Possehl Secure

# ANGEBOTSKATALOG PENETRATIONSTESTS

**Possehl Secure GmbH**

08.08.2025

Version 1.0

**Possehl Secure GmbH**
Eiler Straße 3N | 51107 Köln | +49 221 466195-20 | info@possehl-secure.de
Geschäftsleitung: Michael Gentzen (Geschäftsführer), Michael Sieben (Geschäftsführer), Christian Ehlen (Prokurist)
Sitz der Gesellschaft: Köln | Amtsgericht Köln | HRB 62035 | Ust-IdNr. DE 814929728
Commerzbank AG | BIC: COBADEFF508 | IBAN: DE 74 5084 0005 0362 1869 00

**www.possehl-secure.de**

# Versionshistorie

| Version | Datum | Beschreibung |
|---|---|---|
| 1.0 | 08.08.2025 | Initiale Version |

© Copyright Possehl Secure GmbH

Dieses Dokument ist urheberrechtlich geschützt. Alle Rechte vorbehalten.

Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung der Possehl Secure GmbH urheberrechtswidrig und damit strafbar.

In diesem Dokument werden eingetragene Warenzeichen, Handelsnamen und Gebrauchsnamen verwendet. Auch wenn diese nicht als solche gekennzeichnet sind, gelten die entsprechenden Schutzbestimmungen.

# Inhalt


1 Einleitung ..... 4

2 Leistungsspezifikationen ..... 5

2.1 Externer Penetrationstest ..... 5

2.2 Interner Penetrationstest ..... 6

2.3 Spear-Phishing ..... 7

2.4 Penetrationstest einer Webanwendung ..... 8

2.5 White-Box Penetrationstest einer (Web-)Anwendung ..... 9

2.6 Mobile-App-Assessment (Android) ..... 10

2.7 USB-Drop-Assessment ..... 11

2.8 Stolen-Asset-Assessment ..... 13

2.9 WiFi-Assessment ..... 13

2.10 Cloud-Assessment ..... 14

2.11 Microsoft 365 Audit ..... 15

2.12 Red-Team-Assessment ..... 16

3 Anhang ..... 19

3.1 Definitionen ..... 19

# 1 Einleitung

Possehl Secure GmbH ist ein auf IT-Sicherheit spezialisiertes Beratungsunternehmen mit umfangreicher Erfahrung im Testen, Beraten, Umsetzen und im Betrieb von Sicherheitslösungen. Possehl Secure GmbH verfügt über langjährige professionelle Erfahrung auf dem Gebiet der Penetrationstests. Die Berater sind von anerkannten Instituten zertifiziert – z.B. Offensive Security Certified Professional (OSCP), Offensive Security Experienced Pentester (OSEP), und Offensive Security Certified Expert 3 (OSCE3).

Dieses Dokument spezifiziert unsere angebotenen Leistungen und Konditionen.

# 2 Leistungsspezifikationen

## 2.1 Externer Penetrationstest

Als externer Penetrationstest wird die Überprüfung des Netzwerk-Perimeters bezeichnet, d.h. über das öffentliche Internet zugänglicher IT-Dienste.

### 2.1.1 Testdefinition

Folgende Leistungen werden erbracht:

- Feststellen aus dem Internet erreichbarer Adressen und Dienste
- Enumeration von Software und Versionen
- Überprüfung auf bekannte Schwachstellen und Fehlkonfigurationen
- Demonstration der Ausnutzung von Schwachstellen und Fehlkonfigurationen

Es wird ein Grey-Box-Verfahren angewendet, d.h. die Tester erhalten im Vorfeld Informationen über IP-Adressen und Domainnamen.

Die Leistungen werden unter Verwendung von Taktiken, Techniken und Prozeduren, durchgeführt, die ein gewöhnlicher Angreifer anwenden würde.

