kaastrup | andersen

7 råd
- der gør dig klar til NIS2-compliance

Forord

I 2025 skal du være compliant med NIS2

Øget digitalisering og et stigende antal af cyberangreb stiller krav til et højt IT-sikkerhedsniveau. EU tager konsekvensen med det nye NIS2-direktiv, som skærper kravene til IT-sikkerhed for en lang række virksomheder og brancher.

Direktivet sikrer:

- Ledelsesforankret risikostyring
- Implementering af organisatoriske og tekniske foranstaltninger
- Rettidig og fælles indberetning af cybersikkerhedshændelser

Det endelige NIS2-direktiv blev offentliggjort i EU-tidende den 27. december 2022 og træder i kraft 20 dage efter. Medlemsstaterne, inklusiv Danmark, skal implementere direktivet i national lovgivning i 2025 - formentlig i første kvartal.

Hvad er nyt med NIS2?
NIS2 indeholder en væsentlig udvidelse i bredden af sektorer, så langt flere organisationer og serviceinstitutioner bliver omfattet af det nye direktiv. NIS1 ramte kun de allermest kritiske sektorer.

For at være klar til at efterleve de skærpede krav i NIS2-direktivet, er der flere overvejelser og aktiviteter, du bør iværksætte nu. Afhængigt af jeres nuværende sikkerhedsniveau, kan der være lang vej til, at du er klar til at efterleve de skærpede krav.

Virksomheder, der ikke overholder NIS2-kravene, kan få bødestraffe på op mod 2-4 mio. euro eller 1-2 % af virksomhedens globale omsætning.

Vær på forkant med NIS2
Vi præsenterer i denne e-bog 7 råd, du bør følge, for at opnå NIS2-compliance.

1. **Forankring i topledelsen**
2. **Overblik, overblik, overblik**
3. **Risikovurdering og prioritering**
4. **Værktøjs- og leverandørvalg**
5. **Incidenthåndtering og kommunikation**
6. **Test og træning**
7. **Business continuity og Disaster recovery**

De 7 aktiviteter har alle en afgørende fællesnævner: *dokumentation*. Udgangspunktet er, at hvis "det" ikke dokumenteres, så findes "det" ikke i virkeligheden. Derfor bliver det dit holdepunkt for sikkerhedsarbejdet.

Dokumentationen har flere formål:

1. Den er et værktøj til at opsamle viden med henblik på at forbedre processer
2. Den tjener til lettere videndeling
3. Den beviser, at der er reelle overvejelser og bevidste valg bag beslutninger

Vi trækker på velgennemprøvede og effektive processer og metoder. Denne erfaring har vi samlet i denne e-bog til dig. Her er vores **7 aktiviteter, der gør dig klar til at nå det rette sikkerhedsniveau**.

Rigtig god fornøjelse!

Thomas Hæstrup
Senior Consultant
thh@kaastrupandersen.dk
Telefon: +45 44 12 77 32

Simon Søgaard Jensen
Sales Manager
ssj@kaastrupandersen.dk
Telefon: +45 44 12 71 91

1 Forankring i topledelsen

Forankring af cyber-dagsordenen i topledelsen kan lyde let, men der kan være mange omkostningstunge beslutninger, der skal træffes, før du kommer dertil.

Cybersikkerhed koster penge, tager tid, kræver ressourcer og prioritering, og skal altid ses i lyset af systemernes kompleksitet, virksomhedens risikoprofil, risikoappetit og eventuelle lovgivningsmæssige krav.

