

CEΘAL



E-bog

NIS2

Konkrete råd til ledelsen.

Indholdsfortegnelse

4

Organisation

Hvordan skal I tænke på ansvar og beføjelser?

6

Struktureret arbejde

Hvordan etableres et struktureret arbejde inden for sikkerhed?

8

Risikobaseret arbejde

Hvad kræves for at opfylde NIS2-kravene om risiko?

10

Sanktioner

Hvad sker der, hvis I ikke følger loven?

12

Risikohåndteringstiltag

Hvilke sikkerhedstiltag kræver NIS2?

14

Hændeshåndtering

Hvad kræver loven, hvis der opstår en hændelse?

16

Uddannelse

Hvilken viden skal ledelsen have?

18

Lokale love og regler

Myndighedernes muligheder for at præcisere loven.

20

Virksomhedsregistrering

Registrering af jeres virksomhed hos tilsynsmyndigheden

22

Opfølgning

Hvordan kan og bør ledelsen følge op på sikkerhedsarbejdet?



Forord

NIS2 handler i bund og grund om effektiv håndtering af informations- og cybersikkerhed.

Tre vigtige hjørnesten inden for informations- og cybersikkerhed er:

- Fortrolighed / Confidentiality
- Integritet / Integrity
- Tilgængelighed / Availability

Disse tre begreber danner, med de engelske betegnelser **CIA**, hjørnestenene i informations- og cybersikkerhed.

Fortrolighed

Kun de personer, der er autoriseret, skal have adgang til informationen.

Integritet

Informationen skal være korrekt.

Tilgængelighed

Informationen skal være tilgængelig, når den er nødvendig.

Disse tre hjørnesten vil danne grundlaget for vores konkrete råd i denne eBog.

A photograph of two men sitting at a wooden table, looking at a laptop. The man on the left has a beard and is wearing a dark shirt with a rainbow lanyard. The man on the right is wearing a light-colored shirt. A large, semi-transparent green number '1' is overlaid on the image, positioned behind the word 'Organisation'.

Organisation

Hvordan bør I forholde jer
til ansvar og beføjelser?



Organisation

Arbejdet med informations- og cybersikkerhed fungerer bedst, når der er klarhed i organisationen om roller og ansvar, både inden for dette område og mere generelt.

Selskabsloven § 115, stk. 1 fremhæver bestyrelsens brede ansvar for virksomhedens overordnede styring med følgende tekst:

”Bestyrelsen varetager den overordnede og strategiske ledelse af kapitalselskabet og skal sikre en forsvarlig organisation af selskabets virksomhed.”

Bestyrelsens ansvar delegeres til virksomhedens ledelse via direktøren, hvor direktørens instruktioner bør indeholde den nødvendige detaljerede information.

NIS2 fastsætter ledelsens ansvar for informations- og cybersikkerhed i artikel 20, stk. 1:

”Medlemsstaterne sikrer, at de væsentlige og vigtige enheders ledelsesorganer godkender de foranstaltninger til styring af cybersikkerhedsrisici, som disse enheder har truffet med henblik på at overholde artikel 21, forer tilsyn med dens gennemførelse og kan gøres ansvarlige for enhedernes overtrædelser af forpligtelserne i nævnte artikel.”

Loven tydeliggør ledelsens ansvar, men I som ledelse skal sikre, at opgaverne kan delegeres til resten af organisationen.

Hvordan denne fordeling udformes, afhænger af, hvordan I ellers er organiseret. Her følger et par konkrete råd:

- En hovedansvarlig bør lede og følge op på alt arbejde inden for området. Rollen som CISO (Chief Information Security Officer) varetager ofte denne opgave.
- Den hovedansvarlige bør ikke rapportere til den chef, der har ansvar for den praktiske implementering.
- Ledelsen skal løbende følge op på arbejdet med informations- og cybersikkerhed.

Placeringen af den hovedansvarlige i organisationen kan være afgørende for, hvor effektivt arbejdet er. Nogle organisationer betragter området som en del af IT og placerer CISO under IT-chefen. Denne placering kan dog skabe interessekonflikter, da CISO både skal give instruktioner til og følge op på IT-chefens arbejde.

