KALVEBOD BRYGGE DEKLARATIONEN

Et opråb for et cybersikkert digitalt Danmark

11.04.2023

FORSLAG TIL ET MERE CYBERSIKKERT DANMARK

1. **Opret** en civil cybersikkerhedsmyndighed med bredere sikkerhedsfokus
2. **Saml** ansvaret for den civile cybersikkerhed, it og digitalisering
3. **Indtænk** sikker digitalisering fra start til slut
4. **Lev op** til et digitalt nærhedsprincip
5. **Håndhæv** overholdelse af ansvaret for cybersikkerhed
6. **Skab** overblik over eksisterende systemer og ejerskaber
7. **Behold** et analogt alternativ til samfundsvigtige digitale tjenester
8. **Udfør** regelmæssige nationale cybersikkerheds-beredskabsøvelser
9. **Prioritér** folkeoplysning om cybersikkerhed og digital selvforståelse

1 Opret en civil cybersikkerhedsmyndighed med bredere sikkerhedsfokus

Desværre må vi erkende, at Danmark ikke er rustet til at håndtere truslen fra særligt kriminelle tilstrækkeligt effektivt. Den eksisterende organisering af cybersikkerhed under en militær efterretningstjeneste beskytter desuden ikke civilsamfundet, befolkningen og de private virksomheder som opretholder den kritiske infrastruktur i tilstrækkelig grad. Og mange virksomheder efterlyser et mere åbent samarbejde.

Derfor anbefaler vi at oprette en civilt forankret myndighed med ansvaret for cybersikkerheden bredt i samfundet. Dette kan ske med inspiration fra bl.a. Israel, Holland og Estland.

Myndigheden skal varetage det tværgående ansvar og koordinering, oplyse om forestående og igangværende angreb og understøtte ministerierne, virksomhederne og borgerne i opbygningen af et tilfredsstillende sikkerhedsniveau. Omorganiseringen bør ske i kombination med implementeringen de strukturelle ændringer som følge af det opdaterede Net og Informationsdirektiv (NIS2).

2 Saml ansvaret for den civile cybersikkerhed, it og digitalisering

Der er behov for at gentænke den danske organisering af cyber- og informationssikkerhed og samle ansvaret ét sted. Derfor anbefaler vi, at man gentænker organiseringen. Vi foreslår, at den førnævnte civile myndighed overtager ansvaret for den civile og virksomhedsrettede cybersikkerhed fra CFCS og Digitaliseringsstyrelsen (DIGST) i en samlet styrelse for cybersikkerhed, som skal varetage kontakt, rådgivning og tilsyn med private og offentlige aktører med særligt blik for den kritiske infrastruktur.

Vi anbefaler derfor, at der oprettes et ministerium med det samlede ansvar for IT, digitalisering og cybersikkerhed.

Ministeriet bør være den ansvarlige myndighed for behandlingen af borgernes data og ikke mindst implementeringen af både nuværende lovgivning og minimumskrav, og kommende EU-direktiver på området. Der er brug for at skabe et samspil i digitalisering- og sikkerhedsdagsordnen som i dag ikke strukturelt er muligt.

3 Indtænk sikker digitalisering fra start til slut

Sikkerhed skal indtænkes i kernen af al digitalisering, frem for at betragtes som en unødig udgift eller en forsinket eftertanke.

Derfor anbefaler vi, at der skabes klare principper og retningslinjer for sikkerheden som forudsætningen for ny digitalisering gennem Security og Privacy by Design .

Dette gælder bl.a. standarder for Security by Design så sikkerheden og privatlivsbeskyttelse i softwareren tænkes ind fra starten og at informationerne holdes tæt på borgeren på en sådan måde at de ikke kan misbruges og løbende bliver slettet. Samtidig bør der indføres produktansvar ift. softwareproducenter, så de er forpligtede til at rette sikkerhedsbrister.

Nye systemer bør, som EU anbefaler, opbygges ud fra principper om Privacy by Design. Dette minimerer risikoen for læk, hacking og misbrug og øger tilliden. Danmark bør også være foregangsland i arbejdet med, og efterlevelsen af, EU lovgivningen som NIS2 og Cyber Resilience Act.

