NIS2/DORA/CRA Compliance durch Penetration Tests:

Deshalb ist die Zusammenarbeit von Technikern und Managern notwendig

Dipl.-Ing. Daniel Mrskos, BSc

SECURITY MIT PASSION

Über mich

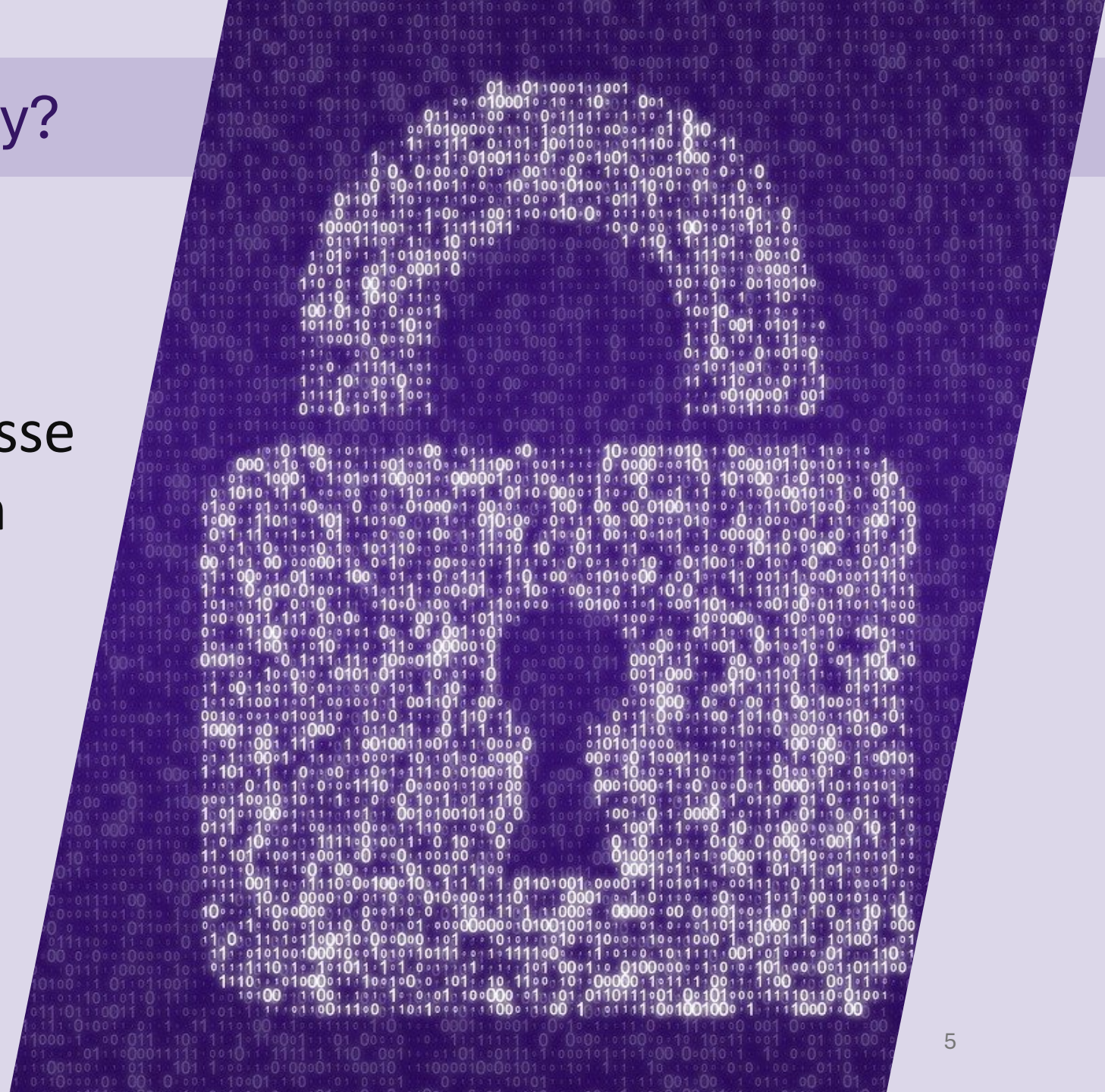
Dipl.-Ing. Daniel Mrskos, BSc
CEO von Security mit Passion | Penetration Tester | Mentor | FH-Lektor | NIS Prüfer

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 | OSCC | CNSP | Comptia Pentest+ | ITIL Foundation V3 | ICCA | CCNA | eJPTv2 | Developing Security Software (LFD121) | CAP | Checkmarx Security Champion

Anekdote aus CISO-Mandat

Wie funktioniert IT-Security?

- Schutz der Geschäftsprozesse
- Minimierung von Ausfällen
- Rechtliche Absicherung
- Business First!



Compliance Anforderungen I

NIS2 (Network and Information Security 2 Directive): EU-Richtlinie zur Erhöhung der Cybersicherheit in kritischen Infrastrukturen. Überblick über die Schwerpunkte, z.B. Risikoanalysen, Incident Reporting, Cybersicherheitsstrategien.

