littlebit
TECHNOLOGY

Cyber Security im IT-Handel: Checkliste für Entscheider

Handlungsfeld	Maßnahme / Ziel	Umsetzungsverantwortung	Umsetzungsstatus	Technischer Umsetzungsauftrag
Governance & Verantwortung	Cybersicherheit auf Leitungsebene verankern (CISO benennen und in Management einbinden)	Geschäftsführung / Vorstand	☐	CISO-Rolle einführen; klare Zuständigkeiten und Ressourcen definieren
Identitäts- & Zugriffsschutz	Multi-Faktor-Authentifizierung (MFA) unternehmensweit verpflichtend einführen	IT-Sicherheitsverantw. / IT-Leitung	☐	IT: MFA-Lösung für alle Benutzerkonten implementieren
Identitäts- & Zugriffsschutz	Remote-Zugänge und Fernwartung konsequent absichern (z. B. nur via VPN/Zero Trust mit MFA)	IT-Leitung / Netzwerkadmin	☐	IT: VPN/Zero Trust Network Access einrichten; MFA für alle Remote-Logins aktivieren
Schulung & Sensibilisierung	Regelmäßige Phishing-Tests und Security-Awareness-Schulungen für alle Mitarbeitenden durchführen	HR-Abteilung / IT-Security-Team	☐	HR/IT: Schulungsprogramm aufsetzen; Phishing-Simulationstools einsetzen
Lieferantenmanagement	Vertrauenswürdigkeit und Sicherheitsstandards aller Lieferanten regelmäßig prüfen und dokumentieren	Einkauf / Supply-Chain-Management	☐	Einkauf: Sicherheits-Fragebögen & Zertifikate (z. B. ISO 27001) einholen und auswerten
Lieferantenmanagement	Sicherheitsanforderungen vertraglich festschreiben und Audits bei kritischen Lieferanten vereinbaren	Geschäftsleitung / Compliance	☐	Compliance: Mindest-Sicherheitsstandards (z. B. MFA-Pflicht, Patch-Fristen) in Lieferverträge aufnehmen; IT: Lieferantenaudits durchführen

Netzwerk- & Zugriffskontrolle	Netzwerksegmentierung und -zugangskontrollen umsetzen (nur autorisierte Geräte/Benutzer erhalten Zugriff)	IT-Abteilung / Admins	☐	IT: Netzwerk segmentieren; Network Access Control (NAC) einsetzen (autorisierten Zugriff erzwingen)
Systemsicherheit & Wartung	Konsequentes Patch-Management etablieren (Sicherheitsupdates zeitnah und flächendeckend einspielen)	IT-Abteilung / Admin-Team	☐	IT: Update-Management automatisieren; Patches gemäß Richtlinien zeitnah einspielen
Produkt- & Systemintegrität	Integrität von Software- und Firmware-Updates gewährleisten (nur signierte Updates zulassen)	Produktentwicklung / IT-Sicherheit	☐	IT: Code-Signing einsetzen und Updates vor Verteilung auf Integrität prüfen
Vorfall- & Krisenmanagement	Incident-Response-Plan für Cyberangriffe (inkl. Lieferketten-Vorfälle) erstellen und regelmäßig üben	IT-Security-Team / Krisenstab	☐	IT-Security: Notfallplan dokumentieren; regelmäßige Incident-Response-Übungen (auch mit Partnern) durchführen
Vorfall- & Krisenmanagement	Verfahren für Sicherheitswarnungen und Produktrückrufe festlegen (unsichere Produkte umgehend vom Markt nehmen)	Produkt- / Qualitätsmanagement	☐	