NIS2-direktivet

Governance

Hvad er governance?

Betegnelsen *governance* eller *IT-styring* i NIS2 refererer til den proces, hvormed virksomheder bliver ledet, styret og administreret for at opnå deres mål. Det omfatter de strukturer, politikker, procedurer og praksisser, der skal være på plads for at sikre, at virksomheden fungerer effektivt, overholder lovgivningen og opretholder et højt niveau af ansvarlighed over for sine interessenter. NIS2-direktivet kræver en solid integration både i virksomhedens ledelse og i den daglige drift.

I NIS2-direktivet er det ledelsens ansvar, at der etableres passende strategier, politikker og ressourcer til at beskytte organisationens netværk og informationssystemer. Dette opnås ved udarbejdelse og implementering af IT-strategier ud fra en lang række obligatoriske dokumenter. Dokumenterne bør udarbejdes i henhold til kendte IT-sikkerhedsstandarder som CISv8, ISO27001 og IEC62443.

NIS2 dokumentationsbehov

På de kommende sider, vil vi gennemgå de nødvendige dokumenter, der skal udarbejdes i forbindelse med en NIS2-revision. Dette er en omfattende opgave, der kræver betydelige ressourcer. Derfor har TD-K A/S udviklet en intuitiv dokumentationsplatform, der indeholder skabeloner til alle relevante NIS2-dokumenter. Virksomheden kan selv udfylde skabelonerne, eller TD-K A/S kan bistå med denne opgave. Med TD-K A/S dokumentationsplatform kan virksomheden samle, organisere og administrere al NIS2-relateret dokumentation ét centralt sted.

Dokumenter

Sikkerhedspolitik

Sikkerhedspolitikken indeholder ledelsens krav til IT-sikkerheden, gyldighedsområde og hvilke mål IT-sikkerheden skal opfylde.

Sikkerhedshåndbog

Sikkerhedshåndbogen er et centralt dokument og udmønter IT-sikkerhedspolitikken i konkrete forskrifter, retningslinjer og krav til IT-installationens konfiguration, drift og anvendelse, som fx:

- IT-sikkerhedsorganisation, roller og ansvar
- Retningslinjer for brug af IT i virksomheden
- Sikkerhedsforskrifter og krav til systemer og netværk
- Datakategorisering fx personligt, fortroligt, internt og ingen
- Backup-krav ud fra forretningsmæssige behov
- Krav til logning ud fra lovgivning og forretningsbehov
- Krav og forskrifter til systemopdateringer
- Uddannelse af medarbejdere i IT-sikkerhed

Risikopolitik

Virksomheden skal definere, hvordan risici håndteres, hvor store risici er man villig til at tage og hvor store tab er man villig til at acceptere økonomisk og/eller i omdømme.

Sårbarhedsanalyse

Sårbarhedsanalysen er en teknisk gennemgang af IT-installationen for kendte sårbarheder. Dette udføres med automatiske værktøjer, eksporteres fra Compliance Manageren.

Risikovurdering

Ledelsen skal gennemføre risikovurdering på alle kritiske IT-systemer i forhold til alle relevante trusler og sårbarheder samt rangere dem i forhold til sandsynlighed og konsekvens.

Risikohandlingsplan

Dette dokument indeholder en plan for konkrete tiltag, for at mindske de risici det er besluttet at agere på i risikovurderingen. Der anføres tidsramme, budget, løsning og ansvar for hver risiko.

Beredskabsstrategi

I beredskabsstrategien definerer ledelsen, med udgangspunkt i risikovurderingen, kravene til et IT-beredskab, blandt andet ud fra hvor længe virksomheden kan undvære en given IT-funktion og hvor mange data man kan tåle at miste. Antagelser fastlægges og målsætninger defineres.

Beredskabsplan

Dette er den konkrete plan for indsatsen ved en IT-katastrofe eller et cyberangreb, indeholdende alle detailprocedurer samt rolle-/ansvarsfordelinger.