DORA (Digital Operational Resilience Act): Fokussiert auf die Stärkung der digitalen Widerstandsfähigkeit im Finanzsektor. Relevante Aspekte sind Risikobewertungen, Überwachung und Vorfallmanagement.

CRA (Cyber Resilience Act): EU-Verordnung, um sicherzustellen, dass digitale Produkte und Dienstleistungen angemessene Cybersicherheitsmaßnahmen enthalten.

Compliance Anforderungen II

ISO 27001: Internationaler Standard für Informationssicherheits-Managementsysteme (ISMS). Bietet einen systematischen Ansatz zum Schutz vertraulicher Daten, einschließlich Risikomanagement, Implementierung geeigneter Sicherheitsmaßnahmen und fortlaufender Überprüfung und Verbesserung des ISMS.

TISAX (Trusted Information Security Assessment Exchange): Speziell für die Automobilindustrie entwickelter Standard für Informationssicherheit. Ermöglicht den Austausch von geprüften Informationen zu Sicherheitsniveaus zwischen Unternehmen und gewährleistet die Einhaltung branchenspezifischer Anforderungen und Sicherheitsstandards.
TISAX

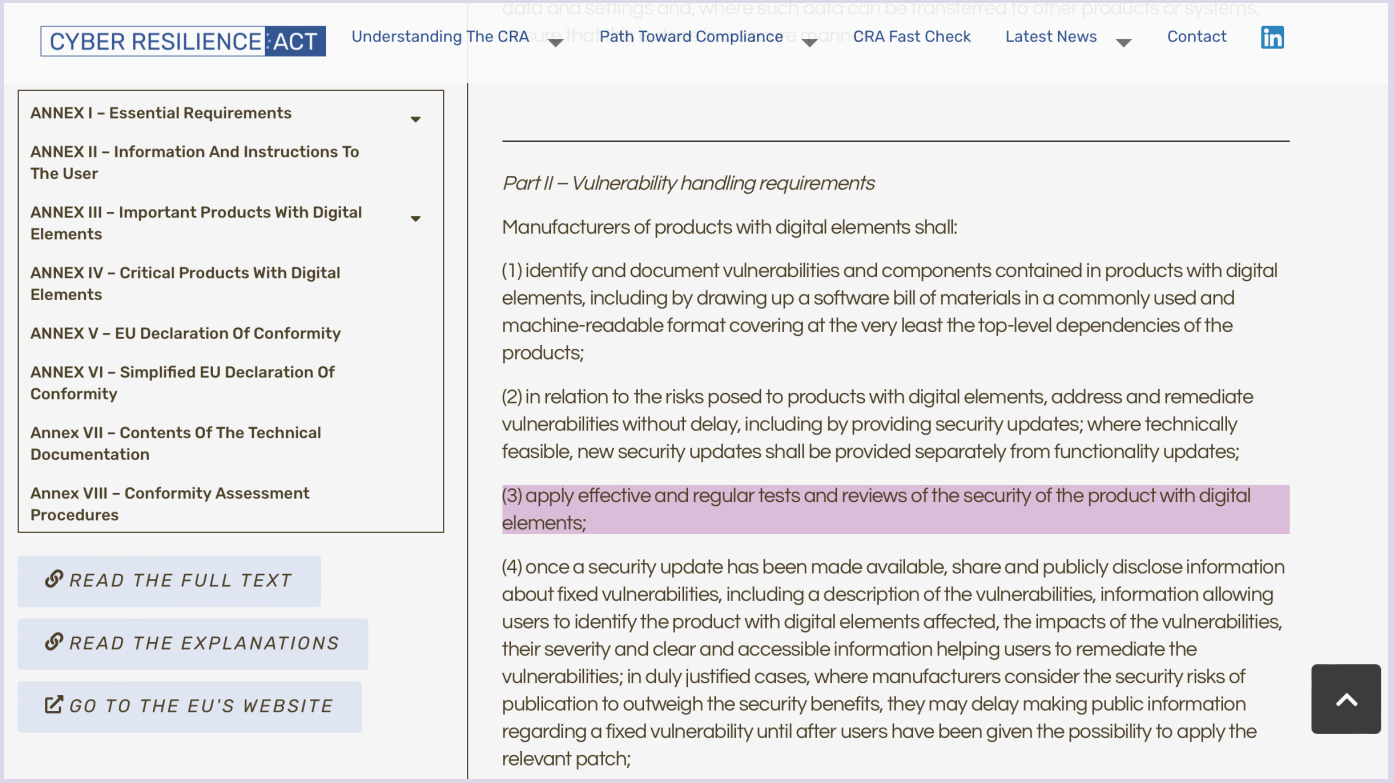
Anforderungen an Penetration Tests I

Test der Resilienz

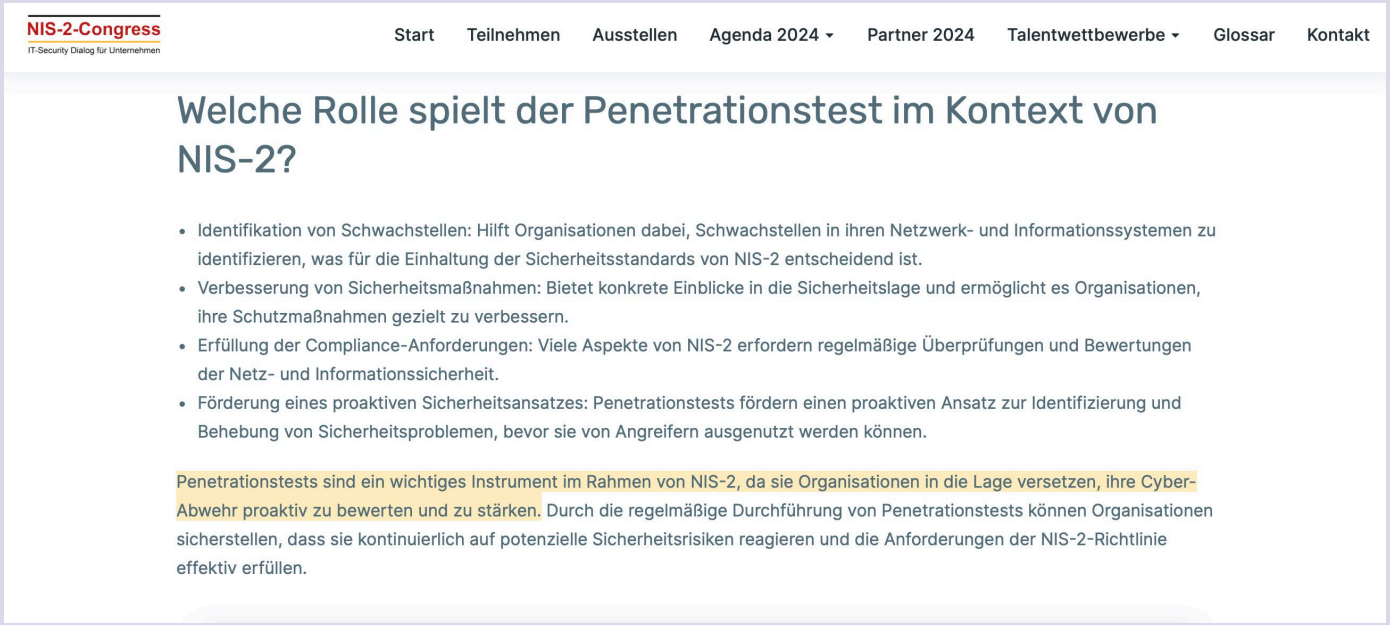
DORA Artikel 24, Artikel 25, Artikel 26 und Artikel 27

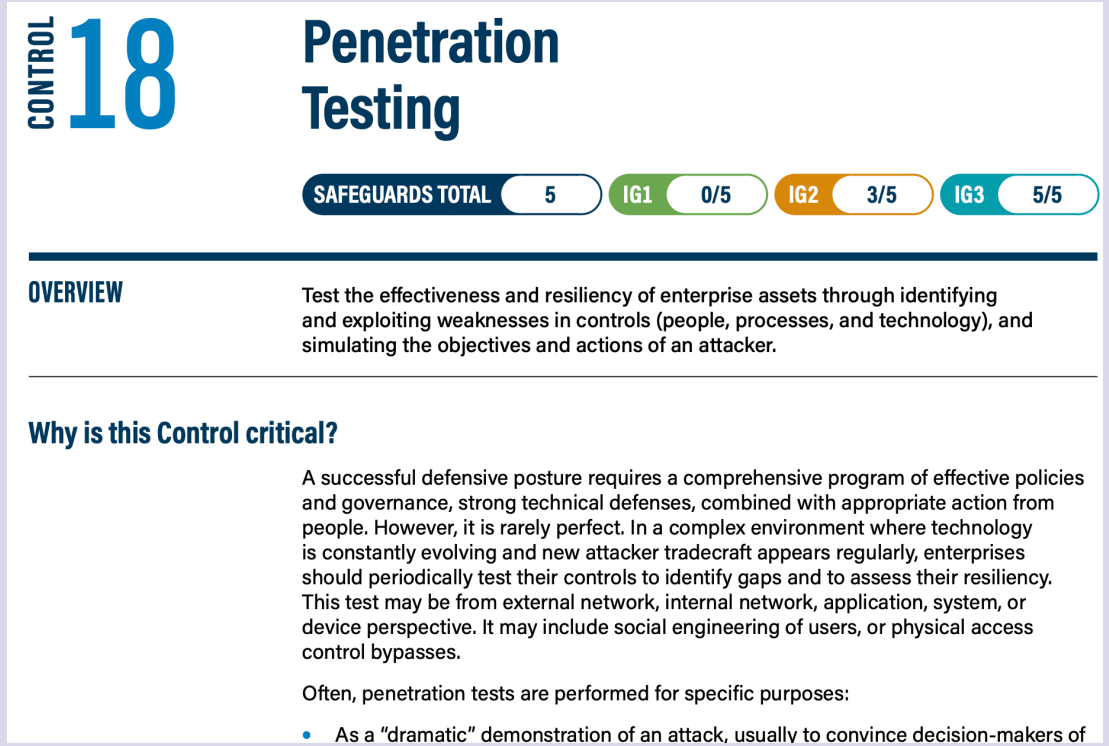
ID	DORA	Anforderung	NIS2	C5:2020	ISO 27001
D.24	Art. 24	Programm für Tests der digitalen operationalen Resilienz	-	-	-
D.25	Art. 25	Testen von IKT-Tools und -Systemen		DEV-02 DEV-10 COM-02	A.8.29 A.8.31 A.8.33 A.8.34
D.26	Art. 26 Art. 27	Thread-led Penetration Testing	-	OPS-19	-

