# Penetrationstests

## Weil Sicherheit Erfahrung braucht.

### Sicherheitsprüfung Ihrer IT-Infrastruktur durch zertifizierte Penetrationstester

„Sind unsere IT-Systeme anfällig für Hacker? Haben wir geeignete Schutzmaßnahmen ergriffen? Wie weit könnte ein Hacker eindringen?“

Diese oder ähnliche Fragen werden Sie sich schon gestellt haben. IT-Infrastrukturen bestehen aus zahlreichen Hard- und Softwarekomponenten, die alle Sicherheitslücken enthalten können.

Bei Penetrationstests nehmen unsere Experten die Rolle eines Hackers ein und simulieren Angriffe auf Ihre IT-Infrastruktur. So können ausnutzbare Schwachstellen und unwirksame Schutzmechanismen entdeckt werden. Sie helfen Ihnen dabei,

- das Schutzniveau Ihrer IT-Systeme besser einzuschätzen
- die Eignung der von Ihnen ergriffenen Schutzmaßnahmen zu überprüfen,
- die Erfüllung von Kundenanforderungen an die Sicherheit Ihrer Systeme nachzuweisen,
- die Einhaltung von Branchenstandards wie z.B. PCI-DSS zu belegen und
- Ihrer Pflicht zur regelmäßigen Kontrolle der ergriffenen Maßnahmen zum Schutz Ihrer Unternehmens- und Kundendaten nachzukommen.

Wesentliche Voraussetzung für die Verlässlichkeit und Vergleichbarkeit der Ergebnisse eines Penetrationstests sind dabei

- die Durchführung nach bewährten und etablierten Standards wie z. B. OWASP Testing Guide, PTES, BSI und
- die Nutzung erprobter, aktueller Werkzeuge sowie
- der Einsatz zertifizierter Penetrationstester.

### Ihre Ansprechpartner

**André Domnick**
zertifizierter Offensive Security Certified Professional (OSCP), TeleTrusT Information Security Professional (T.I.S.P.)

**Stefan Gora**
ISO 27001 Lead Auditor, TeleTrusT Information Security Professional (T.I.S.P.)

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe

Telefon +49 721 255171-0
pentest@secorvo.de
www.secorvo.de

### Über Secorvo

Die Secorvo Security Consulting GmbH ist ein auf Informationssicherheit und Datenschutz spezialisiertes und bereits mehrfach ausgezeichnetes Beratungsunternehmen. Alle Mitarbeiter sind ausgewiesene Experten mit vieljähriger Erfahrung.

*„Besonders gefällt uns die hohe Qualität des Reports. Insbesondere wird auch die Methodik beschrieben, sowie diejenigen Tests dokumentiert, die nicht in der Feststellung einer Schwachstelle mündeten.“*
Falk Schramm, Information Security Officer,
infoscore consumer data GmbH

*„Die Penetrationstests waren stets sehr gut vorbereitet und wurden exakt nach zeitlicher Absprache durchgeführt. Dabei ist die hohe Qualität des Reports und die detaillierte Dokumentation der Prüfung besonders zu erwähnen.“*
Michael Bähr, Spezialist Informationssicherheit, T.I.S.P.,
Markant Handels und Service GmbH

## Unsere Vorgehensweise

- Festlegung des Untersuchungsgegenstands und des Umfangs der Sicherheitsprüfung
- Durchführung eines Kick-Off-Workshops mit den für IT-Sicherheit und den Betrieb der betroffenen IT-Systeme Verantwortlichen Ihres Unternehmens
- Durchführung des Penetrationstests nach bewährten und etablierten Standards
- Einsatz erprobter, aktueller Werkzeuge und Durchführung ergänzender manueller Analysen
- Ergebnisbericht und Präsentation mit priorisierten Maßnahmenempfehlungen
- Durchführung einer Nachkontrolle

## Ihr Mehrwert

- Nachweis der Erfüllung bestimmter Anforderungen etablierter Sicherheits-Standards (wie ISO 27001, BSI Grundschutz, PCI-DSS)
- Ergebnisdokumentation mit priorisierten Handlungsempfehlungen
- Vergleichbarkeit der Ergebnisse aufgrund standardisierter Vorgehensweise und zertifizierter Penetrationstester
- Kalkulationssicherheit (Festpreis)