Leverandørpolitik

Dette dokument beskriver de krav, virksomheden stiller til sine leverandører inkl. sikkerhedskrav, sårbarhed og afhjælpning af forsyningskædesvigt.

Sikkerhedskrav til applikationer

Her defineres hvilke sikkerhedsmæssige minimumskrav virksomheden skal stille ved anskaffelse af applikationer.

Personalehåndbog

Personalehåndbogen skal tilrettes så der fremgår krav til overholdelse af IT-sikkerhed og fortrolighed samt krav til deltagelse i IT-sikkerhedsuddannelse.

Ansættelseskontrakter

Ansættelseskontrakter skal ligeledes tilrettes, så det fremgår tydeligt, at medarbejderen er underlagt fortrolighed og skal overholde retningslinjer for anvendelse af IT i virksomheden.

Procedurer

Det er nødvendigt at etablere og dokumentere en række procedurer til sikring af det definerede IT-sikkerhedsniveau, som minimum følgende:

Håndtering- og anmeldelse af sikkerhedshændelser

Procedure inkl. roller og ansvar, kriterier, kontaktlister og kommunikationsplan.

Ansættelsesprocedure

Procedure hvor det fremgår at medarbejderen introduceres til sikkerhedsforskrifter og uddannelse i IT-sikkerhed.

Afskedigelsesprocedure

Proceduren skal som minimum indeholde orientering om at fortsat fortrolighed er gældende.

Godkendelsesprocedure

Der skal være defineret godkendelsesprocedurer for systemændringer, oprettelse af IT-adgange og tildeling af rettigheder.

Procedure for sletning af data

Der skal være defineret en procedure for sletning af data på en sikker måde.

Procedure for løbende uddannelse af medarbejdere i IT-sikkerhed

Der skal være defineret procedure for løbende træning og videreuddannelse af medarbejdere i IT-sikkerhed.

Registre

Der skal forefindes en række registre (ofte indeholdt i forskellige IT administrationsværktøjer), som giver et overblik over IT-landskabet, bidragsydere til IT-driften, systemadgange og rettigheder mm:

Configuration Management Database (CMDB)

Et samlet arkiv over alle hardware- og software enheder samt data aktiver inkl. ejerskab og ansvar.

Leverandørregister

Register over alle vigtige leverandører inkl. kontrakter, kontaktpersoner og serviceaftaler.

Risikoregister

Risikoregisteret er resultatet af risikovurderingen indeholdende alle identificerede risici samt deres sandsynlighed og konsekvens.

Brugeradgange

Register over alle brugeradgange til alle applikationer inkl. begrundelse for adgang.

Kontaktliste for hændelsesstyring

Liste over alle interne og eksterne kontaktpersoner/kontaktpunkter til brug ved reaktion på en hændelse.

Årshjul

Årshjulet er en rullende kalender med aktiviteter der skal udføres periodisk. Årshjulet skal indeholde alle nødvendige aktiviteter for vedligeholdelse af hele IT-sikkerhedsstyringen, fx:

- Risikovurdering opdateres
- Sårbarhedsanalyse opdateres
- Beredskabsplaner opdateres og afprøves
- Behov for logning opdateres
- Test og opdatering af proces for anmeldelse og håndtering af hændelser
- Vurdering af serviceleverandører og leverandøradgange
- Revision af brugeradgange
- Revision af sikkerhedspolitik
- Sikkerhedshåndbog revideres

Hovedkontor

Rugbjergvej 10, 4623 Lille Skensved

Afdeling Sydsjælland

Køgevej 18, 4700 Næstved

Afdeling Vestsjælland

Norvangen 3D, 4220 Korsør

Afdeling Jylland

Hjulmagervej 4A, 7100 Vejle

Telefon
+45 70 26 69 00

Mail
info@td-k.dk