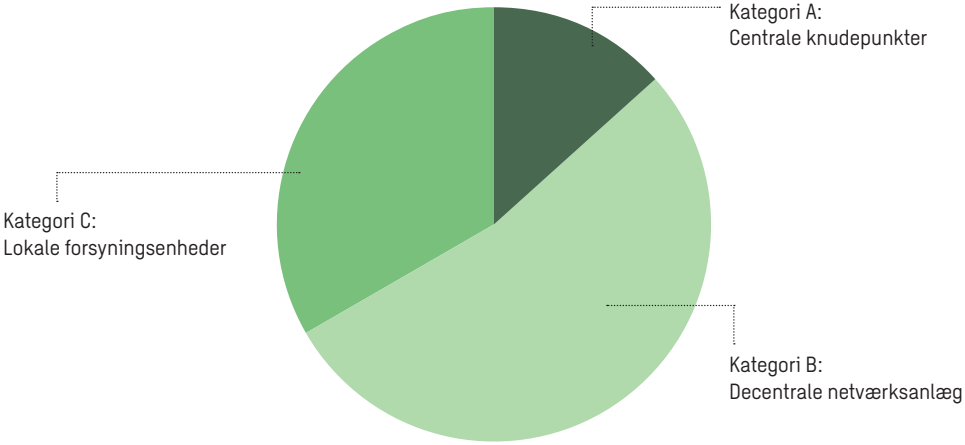
Sweco Notat

I højrisiko for hybridangreb: 8 anbefalinger til sikring af forsyningsanlæg

Hybride angreb og et skærpet trusselsbillede øger behovet for at beskytte de anlæg, der hver dag sikrer danskerne vigtige forsyninger som vand, varme og elektricitet.

Sweco har lang erfaring med beskyttelse af kritisk infrastruktur. Baseret på en række analyser for forsyningsvirksomheder giver dette notat konkrete anbefalinger til, hvordan anlæg kan rustes til sikkerhedssituationen.

Forsyningsanlæg i Danmark



Der er omkring 9000 forsyningsanlæg i Danmark af varierende størrelse og med forskellige krav til sikkerhed, hvor kategori A kræver den største indsats og kategori C kan sikres med simplere midler.

Kilder: Data er sammenstillet af Sweco baseret på tal fra Miljøstyrelsen, Energistyrelsen, DANVA, Danske Vandværker, Dansk Fjernvarme, Green Power Denmark samt kriterier for samfundskritisk infrastruktur under EU's NIS2- og CER-direktiver.

Tryghed i en ny virkelighed

Det nye trusselbillede kræver ikke panikindkøb, men en systematisk og proportionel styrkelse af sikkerheden. Det er vigtigt at få styr på i tide – først og fremmest for at beskytte centrale forsyningsanlæg mod angreb, men også for at være klar, inden EU's CER-direktiv i løbet af 2027 stiller krav til forsyningsselskabernes fysiske sikkerhed.

Pragmatisk sikkerhed for dansk forsyning

Over hele landet er der behov for, at forsyningsvirksomhederne ser kritisk på deres egen sikkerhed og arbejder mere systematisk med sikring, sikkerhed og risikostyring. Behovet er presserende i den nuværende situation. Danske myndigheder har for nyligt hævet trusselsniveauet for hybridangreb mod dansk infrastruktur, og organisationen Danske Vandværker oplever, at medlemmerne i stigende grad er mål for angreb.

Sweco har på det seneste udarbejdet flere sikkerhedsanalyser for nogle af landets største forsyningsvirksomheder. Analyserne kan være første skridt til at åbne øjnene for alvorlige sikkerhedsbrister, som kræver en øjeblikkelig indsats for at oprette sikkerheden. Udfordringerne kan løses gennem målrettede sikkerhedstiltag, øget sikkerhedsbevidsthed og en mere systematisk tilgang til beskyttelse af den kritiske infrastruktur.

Baseret på Swecos erfaringer fra en række screeninger i forsyningssektoren ser vi typiske disse udfordringer:

- Overgangen mellem IT og OT (Operational Technology): At adgangskoder til driftscomputere er tilgængelige for alle (f.eks. på en tavle), fordi anlægget historisk er bygget til tillid.
- Manglende zonering: At man, hvis man først er inde i bygningen, har adgang til alt.
- Begrænset overvågning: På flere anlæg ser vi, at der ikke er tilstrækkelig overvågning, så virksomhederne har svært ved at opdage, når der er ubudne gæster.
- Perimetersikring: Utilstrækkelig indhegning af anlæggets samlede grund, typisk manglende hegn, mure eller porte. Dermed kan man ikke nå at reagere, før der er ubudne gæster i bygningen.
- Uhensigtsmæssige rutiner omkring løsning af døre. Ulåste døre og manglende sikkerhed omkring sikkerhedssluser og mekaniske låse.

