Fremtidens beskyttelse af det digitale Danmark

Baggrund

Danmark er et af verdens mest digitaliserede lande. Digitaliseringen bringer os mange goder som samfund og bidrager til, at danske virksomheder er blandt de mest konkurrencedygtige i verden. Til gengæld følger der med digitaliseringen også en øget eksponering og risiko for cyberangreb mod danske virksomheder, kritisk infrastruktur, myndigheder og borgere. Det er en risiko, som må forventes at stige markant i den kommende tid som følge af krigen i Ukraine og udviklingen i den generelle sikkerhedspolitiske situation.

I mange år har der i Danmark været et mismatch mellem digitaliseringsinvesteringer og investeringer i cybersikkerhed. Opgørelser peger på, at der investeres mia. af kr. i digital omstilling[1], og samlet set skønner IT-Branchen, at de offentlige investeringer og de private investeringer i 2022 tilsammen overstiger 100 mia. kr. Samtidig skønner vi, at maksimalt 5 pct. af denne sum anvendes til direkte sikkerheds- og beskyttelsesinitiativer.

At cybersikkerheden ressourcemæssigt er et underprioriteret område i Danmark illustreres af, at der blot er afsat 270 mio. kr. over tre år til gennemførsel af de 34 initiativer, der fremgår af regeringens netop lancerede nationale strategi for cyber- og informationssikkerhed. IT-Branchen finder generelt, og særligt i den aktuelle situation, at det på ingen måde er tilstrækkeligt, og vi er nødt til at skrue gevaldigt op for ambitionsniveauet og finansieringen, hvis vi vil skabe et cyber-robust samfund. At vi har underinvesteret i cyber- og informationssikkerhed ses også af internationale benchmarks, hvor Danmark rangerer som nr. 1 på EU's Digital Economy and Society Index, imens vi er placeret på en beskeden plads som nr. 32 – lige efter Kasakhstan – på Global Cybersecurity Index.

Vores efterslæb inden for cybersikkerhed kan komme til at koste os dyrt i Danmark. Vi befinder os i øjeblikket i en højspændt sikkerhedspolitisk situation i Europa og resten af verden. Ruslands invasion af Ukraine har placeret Danmark og øvrige europæiske lande i skudlinjen i en hybrid krig, der frygtes også at tage form af en regulær cyberkrig. Vi har allerede set flere cyberhændelser relateret til krigen, og vi bør forholde os til en overhængende risiko for, at Danmark som en del af krigen i Europa – og i tilfælde af et forværret forhold mellem NATO-landene og Rusland – kan blive

[1] DI estimerer, at virksomhederne investerer 78 mia. kr. i 2022

IT·BRANCHEN

et direkte mål for cyberangreb. Vi befinder os i en helt ny virkelighed, og står over for en ny type krigsførelse, som vi i Danmark ikke er tilstrækkeligt rustet til at imødegå.

IT-Branchens forslag til konkrete initiativer for at styrke Danmarks cyberforsvar

IT-Branchen har identificeret en række initiativer, som vi mener bør realitetsbehandles af Folketingets partier bag Nationalt kompromis om dansk sikkerhedspolitik.

På kort sigt

Det er afgørende, at den samlede cyberforsvarsindsats prioriteres i de politiske forhandlinger om udmøntningen af den *generelle reserve på 3,5 mia. kr. årligt i 2022 og 2023 i lyset af Ruslandskrisen*. Ifølge IT-Branchen bør denne indsats inkludere følgende væsentlige initiativer:

1) **Styrkelse af robustheden i offentlige it-systemer og kritisk national infrastruktur**

Vi skal være bedre beredt på destruktive cyberangreb rettet mod kritisk national infrastruktur med det formål at skade samfundsvigtige funktioner i Danmark. Ifølge Statens it-projektråd har næsten en tredjedel af de kritiske, offentlige it-systemer ikke tilfredsstillende it-sikkerhed. Herudover konkluderede Rigsrevisionen tidligere i år, at flere statslige myndigheders ikke lever op til de tekniske minimumskrav til it-sikkerhed. Ikke kun på statsligt niveau, men også i regionerne og ikke mindst kommunerne, halter det med it-sikkerheden. I en nylig rundspørge fra DR svarer tre ud af fire af kommuner, at antallet af forsøg på cyberangreb er steget gennem de seneste fem år. Fra april 2020 til september 2021 har kommunerne indberettet 3345 sikkerhedsbrug til Datatilsynet.

