

NIS2 i praksis En erfaringsbaseret tilgang

Lisbeth Loft, Globeteam
21.08.2024

Lisbeth Loft, PhD.

Jeg er seniorrådgiver for Risk & Security i Globeteam. Min baggrund er fra anvendt forskning, og jeg har i mange år arbejdet på tværs af landegrænser og tilbragt en stor del af mit liv i USA. For nogle år siden forelskede jeg mig i en lille landsby i Hedehusene og flyttede fra New York dertil. I dag bor jeg fast i Danmark, men har bibeholdt lidt af det internationale og er for eksempel stadig ekspertrådgiver for EU-Kommissionen.

Jeg har en passion for data og mennesker. Min vej ind i it-sikkerhed går gennem en kombination af sociologiens forståelse for menneskers adfærd kombineret med det, man i dag vil kalde data science. Min interesse er faktisk så stor, at jeg har en doktorgrad inden for hvert område. Man skal forstå værdien af sine egne og hinandens data, informationer og viden og passe på dem. Forankring af it-sikkerhed lykkes ved at skabe en forståelse for, hvorfor vi som mennesker gør, som vi gør.

I dag skal jeg fortælle om, hvordan man konkret kan gribe arbejdet med NIS2 an. Jeg har erfaring med den praktiske implementering af NIS2 i kritisk infrastruktur, som for eksempel forsyningsbranchen, og det er den erfaring, jeg vil trække på i dag. Desuden har jeg arbejdet med fx transportsektoren, regionerne, forskellige offentlige myndigheder, større private virksomheder, universitetsverdenen, fagforeninger og a-kasser mv.

GLOBETEAM

Lisbeth Loft

lil@globeteam.com
Mobile +45 2680 1415



integritet · relationer · kompetencer
www.globeteam.com

Program

1. Den risikobaserede tilgang omsat til virkelighed
2. Godt fra start – nødvendige indledende overvejelser
3. Gap-analyse
4. Implementering – trin for trin
5. Erfaringer - udfordringer og gevinster

Den risikobaserede tilgang omsat til virkelighed

Proportionalitet

- Sikre, at I får mest mulig sikkerhed for de tilgængelige ressourcer.

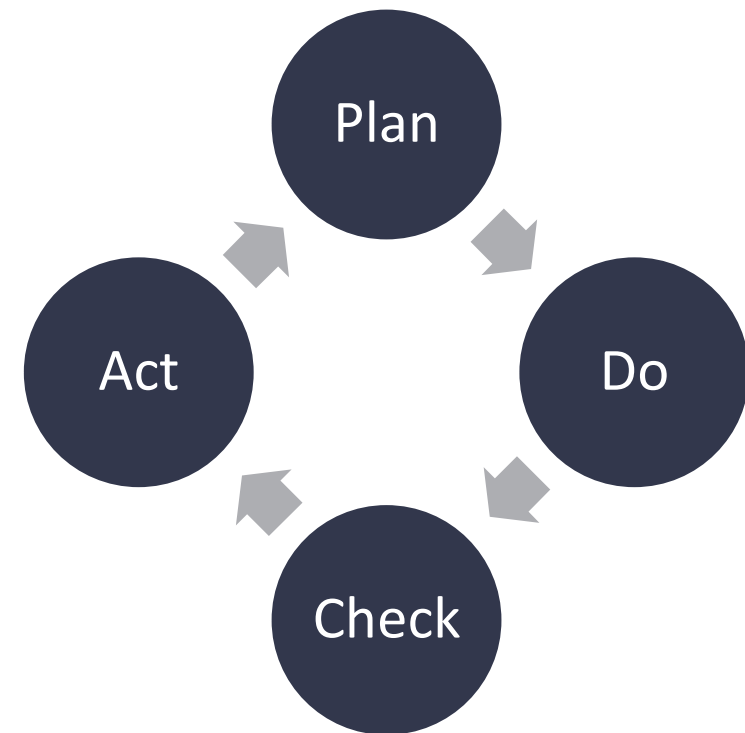
Identificer, vurder og forstå jeres risici

- Hertil skal I bl.a. have en risikostyringsmodel, en risikovurderingsmetode og et risikoregister.

Prioriter og håndter

- Når I har model, metode og register på plads, har I mulighed for at prioritere og dermed arbejde aktivt med mitigerende af jeres risici.
- Adopter en plan-do-check-act tilgang.
- Løbende rapportering til ledelsen.

Forudsætningen for en succesfuld risikostyring er altid kendskab og forståelse hos ledelsen



— Godt fra start – nødvendige indledende overvejelser

Organisatorisk forankring

- Sikre opbakning fra ledelsen: IT-sikkerhed skal altid understøtte strategiske målsætninger.
- Etabler en tværfaglig arbejdsgruppe.

