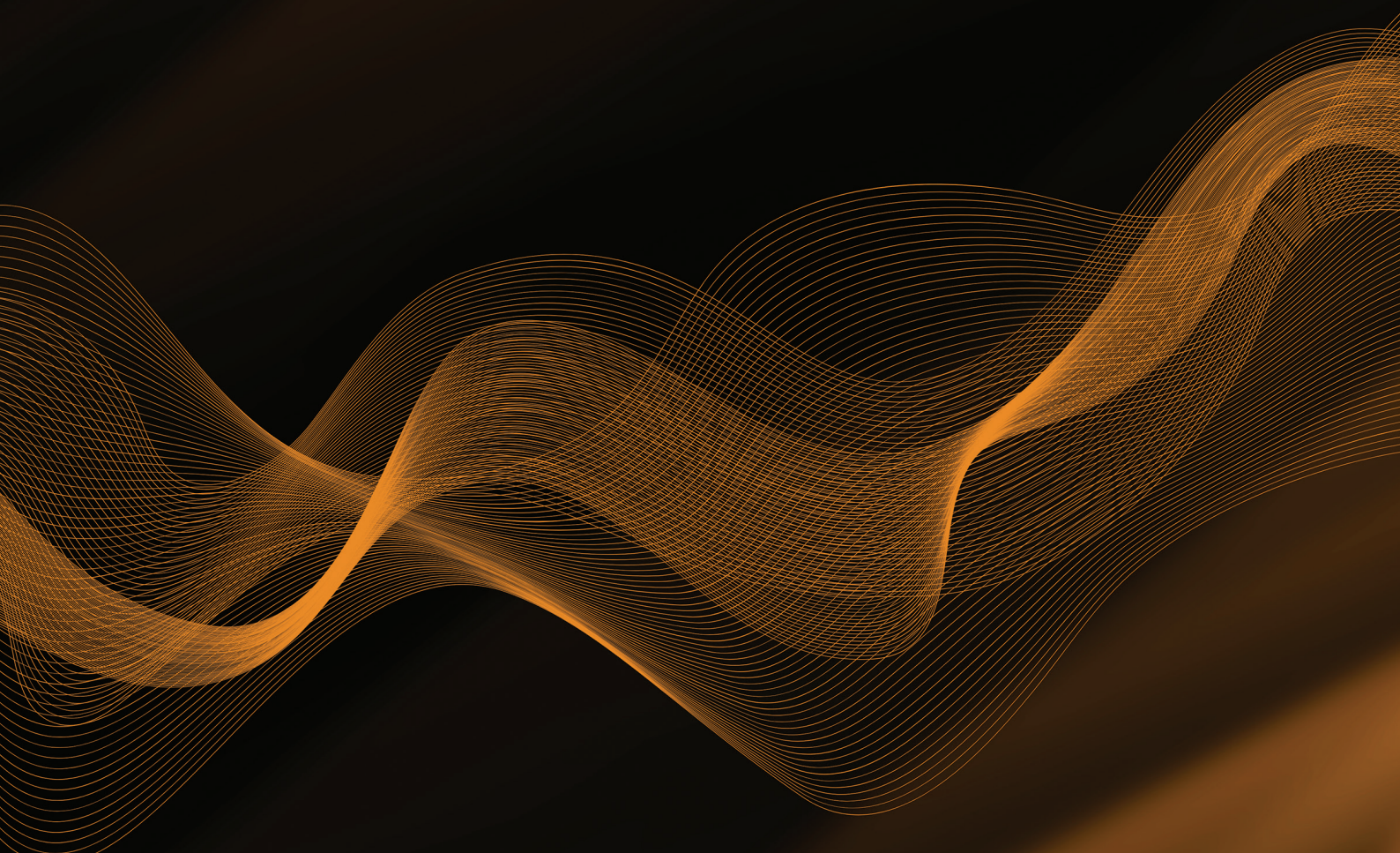


# NIS 2-LOVEN

Ledelsens ansvar for organisationens cyberuddannelse



# INDHOLDSFORTEGNELSE

|    |                                                         |    |
|----|---------------------------------------------------------|----|
| 00 | Introduktion                                            | 04 |
| 01 | Executive Summary                                       | 05 |
| 02 | Strategisk Kontekst                                     | 06 |
| 03 | Løsningen                                               | 07 |
| 04 | Struktureret Roadmap                                    | 09 |
| 05 | NIS 2-loven – Kort fortalt                              | 10 |
| 06 | NIS 2-loven og Campfire Security som strategisk partner | 11 |
| 07 | I dybden med NIS 2-loven                                | 12 |

## 0. INTRODUKTION

# Praktisk understøttelse af jeres NIS 2-compliance: Strategisk, taktisk og operationelt

Implementeringen af NIS 2-direktivet markerer et historisk skift i kravene til dansk cybersikkerhed. Lovgivningen flytter ansvaret direkte ind på ledelsesgangen og stiller skærpede krav til både ledelse, organisation og teknik. Blandt andet kræver loven at ledelsen deltager i relevante kurser og at medarbejderne modtager dokumenteret cybersikkerhedsuddannelse tilpasset deres rolle og risikoprofil.

Det er dermed ikke længere nok at have de rette tekniske løsninger, det er nu ledelsens ansvar at sikre at organisationen er i stand til at modstå cybertruslen som helhed og derigennem forhindre eller minimere konsekvenserne for samfundet.

Forfatterne af dokumentet:



Jens Myrup Pedersen

Medstifter og Product Manager  
i Campfire Security



Martin Yan Hansen

Head of Learning  
Experience & Innovation  
i Campfire Security

Hos Campfire Security har vi specialiseret os i at levere rollebaseret, praktisk og engagerede cybersikkerhedstræning, så vi kan understøtte dig i organisationens NIS 2-compliance. Vi bygger bro mellem lovens krav og den praktiske eksekvering gennem vores læringsplatform og vores unikke rammeværk for kompetenceudvikling, supporteret med lige præcis den ledelsesrådgivning som I har behov for.

