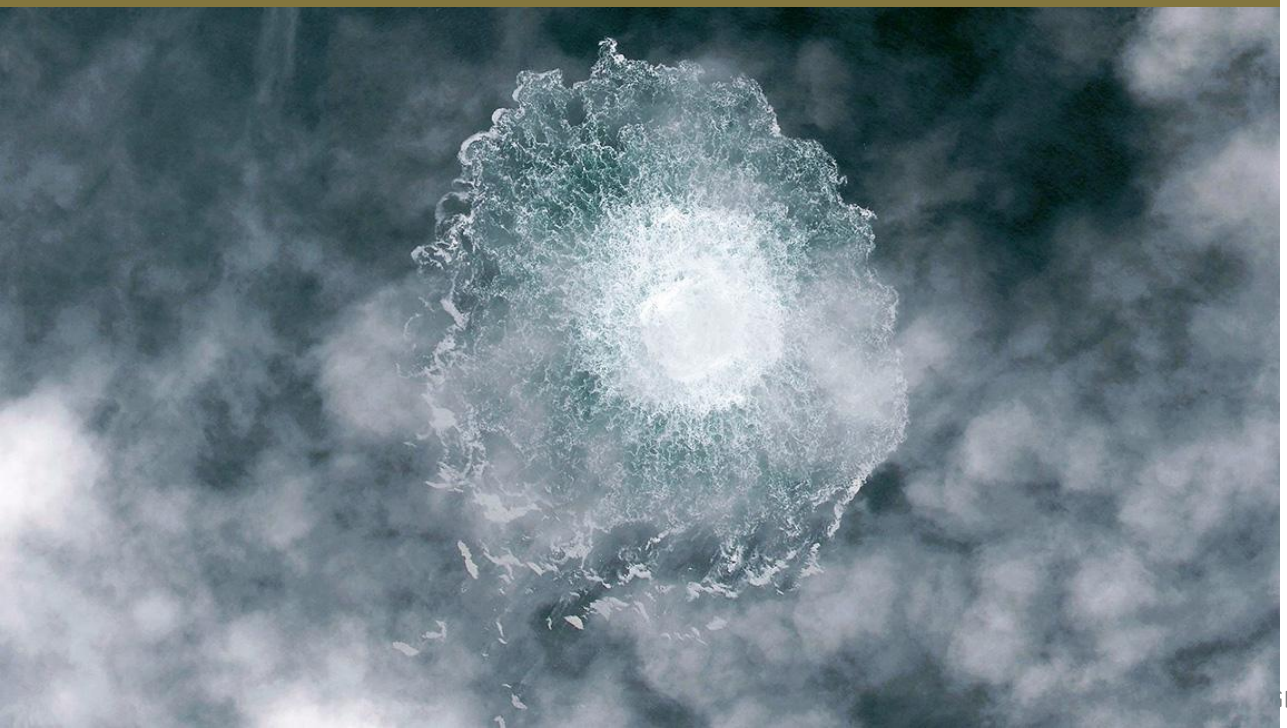
Kommunerne og hybridkrig

Foretræde for Digitaliseringsudvalget, Forsvarsudvalget og Indenrigsudvalget

Kommunerne oplever samme trusselsbillede som det øvrige Danmark

Det hybride trusselsbillede er alvorligt, jf. FE's vurdering, og Statsministeren



Hidtil har danske kommuner holdt de helt alvorlig angreb fra døren

9 ud af 10 kommunale IT-chefer siger, at de ikke længere kan følge med

Mere end 50% af kommunerne oplever mere en 1.000 angrebsforsøg pr. dag

Kommunerne behandler nogle af borgernes mest følsomme data, bl.a. anbringelser, visiteringer, medicindata, diagnoser mv.

De fleste borgere –særligt de mest sårbare - er afhængige af at Kommunerne fungerer - også i en større krise

KL foretræde for 3 udvalg

Status for krav til kommunernes arbejde med cybersikkerhed – Krav til store indsatser

Kommunerne er blevet omfattet af den danske NIS2 lovgivning

Aftale med regeringen om etablering af 4-5 kommunale it-driftsenheder med udg. pkt. i geografien i de fire regioner

Inden udgangen af 2027 overtages kommunernes drift af servere og netværksinfrastruktur

Fælles ambition: enhederne overtager gradvist driften af øvrige dele af basis-it frem mod 2030