### 2.1.2 Lieferumfang

Der folgende Lieferumfang wird vereinbart:

- Abschlussbericht
  - Management Summary
  - Liste von Schwachstellen und Fehlkonfigurationen
  - Risikobasierte Priorisierung der Ergebnisse
  - Detaillierte Gegenmaßnahmen
- *(Optional)* Ergebnispräsentation oder Workshop zur Ergebnisbesprechung

### 2.1.3 Mitwirkungspflichten

Vom Kunden sind folgende Mitwirkungspflichten zu erfüllen:

- Benennung eines Ansprechpartners für technische Fragen
- Benennung des Prüfzeitraumes
- Benennung der gewünschten Sprache des Reports (Englisch/Deutsch)
- Lieferung der externen IP-Adressen und Domainnamen (Scope)
- Ggf. Freischaltung bei Web-Application-Firewalls (WAF) oder Intrusion-Prevention-Systemen (IPS)

## 2.2 Interner Penetrationstest

Als interner Penetrationstest wird die Überprüfung des internen Netzwerks verstanden. Hierbei wird ein sogenannter „Assume Breach“-Ansatz verfolgt, der von einem kompromittierten niedrig privilegierten Benutzer im Netzwerk ausgeht.

### 2.2.1 Testdefinition

Folgende Leistungen werden erbracht:

- Feststellen im internen Netzwerk erreichbarer Adressen und Dienste
- Enumeration von Software und Versionen
- Überprüfung auf bekannte Schwachstellen und Fehlkonfigurationen
- Überprüfung, ob die Windows Domäne sicher konfiguriert ist
- Demonstration der Ausnutzung von Schwachstellen und Fehlkonfigurationen
- Überprüfung, ob laterale Bewegungen (Netzwerkausbreitung) und/oder Privilegieneskalation möglich sind

Es wird ein Grey-Box-Verfahren angewendet, d.h. die Tester erhalten im Vorfeld Informationen über IP-Adressen und Domainnamen sowie einen niedrig privilegierten Benutzeraccount.

Die Leistungen werden unter Verwendung von Taktiken, Techniken und Prozeduren, durchgeführt, die ein gewöhnlicher Angreifer anwenden würde.

### 2.2.2 Lieferumfang

Der folgende Lieferumfang wird vereinbart:

- Abschlussbericht
    - Management Summary
    - Liste von Schwachstellen und Fehlkonfigurationen
    - Risikobasierte Priorisierung der Ergebnisse
    - Detaillierte Gegenmaßnahmen
- *(Optional)* Ergebnispräsentation oder Workshop zur Ergebnisbesprechung

### 2.2.3 Mitwirkungspflichten

Vom Kunden sind folgende Mitwirkungspflichten zu erfüllen:

- Benennung eines Ansprechpartners für technische Fragen
- Benennung des Prüfzeitraumes
- Benennung der gewünschten Sprache des Reports (Englisch/Deutsch)

- Einrichtung und Betrieb sowie Sicherstellen der Erreichbarkeit der bereitgestellten Pentest-VM (Unterstützung durch Possehl Secure bei Bedarf möglich)
- Bereitstellen eines niedrig privilegierten Domänen-Benutzers („Standardmitarbeiter“-Account)
- Ggf. Freischaltung bei Web-Application-Firewalls (WAF) oder Intrusion-Prevention-Systemen (IPS)

## 2.3 Spear-Phishing

Als Spear-Phishing werden gezielte Angriffe auf Benutzer per E-Mail bezeichnet. Benutzer werden dazu verleitet, auf einen Link zu klicken und ihre Anmeldedaten einzugeben, die dann abgegriffen werden. Das Ziel der Kampagne ist die Überprüfung der technischen Maßnahmen gegen Spear-Phishing sowie die Überprüfung der Verhaltensweisen der Benutzer.

