) 40 / 69 69 85-31

**[www.ibs-hamburg.com](http://www.ibs-hamburg.com)**

**[info@ibs-hamburg.com](mailto:info@ibs-hamburg.com)**