Ihr Spezialist für Informationssicherheit

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

# Penetrationstests und IT-Sicherheitsprüfungen

## Warum sollten Sie einen Penetrationstest durchführen?

**Realistische Simulation**

Unsere Penetrationstests nutzen dieselben Angriffswerkzeuge und Methoden, die auch realen Angreifern zur Verfügung stehen

**Manuelle Angriffe von erfahrenen Testern**

Alle Angriffe werden manuell von unseren erfahrenen Penetrationstestern durchgeführt, die langjährige Erfahrung mit offensiven Sicherheitstechniken haben. Dies ermöglicht eine gezieltere Identifikation von Schwachstellen und eine Bewertung entsprechend Ihrer spezifischen Geschäftsanforderungen. Wir führen nicht einfach nur Vulnerability Scans durch

**Identifizieren von Schwachstellen**

Penetrationstests und Security Assessments bewerten die Sicherheit eines Informationssystems oder einer Anwendung. Ziel ist es, durch konkrete Angriffe Schwachstellen zu identifizieren, die genau so auch ein bösartiger Angreifer finden und ausnutzen könnte

**Bestätigung der Sicherheit**

Insbesondere bei der Inbetriebnahme neuer Infrastrukturen, z.B. eines neuen Webportals für Ihre Kunden oder nach dem Update der Windows Domäneninfrastruktur bietet sich ein Penetrationstest an, um möglichst früh Risiken zu erkennen und beseitigen zu können

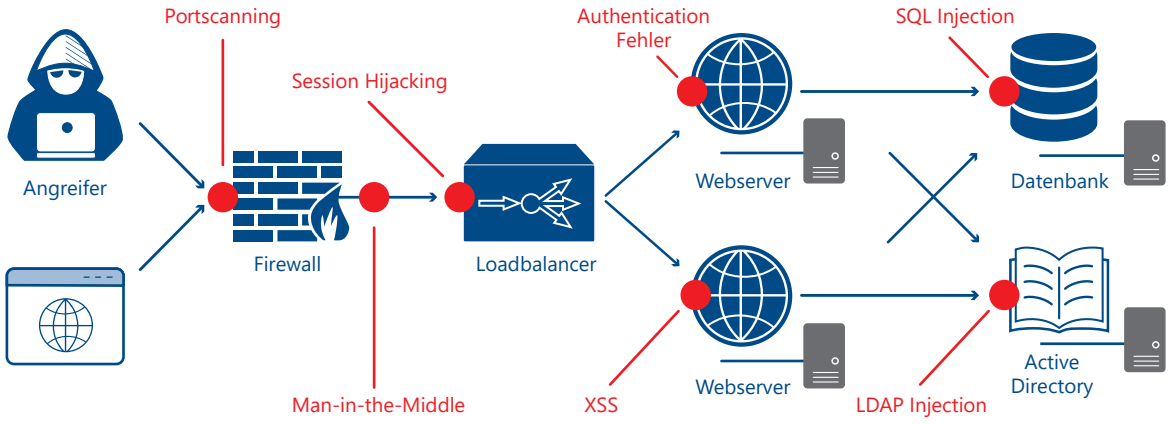
**Aussagekräftige Berichte**

Sie erhalten von uns einen aussagekräftigen Bericht, der Ihnen erläutert, welche Angriffe durchgeführt wurden und welches Risiko mit den konkreten Schwachstellen verbunden ist. Außerdem erhalten Sie Empfehlungen zur Behebung der Schwachstellen und eine Kostenabschätzung der empfohlenen Maßnahmen