### 2.3.1 Testdefinition

Folgende Leistungen werden erbracht:

- Durchführung von gezielten Angriffen auf Nutzer in einer maßgeschneiderten E-Mail-Kampagne
- Prüfung des Nutzerverhaltens im Umgang mit Spear-Phishing-E-Mails
- Validierung der Wirksamkeit aktueller technischer und organisatorischer Sicherheitsmaßnahmen im Zusammenhang mit der E-Mail-Kommunikation

### 2.3.2 Lieferumfang

Der folgende Lieferumfang wird vereinbart:

- Abschlussbericht
  - Management Summary
  - Dokumentation der durchgeführten Kampagne
  - Ergebnisse der durchgeführten Kampagne
  - Detaillierte Gegenmaßnahmen zur Verringerung der Wirksamkeit von Spear-Phishing-Kampagnen
- *(Optional)* Ergebnispräsentation oder Workshop zur Ergebnisbesprechung

### 2.3.3 Mitwirkungspflichten

Vom Kunden sind folgende Mitwirkungspflichten zu erfüllen:

- Benennung eines Ansprechpartners für technische Fragen
- Benennung des Prüfzeitraumes

- Benennung der gewünschten Sprache des Reports (Englisch/Deutsch)
- Bereitstellung der Empfängerliste (E-Mail-Adressen)
- Bereitstellung von weiteren Informationen für die Vorbereitung der Kampagne in Absprache mit Possehl Secure (z.B. geeignete Absender, extern erreichbare Portale, optische Details, Storyline)

## 2.4 Penetrationstest einer Webanwendung

Der Penetrationstest einer Webapplikation dient der gezielten Analyse der Sicherheit einer webbasierten Anwendung. Ziel ist es, Schwachstellen zu identifizieren, die von authentifizierten oder anonymen Angreifern ausgenutzt werden könnten, um unberechtigten Zugriff zu erlangen, Daten zu manipulieren oder zu exfiltrieren.

### 2.4.1 Testdefinition

Folgende Leistungen werden erbracht:

- Identifikation und Analyse technischer Schwachstellen, orientiert an den OWASP Top 10[1] (z. B. XSS, SQL Injection, CSRF, IDOR)
- Überprüfung der Zugriffskontrollen und Benutzerrechte (horizontal und vertikal)
- Analyse der Authentifizierungs- und Session-Management-Mechanismen
- Identifikation unsicherer Konfigurationen und veralteter Komponenten
- Prüfung der Client-seitigen Sicherheit (z. B. JavaScript, lokale Speicherung)
- *(Optional)* Überprüfung von APIs und mobilen Frontends der Anwendung

Es wird ein Grey-Box-Verfahren angewendet, d. h. die Tester erhalten ggf. Zugang zu Benutzerkonten mit unterschiedlichen Berechtigungsstufen innerhalb der Anwendung.

### 2.4.2 Lieferumfang

Der folgende Lieferumfang wird vereinbart:

- Abschlussbericht
  - Management Summary
  - Liste von Schwachstellen und Fehlkonfigurationen
  - Risikobasierte Priorisierung der Ergebnisse
- Detaillierte Gegenmaßnahmen
- *(Optional)* Ergebnispräsentation oder Workshop zur Ergebnisbesprechung

[1] https://owasp.org/www-project-top-ten/

### 2.4.3 Mitwirkungspflichten

Vom Kunden sind folgende Mitwirkungspflichten zu erfüllen:

- Benennung eines Ansprechpartners für technische Fragen
- Benennung des Prüfzeitraumes (inkl. Wartungsfenster oder Downtimes)
- Bereitstellung von Informationen zum Scope (URLs)
- Ggf. Freischaltung bei Web-Application-Firewalls (WAF) und Zugangsdaten für vorgeschaltete Authentifizierungsmechanismen
- Benennung der gewünschten Sprache des Reports (Englisch/Deutsch)
- Testnutzerkonten mit unterschiedlichen Berechtigungen
- *(Optional)* Bereitstellung von API-Dokumentationen
- *(Optional)* Bereitstellung spezifischer Testdaten, z.B. Gutscheincodes oder Rabattaktionen, Dummy-Zahlungsmethoden

## 2.5 White-Box Penetrationstest einer (Web-)Anwendung

Ein White-Box Penetrationstest einer (Web-)Anwendung ist eine Erweiterung des Black-Box-Tests gemäß Abschnitt 2.4. Dabei wird zusätzlich der Quellcode der Anwendung auf Sicherheitslücken und Schwachstellen untersucht. Diese kombinierte Methodik aus statischer und dynamischer Analyse erhöht die Effizienz und Tiefe der Prüfung, da bestimmte Arten von Schwachstellen – insbesondere in der Zugriffskontrolle oder Business-Logik – im Code leichter identifizierbar sind als durch reine externe Tests.

