Business Case: Netværkssegmentering af CTS-systemer i Fynsborg Kommune

HOLTEC.DK®

Dubex:

Indholdsfortegnelse

Kontaktoplysninger

Denne case er udviklet af Jens Bertelsen, Dubex i samarbejde med Jens Lindskov Vestergaard, Holtec A/S. Casen er udviklet med det formål, at understøtte samtalen med kunder og samarbejdspartnere ifm. Cyber sikkerhed i CTS-systemer.

Risikovurderingsmetoden anvendt i casen er fra FAIR Institute der kan findes på https://www.fairinstitute.org/ FAIR Institute er en forskningsdrevet non-profit organisation dedikeret til at fremme disciplinen cyber- og operationel risikostyring gennem uddannelse, standarder og samarbejde.

Denne business case er udarbejdet til brug for Dubex og Holtec i kunde- og samarbejdsrelationer hertil og må ikke anvendes af andre, eksempelvis konsulenter, uden forudgående godkendelse fra Dubex A/S eller Holtec A/S.

Alle henvendelser vedr. denne case skal stilles til:

HOLTEC.DK®

Jens Lindskov Vestergaard
Department Manager

Email: jlv@holtec.dk
Phone: +45 7676 7676
Direct:
Mobile: +45 9189 0572

Holtec Automatic A/S
Haraldsvej 66, 1.
DK-8960 Randers SØ
www.holtec.dk

Jens Bertelsen | **Senior Cyber Security & Trust Advisor**
Dubex A/S | Gyngemose Parkvej 50 | DK-2860 Soeborg
M: +45 40 33 66 08 | D: +45 31 56 03 18

jbe@dubex.dk | LinkedIn | www.dubex.dk | About Dubex
Classification: Confidential between the parties | Email disclaimer

Dubex:

Ledelsesresumé

Denne business case præsenterer et projekt til netværkssegmentering af Fynsborg Kommunes CTS-systemer (Central Tilstands- og Styringssystemer) for at sikre compliance med NIS2-direktivet og reducere cybersikkerhedsrisici. Projektet adresserer en kritisk sårbarhed, hvor 35% af kommunens CTS-installationer har utilstrækkelig adskillelse fra det administrative netværk.

Baseret på en FAIR-risikovurdering estimeres den nuværende årlige risiko til 1.564.000 kr. Implementering af netværkssegmentering vil reducere denne risiko med 78% til 344.000 kr., hvilket giver en årlig nettobesparelse på 1.220.000 kr. Med en investeringsomkostning på 2.675.000 kr. opnås en tilbagebetalingstid på 2,2 år og en 5-årig ROI på 128%.

Udover den direkte økonomiske gevinst bidrager projektet væsentligt til kommunens NIS2-compliance og kan forebygge alvorlige driftsforstyrrelser i kritisk infrastruktur. Ledelsen anbefales at godkende projektet med opstart i Q2 2025 og fuld implementering inden udgangen af 2025.

Baggrund og problembeskrivelse

Nuværende situation

Fynsborg Kommune forvalter 187 bygninger med en samlet ejendomsportefølje på ca. 320.000 m^2. Disse bygninger styres af forskellige CTS-systemer, der kontrollerer kritiske funktioner som varme, ventilation, adgangssikkerhed og energiforsyning. Kommunens CTS-infrastruktur er karakteriseret ved:

- 7 forskellige CTS-systemer fra multiple leverandører
- Heterogen implementering over 20+ år
- Varierende sikkerhedsniveauer og netværkskonfigurationer
- Dokumenterede sikkerhedshændelser, herunder et ransomware-angreb i 2021, der påvirkede CTS-servere

En kortlægning af netværksarkitekturen viser følgende kritiske sårbarheder:

- 35% af CTS-installationerne har utilstrækkelig netværkssegmentering fra kommunens administrative netværk
- 12 systemer har direkte internetforbindelse med minimal sikkerhed
- 43 installationer har særlige konti til leverandører med varierende sikkerhedsniveau
- Mindst 15-20% af ældre installationer kører med standard/default adgangskoder

Dokumenterede sikkerhedshændelser

I oktober 2021 oplevede kommunen et ransomware-angreb, der påvirkede det administrative netværk og spredte sig til 3 CTS-servere på grund af manglende netværkssegmentering. Dette medførte:

