



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 zur sicheren Softwareentwicklung

Datum: [Heutiges Datum]

Einleitung

Diese Richtlinie zur sicheren Softwareentwicklung definiert die Anforderungen und Maßnahmen zur Sicherstellung der Sicherheit und des Schutzes der entwickelten Software innerhalb der IT-Infrastruktur von [Unternehmen]. Diese Richtlinie basiert auf den Best Practices und Empfehlungen von OWASP, Berkeley, Snyk und NIST 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 an der Softwareentwicklung in der IT-Infrastruktur von [Unternehmen] beteiligt sind.

Compliance Matrix

Die Compliance Matrix dient dazu, die Konformität dieser Richtlinie zur sicheren Softwareentwicklung 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
Sicherheitsanforderungen und Planung	8.25.1, 8.25.2	1.1.1, 1.2.1	4.1, 4.2	ORP1, ORP2	IAM-01, IAM-02	PR.AC-1, PR.AC-2	Artikel 5, 6.1	Abschnitt 2.3	Artikel 23	Artikel 4
Sichere Entwicklungsumgebung	8.26.1, 8.26.2	2.1.1, 2.1.2	5.1, 5.2	ORP3, ORP4	IAM-03, IAM-04	PR.AC-3, PR.AC-4	Artikel 5, 6.2	Abschnitt 2.4	Artikel 23	Artikel 4
Source Code Management	8.23.1, 8.23.2	3.1.1, 3.1.2	6.1, 6.2	ORP5, ORP6	IVS-01, IVS-02	DE.CM-1, DE.CM-2	Artikel 6.3	Abschnitt 2.5	Artikel 23	Artikel 4
Schwachstellenanalyse und -management	8.19.1, 8.19.2	4.1.1, 4.1.2	8.1, 8.2	ORP7, ORP8	IVS-03, IVS-04	ID.RA-1, ID.RA-2	Artikel 6.4	Abschnitt 2.6	Artikel 23	Artikel 4
Sicherheitsüberprüfung und Tests	8.16.1, 8.16.2	3.2.1, 3.2.2	5.4, 5.5	ORP9, ORP10	IAM-05, IAM-06	PR.AC-5, PR.AC-6	Artikel 6.5	Abschnitt 2.7	Artikel 23	Artikel 4
Continuous Integration/Continuous Deployment (CI/CD)	8.25.1, 8.25.2	2.2.1, 2.2.2	13.1, 13.2	OPS5, OPS6	IVS-03, IVS-04	PR.IP-1, PR.IP-2	Artikel 6.8	Abschnitt 2.9	Artikel 23	Artikel 4
Sicherheitsmonitoring und Incident Response	8.22.1, 8.22.2	4.2.1, 4.2.2	17.1, 17.2	ORP11, ORP12	DSI-01, DSI-02	PR.AT-1, PR.AT-2	Artikel 6.10	Abschnitt 2.11	Artikel 23	Artikel 4
Lieferanten- und Drittanbieter-Management	8.29.1, 8.29.2	2.3.1, 2.3.2	7.1, 7.2	ORP13, ORP14	IVS-05, IVS-06	PR.IP-1, PR.IP-2	Artikel 6.12	Abschnitt 2.13	Artikel 23	Artikel 4
Sicherheitsbewusstsein und Schulung	6.3.1, 6.3.2	3.3.1, 3.3.2	11.1, 11.2	ORP15, ORP16	DSI-03, DSI-04	RS.RP-1, RS.RP-2	Artikel 6.16	Abschnitt 2.17	Artikel 23	Artikel 4
Risikomanagement und Bewertung	8.9.1, 8.9.2	3.4.1, 3.4.2	13.4, 13.5	ORP17, ORP18	IVS-07, IVS-08	PR.DS-1, PR.DS-2	Artikel 6.18	Abschnitt 2.19	Artikel 23	Artikel 4

Richtlinien und Anforderungen

Sicherheitsanforderungen und Planung

Alle Sicherheitsanforderungen und Planungen müssen in der frühen Phase der Softwareentwicklung berücksichtigt werden (ISO 27001: 8.25.1, 8.25.2). Dies umfasst die Identifizierung von Sicherheitsanforderungen basierend auf den Best Practices und Standards (CIS Controls 4.1, 4.2, TISAX 1.1.1, 1.2.1). Die Planung muss dokumentiert und regelmäßig überprüft werden, um sicherzustellen, dass alle

Sicherheitsanforderungen erfüllt sind (NIST CSF PR.AC-1, PR.AC-2, BSI C5: ORP1, ORP2, CCM IAM-01, IAM-02).

