Securitas

Securitas Danmark

# NIS2 & CER for kritisk infrastruktur



Forstå den nye lovgivning, hvem den kommer til at påvirke, og hvordan det berører jeres sikkerhedsløsninger.

# Tryghed på tværs af Danmark



**Global viden.**
**Lokalt kendskab.**
**Landsdækkende tryghed.**

Med over 10.000 erhvervskunder på tværs af landet, 109 patruljebiler på vejene døgnet rundt og 17 vagtstuer strategisk placeret rundt omkring, er der altid en vagt i nærheden – uanset hvor din virksomhed ligger.

Alle vores vagter og patruljebiler er udstyret med GPS og digitale rapporteringssystemer, så du får opdateringer i realtid. Det giver dig et klart overblik – og tryghed at vide, at vi reagerer med det samme.

## Indhold


Introduktion ..... 5
Et nyt trusselsbillede i udvikling ..... 7
Hvad er NIS2 og CER?..... 9
CER ..... 10
Gælder CER os? .....12
Berørte sektorer .....14
Krav til sikkerhed under CER .....17
Ansvar og konsekvenser ved manglende overholdelse.....18
Fysisk sikring til NIS2-omfattede virksomheder .....20
Når video bliver en digital svingdør .....22
Fysiske sikkerhedssystemer er en cyberrisiko .....23
De 6 vigtigste it-spørgsmål til din sikkerhedsleverandør.....25
Robusthed og resiliens.....28
Hvad kontinuerlig drift kræver i praksis .....30
Sikker drift afhænger også af leverandørerne .....34
Gratis skabelon og spørgsmål til jeres egen risikovurdering .....35
Mød vores sikkerhedsrådgivere .....40
Konklusion .....46

# Introduktion



Med CER og NIS2 bevæger arbejdet med sikkerhed, kontinuerlig drift og robusthed sig nu ind i en mere praktisk fase. For mange virksomheder betyder det, at krav til driftssikkerhed, risikostyring, dokumentation og beredskab skal omsættes til konkrete processer, prioriteringer og foranstaltninger.

Samtidig er der fortsat betydelig usikkerhed. De endelige bekendtgørelser foreligger endnu ikke, og det skaber tvivl om, hvordan kravene konkret skal forstås, hvem der bliver direkte omfattet, og hvordan virksomheder bedst forbereder sig.

Men usikkerheden ændrer ikke på behovet for handling. Tværtimod. Når bekendtgørelserne er på plads, vil mange virksomheder på kort tid skulle omsætte kravene til konkrete tiltag. Jo længere forberedelserne udskydes, desto mindre bliver råderummet til at implementere dem grundigt og rettidigt.

Forberedelserne handler blandt andet om at identificere de mest kritiske funktioner, kortlægge de afhængigheder, der understøtter dem, vurdere hvilke hændelser der kan forstyrre den kontinuerlige drift væsentligt, og dokumentere virksomhedens evne til at forebygge, håndtere og lære af afvigelser.

Nogle virksomheder vil blive direkte omfattet af CER og NIS2. Andre vil møde kravene gennem kunder, kontrakter og samarbejdspartnere, der efterspørger dokumentation for robusthed, kontinuerlig drift og driftssikkerhed på tværs af leverandørkæden.

Derfor er vi allerede nu i tæt dialog med blandt andet energisektoren, som allerede er omfattet af særskilt regulering, samt med virksomheder, der forventes at blive omfattet af CER. Magasinet bygger på de erfaringer og behov, vi møder i disse samarbejder.

Formålet er at give et mere praktisk og anvendeligt grundlag for arbejdet med CER med afsæt i de udfordringer, der allerede nu tegner sig på tværs af sektorer, mens vi fortsat afventer de endelige bekendtgørelser.

*Sune Dellgren, redaktør, Securitas Danmark*

# Et nyt trusselsbillede i udvikling



Michael Evans

Chef for Risk Intelligence Center i Securitas



**Den globale politiske uro, blandt andet den første store krig i Europa i over 70 år, har øget truslen mod virksomheder og organisationer, der driver samfundskritisk infrastruktur. NATO vurderer nu sabotage mod kritisk infrastruktur som en af de største sikkerhedstrusler.**

Forsøg på at forstyrre kritisk infrastruktur sker i dag ofte som såkaldte hybride angreb. Det betyder angreb, hvor flere metoder blandes sammen – for eksempel digitale angreb, fysisk sabotage, tyveri eller påvirkning gennem medier og information. Det er en udvikling, der går hurtigt.

Hybride angreb kan bevæge sig på tværs af landegrænser lige så hurtigt som data og nyheder spredes. Digitaliseringen har gjort det muligt at angribe flere steder end tidligere, men de fysiske risici er også blevet mere avancerede. Det kan for eksempel være indtrængen på sikrede områder eller droner, der går efter el-stationer og anlæg, som ligger langt væk.

Det er vigtigt at kortlægge, hvad man er afhængig af, sprede sine leverandører og sørge for backup-løsninger i vigtige systemer. Men det virker kun, hvis det går hånd i hånd med samlet sikkerhed og risikostyring, der kan opdage, bekræfte og reagere på trusler med det samme.

Mike Evans, chef for Risk Intelligence i Securitas, siger:

"I dag har alle typer trusselsaktører en grund til at gå efter kritisk infrastruktur. Selv simple former for sabotage og tyveri kan føre til alvorlige driftsstop. Nogle trusler er nu reelt uden grænser, fordi moderne infrastruktur hænger så tæt sammen på tværs af lande og sektorer. Trusler mod kritisk infrastruktur respekterer ikke geografi. Den hastighed, problemer kan sprede sig med, er i sig selv en risiko. Vores råd til virksomhedsledere er, at overvågning af regionale risici i realtid bør være en topprioritet."

Evnen til at have et klart situationsbillede er derfor afgørende. Organisationer, der samler fysiske data – som videoovervågning, adgangslogfiler og patruljedata – med digitale advarselssignaler og ekstern viden om trusler, kan hurtigere bekræfte hændelser og reagere på dem. Det kan mindske konsekvenserne både for driften og for samfundet.