### 2.5.1 Testdefinition

Folgende Leistungen werden erbracht:

- Identifikation und Analyse technischer Schwachstellen, orientiert an den OWASP Top 10[2] (z. B. XSS, SQL Injection, CSRF, IDOR)
- Überprüfung der Zugriffskontrollen und Benutzerrechte (horizontal und vertikal)
- Analyse der Authentifizierungs- und Session-Management-Mechanismen
- Identifikation unsicherer Konfigurationen und veralteter Komponenten
- Prüfung der Client-seitigen Sicherheit (z. B. JavaScript, lokale Speicherung)
- Überprüfung der sicheren Speicherung von sensiblen Daten (Passwörter, Tokens, Schlüssel; nicht möglich bei Black-Box)
- Überprüfung von Logging und Error Handling (nicht möglich bei Black-Box)
- Prüfung der Business-Logik auf Missbrauchsmöglichkeiten (oft nicht möglich bei Black-Box)
- *(Optional)* Überprüfung von APIs und mobilen Frontends der Anwendung

[2] https://owasp.org/www-project-top-ten/

### 2.5.2 Lieferumfang

Der folgende Lieferumfang wird vereinbart:

- Abschlussbericht in englischer Sprache
  - Management Summary
  - Dokumentation der vorgefundenen Umsetzung und Risikoeinschätzung, strukturiert nach OWASP Top 10
  - Liste von Schwachstellen und Fehlkonfigurationen
  - Detaillierte Gegenmaßnahmen
- *(Optional)* Ergebnispräsentation oder Workshop zur Ergebnisbesprechung

### 2.5.3 Mitwirkungspflichten

Vom Kunden sind folgende Mitwirkungspflichten zu erfüllen:

- Benennung eines Ansprechpartners für technische Fragen
- Benennung des Prüfzeitraumes
- Bereitstellung von Informationen zum Scope (URLs)
- Bereitstellung des Quellcodes der Anwendung
- *(Optional)* Bereitstellung von Dokumentation zu Architektur, Schnittstellen, Rollenmodell, API
- Testnutzerkonten mit unterschiedlichen Berechtigungen
- *(Optional)* Bereitstellung spezifischer Testdaten: z.B. Gutscheincodes oder Rabattaktionen, Dummy-Zahlungsmethoden

## 2.6 Mobile-App-Assessment (Android)

Das Mobile-App-Assessment dient dazu, mögliche Schwachstellen in Android-Applikationen aufzudecken, die genutzt werden können, um unbefugten Zugriff auf Unternehmensressourcen oder sensible Daten zu ermöglichen.

### 2.6.1 Testdefinition

Folgende Leistungen werden erbracht:

- Testen der verwendeten Frameworks und Konfigurationen auf mögliche Schwachstellen
- Überprüfung, ob unbefugter Zugriff auf Unternehmensressourcen oder sensible Daten erlangt werden kann

Es wird ein Grey-Box-Verfahren angewendet, d.h. die Tester erhalten ggf. Zugang zu niedrig privilegierten Accounts in der App.

### 2.6.2 Lieferumfang

Der folgende Lieferumfang wird vereinbart:

- Abschlussbericht
  - Management Summary
  - Liste von Schwachstellen und Fehlkonfigurationen
  - Risikobasierte Priorisierung der Ergebnisse
  - Detaillierte Gegenmaßnahmen
- *(Optional)* Ergebnispräsentation oder Workshop zur Ergebnisbesprechung

### 2.6.3 Mitwirkungspflichten

Vom Kunden sind folgende Mitwirkungspflichten zu erfüllen:

- Benennung eines Ansprechpartners für technische Fragen
- Bereitstellung der Android-Applikation im apk-Format oder als Verweis auf Google Play
- *(Optional)* Bereitstellung niedrig privilegierter Accounts
- *(Optional)* Bereitstellung von Test-Hardware
- Benennung des Prüfzeitraumes
- Benennung der gewünschten Sprache des Reports (Englisch/Deutsch)