4 Lev op til et digitalt nærhedsprincip

Vi anbefaler, at samfundskritiske it-systemer og infrastruktur bør holdes tættest muligt på Danmark og under højere grad af demokratisk kontrol for at øge sikkerheden.

Et såkaldt digitalt nærhedsprincip indebærer at man afsøger; først, om det er muligt at udvikle og drive systemerne i Danmark, sekundært i Norden og endelig i en europæisk kontekst.

Der bør også lægges vægt på at sikre en højere grad af demokratisk kontrol ved at øge kapaciteten i den offentlige sektor både til at udvikle og drive systemerne, og i højere grad at styre og kontrollere processerne omkring udbud. Det er en åbenlys sikkerhedsrisiko, hvis samfundskritiske systemer eller infrastruktur ejes og drives af et væld af private og udenlandske virksomheder hvor vi ikke har nogen mulighed for at styre sikkerheden, herunder hvem der har adgang til data.

En oplagt mulighed er at opbygge samarbejdet med vores nordiske nabolande, der har teknisk kapacitet, og hvor vi allerede har et tæt politisk samarbejde og fælles geopolitiske sikkerhedshensyn.

5 Håndhæv overholdelse af ansvaret for cybersikkerhed

Der er brug for en fornyet politisk prioritering af, at alle eksisterende krav rent faktisk overholdes. For vores it-systemer lever på ingen måde op til de basale krav for sikkerhed.

Vi anbefaler, at cybersikkerhed håndteres seriøst, gennem produktansvar for private virksomheder, dedikerrede ressourcer til retssystemet, forstærket håndhævelse i det offentlige og klageadgang til borgere.

For private virksomheder skal der indføres producentansvar for softwarebaserede løsninger og produkter, for at sikre øget fokus på cybersikkerhed og reducere risikoen for databrud. Samtidig skal retssystemet styrkes med specialistkompetencer, og der bør overvejes en særlig teknologidomstol for sager om cybersikkerhed og softwareansvar.

Indsatsen for et minimumsniveau af cybersikkerhed i hele den offentlige sektor skal forstærkes. Implementeringen skal følges op med et sæt detaljerede, binære kontroller baseret på et internationalt rammeværk, som offentlige organisationer skal overholde, for at sikre en ensartet og effektiv tilgang til cybersikkerhed.

Topledelsens ansvar for organisationens cybersikkerhed skal fremhæves, gennem styrket kontrol af målopfyldelsen. Organisationerne skal forsyne en central enhed med ressourcer og kompetencer til kontrol, og resultaterne af kontroller bør offentliggøres årligt i anonymiseret form.

Borgere skal have bredere mulighed for at klage over manglende beskyttelse af egne data, herunder algoritmebaserede afgørelser. Det kan fx sikres igennem oprettelsen af en digital ombudsmandsfunktion og ved at udvide Datatilsynets ressourcer og mulighed for at fastholde og opkvalificere medarbejdere.

6 Skab overblik over eksisterende systemer og ejerskaber

Vi anbefaler, at der skabes et overblik over systemer af større samfundsmæssig væsentlighed for at klarlægge, hvem der ejer vores systemer, hvem der har adgang til dem og om de lever op til de nødvendige sikkerhedsstandarder.

Den ansvarlige myndighed skal også udarbejde en plan for at få afviklet, opdateret og dokumenteret de systemer og ejerforhold, der udgør en sikkerhedsrisiko, og sikre at systemer fremover bliver kortlagt og fulgt op.

7 Behold et analog alternativ til samfundsvigtige digitale tjenester

Vi anbefaler, at der altid skal være et analog alternativ til samfundsvigtige digitale tjenester, der skal tjene det dobbelte hensyn at øge samfundets modstandsdygtighed overfor angreb og være en livline for borgerne.

Man fjerner ikke brandtrapperne bare fordi man har fået en elevator. Hvis nettet, der forbinder kraftvarmeværkerne og vindmøllerne ødelægges, kan vi så stadig få strømmen ud i ledningerne og varmen frem til forbrugerne? Og hvis MitID ødelægges, kan vi så stadig opretholde en administration?