Tabelle: *Eigene Zusammenstellung · Stand April 2024 · Ohne Gewähr der Vollständigkeit und Korrektheit*

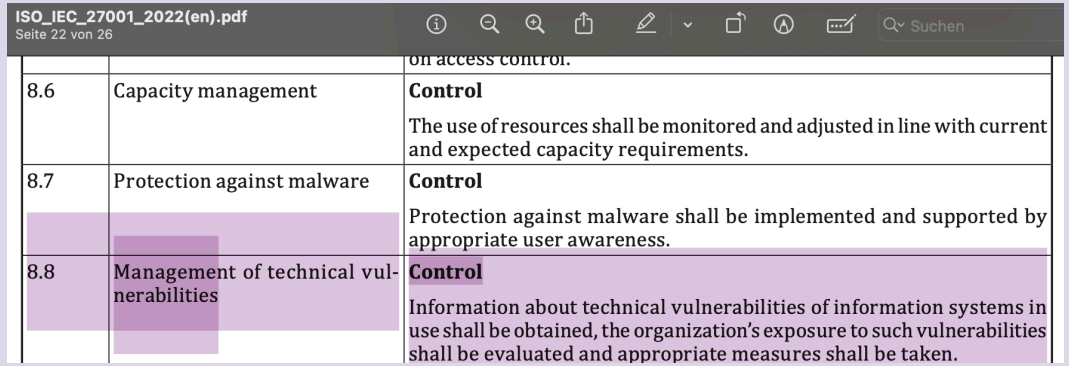


Anforderungen an Penetration Tests II

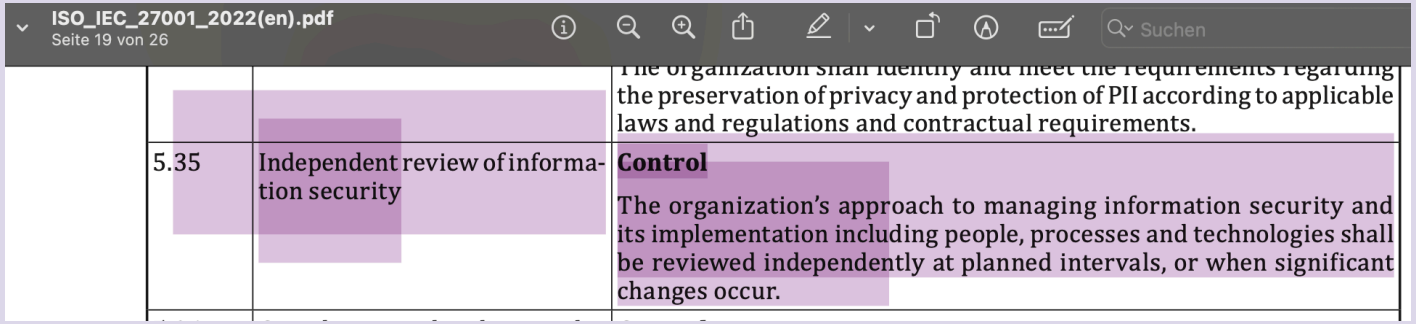




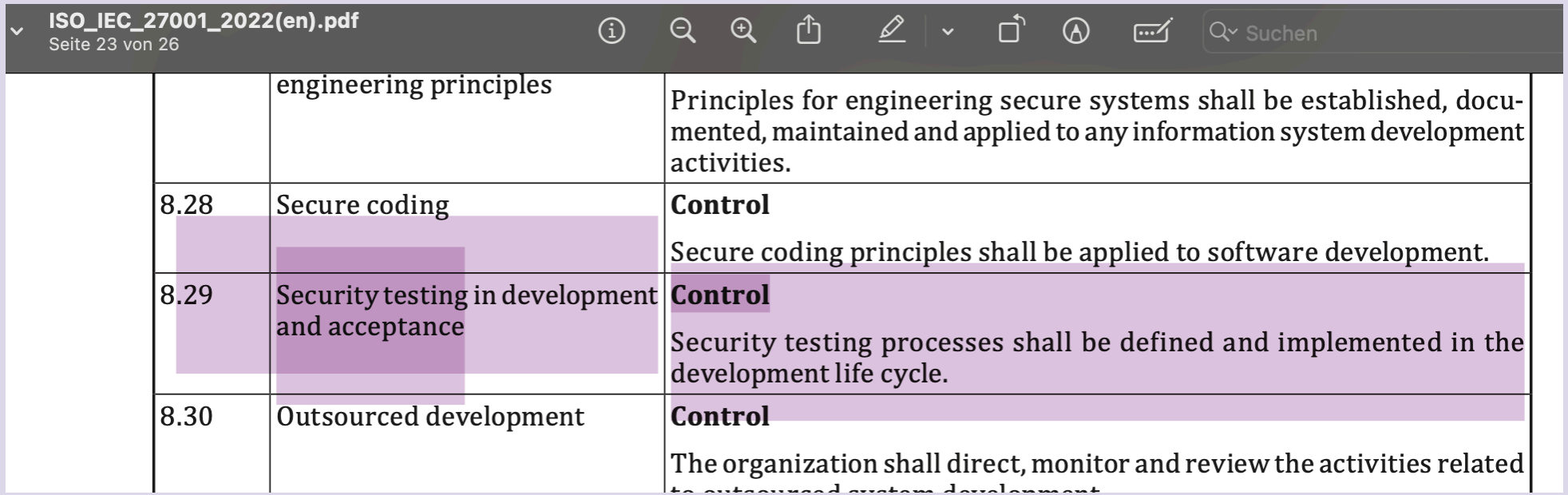
Anforderungen an Penetration Tests III


ISO_IEC_27001_2022(en).pdf
Seite 22 von 26

		on access control.
8.6	Capacity management	**Control** The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.
