NIS-2 Anforderungen	Sicherheitsvorfälle bewältigen	Backup- und Krisenmanagement	Lieferketten- und Dienstleistersicherheit	Sicherheit in Entwicklung und Wartung	Bewertung der Cybersicherheit
	End-to-End Anomalie und Angriffserkennung *Umfassende Erkennung und Protokollierung aller Ereignisse sowie automatische Reaktion auf Anomalien und Angriffe*	**Prozessstörungen vermeiden** *Planung und Implementierung von Sicherheitsmaßnahmen*	**Überwachung technischer Schnittstellen** *Überwachung und Auswertung der Schnittstellenkommunikation sowie Etablierung automatisierter Maßnahmen*	**Software und Infrastruktur Prüfung** *Regelmäßige Durchführung von Penetrationstests für die eigene Software und Infrastruktur.*	**Kont. Überprüfung der Cybersicherheit** *Kontinuierliche Überprüfung und Verbesserung des Cybersicherheitssystem durch automatisierte Analysen*
	Frühzeitige Erkennung von Bedrohungen *Frühzeitige Erkennung von Angriffen und böswilligen Aktivitäten, die kritische Dienste gefährden könnten*	**Business-Continuity-Plan erstellen** *Entwicklung eines Plans zur Sicherstellung der Betriebsfortführung im Krisenfall*	**Minimale Rechte für Lieferanten** *Implementierung von Zugriffsbeschränkungen nach dem Prinzip der minimalen Berechtigung für Lieferanten*	**Behebung von Schwachstellen** *Effektive und sichere Behebung von Schwachstellen*	**Bewertung der Cybersicherheitslage** *Regelmäßige Bewertung der Cybersicherheitslage und Risikoexposition*
	Effective Incident Response *Schnelle und gezielte Reaktion auf Cybervorfälle durch Erstellung eines Notfallplans*	**Mehrst. Backup-Management etablieren** *Implementierung eines mehrstufigen Backup-Systems zur Sicherstellung umfassender Datensicherung und Wiederherstellung*	**Sicheren Lieferanten-Zugang gewährleisten** *Erstellung von Lieferanten Zugängen z.B. über VPN's mit MFA*	**Kont. Schwachstellenüberwachung** *Kontinuierliche Überwachung und Bewertung von Schwachstellen*	
	Schnelle forensische Analyse *Sicherstellung einer zügigen Analyse und Bewertung der Auswirkungen nach einem Vorfall*	**Schnelle Notfallwiederherstellung** *Gewährleistung einer schnellen Wiederherstellung durch die Einführung eines IT-Notfallplans*			
	Abwehr von Schadsoftware und Angreifern *Abwehr von Schadsoftware und Angreifern an Netzwerkgrenzen durch die Einführung einer Firewall mit IDS/IPS und NDR*	**Krisenbewältigung und -kommunikation** *Einrichtung professioneller Prozesse für Krisenbewältigung und -kommunikation mittels eines IT-Notfallplan*			
	Managed Detection and Response (MDR) *Professionelle Überwachung sowie Reaktion auf Bedrohungen durch spezialisierte Anbieter für MDR*				

IT IN **BESTFORM.**

Technische Maßnahmen **Organisatorische Maßnahmen**

Schulungen in Cybersicherheit und -hygiene	Kryptografie und Verschlüsselung	Personalsicherheit und Zugriffskontrolle	Multi-Faktor und kont. Authentifizierung	Sichere Kommunikation	Risiko- und Schwachstellenanlyse
Defense-in-Depth-Architektur *Frühzeitige Erkennung von Sicherheitsproblemen an der Netzwerkgrenze und umfassende Überwachung des int. Netzwerks*	**Überwachung verschl. Verbindungen** *Überwachung und Überprüfung verschlüsselter Verbindungen gemäß dem aktuellen Stand der Technik*	**Überwachung kritischer Zugriffe** *Unternehmensweite Überwachung von Zugriffen auf kritische Dateien und Verzeichnisse*	**Schutz digitaler Assets** *Unbefugten Zugriff auf digitale Assets verhindern sowie Überwachung alle Logins und Loginversuche*	**Überw. von Kommunikationssystemen** *Überwachung sämtlicher Kommunikationssysteme und verschlüsselter Verbindungen*	**Risiko- und Schwachstellenmgmt.** *Identifizierung und Bewertung von Risiken und Schwachstellen*
Schutz gefährdeter Assets *Überwachung und Abschirmung von Assets, bei denen keine Patches oder Aktualisierungen möglich sind*	**Durchgehende verschl. Kommunikation** *Einrichtung und Sicherstellung durchgehender verschlüsselter Kommunikation im internen Netz*	**SÜ im Einstellungsprozess** *Integration von Sicherheitsüberprüfungen (SÜ) und -sensibilisierung in das Einstellungs- und Vertragsvergabeverfahren*	**Personalisierte MFA** *Sicherstellung einer personalisierten MFA (Multi-Faktor-Authentifizierung)*	**Frühwarnung an CSIRT** *Innerhalb von 24 Stunden nach einem Vorfall Frühwarnung an das CSIRT übermitteln*	**Asset Discovery und Softwareinventar** *Erfassung aller IT-Assets und Software zur vollständigen Übersicht und Risikominimierung*
Angriffsausbreitung eindämmen *Ausbreitung von Angriffen durch Netzsegmentierung verhindern*		**Physischen Zugriff schützen** *Unbefugten physischen Zugriff auf Assets verhindern*	**Sichere digitale Kommunikation** *Sichere digitale Kommunikation gewährleisten durch Verschlüsselung und Schutz vor unbefugtem Zugriff*	**Erste Bewertung an CSIRT** *Innerhalb von 72 Stunden erste Bewertung an das CSIRT übermitteln, einschließlich Schweregrad, Auswirkungen und Quelle*	**Schwachstellen und Sicherheitslücken entd.** *Entdeckung und Bewertung bestehender Schwachstellen und Sicherheitslücken*
Aktualisierung digitaler Ressourcen *Firmware, Betriebssysteme und andere digitale Ressourcen stets auf dem neuesten Stand halten*				**Statusaktualisierungen an CSIRT** *Auf Anfrage des CSIRT Aktualisierungen zum Status des Vorfallsmanagements bereitstellen*	**Penetrationstests der Infrastruktur** *Regelmäßige Tests der eigenen Infrastruktur und Sicherheitsmaßnahmen zur Identifizierung von Schwachstellen*
Starke Passwortrichtlinien *Strenge Passwortrichtlinien festlegen und umsetzen, die komplexe Anforderungen umfassen*				**Detaillierter Bericht an CSIRT** *Binnen eines Monats: Übermittlung eines det. Bericht an das CSIRT, einschl. Schweregrad, Auswirkungen, Ursache und Abhilfemaßnahmen.*	**Implementierung eines ISMS** *Umsetzung eines Informationssicherheits-Managementsystems nach ISO27001*
Cybersicherheits-schulungen *Regelmäßige Durchführung von Cybersicherheitsschulungen für das Personal*					

Technische Maßnahmen

Organisatorische Maßnahmen