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 Nutzung von IoT (Internet of Things)

Datum: [Heutiges Datum]

Einleitung

Diese Richtlinie zur sicheren Nutzung von IoT (Internet of Things) definiert die Anforderungen und Maßnahmen zur Sicherstellung der Sicherheit und des Schutzes von IoT-Ressourcen innerhalb der IT-Infrastruktur von [Unternehmen]. Diese Richtlinie basiert auf den Best Practices und Empfehlungen von 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 für die Verwaltung und Sicherung von IoT-Ressourcen in der IT-Infrastruktur von [Unternehmen] verantwortlich sind.

Compliance Matrix

Die Compliance Matrix dient dazu, die Konformität dieser Richtlinie zur sicheren Nutzung von IoT 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
Verwaltung von Identitäten und Zugriffsrechten	9.2.1, 9.2.2	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
Least Privilege und Zugriffskontrollen	9.1.2, 9.1.3	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

Überwachung und Protokollierung	8.16.1, 8.16.2	3.1.1, 3.1.2	6.1, 6.2	OPS1, OPS2	IVS-01, IVS-02	DE.CM-1, DE.CM-2	Artikel 6.3	Abschnitt 2.5	Artikel 23	Artikel 4
Sicherheitsüberprüfung und Audits	8.16.1, 8.16.2	4.1.1, 4.1.2	8.1, 8.2	OPS3, OPS4	IVS-03, IVS-04	ID.RA-1, ID.RA-2	Artikel 6.4	Abschnitt 2.6	Artikel 23	Artikel 4
Verwaltung von Servicekonten und API-Schlüsseln	9.4.1, 9.4.2	3.2.1, 3.2.2	5.4, 5.5	ORP5, ORP6	IAM-05, IAM-06	PR.AC-5, PR.AC-6	Artikel 6.5	Abschnitt 2.7	Artikel 23	Artikel 4
Netzwerk- und Infrastruktursicherheit	8.14.1, 8.14.2	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
Schulung und Sensibilisierung	6.3.1, 6.3.2	4.2.1, 4.2.2	17.1, 17.2	ORP7, ORP8	STA-01, STA-02	PR.AT-1, PR.AT-2	Artikel 6.10	Abschnitt 2.11	Artikel 23	Artikel 4
Patching und Schwachstellenmanagement	8.28.1, 8.28.2	2.3.1, 2.3.2	7.1, 7.2	ORP9, ORP10	IVS-05, IVS-06	PR.IP-1, PR.IP-2	Artikel 6.12	Abschnitt 2.13	Artikel 23	Artikel 4
Backup und Wiederherstellung	8.32.1, 8.32.2	3.3.1, 3.3.2	11.1, 11.2	ORP11, ORP12	DSI-01, DSI-02	PR.IP-4, PR.IP-5	Artikel 6.14	Abschnitt 2.15	Artikel 23	Artikel 4
Incident Response	8.27.1, 8.27.2	4.3.1, 4.3.2	16.1, 16.2	ORP13, ORP14	DSI-03, DSI-04	RS.RP-1, RS.RP-2	Artikel 6.16	Abschnitt 2.17	Artikel 23	Artikel 4
Logging und Monitoring	8.16.1, 8.16.2	3.1.1, 3.1.2	6.1, 6.2	OPS1, OPS2	IVS-01, IVS-02	DE.CM-1, DE.CM-2	Artikel 6.3	Abschnitt 2.5	Artikel 23	Artikel 4
Verschlüsselung und Schlüsselmanagement	8.24.1, 8.24.2	3.4.1, 3.4.2	13.4, 13.5	ORP15, ORP16	IVS-07, IVS-08	PR.DS-1, PR.DS-2	Artikel 6.18	Abschnitt 2.19	Artikel 23	Artikel 4
Sicherheit von Containerdiensten	8.15.1, 8.15.2	2.4.1, 2.4.2	18.1, 18.2	ORP17, ORP18	IVS-09, IVS-10	PR.IP-6, PR.IP-7	Artikel 6.20	Abschnitt 2.21	Artikel 23	Artikel 4
Verwaltung von Firewalls und Netzwerksicherheitsgruppen	8.22.1, 8.22.2	3.5.1, 3.5.2	12.1, 12.2	ORP19, ORP20	IVS-11, IVS-12	PR.PT-1, PR.PT-2	Artikel 6.22	Abschnitt 2.23	Artikel 23	Artikel 4
Verwaltung von Ressourcen- und Kosteneffizienz	8.33.1, 8.33.2	4.4.1, 4.4.2	19.1, 19.2	ORP21, ORP22	IVS-13, IVS-14	PR.IP-8, PR.IP-9	Artikel 6.24	Abschnitt 2.25	Artikel 23	Artikel 4

