PENTARIS SECURITY

PORTFOLIO
OFFENSIVE CYBERSECURITY

DATUM: 05.06.2025
KLASSE: VERTRAULICH
VERSION: 1.4

PENTARIS SECURITY GMBH

Beim Wölfelsbrunnen 8
66346 Püttlingen
Tel.: 06806 937300
info@pentaris-security.de

Amtsgericht Saarbrücken HRB 111107
Geschäftsführer: Sebastian Froede
Firmensitz: Püttlingen
Umsatzsteuer-ID: DE453070634

Bankverbindung
Commerzbank Saarbrücken
DE46 5904 0000 0523 5098 00
COBADEFFXXX

INHALTSVERZEICHNIS

MODUL 01
ANFORDERUNGSANALYSE

Mit unserer Anforderungsanalyse stellen wir sicher, dass alle relevanten Aspekte für die Umsetzung des Projektes klar definiert und dokumentiert sind. Die Analyse hilft uns dabei, Ihre Erwartungen und Ziele zu verstehen, sowie Rahmenbedingungen zu definieren, um ein erfolgreiches Ergebnis sicherzustellen.

1.1 ZIELSETZUNG

- **Scope:** Welche Bereiche, Systeme oder Prozesse sind Teil des Projekts
- **Testtyp:** Black, grey oder white box
- **Definieren der Stakeholder:** Wer ist intern bzw. Extern verantwortlich?

1.2 RISIKEN UND HERAUSFORDERUNGEN

- **Risiken:** Identifizieren von potentiellen Risiken
- **Kritische Systeme:** Einschränkungen oder Ausschlüsse im Projektumfang
- **Externe Dienstleister:** Sind externe Dienstleister involviert?
- **Generelle Risikominimierung**

1.3 ZEITPLAN

- Definieren des **Zeitrahmens**
  - Meilensteine
  - Statusberichte
- **Regelmäßige Abstimmung** / Feedbackschleife zu den Ergebnissen

MODUL 02
OSINT (OPEN SOURCE INTELLIGENCE)

Durch unsere OSINT-Analysen untersuchen wir öffentlich zugängliche Informationen zu Ihrem Unternehmen. So decken wir auf, welche Daten bereits ohne Ihr Wissen im Netz sowie im Darknet kursieren und von Angreifern potenziell genutzt werden könnten.

Unsere OSINT-Analyse erfolgt in mehreren systematischen Schritten:

1.1 INFORMATIONSSAMMLUNG

- **Durchsuchen der öffentlichen Daten:**
  - Suchmaschinen
  - Soziale Netzwerke
  - Webseiten und Blogs
  - Foren
  - Handelsregister und Finanzberichte

1.2 AUTOMATISIERTE UND MANUELLE SUCHE

- **Manuell:** Direktes Durchsuchen von Webseiten, Profilen oder Dokumenten.
- **Automatisiert:** Nutzung von Scraping-Tools, um große Datenmengen effizient zu sammeln.

1.3 ANALYSE UND BEWERTUNG DER DATEN

- **Bewertung:** Sicherstellen, dass die genutzten Daten vertrauenswürdig und aktuell sind
- **Datenbereinigung:** Vermeiden von Dubletten und irrelevanter Daten
- **Verknüpfungen herstellen:** Beziehungen zwischen verschiedenen Datenpunkten erkennen (z. B. IP-Adressen, E-Mail-Konten, Social-Media-Profile).
- **Risikobewertung:** Sicherheitslücken, Bedrohungen oder kritische Informationen identifizieren

MODUL 03
EXTERNER PENETRATIONSTEST

Unser externer Penetrationstest simuliert realistische Cyberangriffe auf Ihre öffentlich zugänglichen Systeme, Netzwerke und Anwendungen. Durch die Identifizierung und Prüfung kritischer Schwachstellen erhalten Sie wertvolle Informationen zur Absicherung ihres digitalen Perimeters.

Unser externer Penetrationstest erfolgt in mehreren systematischen Schritten:

1.1 VORBEREITUNG

- **Scoping:** Welche Systeme, Anwendungen oder Netzwerke sollen geprüft werden?
- **Test Methode:** Black-, grey- oder Whitebox Test
- **Bereitstellung von Daten:** IP-Adressen und Domains

1.2 INFORMATIONSSAMMLUNG (RECONNAISSANCE)

- **Passive Informationssammlung:** Sammeln von Informationen, ohne direkten Kontakt mit den Zielsystemen (z. B. durch DNS-Abfragen, WHOIS-Daten, öffentlich zugängliche Informationen)
- **Aktive Informationssammlung:** Direkte Interaktion mit Zielsystemen, z. B. durch Port-Scans, Netzwerk-Mapping oder Analyse von Diensten

1.3 SCHWACHSTELLENANALYSE

- **Identifizierung von Schwachstellen:** Analyse von Diensten, Software-Versionen und Konfigurationen auf bekannte Schwachstellen.
- **Manuelle Verifizierung:** Überprüfung der Ergebnisse aus automatisierten Tools, um Fehlalarme (False Positives) zu vermeiden.

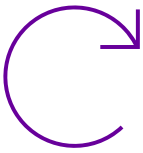
1.4 EXPLOITATION

- **Ausnutzen der Sicherheitslücken:** Simulation von Angriffen, um zu prüfen, ob die identifizierten Schwachstellen tatsächlich ausnutzbar sind durch Exploit-Frameworks und individuell erstellten Skripte.

- **Systemzugriff bewerten:** Ermittlung des Umfangs des Zugriffs (z. B. Zugriff auf vertrauliche Daten oder Systemkontrolle).

1.5 BEWERTUNG MONITORING

- **Monitoring:** Validierung von Alarm- und Überwachungssystemen (z. B. IDS/IPS)



1.6 RETEST (OPTIONAL)

- Überprüfung, ob die empfohlenen Maßnahmen erfolgreich umgesetzt wurden

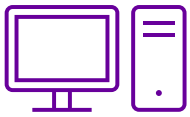
MODUL 04
INTERNER PENETRATIONSTEST

Ein interner Penetrationstest zielt darauf ab, Sicherheitslücken innerhalb der IT-Infrastruktur eines Unternehmens zu identifizieren, indem der Angreifer bereits im internen Netzwerk positioniert wird.