# Hvad er NIS2 og CER?

### NET- OG INFORMATIONS-SIKKERHEDSDIREKTIVET (NIS2)

NIS2 skærper kravene til cybersikkerhed og udvider kredsen af omfattede sektorer og virksomheder.

Enheder omfattet af reglerne inddeles som *væsentlige* eller *vigtige*, men begge skal leve op til skærpede krav til risikostyring, sikkerhedsforanstaltninger og hændelseshåndtering.

I Danmark er NIS2 gennemført i NIS2-loven, og tilsynet varetages af de kompetente myndigheder på tværs af sektorer.

### CRITICAL ENTITIES RESILIENCE-DIREKTIVET (CER)

CER skal sammen med NIS2 styrke modstandsdygtigheden i kritiske enheder. Hvor NIS2 retter sig mod cyber- og informationssikkerhed, fokuserer CER på robusthed i bredere forstand – herunder fysisk beskyttelse, risikovurdering, hændelseshåndtering og genopretning ved fx sabotage, naturhændelser og andre driftsforstyrrelser.

I Danmark er CER gennemført i CER-loven, og tilsynet varetages af de kompetente myndigheder på tværs af sektorer.

### VIGTIGE DATOER FOR CER

- I Danmark trådte CER-loven i kraft 1. juli 2025.
- Kritiske enheder skal identificeres senest 17. juli 2026. De berørte virksomheder skal underrettes af myndighederne senest én måned efter identifikationen.
- 9 måneder efter underrettelsen skal kritiske enheder have en risikovurdering på plads.
- 10 måneder efter underrettelsen skal kritiske enheder leve op til kravene i CER-loven.

# 1

# **CER -** Critical Entities Resilience




> “Hvis virksomheden ikke har taget aktivt stilling til sine risici, har den i praksis accepteret en nedetidsrisiko uden at vide, om økonomien kan bære det.

Klaus Jensen, HSEQ Business Partner,
Securitas Danmark

# Gælder CER os?

**Det er et af de spørgsmål, der fylder mest lige nu hos virksomheder med samfundskritiske funktioner – og i stigende grad også hos dem, der leverer ydelser, teknologi og komponenter til kritisk infrastruktur.**



Claus Fibiger

Adm. direktør, Securitas Danmark

**Men for mange er det også det forkerte sted at starte.**

CER handler grundlæggende om at styrke resiliensen i kritiske enheder og i de funktioner, som samfundet er afhængigt af. I praksis betyder det, at nogle virksomheder kan blive mødt af stigende forventninger til beredskab, driftssikkerhed og dokumentation – både fra myndigheder og kunder, fordi deres funktioner er vigtige for andres drift.

“Det vigtigste spørgsmål er sjældent, om man formelt er omfattet, men hvad der forventes af ens robusthed, hvis man leverer noget, der er kritisk for andres drift,” siger Claus Fibiger, adm. direktør i Securitas Danmark og bestyrelsesleder i Vagt- og Sikkerhedsindustrien i Dansk Industri.

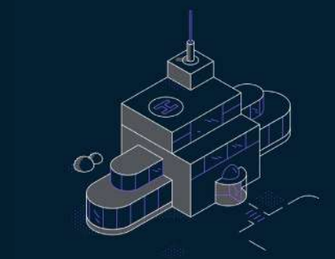
Af den grund er CER mere end compliance. Det er også et spørgsmål om ledelse, risikoforståelse og konkurrencekraft. Virksomheder, der forstår deres egen rolle i de kæder, de indgår i, kan bruge modstandsdygtighed som en styrkeposition – ikke bare som et krav, der skal opfyldes.

Det kan ligefrem være en konkurrencefordel at være på forkant. Når kravene skærpes, står de bedst forberedte stærkere – i tilbudsgivning, i kundedialog og i driftsleverancen.

”Mange er stadig optaget af at få afklaret, om CER gælder for dem. Det er forståeligt. Men ofte er det vigtigere at stille et andet spørgsmål: Hvor vigtig er vores leverance for andres drift, og hvor robuste forventes vi at være? Det er i sidste ende den tankegang, CER bygger på,” siger Claus Fibiger.



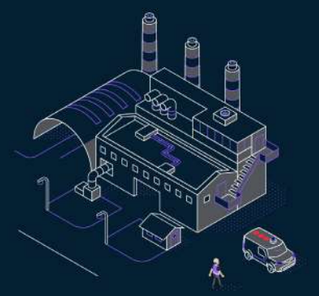
# Berørte sektorer



## SUNDHEDSSEKTOREN

Omfatter hospitaler, sundhedstjenester og producenter af medicinsk udstyr.

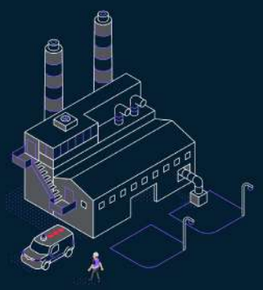
Sundhedsstyrelsen er kompetent myndighed for sundhedstjenesteydere, mens Lægemiddelstyrelsen er kompetent myndighed for lægemiddelrelateret forskning og udvikling.



## FØDEVARESEKTOREN

Omfatter produktion, tilvirkning og distribution af fødevarer.

Fødevarestyrelsen er kompetent myndighed for kritiske enheder inden for logistik, engrosdistribution og industriel fødevareproduktion.



## ENERGISEKTOREN

Omfatter produktion, transmission og distribution af energi, herunder blandt andet elektricitet, gas, fjernvarme og olie.

Energisektoren er omfattet af CER, men reguleres i Danmark særskilt gennem lov om styrket beredskab i energisektoren.



## DRIKKE- OG SPILDEVANDSSEKTOREN

Omfatter produktion og distribution af drikkevand, men inkluderer også indsamling, behandling og bortskaffelse af spildevand.

