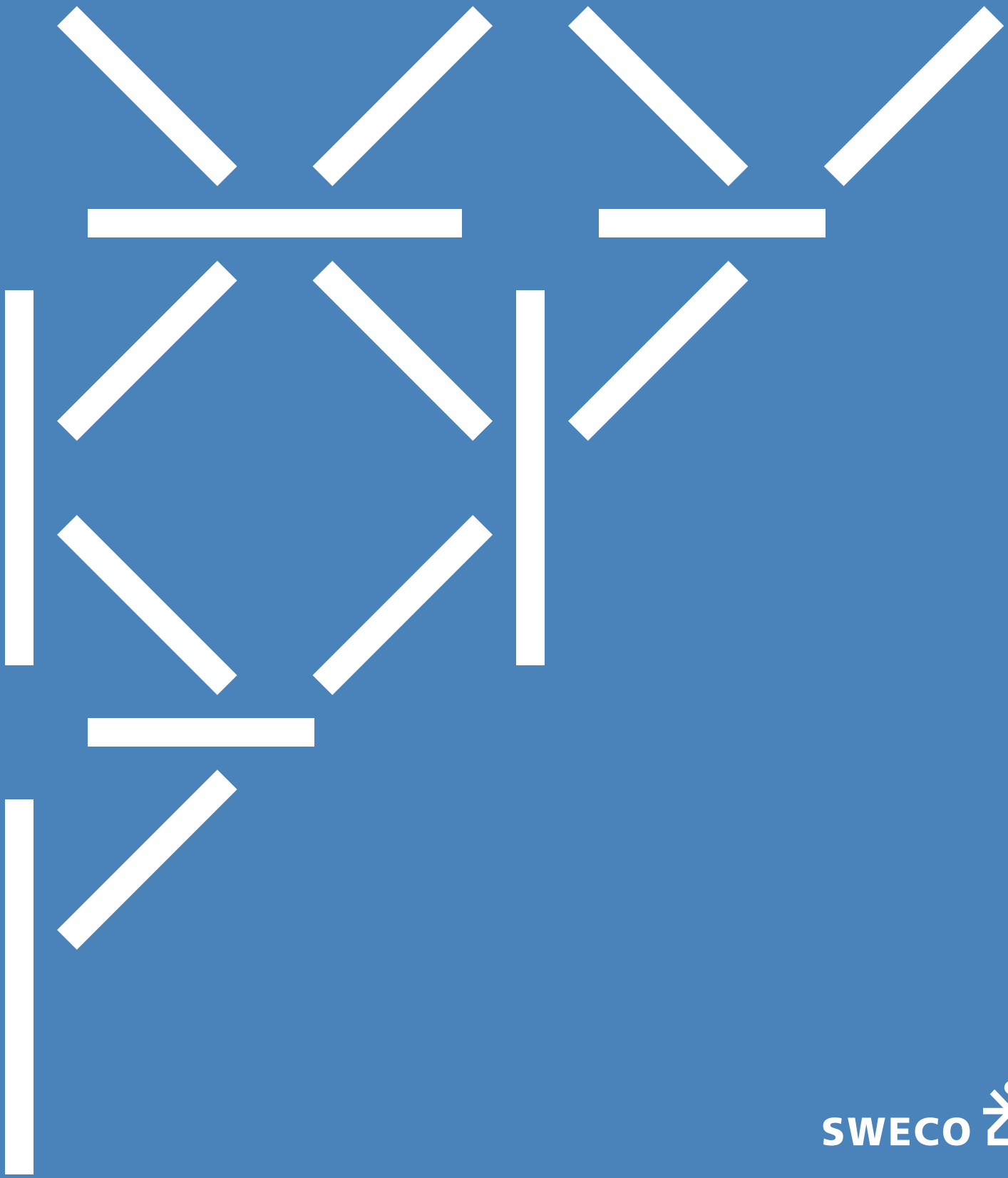
Cybersikkerhed

Pragmatiske løsninger på komplekse udfordringer



SWECO

“I en tid med stadigt større trusler er det afgørende for mig, at løsninger ikke kun opfylder lovgivningskrav, men bliver en naturlig del af organisationens cybersikkerhed”

Benno Nagbøl – Chef for Sikkerhed og Forsvar

En struktureret vej mod øget cybersikkerhed

Cybertrusler påvirker ikke kun én sektor, men udgør en fælles udfordring for danske virksomheder, offentlige institutioner samt kritiske områder som finans, sundhed, industri, transport og energi.

Med det stigende antal cyberangreb, skærpede nationale krav, EU-krav som NIS2-direktivet og internationale handelskrav fra eksempelvis USA, er behovet for en helhedsorienteret og effektiv tilgang til cybersikkerhed større end nogensinde.

