Cyberalliancen består af Green Power Denmark, Danske Rederier, Finans Danmark, Teleindustrien og DANVA

Cyberalliancens input til national strategi for cybersikkerhed 2025-2027

Digitaliseringen skaber vækst og arbejdspladser i Danmark, styrker demokratiet og adgang til information og giver danske virksomheder en konkurrencefordel på de internationale markeder. Men digitaliseringen gør os også sårbare overfor cyberangreb og spionage. I lyset af den voksende cybertrussel fra særligt Rusland, er der god grund til at se nærmere på, hvordan Danmarks cyberforsvar kan styrkes.

Tidligere nationale strategier for cybersikkerhed har skabt et solidt fundament for arbejdet med cybersikkerhed i Danmark. De igangsatte aktiviteter og den retning, der er sat for sikkerhedsarbejdet bør i vid udstrækning fastholdes. Med en stærk forpligtelse til at beskytte vores digitale og fysiske infrastruktur og samfundet som helhed, præsenterer Cyberalliancen *(bestående af Green Power Denmark, Danske Rederier, Finans Danmark, Teleindustrien og DANVA)* her vores input til, hvad der bør sættes fokus på i en national cybersikkerhedsstrategi for de kommende år.

1. Styrkelse af samarbejde og videndeling

I lyset af den voksende trussel rettet mod Danmark er det Cyberalliancens anbefaling, at arbejdet med sikker udveksling af efterretninger og informationer mellem virksomheder, sektorer og myndigheder intensiveres og udbygges yderligere.

Et vigtigt element i et effektivt cyberforsvar handler om hurtig adgang til opdaterede varsler og efterretninger om trusler, sårbarheder og risikovurderinger. Jo bedre informationer der er til rådighed om trusler, sårbarheder og risici, jo bedre kan sektorerne og virksomhederne håndtere angreb og styrke robustheden og modstandskraften i deres tjenester og infrastruktur.

Sektoransvarsprincippet er det rigtige udgangspunkt. Men der er brug for at styrke samarbejde og videndeling mellem sektorerne, de ansvarlige sektormyndigheder og Center for Cybersikkerhed. Virksomhederne ude i sektorerne har brug tidlig varsling og for relevante efterretningsbaserede informationer til at styrke deres beredskab og forsvar for dermed at kunne beskytte deres forretning og sikre deres leverancer til deres kunder i samfundets interesse. Den geopolitiske udvikling medfører, et øget behov for ”intelligence sharing” med virksomhederne.

Myndighedernes vidensdeling bør tilsvarende omfatte øget rådgivning om tolkning af risikovurderinger bl.a. i forbindelse med leverandørsamarbejde og afgrænsning af, hvad der defineres som kritisk infrastruktur.

Det er helt afgørende at sikre en skarp adskillelse af samarbejds- og rådgivningsindsatsen fra tilsynet med sektorerne og virksomhederne.

2. Fokus på afhængigheder mellem samfundskritiske sektorer

Med den øgede digitalisering bliver afhængighederne mellem sektorerne meget tydelige. Uden elektricitet og internet er mange opgaver svære at varetage og opretholde. Hvis mobilnettene er nede, så er det vanskeligt at tilkalde hjælp. Uden en velfungerende vandforsyning er sundhedssektoren udfordret. Uden en velfungerende transportsektor besværliggøres adgangen til nødvendige forsyninger og transport af borgere og varer fra A til B.

Den skærpede sikkerhedspolitiske situation kræver et styrket nationalt samarbejde mellem myndigheder på tværs af sektorerne.

Det er Cyberalliancens anbefaling, at der bør tages initiativ til at gennemføre grundige, nationale analyser og øvelser med deltagelse af medarbejdere på tværs af sektorerne for at identificere og træne håndtering af potentielle kritiske afhængigheder og svagheder i vores digitale infrastruktur.

3. Mere operationelle trusselsvurderinger

Truslen mod den kritiske infrastruktur har ændret sig og er blevet mere konkret og omfatter nu i højere grad end tidligere også en risiko for fysisk sabotage.

