Securitas

RISK INTELLIGENCE CENTER · INTREP: DANMARK

Virksomheders sikkerhedstrusler og risikoprioriteter for 2027

29. oktober 2026

Denne rapport er omfattet af GDPR og af retningslinjer for opbevaring af data i overensstemmelse med denne lovgivning.

Securitas stiller denne efterretningsrapport (INTREP) fra Risk Intelligence Center (RIC) til rådighed for modtagerens interne forretningsmæssige brug. Rapportens indhold skal behandles forsvarligt og sikkert. Securitas påtager sig intet ansvar for beslutninger, som modtageren træffer på baggrund af rapportens indhold. Oplysningerne og analyserne i rapporten er ingen garanti for, at begivenheder indtræffer som vurderet. Rapportens indhold er fortrolig information, der udelukkende er tiltænkt adressaterne eller den ovenfor nævnte enhed.

Det er strengt forbudt at anvende Securitas' navn, varemærker, logoer, taglines, slogans eller andre kendetegn uden skriftlig tilladelse. Det er ligeledes strengt forbudt at videregive, kopiere, distribuere eller anvende nogen del af RIC's rapporter, elektronisk eller på anden måde, til andet end det formål, de er stillet til rådighed for.

INDHOLD

Fire trusselsområder for 2027

—	Metode	3
—	Overblik	4
01	**Cyberangreb og digitale nedbrud**	6
02	**Sabotage, spionage og droneaktivitet**	9
03	**Kritisk infrastruktur og transportforstyrrelser**	12
04	**Målrettet aktivisme, protester og arbejdskonflikter**	16

Hvert område samler et tilbageblik på 2026, forventede tendenser, udsatte brancher, mulige udløsende begivenheder og konkrete sikkerhedsovervejelser.

METODE

Sådan læser du vurderingen

Trusselsniveauer

5 – EKSTREM	Meget høj/ekstrem trussel. Vurdér og reagér om nødvendigt.
4 – HØJ	Høj/betydelig trussel. Overvej passende tiltag.
3 – MODERAT	Moderat trussel. Bevar opmærksomheden og overvej forholdsregler.
2 – LAV	Lav/begrænset trussel. Til orientering.
1 – MEGET LAV	Meget lav/ubetydelig trussel. Til almindelig orientering.

Sandsynlighedsskala

Trusselsvurderingen anvender RIC's sandsynlighedsskala til at vurdere, hvor sandsynligt det er, at en trussel bliver til virkelighed. Vurderingen tager udgangspunkt i en sandsynlighed udtrykt som procent, brøk eller forhold. Det skaber kontekst og klarhed og sikrer en ensartet tilgang.



Næsten udelukket	Meget usandsynligt	Usandsynligt	Reel mulighed	Sandsynligt	Meget sandsynligt	Næsten sikkert
0–4 %	10–20 %	25–35 %	40–50 %	55–75 %	80–90 %	95–99 %

OVERBLIK

Trusselsbilledet for 2027

Virksomheder i Danmark går ind i 2027 med et trusselsbillede, der er præget af digital afhængighed, sammenkoblede transport- og forsyningsnet og Danmarks rolle i nordisk og europæisk sikkerhed. Cyberhændelser, infrastruktursvigt, fjendtlige aktiviteter og målrettede protester udgør trusler mod danske lokationer, medarbejdere, forsyningskæder og virksomheders omdømme.

Eksponeringen varierer fra virksomhed til virksomhed. Trusselsbilledet peger ikke på en generel stigning i hændelsernes hyppighed eller alvor for alle virksomheder, men et indgående kendskab til det sammensatte trusselsbillede giver virksomhederne et grundlag for at træffe velinformerede sikkerhedsbeslutninger.

Rapporten prioriterer fire centrale trusselsområder for Danmark: cyberangreb og digitale nedbrud; sabotage, spionage og droneaktivitet; kritisk infrastruktur og transportforstyrrelser; samt målrettet aktivisme, protester og arbejdskonflikter. Eksponeringen afhænger af branche, beliggenhed, kommercielle relationer og afhængighed af fælles tjenester. Blandt de mest udsatte og/eller ramte brancher er forsvars- og luftfartsindustrien, transportvirksomheder, forsyningsselskaber, life science-virksomheder, forskningsinstitutioner og virksomheder med tilknytning til omstridte investeringer eller forsyningskæder.