Vi er nødt til at have analog redundans, et fysisk fungerende alternativ, der kan sikre, at samfundet kan fungere, hvis det digitale svigter. I militærstrategiske termer hedder det 'deterrence by denial' – at man gør det mindre attraktivt at angribe, ved at gøre det sværere for fjenden at lægge landet ned ved et simpelt angreb på kritisk infrastruktur. Hertil kommer det afgørende hensyn, at statens ydelser også vil være tilgængelige for de 25-35% af befolkningen, som ifølge undersøgelser af Ældresagen og Justitia, oplever at være digitalt udfordret.

8 Udfør regelmæssige nationale cybersikkerheds-beredskabsøvelser

Det er nødvendigt at øge samfundets samlede resiliens og cybersikkerhed og ikke mindst koordinering på tværs sektorer og niveauer.

Derfor anbefaler vi, at der årligt gennemføres beredskabsøvelser af cybersikkerhed i den samfundsvigtig kritisk infrastruktur med inddragelse af civile myndigheder, kommuner og private virksomheder.

Dette er i dag en mangel, som udstiller vanskelighederne ved at tænke på tværs af sektorer. De nuværende øvelser i både EU- og NATO-regi afholdes i en lukket kreds og med overvægt på forsvaret. Der udestår derfor faste øvelser som tester, træner og evaluerer cyber-beredskabet bredt i samfundet.

Desuden bør der indføres en national konference og tilstødende kurser i et koordineret samarbejde mellem Forsvaret, civile myndigheder og den private sektor, hvor deltagerne får en omfattende koordineret introduktion til de forskellige områder af sikkerhed i samfundet, gennem foredrag, besøg og øvelser. Gennem den tværgående dialog, vil deltagerne forstå og se de vigtige sammenhænge for samfundets sikkerhed.

9 Prioritér folkeoplysning om cybersikkerhed og digital selvforståelse

Danmarks position som digital frontløber stiller store krav til den enkelte borger om brugen af avancerede systemer og teknologier.

Vi anbefaler, at oplysning om cybersikkerhed skal være en del af public service-forpligtelsen for at styrke borgernes handleevne i et digitalt og demokratisk samfund.

Det kræver nem adgang til kontinuerlig og vedvarende kvalificeret oplysning. En public service-forpligtelse på at oplyse borgerne om brede aspekter ved cybersikkerhed, aktuelle trusselsbilleder og beskyttelse af privatliv vil være et vigtigt skridt mod et højnet niveau af samfundssikkerhed.

Vi anbefaler også, at det generelle arbejde med, og uddannelse i, digital selvforståelse bliver styrket fra det tidspunkt, hvor en borger forventes at være digital.

Den digitale selvforståelse handler om en bevidstgørelse af, hvad det indebærer at have en digital tilstedeværelse og opbygge kompetencer til sikkert at navigere i det digitale rum. Det kalder på en tidlig indsats fra de yngste klasser i folkeskolen, men også en generel forpligtelse for organisationer til at uddanne og stille relevant viden til rådighed for deres brugere og ansatte. En forventning om anvendelse af digitale teknologier skaber ligeledes en forpligtelse overfor brugeren.

BAGGRUND

Danmark er ét af verdens mest digitaliserede lande, men det står desværre klart, at sikkerheden ikke har fulgt med.

Cyberangreb bliver af World Economic Forum kategoriseret som en af de potentielt mest ødelæggende trusler på verdensplan.

Ligeledes vurderer Center for Cybersikkerhed (CFCS), at truslen fra cyberkrimi-nalitet og cyberspionage mod Danmark er "meget høj".

Cybersikkerheden af den kritiske infrastruktur er gentagende gange kritiseret i stærke vendinger af Rigsrevisionen, som i november 2022 fastslog, at der »er risiko for, at it-nedbrud og datatab medfører, at staten ikke kan opretholde eller markant får forstyrret samfundskritiske opgaver«.

Problemerne med cyber- og informationssikkerhed skyldes blandt andet et ansvarsvakuum i koordineringen som forhindrer informations- og vidensdeling. Der sker ikke en effektiv håndtering at truslen fra kriminelle aktører. Og der mangler efterlevelse og kontrol af eksisterende krav, såvel som langsigtet planlægning.