Unser interner Penetrationstest erfolgt in mehreren systematischen Schritten:

1.1 VORBEREITUNG

- **Scoping:** Welche Systeme, Anwendungen oder Netzwerke innerhalb des internen Netzwerks sollen getestet werden?
- **Testmethode:** Soll der Test mit oder ohne Zugangsdaten (z. B. AD-User) durchgeführt werden?
- **Startpunkt:** Netzwerkzugriff / VPN-Zugang oder ein dedizierter Testserver.



1.2 INFORMATIONSSAMMLUNG (RECONNAISSANCE)

- **Netzwerk-Mapping:** Identifizierung der Netzwerktopologie (Subnetze, Gateways, Firewalls, VLANs)
- **Analyse von Diensten:** Identifizierung laufender Dienste, verwendeter Ports und Versionen bzw. Konfigurationen (Service Enumeration).
- **Informationsgewinnung aus internen Ressourcen:** Nutzung freigegebener Ordner, interner Dokumentationen oder schlecht gesicherter Datenbanken

1.3 SCHWACHSTELLENANALYSE

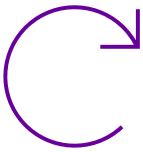
- **Identifizierung von Schwachstellen:** Analyse von Diensten, Software-Versionen und Konfigurationen auf bekannte Schwachstellen.
- **Manuelle Verifizierung:** Überprüfung der Ergebnisse aus automatisierten Tools, um Fehlalarme (False Positives) zu vermeiden.
- **Manuelle Analyse:** Suche nach spezifischen Schwachstellen, die nicht automatisiert erkannt werden, z.B. Schwächen in Benutzerkonten oder Berechtigungen

1.4 EXPLOITATION

- **Ausnutzen der Sicherheitslücken:** Simulation von Angriffen, um die identifizierten Sicherheitslücken praktisch durch Exploit-Frameworks und individuell erstellte Skripte auszunutzen.
    - Privilege Escalation
    - Passwort-Spraying / Cracking
    - Zugriff auf sensible Daten
- **Post-Exploitation:** Untersuchung der erreichbaren Daten und Systeme nach erfolgreichem Zugriff.
- **Lateral Movement:** Erweiterung der Angriffsfläche durch seitliche Bewegungen im Netzwerk
- **AD-Audit**

1.5 BEWERTUNG MONITORING

- **Monitoring:** Validierung von Alarm- und Überwachungssystemen (z. B. IDS/IPS)



1.6 RETEST (OPTIONAL)

- Überprüfung, ob die empfohlenen Maßnahmen erfolgreich umgesetzt wurden

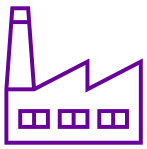
MODUL 05
OT-PENETRATIONSTEST

Unser OT-Penetrationstest simuliert realistische Angriffe auf kritische Infrastruktur, industrielle Steuerungssysteme (ICS) und OT-Netzwerke, um Schwachstellen zu identifizieren und die Sicherheit der Systeme zu verbessern. Ziel ist es, die Verfügbarkeit, Integrität und Vertraulichkeit von OT-Systemen zu schützen, ohne deren Betrieb zu stören.

Unser OT-Penetrationstest erfolgt in mehreren systematischen Schritten:

1.1 VORBEREITUNG

- **Scoping:** Welche Systeme und Komponenten z.B. SCADA-Systeme, PLCs, RTUs oder Netzwerksegmentierung sollen getestet werden?
- **Testmethode:** Soll der Test mit oder ohne Zugang zu Steuerungseinheiten durchgeführt werden?
- **Startpunkt:** Netzwerkzugriff



1.2 INFORMATIONSSAMMLUNG (RECONNAISSANCE)

- **Architekturreview:** Prüfung von Konfigurationsdateien und Netzwerkdokumentation
- **Netzwerk-Mapping:** Identifizierung von Geräten, Protokollen, Subnetzen und Schnittstellen
- **Netzwerkverkehrsanalyse:** Passives Monitoring des Datenverkehrs zur Identifikation von OT-spezifischen Protokollen wie Modbus, DNP3, IEC 60870-5-104 oder OPC UA.
- **Geräteidentifikation:** Identifikation von Steuergeräten wie PLCs (Programmable Logic Controllers), RTUs (Remote Terminal Units) und HMIs (Human-Machine Interfaces).
- **Protokollanalyse:** Untersuchung der verwendeten OT-Protokolle auf unsichere Konfigurationen oder unverschlüsselte Kommunikation.
- **Konfigurationsanalyse:** Untersuchung von Zugangskontrollen, Benutzerrechten und Passwörtern innerhalb der OT-Umgebung.

1.3 SCHWACHSTELLENANALYSE

- **Identifizierung von Schwachstellen:** Identifikation von ungesicherten Verbindungen, veralteter Firmware oder öffentlich bekannten Schwachstellen (CVE-Datenbanken).
- **Fehlkonfigurationen von Systemen:** Analyse von Steuerungssystemen (PLCs, HMI, SCADA) auf Fehlkonfigurationen und unsichere Einstellungen.
- **Default Zugänge:** Suche nach Standardpasswörtern und ungesicherten Remote-Zugriffsmöglichkeiten.
- **Überprüfung der Netzwerksegmentierung:** Test der Trennung zwischen IT- und OT-Netzwerken sowie zwischen verschiedenen OT-Segmenten.
- **Software und Firmware Überprüfung:** Identifikation von veralteten oder unsicheren Versionen.