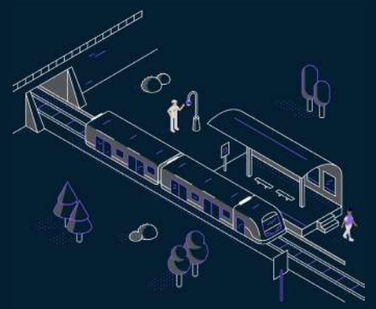
Miljøstyrelsen er kompetent myndighed for kritiske enheder, der opererer inden for drikke- og spildevandsektoren.



## BANKVÆSEN OG FINANSIEL MARKEDSINFRASTRUKTUR

Omfatter banker, betalingssystemer og anden infrastruktur, der er essentiel for finansielle transaktioner.

Finanstilsynet er kompetent myndighed for kritiske enheder inden for bankvæsen og finansiel markedsinfrastruktur.



## TRANSPORTSEKTOREN

Omfatter luftfart, jernbaner, vejtransport og skibsfart, samt infrastruktur som lufthavne, jernbanestationer og havne.

På transportområdet er myndighedsansvaret fordelt mellem Trafikstyrelsen, Søfartsstyrelsen og Styrelsen for Samfundssikkerhed.



## OFFENTLIG ADMINISTRATION

Omfatter myndigheder med kritiske funktioner for samfundet, herunder centrale enheder med ansvar for sikkerhed, beredskab og andre væsentlige samfundsopgaver.

Styrelsen for Samfundssikkerhed er kompetent myndighed.



## DIGITAL INFRASTRUKTUR

Omfatter datacentre, cloudtjenester, DNS, topdomæner og kommunikationsinfrastruktur, der er afgørende for digital kommunikation og databehandling.

Digitaliseringsstyrelsen og Styrelsen for Samfundssikkerhed er kompetente myndigheder.



# Krav til sikkerhed under CER

Bliver en virksomhed udpeget som kritisk enhed, er det ikke nok at have enkelte sikkerhedsforanstaltninger på plads. Der vil være en forventning om, at virksomheden kan opretholde sine væsentlige funktioner, også hvis driften bliver forstyrret.

Det kræver blandt andet, at virksomheden løbende vurderer, hvilke hændelser der kan ramme den, hvor de største sårbarheder ligger, og hvilke konsekvenser det kan få for drift og leveringsevne. Det gælder både i forhold sig selv og de afhængigheder, der knytter sig til leverandører, samarbejdspartnere og kritiske forsyninger.

Samtidig vil virksomheder skulle forholde sig til risici, som tidligere ofte har ligget mere i periferien af sikkerhedsarbejdet. Det gælder fx klimarelaterede hændelser som ekstremt vejr, oversvømmelser og længerevarende strømafbrydelser.

**RISIKOVURDERING OG -STYRING**

Virksomheder skal lave løbende risikovurderinger for at afdække mulige fysiske sikkerhedsrisici.

**ADGANGSKONTROL-SYSTEMER**

Sikre sikkerheden gennem adgangsrettigheder og baggrundskontrol af medarbejdere.

**FYSISK BESKYTTELSE AF INFRASTRUKTUR**

Installation af kameraer og andre relevanter sensorer for at sikre løbende overvågning.

**SIKKERHEDSPLANLÆGNING OG -PROCEDURER**

Udarbejdelse af sikkerhedsplaner, herunder bl.a. nødberedskabs- og genopretningsprocedurer.

**FYSISKE SIKKERHEDSAUDITS OG SIKKERHEDSTRÆNING**

Regelmæssige sikkerheds-audits og udvikling af en stærk sikkerhedskultur i virksomhederne.

**LEVERANDØRSTYRING**

Sikre at leverandører og samarbejdspartnere også opfylder sikkerhedsstandarder for at beskytte værdikæden.

# Ansvar og konsekvenser ved manglende overholdelse af CER

CER-loven flytter ansvaret tættere på virksomheden selv. Kritiske enheder skal kunne dokumentere, at de kan forebygge, modstå og håndtere alvorlige hændelser, og manglende efterlevelse kan føre til tilsyn, påbud og bødestraf.

Bliver en enhed identificeret som kritisk enhed efter CER-loven, følger der en række konkrete forpligtelser til at styrke enhedens modstandsdygtighed.

Kravene omfatter blandt andet risikovurdering, forholdsmæssige modstandsdygtighedsforanstaltninger, udpegning af en kontaktperson, underretning om hændelser samt samarbejde med den kompetente myndighed.

Ansvaret omfatter ikke kun tekniske sikkerhedsløsninger og interne procedurer, men også et bredere arbejde med robusthed, beredskab, fysisk sikring, krisehåndtering og genopretning.

Enheden skal kunne dokumentere både planlægning, implementering og opfølgning, så arbejdet kan danne grundlag for tilsyn og myndighedskontrol.

Manglende overholdelse af reglerne kan føre til myndigheds påbud, krav om oplysninger, skærpet opfølgning og bødestraf efter CER-loven. Efter dansk ret kan juridiske personer desuden pålægges strafansvar.

I praksis bør arbejdet med CER ses i sammenhæng med øvrige regulatoriske krav, herunder NIS2, hvor det er relevant, så enheden sikrer en samlet og sammenhængende tilgang til modstandsdygtighed og sikkerhed.



2

# Fysisk sikring til **NIS2**-omfattede virksomheder

> “Det sker alt for tit, at brugere ikke fjernes, når medarbejdere stopper. For en NIS2-omfattet virksomhed ville det være et decideret compliance-brud.
>
> **Nicklas Riedel, afdelingsleder for Remote Video Services, Securitas Danmark**

# Når video bliver en digital svingdør

For virksomheder, der er direkte omfattet af NIS2-loven, indgår fysisk sikring som en del af den samlede styring af risici. Reglerne stiller krav om tekniske, operationelle og organisatoriske foranstaltninger, herunder forsyningskædesikkerhed, driftskontinuitet, personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.

