NYT EU-DIREKTIV SKÆRPER KRAVET TIL CYBERSIKKERHED

Det nye NIS2-direktiv fra EU er trådt i kraft. Det skærper kravene til cyber- og informationssikkerhed og kræver en helhedsorienteret og risikobaseret tilgang for danske virksomheder. Flere virksomheder vil nu blive betragtet som kritisk infrastruktur i kraft af deres rolle som underleverandører.

DBI
BRAND OG SIKRING

Cyberangrebet på en række danske banker og Nationalbanken i januar var en aktuel understregning af nødvendigheden af EU's opdatering af NIS-direktivet for cyber- og informationssikkerhed. Meget tyder på, at det var den prorussiske hackergruppe Killnet, der gennemførte angrebet, hvilket stemmer overens med den øgede cybertrussel pga. krigen i Ukraine.

- Det oprindelige NIS-direktiv var vagt formuleret, og derfor er der stor forskel på, hvordan det er blevet implementeret i de enkelte medlemslande. Det nye NIS2, der trådte i kraft i Danmark i januar, stiller meget strengere krav og er et ønske om at standardisere cyber- og informationssikkerheden på tværs af EU-landene, siger Andreas Norstedt, som er sikkerhedsrådgiver hos DBI.

Både NIS og NIS2 er rettet mod sektorer med kritisk infrastruktur, men med NIS2 udvides kravet til at gælde flere sektorer samt de påvirkede virksomheders underleverandører.

- Det vil f.eks. sige, at en virksomhed, der producerer kabler til energisektoren, også skal leve op til NIS2, forklarer Andreas Norstedt.

Helhedsorienteret tilgang

Direktivet lægger op til, at virksomheder med flere end 50 ansatte og en årlig omsætning på 10 mio. euro eller en årlig balance på 43 mio. euro skal efterleve kravene, og det vil være virksomhedernes ledelse, som skal godkende sikkerhedsforanstaltningerne og sikre egenkontrollen af dem.

- Mange af dem får travlt, for foranstaltningerne skal være implementeret senest i oktober 2024 jf. dansk lovgivning. De fleste danske virksomheder har godt styr på it-sikkerheden, men som noget nyt kræver NIS2 en risikobaseret tilgang til cyber- og informationssikkerhed. Det vil sige, at der også skal foretages en risikovurdering, udarbejdes en beredskabsplan og være styr på de fysiske omgivelser. En helhedsorienteret tilgang betyder, at et energiselskab skal have en plan for at kunne fortsætte med at levere strøm, uanset om det er et cyberangreb eller en oversvømmelse i serverrummet, der kompromitterer cyber- og informationssikkerheden, eksemplificerer Andreas Norstedt.

Bøder så store som GDPR

I 2025 skal de relevante tilsynsmyndigheder begynde at føre tilsyn med, om de virksomheder, der er omfattet af NIS2, lever op til kravene.

- Tilsynsmyndighederne får vidtgående beføjelser – herunder adgang til data, dokumenter og oplysninger om f.eks. risikovurderinger og implementering af foranstaltninger. Viser det sig, at en virksomhed ikke lever op

til NIS2, kan det give en stor bøde. EU har skelet til bødestørrelserne på overtrædelser af GDPR, så der kan blive tale om bøder på op til 10 mio. euro eller 2 % af virksomhedens globale omsætning, siger Andreas Norstedt.

Fakta om NIS2

EU's NIS2-direktiv stiller minimumskrav til:

- Forebyggelse (risikoanalyser, udvikling af politikker og beredskasplaner)
- Håndtering af hændelser (detektion og reaktion)
- Krisestyring og driftskontinuitet
- Forsyningskædesikkerhed
- Sikkerhed ved anskaffelse, udvikling og vedligeholdelse af netværks- og informationssystemer
- Politik og procedure for vurdering af effekten af foranstaltninger til styring af risici
- "Cyberhygiejne" og uddannelse i cybersikkerhed
- Politik og procedure for kryptering
- Sikkerhed for menneskelige ressourcer, politik for adgangskontrol og styring af aktiver
- Multifaktorautentificering eller kontinuerlige autentificering-sløsninger, sikker tale-, video- og tekstkommunikation og sikre nød-kommunikationssystemer

Sektorer, som ifølge direktivet er omfattet af NIS2:

- Affaldshåndtering
- Digital infrastruktur
- Digitale udbydere
- Drikkevand
- Energi
- Finans
- Finansiel markedsinfrastruktur
- Forskning
- Fremstilling af elektroniske produkter, maskiner og køretøjer
- Fremstilling, produktion og distribution af kemikalier
- Informations- og kommunikationsteknologi
- Offentlig forvaltning
- Post- og kurertjenester
- Produktion, forarbejdning og distribution af fødevarer
- Rummet
- Spildevand
- Sundhed
- Transport

Kilde: NIS2

Business Continuity Management

Det er ikke nok at beskytte sig med et hegn. Man skal også vide, hvad man gør, hvis hegnet bliver forceret, og skaden sker. Det er – billedligt talt – essensen i den nye, holistiske tilgang til cyber- og informationssikkerhed, som NIS2 lægger for dagen. Det handler om Business Continuity Management, og inden for det felt tilbyder DBI:

- Risikoanalyse
- GAP-analyse
- Business Impact-analyse
- Udarbejdelse af rammer for informationssikkerhedspolitikker, herunder krisehåndtering og krisekommunikation
- Udarbejdelse af beredskabsplaner
- Udarbejdelse af Business Continuity-planer (BCP)
- Recovery-planer
- Træning af medarbejdere
- Krisestyringsøvelser