## Unser Angebot

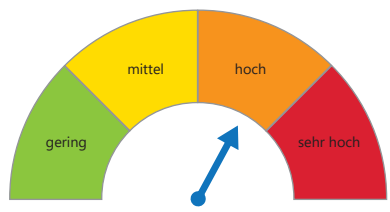
<table>
<tr><th></th><th colspan="2"></th><th colspan="4">Angreifer</th></tr>
<tr><th></th><th colspan="2">Sicht</th><th>Externer Angreifer</th><th></th><th>Interner Angreifer</th><th>Administrator</th></tr>
<tr><td rowspan="4">Art der Angriffe</td><td>Einzelne Webanwendungen und Web-APIs</td><td>URLs von Anwendungen</td><td>Penetrationstest der Webanwendung von außen<br><br>Schwachstellenanalyse des Webservers</td><td rowspan="4">Red Team</td><td>Penetrationstest der Webanwendung mit Authentifizierung<br><br>Prüfung von Berechtigungen</td><td>Prüfung des Quellcodes der Anwendung</td></tr>
<tr><td>Aus dem Internet erreichbare Infrastruktur</td><td>Öffentliche IP-Adressen des Unternehmens</td><td>Externer Penetrationstest<br><br>Schwachstellenanalyse von Firewall, VPN, E-Mail, etc.</td><td>Penetrationstest der Infrastruktur mit Enterprise-Zugängen (VPN, RDP, Citrix)</td><td rowspan="2">Prüfung der Konfiguration der Serverinfrastruktur<br><br>Prüfung der Konfiguration von System- und Netzwerkkomponenten</td></tr>
<tr><td>Interne Infrastruktur, z.B. Netzwerk, Server, Windows-Domäne, Clients, WLAN, VoIP</td><td>Private interne IP-Adressen des Unternehmens</td><td>Interner Penetrationstest mit LAN-Zugang<br><br>WLAN-Penetrationstest</td><td>Penetrationstest von Windows-Domäne und Standard-Clients<br><br>VoIP-Penetrationstest</td><td>Prüfung der Gruppenrichtlinien<br><br>Prüfung der Sicherheitsarchitektur</td></tr>
<tr><td>Sicherheitsbewusstsein der Mitarbeiter</td><td>Liste von Mitarbeitern mit E-Mail-Adresse und Telefonnummer</td><td>Social Engineering Angriffe (Phishing, Malware)</td><td colspan="3">Awareness-Training für technische und nicht-technische Mitarbeiter sowie Administratoren</td></tr>
</table>

## Penetrationstest für Webanwendungen




## Risikobewertung

| | |
|---|---|
| **Nummer** | WEB-1 |
| **Host / Zielsystem** | Webserver |
| **Schwachstelle** | SQL-Injection im E-Mail-Formular |
| **Einstufung** | Vulnerability |
| **Beschreibung** | Ein Angreifer kann im E-Mail-Formular im Absender-Feld zusätzliche SQL-Befehle angeben, die auf dem Datenbank-server ausgeführt werden |
| **Potenzieller Schaden** | Hoch – Ein Angreifer erhält Zugriff auf die komplette SQL-Datenbank und kann alle Daten auslesen und/oder verändern |
| **Eintrittswahr-scheinlichkeit** | Mittel – Der Angriff ist relativ einfach durchführbar, die Lücke wird jedoch von automatischen Vulnerability Scannern nicht direkt erkannt |
| **Empfehlung** | Korrektur der Anwendung, ggf. Meldung an Hersteller |
| **Aufwand zur Behebung** | Gering – Anpassung des Programms, Sonderzeichen filtern<br>Mittel – Umstellung auf Prepared Statements |




## Unsere Verpflichtung

**Vertraulichkeit**
Unsere Prüfung und Berichterstattung erfolgen auf einer dedizierten Infrastruktur. Alle Auswertungen und Berichte werden sicher verschlüsselt gespeichert und nach Abschluss der Prüfung gelöscht

**Zuverlässigkeit**
Wir kombinieren standardisierte Methodiken, z.B. OWASP und OSSTMM mit einer gründlichen Vorgehensweise um zuverlässig und reproduzierbar Schwachstellen aufzuspüren und zu identifizieren

**Ethisches Handeln**
Wir halten uns an den vereinbarten Umfang und führen keine unautorisierten Angriffe durch. Wir teilen Ihnen sofort mit, wenn ein kritisches Risiko entdeckt wird

**Technische Stärke**
Wir verfügen über zertifizierte Penetrationstester mit jahre-langer Erfahrung, die eigene Hacking-Tools und Werkzeuge entwickeln

**Seminare**
In unseren Hacking-Seminaren geben wir unser Wissen gerne an Sie weiter

**NESEC**
**Gesellschaft für angewandte Netzwerksicherheit mbH**

Fürholzener Straße 5a
85386 Eching
Telefon: 089 - 45217100
E-Mail: welcome@nesec.de
Internet: www.nesec.de

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH