Cyberalliancens ideer til den kommende nationale strategi for cyber- og informationssikkerhed

Danmark er et af de mest digitaliserede samfund i verden. Det gør livet lettere for både borgere, det offentlige og erhvervslivet. Digitaliseringen skaber vækst og arbejdspladser, og den giver danske virksomheder en konkurrencefordel på de internationale markeder.

Medlemmerne af Cyberalliancen – Dansk Energi, Danske Rederier, Finans Danmark, Teleindustrien og DANVA, som er repræsentanter for en række samfundsvigtige sektorer, har et særligt fælles ansvar. For skal vi fortsat høste gevinsterne ved øget digitalisering, kræver det, at der stadig er tillid til den digitale infrastruktur og de digitale services i Danmark, hvad enten det er knyttet til energi- og vandforsyning, spildevandsrensning, transport af mennesker og gods, sundhedsområdet, finansielle transaktioner eller brug af telefoni og internet.

Danmark står stærkere på cyberområdet, når vi marcherer i takt på tværs af private og offentlige aktører. Derfor følger en række af Cyberalliancens medlemmer - Dansk Energi, Danske Rederier, Teleindustrien, DANVA og Finans Danmark de 20 tekniske minimums it-sikkerhedskrav, som staten stiller til sig selv. Implementeringen sker på baggrund af en risikobaseret tilgang.

Cyberalliancens medlemmer - Dansk Energi, Danske Rederier, Teleindustrien, DANVA og Finans Danmark finder, at der behov for yderligere at forbedre cyber- og informationssikkerheden i hele Danmark. Vi har derfor en række konkrete ideer til, hvad der er vigtigt at medtage i den kommende nationale strategi.

1. Klare rammer for samfundsvigtig infrastruktur og brug af leverandører

Det bliver i stigende omfang en del af virksomheders og myndigheders sikkerhedspolitiske overvejelser, om der i kritisk infrastruktur kan være udstyr og services fra leverandører, der har hjemme i lande, som ikke er blandt Danmarks tætteste allierede. Det gælder i komponenter som pc'er, kameraer og hardware og software af forskellig art. Problemstillingen gælder også i forhold til, hvad myndighederne vil tillade og acceptere af ejerskab af selskaber, som er en del af de samfundsvigtige sektorer i Danmark. For alle aktører er det vigtigt, at der er klare rammer, og passende krav og regler på området, så det fx er afklaret, hvad der er kritisk infrastruktur, og hvilke krav der stilles til leverandører. Det vil give forudsigelighed og gennemsigtighed for alle parter.

Vi mener derfor, at regeringen som en del af en samlet strategi på cybersikkerheds- og beredskabsområdet bør have fokus på at sikre klare og forudsigelige rammer for selskaber i de samfundsvigtige sektorer, bl.a. hvad angår ejerskab og brug af leverandører. Vi finder det vigtigt, at vi både som nation og som europæisk fællesskab på en ensartet måde definerer, hvem og hvad der eventuelt underlægges regulering, og hvilke begrænsninger der gælder.

2. Sikring af tilstrækkelige ressourcer til politiet til opklaring af cyberangreb mod virksomheder

Det er ofte vanskeligt og ressourcekrævende at opklare cyberangreb på virksomheder. Politiet har ikke tilstrækkelige ressourcer i det nationale center for Cybercrime (NC3) til at opklare de ofte meget alvorlige angreb. Cyberangreb er blevet hverdag i dansk erhvervsliv. Forsvarets Efterretningstjeneste vurderer, at truslen fra cyberkriminalitet er meget høj. Myndigheder og virksomheder i samtlige sektorer i Danmark kan forvente løbende at blive udsat for cyberkriminalitet.

Visse typer cyberkriminalitet kan have alvorlige konsekvenser for myndigheder og virksomheder i samfundsvigtige sektorer og derfor for det danske samfund. Der er flere eksempler på meget store tab i virksomheder. Derfor foreslås det, at det nationale Center for Cybersikkerhed (NC3) sikres tilstrækkelige ressourcer til at opklare cyberangreb. Det er helt afgørende i forhold til at få stoppet og forebygget angrebene.

3. Styrk den operationelle videndeling mellem de samfundsvigtige sektorer gennem regulatoriske frirum

Det er en udfordring at sikre tilstrækkelig videndeling mellem virksomheder og myndigheder. Årsagerne hertil er mange, da både Konkurrenceretten, udsigten til myndighedstilsyn og risikoen for skærpede myndighedskrav spiller ind samt at virksomheder og organisationer ønsker at værne om deres omdømme. Viden om angreb er dog helt afgørende for at forhindre cyberangreb og it-sikkerhedsbrud. At skabe en ramme, hvor viden kan deles i tillid til hinanden, er dog ikke nogen nem opgave. Det vil uvilkårligt kræve, at virksomhederne og organisationerne har ledelsesmæssig opbakning til at "åbne sig op", og at myndighederne samtidig sender et klart signal om, at "pisken" er lagt væk og at man i stedet får skabt de nødvendige og regulatoriske frirum til videndeling.

Den aktuelle Covid-19-situation har – særligt tilbage til nedlukningen af Danmark i marts 2020 – vist, at når vi er beredt og vi står sammen, kan vi agere hurtigt og begrænse konsekvenserne af en udefrakommende påvirkning. Som sektorer og som samfund har vi en interesse i at spotte og identificere de trusler, som nærmer os og banker på vores dør. I Cyberalliancen er vi derfor opmærksom på, at pilen også peger på os selv. For som virksomheder i de samfundsvigtige sektorer udgør vi forposter i det nationale cyber-forsvarsværk.