## 2.7 USB-Drop-Assessment

Ein USB-Drop-Assessment simuliert einen realistischen Angriff durch präparierte USB-Sticks, die gezielt an öffentlich zugänglichen Orten in der Nähe des Unternehmens platziert werden. Ziel ist es, die Bereitschaft von Mitarbeitenden zu testen, unbekannte Geräte anzuschließen, und technische Schutzmaßnahmen auf Endgeräten zu prüfen. Die eingesetzten USB-Geräte simulieren eine Tastatur (HID) und werden in der Regel nicht als Massenspeicher erkannt, wodurch herkömmliche EDR-Lösungen sie oft nicht blockieren und daher Code ausgeführt werden kann.

### 2.7.1 Testdefinition

Folgende Leistungen werden erbracht:

- Bereitstellung präparierter USB-Sticks, die eine Tastatur-Emulation (HID) nutzen
- Ausführung einfacher bis komplexer Payloads (z. B. ein `curl`-Aufruf an einen kontrollierten Server oder eine Reverse Shell), um die Nutzung und Reaktion zu erfassen
- Optional: Zweistufiges Testverfahren:
  1) Technischer Test (sofern ein Kunden-Laptop zur Verfügung gestellt wird):

    - Prüfung, ob technische Sicherheitsmaßnahmen (z. B. Device Control, Execution Prevention) umgangen werden können
    - Versuch, eine Reverse Shell aufzubauen oder andere persistente Kommandos auszuführen

  2) Social-Engineering-Test:
    - Verteilung von USB-Sticks im Umfeld des Unternehmens (z. B. Eingangsbereiche, Kantine, Parkplätze)
    - Aufzeichnung von Zugriffen durch einfache Webrequests zum Kontrollserver

Das Assessment wird entweder als Black-Box- oder Grey-Box-Test durchgeführt.

- Black-Box, wenn nur die Verteilung der USB-Sticks erfolgt, ohne weitere Informationen
- Grey-Box, wenn zusätzlich ein Kunden-Laptop für technische Tests bereitgestellt wird, inklusive Benutzerzugang, um Sicherheitsmaßnahmen gezielt zu prüfen

### 2.7.2 Lieferumfang

Der folgende Lieferumfang wird vereinbart:

- Abschlussbericht
    - Management Summary
    - Liste von Schwachstellen und Fehlkonfigurationen
    - Risikobasierte Priorisierung der Ergebnisse
- Detaillierte Gegenmaßnahmen
- *(Optional)* Ergebnispräsentation oder Workshop zur Ergebnisbesprechung

### 2.7.3 Mitwirkungspflichten

Vom Kunden sind folgende Mitwirkungspflichten zu erfüllen:

- Benennung eines Ansprechpartners für technische Fragen
- Benennung des Prüfzeitraumes und ggf. gewünschter Verteilungsschwerpunkte (z. B. Standort, Gebäude)
- Benennung der gewünschten Sprache des Reports (Englisch/Deutsch)
- Zustimmung zur Platzierung von USB-Geräten in öffentlichen oder halböffentlichen Bereichen des Unternehmens
- *(Optional)* Bereitstellung eines typischen Unternehmensendgeräts (Laptop/Notebook) für technische Tests. Das Gerät sollte ein typisches Setup mit EDR (Endpoint Protection) und Benutzerkonfiguration haben. Ein Benutzerkonto mit entsprechenden Zugriffsrechten ist ebenfalls bereitzustellen.

## 2.8 Stolen-Asset-Assessment

Bei einem Stolen-Asset-Assessment wird die Sicherheit eines entwendeten Gerätes wie z.B. eines Firmen-Laptops geprüft, um mögliche Risiken für das Unternehmen aufzudecken.

### 2.8.1 Testdefinition

Folgende Leistungen werden erbracht:

- Feststellen und mögliches Umgehen von physischen Sicherheitsmaßnahmen
- Feststellen und mögliches Umgehen von technischen Sicherheitsmaßnahmen
- Überprüfung, ob eine Exfiltration sensibler Daten möglich ist
    - Überprüfung, ob das Asset von einem unbefugten Dritten genutzt werden kann, um sich Zugang zu Unternehmensressourcen zu beschaffen

Es wird ein Black-Box-Verfahren angewendet, d.h. die Tester erhalten neben dem Gerät keine weiteren Informationen vom Kunden.

