SEC4YOU

Advanced IT-Audit Services

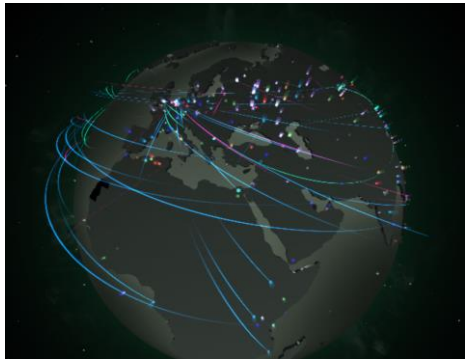
PUBLIC TLP:CLEAR

Welche der Maßnahmen aus ISO 27001, NIS2 und Cybertrust helfen gegen Cybergefahren?

Ing. Andreas Schuster, Senior Manager bei SEC4YOU Advanced IT-Audit Service GmbH,
CMG Director Themenpanel Informationssicherheit & Cybersecurity, CMG-AE
Katharina Rom, MSc, Senior Information Security Consultant bei SEC4YOU Advanced IT-Audit Service GmbH

Warum sollen wir uns gegen Cybergefahren schützen?

- Verschiebung der **Bedrohungen** – nicht nur „die Großen“, auch KMUs
- Umsatzausfälle, Gerichtskosten, Bußgelder, Schadenersatz-ansprüche von Kunden und Partnern werden rasch **existenzbedrohend**
- Die Geschäftsführung **haftet** bei unzureichendem "Basisschutz" solidarisch für den entstandenen Schaden (GmbH Recht § 43 Haftung der Geschäftsführer)



→ Generell steigende **regulatorische Anforderungen**

SEC4YOU
Advanced IT-Audit Services

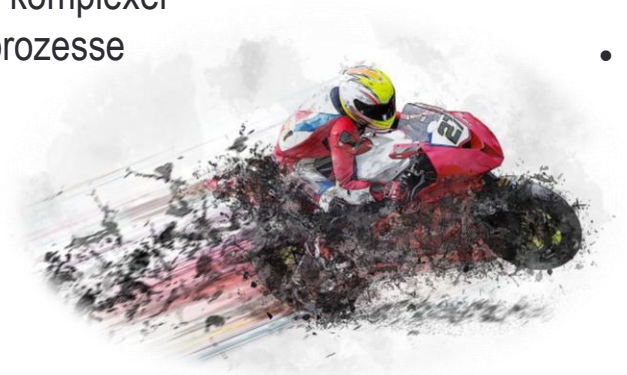
Welche Merkmale und konkrete Maßnahmen gegen Cybergefahren haben die Regelwerke?

	Cyber Trust Silber Label	ISO 27001	NIS 2
Anwendungsbereich	Österreichisches Label; Schema zur **Bewertung des Cyber Risk Ratings** in Unternehmen	**Internationaler** Standard; für alle Sektoren, Branchen und Größen	**EU-Richtlinie**; Cybersicherheit kritischer Infrastrukturen und digitaler Dienste in der EU
Zielsetzung	Schaffung von **Sicherheit, Vertrauen und Transparenz**	Management von **Informationssicherheitsrisiken** und Umsetzung eines **ISMS**	Gewährleistung der **Cybersicherheit kritischer Infrastrukturen** und **digitaler Dienste**
Verpflichtung	freiwillig (geprüft)	freiwillig (geprüft)	bindend (geprüft)
Kritische Infrastruktur	**Können** geschützt werden	**Können** geschützt werden	**Müssen** geschützt werden
Maßnahmen gegen Cybergefahren	**10 “Basisschutz“-Maßnahmen** **2 „Cyberschutz“-Maßnahmen**	**14 „Basisschutz“-Maßnahmen** **8 „Cyberschutz“-Maßnahmen**	**2 „Basisschutz“-Maßnahmen** **2 „Cyberschutz“-Maßnahmen**

Zwei Umsetzungsmethoden

Risikobasierter Ansatz

- Maßnahmen werden auf Basis von Gefährdungen im Zuge eines Risiko-Assessments ermittelt
- Abdeckung komplexer Geschäftsprozesse



Quick-Win Ansatz

- Der Maßnahmenkatalog wird reduziert, um wesentliche Maßnahmen zu priorisieren
- Geeignet für kleinere, nicht zu komplexe Unternehmen
- Nicht geeignet bei Zertifizierungsvorhaben

Was haben wir uns überlegt?

- Wir analysieren die Maßnahmen vom **Cyber Trust Silber Label**, von der neuen **ISO 27001:2022** und der **NIS2 Richtlinie**.
- Dabei klassifizieren wir die Maßnahmen in folgende Kategorien:

„**Basisschutz**“ – Einfache Schutzmaßnahmen die Unternehmen umsetzen sollten.

„**Cyberschutz**“ – Schutzmaßnahmen die präventiv vor Cyberangriffen helfen.

„**Business Continuity**“ – Maßnahmen die Unternehmen helfen resilienter zu werden und Notfälle schneller/besser zu überstehen.