Derfor vil it-leverandører til virksomheder omfattet af NIS2-loven også blive mødt med skærpede krav til deres fysiske sikkerhed som led i kundernes arbejde med forsyningskædesikkerhed og risikostyring. Det kan omfatte sikring af serverrum, teknisk infrastruktur, adgangsforhold og andre fysiske miljøer, hvor kritiske systemer og data opbevares, behandles eller tilgås.

**Nøgleforanstaltninger:**

- **Adgangskontrol for at sikre at kun autoriseret personale har adgang til kritiske systemer**
- **Overvågning og alarmsystemer til at opdage og reagere på hændelser**
- **Procedurer for fysisk adgang, og håndtering af kritisk udstyr som led i den samlede risikostyring.**

# Fysiske sikkerhedssystemer er en stor cyberrisiko

Mange ved ikke, at de kameraer og servere, der skal beskytte virksomhederne i dag er blandt de mest oversete indgange for cyberangreb.



Nicklas Riedel

Ansvarlig for videoløsninger, Securitas Danmark

**I mange virksomheder betragtes videoovervågning stadig som et fysisk værktøj, der bare står og optager. Men virkeligheden er en anden.**

I 2025 viste en stor international sag igen, hvor hurtigt et kamera kan blive adgangsbillet til følsomme data. Hackere fik adgang til titusindvis af kameraer i private hjem og virksomheder – alene ved at gætte simple kodeord. Optagelserne blev misbrugt og solgt kommercielt.

Det mest opsigtsvækkende var ikke, at video var målet, men hvor hurtigt og lavpraktisk angrebet var. Og mange virksomheder gør helt ubevidst adgangen til deres egne systemer alt for nem.

Det bekræfter Nicklas Riedel, ansvarlig for videoløsninger i Securitas Danmark:

”De kameraer og servere, som skal beskytte virksomhederne, ender paradoksalt nok ofte med at være en af deres største cyberrisici.”

Fejlen er ifølge ham den samme mange steder – fra mindre virksomheder til kritisk infrastruktur:

“Video behandles stadig som et stykke fysisk udstyr, der bare står i hjørnet og optager. Man overser, at det er et digitalt system på virksomhedens netværk og dermed en potentiel indgang til forretningskritisk data.”

Nyere data fra drift af fysiske sikkerhedsenheder viser, at omkring 40 % af sikkerhedsdevices er direkte sårbare på grund af forældet firmware, og at over 50 % kører med forældet firmware i det hele taget.

## NÅR ET VIDEOANLÆG BLIVER HACKERNES INDGANG

Nicklas har selv oplevet konsekvenserne på tæt hold tidligere i sin karriere hos en anden sikkerhedsleverandør. Ét angreb, der lagde store systemer ned:

”Det viste sig at hackere havde spammet serveren i halvandet år, hvor de til sidst fik hul. Kunden mistede alle videodata og alle adgangskort. Alt var krypteret, og det kostede virksomheden et stort millionbeløb at få dekrypteret.”




# De 6 vigtigste it-spørgsmål til din sikkerhedsleverandør

“Når leverandører kalder deres løsning “NIS2-kompatibel”, siger det i sig selv ikke ret meget. Det vigtigste er, om de kan give klare svar på ansvar, logning, adgangsstyring, patching og dokumentation – og dermed reelt understøtte deres arbejde med robusthed, hændelseshåndtering og compliance,” forklarer Nicklas Riedel.

**Videoovervågning bliver ofte opfattet som et drifts- eller teknikområde. Men i en NIS2-kontekst er det langt mere end kameraer på væggen. Det er et netværkstilkoblet system med brugere, rettigheder, software, logs og leverandøradgange. Derfor er det ikke nok at spørge, om løsningen lever op til NIS2 på papiret.**

“Det mindst interessante er egentlig, om vi kan sætte et NIS2-mærkat på en løsning. Det mest interessante er, om vi kan hjælpe kunden med at leve op til kravene til ansvar, responstid, logning og dokumentation,” uddyber Nicklas Riedel.

Her er de seks spørgsmål, der gør dialogen konkret.

### 1. START DER, HVOR ANSVARET LIGGER

NIS2 gør det tydeligt, at ansvaret ligger hos virksomheden – ikke hos leverandøren. En leverandør kan ikke gøre jer compliant, men kan gøre det lettere eller sværere at leve op til kravene.

Derfor bør et af de første spørgsmål være:

“Hvad tager I konkret ansvar for i forhold til drift og sikkerhed - og hvad ligger hos os?”

Hvis svaret i praksis er: “Vi leverer systemet, I driver det”, skal I også være klar over konsekvensen. Så er video et it-system, som I selv skal have fuld governance på - fra patching og rettigheder til overvågning, hændelseshåndtering og dokumentation.

“Hvis ikke ansvarsfordelingen bliver taget fra starten, kommer den næsten altid tilbage på det værst tænkelige tidspunkt,” siger Nicklas.

### 2. BRUGERADGANG OG RETTIGHEDER: HVEM KAN LOGGE IND - OG KAN I DOKUMENTERE DET?

Når NIS2 skærper fokus på privilegerede brugere, sporbarhed og adgangslogs, bliver video hurtigt et overset område. Gamle tekniker-konti, delte logins og standard-adgange er præcis den type små huller, der gør en platform sårbar.

Det afgørende er derfor ikke bare, om leverandøren har adgangsstyring, men om identitet og privilegier håndteres på en måde, der kan dokumenteres i en audit.

Spørg for eksempel, hvordan adgange lukkes ned, når medarbejdere eller leverandører stopper, og hvilke logs der viser, hvem der har haft adgang og ændret rettigheder.

Et godt svar lægger vægt på rollebaseret adgang, integration til identity provider og tydelig adskillelse mellem bruger- og administratorrettigheder.

### 3. FIRMWARE PATCHING OG SÅRBARHEDER: HVAD SKER DER, NÅR NOGET BLIVER GAMMELT?

Et videoanlæg består i praksis af små computere: kameraer, recordere, gateways og servere. Hvis firmware og software ikke opdateres, kan sårbarheder stå åbne i årevis. I NIS2-sammenhæng handler det også om netværksdesign og styring af fjernadgang.

