Vejen til et top-cybersikkert Danmark

Denne indsats har tre formål:

1. Bedre beskyttelse af den offentlige sektor.

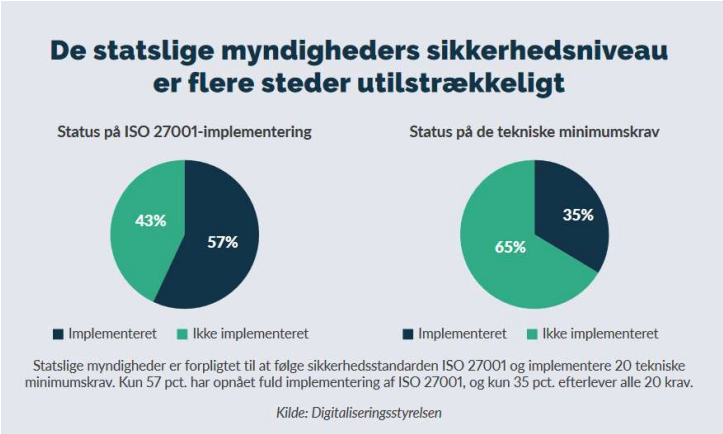
2. Danmark skal have verdens mest tjekkede private virksomheder.

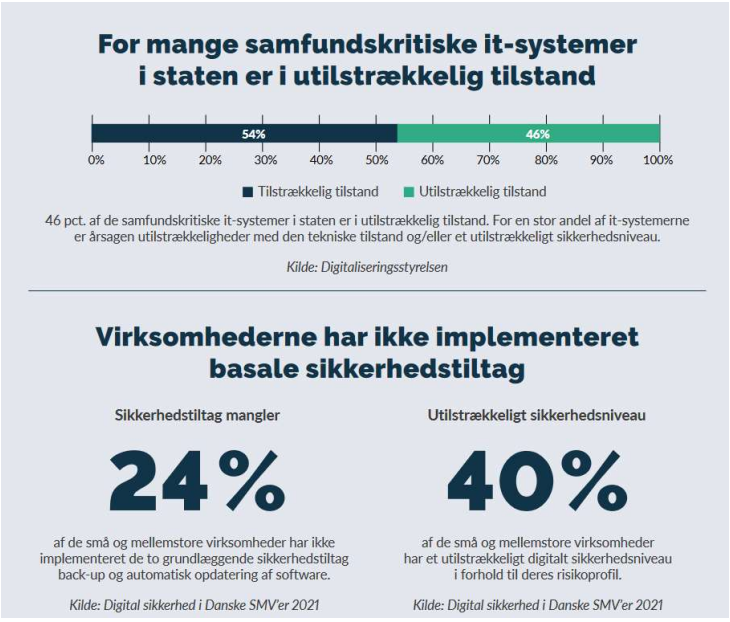
3. Borgernes viden om it-sikkerhed skal være høj.

Der er mange gode fem- og tiårsplaner, men nogle gange er man nødt til at handle hurtigt, der hvor man kan det. Der er rigtig mange fordele at hente i at plukke de lavthængende frugter - vi giver her vores bud på, hvad der kan gøres på bare tre måneder, hvis vi vil det. Det er dog på ingen måder nok. Et tilpas cybersikkerhedsniveau kræver dybere spadestik og har mere realistisk et tre-års sigte. Endelig er der grundlæggende forandringer, som tager tid. Men meget bør alligevel kunne nås på 6 år.

Baggrund

Danmark er i top, når det gælder digitalisering, men ikke helt det samme sted, når det handler om at opfylde krav til it-sikkerhed. Ifølge Danmarks Digitaliseringsstrategi har 40 % af de danske små og mellemstore virksomheder et digitalt sikkerhedsniveau, der er utilstrækkeligt i forhold til deres risikoprofil og mange virksomheder mangler helt grundlæggende tiltag i deres digitale sikkerhed. I den offentlige sektor er kun 54% af de samfundskritiske it-systemer sikkerhedsmæssigt tilstrækkelige og kun 57% har ISO 27001 implementeret. Anmeldelser af økonomisk it-relateret kriminalitet er steget markant de seneste år. Politiets Landsdækkende Center for it-relateret Økonomisk Kriminalitet (LCIK) har siden sin oprettelse i december 2018 modtaget 70.000 anmeldelser om økonomisk it-kriminalitet.[1]