- Midlertidigt tab af styringskapacitet på 28 bygninger
- Manuel drift i 72 timer, herunder nattevagtsdækning
- Ekstra udgifter til IT-forensic, genopretning og sikringsforanstaltninger
- Estimeret total omkostning: ca. 850.000 kr. for den CTS-relaterede del af hændelsen

Relevans ift. NIS2-direktivet

Som kritisk infrastruktur er Fynsborg Kommune underlagt NIS2-direktivet, der stiller skærpede krav til cybersikkerhed. Specifikt stiller NIS2 følgende krav, som adresseres direkte af dette projekt:

- **Artikel 21(2)(d):** Segmentering af netværk for at begrænse og forhindre spredning af cyberhændelser
- **Artikel 21(2)(g):** Implementering af politikker og procedurer til vurdering af effektiviteten af risikostyring
- **Artikel 21(2)(j):** Sikring af kritisk infrastruktur gennem adskillelse af forretningsnetværk og OT-netværk (Operational Technology)

Risikovurdering med FAIR-metoden

FAIR-metodens komponenter[1]

Factor Analysis of Information Risk (FAIR) er en kvantitativ risikovurderingsmetode, der estimerer den finansielle risiko baseret på følgende parametre:

1) **Trussel Event Frequency (TEF):** Hvor ofte en trussel forventes at forekomme
2) **Vulnerability (Vuln):** Sandsynligheden for at en trussel udnytter en sårbarhed
3) **Loss Event Frequency (LEF):** Hvor ofte tab forventes at opstå (TEF × Vuln)
4) **Primary Loss Magnitude (PLM):** Direkte tab ved en hændelse
5) **Secondary Loss Magnitude (SLM):** Indirekte tab ved en hændelse
6) **Loss Magnitude (LM):** Det samlede tab ved en hændelse (PLM + SLM)
7) **Annual Loss Expectancy (ALE):** Forventet årligt tab (LEF × LM)

[1] FAIR Institute på https://www.fairinstitute.org/

FAIR-analyse: Nuværende situation

1) **Trussel Event Frequency (TEF)**
    - Minimum: 6 forsøg pr. år
    - Mest sandsynlig: 12 forsøg pr. år
    - Maximum: 24 forsøg pr. år
    - **Estimeret TEF**: 14 forsøg pr. år

Baseret på: Aktuelle trusselsvurderinger fra Center for Cybersikkerhed, historiske data om angreb mod offentlige institutioner, og Fynsborgs egen erfaring med 6 dokumenterede forsøg det seneste år.

2) **Vulnerability (Vuln)**
    - Minimum: 10% sårbarhed
    - Mest sandsynlig: 20% sårbarhed
    - Maximum: 35% sårbarhed
    - **Estimeret Vuln**: 22% sårbarhed

Baseret på: Penetrationstests udført i 2023, dokumenterede sikkerhedshændelser, og ekspertanalyse af den nuværende netværksarkitektur.

3) **Loss Event Frequency (LEF)**
    - **Beregnet LEF**: TEF × Vuln = 14 × 0,22 = 3,08 hændelser pr. år
4) **Primary Loss Magnitude (PLM) pr. hændelse**
    - Containment-omkostninger: 85.000 kr. (IT-support, overtid, ekstern assistance)
    - Genopretningsomkostninger: 125.000 kr. (systemgenopretning, rekonfigurering)
    - Produktivitetstab: 180.000 kr. (reduceret funktionalitet, manuelle processer)
    - **Subtotal PLM:** 390.000 kr.
5) **Secondary Loss Magnitude (SLM) pr. hændelse**
    - Respondering til tilsynsmyndigheder: 30.000 kr.
    - Omdømmetab: 65.000 kr. (konservativt estimeret)
    - Juridiske konsekvenser: 23.000 kr. (potentielle bøder, reduceret via forsikring)
    - **Subtotal SLM:** 118.000 kr.
6) **Loss Magnitude (LM)**
    - **Samlet LM**: PLM + SLM = 390.000 kr. + 118.000 kr. = 508.000 kr. pr. hændelse
7) **Annual Loss Expectancy (ALE)**
    - **Beregnet ALE**: LEF × LM = 3,08 × 508.000 kr. = 1.564.000 kr. pr. år

FAIR-analyse: Efter netværkssegmentering

Trussel Event Frequency (TEF)

- *Uændret:* 14 forsøg pr. år (eksterne trusselsfaktorer ændres ikke)

Vulnerability (Vuln)

- Minimum: 2% sårbarhed
- Mest sandsynlig: 4% sårbarhed
- Maximum: 9% sårbarhed
- **Estimeret Vuln**: 4,8% sårbarhed

Baseret på: Ekspertvurdering af effekten af netværkssegmentering, branchestandarder, og erfaringer fra sammenlignelige implementeringer.