Spørg derfor, hvem der har ansvaret for opdateringer, hvordan opdateringsprocessen ser ud, og om I kan få dokumentation for, hvilke versioner I kører på.

Spørg også, hvordan video er placeret på netværket, og hvordan leverandørens fjernadgang sikres, begrænses og kan revideres.

"Vi ved, at en stor del af de kameraer, der hænger derude, kører på forældet firmware," siger Nicklas. "Derfor skal opdateringer være en fast del af driften - og de skal kunne dokumenteres."

### 4. OPDAGER LEVERANDØREN FEJL, FØR I GØR?

NIS2 handler også om tilgængelighed og robusthed. Hvis et kamera ikke optager, eller en server er nede, kan det hurtigt blive et problem, hvis video skal indgå i hændelseshåndtering.

Spørg derfor, hvordan løsningen overvåges, hvilke alarmer leverandøren reagerer på, hvad der sker ved nedbrud, og hvilke muligheder der er for redundans.

Men modenheden viser sig først, når noget faktisk går galt. Hvad er planen for genopretning? Hvor hurtigt kan løsningen være oppe igen, og hvor meget data kan I tåle at miste? Og er de testet eller blot antaget?

"Vi kan se i driften, at der næsten altid er en lille andel enheder, der midlertidigt er ude af drift," siger Nicklas. "Forskellen er, om nogen opdager det samme dag og får det løst – eller om man først opdager det, når man står og mangler optagelserne."

### 5. KAN I TRÆKKE DEN DOKUMENTATION, I HAR BRUG FOR?

Når revisor, intern audit eller en myndighed beder om dokumentation, er det ikke nok at sige, at systemet er sikkert. I skal kunne vise, hvem der har haft adgang, hvilke ændringer der er foretaget, og hvordan hændelser er håndteret.

Spørg derfor ind til, hvilke logdata systemet gemmer, hvor længe de gemmes, om det er muligt at se adgang til optagelser og ændringer i indstillinger, og hvilke rapporter der kan trækkes ud.

Det centrale er ifølge Nicklas ikke bare, om der findes logs, men om de er søgbare, brugbare og hurtigt kan fremskaffes.

"Når vi designer videoløsninger, tænker vi fx altid: Hvordan ser det her ud i en audit?" siger Nicklas.

### 6. HVORDAN SER LEVERANDØRENS EGEN SIKKERHED UD?

Til sidst bør I se på leverandøren selv. NIS2 lægger op til, at I også skal forholde jer til sikkerheden hos kritiske leverandører.

Spørg derfor, om leverandøren selv er omfattet af NIS2 eller anden regulering, hvilke sikkerhedsstandarder eller ISO-certificeringer de kan dokumentere, og hvordan I bliver informeret, hvis der sker en sikkerhedshændelse hos dem, som påvirker jeres løsning.

"Hvis en leverandør sælger til NIS2-omfattede virksomheder, men ikke kan forklare sin egen governance, er det et faresignal," afslutter Nicklas Riedel.



3

# Robusthed og resiliens

# Hvad kontinuerlig drift kræver i praksis

Danmark har en af verdens mest stabile elforsyninger. Netop derfor tager mange virksomheder stabil drift for givet. Det gør dem sårbare. For når strømmen forsvinder, er det sjældent kun lyset, der går.

## NÅR STRØMMEN GÅR

Et længerevarende strømsvigt kan hurtigt udvikle sig til en bred driftsforstyrrelse, hvor adgang, video, alarmer, kommunikation og dokumentation påvirkes samtidig. Det er her, virksomhedens robusthed bliver testet.

“Det handler ikke kun om at holde lyset tændt. Det handler om, hvad der sker, når det slukker,” siger Klaus Jensen, ansvarlig for compliance i Securitas Danmark.

Uden klare procedurer og tydelig ansvarsfordeling risikerer virksomheden, at nedetiden varer længere, end økonomien kan bære. Kunder kan søge mod andre leverandører, produktion og lager kan blive ramt, data kan gå tabt, og det kan blive svært bagefter at fastslå, hvad der egentlig skete.

“Efter større brande, oversvømmelser og længerevarende nedbrud ser man igen og igen, at nogle virksomheder aldrig kommer tilbage på niveau. Nogle lukker helt,” siger Klaus Jensen.

## DE FØRSTE SVIGT ER OFTE DE MEST LAVPRAKTISKE

Når strømmen går, er det ikke nødvendigvis it-systemerne, der først bliver den største udfordring. Ofte er det de helt grundlæggende forhold, der afgør, om virksomheden kan bevare kontrollen.

Lokaler bliver mørke. Porte, låse og elektroniske døre reagerer ikke altid, som man forventer. Nogle åbner af sig selv, andre låser sig fast. Hvis medarbejdere, teknikere eller vagter ikke kender de manuelle procedurer, vokser både usikkerheden og nedetiden hurtigt.

Robusthed handler derfor ikke om et stort, abstrakt beredskab, men om evnen til at fungere, når flere centrale funktioner forsvinder på én gang.



## Tre blinde vinkler - har du tænkt på?

- ✓ Hvilke leverancer eller funktioner kan dine kunder ikke undvære, uden at deres drift bliver kritisk påvirket?
- ✓ Hvilke afhængigheder er svære at erstatte hurtigt – fx leverandører, adgang til lokationer, nøglepersoner, systemer, logistik eller bemanding?
- ✓ Kan vi dokumentere vores eget beredskab i praksis – roller, kontaktveje, beslutningskompetencer, regelmæssige øvelser og en plan B, hvis noget svigter?

“I bund og grund afgøres meget af, om virksomheden har forberedt de manuelle greb: fysiske nøgler og nødåbninger, faste mødepunkter, tydelig rollefordeling og en plan for, hvordan man handler, når man ikke kan logge ind for at komme i gang.”