Derfor bør vi investere markant i at højne it-sikkerhedsniveauet i kritiske, offentlige it-systemer og infrastruktur, så vi er bedre sikret mod økonomiske og samfundsmæssige konsekvenser af destruktive cyberangreb.

2) **Styrkelse af cyberforsvaret i de danske virksomheder**

Analyser viser, at it-sikkerhedsniveauet er for lavt i hver fjerde danske SMV, og at hver sjette danske SMV har været ramt af et cyberangreb inden for de seneste 12 måneder. Disse tal er alt for høje i almindelighed og – i særdeleshed – i en højspændt sikkerhedspolitisk tid i Europa, der også skaber usikkerhed på cyberområdet. For at styrke de danske virksomheders muligheder for at sikre sig mod cyberkriminalitet og -angreb bør der investeres i etableringen af et offentlig-privat samarbejde/

partnerskab, der skal varetage opgaven med at indsamle og dele viden om cybertrusler og -hændelser på tværs af offentlige og private videnkilder og komme med råd og aktuelle anbefalinger, som virksomhederne kan tilgå og agere proaktivt og operationelt på. Det er ikke tilstrækkeligt med en tværstatslig enhed, som der til dels lægges op til at etablere i regi af den nationale strategi for cyber- og informationssikkerhed. Der er behov for en uvildig organisation med reel repræsentation og inddragelse af det private erhvervsliv.

Enheden skal have en aktiv og udøvende rolle ift. at indsamle, koordinere og validere viden og yde vejledning om beredskab og forebyggende sikkerhedsforanstaltninger, men også rådgivning og hjælp til håndtering af sikkerhedshændelser i samspil med private cybersikkerhedseksperter.

3) Øget og accelereret uddannelse af cybersikkerhedsspecialister

Ifølge DIGITALEUROPE mangler der 200.000 cybersikkerhedseksperter i Europa. I Danmark efterspørger mere end hver tredje virksomhed i it-branchen medarbejdere med cyberkompetencer i øjeblikket. Manglen på kompetencer er en kæmpe hæmsko for cybersikkerheden i Danmark. Der bør investeres i akut uddannelse af flere cyberspecialister i Danmark. I øjeblikket søger flere unge ind på it-uddannelserne, end uddannelsesinstitutionerne har økonomi til at uddanne.

4) Øget cybersikring af det digitale, danske forsvar

Der er behov for en styrket cybersikring af platforme og våbensystemer, der bliver mere og mere digitale og forbundne. Dette kan ske ved etablering af et offentlig-privat samarbejde, hvor der kan skabes en bedre platform for at sikre, at fremtidens våbensystemer indeholder dansk IP – også ift. cyber- og informationssikkerhed. Det kan i den forbindelse overvejes at skabe puljer, der gør det attraktivt for større danske militær-system-udviklere at indarbejde og arbejde sammen med iværksættere for derigennem at markedsmodne teknologierne og få dem ind i faktiske våbensystemer.

På længere sigt

IT-Branchen mener, at der på længere sigt – men som en del af udmøntningen af Nationalt kompromis om dansk sikkerhedspolitik – bør igangsættes en række analyser, vurderinger og samarbejder omkring skabelse af et cyber-resilient samfund, hvor digitalisering og cyber- og informationssikkerhed går hånd i hånd. Man vil med fordel kunne drive en række af initiativerne som offentlig-private partnerskaber med udgangspunkt i det regeringsnedsatte Cybersikkerhedsråd.