„**Erweiterter Schutz**“ – Maßnahmen, die spezielle Bedrohungen abdecken, z.B. physische Sicherheit oder bei der Softwareentwicklung

Inhalt des Cyber Trust Silber Label → 14 Maßnahmen

B1 Sicherheits-Richtlinien	B2 Security Schulung	B3 InfoSec Verantwortlichen	B4 Asset Verwaltung
B5 Need-to-Know Berechtigungen	B6 Passwort-Sicherheit	B7 Sichere IT-Konfigurationen	B8 Sicherheitscheck Individualsoftware
B9 Updates aller IT-Systeme	B10 Internet-Firewall	B11 Malware Schutz	B12 verschlüsselte Übertragung im Internet
~~B13 Protokollierung~~	~~B14 IT-Notfallplanung~~		

Basisschutz
Cyberschutz
Business Continuity
Erweiterter Schutz

Inhalt der ISO 27001:2022 → 1-25 von 93 Maßnahmen

A5.1 InfoSec-Richtlinien	A5.2 InfoSec Verantwortlichkeiten	A5.3 Aufgaben-trennung	A5.4 Verantwortung der Geschäftsleitung	A5.5 Kontakt mit Behörden
A5.6 Kontakt mit Interessensgruppen	A5.7 Analyse der Bedrohungslage	A5.8 InfoSec im Projektmanagement	A5.9 Asset Verwaltung	A5.10 Zulässige Nutzung von Assets
A5.11 Rückgabe von Vermögenswerten	A5.12 Klassifizierung von Informationen	A5.13 Kennzeichnung von Informationen	A5.14 Übertragung von Informationen	A5.15 Zugangs-kontrolle
A5.16 Identitäts-Management	A5.17 Umgang mit Authentifizierung	A5.18 Zugriffsrechte	A5.19 Lieferanten-Management	A5.20 Lieferanten-vereinbarungen
A5.21 InfoSec in der Lieferkette	A5.22 Überwachung Lieferantenleistungen	A5.23 InfoSec bei Cloud-Diensten	A5.24 Management Sicherheitsvorfälle	A5.25 Bewertung Sicherheitsereignisse

Basisschutz
Cyberschutz
Business Continuity
Erweiterter Schutz

Inhalt der ISO 27001:2022 → 26-50 von 93 Maßnahmen

A5.26 Sicherheits-Vorfälle	A5.27 Lernen aus Sicherheitsvorfällen	A5.28 Sammlung von Beweisen	A5.29 Störungen / Unterbrechungen	A5.30 Geschäfts-Kontinuität
A5.31 Compliance	A5.32 Geistiges Eigentum	A5.33 Schutz von Aufzeichnungen	A5.34 DSGVO - Datenschutz	A5.35 Überprüfung d. Informationssicherheit
A5.36 Einhaltung von Richtlinien	A5.37 Dokumentierte Betriebsverfahren	A6.1 Bewerber Screening	A6.2 InfoSec in Arbeitsverträgen	A6.3 Security Awareness
A6.4 Disziplinar-verfahren	A6.5 Beendigung von Dienstverhältnissen	A6.6 Vertraulichkeits-Vereinbarungen	A6.7 Remote-Arbeit	A6.8 Meldung von Ereignissen/Vorfällen
A7.1 Definition von Sicherheitszonen	A7.2 Physischer Zutritt	A7.3 Sicherung von Standorten	A7.4 Überwachung physische Sicherheit	A7.5 Umwelt-bedrohungen

Basisschutz
Cyberschutz
Business Continuity
Erweiterter Schutz

Inhalt der ISO 27001:2022 → 51-75 von 93 Maßnahmen

A7.6 Arbeiten in Sicherheitsbereichen	A7.7 Arbeitsplatz-sicherheit (Sperre)	A7.8 Schutz von Geräten	A7.9 Geräte außerhalb der Geschäftsräume	A7.10 Speichermedien
A7.11 Versorgungs-Einrichtungen	A7.12 Sicherheit der Verkabelung	A7.13 Wartung der Geräte	A7.14 Sichere Entsorgung	A8.1 Benutzer Endgeräte
A8.2 Privilegierte Zugriffsrechte	A8.3 Beschränkung des Informationszugangs	A8.4 Zugang zum Quellcode	A8.5 Sichere Authentifizierung	A8.6 Verwaltung der Kapazitäten
A8.7 Schutz vor Malware	A8.8 Technische Schwachstellen	A8.9 Verwaltung von Konfigurationen	A8.10 Löschung von Informationen	A8.11 Maskierung von Informationen
A8.12 Verhinderung von Datenverlusten (DLP)	A8.13 Informations-sicherung / Backup	A8.14 Redundanzen	A8.15 Protokollierung	A8.16 Überwachung der Aktivitäten

