


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 für das Incident Management

Datum: [Heutiges Datum]

Einleitung

Diese Richtlinie für das Incident Management definiert die Anforderungen und Maßnahmen zur Sicherstellung eines effizienten und effektiven Umgangs mit Sicherheitsvorfällen innerhalb der IT-Infrastruktur von [Unternehmen]. Diese Richtlinie basiert auf den Best Practices und Empfehlungen von Atlassian, ManageEngine, ITIL und xMatters sowie 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, DORA und den OWASP Best Practices.

Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiter, Auftragnehmer, Berater, Zeitarbeitskräfte, Praktikanten und mit Dritten verbundene Personen, die für das Management und die Reaktion auf Sicherheitsvorfälle in der IT-Infrastruktur von [Unternehmen] verantwortlich sind.

Compliance Matrix

Die Compliance Matrix dient dazu, die Konformität dieser Richtlinie für das Incident Management 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
Incident Identification	8.22.1, 8.22.2	1.1.1, 1.2.1	4.1, 4.2	ORP1, ORP2	IAM-01, IAM-02	DE.CM-1, DE.CM-2	Artikel 5, 6.1	Abschnitt 2.3	Artikel 23	Artikel 4
Incident Classification und Priorisierung	8.22.1, 8.22.2	2.1.1, 2.1.2	5.1, 5.2	ORP3, ORP4	IAM-03, IAM-04	DE.CM-3, DE.CM-4	Artikel 5, 6.2	Abschnitt 2.4	Artikel 23	Artikel 4
Incident Response	8.27.1, 8.27.2	3.1.1, 3.1.2	6.1, 6.2	OPS1, OPS2	IVS-01, IVS-02	RS.RP-1, RS.RP-2	Artikel 6.3	Abschnitt 2.5	Artikel 23	Artikel 4
Incident Mitigation und Containment	8.27.1, 8.27.2	4.1.1, 4.1.2	8.1, 8.2	OPS3, OPS4	IVS-03, IVS-04	RS.MI-1, RS.MI-2	Artikel 6.4	Abschnitt 2.6	Artikel 23	Artikel 4
Incident Recovery	8.27.1, 8.27.2	3.2.1, 3.2.2	5.4, 5.5	ORP5, ORP6	IAM-05, IAM-06	RS.RC-1, RS.RC-2	Artikel 6.5	Abschnitt 2.7	Artikel 23	Artikel 4
Incident Documentation und Reporting	8.27.1, 8.27.2	2.2.1, 2.2.2	13.1, 13.2	ORP7, ORP8	IVS-03, IVS-04	RS.IM-1, RS.IM-2	Artikel 6.8	Abschnitt 2.9	Artikel 23	Artikel 4
Incident Analysis und Lessons Learned	8.27.1, 8.27.2	4.2.1, 4.2.2	17.1, 17.2	ORP9, ORP10	DSI-01, DSI-02	RS.AN-1, RS.AN-2	Artikel 6.10	Abschnitt 2.11	Artikel 23	Artikel 4
Incident Communication	8.27.1, 8.27.2	3.3.1, 3.3.2	11.1, 11.2	ORP11, ORP12	DSI-03, DSI-04	RS.CO-1, RS.CO-2	Artikel 6.12	Abschnitt 2.13	Artikel 23	Artikel 4

Richtlinien und Anforderungen

Incident Identification

Sicherheitsvorfälle müssen umgehend erkannt und identifiziert werden (ISO 27001: 8.22.1, 8.22.2). Dies umfasst die Implementierung von Überwachungs- und Erkennungssystemen, die potenzielle Vorfälle identifizieren und melden können (CIS Controls 4.1, 4.2, TISAX 1.1.1, 1.2.1). Automatisierte Tools sollten eingesetzt werden, um Anomalien und ungewöhnliche Aktivitäten zu erkennen (NIST CSF DE.CM-1, DE.CM-2, BSI C5: ORP1, ORP2, CCM IAM-01, IAM-02).

Incident Classification und Priorisierung

Sicherheitsvorfälle müssen nach ihrer Schwere und ihrem potenziellen Einfluss klassifiziert und priorisiert werden (ISO 27001: 8.22.1, 8.22.2). Dies umfasst die Implementierung eines Systems zur Bewertung und Klassifizierung von Vorfällen (CIS Controls 5.1,

5.2, TISAX 2.1.1, 2.1.2). Regelmäßige Überprüfungen und Aktualisierungen der Klassifizierungskriterien sind notwendig, um sicherzustellen, dass sie den aktuellen Bedrohungen entsprechen (NIST CSF DE.CM-3, DE.CM-4, BSI C5: ORP3, ORP4, CCM IAM-03, IAM-04).

Incident Response

Ein effektiver Incident-Response-Plan muss implementiert werden, um auf Sicherheitsvorfälle schnell und effektiv reagieren zu können (ISO 27001: 8.27.1, 8.27.2). Dies umfasst die Identifizierung, Analyse und Behebung von Sicherheitsvorfällen sowie die Dokumentation und Berichterstattung der Vorfälle (CIS Controls 6.1, 6.2, TISAX 3.1.1, 3.1.2). Regelmäßige Übungen und Überprüfungen des Incident-Response-Plans sind notwendig, um sicherzustellen, dass alle Beteiligten auf Vorfälle vorbereitet sind (NIST CSF RS.RP-1, RS.RP-2, BSI C5: OPS1, OPS2, CCM IVS-01, IVS-02).