Hvis det er muligt, bør CISO rapportere direkte til direktøren og være en del af virksomhedens ledelsesgruppe. Dette sikrer, at informations- og cybersikkerhed bliver integreret i alle vigtige beslutninger på ledelsesniveau.



Struktureret arbejde

Hvordan skaber man struktur
i sikkerhedsarbejdet?

Struktureret arbejde

For at sikre, at arbejdet med informations- og cybersikkerhed udføres effektivt og giver mulighed for opfølgning, anbefales det at etablere et Information Security Management System (ISMS).

Det er dog vigtigt at være opmærksom på, at et ISMS ikke er et selvstændigt produkt, men skal integreres med virksomhedens øvrige ledelsessystemer, politikker, processer og procedurer.

Et eksempel på et område, hvor integration er nødvendig, er HR, hvor sikkerhed omkring personale bliver en del af rekruttering, onboarding og også offboarding.

ISMS bør udvikles af den hovedansvarlige for sikkerheden i samarbejde med de afdelinger, der berøres af de forskellige delområder. Ledelsen bør være aktivt involveret i processen og være dem, der godkender de overordnede styringsdokumenter.

Det er også vigtigt at forstå, at et ISMS skal vedligeholdes løbende for at sikre, at ændringer i både omverdenen og organisationen afspejles i styringsdokumenterne.

Etablering af et ISMS handler ikke kun om at udarbejde styringsdokumenterne, men også om at sikre, at de nødvendige forandringer i organisationen bliver gennemført, samt at der løbende foretages periodisk opfølgning på overholdelsen.

I den indledende fase af etableringen af et ISMS kræves en større indsats og et stærkt fokus på forandringsarbejdet, mens den løbende drift af ISMS primært handler om forvaltning og opfølgning. Derfor er det hensigtsmæssigt at betragte etableringen af ISMS som et projekt, hvor der tildeles de nødvendige ressourcer – både interne og eventuelt eksterne – der kan drive forandringsprocessen effektivt.

Der er ikke et specifikt krav i NIS2 om at etablere et ISMS, men det vil være vanskeligt at udføre et korrekt arbejde og opfylde lovkravene uden denne struktur.



The background features a dark, moody scene with several wooden blocks of varying sizes. Some blocks are stacked, while others are scattered. A large, semi-transparent green number '3' is centered in the background. The text 'Risikobaseret arbejde' is overlaid in white.

Risikobaseret arbejde

Hvad kræves for at arbejde i overensstemmelse
med NIS2-kravene til risiko?



Risikobaseret arbejde

Det beskyttelsesniveau, der skal etableres for jeres virksomhed, skal baseres på de risici, som identificeres gennem strukturerede risikoanalyser. NIS2 omfatter en række specifikke områder, der altid skal indgå i dette risikobaserede arbejde.

Det fremgår af lovgivningen, og er samtidig vigtigt, at også andre områder, der er relevante for virksomhedens sikkerhed, skal inddrages i risikohåndteringen.

Et veludført risikohåndteringsarbejde danner også grundlag for, at virksomhedens ressourcer anvendes på de rigtige tiltag, således at både tid og penge bruges effektivt.

Ledelsens ansvar i henhold til NIS2-direktivet er klart beskrevet i forhold til risiko og risikohåndtering. Følgende er et uddrag fra direktivet:

*"Medlemsstaterne sikrer, at de væsentlige og vigtige enheders **ledelsesorganer** godkender de foranstaltninger til styring af cybersikkerhedsrisici, som disse enheder har truffet med henblik på at overholde artikel 21, forer tilsyn med dens gennemførelse og kan gores ansvarlige for enhedernes overtrædelser af forpligtelserne i nævnte artikel." - 2022/2555, artikel 20*

Risiko består både af sandsynligheden for, at en uønsket hændelse opstår, og de negative konsekvenser, hændelsen medfører. De risikohåndteringsforanstaltninger, der kan iværksættes, omfatter at arbejde for at reducere risikoen, eliminere risikoen helt eller acceptere risikoen.