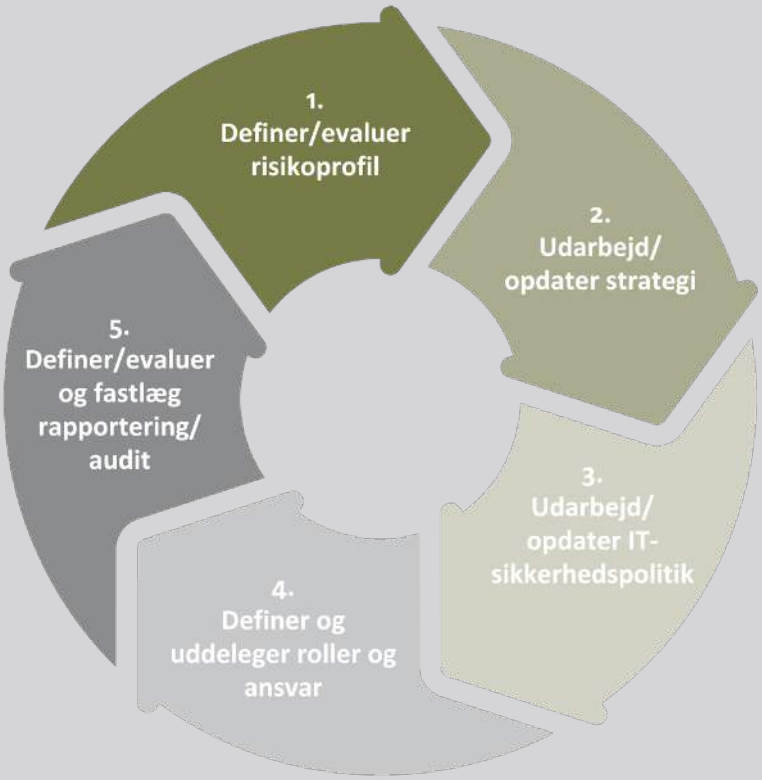
Grundlæggende skal cyber-risici håndteres på lige fod med fx finansielle eller strategiske risici, altså på bestyrelses- og direktionsniveau. Dette er ikke mindst på grund af direktivets fokus på de ledelsesansvarlige og bødestørrelserne på op til 10 mio. euro.

Målrettet ledelseskommunikation er en afgørende faktor

Udarbejdelse af strategier og politikker er én ting, men etablering og implementering af governance-modeller, processer og arbejdsgange, der er efterlevet i hele organisationen, kan være en ganske anden sag.

Her er klar og målrettet ledelseskommunikation en afgørende faktor for at få hele organisationen til at forstå og efterleve, at cybersikkerhed er et fælles ansvar og ikke noget, der skal fikses i IT- eller driftsafdelingen.

5 trin, topledelsen skal igennem:



2 Overblik, overblik, overblik

Når vi taler om prioritering og planlægning af aktiviteter, er nøgleordet: *overblik*.

Uden et klart overblik over **systemer, mennesker og processer**, kan det være svært for dig at sikre, at du beskytter de rigtige aktiver på den rette måde.

ISO 27001-standarden fungerer som en solid ramme for informationssikkerhed, der netop adresserer systemer, mennesker og processer.

Derfor introducerer vi dig allerede nu for ISO 27001. Standarden og NIS2-direktivet deler mange fælles krav, hvilket gør ISO 27001 til et stærkt fundament for at opnå NIS2-compliance.

ISO 27001-standarden opdeler sikkerheden i fire hovedtemaer:

1. IT-sikkerhed: Beskyttelse af digitale data og systemer mod Cyber- og Informationssikkerhedstrusler.

2. Fysisk sikkerhed: Sikring af fysiske faciliteter og udstyr mod uautoriseret adgang og skader.

3. Personalesikkerhed: Beskyttelse af medarbejdere og sikring af, at de er bevidste om sikkerhedsprocedurer.

4. Organisatorisk sikkerhed: Implementering af politikker og procedurer, der understøtter en sikkerhedskultur i hele organisationen.

ISO 27001 fremhæver vigtigheden af en balanceret tilgang, hvor alle aspekter af organisationen spiller en rolle. **Ved at anvende denne standard kan du identificere og håndtere sikkerhedsrisici på en struktureret måde.**

Samtidig opbygger du en sikkerhedskultur, hvor medarbejdere forstår deres ansvar og bidrager til at styrke sikkerheden.

Denne helhedsorienterede tilgang sikrer ikke kun compliance med ISO 27001 og NIS2, men gør også organisationen mere **robust og modstandsdygtig** overfor potentielle trusler.

Overblik over standarden og direktivet

Det kan være svært at danne sig et fuldkomment overblik over, hvordan ISO 27001-standarden og NIS2-direktivet påvirker din organisation.

