


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	<a href="https://www.linkedin.com/in/dipl-ing-daniel-mrskos-bsc-0720081ab/">https://www.linkedin.com/in/dipl-ing-daniel-mrskos-bsc-0720081ab/</a>
Website	<a href="https://security-mit-passion.at">https://security-mit-passion.at</a>

=====

## Richtlinie zur Protokollierung und Überwachung

Datum: [Heutiges Datum]

### Einleitung

Diese Richtlinie zur Protokollierung und Überwachung definiert die Anforderungen und Maßnahmen zur Sicherstellung einer effektiven Protokollierung und Überwachung der IT-Systeme 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 Protokollierung und Überwachung der IT-Systeme von [Unternehmen] verantwortlich sind.

=====

## Compliance Matrix

Die Compliance Matrix dient dazu, die Konformität dieser Richtlinie zur Protokollierung und Überwachung 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
Protokollierungsanforderungen	8.1.1, 8.1.2	1.1.1, 1.2.1	8.1, 8.2	ORP1, ORP2	IVS-01, IVS-02	DE.AE-1, DE.AE-2	Artikel 5, 6.1	Abschnitt 2.3	Artikel 23	Artikel 4
Überwachungsanforderungen	8.2.1, 8.2.2	2.1.1, 2.1.2	9.1, 9.2	ORP3, ORP4	IVS-03, IVS-04	DE.CM-1, DE.CM-2	Artikel 5, 6.2	Abschnitt 2.4	Artikel 23	Artikel 4
Aufbewahrung und Schutz der Protokolle	8.3.1, 8.3.2	3.1.1, 3.1.2	10.1, 10.2	OPS1, OPS2	DSI-01, DSI-02	PR.DS-1, PR.DS-2	Artikel 6.3	Abschnitt 2.5	Artikel 23	Artikel 4
Analyse und Reaktion auf Ereignisse	9.1.2, 9.1.3	3.2.1, 3.2.2	11.1, 11.2	OPS3, OPS4	IVS-05, IVS-06	RS.CO-1, RS.CO-2	Artikel 6.4	Abschnitt 2.6	Artikel 23	Artikel 4
Zugriffskontrollen für Protokollaten	9.2.1, 9.2.2	4.1.1, 4.1.2	12.1, 12.2	OPS5, OPS6	IAM-01, IAM-02	PR.AC-1, PR.AC-2	Artikel 6.5	Abschnitt 2.7	Artikel 23	Artikel 4
Schulung und Sensibilisierung	6.3.1, 6.3.2	4.2.1, 4.2.2	13.1, 13.2	ORP5, ORP6	STA-01, STA-02	PR.AT-1, PR.AT-2	Artikel 6.6	Abschnitt 2.8	Artikel 23	Artikel 4

## Richtlinien und Anforderungen

### Protokollierungsanforderungen

Alle sicherheitsrelevanten Ereignisse und Aktivitäten in den IT-Systemen müssen protokolliert werden (ISO 27001: 8.1.1, 8.1.2). Dies umfasst das Erstellen von Protokollen für Benutzerzugriffe, Systemänderungen und sicherheitsrelevante Ereignisse (CIS Controls 8.1, 8.2, TISAX 1.1.1, 1.2.1). Die Protokollierung muss regelmäßig überprüft und aktualisiert werden, um sicherzustellen, dass sie den aktuellen Sicherheitsanforderungen entspricht (BSI C5: ORP1, ORP2, CCM IVS-01, IVS-02).

### Überwachungsanforderungen

Alle IT-Systeme müssen kontinuierlich überwacht werden, um sicherheitsrelevante Ereignisse frühzeitig zu erkennen (ISO 27001: 8.2.1, 8.2.2). Dies umfasst die Implementierung von Überwachungssystemen, die in der Lage sind, ungewöhnliche Aktivitäten zu erkennen und zu melden (CIS Controls 9.1, 9.2, TISAX 2.1.1, 2.1.2). Die Überwachung muss regelmäßig überprüft und angepasst werden, um die Effektivität sicherzustellen (BSI C5: ORP3, ORP4, CCM IVS-03, IVS-04).