8.7	Protection against malware	**Control** Protection against malware shall be implemented and supported by appropriate user awareness.
8.8	Management of technical vulnerabilities	**Control** Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.

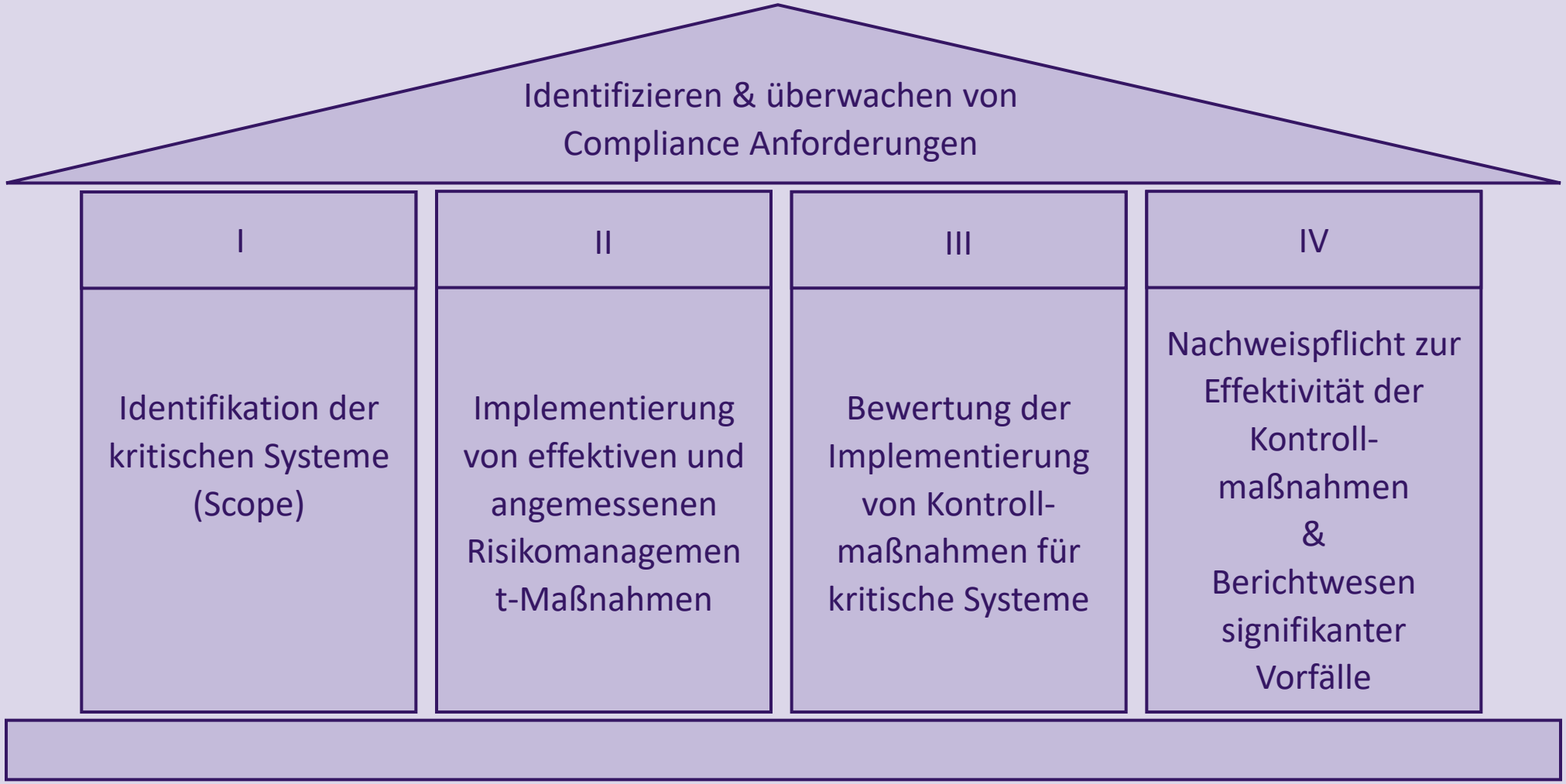

ISO_IEC_27001_2022(en).pdf
Seite 19 von 26

		The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.
5.35	Independent review of information security	**Control** The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.