Sikkerhed er komplekst, og én løsning passer ikke alle. Derfor har vi i denne publikation valgt at fokusere på tre nøgleområder, der er centrale for at styrke jeres cybersikkerhed og sikre konkrete og anvendelige tiltag:

— **Gap-analyser (ISO 2700x, NIST CSF)**
— **NIS2 Readiness**
— **Udvikling af et Cyber Roadmap**

Uanset om du repræsenterer en privat virksomhed, en offentlig organisation eller en anden interessent, vil disse områder være relevante for at sikre, at jeres arbejde med cybersikkerhed både er anvendelig, lever op til gældende standarder og er fremtidssikret.

Europas førende rådgiver

Om Sweco

Sweco er Europas førende rådgivningsvirksomhed med **22.000 eksperte**r, der udvikler løsninger inden for sundhed, industri, infrastruktur, energi, vand og samfund. Denne brede faglige erfaring giver os en unik kombination af teknisk ekspertise og strategisk indsigt – kompetencer, vi aktivt anvender, når vi rådgiver om sikkerhed, herunder både fysisk sikring og cybersikkerhed.

I Danmark har vi et dedikeret sikkerheds- og forsvarsteam bestående af erfarne specialister, der trækker på Swecos omfattende internationale netværk.

Vi kombinerer dyb teknisk viden inden for cybersikkerhed med en helhedsorienteret tilgang til strategisk planlægning og organisatorisk robusthed. Dette gør os i stand til at håndtere komplekse trusler, der spænder fra cyberangreb og datafortrolighed til fysisk sikring og kriseberedskab.

Hos Sweco ved vi, at sikkerhed handler om mere end teknologi – det handler om, hvordan mennesker, processer og systemer arbejder sammen. Vi tilpasser vores løsninger til de specifikke behov, vores kunder har, og sikrer, at de både lever op til lovgivningen og giver praktisk værdi.

Hvem er vores kunder?
Vi arbejder med organisationer på tværs af sektorer, herunder:

- Private virksomheder
- Offentlige institutioner
- Forsyningsselskaber
- Transport og infrastruktur
- Finanssektoren
- Industri og produktion
- Pharma
- Fødevareindustrien

Hvem er vi?

Hans Larsen – Cyber & Geopolitisk Chefspecialist
Hans Larsen har over 12 års international erfaring, primært fra den finansielle sektor og konsulentbranchen, med fokus på risikostyring og krisehåndtering. Hans' ekspertise inden for cybersikkerhed og geopolitik giver ham et skarpt analytisk blik for risikovurdering og håndtering på både strategisk og operationelt niveau.

Hans har stor erfaring med at udvikle løsninger, der både adresserer aktuelle udfordringer og forbereder organisationer på fremtidens behov. Han arbejder tæt sammen med kunderne for at identificere potentielle problemer tidligt og levere løsninger, der forbedrer deres sikkerhed og styrker organisationens modstandskraft.

"Min tilgang er altid proaktiv, pragmatisk og løsningsorienteret. Jeg arbejder tæt sammen med mine kunder for at identificere og håndtere potentielle problemer, før de bliver reelle trusler. Jeg hjælper med at implementere skræddersyede løsninger, der ikke kun beskytter mod aktuelle udfordringer, men også skaber et solidt fundament for fremtidens behov."

Benno Nagbøl – Chef for Sikkerhed og Forsvar
Benno Nagbøl er specialist i teknisk sikring og forsvar med over 20 års erfaring. Han har rådgivet om og implementeret løsninger til beskyttelse af bygninger, perimetersikring og beskyttelse mod tunge køretøjer. De senere år har han haft en central rolle i implementeringen og tilpasningen af NIS2- og CER-direktiverne for kritisk infrastruktur, hvilket har givet ham omfattende erfaring i at omsætte EU's krav til konkrete løsninger.

Hans tilgang fokuserer på praktisk anvendelighed, hvor han sikrer, at løsningerne fungerer effektivt i en kompleks og dynamisk verden, samtidig med at de imødekommer de strategiske behov for fremtidig sikkerhed.

"I en tid med stadigt større trusler er det afgørende for mig, at løsninger ikke kun opfylder lovgivningskrav, men bliver en naturlig del af organisationens cybersikkerhed. Jeg hjælper mine kunder med at forstå og implementere de komplekse krav fra NIS2- og CER-direktiverne, så de ikke blot overholder dem, men integrerer dem i deres daglige sikkerhedsarbejde."

Tre fokusområder, der styrker jeres sikkerhed og håndtering af risici

Cybersikkerhed er en central prioritet, men vi ved, at udfordringerne og behovene varierer alt efter organisationens størrelse, sektor og aktuelle sikkerhedsniveau. Derfor har vi udvalgt tre nøgleområder, der er relevante, uanset om du repræsenterer en privat virksomhed, en offentlig organisation eller en anden type interessent.