Incident Mitigation und Containment

Alle Maßnahmen zur Eindämmung und Minderung von Sicherheitsvorfällen müssen umgehend umgesetzt werden (ISO 27001: 8.27.1, 8.27.2). Dies umfasst die Implementierung von Verfahren und Techniken zur Eindämmung von Vorfällen und zur Minderung ihres Einflusses (CIS Controls 8.1, 8.2, TISAX 4.1.1, 4.1.2). Regelmäßige Überprüfungen und Aktualisierungen der Eindämmungs- und Minderungstechniken sind notwendig (NIST CSF RS.MI-1, RS.MI-2, BSI C5: OPS3, OPS4, CCM IVS-03, IVS-04).

Incident Recovery

Ein effektiver Recovery-Plan muss implementiert werden, um nach einem Sicherheitsvorfall schnell wieder in den Normalbetrieb zurückzukehren (ISO 27001: 8.27.1, 8.27.2). Dies umfasst die Wiederherstellung von Systemen und Daten sowie die Überprüfung und Validierung der Wiederherstellungsmaßnahmen (CIS Controls 5.4, 5.5, TISAX 3.2.1, 3.2.2). Regelmäßige Übungen und Überprüfungen des Recovery-Plans sind notwendig, um sicherzustellen, dass die Wiederherstellungsprozesse effektiv sind (NIST CSF RS.RC-1, RS.RC-2, BSI C5: ORP5, ORP6, CCM IAM-05, IAM-06).

Incident Documentation und Reporting

Alle Sicherheitsvorfälle müssen dokumentiert und an die relevanten Stakeholder berichtet werden (ISO 27001: 8.27.1, 8.27.2). Dies umfasst die Erstellung von detaillierten Berichten, die die Art des Vorfalls, die durchgeführten Maßnahmen und die Ergebnisse dokumentieren (CIS Controls 13.1, 13.2, TISAX 2.2.1, 2.2.2). Die Berichte müssen regelmäßig überprüft und analysiert werden, um Verbesserungspotenziale zu identifizieren (NIST CSF RS.IM-1, RS.IM-2, BSI C5: ORP7, ORP8, CCM IVS-03, IVS-04).

Incident Analysis und Lessons Learned

Nach jedem Sicherheitsvorfall muss eine umfassende Analyse durchgeführt werden, um die Ursachen und Auswirkungen des Vorfalls zu verstehen (ISO 27001: 8.27.1, 8.27.2). Dies umfasst die Durchführung von "Lessons Learned"-Sitzungen, um die Erkenntnisse aus dem Vorfall zu dokumentieren und Maßnahmen zur Vermeidung zukünftiger Vorfälle zu implementieren (CIS Controls 17.1, 17.2, TISAX 4.2.1, 4.2.2). Die Ergebnisse der Analyse müssen dokumentiert und regelmäßig überprüft werden (NIST CSF RS.AN-1, RS.AN-2, BSI C5: ORP9, ORP10, CCM DSI-01, DSI-02).

Incident Communication

Eine effektive Kommunikation ist während und nach einem Sicherheitsvorfall von entscheidender Bedeutung (ISO 27001: 8.27.1, 8.27.2). Dies umfasst die Benachrichtigung der relevanten Stakeholder, die Kommunikation mit betroffenen Parteien und die Bereitstellung von regelmäßigen Updates zum Status des Vorfalls (CIS Controls 11.1, 11.2, TISAX 3.3.1, 3.3.2). Die Kommunikationsprozesse müssen regelmäßig überprüft und aktualisiert werden, um sicherzustellen, dass sie effektiv sind (NIST CSF RS.CO-1, RS.CO-2, BSI C5: ORP11, ORP12, CCM DSI-03, DSI-04).

Verantwortliche

Die Implementierung und Einhaltung dieser Richtlinie liegt in der Verantwortung des IT-Sicherheitsbeauftragten und des Incident 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
Atlassian Incident Management Best Practices	Leitfaden für Incident Management	Atlassian Incident Management
ManageEngine Major Incident Management Best Practices	Best Practices für Incident Management	ManageEngine Incident Management
ITIL Incident Management	ITIL-Leitfaden für Incident Management	ITIL Incident Management
xMatters Incident Management Best Practices	Best Practices für langfristigen Erfolg im Incident Management	xMatters Incident Management
ManageEngine IT Incident Management	Definition und Überblick über IT Incident Management	ManageEngine IT Incident Management

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 Incident Managements bei [Unternehmen].

Dokumentinformationen

Titel: Richtlinie für das Incident Management

Version: 1.0

Datum: [Heutiges Datum]

Verantwortlich: IT-Sicherheitsbeauftragter

Genehmigt von: [Name der genehmigenden Person]

Nächste Überprüfung: [Datum der nächsten Überprüfung]