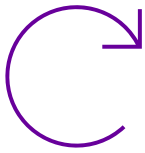
1.4 EXPLOITATION

- **Ausnutzen der Sicherheitslücken:** Simulation von Angriffen, zur Durchführung sicherer Tests, um Schwachstellen ohne Betriebsstörungen auszunutzen
- **Zugriffsmöglichkeiten:** Prüfung von Zugriffsmöglichkeiten auf Geräte und Netzwerke
- **Kiosk-Mode Ausbruchsmöglichkeiten:** Untersuchung der Ausbruchsmöglichkeiten aus dem Kiosk-Mode

Wichtig: *Alle Exploitation-Tests in OT-Umgebungen müssen extrem vorsichtig und kontrolliert durchgeführt werden, um unbeabsichtigte Störungen zu vermeiden.*

1.5 BEWERTUNG MONITORING

- **Monitoring:** Validierung von Alarm- und Überwachungssystemen (z. B. IDS/IPS)



1.6 RETEST (OPTIONAL)

- Überprüfung, ob die empfohlenen Maßnahmen erfolgreich umgesetzt wurden

MODUL 06
ENDPOINT SECURITY STRESSTEST

Mithilfe simulierter Schadsoftware testen wir die Widerstandsfähigkeit Ihrer Endpunkte und analysieren, wie sich u.a. Malware in Ihren Systemen verbreiten kann. So lassen sich Maßnahmen entwickeln, um Infektionen und deren Ausbreitung zu verhindern, sowie bereits implementierten Sicherheitsmaßnahmen bewerten.

Unser Endpoint Security Stresstest beinhalten die folgenden Schritte:

1.1 VORBEREITUNG

- **Scoping:** Welche Geräte (Windows, Linux, MacOS oder mobile Geräte) sollen getestet werden?
- **Bereitstellung Geräten und Zugangsdaten:** Bereitstellung des zu testenden Gerätes und eines AD-User (Standard, kein Admin)

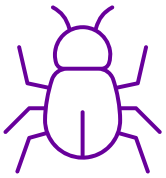
1.2 INFORMATIONSSAMMLUNG (RECONNAISSANCE)

- **Schnittstellen-Überprüfung:** Identifizieren der verfügbaren Interfaces und Schnittstellen (z.B. Bluetooth, LoRa, Zigbee, Ethernet, USB, Profibus, UART etc.) inkl. eigener Bus-Protokolle und Schnittstellen
- **Software:** Überprüfung der installierten Softwareversionen sowie eigenimplementierten Softwarekomponenten
- **VPN:** Identifizierung der VPN-Parameter

1.3 SCHWACHSTELLENANALYSE

- **Konfigurationsprüfung:** Analyse der Einstellungen von Sicherheitslösungen (z. B. Firewalls, Antivirus-Software).
- **Hardening:** Identifikation von Schwachstellen in der Gerätehärtung, wie schwache Passwörter oder deaktivierte Sicherheitsfunktionen.
- **Patch-Management prüfen:** Überprüfung, ob Betriebssysteme und Software auf dem neuesten Stand sind. Identifikation von veralteten oder unsicheren Anwendungen.

- **Sicherheitsrichtlinien validieren:** Analyse von Richtlinien wie Passwortanforderungen, Bildschirmsperre und Zwei-Faktor-Authentifizierung.
- **Netzwerkverbindungen analysieren:** Überprüfung der ein- und ausgehenden Verbindungen der Endgeräte, Zugriffe auf Netzwerksegmente sowie Identifikation von ungesicherten Ports und offenen Diensten.
- **Benutzerrechte und -rollen überprüfen:** Analyse der Berechtigungen und Rollen der Benutzer, um übermäßige Rechte zu erkennen.

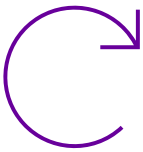


1.4 ANGRIFFSSIMULATION

- **Bewertung der Einfallsvektoren:** Überprüfung der Angriffsmöglichkeiten, z.B. USB-Sticks, E-Mail, CD-ROM, Internet
- **Simulation von Angriffen:** Durchführung von Angriffsszenarien wie Malware-Infektionen und Ransomware-Tests
- **Malware Obfuskation:** Testen von Umgehungsmöglichkeiten für Sicherheitslösungen, z. B. durch Obfuskation von Malware.
- **Prüfung der Sicherheitsmaßnahmen:** Bewertung der Erkennungs- und Reaktionsfähigkeiten von EPP (Endpoint Protection), EDR (Endpoint Detection and Response) und Firewall.

1.5 BEWERTUNG MONITORING

- **Monitoring:** Validierung von Alarm- und Überwachungssystemen (z. B. IDS/IPS)



1.6 RETEST (OPTIONAL)

- Überprüfung, ob die empfohlenen Maßnahmen erfolgreich umgesetzt wurden

MODUL 07
SOCIAL ENGINEERING

Unsere Social-Engineering-Module testen die menschliche Komponente Ihrer Sicherheitsstrategie und helfen dabei, Schwachstellen im Verhalten und den Prozessen Ihrer Mitarbeiter zu erkennen und zu beheben.

Unser Social Engineering beinhalten die folgenden Module:

1.1 PHISHING

Phishing zielt darauf ab, vertrauliche Informationen wie Passwörter, Kreditkartendaten oder persönliche Informationen zu erschleichen, indem gefälschte, vertrauenswürdige Kommunikationsmethoden verwendet werden (z. B. E-Mails oder gefälschte Webseiten).

Schritte eines Phishing-Tests

- **Vorbereitung:**
  - Analyse des Zielunternehmens und Identifikation von Kommunikationsmustern (z. B. typische E-Mail-Vorlagen).
  - Auswahl eines Szenarios, z. B. gefälschte Sicherheitswarnungen oder E-Mails von angeblichen Geschäftspartnern.
- **Erstellung einer Kampagne:**
  - Entwicklung realistischer Phishing-Nachrichten mit gefälschten Absendern.
  - Integration von Links zu speziell eingerichteten Testseiten oder Anhängen, die Aktionen der Zielpersonen protokollieren.
- **Durchführung:**
  - Versand der Phishing-E-Mails an ausgewählte Testpersonen oder Gruppen.
  - Überwachung der Reaktionen, z. B. Klicks auf Links, Eingabe von Daten oder Downloads.
- **Auswertung:**
  - Analyse der Ergebnisse: Wie viele Personen haben auf die Nachricht reagiert?
  - Empfehlungen für Sicherheitsmaßnahmen und Schulungen.

1.2 VISHING (VOICE PHISHING)

Vishing nutzt telefonische Kommunikation, um Personen dazu zu bringen, sensible Informationen preiszugeben oder bestimmte Aktionen auszuführen.

Schritte eines Vishing-Tests

- **Vorbereitung:**
  - Identifikation von Zielgruppen, z. B. Support-Teams, HR oder IT-Abteilungen.
  - Erstellung realistischer Szenarien, z. B. vorgetäuschte Anrufe von IT-Support oder Geschäftspartnern.
- **Skriptentwicklung**
  - Erstellung eines Anrufskripts mit glaubwürdigen Informationen und möglichen Fragen.
  - Festlegen von Techniken, um das Vertrauen der Zielperson zu gewinnen.
- **Durchführung:**
  - Simulieren von Anrufen mit verdeckter Identität.
  - Protokollierung der Reaktionen und der bereitgestellten Informationen.
- **Auswertung:**
  - Analyse der Anrufe: Welche Informationen wurden preisgegeben?
  - Empfehlungen zur Verbesserung der Sensibilisierung und Authentifizierungsprozesse.

1.3 MEDIA DROPPING

Media Dropping setzt auf die Neugier von Personen, indem manipulierte Speichermedien (z. B. USB-Sticks oder CDs) in Bereichen platziert werden, in denen Zielpersonen sie finden und nutzen könnten.

Schritte eines Media-Dropping-Tests

- **Vorbereitung:**
  - Erstellung manipulierter Medien mit harmloser, aber protokollierender Software, die keine Schäden verursacht.
  - Auswahl von Zielbereichen, z. B. Parkplätze, Empfangsbereiche oder Konferenzräume.
- **Platzierung:**
  - Diskrete Platzierung der Medien an Orten, an denen sie wahrscheinlich gefunden werden.
  - Überwachung der Medien, um festzustellen, ob und wo sie genutzt werden.
- **Reaktionstest:**
  - Protokollierung von Aktionen der Finder, z. B. ob die Medien angeschlossen und Inhalte geöffnet wurden.
  - Überprüfung, ob Sicherheitssoftware die Aktivität erkannt hat.
- **Auswertung:**
  - Analyse der Ergebnisse: Wie viele Personen haben die Medien genutzt?
  - Empfehlungen zur Sensibilisierung und für Richtlinien zum Umgang mit fremden Medien.

1.4 TAILGATING

Tailgating ist eine physische Social-Engineering-Technik, bei der der Angreifer unberechtigt Zugang zu gesicherten Bereichen erlangt, indem er anderen Personen folgt.

Schritte eines Tailgating-Tests

- **Vorbereitung:**
  - Analyse der physischen Sicherheitsmaßnahmen und Zugangskontrollpunkte.
  - Auswahl der Testumgebung (z. B. Büroeingänge, Lagerhallen).
- **Szenarien Planung:**
  - Entwicklung realistischer Szenarien, z. B. "verlorene Zugangskarte" oder "Lieferant mit schwerem Paket".
  - Identifikation von potenziellen Schwachstellen, z. B. mangelnde Aufmerksamkeit des Sicherheitspersonals.
- **Durchführung:**
  - Simuliertes Tailgating, z. B. durch direktes Folgen einer berechtigten Person oder höfliche Bitten um Zutritt.
  - Dokumentation des Erfolgs oder Misserfolgs der Versuche.
- **Auswertung:**
  - Analyse der Sicherheitslücken und der Reaktionen des Personals.
  - Vorschläge für verbesserte Schulungen und physische Sicherheitsmaßnahmen.

Hinweis: Jedes dieser Module kann einzeln oder kombiniert durchgeführt werden, um Schwachstellen im Verhalten von Mitarbeitern und der organisatorischen Sicherheitskultur aufzudecken.

PAKETE

Zeitraum: 1 Monat

- 1x Phishing E-Mails
- 3x USB Drops
- 1x Vishing Call
- 0x Tailgating

Zeitraum: 3 Monate

- 3x Phishing E-Mails
- 6x USB Drops
- 2x Vishing Call
- 1x Tailgating

Zeitraum: 6 Monate

- 10x Phishing E-Mails
- 10x USB Drops
- 3x Vishing Call
- 1x Tailgating

MODUL 08
REDTEAMING

Unser Red-Teaming-Ansatz testet Ihre Sicherheitsstrategien unter realistischen Bedingungen und simuliert gezielte Angriffe auf die gesamte Sicherheitsstruktur eines Unternehmens, um Schwachstellen in technischen, physischen und organisatorischen Abwehrmechanismen zu identifizieren. Ziel ist es, nicht nur technische Schwächen aufzudecken, sondern auch die Reaktion von Mitarbeitern und Sicherheitslösungen zu testen. Wir bieten Ihnen umfassende Einblicke in Ihre Sicherheitslage und konkrete Empfehlungen zur Verbesserung.

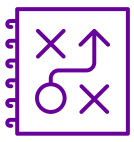
Unsere Red-Teaming beinhalten die folgenden Schritte:

1.1 VORBEREITUNG

- **Scoping:** Welche Systeme, Anwendungen oder Netzwerke und welche Sicherheitsmaßnahmen sollen getestet werden?
- **Vorgehensweise**: Festlegen der Vorgehensweise (Intensität, involvierte Personen, inkludierte Standorte/Bereiche etc.)