## 1. EXECUTIVE SUMMARY

# Vejen til en stærk cyberkultur under NIS 2

## A. Strategisk nødvendighed

Beskyttelse af samfundets fundament

Med NIS 2 placeres cybersikkerhed som et strategisk ledelsesansvar i private virksomheder, der leverer væsentlige eller vigtige tjenester. Når en virksomhed bliver omfattet af NIS 2, betyder det, at et cyberangreb ikke længere blot påvirker intern drift — det kan true samfundskritisk infrastruktur, tillid og stabilitet i de tjenester, virksomheden understøtter. Ledelsesorganet har det direkte ansvar for at sikre et dokumenteret og løbende styrket cybersikkerhedsniveau. Det indebærer strategisk prioritering, risikobaseret styring og investering i den nødvendige kompetenceudvikling, herunder krav om målrettet cybersikkerhedsuddannelse for ledelsen selv. Dette dokument giver ledelsesorganet et koncentreret overblik over de centrale NIS 2-krav og det ansvar, der følger med at være en væsentlig eller vigtig enhed under direktivet.

## C. Løsningen

Lær "Hacker mindset" — og skab menneskelig modstandskraft

Campfire Security bygger bro mellem lovkrav og den praktiske eksekvering, ved at erstatte passiv awareness med engagerende træning. Derigennem lærer vi medarbejderne at tænke som en hacker - vi tror nemlig på, at man er nødt til at forstå de som angriber, for at kunne opsætte et effektivt forsvar.

### For ledelsen:

Målrettede workshops der styrker beslutningskraften og imødekommer kravet i NIS 2

### For medarbejderne:

En læringsplatform med fokus på vigtige cybersikkerhedsområder, blandt andet multifaktorautentificering (MFA), netværkssegmentering og adgangskontrol

### For organisationen:

Fælles sprog og dokumenteret kompetenceudvikling via vores Cyber KPI Framework, som kan benyttes som dokumentation til tilsynsmyndigheder

## B. NIS 2-loven

Fra lovkrav til ledelsesdisciplin

NIS 2 stiller klare og bindende krav til virksomhedens ledelsesorgan. Ledelsen skal ikke blot godkende sikkerhedsindsatser, men aktivt deltage i træning inden for cybersikkerhed, og risikostyring. Direktivet kræver, at virksomheden etablerer dokumenteret, rollebaseret uddannelse og sikrer, at hele organisationen efterlever grundlæggende cyberhygiejne.

Manglende efterlevelse er ikke længere et teknisk problem — det er et brud på ledelsens lovmæssige ansvar. Da NIS 2 bygger på en risikobaseret tilgang, er det et særskilt krav, at ledelsesorganet besidder de nødvendige kompetencer til at implementere, forankre, overvåge og kontinuerligt forbedre virksomhedens cybersikkerhedsniveau.

## D. Resultatet

En proaktiv og mere sikker virksomhed

Ved at styrke medarbejdernes cybersikkerhedskompetencer opbygger virksomheden sit stærkeste forsvar: den menneskelige modstandskraft. Gennem målrettet træning giver ledelsen organisationen et effektivt og dokumenterbart værktøj til at reducere risici — ikke gennem tunge teknologiinvesteringer, men gennem bevidsthed, fælles viden og forskningsbaseret læring.

Resultatet er en virksomhed, hvor sikkerhed er en integreret del af hverdagen, og hvor kulturen er baseret på en fælles forståelse af cybertruslen, angribernes metoder og nødvendigheden af årvågenhed. Det er denne kultur, der skaber fundamentet for en robust, konkurrencedygtig og digitalt tryk organisation.

## 2. STRATEGISK KONTEKST

# Ledelsens ansvar i NIS 2

Når virksomheder er omfattet af NIS 2-loven direktivet, og dermed klassificeres som leverandører af samfundskritiske eller væsentlige tjenester, ændres spillereglerne markant. Det nuværende komplekse trusselsbillede viser tydeligt, at cyberangreb ikke blot truer driften, men selve fundamentet for tilliden til den digitale infrastruktur, som samarbejdspartnere og kunder er afhængige af.

For NIS 2-omfattede virksomheder er det derfor en kritisk forudsætning at beskytte følsomme data og sikre stabiliteten i de systemer, som understøtter virksomhedens drift.

Teknologiske værktøjer er ikke nok i sig selv. NIS 2 gør det tydeligt, at sikkerhed kræver en ledelse, der:

- tager aktivt ansvar for cybersikkerheden
- arbejder strategisk og risikobaseret
- prioriterer den menneskelige faktor
- sikrer robuste, dokumenterede og forankrede cyberhygiejnepraksisser i hele organisationen

Med NIS 2 er cybersikkerhed ikke længere en teknisk disciplin alene — det er en integreret ledelsesopgave, som er afgørende for virksomhedens evne til at beskytte sine tjenester, data og sit omdømme.

## Ledelsesorganet i NIS 2

I henhold til NIS 2-lovens definitioner er det virksomhedens ledelsesorgan, der bærer det overordnede ansvar for cybersikkerheden. Det betyder, at det relevante ledelsesorgan som samlet enhed skal sikre udvælgelse, implementering og løbende opfølgning på de nødvendige cybersikkerhedstiltag. Dette ansvar gælder uanset, om konkrete sikkerhedsopgaver delegeres til et udvalg, en funktion eller en underliggende enhed. Ledelsesorganet har altid det endelige strategiske og juridiske ansvar for, at virksomheden efterlever NIS 2-kravene.