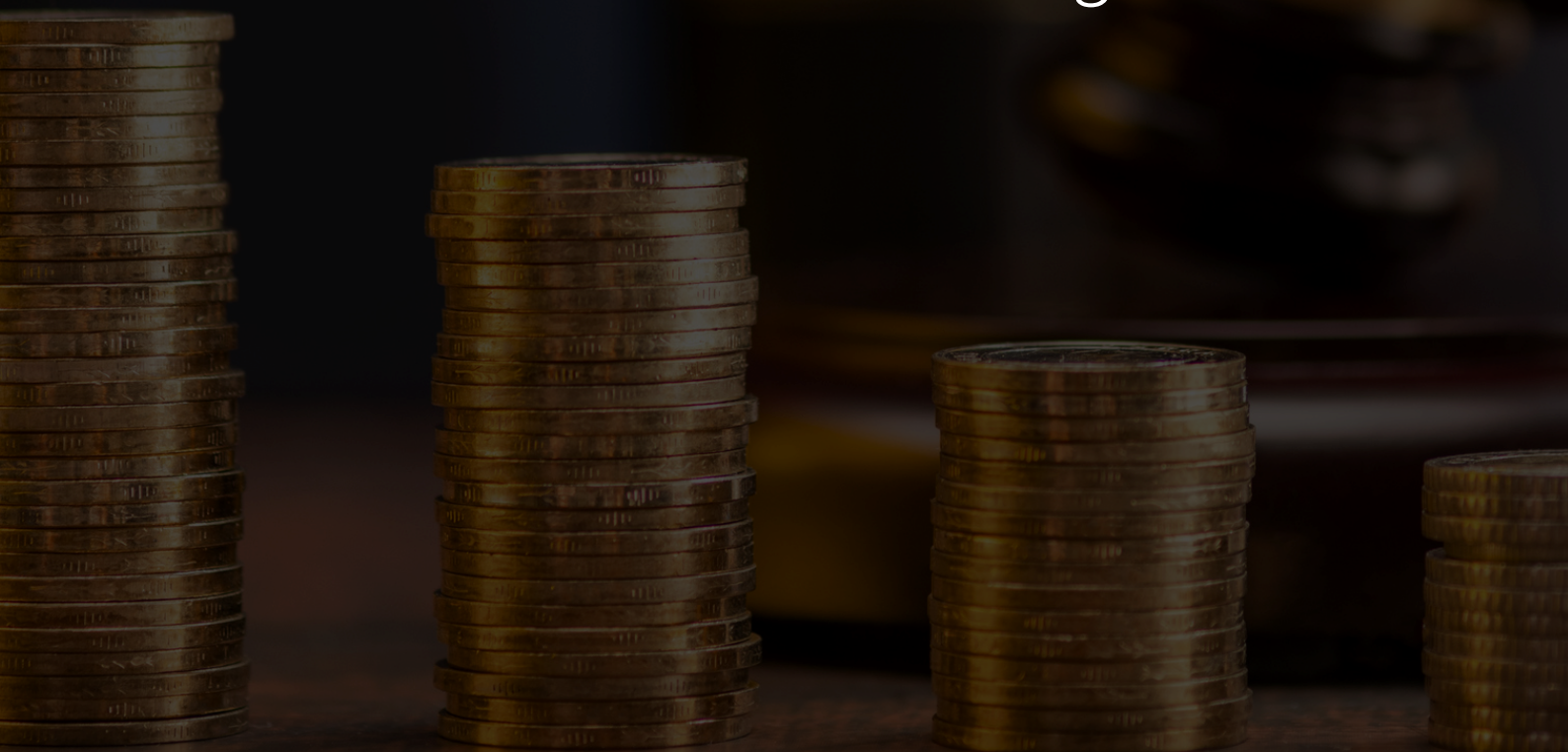
At eliminere en risiko fuldstændigt er ofte vanskeligt, da det kan kræve, at man opgiver aktiviteter, der bidrager positivt til virksomhedens lønsomhed. Mere almindeligt er det at arbejde med at reducere risikoen, enten ved at mindske sandsynligheden for, at hændelsen opstår, eller ved at reducere dens konsekvenser – eller i bedste fald begge dele. Når risikoen ikke vurderes at være betydelig, undertiden efter implementering af tiltag, skal den accepteres. Det er vigtigt, at denne accept sker på det rette niveau, og at virksomhedens samlede risikoniveau er acceptabelt.

