Delphi

Checklista – Grundläggande säkerhets-åtgärder för att uppfylla kraven i NIS2

1. Riskhantering

- Identifiera och analysera risker: Regelbundna riskbedömningar för att identifiera hot och sårbarheter. Dokumentera bedömningarna och utse riskägare.
- Implementera riskreducerande åtgärder: Utveckla och genomför säkerhetskontroller för att hantera identifierade risker. Dokumentera åtgärder och utse ägare av genomförandet.

2. Incidenthantering

- Upprätta en incidenthanteringsplan: Säkerställ att det finns processer för att upptäcka, rapportera och åtgärda säkerhetsincidenter. Se till att inkludera gränssnitt mot leverantörer.
- Rapportering av incidenter: Incidenter som kan påverka nätverks- och informationssäkerhet ska rapporteras till MSB inom vissa bestämda tidsramar.

3. Kontinuitetsplanering

- Beredskap för affärskontinuitet: Utveckla och implementera en kontinuitetsplan för att säkerställa att verksamheten kan fortgå vid driftstörningar eller säkerhetsincidenter.
- Regelbundna tester: Genomför tester och övningar för att säkerställa att beredskapsplaner fungerar i praktiken. Dokumentera! Följ upp eventuella brister som upptäcks.

4. Säkerhet i nätverk och informationssystem

- Tekniska och organisatoriska åtgärder: Implementera brandväggar, antivirussystem, och intrusion detection systems (IDS) för att skydda informationssystem.
- Kryptering: Använd stark kryptering för att skydda känslig information i överföring och lagring.

5. Åtkomstkontroll

- Behörighetsstyrning: Se till att endast auktoriserad personal har tillgång till kritiska system och data. Tillämpa ”the principle of least privilege”. Se till att det är tydligt vem som beslutar om behörighetsnivå i organisationen. Logga och spara loggar för inloggningar.
- Autentisering: Använd flerfaktorsautentisering (MFA) för att skydda tillgång till känsliga system.

6. Leverantörssäkerhet

- Utvärdera leverantörer: Utför säkerhetsbedömningar av leverantörer och partners som har tillgång till viktiga system eller data.
- Säkerhetsavtal: Säkerställ att avtal med tredje part inkluderar krav på informationssäkerhet.

7. Säkerhetsmedvetenhet och utbildning

- Regelbunden utbildning: Genomför regelbundna säkerhetsutbildningar för ledning och anställda för att öka medvetenheten kring nätverkssäkerhet och cyberhot. Observera att utbildning för ledningen är obligatorisk.
- Simulerade attacker: Utför phishing-simuleringar, penetrationstester och andra övningar för att testa personalens beredskap.

8. Säkerhet vid förändring av system

- Säkerhetsgranskning vid systemuppdateringar: Utför säkerhetskontroller vid uppgraderingar och förändringar i IT-system för att undvika introduktion av sårbarheter.
- Dokumentation av förändringar: Håll detaljerad dokumentation över systemändringar och uppdateringar. Försäkra er om att det finns möjlighet att återställa till tidigare läge om ändringen inte lyckas.

9. Efterlevnad och uppföljning

- Regelbunden revision: Utför interna och externa granskningar för att säkerställa att säkerhetsåtgärderna uppfyller NIS2-kraven. ISO 27001 är en bra utgångspunkt.
- Rapportering till tillsynsmyndigheter: Verksamheter ska ha mekanismer för att informera tillsynsmyndigheter om säkerhetsåtgärder och efterlevnad.

10. Sårbarhetshantering

- Patchhantering: Säkerställ att alla system är uppdaterade med de senaste säkerhetspatcharna.
- Övervakning och upptäckt av hot: Implementera övervakningssystem för att upptäcka och agera på potentiella hot i realtid.

Observera att denna sammanställning inte är uttömmande. Checklistan syftar till att ge en översikt över centrala aspekter och ska inte betraktas som fullständig rådgivning.