NIS2 NÆRMER SIG: ER DIN VIRKSOMHED KLAR?

17. oktober skal virksomheder have implementeret NIS2, som skærper kravene til cyber- og informationssikkerhed. Frem til deadlinen bringer DBI en serie artikler om, hvordan danske virksomheder kan imødekomme de nye krav. Her giver DBI's sikkerhedsrådgivere Andreas P. Norstedt og Matilde Møller Christensen gode råd om politikker vedr. risikoanalyse og informationssikkerhed.

DBI
BRAND OG SIKRING

Hvad går politikker vedr. risikoanalyse og informationssikkerhed ud på?

- Generelt handler en politik i en virksomhed om at fastlægge rammer for, hvordan både ledelse og medarbejdere skal arbejde med et givent område – i det her tilfælde informationssikkerhed og risikostyring. Politikken er på et strategisk niveau og er forudsætningen for det operationelle niveau.

Politikken er skelettet, hvor man siger, hvorfor man vil forholde sig til informationssikkerhed, hvordan man vil gøre det, hvilket niveau man sigter mod, hvilke ressourcer man har til det osv. På det skelet hægter man så de planer, man udarbejder efterfølgende, bl.a. sin beredskabsplan.

Desuden kan politikken være med til at skabe en sikkerhedskultur – eller ændre en eksisterende – fordi den beskriver, hvordan man forventer, at medarbejderne agerer på området.

Hvorfor er det en del af NIS2?

- Dels ønsker man at skabe en standardiseret fremgangsmåde og rød tråd hele vejen fra EU-niveau til lande-niveau til den enkelte virksomhed. Dels sikrer det, at virksomhederne starter arbejdet med NIS2 i den rigtige rækkefølge. Det er rigtigt svært at implementere informationssikkerhed og risikostyring, hvis ikke der er taget beslutninger om, hvordan man kan gøre det.

Hvad er en god fremgangsmåde?

- Hvis man som virksomhed er helt grøn på området, anbefaler vi at starte med at få foretaget en risikovurdering for at identificere mulige trusler og risici forbundet med cyber- og informationssikkerhed. For det kan være svært at lave en politik for området, hvis man ikke kender disse risici. Har man derimod erfaring med området, kan man godt starte med at udarbejde sin politik og foretage risikovurderingen efterfølgende. Man kan også inddrage de trusselvurderinger, som Center for Cybersikkerhed udarbejder og opdaterer løbende.

Derudover kan man med fordel anvende standarder som ISO27001 til at strukturere politikken, ligesom man bør kortlægge, hvad der er realistisk. F.eks. nytter det ikke, at man som virksomhed vil implementere en masse kontroller, hvis man i praksis ikke har ressourcer til at udføre dem.

Arbejdsgruppen bør være sammensat af relevante fagpersoner og områdeansvarlige, som kan give et helhedsorienteret perspektiv på muligheder og begrænsninger. Og så er det ekstremt vigtigt, at man har opbakning fra ledelsen, da det ellers bliver svært at udarbejde og forankre en politik.