Det er vigtigt at inddrage eksperter fra de relevante områder i risikoanalyser og handlingsplaner. Kravet i NIS2 er dog altid, at ledelsen skal forstå og godkende risikohåndteringsforanstaltningerne.

[Læs gerne mere om risiko på vores blog >](#)

4 Sanktioner

Hvad sker der, hvis du ikke følger loven?



Sanktioner

NIS2-direktivet fastsætter, at virksomheder kan holdes ansvarlige gennem sanktioner, herunder bøder, og at ledelsen ligeledes kan gøres ansvarlig for manglende efterlevelse.

I særligt alvorlige tilfælde kan der pålægges sanktioner rettet mod ledelsen, hvilket understreger vigtigheden af korrekt efterlevelse af direktivets krav.

Sanktioner kan variere mellem medlemslandene og er fuldt defineret i den nationale lovgivning.

I Danmark reguleres dette i L141 – kapitel 9 – Straf.

EU-direktiv 2022/2555 (NIS2) angiver som vejledende maksimum:

Væsentlige enheder:

Bøder kan være op til **10 000 000** euro eller 2 % af den samlede globale årsomsætning, alt efter hvilket beløb der er højest.

Vigtige enheder:

Bøder kan være op til **7 000 000** euro eller 1,4 % af den samlede globale årsomsætning, alt efter hvilket beløb der er højest.



A hand is shown placing a wooden block onto a Jenga tower. A large, semi-transparent green number '5' is overlaid on the tower. The background is dark and out of focus, showing a person in a suit.

Risikohåndteringstiltag

Hvilke sikkerhedstiltag kræver NIS2?

Risikohåndteringstiltag

NIS2 fastsætter klare krav til risikohåndteringstiltag, som virksomheder skal tage i betragtning for at beskytte deres net- og informationssystemer.

I henhold til artikel 21, stk. 1 i NIS2-direktivet:

"Medlemsstaterne sikrer, at væsentlige og vigtige enheder træffer passende og proportionelle tekniske, operationelle og organisatoriske foranstaltninger til styring af de risici, der truer sikkerheden i net- og informationssystemer, som disse enheder anvender i deres aktiviteter."

Direktivet foreskriver desuden, at arbejdet skal baseres på en risikobaseret tilgang, hvor foranstaltningerne tager udgangspunkt i en grundig risikovurdering og er proportionelle i forhold til de identificerede risici.

Organisationen skal udføre detaljerede risikoanalyser og afveje risikoen mod omkostningen ved foranstaltningerne. NIS2 giver fleksibilitet til at vælge passende tiltag, men stiller krav om, at disse er tilstrækkelige.

De områder, som NIS2 fremhæver som vigtige i overensstemmelse med L 141 § 6, inkluderer:

- 1 håndtering af hændelser
- 2 driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring
- 3 forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere
- 4 sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder
- 5 politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici
- 6 grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse
- 7 politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering
- 8 personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver
- 9 brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikre nødkommunikationssystemer internt i enheden, hvor det er relevant.

Det er vigtigt at bemærke, at NIS2-direktivet i artikel 21, stk. 2, fastsætter, at de nævnte sikkerhedsforanstaltninger "mindst" skal omfatte specifikke områder. Dette betyder, at organisationer også bør inkludere andre relevante risikoområder, hvis de har betydning for cybersikkerheden.

For at kunne opfylde NIS2's krav skal organisationen have den nødvendige ekspertise til at gennemføre risikovurderinger, udarbejde effektive handlingsplaner og sikre, at foranstaltningerne løbende tilpasses nye risici og ændringer i organisationen.



Hændelseshåndtering

Hvad kræver loven, hvis en hændelse opstår?

Hændelseshåndtering

NIS2 fastsætter krav til håndtering og rapportering af hændelser, herunder også hændelser, der kan påvirke de tjenester, der er omfattet af direktivet.