Gap-analyser (ISO 2700x, NIST CSF)
Vi analyserer jeres nuværende sikkerhedsniveau og vurderer, hvordan det står i forhold til både de relevante lovkrav og internationale standarder som ISO 2700x og NIST CSF. Denne analyse hjælper ikke kun med at identificere konkrete forbedringsområder, men giver også et klart billede af, hvordan I kan styrke jeres organisation for at håndtere både nuværende og fremtidige trusler effektivt.

Samtidig sikrer den, at I er i stand til at opretholde og forbedre jeres konkurrenceevne i en stadig mere kompleks og reguleret forretningsverden.

NIS2 Readiness
Med de skærpede krav i NIS2-direktivet, der gælder for alle organisationer, der arbejder med kritisk infrastruktur i EU, er det vigtigt at være forberedt på de kommende ændringer. Vores NIS2 Readiness hjælper jer med at forstå og implementere de nødvendige sikkerhedsforanstaltninger.

Vi tilbyder en grundig vurdering af jeres nuværende situation og udvikler skræddersyede handlingsplaner for at sikre, at I er i compliance med NIS2's krav, og kan beskytte jer mod fremtidige trusler.

Cyber Roadmap
En klar og konkret handlingsplan er nøglen til effektiv cybersikkerhed. Vi hjælper jer med at udvikle et Cyber Roadmap, der ikke kun tager højde for jeres strategiske mål, men også er tilpasset den konkrete virkelighed og de praktiske udfordringer, I står overfor.

Denne plan giver jer et langsigtet overblik, så I kan sikre en vedvarende og operationelt effektiv sikkerhedsindsats.