Både NIS2 og ISO 27001 har til formål at forbedre informationssikkerheden, men de har forskellige tilgange og anvendelsesområder:

Sammenfald:

- Begge kræver, at organisationer implementerer passende tekniske og organisatoriske foranstaltninger for at beskytte informationssystemer.
- De understreger vigtigheden af risikostyring og løbende forbedring af sikkerhedsforanstaltninger.
- Begge rammer kræver dokumentation og rapportering af sikkerhedshændelser.

Forskelle:

- **ISO 27001 er en international standard**, der kan anvendes af enhver organisation, uanset størrelse eller sektor, og fokuserer på etablering af et informationssikkerhedsstyringssystem (ISMS), herunder etablering af politikker og processer til styring af informationssikkerheden.
- **NIS2 er et EU-direktiv**, der specifikt retter sig mod kritiske sektorer og underleverandører til disse.
- NIS2 har en lovgivningsmæssig ramme, hvor ISO 27001 kan betragtes som værktøjet til opfyldelse af lovkravene.

3 Risikovurdering og prioritering

For at stille din virksomhed bedst muligt i en krisesituation, er det vigtigt, at I skaber enighed om risikoanalyser og -vurderinger, prioritering af systemer og data.

Risikovurderinger bør gennemføres på alle systemer mindst en gang årligt, eller ved større ændringer og implementering af nye. Selve udarbejdelsen af vurderingen bør laves der, hvor viden om systemet reelt befinder sig og ikke som en ledelsesmæssig skrivebordsøvelse.

De enkelte risikovurderinger skal gennemføres med det samme værktøj, så de er sammenlignelige. Resultaterne skal samles centralt for at tegne det samlede risikobillede af organisationen, og så topledelsen får input, der kan prioriteres.

NIS2 stiller krav om overblik over 3. parts risici. Det er derfor nødvendigt at vurdere risici i hele forsyningskæden. Måske skal du indføje nye skærpede krav i leverandørkontrakter, som skal kontrolleres gennem revisorerklæringer eller audits.

NIS2 har ikke faste krav om valg af metode, men procesmæssigt adskiller risikovurdering af nyanskaffelser af IT-systemer og IT-systemer i drift sig lidt. Systemer i drift forventes at være risikovurderet tidligere – hvis ikke, bør du vurdere dem som nyanskaffelser.

Der ligger også en opgave i at definere, hvad der i jeres virksomhed betragtes som ”et system”. Add-ons, plugins og mindre værktøjer kan ofte sammenlægges eller undtages for egentlige risikovurderinger, bare dette sker gennem en velovervejet og dokumenteret proces.

De to største faldgruber i risikovurdering:

1. Risikovurderinger gennemføres lokalt med skyklapper på, hvilket betyder risici ikke vurderes tungt i organisationen.

2. Risici opsamles ikke centralt og kommunikeres ikke til topledelsen. Det får indflydelse på prioriteringer og negativ indvirkning på økonomi til mitigerende tiltag.

5 trin, der indgår i risikovurdering i forbindelse med nyanskaffelser og drift af IT-systemer:

