G DATA CyberDefense

NIS-2 Sofortmaßnahmen

Merkblatt zu den dringendsten Punkten

Maßnahmen

1. Projektgruppe bilden
2. Organisatorische Maßnahmen
3. ISMS auf den Weg bringen
4. Lieferketten überprüfen
5. Cybersicherheits-Zertifizierungen
6. Meldeprozesse definieren
7. Vorbereitung auf regelmäßige Austausche
8. Registrierung beim BSI

Projektgruppe bilden

Relevante Ansprechpersonen einbinden:

- Datenschutzbeauftragte (DSB)
- IT & IT-Sicherheitsbeauftragte (IT / ITSB)
- Rechtsabteilung
- Geschäftsführung / Vorstand

Zielstellung:

Zuständige Stellen miteinander vernetzen und „auf Stand bringen“

Mittel:

Cybersicherheitstrainings für die relevanten Personen

Maßnahme 1

Organisatorische Maßnahmen

Verankerung bei Geschäftsführung bzw. Vorstand

Delegierung ist nicht zulässig!

(siehe hierzu §38 NIS2UmsuCG, Version vom 27.9.2023)

Maßnahme 2

ISMS auf den Weg bringen

Zielstellung (initial):

- Dokumentation interner IT-Strukturen
- Bedarfsermittlung für zusätzliche Anschaffungen / Dienstleistungen
- Einführung eines Informationssicherheits-Managementsystem (ISMS)

Ansprechpartner:

- IT-Leitung
- IT-Sicherheitsbeauftragte (ITSB)
- Rechtsabteilung
- Vorstand

Siehe hierzu:

ISO 27001

Teletrust-Dokument zum Stand der Technik

Nachweisdokument gemäß §8a Abs. 3 BSIG

Anforderungen an KRITIS-Betriebe (BSI)

Maßnahme 3

Lieferketten überprüfen

Fragestellung:

Welche Verbindungen zu Kunden und Zulieferern existieren, die im Zusammenhang mit IT-Sicherheit relevant sind? (eingesetzte Software und Produkte mit IT-Komponenten, auch unter Beachtung von Wartungszugängen und Open Source-Software)

Ansprechpartner:

- Vorstand
- IT(SB)
- Einkauf
- Rechtsabteilung

Zielstellung:

Identifizierung aller in Bezug auf IT-Sicherheit relevanten Lieferanten und Prüfung der Sicherheit der eingesetzten Produkte und Dienstleistungen

Siehe hierzu:

ENISA-Untersuchung

Maßnahme 4

Cybersicherheits-Zertifizierungen

Zielstellung:

Ermitteln der Relevanz von Sicherheits-Zertifizierungen für Unternehmen, die entweder Anbieter oder Käufer sicherheitsrelevanter Komponenten oder Dienstleistungen sind; im Bedarfsfall Zertifizierungsprozess einleiten oder Anbieterwechsel prüfen

Ansprechpartner:

- Vorstand
- Rechtsabteilung
- Einkauf
- Vertrieb
- ITSB

Herausforderung:

Vieles ist (Stand Januar 2024) noch ungeklärt

Hintergrund:

Potenziell dürfen NIS-2-Unternehmen keine Produkte / Dienste erwerben oder anbieten, die nicht zertifiziert sind.

Siehe hierzu: Common Criteria | ENISA

Maßnahme 5

Meldeprozesse definieren

Zielstellung:

Meldungen über relevante Vorfälle müssen innerhalb von 24 Stunden ans BSI übermittelt werden können; Folge- / Abschlussberichte erstmals nach 72 Stunden

Ansprechpartner:

- IT
- Rechtsabteilung
- DSB
- ITSB
- Vorstand

Hinweise:

- Der / die Datenschutzbeauftragte kann hier Erfahrungen aus dem eigenen Fachbereich einbringen
- Überschneidung mit BCM / Incident Response

Maßnahme 6

Vorbereitung auf regelmäßige Austausche

Zielstellung:

Das Unternehmen ertüchtigen, an einem regelmäßigen Austausch mit anderen Unternehmen sowie dem BSI teilzunehmen; hier sollen Unternehmen Erfahrungen und Threat Intelligence teilen

Ansprechpartner:

- Vorstand
- IT(SB)
- Rechtsabteilung (nach Bedarf / Möglichkeiten)

Hinweis:

Teilnahmeberechtigt am Austausch sind Unternehmen auch unbeschadet ihrer Kritikalitätsstufe!

Maßnahme 7

Registrierung beim BSI

Zielstellung:

Das Unternehmen beim BSI als wichtigen / wesentlichen Betrieb melden

Ansprechpartner:

- ITSB
- Vorstand

Hinweis:

Meldung kann auch bußgeldbewehrt durch das BSI erfolgen!

Maßnahme 8

G DATA
CyberDefense

Möchten Sie über kommende NIS-2-Webinare informiert bleiben?

Abonnieren Sie unseren Newsletter für die neuesten Termine!

Jetzt kostenlos abonnieren