Foto: Nasa/Unsplash

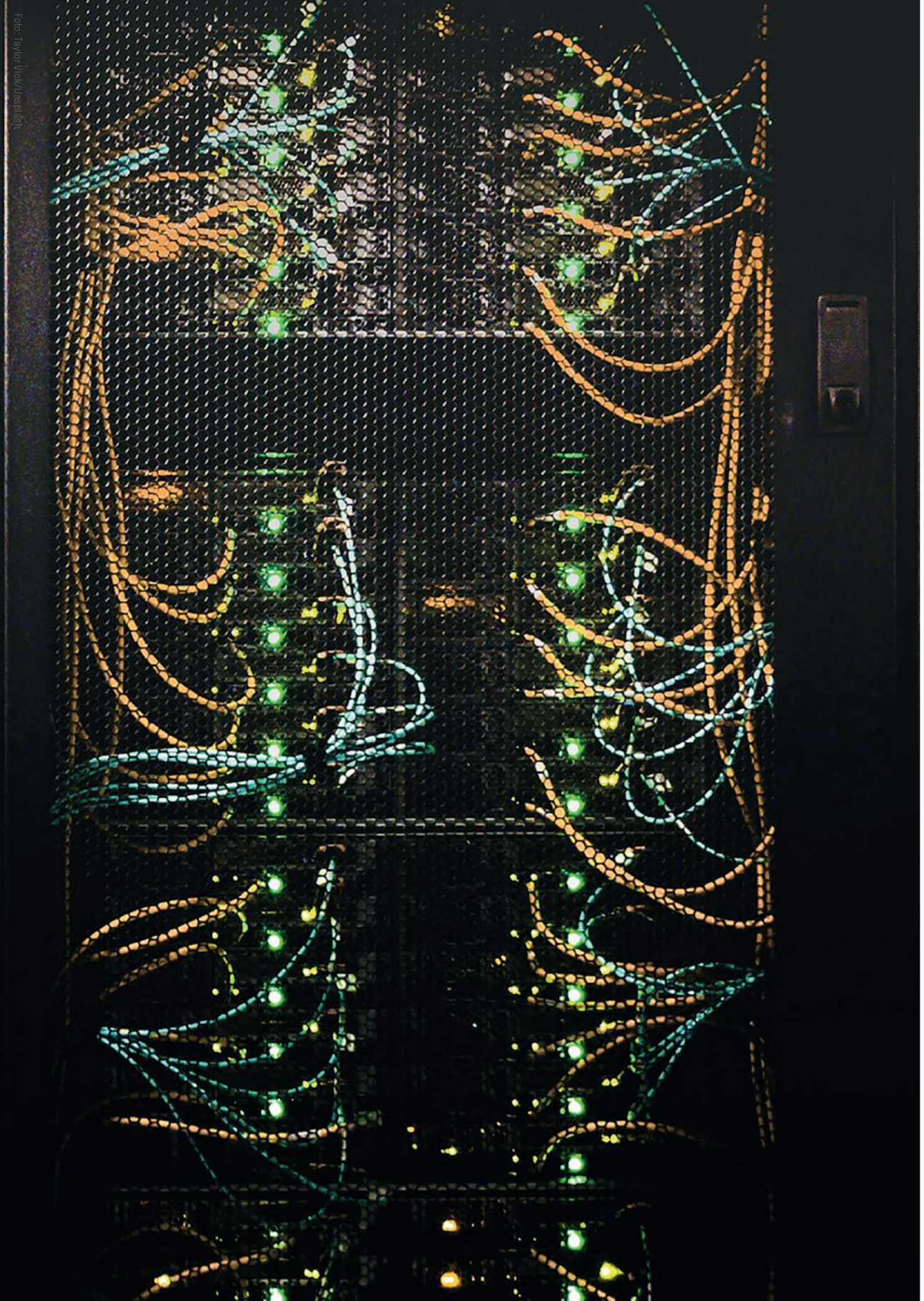


Foto: Taylor Vick/Unsplash

Gap-analyse ISO 2700x

Hvad er en ISO 2700x Gap-analyse?
Swecos ISO 2700x Gap-analyse er en pragmatisk vurdering, der identificerer forskelle mellem en organisations nuværende cybersikkerhedspraksis

og kravene i de relevante ISO 2700x-standarder. Denne analyse refererer til en række førende standarder, som vi benytter os af i denne proces, eksempelvis ISO 27001, 27002, 27005 og 27017.

Formålet med analysen er at afdække områder, hvor jeres organisation kan forbedre sin cybersikkerhed og risikostyring samt at sikre overholdelse af gældende reguleringer og bedste praksis inden for området.

Hvem er analysen relevant for?
Offentlig Sektor:
I den offentlige sektor fokuserer analysen på overholdelse af lovgivningsmæssige krav og beskyttelse af borgerdata. Resultatet giver en klar handlingsplan, der sikrer, at organisationen opfylder standarderne for informationssikkerhed og beskytter borgernes oplysninger.

Privat Sektor:
For private virksomheder er ISO 2700x gap-analysen en kritisk vurdering, der hjælper med at identificere sårbarheder og mangler i sikkerhedsforanstaltningerne. Målet er at forbedre datasikkerheden, reducere risici og sikre overholdelse af lovgivning og branchekrav. Dette beskytter ikke kun virksomhedens aktiver, men styrker også dens konkurrenceevne og omdømme på markedet.

Hvad får du ud af en gap-analyse?
Proaktiv risikohåndtering: Identifikation af svagheder, før de kan udnyttes.

Målrettet indsats: Fokus på de områder, hvor forbedringer gør størst forskel.

Forbedret tillid: Overensstemmelse af 2700x-standarderne styrker tilliden fra kunder og partnere.

Forberedelse på fremtidige trusler: Regelmæssige analyser sikrer, at I er klar til at håndtere nye udfordringer.

ISO 2700x gap-analysen i 5 faser
Identifikation: Vi kortlægger jeres specifikke krav og mål, så analysen bliver skræddersyet til jeres organisation.

Vurdering: Vi vurderer jeres nuværende ISMS (Information Security Management System) for at sikre overensstemmelse med 2700x og identificere eventuelle svagheder.

Evaluering: Vi analyserer jeres sikkerhedsmæssige modenhed gennem interviews, som tilpasses jeres præferencer (fysisk eller digitalt).

Rådgivning: Vi udarbejder en handlingsplan, der fokuserer på at lukke sikkerhedshuller og optimere jeres samlede sikkerhed.

Rapportering: Vi leverer en detaljeret rapport med et executive summary, som giver indsigt, der er anvendelig for både IT-afdelingen og ledelsen.

Priser fra: 74.995 DKK ex. moms.

Foto: NASA/Unsplash

Gap-analyse NIST CSF

Hvad er en NIST CSF gap-analyse?
NIST Cybersecurity Framework (CSF) er et anerkendt rammeværk udviklet af National Institute of Standards and Technology (NIST) i USA. Det hjælper organisationer med at forbedre deres cybersikkerhed ved at identificere, beskytte, opdage, reagere på og håndtere cybertrusler.

En NIST CSF Gap-analyse hjælper med at vurdere og styrke jeres cybersikkerhed i overensstemmelse med disse internationale krav. Den sikrer, at jeres organisation kan identificere risici og svagheder i forhold til NIST CSF-kravene og udvikle løsninger, der gør jeres cybersikkerhed mere robust og fremtidssikret. Denne analyse hjælper jer med at opfylde både amerikanske og internationale standarder og styrker jeres position på det globale marked.

Hvem er analysen relevant for?
NIST CSF er særligt relevant for virksomheder og organisationer, der samarbejder med eller har forretning med amerikanske partnere. Det hjælper dem med at overholde amerikanske cybersikkerhedsstandarder og styrker tilliden hos både amerikanske kunder og samarbejdspartnere.