## NEDBRUD AFSLØRER SKJULTE AFHÆNGIGHEDER

Et strømsvigt gør det tydeligt, hvor tæt moderne sikkerheds- og driftsmiljøer hænger sammen. De systemer, der til hverdag understøtter sikkerhed og tryghed, er ofte afhængige af både strøm, netværk og stabile forbindelser.

Videoovervågning, adgangskontrol, alarmer og brandanlæg reagerer ikke nødvendigvis ens, når strømmen eller netværket svigter. Nogle funktioner fortsætter på backup, andre falder ud. I nogle tilfælde opstår der så mange fejlsignaler, at organisationen har svært ved at skelne mellem støj og reelle hændelser.

“I praksis er det typisk tre spørgsmål, der går igen på tværs af brancher: Hvad virker stadig? Hvem har ansvaret for at reagere? Og hvordan dokumenterer vi, hvad der sker?”

Ifølge Klaus Jensen er det netop i de situationer, at manglende overblik bliver kritisk.

“Det farlige ved nedbrud er ikke kun det, der stopper, men det, der ændrer sig. Alarmer og adgangskontrol har ofte backup, men video og forbindelser kan svigte, og så stiger mængden af fejlsignaler.”

Derfor er det afgørende at kende systemernes adfærd på forhånd.

“Du skal vide, hvordan dine systemer opfører sig ved tab af strøm eller netværk, så du kan skelne mellem støj og reelle hændelser.”

Kommunikation er samtidig en overset sårbarhed. Hvis mobilnettet er belastet, eller hvis Teams og telefoni er utilgængelige, kan koordineringen hurtigt bryde sammen.

“Derfor er det værd at have truffet en tydelig beslutning om, hvem der må kontakte vagt, teknik, energiselskab eller myndigheder,” siger Klaus Jensen.

## DOKUMENTATION OG EKSTERNE AFHÆNGIGHEDER ER TYPISKE BLINDE VINKLER

Når virksomheden skal genvinde kontrollen, bliver det også tydeligt, hvor sårbar dokumentationen kan være. Optagelser, hændelseslog og adgangslogs er ofte netop det, man har størst behov for under og efter et nedbrud. Alligevel er det ikke altid sikkert, at de er komplette eller tilgængelige.

“Det er her, virksomheder ofte opdager deres blinde vinkler: et kamera uden backup, en switch i et teknikrum uden UPS, en port der ikke kan åbnes uden strøm, en recorder der lukker ned før resten, eller et ABA-/ABDL-setup hvor dele af kæden fortsætter, mens andre falder ud.”

Jo mere sammensatte installationerne er, desto større er risikoen for, at noget fejler, uden at det bliver opdaget i tide.

Men robusthed afhænger ikke kun af egne installationer. Mange af de mest kritiske sårbarheder ligger uden for virksomhedens egen matrikel.

“Energiselskaber, teleoperatører, cloud- og hostingpartnere kan ramme dig lige så hårdt som fejl i egne systemer - også selv om du har strøm lokalt. For hvis forbindelsen til omverdenen er nede, kan det føles som om alt er nede.”

Derfor bør redundans ikke kun gælde udstyr, men også forbindelser og leverandørafhængigheder.

## STRØMSVIGT ER ET SPØRGSMÅL OM RISIKOSTYRING

I lyset af CER og NIS2 er strømsvigt, netværksnedbrud og andre forsyningsafbrydelser ikke kun tekniske hændelser. De er en del af virksomhedens samlede risikostyring og robusthed.

Det vigtigste spørgsmål er derfor ikke kun, om virksomheden har backup. Det er, om den har overblik over, hvilke funktioner der er mest kritiske, hvor længe de kan være nede, og hvilke manuelle eller tekniske løsninger der skal tage over, når de normale systemer ikke længere fungerer.

“Konsekvensen ved silotænkning er, at ingen har det samlede billede af, hvilke funktioner der er forretningskritiske, hvor længe de må være nede, og hvilke systemer og manuelle procedurer der skal tage over, når strøm og netværk forsvinder.”

Set med risikostyringsbriller er konsekvensen ifølge Klaus klar:

“Hvis virksomheden ikke har taget aktivt stilling til den risiko, har den i praksis accepteret en nedetidsrisiko uden at vide, om økonomien kan bære den.”



# Sikker drift afhænger også af leverandørerne

For mange virksomheder bliver CER og NIS2 ikke først relevante, når en myndighed kontakter dem. Reglerne bliver ofte aktuelle langt tidligere, nemlig når kritiske kunder begynder at stille spørgsmål til robusthed, dokumentation og sikker drift i leverandørkæden.



Eddie Christoffersen

Key Account Manager, Securitas Danmark

**Det gælder også virksomheder, som ikke selv er direkte omfattet af reglerne. Hvis deres løsning eller leverance er vigtig for kundens drift, vil kunden ofte forvente indsigt i, hvordan virksomheden arbejder med beredskab, adgangsstyring, kritiske afhængigheder og driftskontinuitet.**

Derfor bør området ikke kun ses som et spørgsmål om compliance. For mange virksomheder er det i lige så høj grad et spørgsmål om at være godt forberedt på kundernes krav og forventninger.

Virksomheder, der tidligt skaber overblik over deres kritiske afhængigheder og kan dokumentere deres processer, står typisk stærkere i dialogen med kunderne og i forbindelse med tilbud og udbud.

### DET KRITISKE ENHEDER TYPISK VIL VIDE

Når kravene viser sig gennem værdikæden, spørger kunderne typisk ind til det, der kan påvirke deres egen drift.

**Det kan være:**

- om virksomheden har overblik over sine kritiske funktioner og afhængigheder
- om der findes beredskabs- og genopretningsplaner
- om adgang til kritiske områder er styret og dokumenterbar
- hvordan virksomheden opretholder driften ved nedbrud eller forsinkelser

# Vi har gjort det lidt nemmere

## Få adgang til gratis skabeloner og input til en risikoworkshop, som I selv kan afholde internt.

**Scan QR-koden og få adgang til gratis skabeloner og spørgsmål til jeres risikoworkshop**

Det kan være en udfordring at få overblik over alle risici og dokumentere sine valg på et kvalificeret grundlag. Men I behøver ikke nødvendigvis bruge dyre konsulenttimer for at komme i gang. Med den rette inspiration kan I nemlig nå rigtig langt selv.

