Ministeriet for Samfundssikkerhed og Beredskab

Dato: 26-02-2025
Sagsnr.: 2025 - 227
Akt-id.: 1874

NOTAT: KRAV TIL FORANSTALTNINGER I FORSLAG TIL LOV OM FORANSTALTNINGER TIL SIKRING AF ET HØJT CYBERSIKKERHEDSNIVEAU (NIS 2-LOVEN)

Foranstaltninger til styring af cybersikkerhedsrisici

Forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) forpligter væsentlige og vigtige enheder til at træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester.

Foranstaltningerne skal stå i passende forhold til graden af de væsentlige eller vigtige enheders risikoeksponering og til den samfundsmæssige og økonomiske indvirkning, som en hændelse ville have. Der vil således være tale om en konkret vurdering af enhedens samfundskritikalitet.

Lovforslaget tager udgangspunkt i en risikostyring, der omfatter alle farer (all-hazards approach). Det betyder, at enhederne skal tage højde for alle de trusler, som enhederne er udsat for, og de sårbarheder, enhederne har. Sårbarhederne kan f.eks. bestå i tekniske og menneskelige fejl, miljømæssige påvirkninger (eksempelvis skybrud m.v.) og direkte bevidste handlinger (eksempelvis angreb fra hackere).

Det bemærkes, at den kompetente myndighed som led i sin generelle vejledningsforpligtelse over for enheder vil kunne yde vejledning til omfattede enheder vedrørende foranstaltninger. Der vil derudover blive udarbejdet vejledningsmateriale om bl.a. krav til foranstaltninger, som vil foreligge senest samtidig med lovens forventede ikrafttræden.

Foranstaltningerne skal ifølge lovforslaget som minimum omfatte 10 foranstaltninger, som vil blive uddybet nærmere i det følgende.

1. Politikker for risikoanalyse og informationssystemsikkerhed
Enheder skal bl.a. udarbejde en politik for informationssikkerhed, der fastlægger den overordnede ramme for implementering af foranstaltninger, som understøtter sikkerheden i enhedens net- og informationssystemer. Enheder skal endvidere udarbejde en politik for risikostyring, som indeholder metoder til at identificere og adressere eventuelle risici.

En politik for informationssikkerhed skal være passende i forhold til enhedens forretningsmæssige mål – altså understøtte enhedens kerneaktiviteter og tage højde for de risici, der er relevante for enheden. Politikken kan eksempelvis indeholde:

- Målsætninger for net- og informationssikkerhed – dvs. beskrivelser af, hvad enheden ønsker at opnå med sin cyber- og informationssikkerhed.
- En forpligtelse til at opfylde passende krav i relation til net- og informationssikkerhed.
- En forpligtelse til forsat forbedring af informationssikkerhedspolitikken.

2. Håndtering af hændelser
Enheder skal bl.a. udarbejde procedurer for håndtering af hændelser. Enheder skal i den forbindelse i fornødent omfang implementere logning og monitorering af uregelmæssigheder i enhedens net- og informationssystemer med henblik på at kunne identificere hændelser. Logdata skal derudover sikres mod manipulation og beskyttes mod uautoriseret adgang.

En procedure for håndtering af hændelser kan eksempelvis indeholde:

- Roller og ansvar for håndteringen af hændelser i enheden.
- Processer til at vurdere mistænkelige hændelser for at afgøre, om der er tale om net- og informationssikkerhedshændelser.
- Processer for, hvordan hændelser skal håndteres i enheden,

- Processer, der gør det muligt for medarbejdere, leverandører og kunder at indberette mistænkelige hændelser.

3. Driftskontinuitet, herunder backup-styring og reetablering efter en katastrofe og krisestyring
Enheder skal bl.a. udarbejde procedurer til sikring af driftskontinuitet i tilfælde af en hændelse. På grundlag af enhedernes risikostyring og driftskontinuitets-procedure, skal enheder således udarbejde procedurer for backupstyring og gendannelse af data. Enheder skal foretage en vurdering af behovet for at udarbejde en beredskabsplan for krisestyring og reetablering efter en katastrofe. Enheder skal foretage en vurdering af, om der er behov for at etablere redundans, nødstrømsforsyning, understøttende forsyning eller anden sikring med tilsvarende virkning for enhedens net- og informationssystemer.

Enheder kan i den forbindelse eksempelvis udarbejde og vedligeholde en kontinuitetsplan og en plan for genopretning efter en krise for at kunne agere i tilfælde af en sikkerhedshændelse. Enhedens drift skal kunne genoprettes i overensstemmelse med kontinuitetsplanen. Planen bør baseres på resultaterne af risikovurderingsprocesser og kan eksempelvis indeholde:

- Formål, omfang og målgruppe for planen.
- Roller og ansvar i tilfælde af en krise.
- Nøglekontakter (interne og eksterne) og kommunikationskanaler, der kan anvendes.
- Betingelser for aktivering og deaktivering af enhedens beredskab.
- Genoprettelsesplaner for specifikke driftssystemer og genopretningsmål.
- En beskrivelse af de nødvendige ressourcer inklusive backup og redundans, der skal til for at sikre driften i en krisesituation.
- Genopretning og genstart af aktiviteter ved hjælp af midlertidige foranstaltninger.

4. Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere
Enheder skal bl.a. udarbejde procedurer for leverandørstyring for at sikre passende forsyningskædesikkerhed. Enheder skal i den forbindelse tage hensyn til de sårbarheder, der er specifikke for hver direkte leverandør og tjenesteudbyder, og den generelle kvalitet af deres leverandørers og tjenesteudbyderes produkter og cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer.

Procedurerne bør endvidere tage højde for sikkerhedsrelaterede aspekter vedrørende forholdet mellem enheden og dens direkte leverandører og tjenesteudbydere relateret til enhedens net- og informationssystemer. Enheder skal i den forbindelse bl.a. udarbejde procedurer for aftaleindgåelse med direkte leverandører og tjenesteudbydere af produkter og tjenester, der kan påvirke sikkerheden i enhedens net -og informationssystemer.

5. Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder
Enheder skal bl.a. udarbejde procedurer for sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af enhedens net- og informationssystemer, med udgangspunkt i politikken for informationssystemsikkerhed.

Enheder skal endvidere udarbejde procedurer for håndtering af sårbarheder, der kan have indvirkning på enhedens net- og i formationssystemer.

6. Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici
Enheder skal bl.a. udarbejde en politik og procedurer med henblik på at vurdere effektiviteten af de implementerede foranstaltninger samt for vurdering af behov for tekniske tests for potentielle sårbarheder, herunder f.eks. i form af sårbarheds-scanninger eller penetrationstests.

7. Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse

Enheder skal bl.a. implementere relevante grundlæggende cyberhygiejnepraksisser med udgangspunkt i deres politik for informationssikkerhed, herunder f.eks. gennem brug af passwords og sikker brug af e-mails.

Endvidere skal enheder udarbejde en politik for uddannelse af relevante medarbejdere for at sikre, at medarbejderne har relevant viden og færdigheder om informationssikkerhed.

8. Politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering
Enheder skal bl.a. udarbejde en politik og procedurer for brug af kryptografi og, hvor det er relevant, kryptering for at beskytte deres net- og informationssystemer.
Kryptografi anvendes bl.a. til transformation af data med det formål at skjule oplysninger for uvedkommende.

Politikken og procedurerne skal være passende i forhold til det aktuelle teknologiske stade.

9. Personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver
Enhederne skal implementere foranstaltninger til personalesikkerhed, der skal sikre, at den enkelte medarbejder forstår, udviser og forpligter sig til at leve op til deres ansvar for informationssikkerhed.

Enheder skal derudover udarbejde en politik for adgangskontrol for at beskytte mod uautoriseret adgang til enhedens net- og informationssystemer. Politikken skal som minimum identificere og vurdere risici i forhold til logisk og fysisk adgangskontrol og indeholde procedurer for styring af adgangsrettigheder.

Enheder skal fastlægge, hvordan den forvalter aktiver, der vil kunne påvirke sikkerheden i enhedens net- og informationssystemer.

Enheden kan i den forbindelse eksempelvis vælge at implementere en formel procedure for, hvordan brugere tildeles adgang til de forskellige systemer og netværksdrev i enheden. Proceduren kan eksempelvis indeholde regler for:

- Hvem der kan ansøge om adgang.

- Hvem der kan godkende, at adgang bliver givet.
- Hvem der praktisk giver adgang i enhedens system til styring af adgange til deres net- og informationssystemer.

10. Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt hos enheden, hvor det er relevant

Enheder skal anvende multifaktorautentifikation eller kontinuerlig autentifikation ved adgang til net- og informationssystemer i overensstemmelse med enhedens politik for adgangskontrol.

Enheden kan i den forbindelse eksempelvis vælge, at der skal anvendes multifaktorautentificering, når medarbejdere og eventuelt andre skal have fjernadgang til enhedens netværk. Det vil sige, at når en bruger logger sig på netværket hjemmefra bliver vedkommende bedt om en ekstra kode, som bliver sendt til dennes mobiltelefon.

Enheder skal endvidere anvende sikret tale-, video- og tekstkommunikation i overensstemmelse med politikken for brug af kryptografi og kryptering og under hensyntagen til kommunikationsmidlernes tilgængelighed, også i en nødsituation.

Sikret kommunikation kan eksempelvis være krypterede platforme, der beskytter samtaler og datadeling mod aflytning og manipulation. Endelig kan nødkommunikationssystemer sikre, at kommunikationen kan fortsætte, selv under et cyberangreb eller systemnedbrud. Disse løsninger er designet til at være robuste og fungere uafhængigt af andre teknologier. Det kan desuden indebære, at visse nøglemedarbejdere skal være udstyret med satellittelefon.