Loss Event Frequency (LEF)

- **Beregnet LEF**: TEF × Vuln = 14 × 0,048 = 0,67 hændelser pr. år

Loss Magnitude (LM)

- **Samlet LM**: 508.000 kr. pr. hændelse (uændret, da konsekvenserne af et succesfuldt angreb vil være de samme)

Annual Loss Expectancy (ALE) efter implementering

- **Beregnet ALE**: LEF × LM = 0,67 × 508.000 kr. = 344.000 kr. pr. år

Risikoreduktion

- **Årlig risikoreduktion:** 1.564.000 kr. - 344.000 kr. = 1.220.000 kr. pr. år
- **Procentvis risikoreduktion:** 78%

Projekt- og løsningsbeskrivelse

Projektets formål

Formålet med netværkssegmenteringsprojektet er at etablere en sikker og robust adskillelse mellem Fynsborg Kommunes administrative IT-netværk og de operationelle teknologinetværk (OT), der understøtter CTS-systemer og andre tekniske installationer.

Teknisk løsningsbeskrivelse

Projektet omfatter følgende tekniske komponenter og aktiviteter:

1. **Netværksredesign:**
    - Etablering af dedikerede VLAN'er for CTS-systemer

   - Implementering af demilitariserede zoner (DMZ) for ekstern adgang
   - Firewall-separation mellem IT og OT-netværk
   - Mikrosegmentering af kritiske systemer

2. **Hardware- og infrastrukturinvesteringer:**
   - 6 nye enterprise-grade firewalls til zoneadskillelse
   - 12 layer 3-switches til VLAN-segmentering
   - Netværkskablingsopdatering i 14 tekniske rum
   - 4 IDS/IPS-systemer (Intrusion Detection/Prevention)
3. **Forbedret adgangsstyring:**
   - Implementering af Jump-server for leverandøradgang
   - Etablering af privilegeret adgangsstyring (PAM)
   - 2FA for al adgang til CTS-systemer
   - Revision og konsolidering af administratorkonti
4. **Overvågning og logging:**
   - Implementering af centrallogning for alle CTS-systemer
   - Etablering af SIEM-integration for OT-miljøet
   - Automatiserede alarmer ved mistænkelige aktiviteter

Omfattede systemer

Projektet omfatter alle 187 bygninger, men med særlig fokus på:

- 84 installationer på isolerede VLAN (opgradering af sikkerhedsforanstaltninger)
- 12 installationer med direkte internetforbindelse (fuld reimplementering)
- 31 lokale netværk (etablering af sikker fjernadgang)
- 28 installationer på dedikeret fysisk netværk (integration i det nye sikkerhedsdesign)
- 32 4G/GSM-forbindelser (sikring med VPN og kryptering)

Cost-benefit-analyse

Omkostninger (CAPEX + OPEX over 5 år)

Engangsomkostninger (CAPEX)

- Hardware (firewalls, switches, IDS/IPS): 850.000 kr.
- Software og licenser: 425.000 kr.
- Implementering og konfigurering: 780.000 kr.
- Konsulentbistand: 340.000 kr.

- Projektledelse: 230.000 kr.
- Uddannelse af personale: 150.000 kr.
- Dokumentation: 80.000 kr.
- **Subtotal CAPEX:** 2.855.000 kr.

Note: Det oprindelige budget på 1,3 mio. kr. er opjusteret til 2.855.000 kr. baseret på en mere grundig analyse af omfanget og kompleksiteten.

Driftsomkostninger pr. år (OPEX)

- Vedligeholdelse af hardware: 85.000 kr.
- Licenser og abonnementer: 120.000 kr.
- Driftspersonale (delvis allokering): 275.000 kr.
- Subtotal årlig OPEX: 480.000 kr.
- **Total OPEX over 5 år:** 2.400.000 kr.

Samlede omkostninger over 5 år

- **Total (CAPEX + OPEX):** 5.255.000 kr.

