Forsvarsudvalget 2022-23 (2. samling)
FOU Alm.del - Bilag 116
Offentligt

KL's udspil til ét samlet cyberforsvar

Ét samlet cyberforsvar

Fremtidens trusselsbillede rummer ikke kun traditionelle militære trusler, men også bredere sikkerhedspolitiske udfordringer som fx cyberangreb. Som et af de mest digitale samfund i verden spiller de digitale løsninger også en større rolle i den danske velfærd og de offentlige services. Men risikoen for at blive ramt af ødelæggende, dyre og kritiske cyberangreb er steget væsentligt den seneste tid.

Vi skal sikre os, at de indsatser, der laves i kommunerne for at forebygge cyberangreb, matcher den eksisterende trussel. Det svageste led i kæden kan hurtigt blive bagdøren ind til hele det offentlige Danmark. Derfor er det afgørende at styrke hele landets cyberforsvar og -sikkerhed, så vi står stærkere over for det alvorlige trusselsbillede, vi kigger ind i.

Kommunerne skal indgå som en del af det danske cyberforsvar til gavn for hele rigets sikkerhed. Men det er ikke en opgave, kommunerne kan tage på sig alene. Det er afgørende med national initiativ og finansiering, der sikrer, at indsatser mellem stat, kommuner og regioner koordineres.

KL foreslår:

1. Kommunerne skal indgå som en del af det danske cyberforsvar. Det offentlige er bundet sammen digitalt, og det svageste led kan hurtigt blive bagdøren ind.
2. Folketinget skal sikre de nødvendige økonomiske og politiske prioriteringer, så landets samlede cyberforsvar bliver styrket.
3. Kommunerne skal efterleve minimumskrav for cybertrusler, der er med til at sikre høj sikkerhed i et digitalt tæt koblet Danmark.
4. Kommunerne skal håndtere cyberindsatsen i fællesskab – også med stat, regionerne og private aktører.
5. Der skal sikres de nødvendige kompetencer til den kommunale opgaveløsning med cyber- og informationssikkerhed.

1. Kommunerne skal indgå som en del af det danske cyberforsvar

Kommunerne er tæt forbundet til bl.a. sundhedssektoren, forsyningssektoren og en række samarbejder i forbindelse med trafik, havne, miljø mv. De tætte forbindelser giver en række fordele for borgere og virksomheder i Danmark. Men også risiko for, at angreb i én organisation, kan sprede sig til et angreb på anden.

Det er nødvendigt med et basalt sikkerhedsniveau inden for flere cyberdiscipliner i hele den offentlige sektor for at modvirke det. Det gælder inden for beskyttelse af enheder, styring af brugerrettigheder, kryptering, udveksling af data i private former, opdeling af netværk i segmenter, sikring af Internet of Things (IoT) devices mv.

KL

Det svageste led kan hurtigt blive bagdøren ind.

1. Kommunerne skal indgå som en del af det danske cyberforsvar

Kommunerne er den myndighed med størst borgerkontakt og samlet set flest myndighedsopgaver. Velfærden under cyberangreb sikres kun, hvis kommunerne er med i det samlede danske cyberforsvar og dermed robust kan modstå ondsindet aktivitet.

Kommunerne arbejder tæt sammen med andre myndigheder, om at tilbyde velfærd til danskerne. Trusler og sårbarheder varierer dog fra kommune til kommune. Den enkelte kommunes indsatser skal derfor ske med afsæt i en konkret vurdering af kommunens risici. Derfor bør kommunerne omfattes af Net- og Informationssikkerhedsdirektivet (NIS2).

Tillid opbygges over lang tid, men kan mistes på kort tid. Det er derfor altafgørende, at kommunerne ikke udsættes for store digitale nedbrud med årsag i kriminalitet.

KL

Vi skal stå sammen i Danmark om en velfungerende digital velfærdsstat, derfor er kommunerne kritisk infrastruktur.

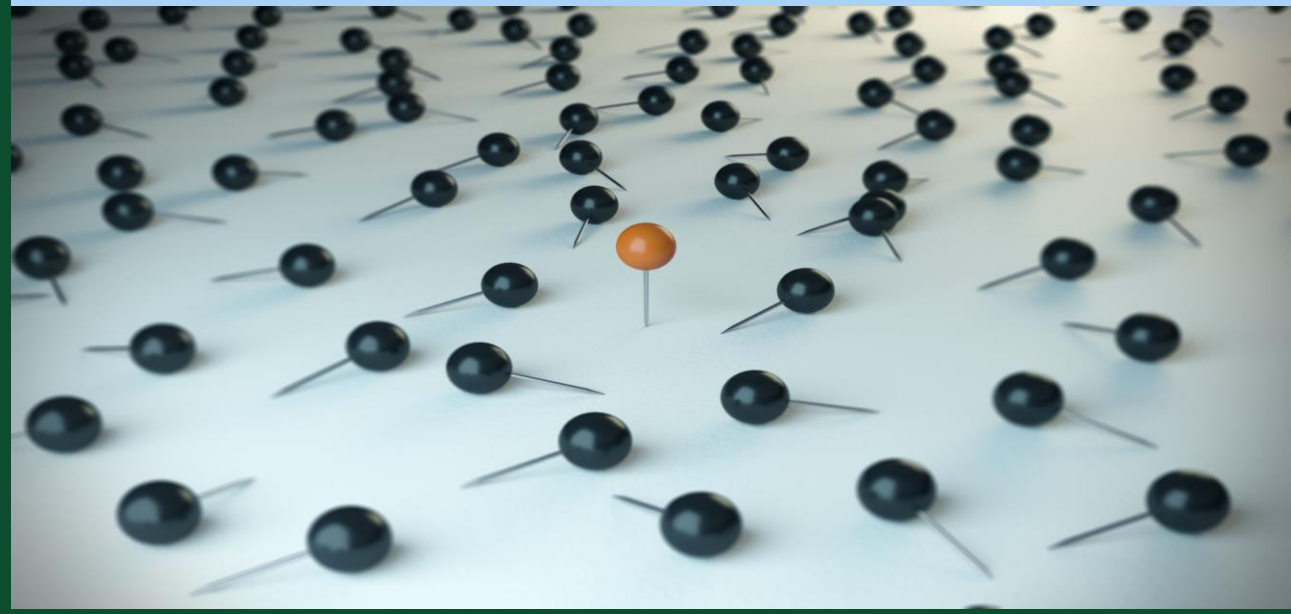
2. Der er brug for at opprioritere cyberforsvaret

