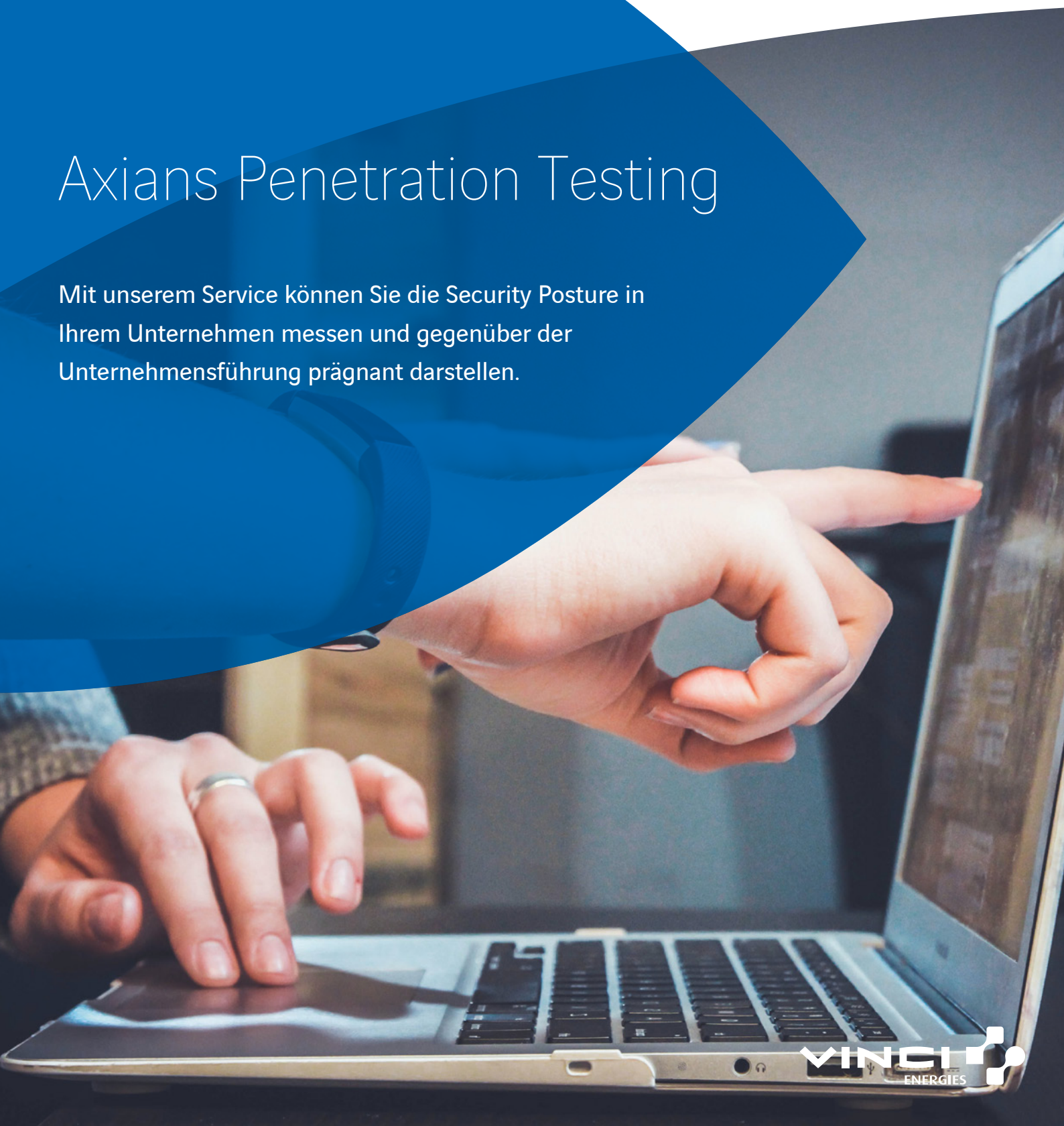
# Axians Penetration Testing

Mit unserem Service können Sie die Security Posture in Ihrem Unternehmen messen und gegenüber der Unternehmensführung prägnant darstellen.



**SIND IHRE CYBER-SECURITY-MASSNAHMEN SINNVOLL EINGESETZT?**

# Axians Penetration Testing

Datenverarbeitung in agilen Cloudumgebungen, Web- und Businessapplikationen im mobilen Zugriff, exponierte Endgeräte und Arbeitsplätze bieten für Cyberkriminelle eine weitläufige Angriffsfläche und eine Vielzahl von Angriffsvektoren. Wenn es darum geht, in solchen dynamischen IT-Infrastrukturen Cyber Security zu gewährleisten, haben Professionalität, Geschwindigkeit und ein korrekt definierter Prüfumfang oberste Priorität.
Zu diesen unmittelbaren Bedrohungsszenarien kommen Compliance-Anforderungen und regelmässige Security Audits. **Um Ihre Cyber-Defense-Strategie effizient und basierend auf reellen Risikofaktoren umzusetzen bedarf es nicht nur den Einsatz von Security Massnahmen, sondern auch deren regelmässige Überprüfung durch Penetration Tests.**

## Sicherheitslücken rechtzeitig erkennen und wertvolle Daten schützen

Penetration Testing ist die Prüfung der Sicherheit möglichst aller Systembestandteile und Anwendungen eines Unternehmens mit Mitteln und Methoden, die ein Angreifer (Hacker) anwenden würde, um unautorisiert in das System einzudringen. Axians setzt dabei auf eine Kombination führender Technologie aus dem Hause Pentera für vollautomatisiertes und kontinuierliches Pentesting sowie gezieltem Einsatz von menschlichem Fachwissen unserer Cyber-Security-Experten. Mittels Automation können so tausende von Angriffsaktivitäten pro Tag gefahren werden, während die manuellen Tests für spezifische Anwendungsfälle eingesetzt werden.