Forståelse for NIS2

- Afsøg viden og erfaringer. Dyk ned i NIS2-direktivet og forstå de specifikke krav og deres formål. Diskuter og søg sparring og vejledning.

Identificer relevante interne interessenter

- Identificer jeres relevante interne interessenter, fx ledelsen, IT-afdelingen, GRC-teamet, juridisk team mv.

Kortlæg jeres vigtige og væsentlige tjenester fra et NIS2-perspektiv

- Hvilke tjenester leverer I, som ifølge NIS2 er vigtige eller væsentlige? Hvilke understøttende processer, systemer/løsninger, afdelinger/enheder og leverandører findes der? Det er der, I skal starte.



Gap-analyse



Gap-analyse

Hvorfor en Gap-analyse

- Undgå over- eller underimplementering
- Organiser og prioriter jeres tiltag og baser jeres beslutninger på praktiske indsigter fra jeres egen organisation
- Få interne interessenter ombord allerede tidligt i forløbet



Gap-analyse

Gap-analysens indhold

- Identifikation af tværgående, overordnede udfordringer.
- Måling af NIS2-modenhed
- Beskrivelse af identificerede gaps
- anbefalinger til udbedringsinitiativer
- Konkrete, praksisorienterede og detaljerede beskrivelser af de anbefalede initiativer, inkl. estimering af ressourceforbrug
- Forslag til implementeringsprogram.
- Forslag til fremadrettet governance-struktur (NIS2 skal driftes!)



Implementering – trin for trin



Implementering - trin for trin



— Implementering - trin for trin

Godkendelse

Gennemgang og afstemning med
forretningsmål

Ledelsens godkendelse af
initiativer inkl. resurseallokering

— Implementering - trin for trin

Projekter

Operationalisering af
projektplaner baseret på
besluttete initiativer.

— Implementering - trin for trin

Organisering

Organisering af projekter i et program.

Etablering af governance-struktur.

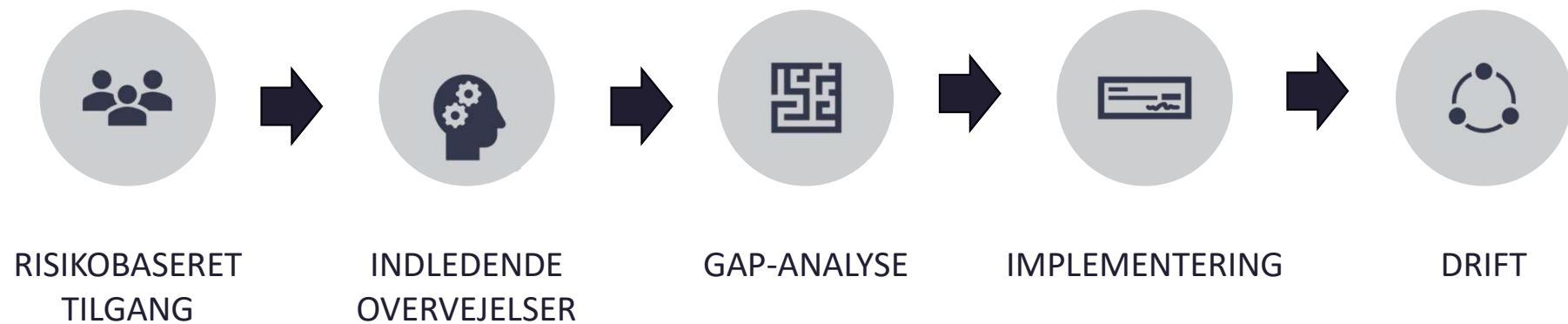
— Implementering - trin for trin

Overlevering til drift

Sikring af drift, forankring, og efterlevelse.

Udarbejdelse og vedligehold af årshjul.

Opsummering



— Erfaringer – udfordringer og gevinster

Typiske udfordringer

- Silotænkning
- Manglende dokumentation
- Personbåren viden
- Manglende risikostyringsmodel, metode og register
- Tillidsbaserede leverandørsamarbejder.
- Uklarhed om roller og ansvar
- Reel forankring af sikkerhedsinitiativer
- Systematik, koordinering og struktur i sikkerhedsarbejdet
- Implementering og forankring går langsomt



Erfaringer – udfordringer og gevinster

Typiske gevinster

- Øget synlighed i alle lag
- Styrket motivation og engagement
- Mere samarbejde og koordinering på tværs (inkl. OT)
- Bedre udnyttelse og forståelse af forskellige fagligheder
- Tydelighed i roller og ansvar
- Bevægelse væk fra, at det hele er it-afdelingen eller jura
- Øget fokus på adfærd
- Bedre forståelse for fordele ved at benytte kendte rammeværk/standarder





Tak fordi I lyttede med

Kontakt: lil@globeteam.com

Lisbeth Loft, Ph.d.
Senior Sikkerhedsrådgiver, Risk & Security