1.2 INFORMATIONSSAMMLUNG (RECONNAISSANCE)

- **Open Source Intelligence (OSINT)**
  - Sammeln von öffentlich zugänglichen Informationen (z. B. Social Media, Unternehmenswebsites, technische Dokumente).
  - Identifizieren potenzieller Schwachstellen, z. B. durch Social Engineering oder technische Fehlkonfigurationen.
- **Technische Informationssammlung**
  - Scannen öffentlicher IP-Adressen und Domains nach offenen Ports und Diensten.
  - Analyse von DNS-Einträgen, Netzwerkinfrastrukturen und eingesetzter Software.
- **Organisatorische Analyse**
  - Identifikation von Schlüsselpersonen, Abteilungen und Prozessen, die Ziel eines Angriffs werden könnten.



1.3 ANGRIFFSSIMULATION

- **Social Engineering**

- Durchführung gezielter Phishing-, Vishing- oder Tailgating-Angriffe, um Zugangsdaten zu erhalten oder physische Sicherheitsmaßnahmen zu umgehen.

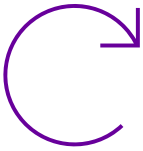
- **Technische Angriffe**
  - Nutzung von Schwachstellen in Anwendungen, Netzwerken oder Betriebssystemen, um Zugriff zu erhalten.
  - Entwicklung von Exploits, um Privilegien auszuweiten oder lateral in Netzwerke vorzudringen.
- **Physische Sicherheitstests**
  - Testen des Zugangs zu sensiblen Bereichen durch Tailgating oder gefälschte Identitäten.
  - Manipulation physischer Systeme, z. B. durch Media Dropping oder Sicherheitslücken in IoT-Geräten.

1.4 PERSISTENZ UND ESKALATION

- **Ausnutzen der Sicherheitslücken**
  - Simulation von Angriffen, um die identifizierten Sicherheitslücken praktisch durch Exploit-Frameworks und individuell erstellte Skripte auszunutzen.
    - Privilege Escalation
    - Passwort-Spraying / Cracking
    - Zugriff auf sensible Daten
- **Post-Exploitation**
  - Untersuchung der erreichbaren Daten und Systeme nach erfolgreichem Zugriff.
- **Persistenz etablieren**
  - Einrichtung versteckter Backdoors in kompromittierten Systemen.
  - Umgehung von Sicherheitslösungen wie Antivirus-Software oder Intrusion Detection Systems (IDS).
- **Lateral Movement**
  - Ausbreitung innerhalb des Netzwerks durch kompromittierte Konten oder Sicherheitslücken.
  - Zugriff auf Datenbanken, Server und andere kritische Systeme.
- **Datenexfiltration (Simulation)**
  - Testen der Möglichkeiten zur unbemerkten Übertragung sensibler Daten aus dem Netzwerk.
  - Bewertung der Reaktion von Sicherheitslösungen auf ungewöhnlichen Datenverkehr.

1.5 ANGRIFFSERKENNUNG UND - REAKTION

- **Trigger gezielter Sicherheitsalarme**
  - Testen, ob Intrusion Detection/Prevention-Systeme (IDS/IPS) Angriffe erkennen und korrekt protokollieren.
  - Bewertung der Reaktion auf verdächtige Aktivitäten.
- **Bewertung der Incident-Response-Fähigkeiten**
  - Analyse, wie schnell und effektiv das Blue Team auf den Angriff reagiert.
  - Überprüfung der Kommunikation und Eskalationsprozesse während eines Sicherheitsvorfalls.
- **Dokumentation der Schwächen**
  - Identifizierung von Lücken in der Überwachung, Analyse und Reaktion auf Bedrohungen.



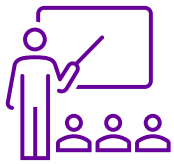
1.6 RETEST (OPTIONAL)

- Überprüfung, ob die empfohlenen Maßnahmen erfolgreich umgesetzt wurden

MODUL 09
AWARENESS TRAINING

Unsere Awareness Trainingsprogramme vermittelt Mitarbeiterinnen und Mitarbeitern das Wissen und die Fähigkeiten, um sich sicher in der digitalen Welt zu bewegen, Sicherheitsrisiken zu erkennen und proaktiv abzuwehren. Der Fokus liegt darauf, langfristig sicherheitsbewusstes Verhalten zu fördern. Durch die Sensibilisierung Ihrer Mitarbeiter minimieren Sie menschliche Schwachstellen.

Unser Awareness Training beinhalten die folgenden Schritte:



1.1 VORBEREITUNG

- **Trainingsinhalte** festlegen
- **Veranstaltungsort** definieren
- **Teilnehmeranzahl** und **Kenntnisstand**

1.2 ZIELSETZUNG

- Vermittlung eines grundlegenden Verständnisses von Cyber-Bedrohungen und deren Auswirkungen auf Ihr Unternehmen.
- Förderung eines sicherheitsbewussten Verhaltens im Alltag.
- Reduktion menschlicher Schwachstellen, die von Angreifern ausgenutzt werden können

1.3 INHALTE (EXEMPLARISCH)

- **Einführung in die IT-Sicherheit**
  - Bedeutung von IT-Sicherheit für Unternehmen und Mitarbeiter
  - Überblick über gängige Bedrohungen (z. B. Phishing, Ransomware, Social Engineering)
  - Rolle der Mitarbeitenden als zentrale Säule der IT-Sicherheitsstrategie
- **Erkennung von Social-Engineering-Angriffen**
  - Typische Angriffsmethoden (Phishing, Vishing, Tailgating, Media Dropping).
  - Hinweise auf Manipulationsversuche und psychologische Tricks
  - Richtiges Verhalten bei verdächtigen Anfragen
- **Passworthygiene und Authentifizierung**
  - Erstellung sicherer Passwörter nach Best Practices
  - Einführung in die Zwei-Faktor-Authentifizierung (2FA)

- Risiken von Passwort-Wiederverwendung und Maßnahmen zur sicheren Passwortverwaltung