Følgende passager findes i vejledningen til ledelsens roller og ansvar på [Styrelsen for Samfundssikkerheds hjemmeside](#):

*I private virksomheder/organisationer er ledelsesorganet i NIS 2-loven defineret i overensstemmelse med definitionerne af henholdsvis det "centrale ledelsesorgan" i § 5, nr. 4 i Lov om aktie- og anpartsselskaber, jf. lovbekendtgørelse nr. 1168 af 1. september 2023 (selskabsloven) og "ledelsen" i § 4 a, nr. 2 i Lov om visse erhvervsdrivende virksomheder, jf. lovbekendtgørelse nr. 249 af 1. februar 2021 (LEV-loven).*

For virksomheder omfattet af selskabsloven er ledelsesorganet:

1. Bestyrelsen i selskaber, der har en direktion og en bestyrelse
2. Direktionen i selskaber, der alene har en direktion
3. Direktionen i selskaber, der både har en direktion og et tilsynsråd

For virksomheder omfattet af LEV-loven er ledelsesorganet:

1. Bestyrelsen i selskaber, der har en direktion og en bestyrelse
2. Direktionen i selskaber, der alene har en direktion
3. For de selskaber, der hverken har en bestyrelse eller en direktion, det ledelsesorgan, der har en kompetence, der svarer til den almindelige opfattelse af den kompetence, der tilkommer en bestyrelse eller en direktion

Den relevante definition afhænger af enhedens selskabsform. Selskabsloven finder alene anvendelse for aktie- og anpartsselskaber, mens LEV-loven gælder for erhvervsdrivende virksomheder, der ikke er omfattet af selskabsloven f.eks. enkeltmandsvirksomheder, interessentskaber, kommanditselskaber, andelsselskaber og fonde eller foreninger med erhvervsmæssig aktivitet. Det vil være op til den enkelte enhed at vurdere deres virksomhedskonstruktion ift. selskabsloven eller LEV-loven.

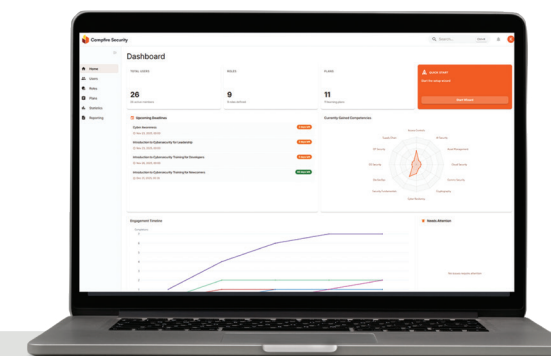
## 3. LØSNINGEN

# Lær "Hacker mindset" — og skab menneskelig modstandskraft

Campfire Securitys løsning er designet til at løfte organisationen fra en simpel compliance-tjekliste til reel menneskelig modstandskraft. Mens ledelsen styrkes gennem målrettede workshops, får medarbejderne adgang til en engagerende læringsplatform, hvor de får tildelt netop det indhold, de har brug for i deres rolle og funktion.

På platformen trænes medarbejderne i alt fra praktisk anvendelse af multifaktorautentificering (MFA) til forståelse af netværkssegmentering gennem "hackerens mindset", og med en indsigt i hackerens værktøjskasse. Ved at forstå, hvordan en angriber tænker, kan medarbejdere tænke sikkerhed ind i deres adfærd. Gennem et fokus på angiberens adfærd og intentioner, opbygges forståelse og viden til effektiv beskyttelse.

Campfire Securitys Cyber KPI rammeværk gør det muligt at dokumentere denne kompetenceudvikling sort på hvidt, og understøtter dermed dokumentationskravet i NIS 2. Gennem engagerende, praktisk, hands-on cybersikkerhedstræning bliver medarbejderne grundelementet i det stærkeste led i organisationens forsvar — nemlig en stærk cyberkultur.



# Build Strong Cyber Culture

Campfire Security er specialister i cybersikkerhedstræning. Vi leverer niveauet over den traditionelle awareness træning, hvor medarbejdere ser videoer og svarer på spørgsmål. Målgruppen er de medarbejdere, der opsætter systemer, tildeler adgange, udvikler tjenester, skaber forbindelser, bygger kode, laver integrationer, arbejder i cloud, anvender AI, og tilsvarende roller, der har brug for mere end videobaseret træning.

Med et fælles begreb kunne de kaldes IT udsatte, da det også inkluderer medarbejder i mange andre afdelinger end IT. IT udsatte findes i økonomiafdelingen, i administrationen, i udviklings- eller indkøbsafdelingen, og dækker også over medarbejdergrupper som projektledere, HR-medarbejdere og juridiske funktioner. Danske virksomheder, som i høj grad er digitaliserede, har et særligt cybersikkerhedsansvar, men besidder i mange situationer ikke de nødvendige cybersikkerhedskompetencer — men det kan der gøres noget ved.

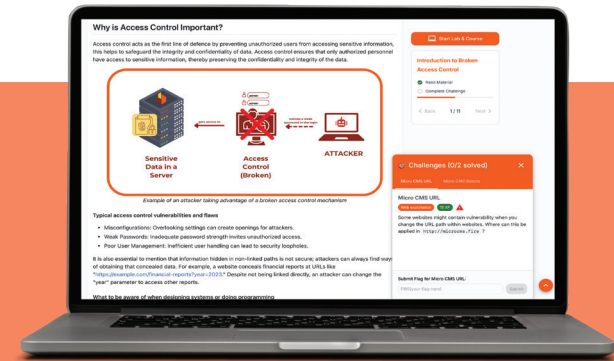
Ved at benytte Cyber KPI rammeværk opnås et ledelses-værktøj, som giver realtidsindsigt i organisationens erhvervede cybersikkerhedskompetencer. Enkelt, hurtigt og dokumenteret. Det er styringsværktøjet, som sikrer at ledelsen lever op til sit ansvar, og at de kan dokumentere det. Samtidigt er det værktøjet, der enkelt og effektivt støtter medarbejderne i etablering af de ønskede cybersikkerhedskompetencer. I Campfire Securitys unikke Cyber KPI rammeværk, findes netop det ledelsen i en dansk virksomhed underlagt NIS 2, har brug for.