1) National rolle- og ansvarsplan for fremtidens digitale Danmark

Danmark har et sektoransvarsprincip, som har tjent os godt. Spørgsmålet er, om det er den rigtige måde at beskytte et højt specialiseret, digitaliseret og interoperabelt samfund på. IT-Branchen mener, at der er brug for en samlet kortlægning og vurdering af "hvem gør hvad, hvornår, hvordan?" ift. samspillet mellem de statslige, regionale og kommunale aktører og de private interessenter som driver national kritisk infrastruktur. Der bør kigges på, om man skal samle alle myndigheds-cyber-interessenter i samme hus, og hvordan samarbejdet i de forskellige sektorer mellem det offentlige og det private tilrettelægges optimalt, b.la. med inspiration fra andre lande, hvor man har haft succes med en anden organisering end i Danmark.

I forlængelse heraf bør det også undersøges, om der kan/skal etableres en enhed, der varetager den samlede udmøntning af midler og initiativer, der har til formål at styrke Danmarks digitale forsvarskraft både i det offentlige og det private, evt. med forankring af dette arbejde hos en National CISO med inspiration fra udlandet.

2) Iværksætterprogram for øget cyber- og informationssikkerheds-innovation

Det bør overvejes at se på etableringen af et program, hvor der sker en samtænkning af markedsmuligheder, ambassadørskab og teknologiinnovation for iværksættere, fx efter en inkubatormodel som i andre lande. Dette vil styrke den danske innovationskraft inden for cyber- og informationssikkerhed samtidig med, at man sammen vil kunne gå til det internationale marked og arbejde for, at "Cybersecurity Made in Denmark" bliver noget, som alle ønsker at være en del af.

Det kan videre overvejes at supplere initiativet med støtte til markedsmodning og en indsats for at fremme (store) virksomheders inddragelse af iværksættere i deres løsningsdesigns.

IT·BRANCHEN

Dette initiativ vil skulle tænkes sammen med det eksisterende økosystem og klyngestrukturen.

3) Øget forskning og udvikling inden for cyber- og informationssikkerhed

Dette initiativ bør understøtte ovenstående initiativ 2 samt have et tværgående fokus på at forankre grundlæggende kompetencer hos langt flere medarbejdere og borgere. Ud fra parolen ”vi skal alle lære at være digitale borgere i et digitalt samfund”, kan folkeoplysningen omkring ens rolle i højnelsen af det samlede danske cyberforsvar være med til at gøre Danmark endnu mere resilient. Man kan overveje en national udrulning af eLæring omkring beredskab og en fælles national udrullet varlings-app (en slags Smittestop for Cyber) for at gøre de danske borgere og medarbejdere til ikke blot de mest digitale i verden, men også de mest cybersikre.

Samtidig bør der sættes fokus på at uddanne fremtidens cybersikre medarbejdere. Der skal sættes fokus på uddannelsesinitiativer over for børn og unge, over for KVU-, MVU- og LVU-studerende samt at styrke muligheden for at efteruddanne sig på cyber- og informationssikkerhedsområdet.

4) Nationalt kompromis og samtænkning af ”styrkede indsatser”

Der er i IT-Branchens optik en række indsatser, som kan gøres for at øge vores samlede modstandskraft over for fx hybrid-angreb. De 20 minimumskrav til staten kunne få en national rolle ift. at skabe en større og mere homogen snitflade mod en angriber – hvis X;Y;Z er lukket land, så vil det være meget vanskeligere for en angriber at identificere, hvor hullerne er. Endvidere bør der etableres en samfundsbaseret tilgang mod misinformation – der bør være en fakta-enhed, som har adgang til at give individer og operatører bøder eller påbud, dersom de gentagne gange understøtter fake-news, propaganda mm., med fuld respekt for Grundlovsfæstnede rettigheder som ytringsfrihed.

5) Internationalt cyberhåndslag

IT-Branchen foreslår, at Danmark stiller sig i spidsen for et globalt initiativ rettet mod at skabe fremtidens offentlig-private rammer mod misbrug af den digitale verden. Der kan arbejdes for en cyber-Geneva-konvention, en borger-cyberbeskyttelses-pagt, og man kan koordinere sine aktiviteter med Interpol, Europol, FBI m.fl. Danmark kunne være stifter sammen med Estland, Israel, US, UK og Sydkorea, og organisationen kunne være en slags cyber-OSCE (sikkerhedsorganisation) på globalt plan.