# Samarbejde med Securitas

4

# Fra udfordring til **løsning**

## Bygningsstyrelsen vælger Securitas efter udbud med skærpede leverandørkrav

I lyset af det ændrede sikkerhedsbillede og de øgede krav på området bliver sikkerhed fra 1. oktober 2026 for første gang etableret som et selvstændigt område i Statens Facility Management.

Aftalen omfatter 100 institutioner fordelt på cirka 242 lokationer i hele landet og markerer et vigtigt skifte i organiseringen og leveringen af sikkerhedsydelser. Fremover vil området være underlagt egne krav til kvalitet, leveringssikkerhed, fleksibilitet, sikkerhedsgodkendelser og digital understøttelse.

*"Securitas er allerede en kendt samarbejdspartner, og vi ser frem til at fortsætte samarbejdet om en stabil og tryg sikkerhedsdrift på de nuværende lokaliteter."*

**Anders Mærkedahl Pedersen**
Direktør, Bygningsstyrelsen

Læs mere på securitas.dk

# Overblik og prioritering

Arbejdet med CER kræver overblik og prioritering.
Vi hjælper jer i flere led af arbejdet.

## Vi hjælper med at styrke

- fysisk sikring
- adgangsstyring
- overvågning og respons
- beredskab og kontinuitet

## Vi hjælper med at vurdere

- risici og sårbarheder
- konsekvenser for driften
- kritiske scenarier
- relevante prioriteringer

## Vi hjælper med at kortlægge

- kritiske funktioner
- anlæg og processer
- leverancer
- afhængigheder

> *De endelige bekendtgørelser for CER er fortsat under afklaring. Hos Securitas følger vi udviklingen tæt og er allerede i dialog med kunder på tværs af sektorer for løbende at forstå deres udfordringer og behov.*





## Erik Johan Madsen
Salgschef, Key Account

**Profil**
Erik bringer en bred erfaring på tværs af sektorer og en stærk kommerciel forståelse ind i samarbejdet. Sammen med teamet arbejder han hver dag på at udvikle relationer og løsninger, der understøtter kundernes langsigtede mål.

**Mail:** erik.johan.madsen@securitas.dk
**Tlf:** +45 2338 5578



## Eddie Christoffersen
Key Account Manager

Sundhed · Offentlig administration · Fødevarer · Tele · Drikke- og spildevand · Digital infrastruktur

**Profil**
Skaber fremdrift i salgsdialoger, hvor sektorindsigt, tillid og relevans er afgørende for at åbne og udvikle relationer.

**Mail:** eddie.dieckmann.christoffersen@securitas.dk
**Tlf:** +45 2541 4440



## Søren Bækkegaard
Key Account Manager

Sundhed · Drikke- og spildevand · Fødevarer · Offentlig administration · Transport

**Profil**
Arbejder stærkt i markeder præget af høj kompleksitet, mange interessenter og behov for præcis kommerciel positionering.

**Mail:** soeren.baekkegaard@securitas.dk
**Tlf:** +45 2541 4421



## Rasmus Andersen
Key Account Manager

Tele · Finansmarkedsinfrastruktur · Transport · Digital infrastruktur · Bankvæsen · Fødevarer

**Profil**
Analytisk stærk rådgiver med dyb teknisk indsigt og fokus på strukturerede, kundetilpassede løsninger.

**Mail:** rasmus.andersen@securitas.dk
**Tlf:** +45 2338 6074



## Jesper Kjærgaard
Key Account Manager

Energi · Finansmarkedsinfrastruktur · Bankvæsen · Digital infrastruktur · Tele · Fødevarer

**Profil**
Bevæger sig sikkert i komplekse markeder, hvor teknisk forståelse og kommerciel skarphed skal gå hånd i hånd.

**Mail:** jesper.kjaergaard@securitas.dk
**Tlf:** +45 2541 4420

# Brancheekspertise

Vores sikkerhedsrådgivere kombinerer specialiseret viden og markedsindsigt med tæt samarbejde på tværs af de sektorer, hvor kravene er størst. Det giver stærkere kundedialoger og et mere relevant grundlag for rådgivning.

| *Sektorer* | *Sælgerprofiler* | *Teamdækning* |
|---|---|---|
| **11** | **5** | **Både dybde og overlap** |

# Sådan ser samarbejdet med Securitas ud

## 1

### STRATEGISK AFDÆKNING

Vi starter altid vores samarbejde med at forstå jeres udfordringer. Vi spørger ind til de primære bekymringer og udfordringer for virksomheden på tværs af forretningen, ikke kun indenfor sikkerhed. Ved at forstå nuværende situation og fremtidige mål kan vi planlægge den bedste vej frem.