Sammen kan vi bygge et stærkt fundament for jeres NIS 2-compliance.

## Vores platform

På vores læringsplatform kan vi opsætte tidsafgrænsede, rollespecifikke kursuspakker og tildele dem de medarbejdergrupper, som har brug for dem. Vi hjælper jer med at afdække jeres kompetencebehov og sammesætte pakkerne. Forløbene planlægges i et samarbejde med Campfire Security, så det sikres at både træningsmængde og periode passer til jer.

Vi har kursuspakker i alle former og størrelser, lige fra fagligt indhold til scenarie-baseret træning. Vores materiale kan sammensættes, så tidsforbruget ved hvert træningsforløb tilpasses jeres ønsker. Helt ned til 30 minutter.



I definerer træningsintervallet og det forventet tidsforbrug, og vi hjælper med at udvælge indholdet. Dermed sikres at medarbejdernes kompetenceløft bliver et supplement til deres daglige opgaver og at træningen bliver første skridt på vejen mod en stærk cyberkultur.

## 4. STRUKTURERET ROADMAP

# Vejen til dokumenteret sikkerhed

I nedenstående leveranceoversigt og Campfire Securitys fem-fasede roadmap kan det ses, hvordan I støttes i rejsen mod jeres NIS 2-compliance — og i etableringen af en stærk cyberkultur.

De fem faser, som præsenteres nedenfor, anbefales som ledelsens styringsværktøj til at eksekvere på organisationens politik for regelmæssig, dokumenteret cybersikkerhedsuddannelse.

### Leveranceoversigt

**Alignment & Ledelseskurser**  
Styrkelse af ledelsens beslutningskompetencer og fastlæggelse af de KPI'er, der skal rapporteres på.

**Rollebaseret Træning**  
Tilpasset indhold i læringsplatformen til de specifikke job-funktioner og risici i de enkelte medarbejdergrupperinger.

**Løbende Dokumentation**  
Gennem vores Cyber KPI rammeværk leveres den nødvendige dokumentation til at I kan bevise over for tilsynsmyndighederne, at I lever op til jeres ansvar under NIS 2 i relation til kravene om cybersikkerhedsuddannelse.

### Roadmap

| FASE                             | HANDLING                                                                                                                          | FORMÅL                                                                                                                                                         |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FASE 1:<br>Tilpasning og opstart | Indledende møde for at fastlægge mål og designe en kompetenceprofil for de relevante medarbejdergrupper med Cyber KPI rammeværket | Bygge fundamentet for etablering af en stærk cyberkultur                                                                                                       |
| FASE 2:<br>Forankring            | Etablering af klare KPI'er for de involverede ledere                                                                              | Sikrer at ansvaret for NIS 2-compliance placeres i hele organisationen — ikke bare hos IT                                                                      |
| FASE 3:<br>Ledelsestræning       | Gennemførelse af træning / keynotes for ledelsen                                                                                  | Opfylder NIS 2-kravet (§7) om ledelsesorganets kompetencer og ansvar beslutningskompetence indenfor cybersikkerhed                                             |
| FASE 4:<br>Engagement            | Udrulning af træning til organisationen, med fokus på praktisk erfaring inden for aftalte kompetenceområder                       | Opfylder NIS 2-kravet (§6) om grundlæggende cyberhygiejne og cybersikkerhedsuddannelse af medarbejdere, og styrker organisationens menneskelige modstandskraft |
| FASE 5:<br>Rapportering          | Løbende rapportering om deltagelse og kompetenceløft                                                                              | Levere den nødvendige dokumentation for kompetenceløft, til tilsynsmyndighederne og til dokumentation af egen progression                                      |

5.

NIS 2-LOVEN  
– KORT FORTALT

# NIS 2-loven og cybersikkerhedsuddannelse

NIS 2-loven stiller skærpede krav til ledelsen om sikring af et højt niveau af cybersikkerhed i organisationen. Ledelsesorganet skal deltage i relevante kurser om styring af cybersikkerhedsrisici og, at alle medarbejdere tilbydes tilsvarende træning. Derudover skal organisationen implementere grundlæggende cyberhygiejnepraksisser og etablere regelmæssig, dokumenteret cybersikkerhedsuddannelse tilpasset roller og risici for både ledelse og medarbejdere.

**Uddannelse til ledelse og medarbejdere**  
Et centralt element i NIS 2-loven er cybersikkerhedsuddannelse for både ledelse og medarbejdere.

