


Author	Dipl.-Ing. Daniel Mrskos, BSc
Funktion	CEO von Security mit Passion, Penetration Tester, Mentor, FH-Lektor, NIS Prüfer
Datum	14. Juni 2024
	
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	https://www.linkedin.com/in/dipl-ing-daniel-mrskos-bsc-0720081ab/
Website	https://security-mit-passion.at

Richtlinie zum Schwachstellenmanagement

Datum: [Heutiges Datum]

Einleitung

Diese Richtlinie zum Schwachstellenmanagement definiert die Anforderungen und Maßnahmen zur Identifizierung, Bewertung und Behandlung von Schwachstellen in IT-Systemen und Anwendungen bei [Unternehmen]. Diese Richtlinie basiert auf den Standards ISO 27001:2022, ISO 27002:2022, CIS Controls v8, BSI C5:2020, der Cloud Controls Matrix (CCM), dem NIST Cybersecurity Framework, dem NIS2 Draft, der OH SzA für KRITIS, dem European Cyber Resilience Act und DORA.

Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiter, Auftragnehmer, Berater, Zeitarbeitskräfte, Praktikanten und mit Dritten verbundene Personen, die für die Identifizierung, Bewertung und Behandlung von Schwachstellen in den IT-Systemen und Anwendungen von [Unternehmen] verantwortlich sind.

Compliance Matrix

Die Compliance Matrix dient dazu, die Konformität dieser Richtlinie zum Schwachstellenmanagement mit den relevanten Sicherheitsstandards und -richtlinien zu gewährleisten. Sie zeigt die Zuordnung der einzelnen Policy-Komponenten zu den spezifischen Anforderungen der Standards wie ISO 27001:2022, CIS Controls V8, BSI C5:2020, der Cloud Controls Matrix (CCM), dem NIST Cybersecurity Framework, dem NIS2 Draft, der OH SzA für KRITIS, dem European Cyber Resilience Act und DORA. Dies erleichtert die Nachverfolgung und Überprüfung, dass alle notwendigen Sicherheitsmaßnahmen implementiert sind und ermöglicht eine klare, transparente Dokumentation unserer Compliance-Verpflichtungen.

Policy-Komponente	ISO 27001:2022 / 27002:2022	TISAX	CIS Controls V8	BSI C5:2020	CCM	NIST CSF	NIS2	OH SzA	European CRA	DORA
Identifizierung von Schwachstellen	8.28.1, 8.28.2	1.1.1, 1.2.1	7.1, 7.2	ORP1, ORP2	IVS-01, IVS-02	ID.RA-1, ID.RA-2	Artikel 5, 6.1	Abschnitt 2.3	Artikel 23	Artikel 4
Bewertung von Schwachstellen	8.29.1, 8.29.2	2.1.1, 2.1.2	7.3, 7.4	ORP3, ORP4	IVS-03, IVS-04	ID.RA-3, ID.RA-4	Artikel 5, 6.2	Abschnitt 2.4	Artikel 23	Artikel 4
Behandlung von Schwachstellen	8.30.1, 8.30.2	3.1.1, 3.1.2	7.5, 7.6	OPS1, OPS2	IVS-05, IVS-06	PR.IP-1, PR.IP-2	Artikel 6.3	Abschnitt 2.5	Artikel 23	Artikel 4
Überwachung und Überprüfung	8.31.1, 8.31.2	4.1.1, 4.1.2	8.1, 8.2	OPS3, OPS4	IVS-07, IVS-08	DE.CM-1, DE.CM-2	Artikel 6.4	Abschnitt 2.6	Artikel 23	Artikel 4
Schulung und Sensibilisierung	6.3.1, 6.3.2	4.2.1, 4.2.2	17.1, 17.2	ORP5, ORP6	STA-01, STA-02	PR.AT-1, PR.AT-2	Artikel 6.5	Abschnitt 2.7	Artikel 23	Artikel 4

Richtlinien und Anforderungen

Identifizierung von Schwachstellen

Alle IT-Systeme und Anwendungen müssen regelmäßig auf Schwachstellen überprüft werden (ISO 27001: 8.28.1, 8.28.2). Dies umfasst die Nutzung automatisierter Tools zur Schwachstellen-Scanning und Penetrationstests, um potenzielle Sicherheitslücken zu identifizieren (CIS Controls 7.1, 7.2, TISAX 1.1.1, 1.2.1). Ergebnisse der Schwachstellenanalysen müssen dokumentiert und regelmäßig überprüft werden, um die Wirksamkeit der Sicherheitsmaßnahmen zu gewährleisten (BSI C5: ORP1, ORP2, CCM IVS-01, IVS-02).