## 2

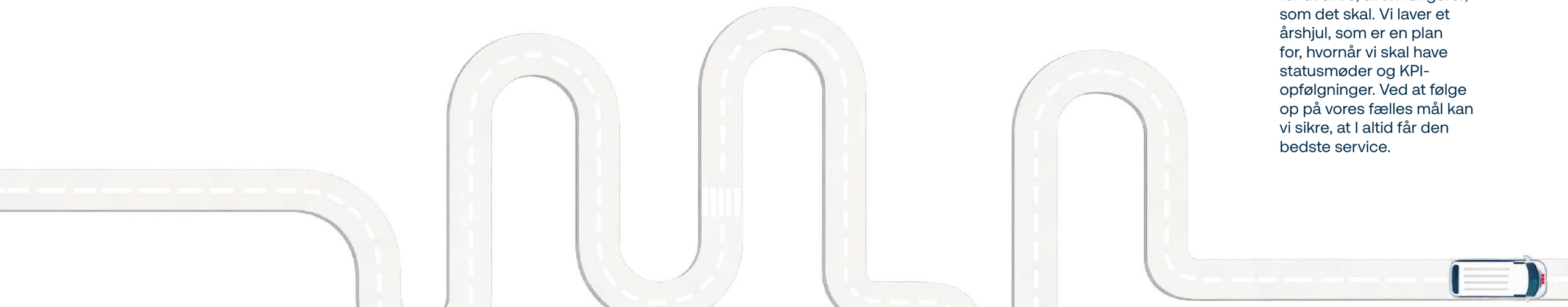
### SIKKERHEDSRÅDGIVNING

Når vi har en god forståelse af jeres behov, går vi videre til sikkerhedsrådgivning. Her laver vi en fyldestgørende risikovurdering. Det betyder, at vi ser på, hvilke risici I står overfor, og hvordan vi bedst kan beskytte mod dem. Vi gennemgår også relevante krav og lovgivning.

## 3

### TILBUD OG KONTRAKT

Når vi har en klar plan, sammensætter vi et skræddersyet tilbud. Vi fastlægger aftalegrundlaget, som er de vilkår og betingelser, vi begge er enige om. Og så fastsætter vi også SLA'er (Service Level Agreements), som er de mål, vi skal opnå for at sikre, at I er tilfredse.



## 4

### IMPLEMENTERING

Når kontrakten er på plads, går vi i gang med implementeringen. Det er her, hvor vi virkelig får tingene til at ske. Vi sammensætter vagtteams, monterer brandsikring og installerer teknik. For at sikre, at alt kører glat, sammensætter vi et dedikeret team, der er ansvarlig for jeres sikkerhed.

## 5

### LØBENDE SAMARBEJDE

Efter implementeringen stopper vores arbejde ikke. Vi fortsætter samarbejdet for at sikre, at alt fungerer, som det skal. Vi laver et årshjul, som er en plan for, hvornår vi skal have statusmøder og KPI-opfølgninger. Ved at følge op på vores fælles mål kan vi sikre, at I altid får den bedste service.

# Hvorfor I skal vælge Securitas





Bliv sikret 360 grader

Få ro i sindet med en løsning fra Securitas. Vi sikrer dig 360 grader, med kombinationen af teknologi, mennesker og data. Det betyder, at vi fanger, hvad andre overser. Derfor behøver du ikke holde et vågent øje med din sikkerhed – det klarer vi for dig.



Spar tid

Giv dine medarbejdere mulighed for at koncentrere sig om det, der skaber mest værdi med en professionel sikkerhedspartner. Vi frigør tid ved at tage ejerskab for jeres sikkerhedssetup. Vi tager ansvar og retter til, hvis der er udfordringer, så du kan bruge din tid på noget andet.



Vær compliant

Compliance er en del af hverdagen for langt de fleste virksomheder. Med en integreret sikkerhedsløsning kan du få den information og den indsigt, du har brug for i dit compliancearbejde. Som en af landets største sikkerhedsudbydere kender vi reglerne, også dem der ændrer sig.



Få mere viden

Få viden og data til at optimere og arbejde smartere. Vores sikkerhedsløsninger skaber store mængder af data. Vi kan integrere vores sikkerhedsprodukter med dine eksisterende systemer, så du kan få data der kan optimere dine arbejdsgange.



Få ekspertrådgivning

Du er ekspert i din virksomhed, så du behøver ikke være ekspert i sikkerhed. Det har vi nemlig 90 års erfaring med. Samtidig trækker vi på et globalt netværk af viden og erfaring fra over 44 markeder, når vi laver innovative og effektive sikkerhedsløsninger.



Fleksibel skalering

Når virksomheden vokser, skal jeres sikkerhedsløsning kunne følge med, uden I skal bøvle med at skifte leverandør. Hos Securitas er vi tilstede lokalt, nationalt og globalt, og vi kan skalere vores sikkerhedsløsninger til jeres behov i alle faser af jeres vækst.



Lad os investere i jer

Vi tager opstartsinvesteringen i din sikkerhedsløsning, så I kan investere i jeres virksomhed i stedet. Sikkerhedsløsningen betales som et fast månedligt gebyr.



Bliv en tryg arbejdsplads og virksomhed

En gennemtænkt sikkerhedsløsning giver en god og tryg oplevelse for både kunder og medarbejdere. Det gør jeres virksomhed til en attraktiv arbejdsplads og samarbejdspartner.



Understøt dine ESG-mål

ESG fylder på de fleste virksomheders agenda. Grib muligheden for at integrere din sikkerhedsløsning i dit bæredygtighedsarbejde med en sikkerhedsleverandør, der er miljøcertificeret og har afgivet DIs diversitetsløfte.

# Konklusion

NIS2- og CER-direktiverne markerer et vigtigt skift i, hvordan sikkerhed tænkes i kritisk infrastruktur og blandt deres leverandører. De skærpede krav til både fysisk og digital sikkerhed betyder, at virksomheder i stigende grad må arbejde mere systematisk og proaktivt med sikkerhed, robusthed og beredskab.

Det kan opleves som en udfordring, men rummer også en mulighed for at styrke virksomhedens modstandsdygtighed og position som samarbejdspartner i en verden med nye trusler og stigende krav. Hos Securitas arbejder vi med at omsætte disse krav til praktiske løsninger, der kan understøtte både compliance og en stærkere sikkerhed på tværs af værdikæden.



Hos Securitas fører vi sikkerheds-branchen ind i fremtiden. Vi samler sikkerhedsservices som vagt, alarm, videoovervågning, adgangskontrol, brandsikring og førstehjælp i innovative sikkerhedsløsninger, der opfylder vores kunders forskellige behov. Vores løsninger er fleksible og kan nemt skaleres i takt med den globale udvikling og din virksomheds behov.

**Securitas A/S**
Sydvestvej 98, 2600 Glostrup
Telefon: +45 4343 4388
www.securitas.dk

© 2026 Securitas A/S