Er man en del af forsyningskæden til den amerikanske regering, er det nødvendigt at forholde sig til NIST CSF. Federal agencies og deres leverandører, herunder kontraktpartnere, er forpligtet til at overholde NIST CSF som en del af deres kontraktlige forpligtelser. Rammeværket giver disse organisationer et fælles sprog og et konkret sæt cybersikkerhedspraksisser, der kan forbedre deres cybersikkerhedsniveau og beskytte kritisk infrastruktur.

Hvad får du ud af en NIST CSF gap-analyse?
Compliance med amerikanske standarder: Vurderingen sikrer, at din organisation opfylder de nødvendige krav i NIST CSF, som er afgørende for samarbejde med amerikanske aktører.

Styrket cybersikkerhed: Vi identificerer svagheder og hjælper med at udvikle løsninger, der beskytter organisationens kritiske systemer og data.

Opbygning af tillid: Overholdelse af NIST CSF-standarderne styrker relationerne med internationale partnere, særligt i USA, og viser en stærk forpligtelse til cybersikkerhed.

NIST CSF gap-analyse i 5 faser:
Identifikation: Vi kortlægger jeres specifikke behov i forhold til NIST CSF og jeres mål, især i relation til samarbejde med amerikanske aktører.

Vurdering: Vi vurderer jeres nuværende cybersikkerhedsmodenhed ved at analysere jeres eksisterende sikkerhedsforanstaltninger i forhold til de fem funktioner i NIST CSF: Identify, Protect, Detect, Respond og Recover.

Evaluering: Vi samler data og gennemfører interviews for at få en detaljeret forståelse af jeres cybersikkerhedslandskab, som kan tilpasses jeres behov (fysisk eller digitalt).

Rådgivning: Vi udarbejder en handlingsplan, der fokuserer på at adressere identificerede svagheder og sikre, at I opfylder NIST CSF-kravene.

Rapportering: Vi leverer en detaljeret rapport med anbefalinger og en executive summary, som giver indsigt, der er anvendelig både for ledelsen og IT-afdelingen.

Priser fra: 79.995 DKK ex. moms.