En betydelig hændelse defineres ud fra faktorer som:

- Varighed og omfang af hændelsen
- Antallet af berørte brugere
- Økonomisk, materiel eller immateriel skade

Alle betydelige hændelser skal rapporteres til den relevante myndighed med CSIRT-ansvar, og første kontakt skal ske senest 24 timer efter, at hændelsen er blevet opdaget.

Ud over kontakt med myndigheder skal væsentlige og vigtige enheder uden unødigt forsinkelse underrette tjenestemodtagere, der potentielt er berørt af en væsentlig cybertrussel. Som angivet i artikel 23, stk. 2:

"I givet fald sikrer medlemsstaterne, at væsentlige og vigtige enheder uden unødigt ophold meddeler modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, eventuelle foranstaltninger eller modforholdsregler, som disse modtagere kan træffe som reaktion på den pågældende trussel. Hvor det er relevant, skal enhederne også informere de pågældende modtagere om selve den væsentlige cybertrussel."

Direktivet foreskriver ikke præcist, hvordan hændelser skal håndteres internt, eller hvor hurtigt de skal løses. Det er dog afgørende, at jeres virksomhed opbygger en stærk evne til at håndtere alvorlige hændelser for at beskytte driften.

I skal tage stilling til, om denne evne skal udvikles internt, eller om I har behov for ekstern støtte til at håndtere de mest kritiske hændelser.





7 Uddannelse

Hvilken viden skal ledelsen have?

Uddannelse

NIS2-direktivet fastsætter, at ledelsen i væsentlige og vigtige enheder skal sikre tilstrækkelig uddannelse for at kunne håndtere risici og cybersikkerhedsudfordringer. Det kræves, at medlemmer af ledelsen gennemgår relevante kurser, og at medarbejdere tilbydes tilsvarende uddannelse, der dækker virksomhedens risikohåndteringstiltag.

Dette indebærer, at virksomheden skal udvikle relevante uddannelsesforløb og dokumentere, hvem der har deltaget og gennemført disse forløb.

Ud over de lovpligtige uddannelseskrav anbefales det, at de medarbejdere, der har ansvar for informations- og cybersikkerhed, løbende får mulighed for efteruddannelse. Trusselsbilledet ændrer sig hurtigt, og det kræver, at virksomheder afsætter tid og budget til at følge med udviklingen af både nye trusler og beskyttelsesmekanismer.





Lokale love og regler

Myndighedernes muligheder
for at præcisere loven

Lokale love og regler

Reguleringer

NIS2 er et EU-direktiv, hvilket kræver, at hver medlemsstat indfører direktivet i national lovgivning, hvor reguleringen fastsætter minimumskravene.

Derfor skal I som organisation gennemgå den lokale implementering af NIS2 i de lande, hvor I opererer og/eller leverer tjenester, der er omfattet af NIS2.

De lokale love kan også give de kompetente myndigheder mulighed for at udarbejde mere detaljerede forskrifter, som kan være branchespecifikke.

For IKT-sektoren er der en EU-implementeringsforordning for NIS2, 2024/2690, som er obligatorisk for de udvalgte typer af IKT-tjenester/funktioner, der er angivet i implementeringsforordningen.

I Danmark er NIS2 implementeret via Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (L 141), vedtaget 29. april 2025.
Loven træder i kraft 1. juli 2025.





Virksomhedsregistrering

Registrering af jeres virksomhed hos
tilsynsmyndigheden

Virksomhedsregistrering

NIS2 fastsætter, at visse virksomheder skal registrere sig hos de relevante tilsynsmyndigheder.

Anmeldelsen skal indeholde følgende oplysninger:

- Identitet
- Kontaktoplysninger
- IP-adresseintervaller
- Virksomhedstype
- Oplysninger om, i hvilke lande virksomheden opererer

Hvis der sker ændringer i oplysningerne, skal de opdateres inden for 14 dage.

et er vigtigt at identificere, hvilken eller hvilke tilsynsmyndigheder virksomheden skal registreres hos.

Dette afhænger af virksomhedens type og de tjenester, der leveres. Det afhænger også af, hvilke medlemsstater jeres virksomhed skal registreres i.