### 2.8.2 Lieferumfang

Der folgende Lieferumfang wird vereinbart:

- Abschlussbericht
    - Management Summary
    - Liste von Schwachstellen und Fehlkonfigurationen
    - Risikobasierte Priorisierung der Ergebnisse
    - Detaillierte Gegenmaßnahmen
- *(Optional)* Ergebnispräsentation oder Workshop zur Ergebnisbesprechung

### 2.8.3 Mitwirkungspflichten

Vom Kunden sind folgende Mitwirkungspflichten zu erfüllen:

- Benennung eines Ansprechpartners für technische Fragen
- Benennung des Prüfzeitraumes
- Benennung der gewünschten Sprache des Reports (Englisch/Deutsch)
- Übersendung des zu testenden Assets

## 2.9 WiFi-Assessment

Das WiFi-Assessment dient dazu, Schwachstellen in der WiFi-Infrastruktur des Kunden aufdecken, die genutzt werden können, um unbefugten Zugriff auf unternehmensinterne Ressourcen zu ermöglichen.

### 2.9.1 Testdefinition

Folgende Leistungen werden erbracht:

- Testen der eingesetzten WiFi-Protokolle und -Konfigurationen auf mögliche Schwachstellen

Es wird ein Grey-Box-Verfahren angewendet, d.h. die Tester erhalten physischen Zugang zu den jeweiligen Standorten des Unternehmens, in denen der Test stattfinden soll.

### 2.9.2 Lieferumfang

Der folgende Lieferumfang wird vereinbart:

- Abschlussbericht
  - Management Summary
  - Liste von Schwachstellen und Fehlkonfigurationen
  - Risikobasierte Priorisierung der Ergebnisse
  - Detaillierte Gegenmaßnahmen
- *(Optional)* Ergebnispräsentation oder Workshop zur Ergebnisbesprechung

### 2.9.3 Mitwirkungspflichten

Vom Kunden sind folgende Mitwirkungspflichten zu erfüllen:

- Benennung eines Ansprechpartners für technische Fragen
- Benennung der jeweiligen Standorte
- Zugang zu den Standorten, falls auch auf dem Gelände des Kunden getestet werden soll
- Benennung des Prüfzeitraumes
- Benennung der gewünschten Sprache des Reports (Englisch/Deutsch)

## 2.10 Cloud-Assessment

Bei einem Cloud-Assessment werden die Cloud-Infrastruktur und genutzte Services systematisch auf Sicherheitslücken, Fehlkonfigurationen sowie potenzielle Maßnahmen zur Verbesserung der Sicherheit geprüft.

### 2.10.1 Testdefinition

Folgende Leistungen werden erbracht:

- Analyse der Cloud-Konfiguration und Berechtigungen auf Basis eines bereitgestellten Benutzerkontos mit Leseberechtigungen
- Überprüfung von Sicherheitsrichtlinien, Zugriffskontrollen und Rollenmodellen

- Prüfung auf potenzielle Fehlkonfigurationen, übermäßige Berechtigungen und ungenutzte Ressourcen
- Bewertung der Umsetzung sicherheitsrelevanter Mechanismen wie Verschlüsselung, Netzwerksegmentierung und Logging
- Identifikation von Lücken in bestehenden Prozessen, z. B. fehlende Notfallkonten

Es wird ein Grey-Box-Verfahren angewendet, bei dem die Tester Zugriff auf ein Benutzerkonto mit Leseberechtigungen erhalten, um die Cloud-Konfiguration und Sicherheitsmaßnahmen zu prüfen.