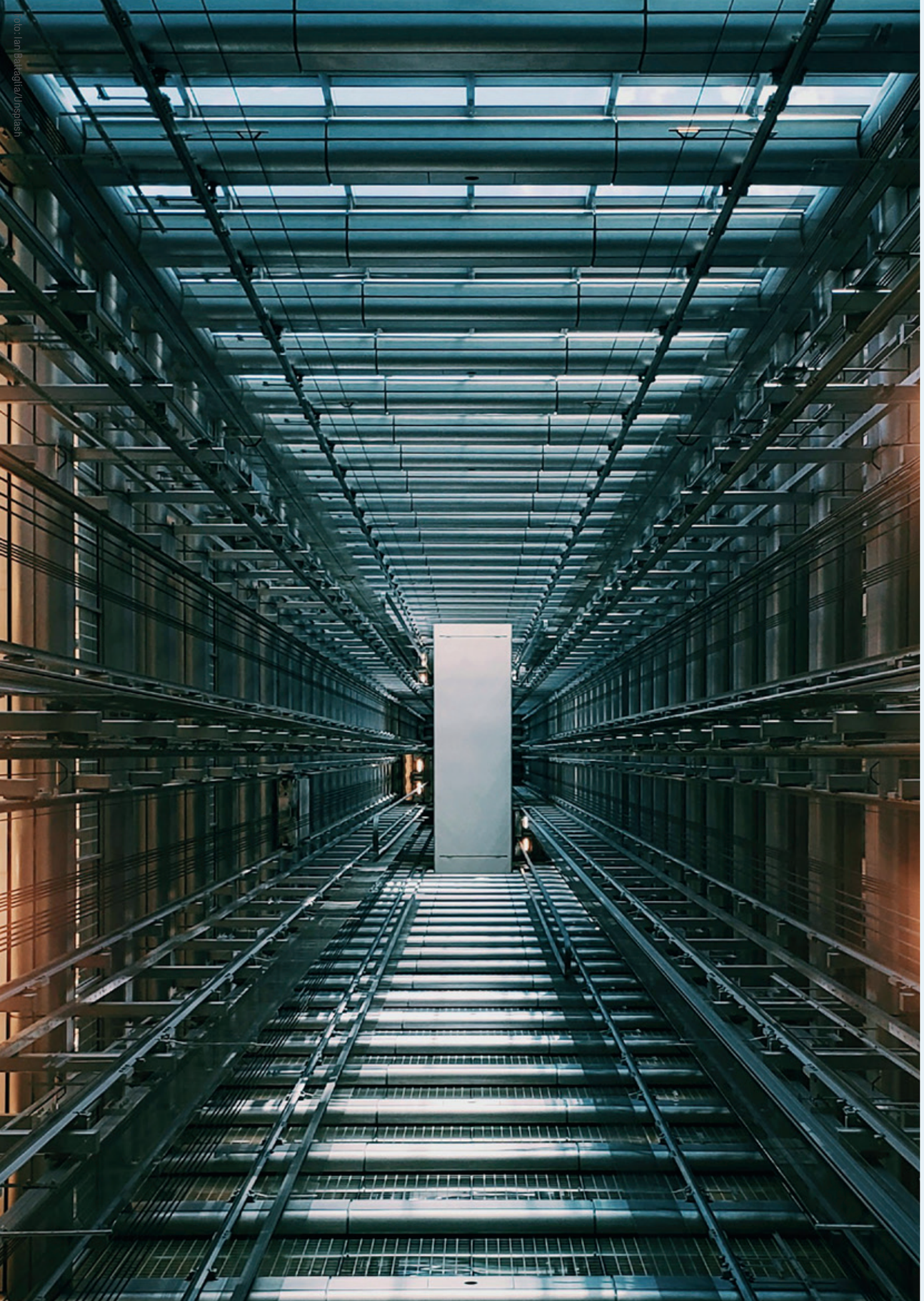


Foto: Ian Battaglia/Unsplash

NIS2 Readiness

Hvad er en NIS2 Readiness-vurdering?
En NIS2 Readiness-vurdering er en essentiel proces for jeres organisation. Den sikrer, at I er klar til at opfylde de skærpede krav i NIS2-direktivet – et EU-regulativ, der stiller høje krav til cybersikkerhed. Direktivet er relevant for sektorer som energi, transport, sundhed og vandforsyning samt for digitale tjenester som cloud-løsninger og data-centre. Det gælder også offentlige myndigheder og telekommunikationsselskaber, der håndterer kritisk infrastruktur og data.

Ved at gennemføre en NIS2 Readiness-vurdering kan I identificere og lukke sikkerhedshuller, minimere risici og sikre, at jeres organisation lever op til de nye krav. Dette er ikke kun nødvendigt for at undgå sanktioner, men også en strategisk investering i jeres fremtidige cybersikkerhed.

Hvem er vurderingen relevant for?
NIS2 Readiness er relevant for:

- Virksomheder, der arbejder med kritisk infrastruktur
- Offentlige myndigheder og organisationer, der ønsker at sikre, at deres sikkerhedsforanstaltninger opfylder de nye EU-krav
- Organisationer, der ønsker at styrke deres cybersikkerhed og fremme en kultur af kontinuerlig forbedring i forbindelse med NIS2

Hvad får du ud af en NIS2 Readiness vurdering?
Proaktiv compliance: Sikrer, at jeres organisation er forberedt på de krav, som NIS2-direktivet stiller.

Risikoafdækning: Identifikation af potentielle risici og udvikling af handlingsplaner for at håndtere dem, før de bliver et problem.

Strategisk forbedring: Fokus på de vigtigste områder, der kræves for at opnå og opretholde compliance med NIS2.

Styrket sikkerhed: Skaber et robust sikkerhedsberedskab, der kan beskytte organisationen mod fremtidige trusler.

NIS2 Readiness i 5 faser
Identifikation: Vi starter med at afklare jeres specifikke behov og mål for at sikre, at vurderingen er skræddersyet til jeres organisation.

Vurdering: Vi udfører en dybdegående evaluering af jeres nuværende sikkerhedsstyring for at vurdere overensstemmelse med NIS2 og identificere eventuelle risici eller mangler.

Evaluering: Vi vurderer jeres sikkerhedsmæssige beredskab gennem interviews, der kan udføres fysisk eller digitalt, afhængig af jeres behov og præferencer.

Rådgivning: Vi udvikler en handlingsplan, der fokuserer på at adressere eventuelle gaps, reducere risici og sikre, at NIS2 kravene bliver overholdt effektivt.

Rapportering: Vi leverer en detaljeret rapport, der giver værdifuld indsigt og anbefalinger til ledelsen og IT-afdelingen, og muliggør en effektiv implementering af NIS2 compliance.

Priser fra: 84.995 DKK ex. moms.