**FÜR JEDE HERAUSFORDERUNG DER PASSENDE SERVICE**

# Unser Angebot

| USE CASE | EXTERNER PENETRATION TEST | INTERNER PENETRATION TEST |
|---|---|---|
| **Business-Applikationen und ERP-Systeme**<br>▸ Private- und Public Cloud ge hostete Applikationen<br>▸ Web Application Firewalls<br>▸ Multi Factor Authentification Infrastruktur<br>▸ Webshops mit Datenbankanbindung und Payment Funktionalität | **Angriffsvektor**<br>▸ Internet<br>**Methodik**<br>▸ Anonym/Authentisiert<br>▸ OWASP 10 und MITR ATT&CK<br>▸ Manuell<br>▸ Ethical und Real Live Hacking<br>▸ Red Team Behaviour<br>**Resultat**<br>▸ Management- und Technik-Report<br>▸ Risikobasierte Massnahmen-Empfehlung<br>▸ Massnahmensimulation/ Impact-Analyse | |
| **Interne Netzwerk-Infrastruktur und Endgeräte**<br>▸ Arbeitsplätze (Windows, Linux, Industrie PCs)<br>▸ Serverumgebungen<br>▸ Aktive Netzwerkkomponenten (W-LAN, Router, etc.)<br>▸ Produktionsanlagen und Shop Floors | | **Angriffsvektor**<br>▸ Intranet<br>**Methodik**<br>▸ Anonym/Authentisiert<br>▸ MITR ATT&CK<br>▸ Manuell/Automatisiert<br>▸ Ethical und Real Live Hacking<br>▸ Red Team Behaviour<br>**Resultat**<br>▸ Management- und Technik-Report<br>▸ Risikobasierte Massnahmen-Empfehlung<br>▸ Massnahmensimulation/Impact-Analyse |
| **Cyber-Security-Komponenten, Filialvernetzung und Remote- Zugang**<br>▸ Firewalls und Proxy-Infrastruktur<br>▸ VPN-Remote-User-Access-Architektur<br>▸ VPN Gateways (Remote Standortanbindung, MPLS Infrastruktur, SD-WAN-Umgebungen) | **Angriffsvektor**<br>▸ Internet<br>**Methodik**<br>▸ Anonym/Authentisiert<br>▸ OWASP 10 und MITR ATT&CK<br>▸ Manuell/Automatisiert<br>▸ Ethical und Real Live Hacking<br>▸ Red Team Behaviour<br>**Resultat**<br>▸ Management- und Technik-Report<br>▸ Risikobasierte Massnahmen-Empfehlung<br>▸ Massnahmensimulation/ Impact-Analyse | **Angriffsvektor**<br>▸ Intranet<br>**Methodik**<br>▸ Anonym/Authentisiert<br>▸ MITR ATT&CK<br>▸ Manuell/Automatisiert<br>▸ Ethical und Real Live Hacking<br>▸ Red Team Behaviour<br>**Resultat**<br>▸ Management- und Technik-Report<br>▸ Risikobasierte Massnahmen-Empfehlung<br>▸ Massnahmensimulation/Impact-Analyse |

# Ihre Vorteile auf einem Blick

- **Bedarfsorientierte Kombination** manueller und automatisierter Penetration Test Methoden
- **Echte Impact Analyse** von empfohlenen Remediation-Massnahmen
- **Erhöhung Effizienz** der Cyber Security Teams
- **On-Demand** Penetration Tests und/oder **fortlaufende Penetration Tests** (PenTest-as-a-Service)
- Garantiert **störungsfreier Betrieb**
- **Vollautomatisiertes** Audit- und Compliance Reporting

# Kosten

<table>
<tr><th>AUTOMATISIERTER PENETRATION TEST</th><th>KOSTEN (CHF)<br>*exkl. MwSt.</th><th>MANUELLER PENETRATION TEST</th><th>KOSTEN (CHF)<br>*exkl. MwSt.</th></tr>
<tr><td>On-Demand Erstanalyse<br>▸ Anzahl geprüfter Systeme: unlimitiert<br>▸ Vorbereitungszeit: 3 Tage<br>▸ Durchführungszeit: 5 Tage<br>▸ Analyse und Präsentation: 1 Tag</td><td>14.475.-</td><td rowspan="2">Prüfung Business-Web-Applikation<br>▸ Bedarfsanalyse<br>▸ Anzahl geprüfter Systeme, Vorbereitungs- und Durchführungszeit: Bedarfsanalyse<br>▸ Erfahrungswert Mindestaufwand: 5 - 15 Tage</td><td rowspan="2">1.952.-/Tag</td></tr>
<tr><td>Axians PenTest as a Service<br>▸ Anzahl geprüfter Systeme: Gemäss Bedarf<br>▸ Mindestvertragslaufzeit: 12 Monate<br>▸ Analyse und Präsentation: Wöchentlich oder monatlich (SLA abhängig)</td><td>Nach Bedarf</td></tr>
</table>


**IHRE ANSPRECHPARTNERIN**

Renata Rekic (Presales Consultant)

E-Mail: renata.rekic@axians.com

07/2021

Axians Cyber Security & BI AG · Rotkreuz · Basel · Zürich
E-Mail: info-ch.security@axians.com · www.axians.ch