### 2.10.2 Lieferumfang

Der folgende Lieferumfang wird vereinbart:

- Abschlussbericht
  - Management Summary
  - Liste von Schwachstellen und Fehlkonfigurationen
  - Risikobasierte Priorisierung der Ergebnisse
- Detaillierte Gegenmaßnahmen
- *(Optional)* Ergebnispräsentation oder Workshop zur Ergebnisbesprechung

### 2.10.3 Mitwirkungspflichten

Vom Kunden sind folgende Mitwirkungspflichten zu erfüllen:

- Benennung eines Ansprechpartners für technische Fragen
- Benennung des Prüfzeitraumes
- Bereitstellung eines Benutzerkontos mit Leseberechtigungen für das zu prüfende Cloud-Projekt
- Benennung der gewünschten Sprache des Reports (Englisch/Deutsch)

## 2.11 Microsoft 365 Audit

Bei einem Microsoft 365 (M365) Audit werden die Microsoft 365 und Entra ID-Konfiguration systematisch auf Fehlkonfigurationen sowie potenzielle Maßnahmen zur Verbesserung der Sicherheit geprüft.

### 2.11.1 Testdefinition

Folgende Leistungen werden erbracht:

- Analyse der Microsoft 365 / Entra ID-Konfiguration und Berechtigungen auf Basis eines bereitgestellten Benutzerkontos mit entsprechender Administrationsrolle im Entra ID

- Überprüfung von Conditional Access Policies, MFA und weiteren Sicherheitsrichtlinien laut des aktuellen Microsoft 365 Foundations Benchmark des Center of Internet Security (CIS)
- Prüfung auf potenzielle Fehlkonfigurationen
- Teilautomatisierte Überprüfung des M365 Tenants mittels Security Assessment Tools (PowerShell Script basiert)
- Manuelle Checks zur Komplettierung des Audits

### 2.11.2 Lieferumfang

Der folgende Lieferumfang wird vereinbart:

- Abschlussbericht
- Bereitstellung des aktuellen M365 Foundations Benchmarks in Form einer PDF-Datei
- Bereitstellung der Prüfungsergebnisse im Excel-Format
- Bereitstellung einer PDF-Datei mit zusammenfassendem Ergebnis des M365 Audits
- *(Optional)* Ergebnispräsentation oder Workshop zur Ergebnisbesprechung

### 2.11.3 Mitwirkungspflichten

Vom Kunden sind folgende Mitwirkungspflichten zu erfüllen:

- Benennung eines Ansprechpartners für technische Fragen
- Bereitstellung eines Admin Benutzers im Microsoft 365 Tenant zur Durchführung des Audits (die Admin Berechtigung wird maximal 4-5 Stunden benötigt)
- Benennung des Prüfzeitraumes
- Benennung der gewünschten Sprache der Ergebniszusammenfassung (Englisch/Deutsch)

## 2.12 Red-Team-Assessment

Ziel eines Red-Team-Assessments ist es, die gesamte Sicherheitslage der Organisation zu testen, indem ein realistischer Angriff ohne vorherige Informationen über das Unternehmen simuliert wird.

Es wird ein zu erreichendes Ziel definiert (z.B. die Kompromittierung eines bestimmten internen Systems oder das Erlangen von Zugriff auf bestimmte interne Daten), das ohne Einschränkung der möglichen Angriffsvektoren zu erreichen ist. Neben technischen Angriffen können auch Social-Engineering und die Penetration von physischen Assets zum Einsatz kommen.

Im Allgemeinen kennt nur der direkte Auftraggeber den Umfang, Zielsetzung und Zeitraum der Durchführung, die zuständigen unternehmensinternen Abteilungen (IT, SOC oder Gebäudesicherheit) werden nicht vorab informiert.

### 2.12.1 Testdefinition

Folgende Leistungen werden erbracht:

- Feststellung der Reaktionsfähigkeit und Effektivität der vom Kunden eingesetzten Schutzmechanismen, Prozesse und Technologien unter Erreichung eines vom Kunden vorgegebenen Ziels

Es wird ein Black-Box-Verfahren angewendet, d.h. die Tester erhalten im Vorfeld keine Informationen über das Unternehmen, die nicht öffentlich zugänglich sind.