ISO_IEC_27001_2022(en).pdf
Seite 23 von 26

	engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.
8.28	Secure coding	**Control** Secure coding principles shall be applied to software development.
8.29	Security testing in development and acceptance	**Control** Security testing processes shall be defined and implemented in the development life cycle.
8.30	Outsourced development	**Control** The organization shall direct, monitor and review the activities related to outsourced system development

4-Säulen Ansatz für Compliance



Challenges bei Penetration Tests zur Erfüllung von Compliance

1. **Compliance-Gap vs. Sicherheitslücke**
• **Herausforderung:** Penetration Tests decken technische Schwachstellen auf, nicht unbedingt Compliance-Gaps. Die Übertragung technischer Findings auf spezifische Compliance-Anforderungen ist komplex.

2. **Regelmäßigkeit und Kontinuität**
• **Herausforderung:** Compliance erfordert kontinuierliche Überwachung und Tests. Ein einmaliger Penetration Test genügt nicht, um die fortlaufende Einhaltung sicherzustellen.

3. **Dokumentation & Reporting**
• **Herausforderung:** Compliance-Standards verlangen detaillierte Berichte und Dokumentationen. Die Ergebnisse von Penetration Tests müssen in einer für Audits geeigneten Form aufbereitet werden.

Challenges bei Penetration Tests zur Erfüllung von Compliance

4. **Priorisierung von Maßnahmen**
• **Herausforderung:** Penetration Tests identifizieren viele Schwachstellen. Die Herausforderung liegt darin, diese nach Compliance-Relevanz zu priorisieren und gezielt zu beheben.

5. **Kostendruck**
• **Herausforderung:** Regelmäßige, umfassende Tests sind kostspielig. Budgetbeschränkungen können dazu führen, dass nicht alle Compliance-relevanten Bereiche abgedeckt werden.

6. **Sicherstellung der Vollständigkeit**
• **Herausforderung:** Compliance-Standards erfordern eine umfassende Prüfung aller relevanten Systeme. Die Herausforderung besteht darin, sicherzustellen, dass der Penetration Test den gesamten Anwendungsbereich abdeckt.

Challenges bei Penetration Tests zur Erfüllung von Compliance

7. **Verständnis der Compliance-Anforderungen**

• **Herausforderung:** Penetration Tester müssen die spezifischen Anforderungen (NIS2, DORA, CRA) genau kennen, um den Test so zu gestalten, dass er relevante Compliance-Kontrollen abdeckt.

8. **Integration in bestehende Prozesse**

• **Herausforderung:** Penetration Tests müssen in bestehende Sicherheits- und Compliance-Prozesse eingebunden werden. Eine fehlende Integration erschwert die systematische Nachverfolgung und Umsetzung der Testergebnisse.

Die Herausforderungen der Zusammenarbeit zwischen Managern und Penetration Testern

1. **Unterschiedliche Risikoperspektiven**
- **Manager:** Geschäftliche Auswirkungen & Kosten.
- **Tester:** Technische Schwachstellen & Angriffsmöglichkeiten.

2. **Kommunikationsprobleme**
- Technisches Vokabular vs. Managementsprache.
- Schwierige Übersetzung technischer Details in geschäftsrelevante Informationen.

3. **Priorisierung von Risiken**
- Unterschiedliche Ansichten zur Dringlichkeit der Maßnahmen.
- Ressourcenallokation erfordert klare Prioritäten.

Die Herausforderungen der Zusammenarbeit zwischen Managern und Penetration Testern

4. **Unterschiedliche Ziele**
- **Manager:** Compliance, Budgeteffizienz, Geschäftsbetrieb.
- **Tester:** Maximale technische Sicherheit.

5. **Kosten und Budget**
- Schwierige Vermittlung des Wertes von Pentests an das Management.
- ROI oft schwer darstellbar.

6. **Fehlendes Bewusstsein im Management**
- Schwierige Einschätzung der technischen Risiken und Bedrohungslage.

Die Herausforderungen der Zusammenarbeit zwischen Managern und Penetration Testern

7. **Umsetzung der Handlungsempfehlungen**
• Manager entscheiden über Ressourcen, Tester können nur Empfehlungen geben.

8. **Nachhaltige Integration**
• Pentests oft als einmaliges Event betrachtet statt als kontinuierlicher Prozess.

9. **Zeitliche Planung**
• Balance zwischen effektiven Tests und minimaler Störung des Geschäftsbetriebs.