- **Erkennung vor Phishing und Malware**
  - Erkennen von gefälschten E-Mails, Links und Anhängen
  - Umgang mit verdächtigen Nachrichten und Webseiten
  - Sicheres Verhalten beim Download und bei der Nutzung von externen Speichermedien
  - Aktuelle Vorgehensweise von Angreifer-Gruppen
- **Sicherer Umgang mit Daten und Systemen**
  - Schutz sensibler Daten vor unbefugtem Zugriff
  - Sichere Nutzung von Geräten und Netzwerken, einschließlich Homeoffice- und Remote-Arbeitslösungen
- **Verhalten im Notfall**
  - Was tun bei verdächtigen Aktivitäten
  - Meldewege und Kommunikationsprozesse bei Sicherheitsvorfällen
  - Vermeidung von Panik und Fokussierung auf schnelle Problemlösung

1.4 ABLAUF

- **Modulares Training**
  - Das Training wird in Modulen durchgeführt
- **Durchführung**
  - Das Training kann sowohl **online** als auch **vor Ort** stattfinden
- **Theoretische Schulung**
  - Vermittlung der Inhalte durch anschauliche Präsentationen und Beispiele aus der Praxis.
- **Praktische Anwendung**
  - Nutzung realitätsnaher Beispiele und Simulationen, um das Gelernte zu vertiefen.
- **Live-Hacking**

Hinweis: Wir empfehlen die Awareness-Training mit unseren Social Engineering Paketen zu kombinieren, um die Awareness langfristig zu erhöhen.

Die empfohlene Gruppengröße bei vor-Ort Vorträgen ist **25 Teilnehmer**.
An einem Tag sind maximal **3 Vorträge** möglich.

MODUL 10
INCIDENT RESPONSE AD-HOC (OHNE VERTRAG)

Im Fall eines Sicherheitsvorfalls stehen wir Ihnen zur Seite. Unser Incident-Response-Team reagiert schnell und effektiv, um die Bedrohung zu beseitigen und den Schaden zu minimieren.

Unsere Incident Response-Dienstleistungen beinhalten die folgenden Schritte:

1.1 ERSTBEWERTUNG UND VORFALLANALYSE

- **Sichtung des Vorfalls:** Sofortige Analyse und Beurteilung des Vorfalls.
- **Schnelle Reaktion:** Identifikation der Schwere des Vorfalls und der betroffenen Systeme.
- **Maßnahmen zur Eindämmung:** Sofortige Maßnahmen zur Eindämmung des Vorfalls, um eine weitere Ausbreitung zu verhindern.

1.2 FORENSISCHE ANALYSE

- **Kommunikationsverhalten:** Analyse von Logdaten der Firewall, sowie der einzelnen Systeme
- **Ursachenanalyse:** Identifikation der Angriffsmethoden und betroffenen Systeme.
- **Einfallstor:** Identifizierung und Analyse des Patient Zero, Ermittlung des Einfallstores
- **Data Loss:** Analyse von Logdateien der Firewall zur Ermittlung exfiltrierter Daten

1.3 ERSTELLUNG EINES INCIDENT-REPORTS

- **Detaillierte Dokumentation:** Erstellen eines umfassenden Berichts über den Vorfall, die durchgeführten Maßnahmen und die Ergebnisse.
- **Empfehlungen zur Verbesserung:** Vorschläge für Maßnahmen, um ähnliche Vorfälle in der Zukunft zu verhindern.

1.4 REMEDIATION

- **Unterstützung bei der Wiederherstellung und Absicherung der Infrastrukur:** Unterstützung bei Rückfragen bzgl. Wiederherstellung betroffener Systeme, Anwendungen und Daten, sowie der Stärkung der Sicherheitsarchitektur und Überprüfung von Schwachstellen.

MODUL 11
TABLE TOP EXERCISE „CYBERATTACK“ (STRATEGISCHE NOTFALLSIMULATION)

Im Fall eines Sicherheitsvorfalls stehen wir Ihnen zur Seite. Unser Incident-Response-Team reagiert schnell und effektiv, um die Bedrohung zu beseitigen und den Schaden zu minimieren.

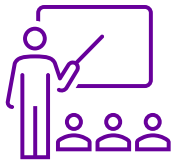
Unsere Incident Response-Dienstleistungen beinhalten die folgenden Schritte:

1.1 VORBEREITUNG

- **Bewertung der Ausgangslage**
  - Bewertung des Notfallhandbuches und der dazugehörigen Dokumente (falls vorhanden)

1.2 ZIELSETZUNG

- **Verbesserung der Reaktionsfähigkeit** bei kritischen Sicherheitsvorfällen
- **Überprüfung bestehender Notfallpläne** und **Identifikation von Schwachstellen**
- **Förderung der Zusammenarbeit** zwischen technischen und nicht-technischen Teams
- **Simulation realer Worst-Case-Szenarien** zur Vorbereitung auf echte Angriffe oder Ausfälle



1.3 INHALT

- **Einführung in die Notfallsimulation**
  - Erklärung der Übungsziele und des geplanten Szenarios
  - Übersicht der bestehenden Notfall- und Incident-Response-Prozesse
  - Überprüfung der Verantwortlichkeiten für aller Teilnehmer
- **Realistisches Worst-Case-Szenario**
  - Definition eines spezifischen Vorfalls, z. B.:
    1. Cyberangriff: Ransomware, Datenlecks, DDoS-Attacken
    2. Systemausfall: Komplettes Versagen kritischer IT-Systeme

    - Szenario wird an die Branche und IT-Infrastruktur des Unternehmens angepasst.
- **Reaktions- und Eskalationsstrategien**
    - Identifikation der ersten Maßnahmen bei einem Vorfall
    - Eskalationsmechanismen und interne Kommunikationswege
    - Zusammenarbeit zwischen internen Teams (z. B. IT, Management, Recht) und externen Partnern (z. B. CERT, Behörden)
- **Entscheidungsfindung unter Stressbedingungen**
    - Umgang mit zeitkritischen Entscheidungen und unvollständigen Informationen
    - Bewältigung von Konflikten und Priorisierung von Maßnahmen
- **Nachverfolgung und Behebung von Vorfällen**
    - Dokumentation der ergriffenen Maßnahmen und Auswirkungen des Vorfalls
    - Rückkehr zur Normalität (Recovery-Prozess)
    - Langfristige Verbesserungsmaßnahmen zur Risikominderung