[1] Regeringens NATIONAL STRATEGI FOR CYBER- OG INFORMATIONSSIKKERHED 2022-2024 19, inkl. Digital sikkerhed i danske SMV'er 2021 og Landsdækkende Center for It-relateret Kriminalitet

Samtidig har forsvarets trusselsvurdering ændret sig siden december 2021, ikke mindst på grund af krigshandlingerne i Ukraine. 18. maj blev truslen fra cyberaktivisme mod danske myndigheder og virksomheder hævet fra lav til middel med sigte på især hackeraktivister. Truslen fra cyberkriminalitet, dvs. primært økonomisk begrundede angreb, er stadig er meget høj, ikke mindst når det kommer til ransomware angreb. Truslen fra cyberspionage mod især universiteter og forskningsinstitutioner fra ikke mindst Rusland og Kina vurderes tilsvarende meget høj.

CFCS har i deres nyeste trusselsvurdering også sat fokus på påvirkning med brug af cyberangreb. Fremmede stater, herunder Rusland, bruger iflg. CFCS aktivt cyberangreb i deres forsøg på at påvirke holdninger og adfærd i andre lande. Historisk er et af de mest kendte eksempler på påvirkning med brug af cyberangreb hack og læk-angrebet mod Demokraternes Nationale Komité (DNC), der blev udført i forbindelse med det amerikanske præsidentvalg i 2016.

De forskellige elementer i cybersikkerhed hænger sammen. Vi er derfor nødt til at sikre os bedre, både når det kommer til organisationer indenfor kritisk infrastruktur, virksomheder og forskningsinstitutioner og borgere og medarbejdere. Vores plan opererer derfor med forslag til forbedringer på alle niveauer i det danske samfund.

Mål for de første 3 måneder: De lavt hængende frugter kan få os langt

Udbred D-mærket
D-mærket er et eksempel på et redskab, der indenfor 3 måneder kan bidrage til væsentlig bedre it-sikkerhed og ikke mindst opmærksomhed på it-sikkerhed i virksomheder og offentlige myndigheder. D-mærket indeholder væsentlige redskaber til selvevaluering på it-sikkerhedsområdet udover en dataetisk vurdering. Evalueringen munder ud i en kontrolleret certificering. Den offentlige sektor bør indføre krav om D-mærket i udbud for at skubbe på udviklingen.

Gennemfør obligatoriske cybersikkerhedskurser i den offentlige sektor
Alle medarbejdere skal på minimumssikkerhedskursus med bl.a. information om at modstå fishing, korrekt brug af passwords etc. Den kan om nødvendigt være et par timer med en times opfølgning – det vigtige er, at der sker noget, hurtigt.
Ledere og nøglemedarbejdere skal gennemgå et videregående kursus med viden om bl.a. risikovurdering, beredskabsplaner og indsats for at løse konkrete mangler. Kurserne kan ske via Statens Digitaliseringsakademi, evt. suppleret af universiteter og erhvervsakademier, GTS-institutter og private virksomhedsudbydere. Kurserne bør tage udgangspunkt i ISO 27001 og NIS2.

Stil krav til cybersikkerhedskurser for virksomhedsledere og bestyrelser
Relevante medlemmer af bestyrelser, ledelsen og medarbejderstaben indenfor kritisk infrastruktur og leverandører til den offentlige sektor skal gennemgå et videregående kursus med viden om bl.a. risikovurdering, beredskabsplaner og indsats for at løse konkrete mangler. Kurserne kan ske via erhvervsorganisationer og Bestyrelsesforeningen, evt. suppleret af aktører som universiteter og erhvervsakademier, GTS-institutter og private kursusudbydere. Kurserne bør tage udgangspunkt i ISO 27001 og NIS2.

Opret taskforce til at sikre implementering af de 20 vigtigste krav fra SikkerDigital i både stat, regioner og kommuner
Når 46% af de samfundskritiske it-systemer i staten ikke har et tilstrækkeligt it-sikkerhedsniveau, er det nødvendigt at sætte ind. Vores forslag på den helt korte bane er oprettelsen af en taskforce, der kan hjælpe med at opprioritere og sætte de nødvendige tiltag i gang. Udfordringen bliver at finde bemanding til en sådan taskforce.