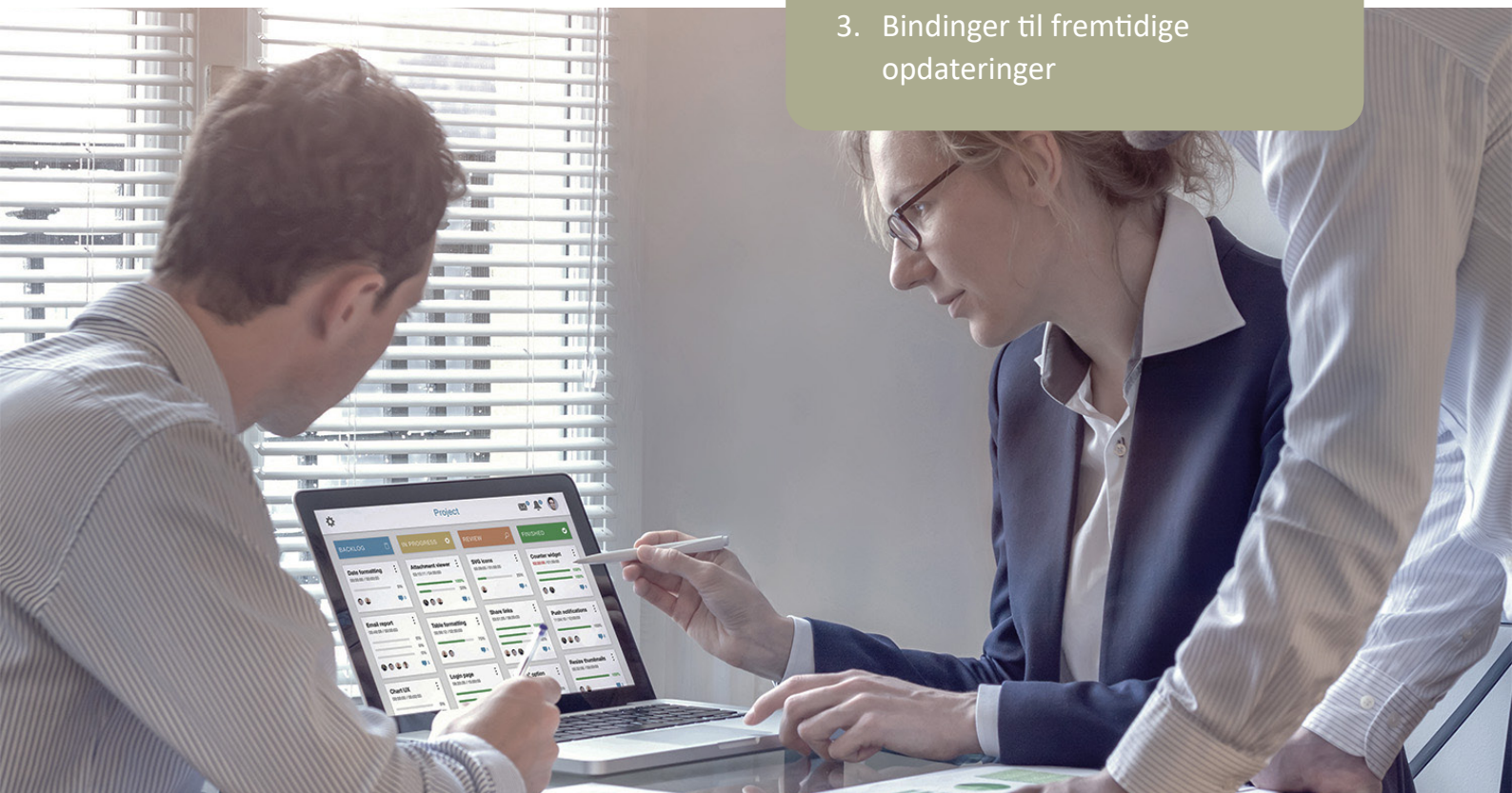
4 Værktøjs- og leverandørvalg

NIS2 dikterer, i lighed med andre standarder, ikke specifikke værktøjsvalg. Men mange virksomheder oplever hurtigt et behov for at få forskellige værktøjer til understøttelse af en række processer.

Markedet bugner af værktøjer og leverandører, der alle peger på egne fordele som uundværlige for enhver virksomhed. Faktum er dog, at "one size fits nobody". Her bør du lave velovervejede til- og fravalg, tilpasninger og potentielt få assistance til implementering.

Tre ting du bør overveje, inden du træffer et system og leverandørvalg:

1. Udgifter til licenser
2. Løbende driftsomkostninger
3. Bindinger til fremtidige opdateringer



NIS2-opgaver, der ofte kræver værktøjsunderstøttelse:

- Disaster recovery og Business continuity i forhold til planlægning, overblik og styring af delelementer, interessenter og kommunikation.

- Kryptering af data både "in motion" og "at rest", hvor afledte effekter som performancetab på netværket og identificering af flaskehalse kan være værktøjsafhængigt. Håndtering af legacy-systemer kan også være problematisk.

- Multifactor autentificering kan være isoleret til enkelte services eller brugerkonti, men kan også ses som et betydeligt større systemvalg i en Identity Management løsning.