1.4 ABLAUF

- **Einleitung und Szenario Vorstellung**
    - Detaillierte Beschreibung des simulierten Vorfalls
- **Durchführung der Simulation**
    - Schrittweises Fortschreiten des Szenarios, wobei neue Informationen nach und nach bereitgestellt werden (z. B. eskalierende Angriffe oder unerwartete Komplikationen)
    - Reaktion der Teilnehmer in Echtzeit, basierend auf den vorhandenen Notfallplänen
- **Zwischenbesprechungen**
    - Regelmäßige kurze Unterbrechungen, um die bisherigen Maßnahmen zu reflektieren
    - Diskussion über Alternativen und Optimierungsmöglichkeiten
- **Abschlussbesprechung und Feedbackrunde**
    - Detaillierte Analyse der Übung: Was hat gut funktioniert, wo lagen die Schwächen?
    - Sammlung von Verbesserungsvorschlägen für Prozesse und Kommunikation

1.5 AUSWERTUNG

- **Bewertung der Reaktionsfähigkeit**
  - Wie effektiv und schnell wurden Maßnahmen ergriffen?
- **Prüfung der Kommunikationswege**
  - Überprüfung interner und externer Kommunikationsprozesse
- **Optimierungspotenzial**
  - Identifikation von Schwachstellen in den bestehenden Notfallplänen
- **Erhöhte Resilienz**
  - Stärkung des Krisenbewusstseins und der Entscheidungsfähigkeit der Teams

MODUL 12
CYBERSECURITY AS A SERVICE (CSAAS) RETAINER

Vertrauen Sie unseren Experten und übertragen Sie Ihre offensive Cybersecurity an uns, während Sie sich voll und ganz ihrem Kerngeschäft widmen. Definieren Sie hierfür ein (monatliches) Budget und stellen Sie sich Ihr ganz eigenes Cybersecurity-Paket, welches am besten zu Ihnen passt, zusammen. Gerne beraten wir Sie über unsere verschiedenen Module und der Einsatzmöglichkeiten. Unsere Module umfassen:

1. OSINT
2. Externer Penetrationstest
3. Interner Penetrationstest
4. OT-Penetrationstest
5. Endpoint Security Stresstest
6. Social Engineering
    1. Phishing
    2. Vishing
    3. Media Dropping
    4. Tailgating
7. Red Teaming
8. Awareness Training / Live Hacking
9. Incident Response
10. Table Top Exercise „Cyberattack“ (Strategische Notfallsimulation)

MODUL 13
WEBAPP PENETRATIONSTEST

Unsere Web Application Penetration Tests identifizieren und bewerten systematisch sicherheitsrelevante Schwachstellen in webbasierten Anwendungen – inklusive Frontend, Backend und zugehöriger Schnittstellen (APIs). Der Fokus liegt auf realistischen Angriffsszenarien zur Beurteilung, ob und wie ein Angreifer in Systeme eindringen oder sensible Daten kompromittieren könnte.

1.1 VORGEHENSWEISE

Der Test folgt einem strukturierten, manuellen und Tool-unterstützten Ansatz basierend auf dem OWASP Testing Guide. Dazu gehören:

- Reconnaissance & Threat Modeling: Analyse der Anwendung, möglicher Angriffsflächen und potenzieller Bedrohungen
- Manuelle Schwachstellenanalyse: Prüfung auf Schwächen wie Injection, Broken Authentication, Insecure Deserialization, etc.
- Business Logic Testing: Validierung von Zugriffssteuerung, Berechtigungen und Workflow-Manipulationen
- API Security Testing: Wenn vorhanden, gezielte Tests auf REST- oder GraphQL-APIs
- Post-Exploitation (kontrolliert): Einschätzung möglicher Schadensszenarien nach einem erfolgreichen Angriff

Alle Tests werden im Blackbox- oder Greybox-Ansatz durchgeführt, optional mit Benutzerzugängen des Kunden.

1.2 TYPISCHE SCHWACHSTELLEN

- Cross-Site Scripting (XSS)
- SQL/NoSQL Injection
- Broken Access Control
- Insecure Direct Object References (IDOR)
- Session Management Fehler
- Sicherheitslücken in Drittanbieter-Komponenten

1.3 ERGEBNISSE

Im Abschlussbericht werden alle identifizierten Schwachstellen dokumentiert, inklusive:

- Technische Details und Exploitability
- Risikobewertung (CVSS-basiert)
- Klare Handlungsempfehlungen zur Absicherung

MODUL 14
DARKNET THREAT HUNTING

Unser Partner Unternehmen führt eine manuelle und teilautomatisierte Recherche in den relevantesten und aktivsten Darknet- Plattformen durch.

ÜBERWACHTE PLATTFORMEN:

- Closed-Source Foren (Exploit, Ramp, Dread, BreachForums-Relikte u.a.)
- Ransomware-Leak-Sites zur frühzeitigen Erkennung von Erpressungskampagnen
- Blackmarket-Kommunikationskanäle (Telegram-Relays, IRC, I2P)
- Paste- und DDoS-Infrastruktur (Stresser/Booster- Angebote, Bulletproof Host-Services)

FOKUS DER ANALYSE / GEZIELTE SUCHE NACH:

Erwähnungen Ihres Unternehmensnamens, Ihrer Domains und IP-Adressräume

- Spezifischen Produkten oder Markenbezug in Underground-Diskussionen
- Auftragsangeboten („Hitlists") gegen Unternehmen und Ihrer Branche
- Verkauf von Zugangsdaten, Angriffsvektoren oder exfiltrierten Daten
- Identifikation von Gruppen oder Einzelpersonen mit Angriffsplänen

FORENSISCHE DOKUMENTATION:

- Vollständige Archivierung mit Zeitstempel, Screenshots und Thread-Historien
- Strukturierter Abschlussbericht mit allen relevanten Erkenntnissen
- Risikobewertung zur Einschätzung der Glaubwürdigkeit und Relevanz

HANDLUNGSEMPFEHLUNGEN:

- Technische Hinweise für Ihre IT-Security-Teams
- TTP-Zuordnung (Tactics, Techniques, Procedures)
- Group Attribution zur Identifikation von Angreifergruppen
- Konkrete Empfehlungen für nächste Schritte

MODUL 15
REPORTING

Unser Sicherheitsreport bietet neben einem kurzen Management Summary, eine strukturierte, detaillierte Zusammenfassung der durchgeführten Arbeiten, der identifizierten Risiken und der vorgeschlagenen Maßnahmen zur Verbesserung der Sicherheitslage.