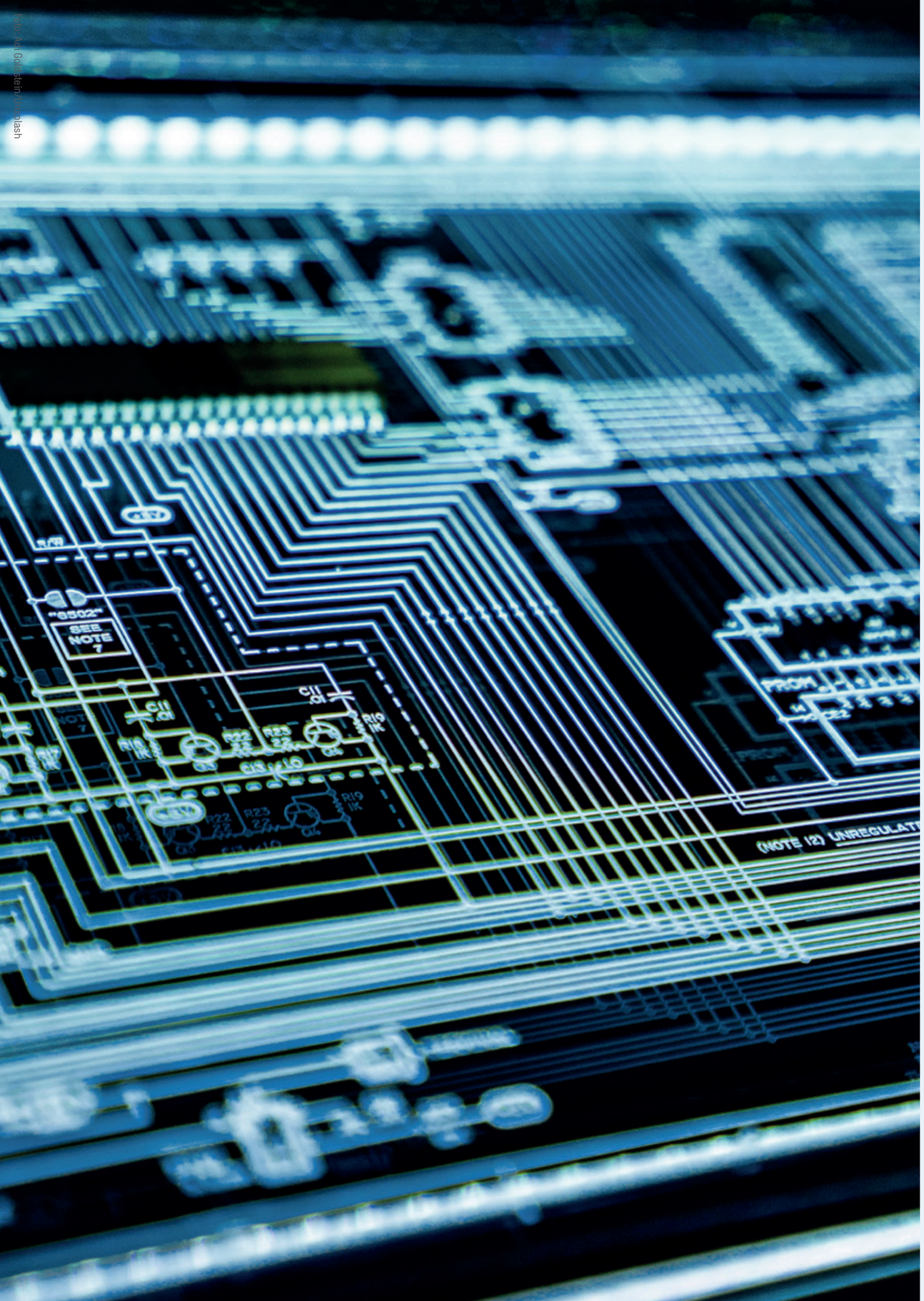


Foto: Ali Gohstein/Unsplash

Cyber Roadmap

Hvad er et Cyber Roadmap?
Et Cyber Roadmap giver din organisation en strategisk plan for cybersikkerhed, der sikrer, at I er godt forberedt på fremtidige trusler og risici. Det hjælper med at prioritere de nødvendige sikkerhedsforanstaltninger, allokere ressourcer effektivt, og implementere langsigtede løsninger, der beskytter kritiske data og systemer.

Roadmap'en guider jer gennem de nødvendige skridt for at opnå en robust cybersikkerhedsinfrastruktur, der er tilpasset jeres forretningsmål og risikoprofil.

Hvem er Cyber Roadmap relevant for?
Cyber Roadmap er relevant for:

- Virksomheder, der ønsker at udvikle en langsigtet cybersikkerhedsstrategi.
- Offentlige myndigheder og organisationer, der er ansvarlige for beskyttelse af kritisk infrastruktur.
- IT-afdelinger, der har brug for en klar og struktureret plan for fremtidig cybersikkerhed.
- Organisationer, der vil optimere og styrke deres nuværende cybersikkerhedsinfrastruktur.

Hvad får du ud af et Cyber Roadmap?
Vores Cyber Roadmap leveres visuelt og pragmatisk, hvilket giver et klart overblik, der både kan bruges i dialog med top-ledelsen og som et solidt fundament for IT-ledelsen. Roadmap'et hjælper organisationen med at implementere cybersikkerhed strategisk og effektivt på tværs af niveauer.

Strategisk retning: En tydelig plan for cybersikkerhed, der er i overensstemmelse med organisationens langsigtede mål.

Prioritering af indsatsområder: Fokus på de mest kritiske områder, der kræver forbedring, for at styrke organisationens sikkerhed.

