


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 Benutzerzugangsmanagement

Datum: [Heutiges Datum]

Einleitung

Diese Richtlinie zum Benutzerzugangsmanagement definiert die Anforderungen und Maßnahmen zur Sicherstellung eines sicheren und effektiven Managements von Benutzerzugängen zu IT-Systemen und Informationen 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 Zugang zu den IT-Systemen und Informationen von [Unternehmen] haben oder für deren Verwaltung verantwortlich sind.

Compliance Matrix

Die Compliance Matrix dient dazu, die Konformität dieser Richtlinie zum Benutzerzugangsmanagement 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
Benutzerregistrierung und -abmeldung	9.2.1, 9.2.2	1.1.1, 1.2.1	6.1, 6.2	ORP1, ORP2	IAM-01, IAM-02	PR.AC-1, PR.AC-2	Artikel 5, 6.1	Abschnitt 2.3	Artikel 23	Artikel 4
Zugriffskontrollen und Authentifizierung	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
Verwaltung privilegierter Zugänge	9.4.1, 9.4.2	3.1.1, 3.1.2	7.1, 7.2	OPS1, OPS2	IAM-05, IAM-06	PR.PT-1, PR.PT-2	Artikel 6.3	Abschnitt 2.5	Artikel 23	Artikel 4
Überwachung und Überprüfung von Zugängen	9.5.1, 9.5.2	4.1.1, 4.1.2	8.1, 8.2	OPS3, OPS4	IVS-01, IVS-02	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

Benutzerregistrierung und -abmeldung

Alle Benutzer müssen gemäß den festgelegten Verfahren registriert und abgemeldet werden (ISO 27001: 9.2.1, 9.2.2). Dies umfasst die Erstellung, Änderung und Deaktivierung von Benutzerkonten sowie die Zuweisung von Zugriffsrechten (CIS Controls 6.1, 6.2, TISAX 1.1.1, 1.2.1). Regelmäßige Überprüfungen der Benutzerkonten sind notwendig, um sicherzustellen, dass nur autorisierte Benutzer Zugriff auf die Systeme haben (BSI C5: ORP1, ORP2, CCM IAM-01, IAM-02).

Zugriffskontrollen und Authentifizierung

Der Zugang zu IT-Systemen und Informationen muss durch geeignete Zugriffskontrollen und Authentifizierungsmechanismen 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 Zugangskontrollen sind notwendig, um die Sicherheit zu gewährleisten (NIST CSF PR.AC-3, PR.AC-4, BSI C5: ORP3, ORP4, CCM IAM-03, IAM-04).

Verwaltung privilegierter Zugänge

Privilegierte Zugänge müssen streng verwaltet und kontrolliert werden (ISO 27001: 9.4.1, 9.4.2). Dies umfasst die Implementierung von Maßnahmen zur Verwaltung und Überwachung privilegierter Benutzerkonten, um Missbrauch zu verhindern (CIS Controls 7.1, 7.2, TISAX 3.1.1, 3.1.2). Regelmäßige Überprüfungen der privilegierten Zugänge sind notwendig, um sicherzustellen, dass sie nur für autorisierte Zwecke verwendet werden (NIST CSF PR.PT-1, PR.PT-2, BSI C5: OPS1, OPS2, CCM IAM-05, IAM-06).

Überwachung und Überprüfung von Zugängen

Alle Benutzerzugriffe müssen kontinuierlich überwacht und regelmäßig überprüft werden (ISO 27001: 9.5.1, 9.5.2). Dies umfasst die Einrichtung von Überwachungs- und Protokollierungssystemen, um ungewöhnliche Aktivitäten zu erkennen und zu melden (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-01, IVS-02).

Schulung und Sensibilisierung

Alle Mitarbeiter müssen regelmäßig Schulungen zum Benutzerzugangsmanagement 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 User Access 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 Benutzerzugangsmanagement bei [Unternehmen].

Dokumentinformationen

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