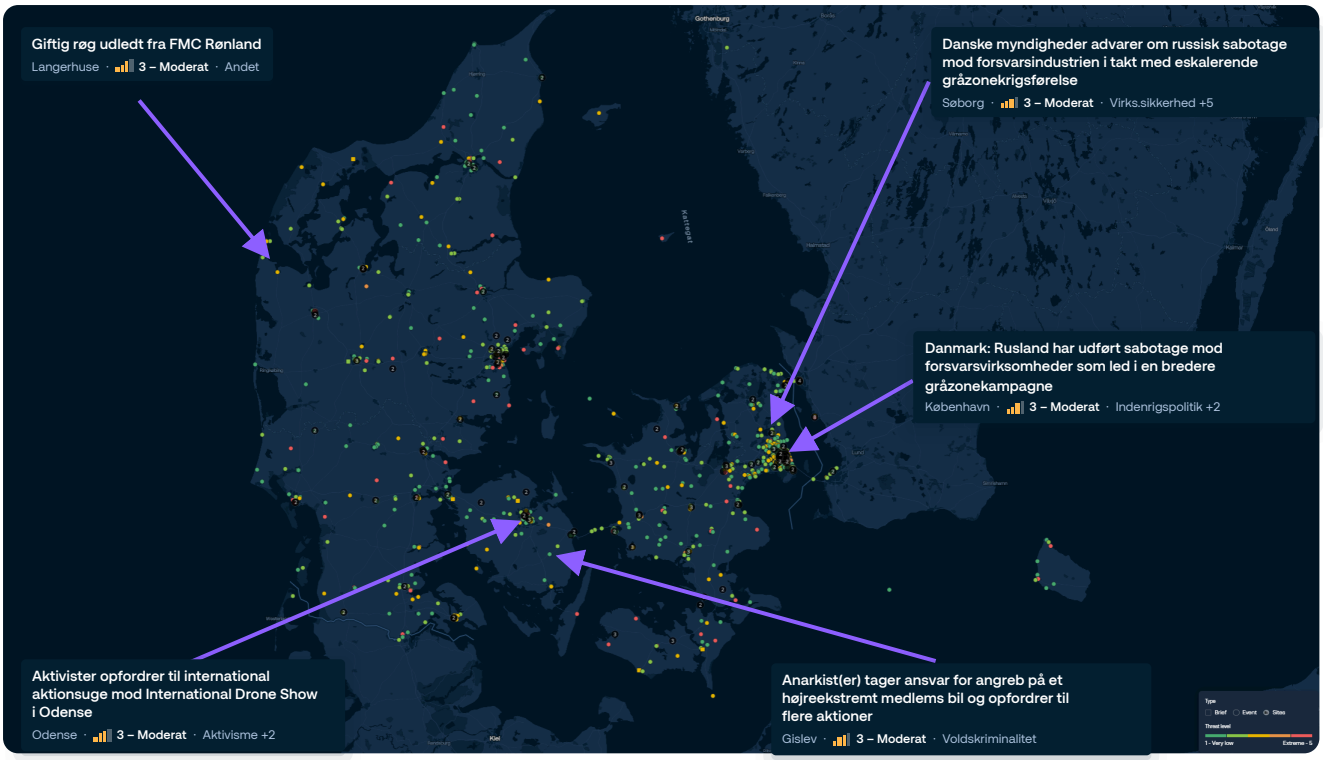
Danmarks digitale afhængigheder skaber en direkte forbindelse mellem informationssikkerhed og fysisk drift. Det nyligt omtalte angreb på hovedentreprenøren på Femern Bælt-forbindelsen satte den elektroniske adgangskontrol og byggeprocesserne ud af drift, mens læk fra CPR-registret viste, hvordan eksponeringen kan ske gennem en betroet privat virksomhed. Ud over cyberhændelser viser strømafbrydelser, signalfejl på jernbaner, hændelser i havne og lukning af broer og veje, hvordan virksomheder kan blive ramt af driftsforstyrrelser i forhold til medarbejdere, leverancer, kommunikation eller kritiske tjenester, også selvom deres egne lokaler ikke er direkte mål eller berørt.

01
Cyberangreb og digitale nedbrud

02
Sabotage, spionage og droneaktivitet

03
Kritisk infrastruktur og transportforstyrrelser

04
Målrettet aktivisme, protester og arbejdskonflikter



Kilde: MySecuritas Briefs & Events

Danmarks maritime forbindelser i Østersøen og forsvarsrelaterede aktiviteter har også betydning for landets eksponering over for fjendtlig rekognoscering og forstyrrelser. Advarsler fra de danske efterretningstjenester fremhæver truslen om sabotage mod virksomheder, der støtter Ukraine. Droneaktivitet og aktivitet til søs giver anledning til yderligere sikkerhedsmæssige bekymringer, selvom hensigt og afsender i nogle tilfælde fortsat er ubekræftet. Derudover viser aktioner mod Mærsk, Terma, FLSmidth, Cheminova og PensionDanmark, hvordan kommercielle forbindelser kan rette protester mod danske virksomheders lokationer.

Rapporten giver en dansk vurdering af, hvordan de fire trusselsområder sandsynligvis vil påvirke virksomheders sikkerhed og driftskontinuitet i 2027. Hvert område samler et tilbageblik på 2026, forventede tendenser, udsatte brancher, mulige udløsende begivenheder og konkrete sikkerhedsovervejelser.

TRUSSELSOMRÅDE

Cyberangreb og digitale nedbrud

Tilbageblik på 2026

Cyberhændelser i Danmark i 2026 viste, at digitale kompromitteringer kan forstyrre både drift og fysisk sikkerhed, og at truslen rækker ud over tab af data. Angrebet på Femern Link Contractors i oktober satte efter det oplyste centrale systemer og elektroniske adgangskort ud af drift, lammede arbejdsfartøjer og tvang Femern Bælt-projektet over på manuelle procedurer. Andre hændelser i 2026 omfattede:

- Personoplysninger om ca. 8,8 mio. personer blev eksponeret via en privat virksomheds autoriserede adgang til CPR-registret, hvilket understreger omfanget af den eksponering, der kan ske gennem betroede tredjeparter.
- Et cyberangreb ramte data om ca. 200.000 nuværende og tidligere studerende og ansatte på Danmarks Tekniske Universitet (DTU), hvilket understreger forskningsinstitutioners eksponering som følge af store mængder personoplysninger.
- En aktør med forbindelse til Rusland tog æren for et overbelastningsangreb (DDoS) mod sundhed.dk, hvilket understreger risikoen for forstyrrelser af digitale offentlige tjenester. Påstanden alene dokumenterer dog ikke omfanget af et eventuelt nedbrud.
- Et datalæk med tilknytning til Novo Nordisk satte fokus på informationssikkerheden i life science-branchen.
- Et IT-nedbrud i paskontrollen i Københavns Lufthavn viste, hvor afhængig grænsekontrollen er af digitale systemer, med mulige konsekvenser for passagerflow, køstyring og bemanding i frontlinjen.