Hvis vi som nation kan lykkes med i fællesskab at samle og operationalisere både myndighedernes og virksomhedernes viden om

trusselsbilledet, så kan vi styrke vores forsvarsværk over for kendte såvel som ukendte trusler og ikke kun begrænset til cybersikkerhed.

Men hvornår er en sikkerhedshændelse kritisk *nok* til, at virksomhederne i en travl hverdag, hvor tingene går stærkt og hvor problemer løses ad hoc, indberetter den mystiske mail, som blev afvist ved hoveddøren. Vi vurderer, at nationale myndigheder har ét behov og ønske om viden om hændelser, mens virksomhederne har et andet.

Vi foreslår derfor, at der skabes et regulatoriske frirum, som kan muliggøre øget dialog mellem myndighederne og de samfundskritiske sektorer for at styrke den tidlige vidensdeling. Jo større viden om angreb i så tidlig en fase som muligt er helt afgørende for at forhindre cyberangreb og it-sikkerhedsbrud.

4. Offentlig-privat samarbejde om sektorernes gensidige afhængigheder

Risiko- og sårbarhedsvurdering er iblandt de grundelementer i den risikostyring, som i dag sker i de enkelte samfundsvigtige sektorer. Men ingen kæde er stærkere end det svageste led. Hverken lokalt, regionalt eller nationalt. Ting kan hurtigt eskalere og påvirker andre sektorer.

Pumper skal have strøm for at kunne køre, men uden IT og adgang til kommunikation og data bliver driften af et elnet, vandværk, et kraftværk eller en vindmølle noget mere bøvlet. Og uden energi og informations- og kommunikationsteknologi (IKT) er det også svært at gennemføre betalinger eller transportere personer og gods samt levere andre services og ydelser. Som sektorer er vi tæt forbundne. I Cyberalliancen ser vi et behov for en mere dybdegående kortlægning af sektorernes gensidige afhængigheder.

I Cyberalliancen bakker vi op om det nuværende sektoransvarsprincip, men vi finder det samtidig meget vigtigt, at cybersikkerhed også anskues

tværsektorielt. Derfor finder vi i Cyberalliancen det vigtigt, at vi som nation får etableret de nødvendige faglige, fortrolige og operationelle offentlige-private fora. Her kan vi fremadrettet i fællesskab løbende analysere, forstå og drøfte sektorernes gensidige afhængigheder.

5. Styrke IoT sikkerhed

Med digitaliseringen bliver et stadigt stigende antal enheder koblet på nettet. Mange producenter tænker først og fremmest på funktionalitet ved udvikling af disse enheder, hvorfor IoT-enheder ofte er usikre og lette at angribe, når enhederne kommer på internettet.

Det betyder, at IoT-enhederne eksempelvis risikerer at blive indlemmet i såkaldte botnets, og blive anvendt til overbelastningsangreb (DDoS) af andre nettjenester på internettet. Cyberalliancen foreslår, at det bliver en prioritet i den nationale strategi for cyber- og informationssikkerhed at styrke sikkerheden i IoT. Konkret foreslås det, at IoT-enheder, der tilsluttes net i EU, skal efterleve fælles europæiske minimumsstandarder for sikkerhed, samt at der arbejdes for globale standarder.

6. Styrk borgeres digitale forsvar

Svindlere bruger i stigende grad digitale kanaler til at lokke personlige oplysninger ud af forbrugerne. Det sker med mails, sms'er og opkald til forbrugerne. I nogle tilfælde sker det med spoofing af telefonnumre, hvor kriminelle, for modtageren, ser ud til ringe fra et troværdigt og kendt telefonnummer som fx dit pengeinstitut, SKAT eller Nets.

Derfor skal rådgivningen og informationsindsatsen over for borgere styrkes betydeligt. Det kunne være gennem en central statslig rådgivningsfunktion, som yder borgerrettet information om it-sikkerhed 24/7. Der skal være mulighed for løbende rådgivning og information, og der bør gennemføres flere kampagner årligt m.m.

7. Udbygning af appen "Mit Digitale Selvforsvar"

Det foreslås, at TÆNKs app "Mit Digitale Selvforsvar" udbygges til at yde beskyttelse mod falske mobilopkald og SMS'er. Dette kan ske ved at tilføre ekstra forebyggende sikkerhedsfunktionalitet til denne app, som gør det muligt at blive advaret imod, hvilke numre svindlerne benytter og blokere for disse. Samtidig kan en udbygning af app'en forbedre kendskabet og den gode oplevelse ved at benytte appen, således at den nye app potentielt kunne blive danskernes foretrukne beskyttelses-app.

Vi foreslår derfor, at app'en udbygges i et offentlig-privat partnerskab mellem nogle af de samfundsvigtige sektorer, Center for Cybersikkerhed, Datatilsynet og de parter, som står bag TÆNKs app i dag.

8. Styrkelse af indsatsen mod spoofing

Spoofing er et komplekst og internationalt problem, som desværre ikke kan løses med et enkeltstående tiltag. Telebranchen bidrager med forskellige tiltag og aktiviteter til at begrænse omfanget, men det er ikke muligt at forhindre helt. Derfor er det også vigtigt, at der fra mange sider er fokus på at styrke indsatsen og styrke brugernes bevidsthed om risikoen for fup-opkald og phishing, og at alle er opmærksomme på aldrig at udlevere personlige oplysninger over telefonen, sms eller mail, hvis det ikke er i forbindelse med opkald eller korrespondance, man selv har taget initiativ til.

Vi vil konkret foreslå, at der i en ny national strategi for cyber- og informationssikkerhed rettes et fokus på netop problemstillingen med fup-opkald og spoofing, hvor man med en fælles indsats i samarbejde mellem telebranchen, finanssektoren og myndigheder kan styrke indsatsen mod både spoofede opkald og sms'er.