Økonomisk kriminalitet, spionage og cyberaktivisme er alle trusler, der vurderes ”meget højt” eller ”højt” i trusselsniveau af Center for Cybersikkerhed. Det haster derfor at få sikret borgernes data i de enkelte kommuner. Er data først stjålet af kriminelle, så er de kompromitteret resten af borgerens levetid.

Det haster også med at sikre, at services i myndighederne er tilgængelige, når kommunerne er under angreb. Hele det offentlige Danmark skal være robust. Det er bedre at starte i dag, end at vente til i morgen.

Der er en bred palet af initiativer, der skal gennemføres, men det vigtige budskab er at starte på cyberområdet nu, for truslen er reel og støt stigende.

Lige nu er der mange trusler imod Danmark, og kommunerne er konstant under virtuelt angreb.



3. Kommunerne skal efterleve minimumskrav for cybertrusler

Myndighedernes indsats i forhold til cyber- og informationssikkerhed har aldrig været vigtigere. Det er en indsats, der løbende er blevet udbygget igennem årene med øget digitalisering i Danmark. Med GDPR kom et sæt spilleregler og krav, som alle skal leve op til. NIS2 er den næste ramme, der skal være med til at højne Danmarks samlede cyber- og informationssikkerhed.

Tre grundpiller skal kontinuert være i fokus i kommunernes opgaveløsning. For det første skal der være en grundlæggende tillid til, at borgernes oplysninger i forbindelse med myndighedsbetjening opbevares forsvarligt. For det andet, at borgernes oplysninger ikke ændres utilsigtet og for det tredje er tilgængeligt til sagsbehandling. Med det niveau for trusler vi har nu, så haster det med en øget indsats.

Myndighedsområderne er ikke underlagt konkurrence, borgerne kan ikke vælge andre til at løse opgaven for sig. Derfor har vi et særligt ansvar for, at de offentlige løsninger er sikre.

4. Kommunerne skal håndtere cyberindsatsen i fællesskab

Sårbarhederne i landets digitale infrastruktur er ensartet på tværs af sektorer og kommuner og kan forebygges ved en samlet og koordineret indsats. Det kræver, at kommunerne, sammen med andre myndigheder, har en stærk base for udveksling af information om trusler og sårbarheder. Det skal bl.a. være med til omkostningseffektivt at dæmme op for sårbarheder i den kommunale infrastruktur.

Indsatserne for at sikre staten, regionerne og øvrige aktører er brede. Derfor er det vigtigt at koordinere ensartet fra staten for at sikre, at kommunerne får den nødvendige støtte til beslutninger ved cyberangreb.

Truslen findes døgnet rundt, året rundt. Kommunerne skal derfor have kapacitet til at dæmme op for trusler, der matcher dette.

Kommunerne kan og vil samarbejde om at modstå cybertrusler. I et bredt samarbejde mellem staten, regionerne, private aktører og kommuner, skal der skabes effektive og sikre værn mod trusler.

5. Der skal sikres nok kompetencer og fastholdelse i kommunerne

Manglen på de rette kompetencer er en af de største udfordringer for at tage nye sikkerhedsteknologier i brug og sikre organisationer. Det vurderer Gartner og andre analyseinstitutter.

Der er behov for flere professionelle cyberspecialister, men også behov for at arbejdsmarkedet generelt ser på nye muligheder for at uddanne og efteruddanne.

Lad også andre faggrupper komme til, hvor det er muligt. Basal træning og kurser kan skabe nye kompetencer, der i samarbejde med specialister kan løse vigtige sikkerheds-opgaver. På den lange bane kan samarbejde med uddannelsessteder sikre medarbejdere med basale digitale sikkerhedskompetencer i fremtiden.

KL

Kompetencer er altafgørende for at kunne sikre en digital velfærdsstat. Kompetencerne skal sikres i alle roller, så der i fremtiden er nok hænder også til de tunge it-tekniske opgaver i kommunerne.