Øg sikkerhedsbevidstheden hos befolkningen
Det er set før, men vi er ikke i mål endnu. Vi har brug for endnu en storstilet kampagneindsats med målsætning om høj viden om og korrekt brug af passwords, to-faktorgodkendelse, risici og krav til internetopkoblede produkter, f.eks. smart tv, spillekonsoller, fjernstyret lys- og varme, app-styrede installationer som tyverialarmer, musikanlæg etc. Samt basalt cyberforsvar i forhold til fishing, fup-opkald etc. Udgangspunktet kan være Sikkerdigital.dk.

Iværksæt analyse af nødvendige langsigtede tiltag
Som forberedelse til de mere langsigtede tiltag, bør der nedsættes en hurtigt arbejdende rådgivende gruppe – evt. under Cybersikkerhedsrådet – der kan uddybe og supplere med forslag til konkret handling, herunder, hvordan vi sikrer et løft i kompetencerne bredt. Opgaverne bør bl.a. omfatte:

- Fokus på konkrete tiltag til styrkelse af it-sikkerhed.
- Styrket samarbejde om videndeling om tekniske nedbrud og angreb.
- Styrket samarbejde mellem relevante offentlige og private aktører.
- Handlingsplan for opfølgning på den Nationale strategi for cyber og informationssikkerhed, samt plan for udvikling af næste strategi.

Det er vigtigt, at den rådgivende gruppe er indstillet på at tænke løsninger på tværs af traditionelle ressortområder i den offentlige sektor.

Mål for de første 3 år: Robusthed er et nøgleord

Sikkerhedstilsyn med kommuner og regioner
Ligesom staten ligger kommuner og regioner inde med samfundskritiske data. Det betyder et behov for at sikre, at alle dele af den offentlige sektor er opdaterede og på rette niveau i forhold til implementering af ledelsesværktøjet ISO 27001 og de 20 vigtigste tekniske minimumskrav. Datatilsynet bør derfor som noget af det første styrkes til at være cybersikkerhedstilsyn på niveau med arbejdstilsynet.

Uddannelsesområdet skal styrkes
Der er et akut behov for at uddanne flere specialister indenfor cybersikkerhed. Det må nødvendigvis bl.a. ske gennem efteruddannelse. Derudover bør et relevant niveau af viden om cybersikkerhed integreres i både bløde og hårde it-uddannelser, så f.eks. udviklere og it-arkitekter er bedre rustet til at udvikle sikre systemer og sikker software. Optimalt set bør cybersikkerhed indlejres i stort set alle uddannelser, da næsten alle nyuddannede i dag kommer til at arbejde med digitalisering.
Vi er også nødt til at øge optaget på de it-uddannelser, hvor efterspørgslen er størst. Det er i den forbindelse ikke hensigtsmæssigt, at fx ITU og AAU ikke kan øge optaget, selv om de hvert år afviser kvalificerede ansøgere.

Efteruddannelse til at sikre cyber-kompetencer for alle relevante medarbejdere i den offentlige sektor
På mellemlangt sigt vil det være nødvendigt at sikre, at kompetencerne er tilstede hos alle relevante medarbejdere. Det kræver bred efteruddannelse til ikke-specialister med en generel introduktion til cybersikkerhed, der skærper opmærksomheden på, hvordan vi kan agere sikkert i dagligdagen. F.eks. at vi ikke deler passwords, er opmærksom på fishing og lignende og ikke mindst, at hver enkelt medarbejder ved, hvad man skal gøre, hvis man f.eks. har trykket på et fjendtligt link eller downloadet filer, man ikke burde have downloadet på sin arbejdscomputer.

At sikre den rigtige efteruddannelse drejer sig også om at sætte det rigtige hold, der har særligt kendskab til sårbarheder i de brugte systemer og overblik over de mest værdifulde emner. Det kan være en stor udfordring at finde den "super-medarbejder", der kan løse alle udfordringer, i stedet bør man fokusere på at en skabe gruppe af relevante medarbejdere, f.eks. sagsbehandlere, jurister, HR-medarbejdere og de it-specialister, man har. Sammen vil en sådan gruppe have fælles kompetencer til at kunne skabe det rette overblik og vide, hvilke tiltag, der er nødvendige og hvordan man bedst implementerer dem.