Danmarks stærkt digitaliserede offentlige sektor, forskningsinstitutioner, store virksomheder og infrastrukturprojekter er fortsat udsat for kompromittering gennem egne systemer og betroede tredjeparter. De mest alvorlige sager i 2026 kombinerede eksponering af følsomme data med forstyrrelser af adgang, kommunikation eller kernedrift.

Trusselsbilledet i 2027

Danske virksomheder vil i hele 2027 fortsat være udsat for ransomware, overbelastningsangreb, kompromitterede loginoplysninger og angreb, der udnytter IT-driftsleverandører og andre betroede tredjeparter. Hændelsen på Femern Bælt viser, hvordan kompromittering af centrale systemer og adgangskort kan standse de normale arbejdsgange og skabe et fysisk sikkerhedsproblem ud over et IT-nedbrud.

Angribere vil sandsynligvis gå efter sammenkoblet driftsteknologi (OT), bygningsautomatik og digital adgangskontrol for at øge presset på ofrene. Datalæk, der berører sundhedsdata, identitetsoplysninger eller store danske virksomheder, kan desuden udløse skærpet tilsyn fra myndighederne og kan svække tilliden.

En yderligere konsekvens for 2027 er, at genopretningen efter en digital hændelse kan forløbe ujævnt på tværs af en virksomheds lokationer. Når de centrale IT-tjenester er genetableret, er elektronisk adgang, overvågning, produktion og forbindelser til leverandører ikke nødvendigvis genetableret i samme tempo. Midlertidige manuelle løsninger kan derfor vare længere end selve nedbruddet, hvilket øger presset på sikkerhedspersonalet og gør det vanskeligere at kontrollere besøgende, underleverandører og leverancer. Virksomheder, der er afhængige af fælles platforme, vil sandsynligvis opleve forstyrrelser på flere lokationer samtidig, hvilket begrænser muligheden for at flytte aktiviteter til en lokation, der ikke er ramt.

Sammenfaldet mellem datatyveri og driftsforstyrrelser skaber også risiko for en langvarig krise frem for en enkeltstående hændelse. Det er en reel mulighed, at en virksomhed på samme tid skal håndtere driftsafbrydelser, usikkerhed om kompromitterede oplysninger og gentagne krav om ekstern kommunikation. Den mest alvorlige eksponering er derfor ikke begrænset til selve indtrængningen, men omfatter også, hvor længe driften er nedsat, om der er betroet hjælp til genopretning, og om virksomheden kan opretholde sikker fysisk adgang, mens de digitale kontroller er upålidelige. I 2027 vil virksomheders robusthed ikke kun afhænge af evnen til at genetablere systemer, men også af evnen til at opretholde en sikker drift på lokationerne, når platforme til identitet, netværk, adgangskontrol eller leverandører ikke er tilgængelige.

HOVEDKONKLUSION

Cyberangreb vurderes som en meget højt prioriteret trussel mod virksomheder i Danmark. Aktiviteten vil sandsynligvis bevæge sig fra datatyveri mod driftsafbrydelser, kompromittering af tredjeparter og tab af fysisk adgangskontrol eller styringssystemer med direkte konsekvenser for faciliteter, medarbejdere, kunder og forsyningskæder.

Mest sandsynlige målbrancher

Branche	Eksponering	Sandsynlighed	Konsekvens	Væsentligste drivere
Teknologi, datacentre og telekommunikation	5 – EKSTREM	5 – EKSTREM	5 – EKSTREM	Sammenkoblede platforme og betroede leverandørers adgang koncentrerer eksponeringen for kompromittering og driftsforstyrrelser. Fælles afhængigheder kan sprede nedbrud på tværs af kunder og lokationer og samtidig ramme kommunikation og fysisk adgangskontrol.
Sundhed og life science	5 – EKSTREM	4 – HØJ	5 – EKSTREM	Følsomme person- og lægemiddeloplysninger øger konsekvenserne af datakompromittering. Afhængigheden af digitale tjenester skaber samtidig en kontinuitetsrisiko, hvor nedbrud kan begrænse sundhedsydelser og life science-drift, selv når data forbliver sikre.
Myndigheder og offentlig service	4 – HØJ	4 – HØJ	5 – EKSTREM	Centraliserede identitetsdata og afhængighed af digitale tjenester forstærker konsekvenserne af uautoriseret adgang og nedbrud. Autoriserede tredjeparter kan eksponere offentlige data uden at bryde ind i myndighedernes egne systemer.
Transport, logistik og søfart	4 – HØJ	4 – HØJ	5 – EKSTREM	Nedbrud i digital sagsbehandling, kommunikation og adgang kan forstyrre transporten af passagerer og gods. Lavere kapacitet og manuelle kontroller kan sprede forstyrrelserne til forbundne forsyningskæder.
Byggeri og anlæg	4 – HØJ	3 – MODERAT	4 – HØJ	Afhængigheden af entreprenørplatforme og elektronisk adgangskontrol knytter den digitale tilgængelighed direkte til driften på byggepladsen. Nedsatte systemer kan standse arbejdet og øge behovet for manuel godkendelse, hvilket stiller større krav til drifts- og sikkerhedsfunktionerne.

Udløsende begivenheder, der sandsynligvis indikerer et forestående eller igangværende skærpet trusselsbillede

- Offentlig omtale af sårbarheder, der påvirker udbredt anvendte danske leverandører, adgangskontrolplatforme eller IT-driftsleverandører.
- Flere phishingforsøg, forsøg på nulstilling af loginoplysninger, scanninger eller påståede overbelastningsangreb mod en bestemt branche.
- Geopolitiske begivenheder, der udløser trusler fra hacktivister mod danske virksomheder eller samfundskritiske tjenester.
- Uforklarlige fejl på adgangskort, nedsat netværksydelse eller samtidige forstyrrelser på tværs af forbundne lokationer.