Basisschutz
Cyberschutz
Business Continuity
Erweiterter Schutz

Inhalt der ISO 27001:2022 → 76-93 von 93 Maßnahmen

A8.17 Uhren-Synchronisation	A8.18 Privilegierte Dienstprogramme	A8.19 Installation von Software	A8.20 Netzwerk-Kontrollen	A8.21 Sicherheit der Netzdienste
A8.22 Netzwerk-Trennung / Segmentierung	A8.23 Web-Filterung	A8.24 Einsatz von Kryptographie	A8.25 Lebenszyklus der Entwicklung	A8.26 InfoSec bei der Beschaffung
A8.27 Secure Coding Grundsätze	A8.28 Sichere Softwareentwicklung	A8.29 Sicherheits-test in der Entwicklung	A8.30 Ausgelagerte Entwicklung	A8.31 Ausgelagerte Entwicklung
A8.32 Verwaltung von Änderungen	A8.33 Testdaten	A8.34 Schutz der IT während Prüfungen		

Basisschutz
Cyberschutz
Business Continuity
Erweiterter Schutz

Inhalt der NIS2 → 10 Risikomanagementmaßnahmen in Artikel 21

a) Risikoanalyse, Sicherheit IT-Systeme	b) Bewältigung von Sicherheitsvorfällen	c) Aufrechterhaltung des Betriebs	d) Sicherheit der Lieferkette
e) Sicherheit bei Erwerb/Entwicklung	f) Bewertung Risiko für Cybersicherheit	g) Verfahren zur Cyberhygiene*	h) Einsatz von Kryptographie
i) Personalsicherheit, Zugriffskontrolle	j) Multi-Faktor-Authentifizierung		

*) primär Asset-Management, Endgerätschutz/Malschutz, Patch-Management, Konfig-Management, Verschlüsselung

Basisschutz
Cyberschutz
Business Continuity
Erweiterter Schutz

Maßnahmen der Kategorie „Basisschutz“

Cyber Trust Silber Label	Zusätzlich aus der ISO 27001	Zusätzlich aus der NIS2
Sicherheitsrichtlinien	Zulässige Nutzung von Assets	~~Verfahren zur Cyberhygiene~~ (bereits abgedeckt)
InfoSec Verantwortlichen	Zugangskontrolle	
Asset Verwaltung	Identitätsmanagement	
Berechtigungen nach „Need-to-Know“	Umgang mit Authentifizierung	
Passwort-Sicherheit	InfoSec in Arbeitsverträgen	
Sichere Konfigurationen	Vertraulichkeitsvereinbarungen (NDA)	
Sicherheitscheck Individualsoftware	Benutzer-Endgeräte	
Updates aller Systeme	Informationssicherung / Backup	
Internet Firewall	Einsatz von Kryptographie	
Malware Schutz		

Maßnahmen der Kategorie „Cyberschutz“

Cyber Trust Silber Label	Zusätzlich aus der ISO 27001	Zusätzlich aus der NIS2
Security Awareness Schulungen	Überprüfung der Informationssicherheit	Verpflichtend Multi-Faktor-Authentifizierung
Verschlüsselte Übertragung im Internet	Meldung von Ereignissen/Vorfällen	
	Management privilegierter Zugriffsrechte	
	Sichere Authentifizierung	
	Prüfung auf technische Schwachstellen	
	Web-Filterung	

Empfohlene Vorgangsweise für KMUs

1. Setzen Sie alle Maßnahmen von **„Basisschutz“** und **„Cyberschutz“** um!
2. Prüfen Sie dann ob Maßnahmen von **„Erweiterter Schutz“** für Sie zutreffen und behandeln sie diese.
3. Implementieren Sie anschließend Maßnahmen von **„Business Continuity“** in Art und Umfang angemessen.

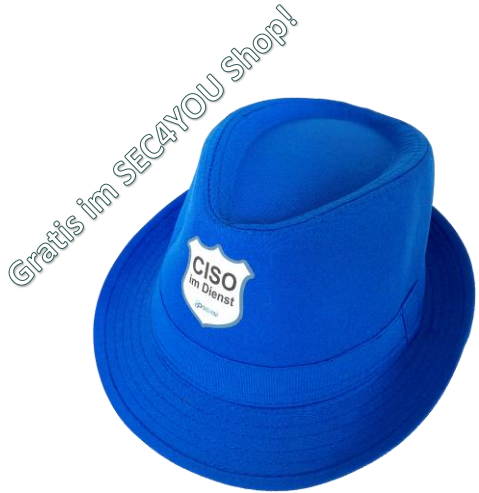
- Eine Sicherheitszertifizierung nach ISO 27001 oder TISAX® ist nach Umsetzung der Punkte 1-3 mit geringem Aufwand möglich.

Empfohlene Vorgangsweise für Großkunden

1. Setzen Sie alle Maßnahmen von **„Basisschutz“** und **„Cyberschutz“** um!
2. Implementieren Sie anschließend die Maßnahmen von **„Business Continuity“.**
3. Prüfen Sie dann welche Maßnahmen von **„Erweiterter Schutz“** für Sie zutreffen und behandeln sie diese.

- Eine Sicherheitszertifizierung nach ISO 27001 oder TISAX® ist nach Umsetzung der Punkte 1-3 mit mittlerem Aufwand möglich.

Fragen?



Katharina.Rom@sec4you.com
https://sec4you.com
Tel.: +43 676 5111247

Andreas.Schuster@sec4you.com
https://sec4you.com
Tel.: +43 678 1216943