Lagdelt sikkerhed

En god tilgang til at sikre sit forsyningsanlæg er at se sikkerheden som lagene i et løg. Man kalder det også lagdelt sikkerhed eller "defense in depth".

Det handler om at sikre sit anlæg i lag og få forståelse for, at sikkerhed ikke handler om uigennemtrængelige mure, men om forsinkelse og reaktionstid.

Der ikke nødvendigvis en hardwareløsning, som passer til alle; man skal analysere hver enkelt lokation og implementere det set-up, som matcher med ambitionerne for det pågældende anlæg.

Hvert lag skal bidrage til den samlede sikkerhed. Hvis ét lag svigter, skal de øvrige lag fortsat reducere risikoen.

Ofte bruger vi den engelske D-D-D model: Deter, Detect, Delay – Afskrække, detektere, forsinke. Formålet er, at man afskrækker et angreb eller uønsket adgang. Dernæst detekterer man, at en hændelse eller et angreb finder sted, og endeligt forsinker man angrebet, så der skabes tid til reaktion.

Lag 1 – Perimetersikring
Det yderste lag skal forhindre eller opdage, at uvedkommende kommer ind på området. Det kan omfatte hegn, bomme, belysning, skiltning, kameraovervågning og perimetersensorer.

Lag 2 – Skalsikring
Det næste lag beskytter bygninger og tekniske installationer. Fokus er på døre, vinduer, ventilationsåbninger og kabelgennemføringer. Adgangskontrol, robuste låseenheder, indbrudsalarm og overvågning kan anvendes efter behov.

Lag 3 – Indre zoner og adgangsbegrænsning
Hvis en person kommer ind i bygningen, skal den indre opdeling forhindre fri adgang til hele anlægget. Områder bør derfor opdeles efter funktion, eksempelvis i almindeligt tilgængelige områder, drifts- og serviceområder, kontrolrum, teknikrum samt områder med særligt vitale systemer.

Lag 4 – Beskyttelse af IT- og OT-systemer
Det inderste lag beskytter de systemer, der overvåger og styrer forsyningen, som f.eks. servere, netværk og fjernadgang.

Sikkerhedskrav til danske forsyningsanlæg

Man kan opdele danske forsyningsværker i tre kategorier efter, hvor kritiske funktioner anlægget har.

Typer af anlæg	Omfang i Danmark	Risikoprofil & Hovedudfordring	Fokus i lagdelt sikkerhed
Centrale knudepunkter (Store multiforsyninger, el-transmission, store rensningsanlæg og kraftvarme)	Cirka 1000 adresser	**Særligt kritisk infrastruktur:** Komplekse systemer, mange medarbejdere og eksterne leverandører.	**Kerne & Indre zoner:** Stram rollebaseret adgangskontrol, adskillelse af drift og administration samt beredskabstest.
Decentrale anlæg (Fjernvarmeværker, pumpestationer, koblingsstationer, biogasanlæg)	Cirka 5.000 adresser	**Geografisk spredning / Ubemandet drift:** Sårbarhed over for fysisk indtrængen, hærværk og lokal sabotage.	**Perimeter & Skalsikring:** Elektronisk overvågning, tidlig opdagelse/verifikation, hegn og mekanisk modstand.
Lokale forsynings-enheder (Mindre forbrugerejede vandværker og lokale varmeværker)	Cirka 3000 adresser	**Ressourceknaphed / Basissårbarheder:** Manglende grundsikring (ulåste døre, adgangskoder tilgængelige, manglende alarmering).	**Basissikring & Adfærd:** Låseprocedurer, kodehygiejne, organisatoriske rutiner og simpel skalsikring.

En samlet vurdering

Sweco kan bidrage med et udefrakommende og uvildigt blik.

Konkret består det i at hjælpe forsyningsvirksomheder med at identificere og forstå det aktuelle trusselsbillede for deres segment, kortlægge sårbarheder og omsætte analysen til specifikke og prioriterede sikkerhedstiltag.

Det kan blandt andet være gennem trussels- og risikoanalyser, sikkerhedsscreeninger, sårbarhedsvurderinger, fysisk sikring, adgangskontrol, overvågning, beredskabsplanlægning og rådgivning om organisatorisk og digital sikkerhed.