Væsentligste fysiske sikkerhedstrusler og sandsynlige angrebsveje

- Tab af elektronisk adgangskontrol, tv-overvågning, alarmer, besøgsregistrering eller bygningsstyring under et nedbrud.
- Fjernkompromittering af driftsteknologi (OT) eller bygningsautomatik, der gør faciliteter usikre eller utilgængelige.
- Tredjeparters loginoplysninger, der giver adgang til flere lokationer, platforme eller følsomme datasæt.

Anbefalinger

- Segmentér virksomhedens administrative netværk, driftsnetværk og netværk til fysisk sikring, og håndhæv princippet om mindst mulige rettigheder.
- Test offline-procedurer for adgang, produktion, kundeservice og kritisk kommunikation. Øv scenarier med ransomware, databrud og svigt i adgangskontrollen sammen med cyber-, facility-, sikkerheds- og ledelsesteams.
- Styrk kontrollen med leverandører, og stil krav om hurtig underretning ved hændelser, der berører fælles tjenester.

TRUSSELSOMRÅDE

Sabotage, spionage og droneaktivitet

Tilbageblik på 2026

Russisk gråzoneaktivitet og fjendtlig interesse for forsvarsrelaterede virksomheder var fremtrædende sikkerhedsmæssige bekymringer for Danmark i 2026. I september og oktober advarede Politiets Efterretningstjeneste (PET) offentligt om, at Rusland forberedte sig på at ramme – og var begyndt at udføre sabotage mod – danske forsvarsvirksomheder, der støtter Ukraine. Den sikkerhedsrelevante aktivitet viste et sammensat mønster snarere end én bekræftet, koordineret kampagne.

Eksempler omfattede en droneobservation nær forsvarsministerens bopæl, krænkelser af lukket luftrum, russiske flådefartøjers sejladser og aktivitet i de danske stræder samt en russisk fregat, der affyrede nødblus nær en dansk helikopter. Efterretningstjenesternes advarsler pegede også på hvervning af almindelige borgere via nettet til rekognoscering eller andre enkle opgaver. I september advarede PET om russiske sabotageaktiviteter i Danmark, herunder hvervningskampagner via sociale medier, gamingplatforme og beskedtjenester som Telegram.

Det mest udsatte netværk bestod af forsvarsproducenter, havne, transportforbindelser, leverandører af dual use-produkter og organisationer, der støtter Ukraine. Eksemplerne viser betydningen af skjult aktivitet, som kan benægtes, men understreger samtidig, at enkeltstående observationer skal bekræftes, før der kan konstateres en fjendtlig hensigt.

Trusselsbilledet i 2027

Danske efterretningsvurderinger peger på et skift fra strategisk varsling over mod bekymring for aktiv sabotage mod forsvarsrelaterede virksomheder. Fremtidige hændelser vil sandsynligvis kombinere cyberindtrængning, fysisk rekognoscering, rekruttering af insidere, droneovervågning og diskret forstyrrende aktivitet, så aktøren bevarer muligheden for at benægte sin involvering. Droner vil sandsynligvis fortsat blive brugt til at kortlægge perimetre, sikkerhedsrutiner, udstyr og infrastruktur. Underleverandører, kommercielle mellemled og hvervning via nettet er også realistiske veje, som især statsstøttede trusselsaktører kan udnytte for at få yderligere adgang til følsomme oplysninger eller lokationer.

I 2027 vil eksponeringen sandsynligvis også omfatte hele det kommercielle netværk, der understøtter følsomme aktiviteter, og ikke kun den primære forsvars- eller infrastrukturlokation. Leverandører, logistikvirksomheder og servicepartnere kan ligge inde med oplysninger eller understøtte aktiviteter, hvor en afbrydelse rammer mere end én kunde. Den driftsmæssige betydning af en virksomheds kontrakter og samarbejder kan derfor være mere afgørende for dens eksponering end dens synlighed eller størrelse. Ændringer i disse relationer vil sandsynligvis ændre trusselsbilledet, også selvom virksomhedens egne aktiviteter er uændrede.

Droneobservationer, uforklarlige fejl på udstyr og usædvanlige henvendelser kan forstyrre driften, før årsag eller hensigt er klarlagt. Den driftsmæssige konsekvens kan blive større end selve hændelsen, hvis efterforskning og midlertidige sikkerhedsrestriktioner forlænger forstyrrelsen. En enkeltstående observation er dog ikke nok til at fastslå en fjendtlig hensigt. Om en sådan aktivitet er udtryk for en bredere trussel, afhænger derfor af, om der kan identificeres tilbagevendende mønstre i bekræftede hændelser over tid, på tværs af lokationer eller blandt forbundne virksomheder, frem for at behandle enkeltstående hændelser som bevis på en koordineret kampagne.

HOVEDKONKLUSION

Forsvarsleverandører, transportforbindelser, energianlæg og virksomheder, der støtter Ukraine, er vedvarende udsat for fjendtlig rekognoscering, spionage, aktioner via stedfortrædere, droneaktivitet og forstyrrelser, som kan benægtes. Danmarks strategiske geografiske placering og rolle i nordisk og europæisk sikkerhed øger relevansen af målretning fra både statstilknyttede aktører og aktører, der handler i overensstemmelse med statslige interesser.

