OFFENSIVE SECURITY

IHR PARTNER FÜR UMFASSENDES IT- & OT-PENETRATION TESTING

Aufklärung und Vorbereitung › Scannen › Eindringen › Bereinigung › Bericht-erstellung › Maßnahmen-katalog › Umsetzung: Systemhärtung

In einer Welt zunehmender Cyberbedrohungen ist Sicherheit essenziell. Wir schützen Ihr Unternehmen mit maßgeschneidertem Penetration Testing, decken Sicherheitslücken auf und beheben diese, bevor Angreifer zuschlagen können.

WARUM PENETRATION TESTING?

- **Schwachstellen erkennen:** Wir identifizieren Sicherheitslücken in Ihren Systemen und untersuchen die Möglichkeiten zur Ausnutzung dieser Schwachstellen.
- **Proaktive Sicherheit:** Durch das Schließen der relevanten Sicherheitslücken stärken Sie Ihre Systeme lange, bevor Monitoring-Lösungen Angreifer im Netzwerk melden könnten.
- **Schutz Ihrer Daten:** Durch die Absicherung Ihrer Systeme und Netzwerke schützen Sie Ihr Unternehmen vor Datenverlust und -diebstahl.

UNSERE DIENSTLEISTUNGEN

ARTEN VON SECURITY TESTS

Vulnerability Assessment

- Identifizierung von **Schwachstellen** im System
- **Automatisiert** mithilfe von Tools wie NMAP, Nessus Pro oder Nikto
- **Manuelle Prüfung** von Geräten, Servern und Webanwendungen
- **Kein** aktives Angreifen

IT-Penetration Test

- Identifizierung von Schwachstellen im IT-System
- **Verifikation gefundener Schwach-stellen durch aktives Angreifen**
- Umfangreiche Untersuchung durch Betrachtung verschiedener **Angriffs-möglichkeiten**

OT-Penetration Test

- Identifizierung von Schwachstellen im **OT-System**
- Experten für OT mit Kenntnis über sensible Komponenten und spezielle Protokolle
- Umfangreiche Untersuchung durch Betrachtung verschiedener Angriffs-möglichkeiten

Physical Penetration Test

- Identifizierung von physischen Sicherheitslücken **(Zutritt und Zugriff)**
- Überprüfung der Sicherheit von **Gebäuden und Anlagen**
- Spezialist versucht unberechtigten Zutritt bzw. Zugriff zu erlangen
- Anwendung von **Social Engineering**

Red Team Assessment

- Anwendung von Taktiken, Techniken und Prozeduren (TTPs) eines **echten Angreifers**
- Überprüfung des Blue Teams
- Red Team hat hohe Priorität, **unbemerkt zu bleiben**
- Ausführliche Nachbesprechung

Phishing Kampagne

- Überprüfung der Security Awareness von Mitarbeitenden
- Diverse Möglichkeiten, mit und ohne Erfassung von Zugangsdaten
- **Anonymisierte Auswertung**

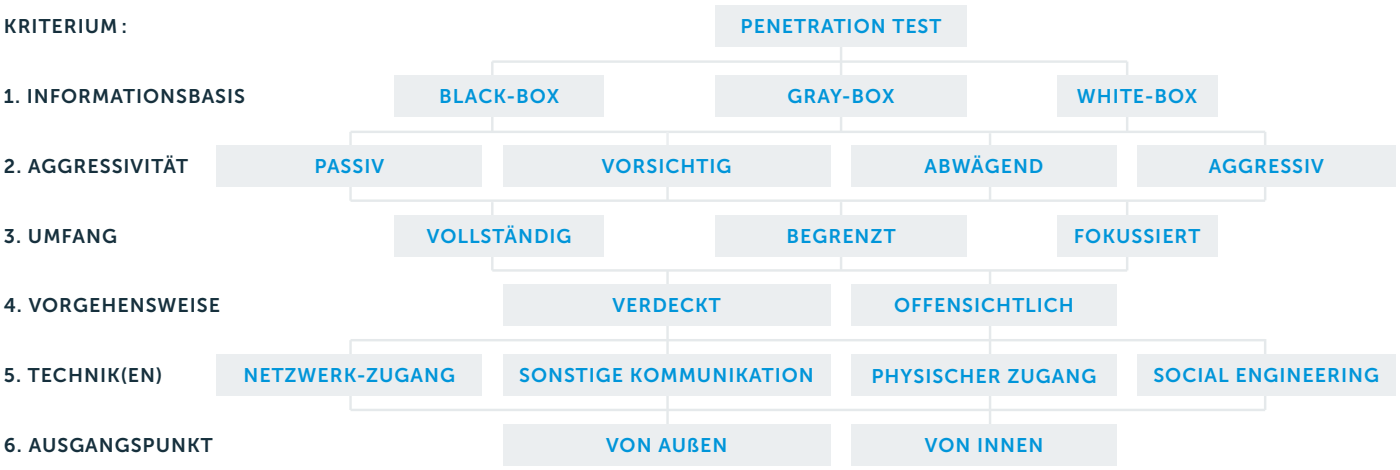
WARUM ICS?

- **Expertenwissen:** Fundierte Erfahrung im IT- und OT-Penetration Testing, auch für KRITIS Unternehmen.
- **Maßgeschneiderte Lösungen:** Beliebige Konfiguration des Projektes gemäß BSI Klassifikation.
- **Höchste Qualität:** Penetration Tests mit fester Scope-Definition zur Aufrechterhaltung Ihrer Wertschöpfungsketten.
- **Vertraulichkeit:** Höchster Schutz Ihrer sensiblen Daten.

OFFENSIVE SECURITY

INDIVIDUELLE ANPASSUNG DER KONFIGURATION IHRES PENETRATION TESTS

KLASSIFIKATION NACH BSI



PROZESSABLAUF

Informationsbeschaffung

1 AUFKLÄREN & SCANNEN

- Internet- und Serveradressen und Komponenten
- Prüfung der IP-Adresse auf Aktivitäten
- Domänen der Internetpräsenz erfassen
- Analyse der Betriebssysteme, Protokolle und Ports
- Schwachstellen identifizieren

Penetration Test

2 EINDRINGEN & BEREINIGEN

- Zielsystem angreifen
- Zugang zum System verschaffen
- Zugriffsrechte im System erweitern

Nach Abschluss der Tests:

- Wiederherstellung des ursprünglichen Zustandes
- Erstellte Accounts löschen
- Konfigurationen zurücksetzen
- Abnahmebericht

Penetration Test Report

3 BERICHTERSTELLUNG & MASSNAHMENKATALOG

- Vorgehen und Testfälle
- Identifizierte Sicherheitslücken
- Risikobewertung je Schwachstelle
- Bewertung mit CVSS
- Maßnahmen der Systemhärtung

Optional: Schließen der Lücken

4 UMSETZUNG SYSTEMHÄRTUNG

- Unterstützung beim Schließen der Sicherheitslücken
- Bei Bedarf: Definition alternativer Maßnahmen (z.B. bei Bestandstechnik)

ICS GmbH
+49 711 21037-42
vertrieb@ics-gmbh.de
think-safe-think-ics.de