Richtlinien und Anforderungen

Verwaltung von Identitäten und Zugriffsrechten

Alle Identitäten und Zugriffsrechte müssen gemäß den festgelegten Verfahren verwaltet werden. Dies umfasst die Erstellung,Änderung und Deaktivierung von Benutzerkonten sowie die Zuweisung von Zugriffsrechten in IoT-Systemen (CIS Controls 4.1, 4.2, TISAX 1.1.1, 1.2.1). Regelmäßige Überprüfungen der Identitäten und Zugriffsrechte sind notwendig, um sicherzustellen, dass nur autorisierte Benutzer Zugriff auf die Systeme haben (BSI C5: ORP1, ORP2, CCM IAM-01, IAM-02).

Least Privilege und Zugriffskontrollen

Der Zugang zu IoT-Systemen und Informationen muss durch das Prinzip der minimalen Rechte (Least Privilege) und durch geeignete Zugriffskontrollen gesichert werden (ISO 27001: 9.1.2, 9.1.3). Dies umfasst die Implementierung von Multi-Faktor-Authentifizierung und strikten Zugangskontrollen, um unbefugten Zugriff zu verhindern (CIS Controls 5.1, 5.2, TISAX 2.1.1, 2.1.2). Regelmäßige Überprüfungen und Aktualisierungen der Zugriffskontrollen sind notwendig, um die Sicherheit zu gewährleisten (NIST CSF PR.AC-3, PR.AC-4, BSI C5: ORP3, ORP4, CCM IAM-03, IAM-04).

Überwachung und Protokollierung

Alle Aktivitäten im Zusammenhang mit der Verwaltung von IoT-Ressourcen müssen kontinuierlich überwacht und regelmäßig überprüft werden (ISO 27001: 8.16.1, 8.16.2). Dies umfasst die Einrichtung von Überwachungs- und Protokollierungssystemen, um ungewöhnliche Aktivitäten zu erkennen und zu melden (CIS Controls 6.1, 6.2, TISAX 3.1.1, 3.1.2). Die Ergebnisse der Überwachung müssen dokumentiert und analysiert werden, um Verbesserungspotenziale zu identifizieren (NIST CSF DE.CM-1, DE.CM-2, BSI C5: OPS1, OPS2, CCM IVS-01, IVS-02).

Sicherheitsüberprüfung und Audits

Regelmäßige Sicherheitsüberprüfungen und Audits müssen durchgeführt werden, um die Wirksamkeit der Sicherheitsmaßnahmen zu überprüfen und Schwachstellen zu identifizieren (ISO 27001: 8.16.1, 8.16.2). Dies umfasst die Durchführung von internen und externen Audits sowie die regelmäßige Bewertung der Sicherheitskonfigurationen (CIS Controls 8.1, 8.2, TISAX 4.1.1, 4.1.2). Die Ergebnisse der Audits müssen dokumentiert und analysiert werden, um Maßnahmen zur Verbesserung der Sicherheit zu identifizieren (NIST CSF ID.RA-1, ID.RA-2, BSI C5: OPS3, OPS4, CCM IVS-03, IVS-04).