Mest sandsynlige målbrancher

Branche	Eksponering	Sandsynlighed	Konsekvens	Væsentligste drivere
Forsvars- og luftfartsindustri	5 – EKSTREM	5 – EKSTREM	5 – EKSTREM	Støtte til Ukraine og deltagelse i følsomme forsyningskæder på forsvarsområdet øger eksponeringen for spionage og sabotage, mens afhængigheden af underleverandører og specialiserede leverandører udvider sikkerhedskravene ud over den primære produktionslokation.
Transport, logistik og søfart	5 – EKSTREM	5 – EKSTREM	5 – EKSTREM	Havnenes og Østersø-forbindelsernes rolle i følsomme kommercielle og militære transporter øger deres strategiske betydning, og forstyrrelser ved fælles knudepunkter kan ramme flere operatører og forsyningskæder, uden at den enkelte virksomhed er direkte mål.
Myndigheder og offentlig service	4 – HØJ	4 – HØJ	5 – EKSTREM	Myndigheder med opgaver inden for forsvar og national sikkerhed ligger inde med oplysninger af efterretningsmæssig værdi, og forstyrrelser af myndighedsfunktioner kan presse kontinuiteten i den offentlige service. Mistænkelig aktivitet omkring offentlige bygninger skal dog verificeres, før der kan vurderes at være tale om en fjendtlig hensigt.
Energi og forsyning	4 – HØJ	4 – HØJ	5 – EKSTREM	Virksomheders og den offentlige sektors afhængighed af en stabil energiforsyning øger de mulige konsekvenser af bevidst indgriben. Anlæggenes strategiske betydning er dog ikke i sig selv ensbetydende med, at der er sandsynlighed for fjendtlig aktivitet på en bestemt lokation.
Industri, produktion og kemi	4 – HØJ	3 – MODERAT	4 – HØJ	Produktion af dual use-produkter og leverancer af komponenter kan gøre producenter til mål for efterretningsindhentning eller forstyrrelser på grund af deres kunder. Kontrakternes følsomhed og de driftsmæssige afhængigheder er derfor mere afgørende for eksponeringen end virksomhedens størrelse eller synlighed alene.

Udløsende begivenheder, der sandsynligvis indikerer et forestående eller igangværende skærpet trusselsbillede

- Nye danske forsvarskontrakter, meldinger om støtte til Ukraine, militære bevægelser eller sanktioner.
- Gentagne droneobservationer, usædvanlig fotografering eller uforklarlig interesse for driften på lokationen og for medarbejderne.
- Udvisning af diplomater, placering af ansvar for fjendtlige aktiviteter eller skærpede advarsler fra efterretningstjenesterne.
- Mistænkelige henvendelser fra underleverandører, hvervningsforsøg eller anmodninger om tekniske oplysninger.

Væsentligste fysiske sikkerhedstrusler og sandsynlige angrebsveje

- Rekognoscering med droner af perimetre, sikkerhedsforanstaltninger/-procedurer, læsseområder, kommunikationsudstyr og vagtskifter.
- Skjult adgang via underleverandører, leverandører, vikarer eller kompromitterede loginoplysninger.
- Enkel sabotage mod strømforsyning, kabler, køretøjer, kommunikation eller sikkerhedssystemer.

Anbefalinger

- Kortlæg afhængigheder med relation til staten, og identificér de faciliteter, kontrakter og medarbejdere, der har størst strategisk interesse.
- Skærp sikkerhedsgodkendelser, adgangsgennemgange og kontrol med underleverandører samt indrapportering af pres eller hvervningsforsøg.
- Overvåg droner og afvigende aktivitet omkring følsomme lokationer, herunder ved at vurdere dækningen fra tv-overvågning og mobil vagtpatrulje.
- Etablér klare kontakt- og eskalationsveje til de danske myndigheder samt interne kommunikationskanaler i tilfælde af en hændelse.

TRUSSELSOMRÅDE

Kritisk infrastruktur og transportforstyrrelser

Tilbageblik på 2026

Forstyrrelser af infrastrukturen i Danmark i 2026 skyldtes oftest tekniske fejl, ulykker, ekstremt vejr og lokale driftshændelser, men fik alligevel konsekvenser over store områder eller i form af dominoeffekter. Eksempler omfattede en strømafbrydelse på hele Bornholm i forbindelse med en fejl på et søkabel, brande i transformere og kraftværker, lokale strøm- og telenedbrud samt brud på gas- og vandledninger. Hændelserne viser, at et svigt i ét kabel, én transformerstation, én transformer eller ét forsyningsknudepunkt kan ramme flere tjenester og lokationer samtidig, særligt hvor der er begrænset geografisk redundans eller begrænset redundans i nettet.

Cyberhændelsen på Femern Bælt viste også samspillet mellem digital og fysisk infrastruktur. Efter det oplyste, satte den elektroniske adgangskort ud af drift, begrænsede brugen af computere og wi-fi, lammede arbejdsfartøjer og tvang visse processer over på manuel håndtering. Det viser, hvordan kompromittering af en entreprenørs systemer kan lamme fysiske aktiver og afbryde et stort anlægsprojekt, selv når selve transportinfrastrukturen er intakt. Hyppigheden og de indbyrdes afhængigheder var mere afgørende end alvoren af den enkelte hændelse: Gentagne korte forstyrrelser kan samlet føre til tabt produktion, mistede forbindelser, forsinket distribution og problemer med bemandingen.

CASE

Datacentre

Det statsejede Energinet indførte i maj et tre måneders stop for nye aftaler om nettilslutning af store forbrugere, efter at ansøgningerne om elkapacitet var steget til ca. 60 GW – langt over Danmarks maksimale elforbrug på ca. 7 GW. Ifølge danske myndigheder har den hastigt stigende efterspørgsel fra hyperscale-datacentre, AI-infrastruktur, batterilagre og elektrificering af industrien lagt et uholdbart pres på elnettet.

