protiviti®
Global Business Consulting

Foto: Getty Images

ATTACK & PENETRATION TESTING

Wir testen Ihre Sicherheit nicht nur – wir stellen sie auf die Probe. Unser Team denkt wie echte Angreifende, handelt präzise und liefert Erkenntnisse, die wirklich zählen. Gestützt auf reale Bedrohungsinformationen und tiefgehendes technisches Know-how decken wir auf, was andere übersehen und unterstützen Sie dabei, die Lücken zu schließen.

Denken wie Angreifende

Unsere Attack & Penetration Testing Services sind darauf ausgelegt, reale Angriffe mit den neuesten Taktiken, Techniken und Verfahren zu simulieren. Wir verbinden tiefgehende technische Expertise mit aktueller Bedrohungsintelligenz, um nicht nur Schwachstellen sondern auch deren Ursachen zu identifizieren.

Jeder Einsatz ist individuell auf Ihre Umgebung zugeschnitten und liefert klare, umsetzbare Ergebnisse, die sich an Ihren Geschäftsprioritäten orientieren. Ob Red Teaming, Anwendungstests oder Social Engineering – wir gehen weit über Checklisten hinaus und decken auf, was wirklich zählt.

68 %
MENSCHLICHES VERSAGEN

68 % aller Sicherheitsverletzungen beinhalten einen menschlichen Faktor.

Quelle: Verizon DBIR

162
STUNDEN

162 Stunden (≈ 7 Tage) brauchen Unternehmen im Durchschnitt, um Cybervorfälle vollständig zu erkennen und darauf zu reagieren.

Quelle: Crowdstrike

Wir testen nicht nur. Wir validieren. Wir liefern. **Unser Ziel:** Sie dabei zu unterstützen, Risiken zu reduzieren, Resilienz zu stärken und Bedrohungen immer einen Schritt voraus zu sein.

Mehr als ein Test – ein echter Mehrwert

Unsere Attack & Penetration Tests liefern Ihnen echte Mehrwerte: realistische Angriffssimulationen, individuell auf Ihre Umgebung zugeschnittene Szenarien und Ergebnisse, die sich direkt umsetzen lassen. So gewinnen Sie Klarheit über Ihre Risiken und erhalten konkrete Handlungsempfehlungen, die Ihr Unternehmen nachhaltig voranbringen.

Ihr Nutzen:

- **Realistische Angriffe**
  Simulation echter Hacker-Taktiken
- **Individuelle Szenarien**
  Passgenau für Ihre Systeme & Prozesse
- **Klare Ergebnisse**
  Schwachstellen sichtbar & verständlich dokumentiert
- **Direkte Umsetzbarkeit**
  Konkrete Maßnahmen statt theoretischer Listen
- **Nachhaltiger Mehrwert**
  Risiken reduzieren, Resilienz stärken

Wie wir grundsätzlich vorgehen

OSINT, RECON & ENUMERATION
↓
EXPLOITATION
↓
POST-EXPLOITATION
↓
REMEDIATION RECOMMENDATION

Unser Servicekatalog im Kontext von Attack & Penetration Testing

Open-Source Intelligence (OSINT)
Gezielte OSINT-Recherchen decken Angriffsflächen, exponierte Personen und aktuelle Risiken auf und liefern abteilungsspezifische Gefährdungsprofile als Basis für Assessment-Szenarien.

Network Penetration Testing
Wir prüfen die Widerstandsfähigkeit Ihrer Netze und Clients mit praxisnahen Angriffssimulationen:
Internal & External Penetration Test • Wi-Fi Penetration Test • OT Penetration Test

Web Application & API Penetration Testing
Wir prüfen Anwendungen entlang der OWASP Top 10 und entwickeln maßgeschneiderte Exploits und Proof-of-Concepts, um echte Angriffsvektoren aufzudecken und sofort umsetzbare Präventionsmaßnahmen zu liefern.

Active Directory Penetration Testing
Technischer Angriff auf ihr Active Directory (on-premise und Entra ID) zur Aufdeckung von Angriffspfaden, Lateral Movement Risiken und ausnutzbaren privilegierten Konten.

Cloud Penetration Testing
Wir führen technische Tests in Cloud-Umgebungen (AWS/Azure/GCP) durch, prüfen Konfigurationen und Infrastruktur (Storage-Policies, Netz-ACLs, Security-Groups), analysieren IAM/RBAC-Setups inklusive Rollen, Service-Principals und Cross-Account-Trusts sowie Management-APIs, Token Handling und Rate-Limits.

SAP Penetration Testing
Wir prüfen Ihre SAP-Landschaft (ECC/S/4HANA) auf Konfigurationsfehler, Berechtigungslücken, Zero-Days und weitere kritische Schwachstellen, von der Applikationsebene über Server/Infrastruktur bis zur Datenbankschicht.

Red Teaming
Wir simulieren realistische Angriffe auf Ihre Organisation, um Sicherheitslücken in Prozessen, Anwendungen und Infrastruktur aufzudecken. Dabei prüfen wir End-to-End-Angriffspfade, testen Detection- und Response-Maßnahmen und analysieren organisatorische Schwachstellen.

Ansprechpartner

SAED ALAVI
Senior Manager
+49 175 715 09 60
saed.alavi@protiviti.de

LEONARDO SCHWAMBERGER
Manager
+49 151 4387 62 74
leonardo.schwamberger@protiviti.de

KONTAKTIEREN SIE UNS!
+49 69 963 768 100
contact@protiviti.de
www.protiviti.de

protiviti®
Global Business Consulting

90	25	11.000
Standorte	Länder	Mitarbeitende

Protiviti berät Unternehmen praxisorientiert und auf Augenhöhe in den Bereichen Strategie, Organisationstransformation und -optimierung, ESG, Digitale Transformation, Risikomanagement, Interne Revision und Kontrollsysteme, Compliance sowie IT. Gemeinsam finden wir individuelle Lösungsansätze, um Ihr Unternehmen zukunftssicher aufzustellen.

We Care. We Collaborate. We Deliver.