Iværksæt plan for at blive klar til NIS2 - både i virksomheder og i det offentlige, inkl. kommuner og regioner
Der er brug for regulering og klart definerede krav, når det handler om borgernes sikkerhed. Net- og Informationssikkerhedsdirektivet (NIS2) er netop vedtaget og EU's medlemslande har nu 21 måneder til at implementere det nye direktiv. NIS2-direktivet er en opdatering af NIS-direktivet fra

2016, der har til formål at sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele EU. NIS2 omfatter organisationer i sektorer med kritisk infrastruktur, herunder energi, transport, sundhed, drikkevand, spildevand, affaldshåndtering og offentlig administration. Det er vigtigt at lære af erfaringerne fra implementeringen af GDPR, hvor uens fortolkninger og overimplementering i flere tilfælde skabte unødigt bureaukrati og unødigt dårlig service for borgerne. Det er vores anbefaling, at den danske implementering skal ske på et klart og præcist lovgrundlag og at der udvikles en plan for, hvordan vi bedst muligt får gjort virksomheder og offentlige institutioner klar til de kommende krav.

It-sikkerhed skal være et krav i alle offentlige indkøb
Cybersikkerhed skal ikke være noget, man skal bede om eller spørge efter, men en forudsætning, når det gælder offentlige indkøb. En del af kravene kan findes i D-mærkets krav, men der bør også stilles krav til proces for opdateringer og sårbarhed. Det er vigtigt at stille obligatoriske krav til softwareudviklere og it-arkitekter om cybersikkerhed. Det er vigtigt at indse, at digitalisering ikke er en spareøvelse, men at vi simpelthen har været for lemfældige med de systemer og it-produkter, der bruges i det offentlige. Der skal ryddes op og der skal stilles skærpede krav fremover.

Udbredelse af D-mærket
50% af danske SMV'er skal have kendskab til D-mærket og min. 50 % af de danske SMV'er over 10 medarbejdere skal have D-mærket eller en certificering af lignende krav og kvalitet. Det er muligt for helt små virksomheder at søge om 50.000 kr. i tilskud til konsulenthjælp til ordningen.

D-mærket next level
Der bør igangsættes et niveau 2 for D-mærket, som bevæger sig op over de nuværende krav og som minimum er i overensstemmelse med kravene i NIS2. Det gælder både for de dataetiske og it-sikkerhedsmæssige kriterier. Målet er at give værdi til de virksomheder, der bliver certificeret i form af en blåstempling af, at man som kunde er garanteret et højt niveau af privacy og it-sikkerhed. Det forventes, at et højt niveau af it-sikkerhed i stigende grad vil blive et reelt konkurrenceparameter.

It-kørekort og sikre løsninger til borgerne
Der er ikke en klar adskillelse mellem metoderne til økonomisk it-kriminalitet rettet mod borgerne og cyberspionage, destruktive cyberangreb og cyberaktivisme. Hvis Danmark skal løftes på cybersikkerheden, så er en grundlæggende uddannelse af borgerne et vigtigt fundament. Da vi er et højt digitaliseret samfund, er det en omfattende, men nødvendig indsats. Den kollektive viden kan løftes med et it-kørekort baseret på basale regler og basal viden om digitale sårbarheder. Vi anbefaler, at en indsats koordineres med interesseorganisationer, biblioteker og oplysningsforbund med et mål om at 80% af den voksne befolkning er igennem indenfor de næste tre år. Samtidig skal der indføres basale it-sikkerhedskurser i folkeskole og på gymnasier, der hvor det ikke allerede er sat igang. Det kan være 2 x 2 timers undervisning med film og basalt materiale.

Den enkelte borger kan ikke forventes at have det fulde overblik over alle de platforme og services, vi benytter os af i det daglige. Ligesom der skal indføres klare krav til offentlige indkøb, bør der også stilles klare definerede krav til sikkerhed i it-løsninger til private borgere f.eks. it-systemer brugt i undervisning, sports- og fritidsklubber m.v.

T*askforce til at styrke cybersikkerheden i forsvarsindustriens materiel*
Der bør iværksættes en indsats for at sikre, at forsvarets digitalt baserede materiel er sikkert nok. Det gælder alt fra kommunikation til droner, sensorer og antenner. Der bør udarbejdes klare krav til cybersikkerhedsniveauet hos leverandører og udviklere til forsvaret. Samtidig er det vigtigt at sikre, at udviklere og indkøbere hos forsvarsindustrien og FMI, Forsvarets Materiel Indkøb, er opdaterede på kravene til cybersikkerhed.