Bewertung von Schwachstellen

Identifizierte Schwachstellen müssen bewertet und nach ihrem Schweregrad priorisiert werden (ISO 27001: 8.29.1, 8.29.2). Dies umfasst die Bewertung der potenziellen Auswirkungen und der Wahrscheinlichkeit eines Exploits (CIS Controls 7.3, 7.4, TISAX 2.1.1, 2.1.2). Schwachstellen mit hohem Risiko müssen sofort behandelt werden, während geringere Risiken entsprechend ihrer Priorität bearbeitet werden (BSI C5: ORP3, ORP4, CCM IVS-03, IVS-04).

Behandlung von Schwachstellen

Alle identifizierten und bewerteten Schwachstellen müssen gemäß ihrer Priorität behandelt werden (ISO 27001: 8.30.1, 8.30.2). Dies umfasst die Implementierung von Patches, Updates und anderen Maßnahmen zur Beseitigung der Schwachstellen (CIS Controls 7.5, 7.6, TISAX 3.1.1, 3.1.2). Die Behandlung von Schwachstellen muss dokumentiert und regelmäßig überprüft werden, um die Wirksamkeit der Maßnahmen sicherzustellen (NIST CSF PR.IP-1, PR.IP-2, BSI C5: OPS1, OPS2, CCM IVS-05, IVS-06).

Überwachung und Überprüfung

Alle Aktivitäten im Zusammenhang mit dem Schwachstellenmanagement müssen kontinuierlich überwacht und regelmäßig überprüft werden (ISO 27001: 8.31.1, 8.31.2). Dies umfasst die Einrichtung von Überwachungs- und Protokollierungssystemen, um den Fortschritt der Schwachstellenbehandlung zu verfolgen (CIS Controls 8.1, 8.2, TISAX 4.1.1, 4.1.2). Die Ergebnisse der Überwachung

müssen dokumentiert und analysiert werden, um Verbesserungspotenziale zu identifizieren (NIST CSF DE.CM-1, DE.CM-2, BSI C5: OPS3, OPS4, CCM IVS-07, IVS-08).

Schulung und Sensibilisierung

Alle Mitarbeiter müssen regelmäßig Schulungen zum Schwachstellenmanagement durchlaufen (ISO 27001: 6.3.1, 6.3.2). Diese Schulungen müssen die aktuellen Bedrohungen, Sicherheitsmaßnahmen und Best Practices abdecken (CIS Controls 17.1, 17.2, TISAX 4.2.1, 4.2.2). Sensibilisierungsmaßnahmen müssen implementiert werden, um sicherzustellen, dass alle Mitarbeiter über die aktuellen Sicherheitsanforderungen informiert sind (NIST CSF PR.AT-1, PR.AT-2, BSI C5: ORP5, ORP6, CCM STA-01, STA-02).

Verantwortliche

Die Implementierung und Einhaltung dieser Richtlinie liegt in der Verantwortung des IT-Sicherheitsbeauftragten und des Vulnerability Management Teams. Alle Mitarbeiter sind verpflichtet, sich an diese Richtlinie zu halten und jegliche Verstöße umgehend zu melden.

Quellen und Referenzen

Quelle	Zweck	Link
ISO27001:2022	Aufbau und Implementierung eines ISMS	ISO 27001:2022
CIS Controls v8	Sicherheitsmaßnahmen gegen Cyberangriffe	CIS Controls v8
BSI C5:2020	Cloud Security Standard	BSI C5:2020
Cloud Controls Matrix (CCM)	Sicherheitskontrollen für Cloud-Dienste	Cloud Controls Matrix
NIST Cybersecurity Framework	Rahmenwerk zur Verbesserung der Cybersicherheit	NIST CSF
NIS2 Draft	EU-Richtlinie zur Netz- und Informationssicherheit	NIS2 Draft
OH SzA für KRITIS	Orientierungshilfe Angriffserkennung für Kritische Infrastrukturen	OH SzA
European Cyber Resilience Act	EU-Verordnung zur Cyber-Resilienz	European CRA
Digital Operational Resilience Act (DORA)	EU-Verordnung zur digitalen operationellen Resilienz	DORA

Diese Quellen und Referenzen bieten umfassende Leitlinien und Best Practices für die Entwicklung und Implementierung von Sicherheitsmaßnahmen sowie für die Einhaltung der relevanten Standards und Richtlinien. Sie dienen als Grundlage und Unterstützung bei der Implementierung und Aufrechterhaltung eines effektiven Schwachstellenmanagements bei [Unternehmen].

Dokumentinformationen

Titel: Richtlinie zum Schwachstellenmanagement
Version: 1.0
Datum: [Heutiges Datum]
Verantwortlich: IT-Sicherheitsbeauftragter
Genehmigt von: [Name der genehmigenden Person]
Nächste Überprüfung: [Datum der nächsten Überprüfung]