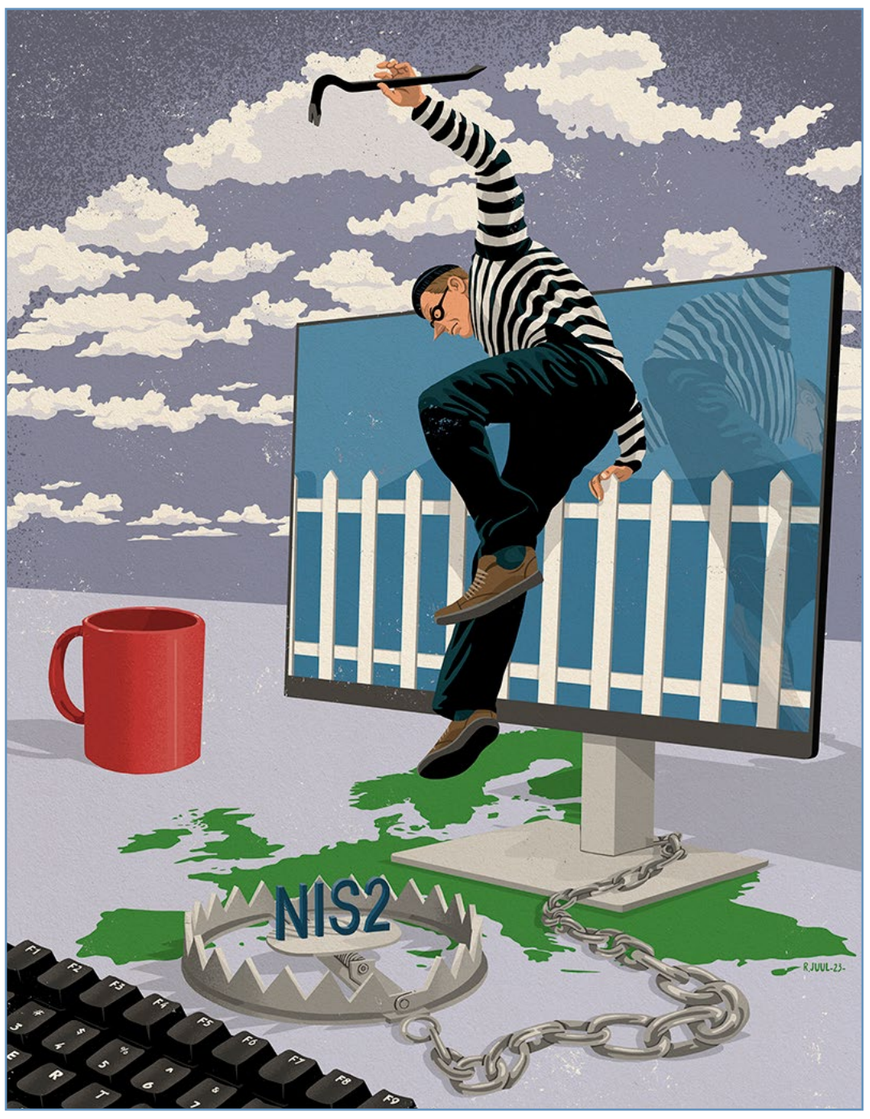

Illustration af Rasmus Juul Pedersen

Hvad er forskellen på en risikovurdering og en risikoanalyse?

- Risikoanalysen er en del af risikovurderingen. Når man har lavet en risikovurdering, har man taget stilling til, hvilke risici man vil analysere, og hvordan man vil analysere dem – f.eks. deres sandsynlighed og konsekvens. Og man har evalueret de forskellige risici i forhold til hinanden, og hvilke man skal tage udgangspunkt i i politikken.

Hvad skal man have med i sin politik?

- På sikkerdigital.dk er der en vejledning i informationssikkerhedspolitik. Politikken bør have en indledning, som definerer formål, målsætning, og hvem den gælder for, ligesom den bør tage stilling til roller og ansvar – både internt og eksternt. Den skal forankre informationssikkerheden i virksomheden, så alle ved, hvordan de skal forholde sig til den – herunder også awareness-træning af medarbejderne.

Den bør etablere klare retningslinjer for adgangskontrol, dataklassifikation, fysisk sikring, beredskab, anskaffelse af udstyr etc. – virksomhedens kontekst definerer, hvad der er relevant. Og den bør tage stilling til, hvordan man håndterer sikkerhedsbrud og rapporterer dem internt og til myndigheder.

Er der "faldgruber", man bør være opmærksom på?

- Det er fint at lade sig inspirere af en skabelon som vejledningen på sikkerdigital.dk. Man bør bare huske på, at politikkerne skal tage udgangspunkt i ens egen virksomhed. Man kan ikke kopiere en anden virksomheds politikker. Det handler ikke mindst om niveauet. Man bliver nødt til at være realistisk i forhold til, hvad man kan føre ud i livet.

Derudover skal man passe på med ikke at gøre politikken kompleks. Den skal selvfølgelig leve op til myndighedernes minimumskrav, men hvis den bliver for lang og omfattende, risikerer man at miste overblikket og dermed forankringen i virksomheden.

Desuden er det vigtigt, at man ikke stopper, når politikken er udarbejdet. Der bør være en person, som løbende rapporterer til ledelsen, hvordan det går, og som løbende sikrer, at virksomheden lever op til de krav og også dokumenterer det, som tilsynsmyndigheden kommer og tjekker.

Samtidig bør man huske at få den menneskelige faktor med i politikken. Man kommer nemt til at fokusere på systemer og glemmer, at ca. 90 % af alle cybersikkerhedshændelser sker pga. menneskelige fejl.

Sidst, men ikke mindst er det supervigtigt, at man løbende opdaterer sin politik. Hvis den havner i skuffen, går der ikke lang tid, før den kan være utidssvarende pga. teknologiudvikling og ændret trusselbillede.