- Sårbarhedsscanninger, hvor værktøjsvalget kan være afhængigt af mulige, eller ikke-mulige automatiseringer gennem API'er (Application Programming Interface) til eksisterende ITSM-systemer (IT Service Management).

5 trin til et struktureret værktøjs- og leverandørvalg:

5 Incidenthåndtering og kommunikation

Håndtering af cybersikkerhedshændelser er ikke en lineær proces.
Det er en cyklus, der består af:

- Forberedelse
- Afsløring
- Inddæmning af hændelser
- Mitigering
- Genskabelse af operationel stabilitet

Den sidste fase består i at drage lære af hændelsen med henblik på at forbedre processen og forberede sig på fremtidige hændelser. Her er kommunikation med både interne og eksterne interessenter samt (eventuelt) myndigheder vigtig.

De enkelte discipliner kræver ofte specialiserede kompetencer, der ikke nødvendigvis er tilgængelige i din virksomhed. Derfor kan du her overveje eksterne specialister.
Incidenthåndtering er en proces, der ofte involverer flere niveauer og funktioner i organisationen.

5 trin i incidenthåndteringsprocessen:

6 Test og træning

Cybersikkerhedstest er et centralt NIS2-krav. Det er en disciplin, der kræver meget i forhold til planlægning og gennemførelse, hvis omkostningerne skal stå mål med reel værdi.

Hvad enten der er tale om test af den organisatoriske awareness, PEN test, Assumed breach test, Redteam øvelser eller blot periodiske sikkerhedsscanninger, er der spørgsmål, du bør afklare, før du bruger ressourcer.

Afklar følgende:

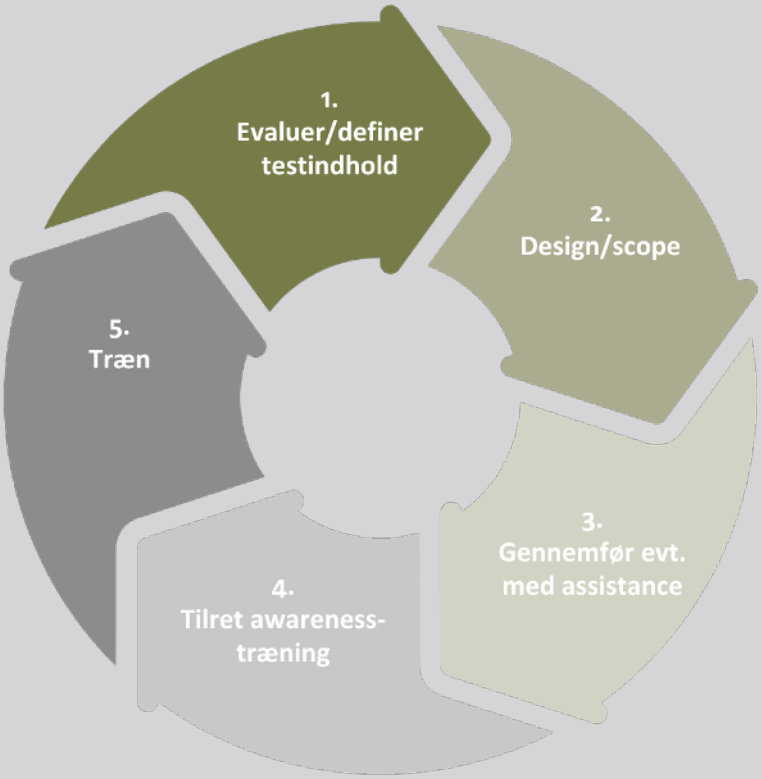
- Hvordan timer man test?
- Hvem designer test?
- Hvem kan give de nødvendige tilladelser til eventuelle afgivelser?
- Hvilke datasæt og systemer skal testes?
- Hvilke typer af test egner sig til hvad?
- Hvad er det basalt set, der ønskes testet?
- Hvad skal der ske med testresultaterne?
- Hvem skal have dem - og hvor hurtigt?

Uden disse nødvendige afklaringer i organisationen er der en betydelig risiko for, at både tid og penge er helt eller delvist spildt.

Når de besluttede tests er gennemført og resultaterne foreligger, har du dokumentation for, hvad den kommende træningsindsats skal have fokus på, og hvad du kan nedtone i en periode.

