NIS2-tjekliste: Hold styr på din compliance-fremgang

Brug denne NIS2-tjekliste til at holde styr på jeres compliance-fremgang. Den hjælper jer med at se, hvad I allerede har på plads, hvad der mangler, og hvor I skal sætte ind næste gang.

Print den, del den med dine kolleger, eller brug den som et arbejdsdokument, mens I bevæger jer gennem jeres NIS2-implementering.

Governance

- [ ] Sørg for, at ledelsen definerer virksomhedens mål og risikoappetit.
- [ ] Sørg for, at jeres NIS2-compliance-framework understøtter virksomhedens mål.
- [ ] Involvér relevante interessenter, afstem forventninger, og hold alle med interesse i virksomhedens drift og NIS2-compliance løbende opdateret.
- [ ] Udpeg ansvarsområder for compliance i virksomheden.
- [ ] Sørg for, at ledelsen fører tilsyn med og giver grønt lys til implementeringen af cybersikkerhedsforanstaltninger.
- [ ] Planlæg en løbende gennemgang af frameworket.
- [ ] Benyt indsigter fra tidligere compliance-initiativer på andre områder.

Sikkerhed

- [ ] Sørg for, at sikkerhedsniveauerne er passende og proportionale i forhold til at håndtere de relevante risici.
- [ ] Sørg for, at ledelsen og relevante medarbejdere gennemfører den påkrævede cybersikkerhedstræning.
- [ ] Sørg for, at følgende minimumforanstaltninger bliver implementeret (læs mere i den danske NIS2-vejledning):

    - Politikker for risikoanalyse og sikkerhed i informationssystemer.
    - Håndtering af hændelser.
    - Forretningskontinuitet, såsom backup-styring og disaster recovery, samt krisehåndtering.

- Sikkerhed i forsyningskæden, herunder sikkerhedsrelaterede aspekter i forholdet mellem hver enhed og dens direkte leverandører eller serviceudbydere.
- Sikkerhed i forbindelse med anskaffelse, udvikling og vedligeholdelse af netværk og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder.
- Politikker og procedurer til vurdering af effektiviteten af risikostyringsforanstaltninger for cybersikkerhed.
- Grundlæggende cyberhygiejne og cybersikkerhedstræning.
- Politikker og procedurer for brug af kryptografi og, hvor det er relevant, kryptering.
- Human resources-sikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.
- Brug af multifaktorautentificering eller løbende autentificeringsløsninger, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer i virksomheden, hvor det er relevant.

Rapportering og kommunikation

- [ ] Vær i stand til at opdage hændelser og analysere deres samlede indvirkning.
- [ ] Vurdér, om hændelser er væsentlige i henhold til NIS2.
- [ ] Rapportér væsentlige hændelser til relevante myndigheder.
- [ ] Kommunikér væsentlige hændelser til modtagere af dine tjenester.
- [ ] Overhold krav til indhold og rapporteringsfrister.

Dokumentation

- [ ] Dokumentér jeres governance-proces, beslutninger og compliance-indsats undervejs.
- [ ] Overvej at følge et ISMS, fx baseret på ISO/IEC 27001:2022 for at sætte din cybersikkerhed i system.
- [ ] Automatisér så meget af processen som muligt.

Har du brug for en mere struktureret måde at arbejde med NIS2 på? Hvis du vil gå fra tjekliste til løbende compliance, kan vores eksperter hjælpe dig med at **etablere et praktisk NIS2-workflow, der holder styr på opgaver, dokumentation og opfølgning.**

Ja tak til en ekspert-snak