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 Business Continuity Management

Datum: [Heutiges Datum]

Einleitung

Diese Richtlinie für das Business Continuity Management (BCM) definiert die Anforderungen und Maßnahmen zur Sicherstellung der Kontinuität der Geschäftstätigkeiten von [Unternehmen] im Falle von Störungen oder Krisen. Diese Richtlinie basiert auf den Best Practices und Empfehlungen des BSI, Continuity2, CIO.com, Continuity Central und PhoenixNAP 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 Business Continuity Management in der IT-Infrastruktur von [Unternehmen] verantwortlich sind.

Compliance Matrix

Die Compliance Matrix dient dazu, die Konformität dieser Richtlinie für das Business Continuity 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
BCM Policy und Programmmanagement	8.24.1, 8.24.2	1.1.1, 1.2.1	4.1, 4.2	ORP1, ORP2	IAM-01, IAM-02	ID.BE-1, ID.BE-2	Artikel 5, 6.1	Abschnitt 2.3	Artikel 23	Artikel 4
Business Impact Analysis (BIA)	8.24.1, 8.24.2	2.1.1, 2.1.2	5.1, 5.2	ORP3, ORP4	IAM-03, IAM-04	ID.BE-3, ID.BE-4	Artikel 5, 6.2	Abschnitt 2.4	Artikel 23	Artikel 4
Risk Assessment und Management	8.24.1, 8.24.2	3.1.1, 3.1.2	6.1, 6.2	OPS1, OPS2	IVS-01, IVS-02	ID.RA-1, ID.RA-2	Artikel 6.3	Abschnitt 2.5	Artikel 23	Artikel 4
Strategieentwicklung	8.24.1, 8.24.2	4.1.1, 4.1.2	8.1, 8.2	OPS3, OPS4	IVS-03, IVS-04	ID.RA-3, ID.RA-4	Artikel 6.4	Abschnitt 2.6	Artikel 23	Artikel 4
Implementierung und Betrieb	8.24.1, 8.24.2	3.2.1, 3.2.2	5.4, 5.5	ORP5, ORP6	IAM-05, IAM-06	ID.RA-5, ID.RA-6	Artikel 6.5	Abschnitt 2.7	Artikel 23	Artikel 4
Schulung und Bewusstsein	8.24.1, 8.24.2	2.2.1, 2.2.2	13.1, 13.2	ORP7, ORP8	IVS-03, IVS-04	PR.AT-1, PR.AT-2	Artikel 6.8	Abschnitt 2.9	Artikel 23	Artikel 4
Testen und Übung	8.24.1, 8.24.2	4.2.1, 4.2.2	17.1, 17.2	ORP9, ORP10	DSI-01, DSI-02	PR.IP-1, PR.IP-2	Artikel 6.10	Abschnitt 2.11	Artikel 23	Artikel 4
Wartung und Aktualisierung	8.24.1, 8.24.2	3.3.1, 3.3.2	11.1, 11.2	ORP11, ORP12	DSI-03, DSI-04	PR.IP-3, PR.IP-4	Artikel 6.12	Abschnitt 2.13	Artikel 23	Artikel 4
Kommunikation und Berichterstattung	8.24.1, 8.24.2	3.4.1, 3.4.2	13.4, 13.5	ORP13, ORP14	IVS-07, IVS-08	PR.IP-5, PR.IP-6	Artikel 6.14	Abschnitt 2.15	Artikel 23	Artikel 4
Incident Response und Wiederherstellung	8.27.1, 8.27.2	4.1.1, 4.1.2	5.4, 5.5	ORP15, ORP16	DSI-03, DSI-04	RS.RP-1, RS.RP-2	Artikel 6.16	Abschnitt 2.17	Artikel 23	Artikel 4

Richtlinien und Anforderungen

BCM Policy und Programmmanagement

Ein umfassendes Business Continuity Management Programm muss entwickelt und implementiert werden, um die Kontinuität der Geschäftstätigkeiten zu gewährleisten (ISO 27001: 8.24.1, 8.24.2). Dies umfasst die Entwicklung einer BCM-Policy, die Rollen und

Verantwortlichkeiten definiert und die regelmäßige Überprüfung und Aktualisierung der Policy (CIS Controls 4.1, 4.2, TISAX 1.1.1, 1.2.1). Regelmäßige Schulungen und Sensibilisierungsmaßnahmen sind notwendig, um sicherzustellen, dass alle Mitarbeiter die BCM-Policy verstehen und umsetzen können (NIST CSF ID.BE-1, ID.BE-2, BSI C5: ORP1, ORP2, CCM IAM-01, IAM-02).