Beskyttelse af landets borgere og virksomheder mod fysiske angreb er en naturlig samfundsopgave. En styrkelse af sektorernes sikkerhed – både den digitale og den fysiske - kræver et intensiveret samarbejde mellem myndighederne, forsvaret og de enkelte sektorer.

Myndighederne skal for hver samfundskritisk sektor udarbejde mere detaljerede og operationelle trusselsvurderinger – både for den fysiske og for den digitale infrastruktur. De mest kritiske elementer i infrastrukturen bør identificeres i samarbejde mellem virksomhederne og myndighederne, og der bør sikres meget klare rammer for rolle- og ansvarsfordelingen, herunder overvågning og beskyttelse af knudepunkter, centraler og stationer, kabler, rør og andre kritiske infrastrukturelementer.

4. Styrkelse af det nordiske samarbejde

Med den seneste cybersikkerhedsstrategi blev der sat fokus på betydningen af internationalt samarbejde for at styrke cybersikkerheden i Danmark. Det internationale samarbejde bør styrkes yderligere, herunder særligt det nordiske samarbejde.

Med Finlands og Sveriges indtræden i NATO er der grund til at intensivere det nordiske samarbejde og sikre aktiv deltagelse i NATO-initiativer og -øvelser for at styrke vores cyberberedskab og koordinere indsatsen mod cybertrusler.

De nordiske lande deler mange karakteristika, og der kan derfor være stor værdi i en stærkere udveksling af information og et stærkere samarbejde mellem myndigheder og inden for de enkelte sektorer på tværs af lande i Norden.

Med et styrket nordisk samarbejde bør det sikres, at der etableres et mere enkelt og mere effektivt system til sikkerhedsgodkendelse af medarbejdere, f.eks. gennem gensidig anerkendelse af eksisterende sikkerhedsgodkendelser.

5. Uddannelse og kvalificeret arbejdskraft

Allerede i dag er der mangel på it- og cybersikkerhedsspecialister i Danmark. Manglen på kvalificerede it- og cybersikkerhedsspecialister er en stor udfordring i erhvervslivet og udgør en trussel for vores sikkerhed. Og problemet bliver kun større i fremtiden efterhånden som digitaliseringen øges og behovet for at styrke vores sikkerhed vokser.

Der bør derfor sættes politisk fokus på at sikre et øget optag af unge på it-uddannelserne. Og der bør sikres øgede investeringer i avanceret træning og videreuddannelse af personale inden for cybersikkerhed og -beredskab gerne i samarbejde med virksomhederne og organisationer som ISACA, Women4Cyber m.fl.

6. Kunstig intelligens

Kunstig intelligens har potentialet til på en række områder at øge vores robusthed mod cybertruslen. Fx kan kunstig intelligens styrke cybersikkerheden ved at automatisere hændelsesrespons, overvåge anomalier i netværkstrafik og kombinere menneskelig intelligens med AI.

Men med kunstig intelligens risikerer vi også at cybertruslen øges. Det vil fx give nye muligheder for at konstruere deep fakes og automatisere udsendelsen af målrettet og skræddersyet manipuleret indhold til både myndigheder, virksomheder og borgere.

Samme teknologi vil også øge risikoen for en stigning i den allerede markant voksende it-relaterede økonomisk svindel, der også bliver anvendt til at finansiere anden kriminalitet, herunder cyberkriminalitet.

For at sikre en mere effektiv indsats mod risikoen for de negative virkninger af kunstig intelligens er der behov for at samle ansvaret og koordinere indsatsen med udgangspunkt i en målrettet strategi.

Mange aktører skal bidrage til dette arbejde. Det gælder lige fra politiet, universiteterne, ministerier og myndigheder, til finanssektoren, telesektoren, sikkerhedsbranchen og store teknologivirksomheder som fx Meta, Google og Apple.

Cyberalliancen er fast besluttet på at arbejde tæt sammen med regeringen og andre relevante interessenter for at styrke Danmarks cybersikkerhed og forblive robust over for fremtidige trusler. Vi ser frem til at samarbejde om implementeringen af disse forslag og skabe grundlaget for et mere sikkert og robust digitalt samfund.

Cyberalliancen består af Green Power Denmark, Danske Rederier, Finans Danmark, Teleindustrien og DANVA

Noter: