VORTRIEB · CHECKLISTE

Meldepflichten bei Cybervorfällen: ISG, DSG und der EU Cyber Resilience Act im Meldeprozess

FÜR WEN

IT-Leitung, Geschäftsleitung und Produktverantwortliche von KMU mit 10 bis 200 Mitarbeitenden, die kritische Infrastrukturen betreiben oder beliefern, Personendaten bearbeiten oder Software und Geräte in die EU verkaufen

	AUFGABE	WER	BIS WANN
☐	Betroffenheit nach Art. 74b ISG geprüft, auch Bst. u für Hersteller, und Ergebnis dokumentiert		
☐	Bei Unsicherheit beim BACS Auskunft zur Meldepflicht verlangt		
☐	Prüfung abgeschlossen, ob Produkte mit digitalen Elementen in der EU verkauft werden		
☐	Zuständigen EU-Mitgliedstaat für CRA-Meldungen bestimmt und festgehalten		
☐	Vorfallleitung und Stellvertretung bestimmt, auch für Wochenenden		
☐	Erfassung von Entdeckungs- und Kenntniszeitpunkt mit Uhrzeit im Prozess verankert		
☐	Zugang zum BACS-Meldeformular geklärt, Pikettnummer hinterlegt		
☐	EU-Login-Konten mit Zwei-Faktor für zwei Personen angelegt		
☐	DSG-Entscheid mit drei Fragen vorbereitet: Personendaten, Verletzung, hohes Risiko		
☐	Meldepflicht des IT-Dienstleisters und der Auftragsbearbeiter vertraglich geregelt		
☐	Meldeprozess von der Geschäftsleitung freigegeben und ausserhalb der IT abgelegt		
☐	Jährliche Übung mit Szenario terminiert		

ZUR ANLEITUNG

Schritte, Beispiele, Quellen, Vorlage und KI-Skill: www.vortrieb.ch/meldepflicht-cyberangriff-schweiz/