Verwaltung von Servicekonten und API-Schlüsseln

Servicekonten und API-Schlüssel müssen sicher verwaltet und geschützt werden (ISO 27001: 9.4.1, 9.4.2). Dies umfasst die Erstellung von beschreibenden Servicekonten, den Schutz von Servicekontenschlüsseln mit Cloud Key Management Service (KMS) und deren sichere Speicherung (CIS Controls 5.4, 5.5, TISAX 3.2.1, 3.2.2). Regelmäßige Überprüfungen und Rotation der Schlüssel sind notwendig, um die Sicherheit zu gewährleisten (NIST CSF PR.AC-5, PR.AC-6, BSI C5: ORP5, ORP6, CCM IAM-05, IAM-06).

Netzwerk- und Infrastruktursicherheit

Netzwerk- und Infrastruktursicherheit müssen gewährleistet werden, um die Vertraulichkeit, Integrität und Verfügbarkeit der IoT-Ressourcen zu schützen (ISO 27001: 8.14.1, 8.14.2). Dies umfasst die Implementierung von Firewalls, Netzwerksicherheitsgruppen und anderen Sicherheitsmechanismen, um unbefugten Zugriff und Angriffe zu verhindern (CIS Controls 13.1, 13.2, TISAX 2.2.1, 2.2.2). Regelmäßige Überprüfungen und Aktualisierungen der Netzwerksicherheitskonfigurationen sind notwendig (NIST CSF PR.IP-1, PR.IP-2, BSI C5: OPS5, OPS6, CCM IVS-03, IVS-04).

Schulung und Sensibilisierung

Alle Mitarbeiter müssen regelmäßig Schulungen zur Verwaltung von IoT-Ressourcen 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: ORP7, ORP8, CCM STA-01, STA-02).

Patching und Schwachstellenmanagement

Alle Systeme und Anwendungen müssen regelmäßig auf Sicherheitspatches überprüft und aktualisiert werden (ISO 27001: 8.28.1, 8.28.2). Dies umfasst die Implementierung eines Schwachstellenmanagementprozesses, um Sicherheitslücken zu identifizieren und zu beheben (CIS Controls 7.1, 7.2, TISAX 2.3.1, 2.3.2). Automatisierte Tools und Verfahren sollten eingesetzt werden, um die Effizienz und Genauigkeit des Patching-Prozesses zu erhöhen (NIST CSF PR.IP-1, PR.IP-2, BSI C5: ORP9, ORP10, CCM IVS-05, IVS-06).

Backup und Wiederherstellung

Regelmäßige Backups aller kritischen Daten und Systeme müssen durchgeführt werden, um die Wiederherstellung im Falle eines Datenverlustes zu gewährleisten (ISO 27001: 8.32.1, 8.32.2). Die Backup-Prozesse müssen dokumentiert und regelmäßig getestet werden, um ihre Wirksamkeit sicherzustellen (CIS Controls 11.1, 11.2, TISAX 3.3.1, 3.3.2). Die Backups müssen sicher gespeichert und vor unbefugtem Zugriff geschützt

werden (NIST CSF PR.IP-4, PR.IP-5, BSI C5: ORP11, ORP12, CCM DSI-01, DSI-02).

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 16.1, 16.2, TISAX 4.3.1, 4.3.2). 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: ORP13, ORP14, CCM DSI-03, DSI-04).

Logging und Monitoring

Alle sicherheitsrelevanten Aktivitäten müssen kontinuierlich protokolliert und überwacht werden (ISO 27001: 8.16.1, 8.16.2). Dies umfasst die Implementierung von Logging- und Monitoring-Lösungen, um verdächtige Aktivitäten zu erkennen und zu analysieren (CIS Controls 6.1, 6.2, TISAX 3.1.1, 3.1.2). Die Protokolldaten müssen sicher gespeichert und regelmäßig überprüft werden, um Sicherheitsvorfälle zu identifizieren und zu beheben (NIST CSF DE.CM-1, DE.CM-2, BSI C5: OPS1, OPS2, CCM IVS-01, IVS-02).

Verschlüsselung und Schlüsselmanagement

Alle sensiblen Daten müssen während der Übertragung und im Ruhezustand verschlüsselt werden (ISO 27001: 8.24.1, 8.24.2). Dies umfasst die Implementierung von Verschlüsselungslösungen und Schlüsselmanagementprozessen, um die Vertraulichkeit und Integrität der Daten zu gewährleisten (CIS Controls 13.4, 13.5, TISAX 3.4.1, 3.4.2). Die Verschlüsselungsschlüssel müssen sicher gespeichert und regelmäßig überprüft und aktualisiert werden (NIST CSF PR.DS-1, PR.DS-2, BSI C5: ORP15, ORP16, CCM IVS-07, IVS-08).