### Aufbewahrung und Schutz der Protokolle

Protokolle müssen sicher aufbewahrt und vor unbefugtem Zugriff geschützt werden (ISO 27001: 8.3.1, 8.3.2). Dies umfasst die Nutzung sicherer Speicherorte und die Implementierung von Zugriffskontrollen (CIS Controls 10.1, 10.2, TISAX 3.1.1, 3.1.2). Regelmäßige Überprüfungen der Aufbewahrung und des Schutzes der Protokolle sind notwendig, um die Sicherheit zu gewährleisten (NIST CSF PR.DS-1, PR.DS-2, BSI C5: OPS1, OPS2, CCM DSI-01, DSI-02).

### Analyse und Reaktion auf Ereignisse

Alle protokollierten Ereignisse müssen regelmäßig analysiert und bewertet werden (ISO 27001: 9.1.2, 9.1.3). Dies umfasst die Identifizierung von Sicherheitsvorfällen und die Implementierung von Reaktionsmaßnahmen (CIS Controls 11.1, 11.2, TISAX 3.2.1, 3.2.2). Die Ergebnisse der Analyse müssen dokumentiert und zur Verbesserung der Sicherheitsmaßnahmen verwendet werden (NIST CSF RS.CO-1, RS.CO-2, BSI C5: OPS3, OPS4, CCM IVS-05, IVS-06).

**Zugriffskontrollen für Protokolldaten**

Der Zugriff auf Protokolldaten muss streng kontrolliert werden (ISO 27001: 9.2.1, 9.2.2). Dies umfasst die Implementierung von Zugriffskontrollen und Authentifizierungsmechanismen, um unbefugten Zugriff zu verhindern (CIS Controls 12.1, 12.2, TISAX 4.1.1, 4.1.2). Regelmäßige Überprüfungen der Zugriffskontrollen sind notwendig, um die Sicherheit der Protokolldaten zu gewährleisten (NIST CSF PR.AC-1, PR.AC-2, BSI C5: OPS5, OPS6, CCM IAM-01, IAM-02).

**Schulung und Sensibilisierung**

Alle Mitarbeiter müssen regelmäßig Schulungen zur Protokollierung und Überwachung durchlaufen (ISO 27001: 6.3.1, 6.3.2). Diese Schulungen müssen die aktuellen Bedrohungen, Sicherheitsmaßnahmen und Best Practices abdecken (CIS Controls 13.1, 13.2, 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 Monitoring 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	<a href="#">ISO 27001:2022</a>
CIS Controls v8	Sicherheitsmaßnahmen gegen Cyberangriffe	<a href="#">CIS Controls v8</a>
BSI C5:2020	Cloud Security Standard	<a href="#">BSI C5:2020</a>
Cloud Controls Matrix (CCM)	Sicherheitskontrollen für Cloud-Dienste	<a href="#">Cloud Controls Matrix</a>
NIST Cybersecurity Framework	Rahmenwerk zur Verbesserung der Cybersicherheit	<a href="#">NIST CSF</a>
NIS2 Draft	EU-Richtlinie zur Netz- und Informationssicherheit	<a href="#">NIS2 Draft</a>
OH SzA für KRITIS	Orientierungshilfe Angriffserkennung für Kritische Infrastrukturen	<a href="#">OH SzA</a>
European Cyber Resilience Act	EU-Verordnung zur Cyber-Resilienz	<a href="#">European CRA</a>
Digital Operational Resilience Act (DORA)	EU-Verordnung zur digitalen operationellen Resilienz	<a href="#">DORA</a>

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 einer effektiven Protokollierungs- und Überwachungsstrategie bei [Unternehmen].

**Dokumentinformationen**

**Titel:** Richtlinie zur Protokollierung und Überwachung  
**Version:** 1.0  
**Datum:** [Heutiges Datum]  
**Verantwortlich:** IT-Sicherheitsbeauftragter  
**Genehmigt von:** [Name der genehmigenden Person]  
**Nächste Überprüfung:** [Datum der nächsten Überprüfung]