Det er også en udfordring, at digitaliseringen i for høj grad er drevet af effektiviserings- og omkostningshensyn uden skelnen til sikkerheden.

Dette medfører at Danmark efterlades mere sårbar overfor cyberangreb, og at omkostningerne i sidste ende bliver langt højere, end hvis sikkerheden havde været tænkt ind for starten.

Tilliden til ikke kun digitaliseringen, men også samfundet står for skud, hvis ikke den fundamentale sikkerhed bliver forstærket.

Vi er en dedikeret samling af professionelle IT- fagfolk, cybersikkerhedseksperter og forskere mm., der er bekymrede over udviklingen, og kalder derfor på handling for et mere cybersikkert digitalt Danmark.

Derfor har vi i det sidste halve år diskuteret og samlet den viden, der er kondenseret i disse anbefalinger. Vi håber, at det kan bidrage til debat og udvikling af vores fælles cybersikkerhed.

BIDRAGSYDERE

Deklaration er lavet med bidrag fra bl.a.:

***John Foley**, IT- og cybersikkerhedsrådgiver*

***Eva Flyvholm**, (EL) tidligere medlem af Folketinget*

***Mogens Nørgaard**, fast klummeskriver og debattør i Computerworld*

***Morten Hybschmann**, statskundskabsstuderende, KU*

***Mette Nikander**, Senior Security Advisor, NIXU Corporation*

***Jens Roed Andersen**, selvstændig cybersikkerhedskonsulent*

***Anders Kjærulff**, Techkritiker*

***Leif Jensen**, ESET Nordic*

BAGGRUND FOR DEKLARATIONEN

Kalvebod Brygge Deklarationen om Cybersikkerhed, er blevet til som opfølgning på en heldagskonference om data, -it og cybersikkerhed gennemført den 10. november 2022 i IDA's Kongressal på Kalvebod Brygge, samt seks TV-udsendelser fra IDA's TV studie.

Oplæg fra IDA konference om cybersikkerhed:

– Vores største trussel: Cybercrime v/ **Troels Ørting Jørgensen**, World Economic Forum og **Tobias Liebetrau**, Ph.d og Post.doc.

– Passes der godt nok på Danmark? v/ **Torben Ørting Jørgensen**, formand for foreningen Folk og Sikkerhed

– Cybersikkerhed i et offentligt -privat samarbejde v/ **Peter Kruse**, Kruse Industries

– NIS2 direktivets betydning og konsekvenser v/ **John Foley**, It- og Cybersikkerhedsrådgiver

– Paneldebat Cybersikkerhed Konference - Politikere, topfolk dansk erhvervsliv og oplægsholdere v/ **Michael Aastrup Jensen** (V); **Eva Flyvholm** (EL); **Aaja Chemnitz Larsen**, Medlem af Folketinget; **Jeanette Hartz**, Dansk IT; **Janus Sandsgaard**, Dansk Erhverv; **Morten Rosted Vang**, Dansk Industri; **Christian Spohr**, Eagle Shark; **Peter Kruse**, Kruse Industries; **Tobias Liebetrau**, Ph.d og Post.doc; **John Foley**, It- og Cybersikkerhedsrådgiver; **Torben Ørting Jørgensen**, Folk og Sikkerhed

Seks udsendelser fra IDA's TV-studie:

– Samfundssikkerhed og cybersikkerhed v/ **Alexander Høgsberg Tetzlaff**, Center for Militære Studier, Københavns Universitet

– Cybersikkerhed og samfundsvigtig kritisk infrastruktur v/ **Henning Mortensen**, Rådet for Digitalsikkerhed og **Morten Hybschmann**, København Universitet

– Cybersikkerhed debat **med Leif Jensen,** ESET (cybersikkerhedsekspert) og **Ditte Vinterberg Weng,** Computerworld

– Cybersikkerhed debat med **Amalie Lyhne,** Berlingske og **Kasper Skov Mikkelsen,** direktør for Sikkerhedsbranchen

– Cybersikkerhed debat med **Mette Nikander,** Nixu og **John Foley,** It- og Cybersikkerhedsrådgiver

– Cybersikkerhed - Den estiske model v/ **Lauri Almann**, CybExer Technologies

Udsendelserne er også produceret som en podcastserie.