I august fremlagde energiminister Samira Nawa et lovforslag, der ændrer adgangen til elnettet og nedprioriterer store elforbrugere, herunder datacentre, med henvisning til, at det nuværende system risikerer at »afspore« den grønne omstilling. Reformen skal sikre en bedre fordeling af nettilslutninger og mindske det samlede pres på elnettet ved at give ministeriet beføjelse til at afgøre, hvem der får fortrinsret til nettet, i stedet for det hidtidige »først til mølle«-princip. Prioriteringen sker i fire kategorier, hvor den højeste prioritet gives til eksisterende kunder, nye husstande, mindre virksomheder og projekter, der driver Danmarks grønne omstilling. Blandt dem, der nedprioriteres i tredje og fjerde kategori, er storforbrugere af energi, herunder datacentre.

Den nye model for prioritering af nettilslutninger blev vedtaget i Folketinget og trådte i kraft i begyndelsen af oktober. Selvom energitunge datacentre har fået den laveste prioritet, fremgår det af aftalen, at »datacentre med tilknytning til samfundskritiske funktioner kan prioriteres i kategori 1«, da den kategori omfatter »beskyttede behov og samfundskritiske funktioner«.

Kommentar: Den nye lovgivning vil sandsynligvis medføre betydelige forsinkelser i nettilslutningen af nye datacentre og andre nedprioriterede forbrugere i Danmark. Det er en reel mulighed, at ansøgninger bliver sat i bero eller trukket tilbage, hvis kapaciteten ikke kan dække efterspørgslen.

Trusselsbilledet i 2027

Strømafbrydelsen på hele Bornholm i forbindelse med en fejl på et søkabel viser, hvordan en enkelt teknisk fejl kan ramme et helt geografisk område. Indstillet togdrift, transformerbrande og netværksforstyrrelser viser desuden, at almindelige driftsfejl kan få konsekvenser på linje med bevidst indgriben. Virksomheder med centraliseret distribution, just in time-forsyningskæder eller afhængighed af én lokation vil være særligt udsatte for lignende hændelser – både utilsigtede og ondsindede – som sandsynligvis vil forekomme i hele 2027. Indbyrdes afhængigheder mellem el, telekommunikation, adgangskontrol, betalingssystemer og transport vil øge risikoen for dominoeffekter.

En central konsekvens for 2027 er, at forstyrrelser af infrastrukturen i stigende grad sandsynligvis vil ramme virksomheder, selv når deres egne faciliteter er uskadte. Medarbejdernes og underleverandørernes fremmøde, leverancer og kundernes adgang kan alle blive påvirket, når den omkringliggende transport eller forsyning svigter. Virksomheder, der deler den samme regionale infrastruktur, kan også opleve, at deres alternative lokationer eller leverandører er ramt af de samme forstyrrelser. Geografisk koncentration skaber derfor et muligt fælles svigtpunkt, som ikke kan vurderes alene ud fra robustheden på den enkelte lokation.

Genopretningens varighed og rækkefølge vil have stor betydning for konsekvenserne for virksomhederne. Strømmen kan vende tilbage, før telekommunikation, transportkapacitet eller den normale drift på lokationen er fuldt genetableret, så virksomhederne må drive forretning med delvise begrænsninger. Gentagne korte afbrydelser kan også samlet føre til tabt produktion, forsinket distribution og problemer med bemandingen, uden at der er tale om én langvarig nedlukning.

HOVEDKONKLUSION

Strømforsyning, jernbane, havne, telekommunikation og store anlægsprojekter i Danmark vil fortsat være sårbare over for tekniske fejl, ulykker, ekstremt vejr og bevidst indgriben. Lokale svigt kan hurtigt standse driften, begrænse adgangen, forsinke leverancer og skabe dominoeffekter på tværs af afhængige virksomheder.

Mest sandsynlige målbrancher

Branche	Eksponering	Sandsynlighed	Konsekvens	Væsentligste drivere
Transport, logistik og søfart	5 – EKSTREM	5 – EKSTREM	5 – EKSTREM	Transportvirksomheder er afhængige af sammenhængende net af jernbaner, havne, veje, broer, tunneler og lufthavne, så en forstyrrelse ved ét knudepunkt kan forsinke medarbejdere og gods og skabe dominoeffekter i forsyningskæderne.
Energi og forsyning	5 – EKSTREM	5 – EKSTREM	5 – EKSTREM	Energi- og forsyningsnet har koncentrerede svigtpunkter som transformerstationer, transformere og søkabler, og nedbrud kan afbryde kritiske tjenester i hele lokalområder.
Myndigheder og offentlig service	4 – HØJ	4 – HØJ	4 – HØJ	Myndigheder, beredskab og udbydere af offentlig service oplever øget efterspørgsel, når transport eller forsyning svigter, samtidig med at forstyrrelserne kan begrænse adgangen til faciliteter og forsinke kritiske ydelser.
Teknologi, datacentre og telekommunikation	4 – HØJ	3 – MODERAT	4 – HØJ	Udbydere af teknologi, datacentre og telekommunikation er afhængige af stabil strøm og netforbindelse, og et nedbrud kan derfor forstyrre mobiltjenester, betalinger, cloudplatforme og opkoblet bygnings- eller driftsstyring.
Forsvars- og luftfartsindustri	4 – HØJ	3 – MODERAT	4 – HØJ	Forsvars-, luftfarts- og sikkerhedsvirksomheder er afhængige af sikrede faciliteter, lufthavne, kommunikation og strategisk infrastruktur, og forstyrrelser af adgang eller net kan få alvorlige konsekvenser for følsomme aktiviteter og leveringsforpligtelser.