Lösungsansätze

1. **Gemeinsames Risikobewertungs-Framework:** Entwickeln Sie ein gemeinsames Modell, das technische und geschäftliche Risiken verbindet, um eine klare Priorisierung von Maßnahmen zu ermöglichen.

2. **Klarer Kommunikationsprozess:** Nutzen Sie „Übersetzungsleitfäden“ und standardisierte Reporting-Templates, um Testergebnisse in verständlicher, geschäftsrelevanter Sprache für das Management aufzubereiten.

3. **Regelmäßige Abstimmung:** Führen Sie gemeinsame Risikoworkshops und regelmäßige Meetings durch, um Pentester und Manager aufeinander abzustimmen und gemeinsame Ziele zu setzen.

4. **Schulungen & Awareness:** Organisieren Sie Schulungen für Manager und Pentester zu Cyberrisiken und Compliance-Anforderungen, um ein besseres gegenseitiges Verständnis zu schaffen.

Lösungsansätze

5. **Pentesting-Zyklus etablieren:** Integrieren Sie regelmäßige Penetration Tests in die IT-Sicherheitsstrategie, um eine kontinuierliche Überwachung und Erfüllung der Compliance-Anforderungen sicherzustellen.

6. **Verantwortlichkeiten & Nachverfolgung:** Definieren Sie klare Prozesse zur Umsetzung der Handlungsempfehlungen, inklusive Verantwortlichkeiten, Fristen und regelmäßigen Statusupdates.

7. **Integration in Geschäftsprozesse:** Binden Sie Penetration Tests in bestehende Sicherheits- und Compliance-Prozesse ein und nutzen Sie sie als festen Bestandteil des kontinuierlichen Verbesserungsprogramms (CIP).

Stakeholder

Die Testmethodik sieht in der Testphase die Einbindung diverser Stakeholder vor

TLPT Cyber Team – Gutachter (TIBER-DE)

- Bestätigt die regelkonforme Test-durchführung
- Fachliche und prozessuale Betreuung
- Ansprechpartner für das Control Team
- Hält Kontakt zu externen Stellen

Threat Intelligence-Anbieter – Spion

- Sammelt unternehmens-spezifische Bedrohungs-informationen
- Erstellt Angriffsszenarien

Tester- Angreifer

- Führt Angriffsszenarien auf das Unternehmen durch
- nutzt durch den TI-Anbieter gesammelte Informationen