Det er dog vigtigt, at test og træning er kontinuerlig. Forskellige tests 3-4 gange om året er passende, hvis den generelle awareness blandt medarbejdere skal fastholdes.

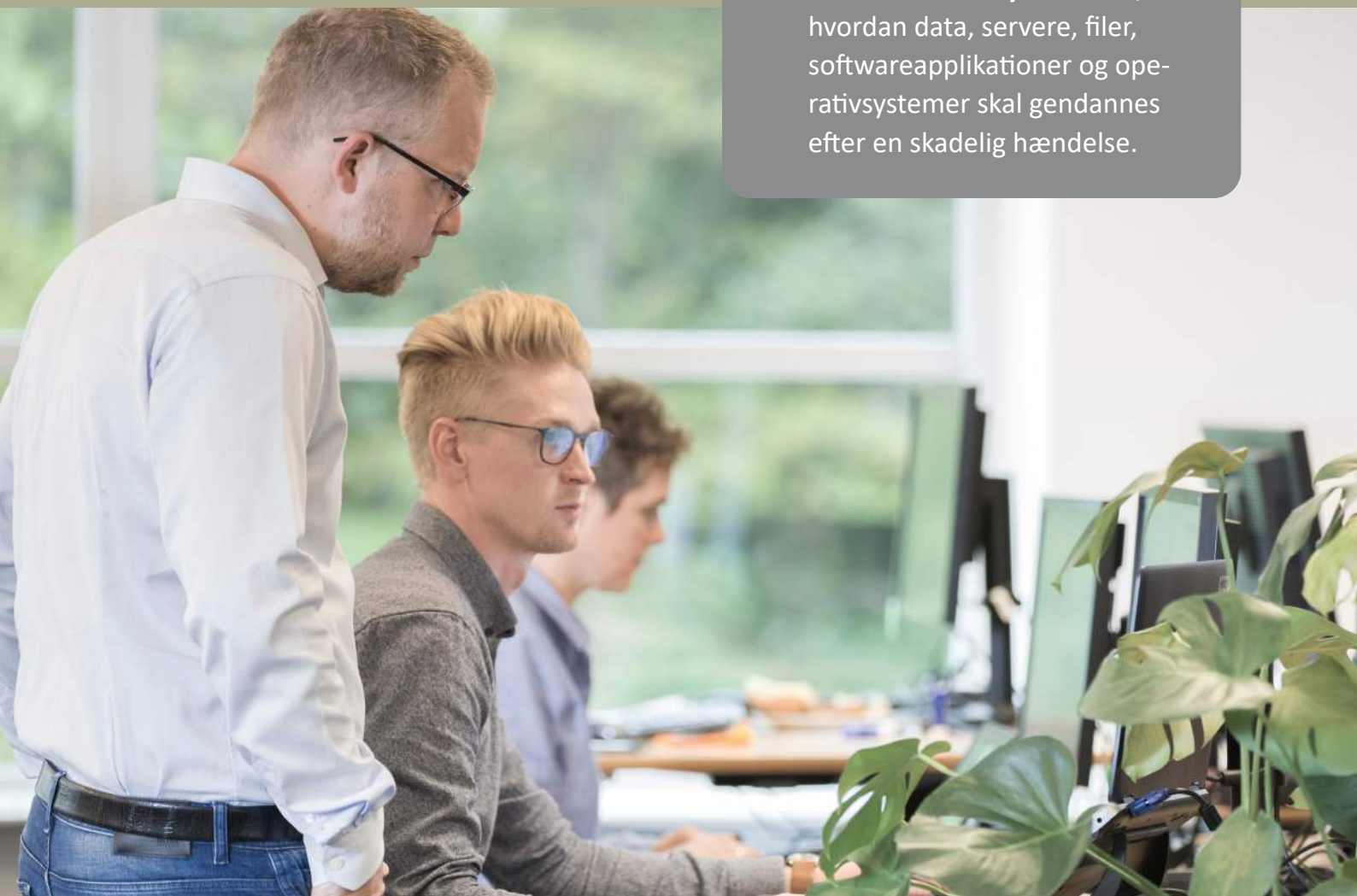
5 trin i processen for IT-sikkerhedstest:



7 Business continuity og Disaster recovery

Planer for Business continuity og Disaster recovery er en central del af hele beredskabet. De fokuserer på, hvad I skal gøre, og hvordan I skal handle, når uheldet er ude.