## Prüfbereiche
## Flexibles Baukastenprinzip

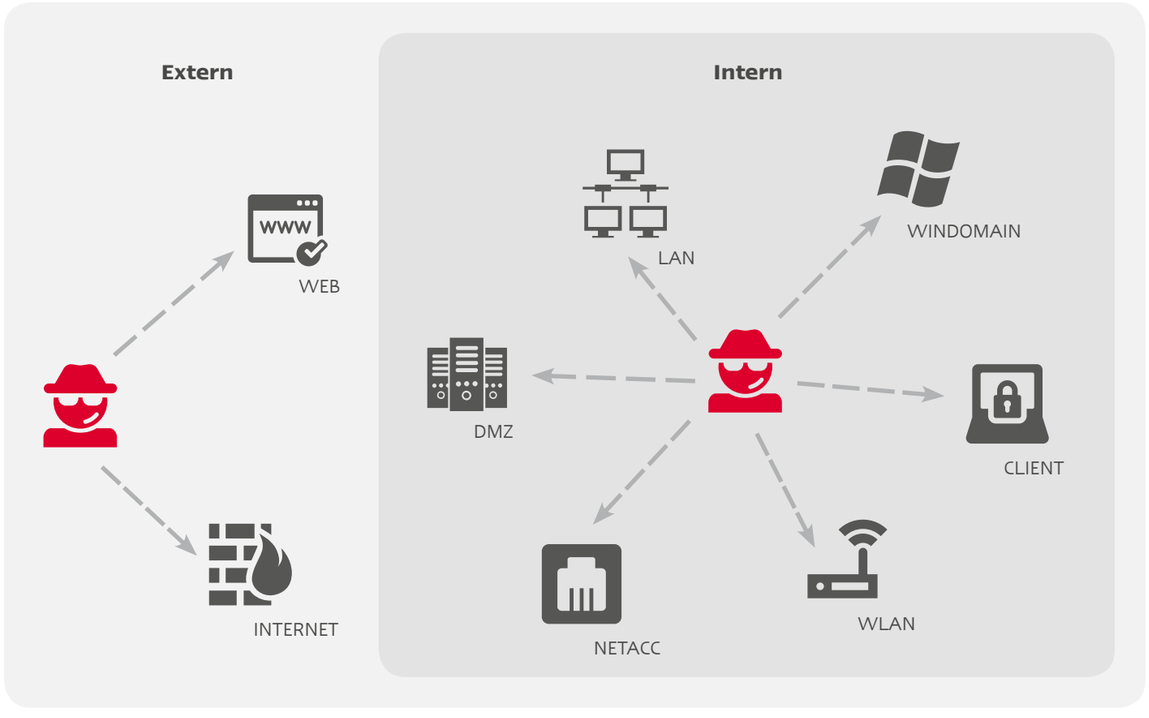
Ein Penetrationstest setzt sich aus verschiedenen Teilprüfungen zusammen, die passend zu Ihrer IT-Infrastruktur ausgewählt und mit Ihnen abgestimmt werden.

Die Teilprüfungen lassen sich in drei Bereiche gliedern:

- Externe Untersuchungen: über das Internet erreichbare Systeme und Web-Anwendungen
- Interne Untersuchungen: Unternehmens-LAN, WLANs, DMZ, Netzkomponenten, Domänen, Client-Systeme
- Spezialuntersuchungen: Produktprüfung, Ausbruch aus virtualisierten Umgebungen, Web-Anwendungen (ASVS), Systemhärtung

Wir bieten Ihnen unsere Leistungen zu einem festen Paketpreis an: als Basis-Pentest, Standard-Pentest oder erweiterter Pentest (siehe Tabelle).

Selbstverständlich können Sie zu diesen Paketen einzelne Untersuchungen hinzubuchen. Gerne machen wir Ihnen ein Angebot - sprechen Sie mit uns.




Icons designed by Freepik

## Übersicht der Teilprüfungen

| | Arbeitspaket | Basis | Standard | Erweitert |
|---|---|---|---|---|
| | **Kick-off-Workshop** | ✓ | ✓ | ✓ |
| Extern | **INTERNET**<br>Prüfung über das Internet erreichbarer Systeme und Netze | ✓ | ✓ | ✓ |
| Extern | **WEB**<br>Prüfung von Web-Anwendungen, Web-Services und Mobilen Anwendungen (Apps) | ✓ | ✓ | ✓ |
| Intern | **LAN**<br>Prüfung des internen Unternehmensnetzes einschließlich der erreichbaren VLANs | | ✓ | ✓ |
| Intern | **WINDOMAIN**<br>Prüfung, ob ein Benutzer seine Rechte erweitern kann | | ✓ | ✓ |
| Intern | **CLIENT**<br>Prüfung, ob ein Standard-Client-System (z. B. Notebook) gegen Angriffe wie Spear-Phishing oder trojanisierte Geräte geschützt ist | | ✓ | ✓ |
| Intern | **NETACC**<br>Prüfung, inwiefern es einem Angreifer mit physischem Zugang (z. B. Besucher) möglich ist, Zugang zu internen Netzen zu erlangen | | | ✓ |
| Intern | **DMZ**<br>Prüfung der DMZ-Systeme innerhalb der Demilitarisierten Zone und aus dem internen Netz | | | ✓ |
| Intern | **WLAN**<br>Prüfung, ob Angreifer in Ihre WLANs einbrechen können | | | ✓ |
| | **Bericht und Maßnahmenempfehlungen** | ✓ | ✓ | ✓ |
| | **Abschlusspräsentation** | ✓ | ✓ | ✓ |
| | **Nachkontrolle der Maßnahmenumsetzung** | | ✓ | ✓ |
| Spezial | **CUSTOM**<br>Kundenspezifische Prüfungen je nach Ihrem Bedarf, beispielsweise Produktprüfungen | | | |
| Spezial | **BENCHMARK**<br>Prüfung der Härtung von Betriebssysteminstallationen und Serverdiensten im White-Box-Verfahren auf Basis der Benchmarks des Center for Internet Security (CIS) | | | |
| Spezial | **ASVS**<br>Prüfung Ihrer Webanwendungen im White-Box-Verfahren auf Basis des OWASP Application Security Verification Standard | | | |