### 2.12.2 Lieferumfang

Der folgende Lieferumfang wird vereinbart:

- Abschlussbericht
  - Management Summary
  - Liste der ausgenutzten Schwachstellen, die zur Erreichung des Ziels geführt haben
  - Detaillierte Gegenmaßnahmen
- *(Optional)* Ergebnispräsentation oder Workshop zur Ergebnisbesprechung

### 2.12.3 Mitwirkungspflichten

Vom Kunden sind folgende Mitwirkungspflichten zu erfüllen:

- Benennung eines 24/7 erreichbaren Ansprechpartners mit der Befugnis und den Möglichkeiten, das Assessment zu stoppen und betroffene Abteilungen/Personen innerhalb der Organisation zu informieren
- Ausstellen eines Dokuments, das die jeweiligen Tester gegenüber unwissenden Parteien als autorisiert ausweist, den Test durchzuführen, und die jeweiligen Ansprechpartner beinhaltet („Get out of Jail“-Card)
- Benennung der Ziele, die erreicht werden sollen
- Benennung des Prüfzeitraumes
- Benennung der gewünschten Sprache des Reports (Englisch/Deutsch)

### 2.12.4 Physical-Assessment

Ziel eines Physical-Assessments im Rahmen einer Red-Teaming-Operation ist das Eindringen in Gebäude vor Ort durch Überwindung möglicher Sicherheitssysteme und

Prozesse. Es wird ein spezifisches Ziel definiert, das nach erfolgreichem Eindringen erreicht werden muss.

#### 2.12.4.1 Testdefinition

Folgende Leistungen werden erbracht:

- Auffinden von Schwachstellen in vor Ort bestehenden Sicherheitskonzepten
- Unbemerktes Eindringen in das Gebäude
- Anschluss eigener Hardware / Erbringung eines Nachweises über erfolgtes Eindringen

#### 2.12.4.2 Lieferumfang

Der folgende Lieferumfang wird vereinbart:

- Abschlussbericht
- Management Summary
- Liste der ausgenutzten Schwachstellen, die zur Erreichung des Ziels geführt haben
- Detaillierte Gegenmaßnahmen
- *(Optional)* Ergebnispräsentation oder Workshop zur Ergebnisbesprechung

#### 2.12.4.3 Mitwirkungspflichten

Vom Kunden sind folgende Mitwirkungspflichten zu erfüllen:

- Benennung eines 24/7 erreichbaren Ansprechpartners mit der Befugnis und den Möglichkeiten, das Assessment zu stoppen und betroffene Abteilungen/Personen innerhalb der Organisation zu informieren
- Ausstellen eines Dokuments, das die jeweiligen Tester gegenüber unwissenden Parteien als autorisiert ausweist, den Test durchzuführen, und die jeweiligen Ansprechpartner beinhaltet („Get out of Jail“-Card)
- Benennung der Ziele, die erreicht werden sollen
- Benennung des Prüfzeitraumes
- Benennung der gewünschten Sprache des Reports (Englisch/Deutsch)

# 3 Anhang

## 3.1 Definitionen

**Penetrationstest**: Kontrollierter Versuch, in ein bestimmtes Computersystem oder Netzwerk einzudringen, um existierende Schwachstellen zu identifizieren und zu demonstrieren.

**Black-Box**: In einem Black-Box-Verfahren liegen im Vorhinein keine Informationen über die Umgebung und die Zielsysteme des Kunden vor (z.B. IP-Adressen). Dadurch wird der Test aus dem Blick eines externen Angreifers durchgeführt. Jedoch entstehen höhere Aufwände durch die Notwendigkeit während des Tests Informationen zu sammeln.

**White-Box**: In einem White-Box-Verfahren liegen im Vorhinein alle Informationen über die Umgebung und Zielsysteme des Kunden vor (z.B. Source-Code für eine Webapplikation). Dadurch kann deutlich tiefer geprüft werden, als es in Black-Box- oder Grey-Box-Verfahren der Fall ist.

**Grey-Box**: Ein Grey-Box-Verfahren ist eine Mischung aus Black-Box- und White-Box-Verfahren. Es werden bestimmte Informationen zur Umgebung und die Zielsysteme bekanntgegeben (z.B. IP-Adressen). Dieses Verfahren bietet ein gutes Gleichgewicht zwischen Aufwänden und Ergebnissen.