- **Business continuity** beskriver, hvordan du opretholder driften i en periode med teknologiske funktionsfejl eller afbrydelse.
- **Disaster recovery** definerer, hvordan data, servere, filer, softwareapplikationer og operativsystemer skal gendannes efter en skadelig hændelse.



Aktiviteterne, vi tidligere har beskrevet, danner grundlag for både Business continuity og Disaster recovery.

Aktiviteten 'Overblik, overblik, overblik' indeholder en af grundstenene til begge discipliner. Uden overblik over hardware, software, systemer og integrationer er det ikke muligt at prioritere og dermed bestemme i hvilken rækkefølge, de forskellige enheder og systemer skal håndteres.

Indholdet i "Risikovurderinger og prioriteringer" bygger videre på dette overblik og danner dermed den næste trædesten i begge planer. Især afsnittet om risikovurdering af systemer i drift er centralt.

"Værktøjs- og leverandørvalg" kommer ofte i spil, da der vil være behov for at understøtte Business continuity og Disaster recovery-arbejdet. Der er mange tværorganisatoriske/tværfaglige processer og kommunikation, som med fordel kan værktøjsunderstøttes.

Aktiviteten "Incidenthåndtering og kommunikation" bidrager med væsentlig viden i forhold til både Business continuity og Disaster recovery. Ikke mindst i arbejdet med "Kategorisering og prioritering", men også "Eftersporing generelt" hvor nye sammenhænge eller afhængigheder kan identificeres.

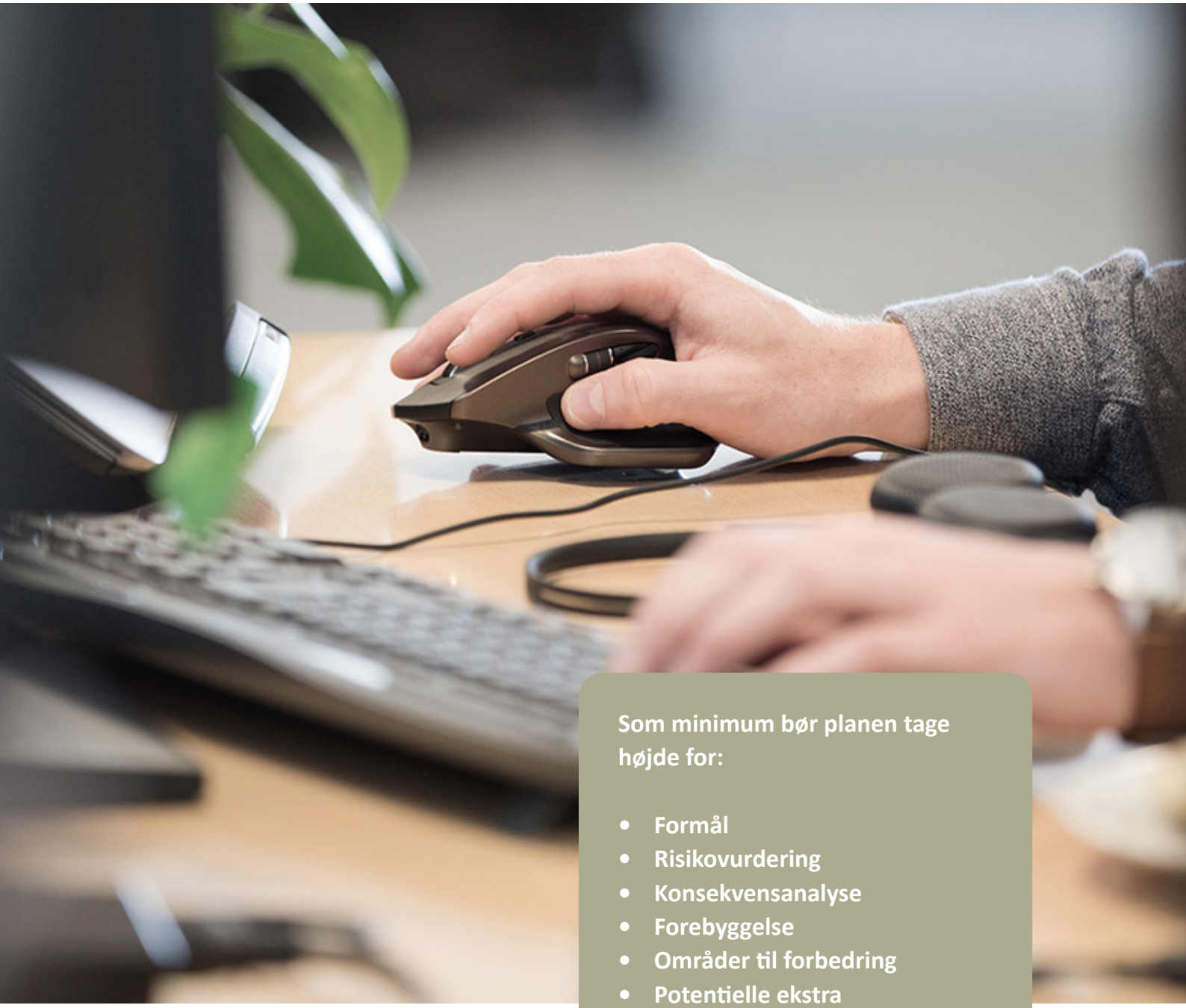
Business continuity-planer
Business continuity-planer bør være veldokumenterede og beskrive flest mulige aspekter af den aktuelle organisatoriske parathed til at håndtere forstyrrelser og potentielle kriser.