Udløsende begivenheder, der sandsynligvis indikerer et forestående eller igangværende skærpet trusselsbillede

- Gentagne fejl eller varsler om vedligeholdelse ved vigtige knudepunkter for jernbane, havne, strøm eller telekommunikation.
- Ekstremt vejr, vigtige milepæle i store anlægsprojekter, arbejdskonflikter eller hændelser til søs.
- Uforklarlig aktivitet nær søkabler, energianlæg, broer eller styringssystemer til transport.
- Samtidige forstyrrelser af forsyning og transport, der tyder på en bredere systemisk hændelse.

Væsentligste fysiske sikkerhedstrusler og sandsynlige angrebsveje

- Strømsvigt, der sætter sikrings-, produktions-, kommunikations- og adgangssystemer ud af drift.
- Spærrede eller ufremkommelige veje, jernbaner, havne og broer, der forhindrer medarbejdere og leverancer i at nå frem.
- Skader eller indgreb ved dårligt sikrede transformerstationer, kabelilandføringer, signalanlæg eller netknudepunkter.

Anbefalinger

- Kortlæg afhængigheder af strøm, telekommunikation, transport, vand og kritiske leverandører, og identificér enkeltstående svigtpunkter, der kan ramme flere lokationer eller tjenester samtidig.
- Test nødstrøm, kommunikation, adgangskontrol og manuelle driftsprocedurer for at sikre, at lokationerne kan forblive sikre og fungere under en langvarig eller trinvis genetablering.
- Udarbejd beredskabsplaner for medarbejdernes adgang, leverancer, alternative ruter, midlertidige arbejdssteder og udskiftning af leverandører, når regionale infrastrukturforstyrrelser rammer både de primære løsninger og nødløsningerne.
- Hold øje med varsler om forsyning, transport, vejr og vedligeholdelse, og fastlæg klare tærskler for eskalering og kontaktaftaler med infrastrukturoperatører og danske myndigheder.

TRUSSELSOMRÅDE

Målrettet aktivisme, protester og arbejdskonflikter

Tilbageblik på 2026

Aktivismen i Danmark i 2026 omfattede målrettede aktioner mod hovedkontorer, produktionsanlæg, investeringsselskaber og transportrelaterede virksomheder ud over almindelige protester, demonstrationer og møder. Centrale eksempler:

- Mærsk blev gentagne gange mål for aktioner på grund af påståede forbindelser til Israel, herunder forsøg på blokader og ulovlig indtrængen ved hovedkontoret i København.
- Terma oplevede i august en vejblokade, hærværk med maling og massearrestationer ved hovedkontoret. Gruppen bag aktionerne begrundede dem med virksomhedens produktion af komponenter til Forsvarets F-35-kampfly, radarer og luftforsvar.
- Kampagnen »Break the Chain« stod bag koordinerede aktioner mod Cheminova, raffinaderiet i Kalundborg, FLSmidth og PensionDanmark. Det viser, hvordan én kampagnefortælling kan forbinde producenter, investorer, ingeniørvirksomheder og industrianlæg, der indgår i forskellige led af det, aktivisterne opfatter som den samme værdikæde.

Taktikker og driftsmæssige konsekvenser varierede betydeligt, men de fleste aktioner gik ud på at forstyrre den fysiske drift på lokationerne og skade de berørte virksomheders omdømme. I andre tilfælde brugte landmænd traktorer og vejblokader i protest mod gødningsregler, bygningsarbejdere blokerede adgangen til Novo Nordisks anlæg i Kalundborg, og arbejdskonflikter i luftfarten og på jernbanen ramte transporten. Til gengæld forløb mange demonstrationer om klima og miljø, internationale konflikter, Grønland, migration og arbejdsforhold fredeligt og skabte kun begrænsede direkte forstyrrelser. De fandt dog sted hyppigt over hele landet og afspejler bredere tendenser i Europa og resten af verden.

Aktiviteten i 2026 viste også, hvordan fysisk og online mobilisering kan forstærke hinanden. Billeder fra en lokal aktion kan blive delt i ligesindede netværk og forlænge skaden på omdømmet ud over hændelsens varighed og sted. Kampagner bevæger sig desuden videre mellem forbundne virksomheder eller finder sted i forbindelse med udløsende begivenheder som generalforsamlinger, messer, domsafsigelser, kontraktmeddelelser eller mærkedage.

Trusselsbilledet i 2027

Den seneste aktivitet i Danmark viser, hvor bredt et udsnit af virksomheder der kan blive mål for kampagner. Aktivister vil sandsynligvis vælge lokationer, hvor få deltagere kan skabe uforholdsmæssigt store driftsmæssige eller mediemæssige konsekvenser. Arbejdskonflikter vil sandsynligvis forstærke forstyrrelserne fra protester, særligt inden for luftfart, logistik og kollektiv trafik. Mobilisering på nettet, livestreaming og hurtig deling af taktikker på tværs af landegrænser vil forkorte varslingstiden og øge eksponeringen for omdømmeskader.

I 2027 vil virksomheders eksponering sandsynligvis i stigende grad blive bestemt af forbindelser til kunder, investorer og leverandører og ikke kun af virksomhedens egen adfærd. En virksomhed kan blive mål for en kampagne på grund af en kommerciel relation eller en omstridt offentlig påstand, også når relationen er indirekte. Det betyder, at kampagner kan bevæge sig mellem forbundne virksomheder og lokationer.
Hvor relevant et bestemt emne er, afhænger af virksomhedens branche, lokale tilstedeværelse og synlighed, og der er ikke tale om et ensartet risikoniveau for danske virksomheder.