I Danmark skal registrering ske via virk.dk, senest den 1. oktober 2025.

Det er vigtigt at udpege klare ansvarsområder for at sikre, at registrerede oplysninger opdateres rettidigt inden for 14 dage, når der sker ændringer.

Ansaret kan fordeles, så IT-afdelingen håndterer de tekniske aspekter af registreringen, mens mere overordnede oplysninger om virksomheden og dens aktiviteter varetages af en anden relevant funktion.

Name: _____

Company: _____

Address: _____

City: _____

Phone: _____

A background image showing two women in a professional setting, likely a meeting. One woman is in the foreground, looking towards the other woman who is slightly out of focus in the background. They are both wearing lanyards with 'CEGAL' on them. The image is dimmed to allow text to be overlaid.

10 Opfølgning

Hvordan kan og bør ledelsen følge op
på arbejdet med sikkerhed?

Opfølgning

NIS2-direktivet fastsætter, at sikkerhedsforanstaltninger skal evalueres, som angivet i artikel 21:

"Medlemsstaterne sikrer, at en enhed, der finder, at den ikke overholder foranstaltningerne i stk. 2, uden unødigt ophold træffer alle nødvendige, passende og forholdsmæssige korrigerende foranstaltninger."

Baseret på NIS2-direktivets formål er de to primære fokusområder for evaluering:

- Proaktive sikkerhedsforanstaltninger - Hvor godt beskytter vi os mod potentielle trusler?
- Reaktive sikkerhedsforanstaltninger - Hvor hurtigt og effektivt håndterer vi alvorlige hændelser?

Da ledelsen har hovedansvaret i henhold til NIS2, er det vigtigt, at evalueringen gennemføres på en måde, der giver ledelsen den nødvendige indsigt og forståelse.

Ud over lovkravene bør virksomheden også tage egne interesser i betragtning, herunder sikre, at de mest effektive metoder anvendes. Effektiviteten af de valgte løsninger bør vurderes med henblik på at optimere sikkerheden og minimere omkostningerne.

At sikre en optimal sikkerhedsniveau kan være udfordrende. En utilstrækkelig sikkerhed kan først opdages, når det er for sent, og i værste fald kan hele IT-systemer blive lammet som følge af et cyberangreb.

En for høj grad af sikkerhed kan på den anden side have langsigtede negative effekter, herunder øgede omkostninger og lavere konkurrenceevne.

Ved implementering af sikkerhedsfunktioner er det vigtigt også at tage stilling til, hvordan opfølgningen skal gennemføres. Det anbefales at opdele opfølgningen i flere niveauer, hvor ledelsen modtager overordnede rapporter og nøgleinformation.

Her er nogle relevante spørgsmål, som ledelsen kan stille til de ansvarlige:

- Har vi åbne afvigelser i forhold til vores informationssikkerhedspolitik?
- Hvor mange angreb identificerer og forhindrer vi hver måned?
- Hvor mange sårbarheder opdager vi i vores systemer hver måned?
- Hvor mange sårbarheder har vi opdaget, men endnu ikke udbedret?
- Hvor mange sikkerhedshændelser har vi håndteret månedligt?
- Hvilke øvelser og tests har vi gennemført for at sikre incident- og kontinuitetshåndtering?
- Hvordan har vi fulgt op på vores kritiske leverandørers sikkerhedsarbejde?

Det bør overvejes at udføre ekstern revision af sikkerheden, både på procesniveau og teknisk implementeringsniveau. Da dette i stigende grad er et krav fra kunder, kan det opfyldes gennem certificeringer som ISO 27001 eller mere dybdegående vurderinger via SOC2 Type 2-revisioner.



Om forfatteren



Daniel Andersson

Daniel er certificeret informationssikkerhedschef (ISACA CISM) med 25 års erfaring inden for IT både i tekniske og ledelsesmæssige roller.

Daniel har arbejdet med informations- og cybersikkerhed i over 15 år på tværs af brancher som bank og finans, energi, detailhandel, IT og medier m.fl.

Han er en af Cegals konsulenter inden for cybersikkerhed, der kan hjælpe jer med arbejdet med NIS2.