Effektiv ressourceplanlægning: Hjælp til at allokere ressourcer og investeringer på de områder, der giver størst værdi i forhold til cybersikkerhed.

Fremtidssikret cybersikkerhed: Et roadmap, der hjælper med at sikre, at organisationen er forberedt på at modstå fremtidige trusler og cyberangreb.

Cyber Roadmap i fem faser
Identifikation: Vi starter med at afklare jeres mål, behov og nuværende cybersikkerhedsforhold for at skræddersy roadmap'en til jeres organisation.

Vurdering: Vi gennemgår og vurderer jeres nuværende cybersikkerhedsforanstaltninger, herunder eventuelle svagheder og risici.

Evaluering: Vi analyserer, hvilke områder der kræver forbedring, og udarbejder en prioriteret liste af indsatsområder.

Rådgivning: Vi udvikler en handlingsplan og roadmap med konkrete skridt, tidslinjer og ressourcebehov for at nå jeres cybersikkerhedsmål.

Rapportering: Vi leverer en detaljeret roadmap, der indeholder en strategisk oversigt og anbefalinger, som kan implementeres effektivt i organisationen.

Priser fra: 82.995 DKK ex. moms.

Bliv klogere på alle vores kompetencer

Hos Sweco Security and Defence tilbyder vi en bred vifte af ekspertise inden for forsvar og sikkerhed, der strækker sig langt ud over cybersikkerhed. Vi er jeres one-stop shop for 360 graders sikkerhedsrådgivning, hvor I kan samle alle jeres behov under ét tag. Kontakt os for at høre, hvordan vi kan hjælpe jer med at optimere jeres sikkerhedsstrategi

Vores rådgivning omfatter bl.a.:

Sikkerhed til alle slags bygninger og enheder

Vi har omfattende erfaring, bred viden og løser alle vores kunders behov inden for fysisk sikring og sikkerhedssystemer - fra forundersøgelse over projektering og udbud til tilsyn, kontrol og idriftsættelse. Vi har opbygget en specialiseret viden inden for terrorsikring, detekteringssystemer og den yderste perimeter-sikring, som danner grundlaget for at bygherren har fuld kontrol over det sikrede område.

Fysisk sikkerhed op imod standarder

Vi sørger for at din virksomhed lever op til EU-direktiver samt relevante branchestandarder.

ISPS-rådgivning og havnesikkerhed

Som godkendt Recognized Security Organization (RSO) fra Trafikstyrelsen rådgiver vi om sårbarhedsvurdering og sikkerhedsplaner for havnefaciliteter.

Sikkerhed i infrastrukturelle projekter

Fra vurdering til implementering af sikkerhedsforanstaltninger i transportinfrastruktur og større byggeri, med fokus på både praktiske og lovgivningsmæssige krav.

Business Continuity og Crisis Management Live Exercises

Vi tilbyder omfattende træningsprogrammer inden for Business Continuity og Crisis Management, som er skræddersyet til at forberede jeres organisation på at håndtere uforudsete hændelser og krisesituationer. Gennem deltagelse i vores live øvelser kan I sikre, at jeres organisation er optimalt rustet til at tackle enhver form for krise, samtidig med at I opretholder kontinuiteten i jeres forretningsaktiviteter.

Business Continuity Live Exercises

Formål: At sikre, at jeres organisation kan opretholde kritiske funktioner både under og efter en krise.

Indhold: Realistiske scenarier, der tester jeres beredskabsplaner og evne til at opretholde driften under forskellige typer forstyrrelser, såsom ransomware-angreb, misinformationkampagner og naturkatastrofer.

Resultat: Identifikation af svagheder i jeres nuværende planer og procedurer samt konkrete anbefalinger til forbedringer.

Crisis Management Live Exercises

Formål: At træne jeres ledelsesteam i effektiv krisehåndtering og beslutningstagning under pres.

Indhold: Simulerede krisesituationer, der kræver hurtig og koordineret respons fra alle involverede parter. Scenarier inkluderer håndtering af ransomware-angreb, misinformationkampagner og naturkatastrofer.

Resultat: Forbedret kriseberedskab, styrket evne til at minimere skader og hurtigere genopretning af normal drift.

“Jeg arbejder tæt sammen med mine kunder for at identificere og håndtere potentielle problemer, før de bliver reelle trusler”

Hans Larsen – Cyber & Geopolitisk Chefspecialist

Kontakt

Hans Larsen

Cyber & Geopolitisk Chefspecialist

hans.larsen2@sweco.dk
+45 4282 1518

Benno Nagbøl

Chef for Sikkerhed og Forsvar

benno.nagbol@sweco.dk
+45 4282 1020

Sweco Danmark A/S
Ørestads Boulevard 41
DK-2300 København S
Tel +45 72 20 72 07

www.sweco.dk