Getestetes Unternehmen

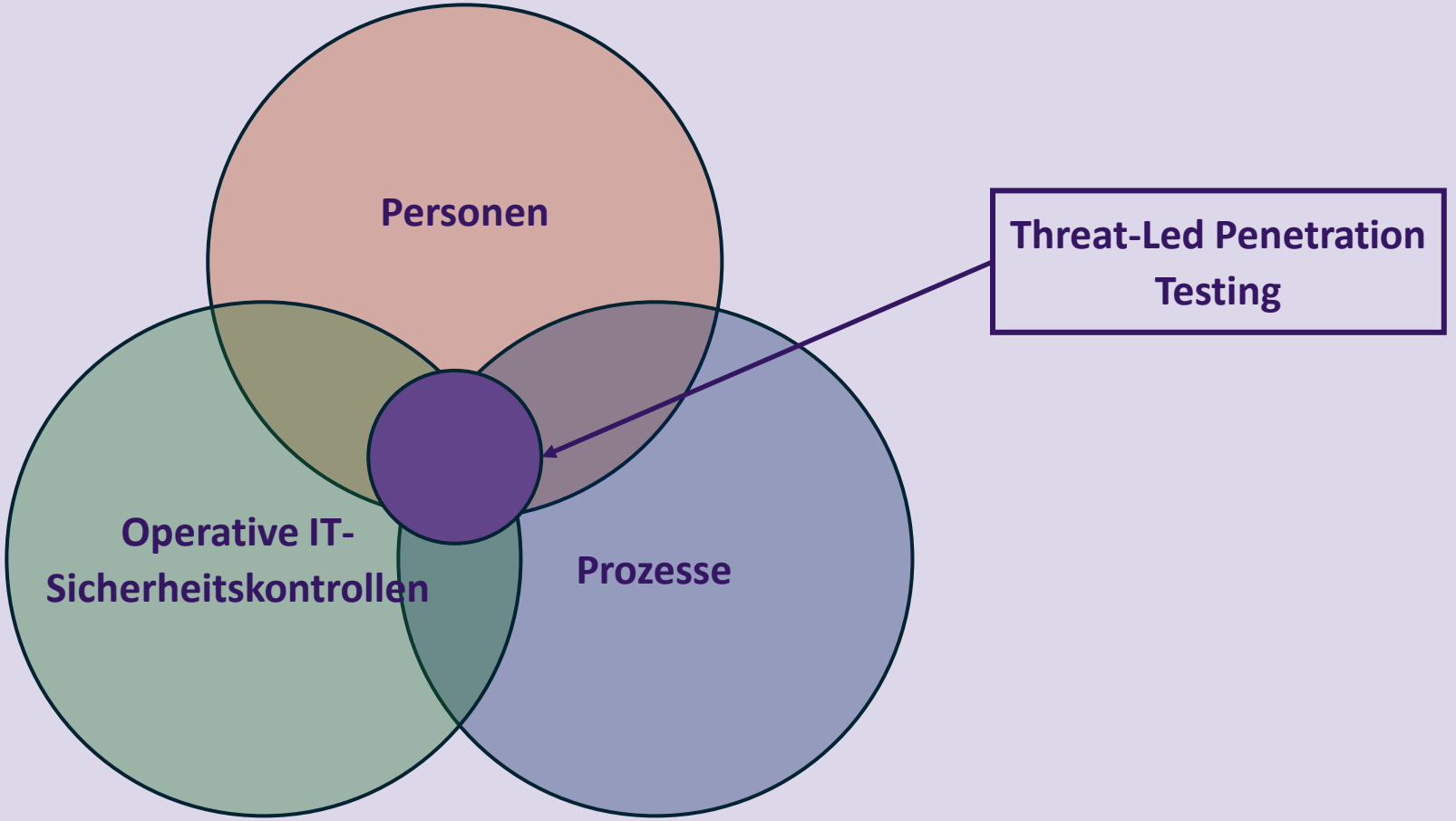
Control Team – Manager

- Zentraler Ansprechpartner und Entscheidungsträger
- Monitoring und Risikomanagement

Blue Team – Verteidiger

- Cyberabwehr (SOC/CERT)
- Alle Mitarbeiter außerhalb des Control Teams
- Nicht über die Durchführung des Tests informiert

Threat-Led Penetration Testing



Beispiel aus Permission to Attack

Informationen zu Compliance GAP-Analyse im Rahmen des Penetration Tests

Ist eine Compliance GAP-Analyse im Rahmen des Penetration Tests enthalten?	Ja
Welche/r Norm/Standard soll als Basis für die Compliance gelten?	CIS Controls V8, OWASP Top 10 und CWE Top 25
Gibt es interne Richtlinien oder Dokumente die im Rahmen des Penetration Tests herangezogen werden können?	-
Was ist die aktuelle Maturität (nach CMMI) ?	-

Beispiel aus Report

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		

Beispiel aus Abschlusspräsentation

Kritische Befunde

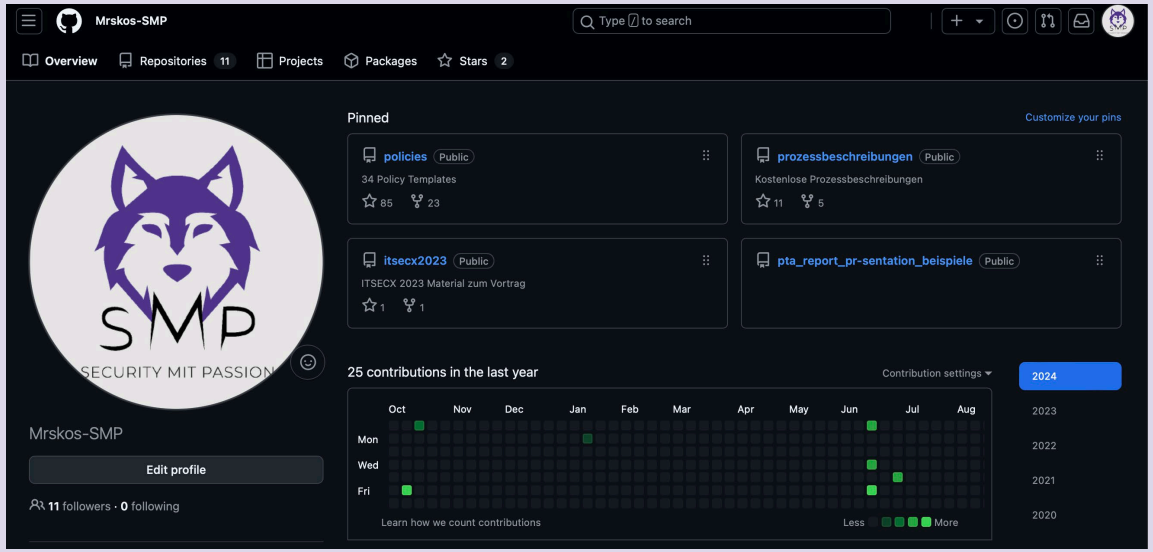
Kritische Befunde

Aspekt-ID	Beschreibung	Auswirkung	Risiko	Compliance Verstoß	Verantwortung
SEC-YNH-001	**Kompromittierung des Domain-Administrators durch GMSA-Gruppe**	Übernahme der kompletten Infrastruktur	Kritisch	4.2 Establish and Maintain a Secure Configuration Process	Max Mustermann

SECURITY MIT PASSION

Kostenlose Ressourcen & Fragen?

- https://github.com/Mrskos-SMP/



- https://www.linkedin.com/in/daniel-mrskos-0720081ab/
- daniel.mrskos@security-mit-passion.at