Darüber hinaus stellen wir Ihnen eine Schwachstellentabelle zur Nachverfolgung der noch offenen, zu behebenden Maßnahmen, bereit.

Alle Ergebnisse sowie den Report gehen wir gemeinsam mit Ihnen im Rahmen einer Abschlussbesprechung durch.

Der Bericht ist sowohl für technische Fachkräfte als auch für nicht technische Entscheidungsträger verständlich formuliert und in der Regel folgendermaßen aufgebaut:

1.1 EINLEITUNG

- **Zielsetzung** des Projekts.
- **Scope:** Umfang der Analyse oder Simulation
- **Methoden und Tools:** Übersicht der eingesetzten Tools und Methoden

1.2 MANAGEMENT SUMMARY

- **Kompakte und Prägnante Zusammenfassung** der wichtigsten Erkenntnisse
- Hervorhebung **kritischer Schwachstellen** und **Risiken**
- **Priorisierung** der gefundenen Erkenntnisse (z. B. größte Risiken bzw. wichtigste Erfolge)
- **Maßnahmenempfehlungen**
- **Fazit mit Gesamtbewertung** der aktuellen Sicherheitslage

1.3 ERGEBNISSE

- **Kurzfassung der wichtigsten Erkenntnisse**
- **Identifizierte Schwachstellen** und Risiken
- **Priorisierung** der gefundenen Probleme basierend auf ihrem Risiko

1.4 DETAILLIERTE ANALYSE

- **Beschreibung** der durchgeführten Tests, Angriffe oder Simulationen
- **Technische Details** zu gefundenen Schwachstellen (z. B. CVE-Nummern, Angriffspfade)
- **Nachvollziehbare Belege** (z.B. Screenshots, Codes) der durchgeführten Arbeiten

1.5 EMPFEHLUNGEN

- **Maßnahmen** zur Behebung identifizierter Schwachstellen
- **Verbesserungen** von Prozessen, Technologien oder Mitarbeiterschulungen
- **Langfristige Strategien** zur Verbesserung der IT- und OT-Sicherheit

1.6 SCHWACHSTELLENÜBERSICHT

- **Schwachstellentabelle** zur Nachverfolgung der noch offenen, zu behebenden Maßnahmen
- **Priorisiert** nach Kritikalität und Aufwand

1.7 C-LEVEL PRÄSENTATION (OPTIONAL)

- **Aufbereitung der Ergebnisse** in ein C-Level Briefing
- **Präsentieren** der aufbereiteten Ergebnisse vor dem Management
- **Fragerunde**

GÜLTIGKEIT

Die Angebote sind generell 30 Tage gültig.

ZAHLUNGSBEDINGUNGEN ALLGEMEIN

Die Zahlung erfolgt nach Abschluss der Arbeiten, mit einem

Zahlungsziel **14 Tage netto ohne Abzug** nach Rechnungsstellung.

ZAHLUNGSBEDINGUNGEN INCIDENT RESPONSE

Die Zahlung für Vorfall-Tage erfolgt nach Abschluss des Vorfalls, mit einem

Zahlungsziel **14 Tage netto ohne Abzug** nach Rechnungsstellung.

Die Abrechnung für die erbrachten Incident Response Leistungen erfolgt **nach tatsächlich geleistetem Aufwand**, basierend auf den für die Bearbeitung des Vorfalls aufgewendeten Stunden und Ressourcen. Dies bedeutet, dass nur die tatsächlich geleisteten Leistungen, wie z. B. Stunden für Remote- oder Vor-Ort-Unterstützung, Analysen, Untersuchungen und andere direkt mit dem Vorfall verbundene Tätigkeiten, in Rechnung gestellt werden.

Trotz der Abrechnung nach tatsächlichem Aufwand gilt eine **Mindestabrechnung von 1 Manntag** pro Vorfall (1 Manntag ≙ 8 Stunden). Das bedeutet, dass unabhängig von der tatsächlichen Zeit, die zur Bearbeitung des Vorfalls aufgewendet wird, für den ersten Tag eine vollständige Tagespauschale (z. B. **1.900,00 EUR bzw. 2.400 EUR / Tag**) abgerechnet wird.

REISEZEIT UND MEHRKOSTEN

Die Fahrtkosten werden mit 0,75 Euro pro km abgerechnet.

Reisezeit der Analysten werden mit 90 Euro pro Stunden berechnet.

Reisekosten werden gesondert berechnet auf Basis der tatsächlich anfallenden Kosten.

Leistungen außerhalb der gewöhnlichen Geschäftszeiten (7:00 - 20:00 Uhr), sowie an Samstag, Sonntag und Feiertagen werden mit dem 1,5-fachen Preis des jeweiligen Tagessatzes fakturiert.

Sämtliche Preise verstehen sich zuzüglich der gesetzlichen Mehrwertsteuer.

Mit freundlichen Grüßen

HELGE HUSEMANN

PENTARIS SECURITY

VIELEN DANK FÜR DIE GUTE ZUSAMMENARBEIT!

PENTARIS SECURITY

PENTARIS SECURITY GMBH
BEIM WÖLFELSBRUNNEN 8
66346 PÜTTLINGEN
TEL.: 06806 937300
INFO@PENTARIS-SECURITY.DE
WWW.PENTARIS-SECURITY.DE