Det er vigtigt, at planerne beskriver, hvem der har det organisatoriske ejerskab, og hvem nøgleinteressenterne er.

Afklar følgende:

- **Formål**
- **Risikovurdering**
- **Konsekvensanalyse**
- **Forebyggelse**
- **Områder til forbedring**
- **Potentielle ekstra omkostninger**
- **Kommunikation**
- **Test**

Få uddybende information om business continuity-planer på vores hjemmeside.



Som minimum bør planen tage højde for:

- **Formål**
- **Risikovurdering**
- **Konsekvensanalyse**
- **Forebyggelse**
- **Områder til forbedring**
- **Potentielle ekstra omkostninger**
- **Kommunikation**
- **Test**

Få uddybende information om disaster recovery-planer på vores hjemmeside.

Disaster recovery-planer

Disaster recovery-planer bør omfatte alle de procedurer, teknologier og mål, der er nødvendige for at foretage en hurtig genopretning efter et angreb eller nedbrud.

Arbejdet med Business continuity og Disaster recovery bør du se som en iterativ proces.

Arbejdet baserer sig på flere af de tidligere beskrevne aktiviteter, og kan opsummeres i 5 trin:

5 trin til at arbejde med Business continuity og Disaster recovery:

Skal vi hjælpe dig med at opnå det rette IT-sikkerhedsniveau?

Vi håber, du har fundet inspiration i vores guide til, hvordan du kommer godt i gang med at blive NIS2-compliant.

Vi kan også hjælpe dig. Uanset teknisk og organisatorisk modenhedsniveau, status på opgaverne og størrelse af jeres organisation stiller vi med de nødvendige kompetencer og værktøjer til hjælpe jer gennem hele processen. Vi benytter velgennemprøvede og effektive processer og metoder, der hjælper jer med at få implementeret de nødvendige tiltag. Vi ser på, hvor I står lige nu og tilpasser løsningerne, så de matcher jeres behov.

Tag fat i os, hvis du vil høre mere om, hvordan vi sammen kan sikre dig og din virksomhed det rette IT-sikkerhedsniveau.

Vi glæder os til at høre fra dig.

Book afklaringsmøde

Thomas Hæstrup
Senior Consultant
thh@kaastrupandersen.dk
Telefon: +45 44 12 77 32

Simon Søgaard Jensen
Sales Manager
ssj@kaastrupandersen.dk
Telefon: +45 44 12 71 91