Flere undervisere – flere eksperter
Der skal udvikles en strategi for at uddanne og tiltrække flere forskere og undervisere indenfor cybersikkerhedsrelaterede fag. Forskning er en forudsætning for forskningsbaseret undervisning, hvilket er et krav til universiteterne, der skal uddanne de forskere, der skal undervise på højeste niveau indenfor cybersikkerhed. Dette er igen en forudsætning for, at der kan udbydes undervisning og opbygges kompetencer på alle niveauer i de offentlige og private uddannelsesudbydere.

Et første skridt vil være at kunne rekruttere og fastholde flere danske Ph.D.-studerende - og holde på dem. En stor andel af de nuværende Ph.D.'er på cyberområdet er udenlandske, hvilket bl.a. skyldes manglende søgning fra danske studerende. Der er sjældent den store gevinst for den enkelte i at fortsætte som Ph.D.-studerende, når der findes private virksomheder, der står parat til at betale en høj løn, så snart den studerende er færdiguddannet. Men for samfundet har det en betydning, da Ph.D.-niveauet er nødvendigt for at skabe de forskere, der skal uddanne undervisere i resten af samfundet, samt skabe radikal innovation.

P.t. mangler der undervisere på alle niveauer i systemet. Det bliver en endnu større udfordring, da it-sikkerhed også må integreres på relevante områder indenfor f.eks. sundheds- og samfundsvidenskaberne, ligesom erhvervsskolerne og efter/videreuddannelsesinstitutionerne akut mangler undervisere.

Mål for de første 6 år: Danmark bliver førende indenfor it-sikkerhed, som vi i dag er det på digitalisering.

Styrk forskning i cybersikkerhed
Det er nødvendigt at sikre den rette fokus på cybersikkerhed som forskningsfelt. Det handler om at sikre hele fødekæden fra PhD'er til seniorforskere, men også om at styrke forskningsfeltet bredt. Det er vigtigt at sikre bæredygtige forskningsmiljøer på de forskellige forskningsinstitutioner, som ikke kan næres kun af små puljer, der udbydes bredt og med lange og varierende mellemrum.

Uddannelsesmæssigt skal cybersikkerhed defineres bredere
Vi er langt fra dengang it var for it-afdelingen. Hvis cybersikkerhedsniveauet skal hæves, skal der skabes en basis af viden indenfor en lang række fagområder fra tekniske specialområder til administration og bestyrelsesarbejde. Det kræver opbygning af differentieret undervisning for at sikre kompetenceløft på forskellige områder.

Styrk forskning i software "udviklet til mennesker"
Det skal ikke være besværligt at agere cybersikkert. Med vores nuværende systemer er vi afhængige af mails og usb-sticks. Vi er derfor nødt til at retænke en del af vores it-systemer, så cybersikkerhed bliver "bruger-sikkert". Danske softwareudviklere og software arkitekter skal have en grundlæggende forståelse af både sikkerhed og UX (User Experience), så der fremover udvikles systemer, der reducerer muligheden for misforståelser og betjeningsfejl og gør det vanskeligt at gennemføre et angreb baseret på "social engineering". Det er især vigtigt, at arkitekten og den UX-ansvarlige tager som udgangspunkt, at de udvikler til mennesker med alle de styrker og svagheder mennesker har. F.eks. får medarbejdere ofte at vide, at de ikke må klikke på links i e-mails, der kommer udefra, men forventes efterfølgende at deltage i en medarbejdertilfredshedsundersøgelse, de skal tilgå gennem et link i en e-mail fra et eksternt bureau – dette er et eksempel på et blandet budskab, der gør det vanskeligt at oparbejde fornuftige rutiner.

Sikre løsninger til de mindste virksomheder
90% af danske SMV'er med over 10 medarbejdere skal være certificeret i forhold til it-sikkerhed. Der er klare krav til sikkerhed i it-løsninger til små virksomheder, f.eks. bookingsystemer og regnskabssystemer.

Sikre løsninger til borgerne
Der skal være klare krav til sikkerhed i internetopkoblede produkter i it-løsninger til forbrugerne, f.eks. smart tv, spillekonsoller, fjernstyret lys- og varme, app-styrede installationer som tyverialarmer og musikanlæg. Dette krav bør gælde alt udstyr der forbindes til internettet og bør som minimum inkludere et krav om, at produkter kan sikkerhedsopdateres og at leverandøren har tilstrækkelige forpligtelser og procedurer til at håndtere sikkerhedsopdateringer i hele produktets forventede levetid.