Sichere Entwicklungsumgebung

Die Entwicklungsumgebung muss sicher konfiguriert und vor unbefugtem Zugriff geschützt werden (ISO 27001: 8.26.1, 8.26.2). Dies beinhaltet den Einsatz sicherer Entwicklungsplattformen und Tools sowie die Implementierung von Zugriffs- und Änderungskontrollen (CIS Control 5.1, 5.2, TISAX 2.1.1, 2.1.2). Regelmäßige Überprüfungen und Bewertungen der Entwicklungsumgebung sind notwendig, um sicherzustellen, dass sie gegen aktuelle Bedrohungen geschützt ist (NIST CSF PR.AC-3, PR.AC-4, BSI C5: ORP3, ORP4, CCM IAM-03, IAM-04).

Source Code Management

Der Quellcode muss sicher verwaltet und geschützt werden (ISO 27001: 8.23.1, 8.23.2). Dies umfasst die Implementierung von Versionskontrollsystemen, die Nachverfolgung von Änderungen und die Durchführung von Code-Reviews (CIS Controls 6.1, 6.2, TISAX 3.1.1, 3.1.2). Der Quellcode muss regelmäßig auf Sicherheitslücken überprüft und vor unbefugtem Zugriff geschützt werden (NIST CSF DE.CM-1, DE.CM-2, BSI C5: ORP5, ORP6, CCM IVS-01, IVS-02).

Schwachstellenanalyse und -management

Alle entwickelten Softwareprodukte müssen regelmäßig auf Schwachstellen analysiert und diese Schwachstellen müssen zeitnah behoben werden (ISO 27001: 8.19.1, 8.19.2). Dies umfasst die Durchführung von statischen und dynamischen Codeanalysen sowie Penetrationstests (CIS Controls 8.1, 8.2, TISAX 4.1.1, 4.1.2). Automatisierte Tools sollten eingesetzt werden, um Schwachstellen zu identifizieren und zu beheben (NIST CSF ID.RA-1, ID.RA-2, BSI C5: ORP7, ORP8, CCM IVS-03, IVS-04).

Sicherheitsüberprüfung und Tests

Regelmäßige Sicherheitsüberprüfungen und Tests müssen durchgeführt werden, um die Sicherheit der Software zu gewährleisten (ISO 27001: 8.16.1, 8.16.2). Dies umfasst Code-Reviews, Sicherheitstests und die Implementierung von Sicherheitsprüfungen im Rahmen der Continuous Integration/Continuous Deployment (CI/CD) Pipelines (CIS Controls 5.4, 5.5, TISAX 3.2.1, 3.2.2). Die Ergebnisse der Überprüfungen und Tests müssen dokumentiert und analysiert werden, um Maßnahmen zur Verbesserung der Sicherheit zu identifizieren (NIST CSF PR.AC-5, PR.AC-6, BSI C5: ORP9, ORP10, CCM IAM-05, IAM-06).

Continuous Integration/Continuous Deployment (CI/CD)

Die Sicherheitsmaßnahmen müssen in die CI/CD-Prozesse integriert werden (ISO 27001: 8.25.1, 8.25.2). Dies umfasst die Automatisierung von Sicherheitsprüfungen, Tests und Audits innerhalb der CI/CD-Pipelines (CIS Controls 13.1, 13.2, TISAX 2.2.1, 2.2.2). Sicherheitsanforderungen müssen regelmäßig überprüft und aktualisiert werden, um sicherzustellen, dass sie den aktuellen Bedrohungen entsprechen (NIST CSF PR.IP-1, PR.IP-2, BSI C5: OPS5, OPS6, CCM IVS-03, IVS-04).