Business Impact Analysis (BIA)

Eine Business Impact Analysis (BIA) muss durchgeführt werden, um kritische Geschäftsprozesse zu identifizieren und die potenziellen Auswirkungen von Unterbrechungen zu bewerten (ISO 27001: 8.24.1, 8.24.2). Dies umfasst die Identifizierung von Abhängigkeiten, die Bewertung der maximal tolerierbaren Ausfallzeit (MTPD) und die Festlegung von Wiederherstellungszielen (CIS Controls 5.1, 5.2, TISAX 2.1.1, 2.1.2). Die BIA muss regelmäßig überprüft und aktualisiert werden, um sicherzustellen, dass sie den aktuellen Geschäftsanforderungen entspricht (NIST CSF ID.BE-3, ID.BE-4, BSI C5: ORP3, ORP4, CCM IAM-03, IAM-04).

Risk Assessment und Management

Ein umfassendes Risikomanagement muss implementiert werden, um potenzielle Risiken für die Geschäftskontinuität zu identifizieren, zu bewerten und zu managen (ISO 27001: 8.24.1, 8.24.2). Dies umfasst die Durchführung regelmäßiger Risikoanalysen und die Implementierung von Maßnahmen zur Risikominderung (CIS Controls 6.1, 6.2, TISAX 3.1.1, 3.1.2). Die Ergebnisse der Risikoanalysen müssen dokumentiert und regelmäßig überprüft werden, um sicherzustellen, dass alle identifizierten Risiken angemessen gemanagt werden (NIST CSF ID.RA-1, ID.RA-2, BSI C5: OPS1, OPS2, CCM IVS-01, IVS-02).

Strategieentwicklung

Die Entwicklung einer umfassenden Strategie zur Sicherstellung der Geschäftskontinuität ist entscheidend (ISO 27001: 8.24.1, 8.24.2). Dies umfasst die Identifizierung von Alternativlösungen, die Implementierung von Backup- und Wiederherstellungsprozessen und die Festlegung von Prioritäten für die Wiederherstellung (CIS Controls 8.1, 8.2, TISAX 4.1.1, 4.1.2). Die Strategie muss regelmäßig überprüft und aktualisiert werden, um sicherzustellen, dass sie den aktuellen Geschäftsanforderungen und Bedrohungen entspricht (NIST CSF ID.RA-3, ID.RA-4, BSI C5: OPS3, OPS4, CCM IVS-03, IVS-04).

Implementierung und Betrieb

Die Business Continuity Strategie muss implementiert und kontinuierlich betrieben werden (ISO 27001: 8.24.1, 8.24.2). Dies umfasst die Einrichtung eines Business Continuity Management Teams, die Implementierung von Notfallplänen und die Sicherstellung der Verfügbarkeit von Ressourcen und Informationen (CIS Controls 5.4, 5.5, TISAX 3.2.1, 3.2.2). Regelmäßige Überprüfungen und Tests der implementierten Maßnahmen sind notwendig, um ihre Wirksamkeit sicherzustellen (NIST CSF ID.RA-5, ID.RA-6, BSI C5: ORP5, ORP6, CCM IAM-05, IAM-06).

Schulung und Bewusstsein

Regelmäßige Schulungen und Sensibilisierungsmaßnahmen müssen durchgeführt werden, um sicherzustellen, dass alle Mitarbeiter die Business Continuity Prozesse und ihre Rolle darin verstehen (ISO 27001: 8.24.1, 8.24.2). Diese Schulungen müssen die aktuellen Bedrohungen, Sicherheitsmaßnahmen und Best Practices abdecken (CIS Controls 13.1, 13.2, TISAX 2.2.1, 2.2.2). 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 IVS-03, IVS-04).

