Indspil til regeringen:

Her er 8 forslag til fælles styrkelse af cyber- og informationssikkerheden

Cyberangreb er et stigende problem, som kun kan løses gennem en helhedsorienteret og sammenhængende indsats. Derfor præsenterer Cyberalliancen i dag en række anbefalinger, som regeringen med fordel kan lade sig inspirere af til den kommende nationale cyber- og informationssikkerhedsstrategi

Danmark er et af de mest digitaliserede samfund i verden. Det gør livet lettere for både borgerne, det offentlige og virksomhederne. Men både danske og internationale virksomheder rammes i stigende grad af alvorlige angreb med store økonomiske tab til følge. Der er også eksempler på hackere, der forsøger at påvirke demokratierne i de vestlige lande ved hjælp af cyberangreb og spionage. Til sidst er det også nødvendigt at styrke borgernes viden om, hvordan man bedre beskytter sig mod it-kriminalitet.

Cyberalliancen, som repræsenterer de samfundsvigtige sektorer ved Finans Danmark, Dansk Energi, Danske Rederier, DANVA og Teleindustrien, ønsker at bidrage til, at der nationalt tages et ambitiøst og samlet ansvar for at sikre de samfundsvigtige funktioner og styrke cybersikkerheden generelt i samfundet.

Vi finder det derfor helt afgørende, at regeringen nu tager yderligere skridt til at styrke cybersikkerheden i form af en ny national cyber- og informationssikkerhedsstrategi.

Det arbejde vil vi gerne være med til at understøtte gennem otte konkrete anbefalinger.

De otte anbefalinger

1. Der er behov for mere klare og forudsigelige rammer og regler for, hvad der er kritisk infrastruktur, og hvilke krav, der skal stilles til leverandører. Det skyldes, at det i stigende omfang er 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.
2. Sikring af tilstrækkelige ressourcer til politiet til opklaring af cyberangreb mod virksomheder. Det er ofte vanskeligt og ressourcekrævende at efterforske og opklare disse angreb, og politiet har i det nationale center for Cybercrime (NC3) ikke tilstrækkelige ressourcer til at opklare disse ofte meget alvorlige angreb.
3. Øget dialog mellem myndighederne og de samfundskritiske sektorer for at styrke den tidlige vidensdeling. Viden om angreb i så tidlig en fase som muligt er således helt afgørende for at forhindre cyberangreb og it-sikkerhedsbrud.
4. Etablering af faglige, fortrolige og operationelle offentlige-private fora, som kan drøfte og analysere sektorernes gensidige afhængigheder. Pumper skal have strøm for at kunne køre, men uden IT og adgang til kommunikation og data bliver driften af et elnet, telenet vandværk, eller en vindmølle svært.
5. Sikkerheden i forhold til IoT (Internet of Things) skal styrkes. Det bør være en prioritet i den kommende nationale cyberstrategi at styrke sikkerheden i IoT og at IoT-enheder, der tilsluttes net i EU, følger fælles europæiske minimumsstandarder for sikkerhed.
6. Rådgivningen af borgerne skal styrkes, fx gennem en central statslig rådgivningsfunktion, som yder borgerrettet information og rådgivning om it-sikkerhed døgnet rundt. Desuden bør der gennemføres flere årlige kampagner, der skal øge borgernes viden om, hvordan man bedre beskytter sig mod it-kriminalitet.
7. Forbrugerrådet TÆNK's app "Mit Digitale Selvforsvar" bør udbygges til også at yde beskyttelse mod falske mobilopkald og SMS'er. Derfor bør app'en udbygges i et offentlig-

privat partnerskab mellem nogle af de samfundsvigtige sektorer, Center for Cybersikkerhed, Datatilsynet og de parter, som står bag app'en i dag.

8. Øget fokus på fup-opkald herunder spoofing, hvor typisk udenlandske svindlere ændrer visningen af deres eget nummer til et tilfældigt dansk nummer fx for at få kreditkortoplysninger. Her kan det allerede eksisterende samarbejde mellem telebranchen, finanssektoren og myndigheder styrke indsatsen mod både spoofede opkald og sms'er.

Det er vores klare opfattelse, at disse anbefalinger vil styrke forsvaret mod digitale trusler og cyberangreb på danske borgere, offentlige institutioner og virksomheder, og at de derfor med fordel kan implementeres i den kommende nationale cyber- og informationssikkerhedsstrategi.

På vegne af Cyberalliancen,

Ulrik Nødgaard, adm. direktør i Finans Danmark, Lars Aagaard, adm. direktør i Dansk Energi,

Anne H. Steffensen, adm. direktør i Danske Rederier, Carl-Emil Larsen, direktør i DANVA

Jakob Willer, direktør i Teleindustrien.

LINK TIL DE 8 FORSLAG FRA CYBERALLIANCEN

LINK TIL TIDLIGERE PRESSEMEDDELELSER FRA CYBERALLIANCEN