NIS 2-loven stiller krav til cybersikkerhedsuddannelse på to niveauer – træning til ledelsesorganet og træning af medarbejdere.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>1. Kurser til ledelsesorganet (§7, stk. 2)</b></p> <p><i>§7. De foranstaltninger, som en væsentlig eller vigtig enhed træffer på baggrund af § 6, stk. 1 og stk. 2, og regler fastsat i medfør af §6, stk. 3, skal være godkendt af enhedens ledelsesorgan.</i></p> <p><i>Stk. 2: Ledelsesorganet skal deltage i relevante kurser om styring af cybersikkerhedsrisici og tilskynde til, at tilsvarende kurser tilbydes til enhedens øvrige ansatte.</i></p> | <p><b>2. Cybersikkerhedsuddannelse til medarbejdere (§6, stk. 1, nr. 7)</b></p> <p><i>§6. Væsentlige og vigtige enheder skal træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester.</i></p> <p><i>Foranstaltninger skal som minimum omfatte følgende:</i><br/>...<br/><i>7) Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse.</i></p> |
| <p>Formål:<br/>Gøre ledelsen i stand til at vurdere risici og træffe beslutninger om cybersikkerhedsforanstaltninger.</p>                                                                                                                                                                                                                                                                                                                                         | <p>Formål:<br/>Sikre at alle medarbejdere er trænet til at håndtere relevante sikkerhedsrisici og anvender cyberhygiejnepraksisser.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

Styrelsen for Samfundssikkerhed har derudover udgivet [en vejledning til implementering af cybersikkerhedsforanstaltninger](#), som kan understøtte forståelsen af, hvordan disse krav forventes imødekommet. Her defineres cybersikkerhedsuddannelse som:

At sikre at medarbejdere på alle niveauer er opmærksomme på, samt uddannet og trænet til at håndtere, relevante sikkerhedsrisici, samt kender og anvender almindelige cyberhygiejnepraksisser.

6.

NIS 2-LOVEN OG  
CAMPFIRE SECURITY

# NIS 2-loven og Campfire Security som strategisk partner

Nedenstående oversigt uddyber, hvordan Campfire Security fungerer som jeres strategiske partner i arbejdet med at efterleve NIS 2-lovens krav til ledelsens træning og ansvar (§7), samt medarbejdernes anvendelsen af og uddannelse i cybersikkerhedshygiejnepraksisser (§6).

Oversigten viser hvordan vi, i samarbejde med jer, kan imødekomme jeres behov inden for cybersikkerhedsuddannelse.

|  JERES BEHOV            |  VORES UNDERSTØTTELSE                                             |
|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Styrkelse af ledelsens cybersikkerhedskompetencer                                                          | Workshops, keynotes og løbende virtuel træning                                                                                                       |
| Etablering af cyberhygiejnepraksisser                                                                      | Giver jer kompetencerne til at udvælge, prioritere og vurdere praksisser                                                                             |
| Forankring af cybersikkerhedskultur                                                                        | Giver hele organisationen et fælles sprog og samme forståelse for cybertruslen, hackerne og deres metoder gennem vores læringsplatform               |
| Regelmæssig, opdateret træning i relevante sårbarheder, angrebsmetoder, trusler og cyberhygiejnepraksisser | Opdateret, forskningsbaseret læringsmateriale til dine medarbejdere                                                                                  |
| Rollebaseret og specifik sikkerhedsrelevant træning                                                        | Vores læringsplatform understøtter tildeling af specifik træning til grupperinger af individer, på tidspunkter som du styrer, bestemmer og redigerer |
| Dokumenter at medarbejdere har passende viden og færdigheder ift. rolle og risici                          | Gennem vores Cyber KPI rammeværk, giver vi dig den nødvendige indsigt og dokumentation                                                               |

## 7. I DYBDEN MED NIS 2-LOVEN

# NIS 2-loven

På de næste sider, har vi indsat de relevante passager fra vejledningerne og afsluttet med Campfire Securitys fortolkning af disse og de tilhørende lovkrav i relation til kravene om cybersikkerhedsuddannelse af ledelsesorganet.

## Ledelsens rolle og opgaver

*Der er ikke et specifikt form- og indholdskrav til kurserne, men uddannelseskravet skal ses i lyset af den rolle og de opgaver, ledelsesorganet har for cybersikkerheden i deres virksomhed eller myndighed efter NIS 2-lovens § 7, stk. 1. Kurserne skal således gøre ledelsen i stand til at vurdere risici og kunne træffe beslutning om og følge op på enhedens cybersikkerhedsforanstaltninger. Det er ikke et krav, at alle eller et bestemt antal medlemmer af ledelsesorganet skal have gennemført kurser.*

*Men ledelsesorganet skal som kollektiv have de fornødne kompetencer til at styre cybersikkerheden i enheden.*

*Ledelsen spiller en vigtig rolle for medarbejdernes kompetencer og adfærd. Ifølge § 7, stk. 2 i NIS 2-loven skal ledelsesorganet tilskynde til, at ansatte tilbydes kurser, svarende til dem, ledelsen selv gennemfører. Bestemmelsen skal ses i sammenhæng med § 6, stk. 1, nr. 7 i NIS 2-loven, som stiller krav om, at enheden skal have en politik for uddannelse af relevante medarbejdere.*

*Politikken efter § 6, stk. 1, nr. 7 skal sikre, at medarbejderne har viden og færdigheder om cyber- og informationssikkerhed, som er passende i forhold til deres rolle og ansvar.*

*Relevante kurser kan for eksempel være generelle kurser om cyber- og informationssikkerhed, ledelseskurser og workshops om styring af cyber- og informations-sikkerhedsrisici, kurser og certificeringer i anerkendte europæiske og internationale sikkerhedsstandarder eller enhedens egne internt tilrettelagte kurser og seminarer om cyber- og informationssikkerhed målrettet ledelsen. Uddannelsesaktiviteterne skal kunne dokumenteres f.eks. i form af kursusbevis eller bekræftelse på deltagelse i kursus.*

*Kravet om, at ledelsen skal tilskynde til, at ansatte tilbydes kurser, skal således ikke anses som et krav, der går videre end lovens § 6, stk. 1, nr. 7, men blot en understregning af, at medarbejdernes kompetencer og viden inden for cybersikkerhed er ledelsens ansvar.*

## Opsummering af Ledelsens rolle og opgaver

Campfire Security fortolker lovgivningen samt den tilhørende vejledning i relation til kravet om relevante cybersikkerhedskurser for ledelsesorganet til følgende overordnede pointer:

- Ledelsen skal deltage i relevante kurser om styring af cybersikkerhedsrisici
- Der er ingen form eller indholdskrav, men det skal matche den rolle og opgaver som ledelsen har i relation til cybersikkerheden
- Kurserne skal gøre ledelsen i stand til at vurdere risici og træffe beslutninger om cybersikkerhedsforanstaltninger
- Uddannelsesaktiviteterne skal kunne dokumenteres
- Ledelsen skal tilskynde til at ansatte tilbydes kurser tilsvarende dem ledelsen selv gennemfører
- Ledelsen skal sikre at medarbejdere har viden og færdigheder om cybersikkerhed, som er passende for medarbejderens roller og ansvar
- Medarbejdernes kompetencer og viden inden for cybersikkerhed er ledelsens ansvar



# NIS 2-loven

På de næste sider har vi indsat de relevante passager fra vejledningerne og afsluttet med Campfire Securitys fortolkning af disse og de tilhørende lovkrav i relation til kravet om cybersikkerhedsuddannelse af medarbejdere.

## Cyberhygiejnepraksisser og cybersikkerhedsuddannelse

§ 6. Væsentlige og vigtige enheder skal træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester.

Foranstaltninger skal som minimum omfatte følgende:  
...  
7) Grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse.

I vejledningen Implementering af cybersikkerhedsforanstaltninger findes følgende passager:

CYBERHYGIEJNEPRAKSISSE: At opretholde et passende niveau af cybersikkerhed gennem implementering af fundamentale foranstaltninger.

Cyberhygiejne dækker over de grundlæggende foranstaltninger og daglige sikkerhedsvaner, praksisser og procedurer, som beskytter netværk, systemer og data mod almindelige trusler. Dette indebærer blandt andet implementeringen af en række fundamentale foranstaltninger.

### 7.b - CYBERSIKKERHEDSUDDANNELSE:

At sikre, at medarbejdere på alle niveauer er opmærksomme på, og er uddannet og trænet til at håndtere, relevante sikkerhedsrisici, samt kender og anvender almindelige cyberhygiejnepraksisser (se afsnittet overfor).

Enheden skal udarbejde en politik for uddannelse af medarbejdere for at sikre, at de modtager netog informationssikkerhedstræning og uddannelse, der klæder medarbejderne på til at håndtere relevante sikkerhedsrisici og beskytte net- og informationssystemer. Uddannelse og træning skal etableres i overens-stemmelse med enhedens politik for informationssystem-sikkerhed, eventuelle emnespecifikke politikker og relevante procedurer for net- og informationssikkerhed.

Politikken kan eksempelvis indeholde beskrivelser af, hvilke arbejdsmæssige roller der kræver specifikke sikkerhedsrelevante færdigheder og ekspertise. Der kan etableres et egentligt uddannelses- og træningsprogram, som definerer den nødvendige uddannelse og træning for medarbejdere. Uddannelse og træning bør være relevant for medarbejderens jobfunktion, og programmets effektivitet bør vurderes.

Uddannelse og træning bør ske regelmæssigt og være dokumenteret samt tage hensyn til generelle foranstaltninger og kan blandt andet omfatte:

- instruktioner i og træning af gængse cyberhygiejnepraksisser, som bruges i enheden, såsom adgangsstyring, håndtering af opdatering af f.eks. mobile enheder, brug af passwords mv
- løbende orientering om kendte trusler, der er relevante for enheden og for medarbejdere (orienter f.eks. om forskellige relevante angrebsmetoder eller menneskelige sårbarheder (menneskelige bias), og tilpas orienteringen til medarbejdernes roller)
- uddannelse og træning i, hvad medarbejderes skal gøre, når der indtræffer hændelser (gør træningen konkret og handlingsorienteret — brug f.eks. scenarier, der tager udgangspunkt i enhedens risikovurdering og foranstaltninger). Grunduddannelse kan gælde for nye medarbejdere og for dem, der overgår til nye stillinger eller roller med væsentligt anderledes krav til net- og informationssikkerhed. Der er krav til, at ledelsesorganet skal deltage i relevante kurser, samt tilskynde til at tilsvarende kurser tilbydes til enhedens øvrige ansatte (NIS 2-loven § 7, stk. 2.).

# Opsummering af cyberhygiejnepraksisser og cybersikkerhedsuddannelese

Campfire Security fortolker lovgivningen samt den tilhørende vejledning i relation til relevante kravet om cyberhygiejnepraksisser og cybersikkerhedsuddannelse til følgende overordnede pointer:

- Organisationen skal opretholde et passende niveau af cybersikkerhed
- Cyberhygiejne dækker over grundlæggende foranstaltninger og sikkerhedsvaner, som beskytter netværk, systemer og data mod almindelige trusler
- Cyberhygiejne indebærer blandt andet vurdering af cybersikkerheden i forsyningskæder, regelmæssig patching, anti-malware-software, segmentering af netværk, kryptering af data, begrænsning af retigheder, anvendelsen af MFA, begrænsning af port og tjenesteanvendelse, fortegnelse over aktiver samt cybersikkerhedskultur og -bevidsthed gennem regelmæssig træning
- Cybersikkerhedsuddannelse er at sikre at medarbejdere på alle niveauer er uddannet og trænet til at håndtere relevante sikkerhedsrisici og kender samt anvender almindelige cyberhygiejnepraksisser
- Forskellige arbejdsmæssige roller kan kræve specifikke sikkerhedsrelevante færdigheder og ekspertise
- Uddannelses- og træningsprogram bør opdateres og gennemføres med regelmæssige mellemrum under hensyntagen til gældende politikker og regler, tildelte roller, ansvarsområder samt kendte trusler og teknologisk udvikling
- Der kan etableres et træningsprogram, som definerer den nødvendige uddannelse og træning for medarbejdere
- Træning bør være relevant for funktionen og træningens effektivitet bør vurderes
- Træning bør ske regelmæssigt og være dokumenteret
- Træning kan indebære instruktioner i eller træning af cyberhygiejnepraksisser i enheden, orientering og viden om kendte trusler, der er relevante for enheden og for medarbejderne samt træning og uddannelse i hvad medarbejdere skal gøre, når der indtræffer hændelser i organisationen
- Træning kan indeholde orientering om relevante angrebsmetoder eller menneskelige sårbarheder