Økonomiske gevinster over 5 år

Direkte økonomiske gevinster

- Reduceret risiko (ALE-reduktion): 1.220.000 kr. × 5 år = 6.100.000 kr.
- Reducerede driftsnedbrud: 110.000 kr. × 5 år = 550.000 kr.
- Effektivisering af leverandørstyring: 85.000 kr. × 5 år = 425.000 kr.
- **Subtotal direkte gevinster:** 7.075.000 kr.

Indirekte økonomiske gevinster

- Reduceret behov for akutte sikkerhedsopgraderinger: 150.000 kr. × 5 år = 750.000 kr.
- Forbedret energistyring gennem sikker integration: 120.000 kr. × 5 år = 600.000 kr.
- Reduceret compliance-omkostninger: 230.000 kr. × 5 år = 1.150.000 kr.
- **Subtotal indirekte gevinster:** 2.500.000 kr.

Samlede økonomiske gevinster over 5 år

- **Total (direkte + indirekte):** 9.575.000 kr.

Investeringsanalyse

- **Netto nutidsværdi (NPV) ved 4% diskonteringsrate:** 3.670.000 kr.
- **Intern rente (IRR):** 36%
- **Tilbagebetalingstid:** 2,2 år

- **Return on Investment (ROI) over 5 år:** 128%
- **Return on Security Investment (ROSI):** 82%

NIS2-compliance-vurdering

NIS2-krav adresseret af projektet

NIS2-krav	Opfyldelsesgrad før	Opfyldelsesgrad efter	Bemærkninger
Netværkssegmentering (Art. 21.2.d)	Lav (15%)	Høj (90%)	Direkte adresseret af projektet
Adgangskontrol og brugerrettigheder (Art. 21.2.e)	Middel (40%)	Høj (85%)	Forbedret gennem privilegeret adgangsstyring
Sikring af kommunikationsnetværk (Art. 21.2.g)	Lav (20%)	Høj (90%)	Direkte adresseret gennem firewall-separation
Hændelsesdetektering og -håndtering (Art. 21.2.i)	Meget lav (10%)	Middel (70%)	Forbedret gennem IDS/IPS og logging
Leverandørstyring (Art. 21.2.j)	Lav (25%)	Middel (75%)	Forbedret gennem jump-servers og kontrolleret adgang
Beredskabshåndtering (Art. 21.2.k)	Meget lav (10%)	Middel (60%)	Delvist adresseret gennem forbedret segmentering

Samlet NIS2-compliance-effekt

- **Nuværende compliance-niveau:** 20% (estimeret)
- **Forventet compliance-niveau efter implementering:** 65% (estimeret)
- **Resterende gap:** 35% (kræver yderligere projekter)

Note: Fuld NIS2-compliance kræver yderligere indsatser ud over netværkssegmentering, herunder forbedret patch management, hændelsesrapportering og kompetenceudvikling.

Konklusion og anbefaling

Primære konklusioner

1. **Kritisk sikkerhedsbehov:** Fynsborg Kommune har kritiske sårbarheder i CTS-netværksarkitekturen, hvilket udgør en væsentlig risiko for driften af kommunens bygninger og infrastruktur.
2. **Betydelig risikoreduktion:** Netværkssegmenteringsprojektet kan reducere den årlige risikoeksponering med 78%, fra 1.564.000 kr. til 344.000 kr.
3. **Positiv business case:** Med en tilbagebetalingstid på 2,2 år og en 5-årig ROI på 128% udgør projektet en økonomisk fornuftig investering.
4. **NIS2-compliance:** Projektet vil væsentligt forbedre kommunens opfyldelse af NIS2-direktivets krav, særligt vedrørende segmentering af netværk for at begrænse cyberhændelser.

Anbefalinger

1. **Godkendelse af investering:** Det anbefales at godkende en investering på 2.855.000 kr. til implementering af netværkssegmentering for CTS-systemer.
2. **Opjustering af budget:** Det oprindelige budget på 1,3 mio. kr. bør opjusteres til 2.855.000 kr. for at sikre en robust og fremtidssikret implementering.
3. **Styrkelse af governance:** Parallelt med den tekniske implementering bør der etableres en tværgående OT-sikkerhedsgruppe med klart mandat og ansvar.
4. **Faseopdelt implementering:** Implementeringen bør følge den foreslåede faseplan med en grundig pilotfase før fuld udrulning.
5. **Opfølgende projekter:** Dette projekt bør ses som første fase i en samlet NIS2-compliancestrategi, der efterfølgende bør suppleres med yderligere projekter inden for incident response, patch management og leverandørstyring.