Sicherheitsmonitoring und Incident Response

Ein effektives Sicherheitsmonitoring und Incident-Response-Plan müssen implementiert werden, um auf Sicherheitsvorfälle schnell und effektiv reagieren zu können (ISO 27001: 8.22.1, 8.22.2). Dies umfasst die Implementierung von Überwachungs- und Protokollierungssystemen, um ungewöhnliche Aktivitäten zu erkennen und zu melden, sowie die Durchführung regelmäßiger Übungen zur Vorbereitung auf Sicherheitsvorfälle (CIS Controls 17.1, 17.2, TISAX 4.2.1, 4.2.2). Die Ergebnisse müssen dokumentiert und analysiert werden, um Verbesserungspotenziale zu identifizieren (NIST CSF PR.AT-1, PR.AT-2, BSI C5: ORP11, ORP12, CCM DSI-01, DSI-02).

Lieferanten- und Drittanbieter-Management

Alle Lieferanten und Drittanbieter, die an der Softwareentwicklung beteiligt sind, müssen überprüft und ihre Sicherheitsmaßnahmen bewertet werden (ISO 27001: 8.29.1, 8.29.2). Dies umfasst die Durchführung von Sicherheitsüberprüfungen und Audits der Lieferanten sowie die Implementierung von vertraglichen Verpflichtungen zur Einhaltung der Sicherheitsanforderungen (CIS Controls 7.1, 7.2, TISAX 2.3.1, 2.3.2). Regelmäßige Überprüfungen der Sicherheitsmaßnahmen der Lieferanten sind notwendig, um sicherzustellen, dass sie den aktuellen Sicherheitsstandards entsprechen (NIST CSF PR.IP-1, PR.IP-2, BSI C5: ORP13, ORP14, CCM IVS-05, IVS-06).

Sicherheitsbewusstsein und Schulung

Alle Mitarbeiter müssen regelmäßig Schulungen zur sicheren Softwareentwicklung durchlaufen (ISO 27001: 6.3.1, 6.3.2). Diese Schulungen müssen die aktuellen Bedrohungen, Sicherheitsmaßnahmen und Best Practices abdecken (CIS Controls 11.1, 11.2, TISAX 3.3.1, 3.3.2). Sensibilisierungsmaßnahmen müssen implementiert werden, um sicherzustellen, dass alle Mitarbeiter über die aktuellen Sicherheitsanforderungen informiert sind (NIST CSF RS.RP-1, RS.RP-2, BSI C5: ORP15, ORP16, CCM DSI-03, DSI-04).

Risikomanagement und Bewertung

Ein effektives Risikomanagement muss implementiert werden, um Sicherheitsrisiken zu identifizieren, zu bewerten und zu managen (ISO 27001: 8.9.1, 8.9.2). Dies umfasst die Durchführung regelmäßiger Risikoanalysen und die Implementierung von Maßnahmen zur

Risikominderung (CIS Controls 13.4, 13.5, TISAX 3.4.1, 3.4.2). Die Ergebnisse der Risikoanalysen müssen dokumentiert und regelmäßig überprüft werden, um sicherzustellen, dass alle identifizierten Risiken angemessen gemanagt werden (NIST CSF PR.DS-1, PR.DS-2, BSI C5: ORP17, ORP18, CCM IVS-07, IVS-08).

Verantwortliche

Die Implementierung und Einhaltung dieser Richtlinie liegt in der Verantwortung des IT-Sicherheitsbeauftragten und des Softwareentwicklungsteams. 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
OWASP Secure Coding Practices	Best Practices für sicheres Codieren	OWASP Secure Coding
Berkeley Secure Coding Practice Guidelines	Leitlinien für sichere Programmierung	Berkeley Secure Coding
Snyk Secure Coding Practices	Leitfaden für sichere Programmierung	Snyk Secure Coding
NIST Secure Software Development Framework (SSDF)	Rahmenwerk für sichere Softwareentwicklung	NIST SSDF

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 sicheren Softwareentwicklung bei [Unternehmen].

Dokumentinformationen

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