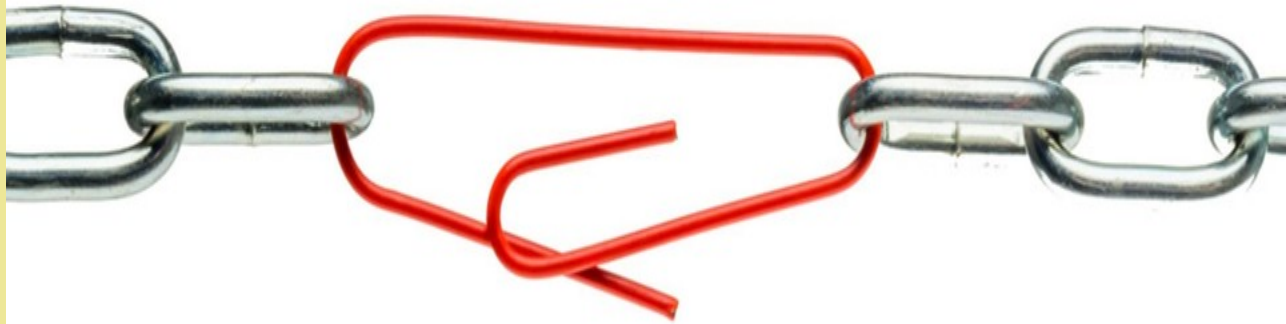
Kommunernes cyber-sikkerhedsarbejde

Kommunerne arbejder fokuseret og seriøst med cyber- og informationssikkerhed. Områder, som skal styrkes i den kommende tid:

- Øge evnen til at opdage og reagere på cyberangreb,
- Styrke de tekniske beskyttelsestiltag, særligt sikkerhed i IOT-udstyr og opdeling af netværket.
- Styrke risikostyring i den samlede organisation
- Sikre et højere niveau i de kommuner der ligger lavest i deres indsatser.

Kommunale behov

- Klare udmeldinger om krav til niveau for cybersikkerhed i kommunerne
- Undlad ”bør” og fokuser på ”skal” i vejledningerne for NIS2.
- At statens sikkerhedstjenester deler viden om sårbarheder og trusler med kommunerne
- Tydelige beredskabsscenarier så kommunerne kan være beredte
- Styrk fælles beredskab ved øvelser på tværs af myndigheder



Kommunale behov

- Styrket cybersikkerhed, en vigtig del af beredskab og robust service til borgerne
- National kapacitet til at bistå med at sikre genopretning i kommuner efter cyberangreb, som en del af cyberforsvaret.
- En stærk CSIRT med ressourcer til at styrke kommunernes NIS2 arbejde, bl.a. i samarbejde med KommuneCERT

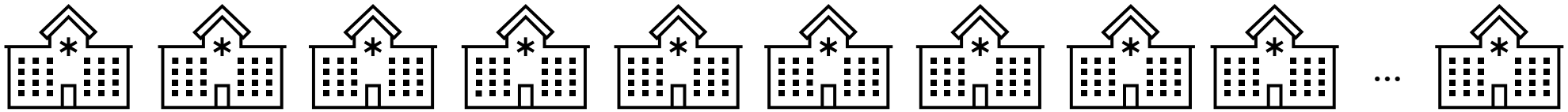
Kommunerne er i gang

- KOMBIT er i gang med at etablere kommunalt samarbejde om cybersikkerhed - en KommuneCERT – vi ønsker formelt ophæng til national sikkerhedsarbejde.
- Kommunernes samarbejde skal sikre styrkede kommuner og gøre det let(tere) for statens sikkerhedsenheder at samarbejde med 98 forskellige myndigheder

Kommunalt interessentlandskab

FORSLAG - ikke aftalt!

- Kommunerne løser alle opgaver, der ikke kan løses i fællesskab ift. NIS2 (tekniske og org.)



Fælles opgaveløsninger, hvor det er muligt:

- Underretning til/fra kommuner
- 24/7 støtte
- Monitorering og overvågning
- Understøtte national myndighed ift. varsler & trusler
- Gendannelseshjælp
- Analyser af logs
- Krav til indkøb
- …

Kommune CERT

- Tilsyn for 890 kommunale systemer v. leverandører
- Skabeloner til systemspecifikke risikovurderinger
- Compliance-pakker til kommunernes kontrol ift. forsyningskædesikkerhed
- Krav til indkøb
- …

DBS Det fælleskommunale DATA BEHANDLER SEKRETARIAT

- Omkostningseffektiv indkøb af sikkerhedsprodukter til kommunerne
- Compliance-pakker til kommunernes kontrol ift. forsyningskædesikkerhed
- Krav til indkøb
- …

SKI

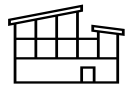
Tilsynsmyndighed

CSIRT

- Varslinger
- Platform til indberetning
- National (fælles) trussels- og sårbarhedsplatform (MISP)
- Fælles test/scanning (?)
- Udrykningsteam (IR) (?)
- Træning og uddannelse (?)

KOMBIT

- Underretning vedr. KOMBIT systemer for kommunerne
- Evt. revisorerklæringer
- Compliance-pakker ift. forsyningskædesikkerhed
- Krav til indkøb
- …



Store leverandører

- Underretning for kommunerne
- Evt. revisorerklæringer
- Compliance-pakker ift. forsyningskædesikkerhed
- Krav til indkøb
- …

4-5 kommunale it-driftsorganisationer

- Aftalt som led i økonomiaftalen for 2026
- Aftalt med baggrund i cybersikkerhed, om end de konkrete scenarier er uklare for kommunerne.
- På den korte bane en reel risiko for cybersikkerheden i kommunerne kan blive udfordret af dette.
- På den lange bane ønske om standardiserede professionelle enheder, hvor den basale cybersikkerhed er indarbejdet.
- Nye spørgsmål om de 4 – 5 centre bliver et attraktivt mål for angreb