Målet er ikke nødvendigvis at sikre alt mod alt, men at skabe et sikkerhedsniveau, der står mål med de aktuelle trusler og virksomhedens kritiske funktioner.

Sweco kan desuden hjælpe med at prioritere investeringerne, så ressourcerne anvendes dér, hvor de reducerer risikoen mest.

Det kan f.eks. være gennem en samlet vurdering af bygninger, tekniske anlæg, perimeter, adgangsforhold, it-systemer, medarbejderadfærd og beredskab.



8 anbefalinger til vigtige sikringspunkter

I analyser for forsyningsvirksomheder undersøger Sweco følgende 8 temaer. Det er de punkter, vi anbefaler kunder at være ekstra opmærksomme på.

1. **Etablér en robust perimetersikring**
   At sikre den yderste grænse omkring bygninger, tekniske anlæg og områder med hegn, porte, mure og eventuelt elektronisk detektering. Formålet er at forhindre uvedkommende adgang og opdage indtrængen så tidligt som muligt.

2. **Implementér effektiv adgangskontrol**
   Begræns adgangen til bygninger, områder og installationer til autoriserede personer. Anvend relevante løsninger som mekaniske låse, sikre døre, nøglekort, adgangssluser og andre adgangsgivende teknologier.

3. **Indfør systematisk besøgsstyring**
   Registrér, hvem der opholder sig på området, formålet med besøget og hvem i virksomheden, der har ansvaret for den besøgende. Sørg samtidig for klare regler for ledsagelse, adgang og udskrivning.

4. **Skab en sikker til- og frakobling af sikkerhedssystemer**
   Fastlæg sikre procedurer for betjening af alarmer og øvrige sikkerhedssystemer. Sørg for, at medarbejderne ved, hvordan systemerne til- og frakobles, og at alarmen altid aktiveres, når et område forlades.

5. **Opdel området i sikkerhedszoner**
   Inddel bygninger og anlæg i zoner med stigende krav til adgang, overvågning og beskyttelse. Tilpas sikkerhedsniveauet til områdets funktion.

6. **Installer elektronisk overvågning**
   Implementér overvågnings- og detekteringsløsninger, der kan opdage, dokumentere og understøtte en hurtig reaktion på uautoriseret adgang eller mistænkelig aktivitet.

7. **Brug rollebaseret adgangsstyring**
   Tildel adgang ud fra den enkelte persons jobfunktion og konkrete arbejdsbehov – ikke alene på baggrund af ansættelsesforhold eller anciennitet. Gennemgå og tilpas adgangsrettigheder regelmæssigt.

8. **Opret et effektivt beredskab og klare procedurer**
   Udarbejd planer for, hvordan virksomheden forebygger, håndterer og følger op på sikkerhedshændelser. Beredskabet bør blandt andet omfatte adgang til kritiske driftsmidler og alternative arbejdsgange ved tekniske nedbrud, procesforstyrrelser eller insider-sabotage.

Specialiseret rådgivning

Sweco Danmark har en specialiseret afdeling med ti medarbejdere, der udelukkende arbejder med sikkerhed.

Swecos afdeling for Forsvar og Sikkerhed er certificeret af brancheorganisation for danske forsikrings- og pensionsselskaber F&P som uvildig sikringsrådgiver. Det betyder, at virksomheder og organisationer kan få rådgivning fra en certificeret og uafhængig part, når sikkerhedsniveau, risici og behov for sikring skal vurderes.

Sweco er desuden anerkendt som Recognized Security Organization (RSO) af Trafikstyrelsen. Det giver tilladelse til at udføre myndighedskrævede sikkerhedsopgaver på havne og havnefaciliteter – områder, der i høj grad udgør en del af den kritiske infrastruktur.

Sweco er desuden medlem af Sikkerhedsbranchen, den danske brancheforening for sikring og sikkerhed.

Vores tilgang er enkel: Vi identificerer de relevante trusler og risici, vurderer sårbarhederne og omsætter dem til konkrete, prioriterede og proportionale sikkerhedstiltag.

På den måde hjælper vi organisationer med at beskytte mennesker, værdier og kritisk infrastruktur – og med at bruge ressourcerne dér, hvor de gør størst forskel.



Kontakt og yderligere information:



Carsten Werner Lund
Chefrådgiver
carstenwerner.lund@sweco.dk
+45 2723 6802

Charlotte Garset
Chefrådgiver
charlotte.garset@sweco.dk
+45 4282 1170

Henrik Sichlau
Seniorspecialist
henrik.sichlau@sweco.dk
+45 3177 9655

Mathias Rose
Pressekontakt
mathias.rose@sweco.dk
+45 5388 3104

SWECO