De driftsmæssige konsekvenser vil sandsynligvis også række ud over stedet for en demonstration eller arbejdskonflikt. Nabovirksomheder kan opleve begrænset adgang, forsinkede leverancer eller ændringer i bemanding og fremmøde til arrangementer uden selv at være mål. Når opmærksomheden på nettet fortsætter efter en fysisk aktion, kan presset på omdømmet vare længere end selve afbrydelsen.

HOVEDKONKLUSION

Kampagner i Danmark rettes i stigende grad mod virksomheders lokationer, investeringer, forsyningskæder og omdømme og ikke kun mod det offentlige rum. Blokader, besættelser, demonstrationer og arbejdskonflikter kan afbryde adgang, transport, arrangementer og kundevendt drift, mens koordineret aktivitet på nettet forstærker presset på omdømmet.

Mest sandsynlige målbrancher

Branche	Eksponering	Sandsynlighed	Konsekvens	Væsentligste drivere
Transport, logistik og søfart	5 – EKSTREM	5 – EKSTREM	4 – HØJ	Synlige og driftsfølsomme lokationer giver aktivister et pressionsmiddel, da blokader, strejker eller demonstrationer kan forstyrre transporten af passagerer og gods og tiltrække medieopmærksomhed.
Forsvars-, luftfarts- og sikkerhedsindustri	5 – EKSTREM	5 – EKSTREM	4 – HØJ	Våben, militærteknologi, droner, F-35-komponenter og støtte til væbnede konflikter kan udløse blokader eller demonstrationer ved hovedkontorer, produktionsanlæg, messer og samarbejdspartnere i forsyningskæden.
Industri, produktion og kemi	4 – HØJ	4 – HØJ	4 – HØJ	Miljøpåvirkning, udledninger, pesticider, minedrift og tilknytning til fossile brændsler kan udløse aktioner, der forstyrrer adgangen til lokationer og forstærker presset på omdømmet.
Fødevarer, landbrug og forbrugsvarer	3 – MODERAT	3 – MODERAT	3 – MODERAT	Dyrevelfærd, klimapåvirkning, landbrugspolitik og forsyningskæder med tilknytning til konflikter kan føre til boykot, pres på omdømmet og demonstrationer ved kontorer, produktionsanlæg og butikker.
Byggeri og anlæg	3 – MODERAT	3 – MODERAT	3 – MODERAT	Store projekter, råstofudvinding, udledninger og kontroversielle kunderelationer kan udløse forstyrrelser på byggepladser, kontorer eller offentlige arrangementer og rette opmærksomheden mod bredere forbindelser i forsyningskæden.

Udløsende begivenheder, der sandsynligvis indikerer et forestående eller igangværende skærpet trusselsbillede

- Meldinger fra regeringen eller virksomheder om forsvar, fossile brændsler, landbrug, udledninger, arbejdsforhold eller kontroversielle investeringer.
- Generalforsamlinger, investorarrangementer, messer, store lanceringer, domsafsigelser og kampagners mærkedage.
- Stigende omtale på nettet af en navngiven virksomhed, lokation, topleder, leverandør eller begivenhed.
- Strejkeafstemninger eller overenskomstforhandlinger, der berører luftfart, havne, jernbane, distribution eller kritiske leverandører.

Væsentligste fysiske sikkerhedstrusler og sandsynlige angrebsveje

- Blokader, fastlåsning, besættelser og bannerhappenings ved indgange, læsseområder, veje eller arrangementssteder.
- Brud på perimetersikringen eller uautoriseret medgang (tailgating) under offentlige arrangementer, vagtskifter eller ved mange besøgende.
- Rekognoscering via fotografering, offentlige registre, stillingsopslag eller legitim adgang til lokationen.

Anbefalinger

- Følg emnebaserede kampagner og fortællinger om virksomheden i både onlinekilder og lokale kilder.
- Beskyt adgangspunkter med passende tiltag uden at optrappe konflikten, og fastlæg procedurer for håndtering af lovlige protester.
- Forbered kommunikation til interessenter, muligheder for hjemmearbejde, alternative leverancer og beredskabsplaner for arrangementer.
- Sørg for, at medarbejdere i frontlinjen ved, hvordan de genkender rekognoscering og hurtigt indrapporterer ny aktivitet.

KONTAKT

Vil du vide mere om trusselsbilledet for jeres virksomhed?

Kontakt Securitas på **info@securitas.dk**

Denne rapport er omfattet af GDPR og af retningslinjer for opbevaring af data i overensstemmelse med denne lovgivning.

Securitas stiller denne efterretningsrapport (INTREP) fra Risk Intelligence Center (RIC) til rådighed for modtagerens interne forretningsmæssige brug. Rapportens indhold skal behandles forsvarligt og sikkert. Securitas påtager sig intet ansvar for beslutninger, som modtageren træffer på baggrund af rapportens indhold. Oplysningerne og analyserne i rapporten er ingen garanti for, at begivenheder indtræffer som vurderet. Rapportens indhold er fortrolig information, der udelukkende er tiltænkt adressaterne eller den ovenfor nævnte enhed.

Det er strengt forbudt at anvende Securitas' navn, varemærker, logoer, taglines, slogans eller andre kendetegn uden skriftlig tilladelse. Det er ligeledes strengt forbudt at videregive, kopiere, distribuere eller anvende nogen del af RIC's rapporter, elektronisk eller på anden måde, til andet end det formål, de er stillet til rådighed for.

Securitas