UNITED SECURITY PROVIDERS

PENETRATION TESTING

Sicherheitslücken identifizieren

Identifizieren Sie potenzielle Angriffspunkte und schützen Sie Ihr Unternehmen vor Cyberbedrohungen

Wissen Sie, wie effektiv Ihre IT-Infrastruktur gegenüber potenziellen Cyberbedrohungen geschützt ist? Wir finden es heraus. Durch den Einsatz proaktiver Methoden identifizieren und beheben wir Sicherheitslücken, bevor es zu einem bösartigen Cybersecurity-Angriff kommt und Ihr Unternehmen erheblichen Schaden erleidet.

Penetration Testing Services - Simulationen von Cyber Attacken

Unsere erfahrenen IT-Security Experten versuchen mittels realistischen Angriffssimulationen sowie verschiedenen Techniken, Taktiken und Werkzeugen in Ihre Systeme einzudringen, vertrauliche Informationen zu extrahieren oder kritische Systeme zu kompromittieren. Ziel ist es, Schwachstellen und potenzielle Angriffspunkte in Ihren Web-/Applikationen, IT-Infrastrukturen, mobilen Geräten, Internet of Things (IoT) und Operations Technology (OT) aufzudecken. Dadurch erhalten Sie einen wertvollen Einblick darüber, welches Erfolgspotenzial ein Angreifer haben könnte und wie wirkungsvoll Ihre derzeitige Systemverteidigung ist.

Dabei geht es nicht nur um technische Aspekte, sondern auch um die Bewertung der Reaktion des Sicherheitsteams, der Sicherheitsrichtlinien und der organisatorischen Abläufe während eines Angriffsszenarios.

Arten von Penetrationstests - Kenntnisse über Ihre IT-Systeme

Blackbox-Tests: Ohne Vorwissen, ähnlich wie echte externe Angreifer

Whitebox-Tests: Detaillierte Kenntnisse mit Zugang zu Quellcodes, Architekturdetails etc.

Greybox-Tests: Begrenzte Informationen (z.B. Benutzerzugangsdaten, Netzwerktopologie etc.)

Für noch mehr Sicherheit und effektiven Schutz

Vervollständigen Sie Ihren Schutz mit ergänzenden Sicherheitsmassnahmen, die in Kombination dazu beitragen, ihre Abwehrmechanismen zu stärken, ihre Reaktion auf Angriffe zu verbessern und ihre Gesamtsicherheit zu erhöhen. Dabei geht es nicht nur um technische Aspekte, sondern auch um die Bewertung der Reaktion des Sicherheitsteams, der Sicherheitsrichtlinien und der organisatorischen Abläufe während eines Angriffsszenarios.

USP Vulnerability Scan - Erkennung von Schwachstellen

Während ein Penetrationstest darauf abzielt, Schwachstellen auszunutzen und das tatsächliche Angriffsrisiko zu bewerten, hat der Vulnerability Scan das Ziel, bekannte Schwachstellen zu identifizieren, ohne tatsächliche Angriffssimulationen durchzuführen. Beide Verfahren sind jedoch von Bedeutung und tragen in Kombination dazu bei, die Sicherheit eines Systems zu erhöhen. Der besondere Nutzen des Vulnerability Scans liegt darin, dass er ein automatisierter Prozess ist, der potenzielle Sicherheitslücken in Ihren Systemen erkennt und eine Liste möglicher Schwachstellen erstellt. Unsere IT-Sicherheitsspezialisten analysieren die protokollierten Ergebnisse und leiten daraus Empfehlungen für Massnahmen ab, die nach Priorität geordnet sind.

Red teaming

Red Teaming geht über das Ausnutzen von Schwachstellen hinaus, indem es die gesamte Sicherheitsstrategie bewertet, einschliesslich technischer, prozessualer und menschlicher Aspekte. Es legt den Fokus darauf, die Widerstandsfähigkeit einer Organisation gegenüber realistischen Angriffsszenarien zu prüfen, indem es die Verteidigungsmechanismen herausfordert und versucht, diese zu überwinden.

PENETRATION TESTING

- ✓ Aufzeigen und ausnutzen von Schwachstellen
- ✓ Bewertung des Bedrohungspotenzials
- ✓ Detaillierte Vorschläge zur Verbesserung des Sicherheitsniveaus
- ✓ Prüfung von gesetzlichen Vorgaben
- ✓ Vermeidung von Reputationsschäden
- ✓ Effektiver Schutz vor kostspieligen Datenverletzungen
- ✓ Verbesserungspotenziale erkennen und aufzeigen

AWARENESS TRAINING

- ✓ Sensibilisierung für Cybersicherheit mittels Mitarbeiterschulungen
- ✓ Mitarbeiter erkennen Bedrohungen und Phishing-Angriffe
- ✓ Sichere Verhaltensweisen (Passwortnutzung und regelmässiges Softwareupdates)
- ✓ Wie sensible Daten schützen
- ✓ Richtlinien und Vorschriften
- ✓ Simulierte Phishing-Angriffe
- ✓ Notfallmassnahmen, was tun im Falle eines Sicherheitsvorfalls

SECURITY TRAINING

- ✓ Massgeschneiderte Trainings für Security Verantwortliche
- ✓ Spezielle Trainings für CISO's
- ✓ Sicherheitstrainings für IT-Techniker und -Verantwortliche
- ✓ Cyber Security Trainings für Softwareentwickler
- ✓ Allgemeine Sicherheitsschulungen für Benutzer
- ✓ Nutzung von Demos und Praxisbeispielen
- ✓ Trainer sind IT-Sicherheitsberater mit breiter Praxiserfahrung

Kontakt

Kontaktieren Sie uns und wir beraten Sie gerne bei weiteren notwendigen Sicherheitsmassnahmen, um das Sicherheitsniveau in Ihrem Unternehmen insgesamt und nachhaltig zu verbessern.

United Security Providers AG
Hauptsitz
Stauffacherstrasse 65/15
3014 Bern

T +41 31 959 02 02

@ info@united-security-providers.ch

United Security Providers AG
Baslerpark
Mürtschenstrasse 27
8048 Zürich

T +41 31 959 02 02

www.united-security-providers.ch