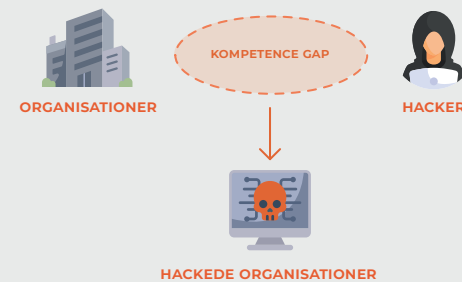
# VEJEN TIL EN STÆRK CYBERKULTUR

MED CAMPFIRE SECURITY

## 01

### VIDEN OM DET UVISSE

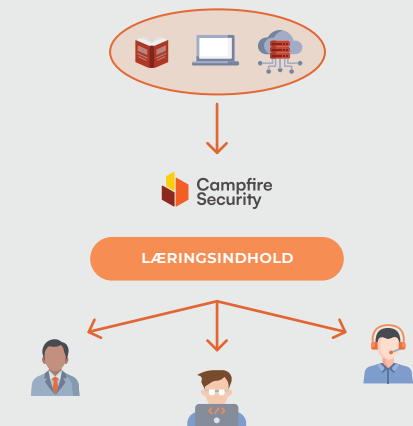
De fleste hackerangreb sker på baggrund af et hul mellem organisationers forståelse af sig selv og eget cybersikkerhedsbehov, og hackernes motiver, metoder og fremgangsmåde. Første skridt er derfor at etablere en fælles forståelse for udfordringen.



## 02

### UDDANNELSESPARAT

Sammen kortlægger vi jeres kompetencebehov og hjælper jer med at tildele lige præcis det læringsindhold, som I behøver – fordelt på de medarbejdergrupper, der mangler det.

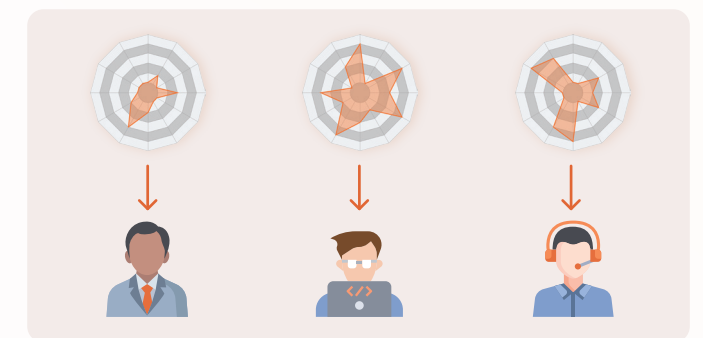
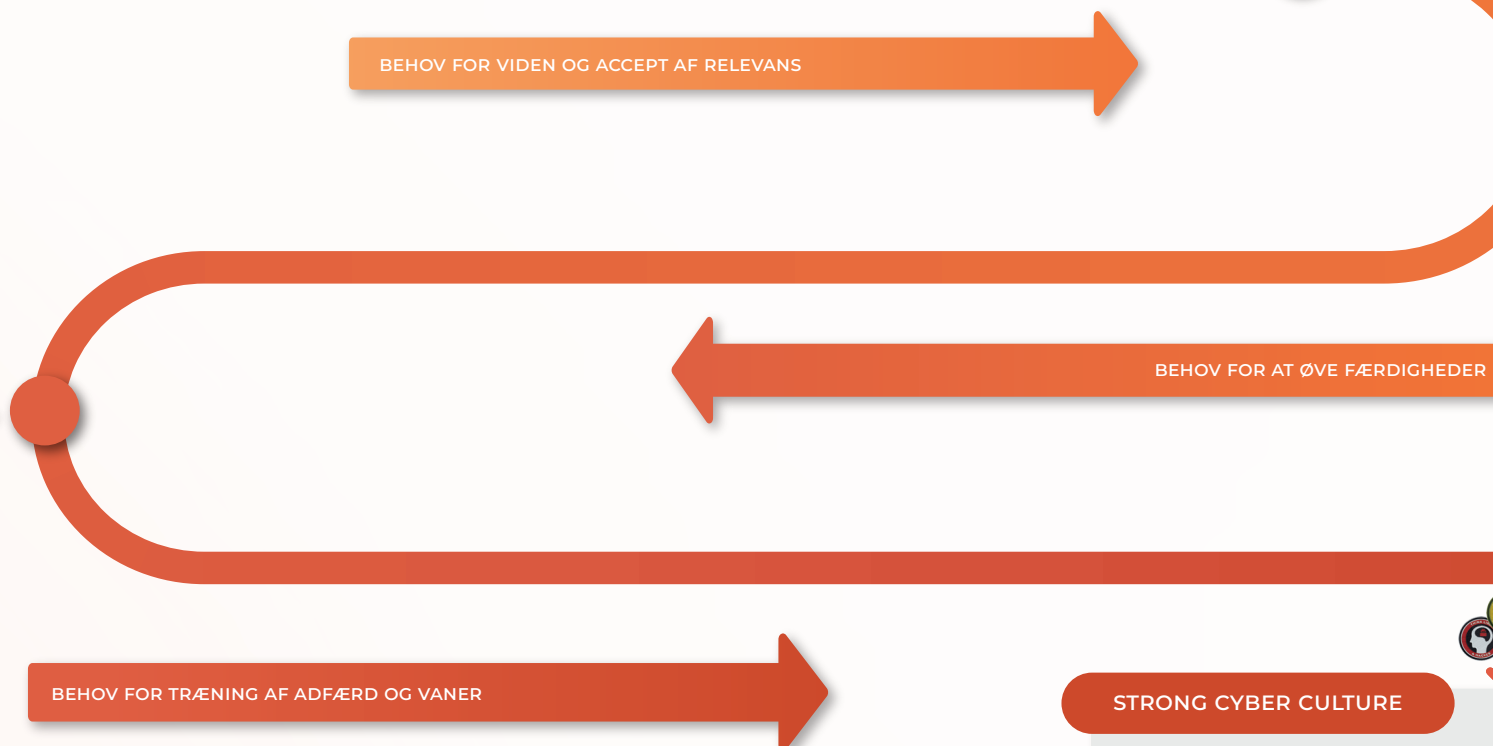


## 03

### KOMPETENCE-BEVIDST

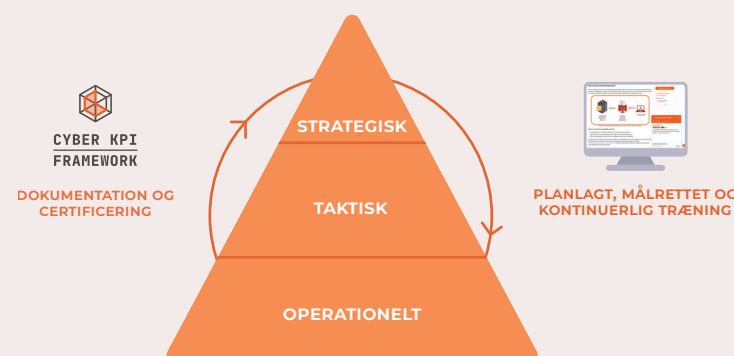
Den gennemførte træning kan nu rapporteres til ledelsen gennem det samme rammeværk, som er benyttet i tilrettelæggelsen af træningen.

Dokumentation og rapportering kan dermed anvendes til at styrke og forbedre den etablerede, kontinuerlige og målrettede træning. På den måde kombineres den strategiske målsætning med den operationelle udførsel.

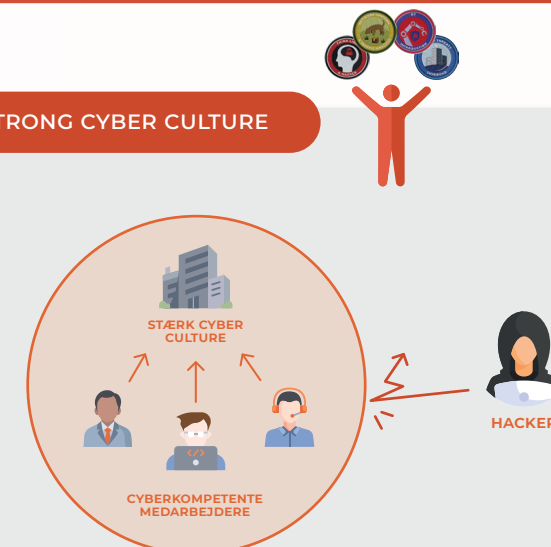


Vi designer jeres træning gennem udarbejdelsen af kompetenceprofiler i vores **Cyber KPI Framework**. På den måde kan vi sikre, at I får præcist de kompetencer som I efterspørger.

BEHOV FOR TRÆNING AF ADFÆRD OG VANER



STRONG CYBER CULTURE



## 04

### FORBEDRET CYBERKULTUR

Med ny forståelse, kontinuerlig, målrettet træning og konkret dokumentation, har I som organisation styrket jeres værn mod cyberangreb, gennem etablering og vedligeholdelse af en stærk cyberkultur.



## OM OS

Campfire Security er en dansk cybersikkerhedsvirksomhed med rødder i akademisk forskning. Vi specialiserer os i praktisk, hands-on træning og kompetenceudvikling i cybersikkerhed for professionelle og organisationer. Med vores interaktive, virtuelle laboratorier gør vi komplekse trusselsscenarier tilgængelige og engagerende, så medarbejdernes evne til at tænke som en angriber benyttes til at forbedre organisationens forsvarsevne.

Vores platform bygger og styrker cyberkultur, understøtter compliance og sikrer robuste færdigheder. Vi er dermed en del af løsningen på den stadig voksende mangel på kvalificeret cyberkompetencer og på den eskalerende cybertrussel.

## VORES TILGANG

Hos Campfire Security skaber vi læringsrum, hvor vi skifter tør teori ud med virkelighedsnære scenarier og hands-on øvelser. Gennem faglig indsigt og fælles refleksion rustes vi deltagerne til at handle hurtigt og klogt på moderne cybertrusler.

Vores mål er at opbygge den handlekraft og selvtillid, der skaber en stærk og modstandsdygtig cyberkultur i hele organisationen.

## KONTAKT OS

### CAMPFIRE SECURITY

 [campfiresecurity.dk/business](https://campfiresecurity.dk/business)

 [kontakt@campfiresecurity.dk](mailto:kontakt@campfiresecurity.dk)

 +45 33 13 13 37



### Dokumenteret fremgang

Målbare resultater, værdifuld indsigt og løbende rapportering sikrer, at I kan dokumentere de kompetencer I udvikler.



### Forskellige niveauer

Et stort udvalg af kurser gør det muligt, at udfordre dig på dit niveau inden for dine interesseområder.



### Baseret på forskning

Cybersikkerhedstræning blandet med akademisk forskning udviklet i et samarbejde med danske cyberfællesskaber.