Testen und Übung

Regelmäßige Tests und Übungen der Business Continuity Pläne sind notwendig, um ihre Wirksamkeit zu überprüfen und sicherzustellen, dass alle Beteiligten auf eine tatsächliche Krise vorbereitet sind (ISO 27001: 8.24.1, 8.24.2). Dies umfasst die Durchführung von Simulationen, Stresstests und die Bewertung der Reaktionsfähigkeit (CIS Controls 17.1, 17.2, TISAX 4.2.1, 4.2.2). Die Ergebnisse der Tests und Übungen müssen dokumentiert und analysiert werden, um Verbesserungspotenziale zu identifizieren (NIST CSF PR.IP-1, PR.IP-2, BSI C5: ORP9, ORP10, CCM DSI-01, DSI-02).

Wartung und Aktualisierung

Die Business Continuity Pläne müssen regelmäßig gewartet und aktualisiert werden, um sicherzustellen, dass sie den aktuellen Geschäftsanforderungen und Bedrohungen entsprechen (ISO 27001: 8.24.1, 8.24.2). Dies umfasst die Überprüfung und Aktualisierung der Pläne basierend auf den Ergebnissen von Tests, Übungen und tatsächlichen Vorfällen (CIS Controls 11.1, 11.2, TISAX 3.3.1, 3.3.2). Regelmäßige Überprüfungen sind notwendig, um sicherzustellen, dass die Pläne aktuell und wirksam sind (NIST CSF PR.IP-3, PR.IP-4, BSI C5: ORP11, ORP12, CCM IVS-03, IVS-04).

Kommunikation und Berichterstattung

Eine effektive Kommunikation und Berichterstattung während und nach einer Krise sind entscheidend (ISO 27001: 8.24.1, 8.24.2). Dies

umfasst die Benachrichtigung der relevanten Stakeholder, die Kommunikation mit betroffenen Parteien und die Bereitstellung von regelmäßigen Updates zum Status der Wiederherstellungsmaßnahmen (CIS Controls 13.4, 13.5, TISAX 3.4.1, 3.4.2). Die Kommunikationsprozesse müssen regelmäßig überprüft und aktualisiert werden, um sicherzustellen, dass sie effektiv sind (NIST CSF PR.IP-5, PR.IP-6, BSI C5: ORP13, ORP14, CCM IVS-07, IVS-08).

Incident Response und Wiederherstellung

Ein effektiver Incident-Response- und Wiederherstellungsplan 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 5.4, 5.5, TISAX 4.1.1, 4.1.2). 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: ORP15, ORP16, CCM DSI-03, DSI-04).

Verantwortliche

Die Implementierung und Einhaltung dieser Richtlinie liegt in der Verantwortung des IT-Sicherheitsbeauftragten und des Business Continuity 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
BSI-Standard 200-4: Business Continuity Management	Leitfaden für Business Continuity Management	BSI BCM
Continuity2: 10 Best Practices for Effective Business Continuity Strategy	Best Practices für Business Continuity	Continuity2 Best Practices
CIO.com: How to Create an Effective Business Continuity Plan	Leitfaden für die Erstellung eines Business Continuity Plans	CIO.com Best Practices
Continuity Central: 7 Best Practices for Business Continuity	Best Practices für Business Continuity	Continuity Central Best Practices
PhoenixNAP: Business Continuity Best Practices	Best Practices für Business Continuity	PhoenixNAP Best Practices

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 Business Continuity Managements bei [Unternehmen].

Dokumentinformationen

Titel: Richtlinie für das Business Continuity Management
Version: 1.0
Datum: [Heutiges Datum]
Verantwortlich: IT-Sicherheitsbeauftragter
Genehmigt von: [Name der genehmigenden Person]
Nächste Überprüfung: [Datum der nächsten Überprüfung]