Sicherheit von IoT-Geräten

AlleIoT-Geräte müssen sicher konfiguriert und vor unbefugtem Zugriff geschützt werden (ISO 27001: 8.15.1, 8.15.2). Dies umfasst die Implementierung von Sicherheitsmaßnahmen wie Netzwerksegmentierung, Zugriffskontrollen und regelmäßige Sicherheitsüberprüfungen der Geräte (CIS Controls 18.1, 18.2, TISAX 2.4.1, 2.4.2). Automatisierte Tools sollten eingesetzt werden, um die Sicherheit der IoT-Umgebung kontinuierlich zu überwachen und Schwachstellen zu identifizieren (NIST CSF PR.IP-6, PR.IP-7, BSI C5: ORP17, ORP18, CCM IVS-09, IVS-10).

Verwaltung von Firewalls und Netzwerksicherheitsgruppen

Firewalls und Netzwerksicherheitsgruppen müssen konfiguriert und verwaltet werden, um den Netzwerkverkehr zu überwachen und zu kontrollieren (ISO 27001: 8.22.1, 8.22.2). Dies umfasst die Implementierung von Regeln zur Beschränkung des Zugriffs auf autorisierte Netzwerke und Ressourcen (CIS Controls 12.1, 12.2, TISAX 3.5.1, 3.5.2). Regelmäßige Überprüfungen und Aktualisierungen der Firewall- und Sicherheitsgruppenkonfigurationen sind notwendig, um die Sicherheit zu gewährleisten (NIST CSF PR.PT-1, PR.PT-2, BSI C5: ORP19, ORP20, CCM IVS-11, IVS-12).

Verwaltung von Ressourcen- und Kosteneffizienz

Die Verwaltung von IoT-Ressourcen muss effizient und kosteneffektiv erfolgen (ISO 27001: 8.33.1, 8.33.2). Dies umfasst die Überwachung und Optimierung der Ressourcennutzung, um sicherzustellen, dass ungenutzte oder überdimensionierte Ressourcen identifiziert und entfernt werden (CIS Controls 19.1, 19.2, TISAX 4.4.1, 4.4.2). Automatisierte Tools und Verfahren sollten eingesetzt werden, um die Ressourcennutzung kontinuierlich zu überwachen und zu optimieren (NIST CSF PR.IP-8, PR.IP-9, BSI C5: ORP21, ORP22, CCM IVS-13, IVS-14).

Automatisierung und Orchestrierung

Automatisierung und Orchestrierung müssen zur Verwaltung und Sicherung der IoT-Ressourcen eingesetzt werden (ISO 27001: 8.25.1, 8.25.2). Dies umfasst die Implementierung von Tools und Verfahren zur Automatisierung von Sicherheitsaufgaben wie Patching, Überwachung und Incident Response (CIS Controls 14.1, 14.2, TISAX 2.5.1, 2.5.2). Die Automatisierung muss sicher konfiguriert und regelmäßig überprüft werden, um sicherzustellen, dass sie korrekt funktioniert und keine neuen Sicherheitsrisiken einführt (NIST CSF PR.AC-1, PR.AC-2, BSI C5: ORP23, ORP24, CCM IAM-07, IAM-08).

Verantwortliche

Die Implementierung und Einhaltung dieser Richtlinie liegt in der Verantwortung des IT-Sicherheitsbeauftragten und des IoT 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
NIST Cybersecurity IoT Program	Best Practices für IoT-Sicherheit	NIST Cybersecurity IoT Program
NIST Internet of Things (IoT)	Leitlinien zur Sicherung von IoT	NIST IoT
OWASP Best Practices	Best Practices für die Sicherheit von IoT	OWASP IoT

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 Verwaltung von IoT-Ressourcen bei [Unternehmen].

Dokumentinformationen

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