Et konkurrencedygtigt dansk erhvervsliv gennem styrket IT-sikkerhed

ANBEFALINGER FRA VIRKSOMHEDSRÅDET FOR IT-SIKKERHED

Marts 2017

Forord fra formanden

Der går stort set ikke en uge uden nyheder om IT-sikkerhedshændelser eller -problemer. Det er alt fra store begivenheder som tyveri af store mængder brugerdata til små fejl som virus i legetøj.

Meget tyder på, at disse historier endda kun er toppen af isbjerget. Risikoen for at blive udsat for cyberspionage eller cyberkriminalitet er stor, og skal håndteres forsvarligt af alle virksomheder. Store og små. På samme måde som alle andre risici, en virksomhed er udsat for.

Samtidig nærer brugere og kunder stor tillid til de digitale kanaler, og de færreste har problemer med at udveksle selv de mest fortrolige informationer digitalt. Til stor gavn for alle parter. Men denne tillid kan hurtigt forsvinde, hvis virksomheder ikke håndterer disse data på en god måde.

Fra maj 2018 vil den kommende Persondataforordning stille nye, skærpede krav til, hvordan virksomheder og organisationer i EU skal agere indenfor IT-sikkerhed og datahåndtering.

Af de grunde bliver tilstrækkelig IT-sikkerhed og god datahåndtering en forudsætning for at drive virksomhed i dag, ikke bare i Danmark, men globalt. Dermed kan god praksis på disse områder blive en konkurrencefordel for danske virksomheder, hvis de i tide bliver gode nok. Desværre tyder meget på, at især de små og mellemstore virksomheder halter bagefter.

I aftalen 'Vækstplan for digitaliseringen i Danmark' mellem SR-regeringen og alle Folketingets øvrige partier fra februar 2015 blev det bestemt, at der skulle nedsættes et Virksomhedsråd for IT-sikkerhed. Rådet skulle blandt andet skulle komme med anbefalinger til erhvervsministeren om, hvordan god digital sikkerhed og god datahåndtering i små og mellemstore virksomheder kunne styrkes.

Rådet begyndte sit arbejde i foråret 2016 og har dels på baggrund af medlemmernes viden og dels ud fra danske og udenlandske erfaringer skabt grundlaget for anbefalingerne.

Rådets medlemmer var udvalgt, så der kom et bredt perspektiv på opgaven. Alt lige fra IT-ansvarlige over leverandører til IT-sikkerhedsspecialister har bidraget.
Medlemmerne var:

Ann Harkjær Frederiksen, Økonomichef, Svend Frederiksen Maskinfabrik
Annette Falberg, Branchedirektør, DI Handel
Charlotte Pedersen, Director, Deloitte
Claus Bak Petersen, CEO, Auditdata
Ingrid Colding-Jørgensen, IT-sikkerhedsspecialist
Jacob Herbst, Chief Technical Officer, Dubex
Lars Neupart, Sikkerhedsdirektør, GRC, Neupart KMD
Marianne Dahl Steensen, CEO, Microsoft Denmark
Max Gersvang Sørensen, Corporate Counsel, LEGO group
Merete Søby, Managing Director, HDS
Michael Busk-Jepsen, Digitaliseringsdirektør, Finans Danmark
Per Palmkvist Knudsen, CIO, JP/Politikens Hus (formand)
Rasmus Theede, Director Cybersecurity, CSC

Resultatet i form af denne rapport er målrettet ministeren, organisationerne og erhvervslivet. Egentlig vejledning til enkeltvirksomheder er andre steder, se eksempelvis PrivacyKompasset og SikkerhedsTjekket.

Jeg ser frem til en fortsat debat om, hvad der skal til for, at danske virksomheder ikke bare har de basale ting på plads indenfor god IT-sikkerhed og datahåndtering, men også kan udnytte dette som en konkurrenceparameter i en stadigt mere digitaliseret verden.

Per Palmkvist Knudsen
Formand for Virksomhedsrådet for IT-sikkerhed
Marts 2017

INDHOLDSFORTEGNELSE

Indledning

Digital tillid er en forudsætning for digital vækst. Den øgede digitalisering af samfundet gør IT-sikkerhed og ansvarlig datahåndtering til kritiske faktorer i alle dele af samfundet. Det gælder for borgerne, den offentlige sektor og ikke mindst virksomhederne - både store og små.

Høj IT-sikkerhed og ansvarlig datahåndtering handler både om, at virksomheden har de nødvendige tekniske foranstaltninger så som antivirus, back-up løsninger mv. på plads. Og om ledelsens opmærksomhed, medarbejdernes viden og kompetencer samt om at have en understøttende organisation og kultur. Det betyder, at det er en opgave for hele organisationen og ikke kun IT-afdelingen at skabe en virksomhed, der er robust i forhold til sikkerhedshændelser, og som håndterer kunders og brugeres data på en forsvarlig måde.

Flere og flere virksomheder rammes i disse år af brud på IT-sikkerheden og oplever læk af følsomme persondata og forretningskritiske data – og truslen fra bl.a. hackere og cyberangreb er stigende. Hændelserne har store konsekvenser for virksomhederne såvel som de kunder og samarbejdspartnere, hvis data lækkes.

Omkostningerne omfatter bl.a. udgifter til genopretning af utilgængelige eller ødelagte systemer, skepsis i forhold til at foretage nye investeringer i digitale løsninger og omkostningerne forbundet med tabt omdømme og troværdighed blandt kunder og samarbejdspartnere.

Et øget fokus på IT-sikkerhed og ansvarlig datahåndtering kan mindske omkostningerne og sikre, at borgere og kunder har tillid til virksomhedens digitale systemer. Men det kan også skabe en ny konkurrencefordel for dansk erhvervsliv i den digitale økonomi. Hvis dansk erhvervsliv er på forkant og bliver kendt som en sikker og dataansvarlig samarbejdspartner og leverandør, kan det give nye forretningsmuligheder og konkurrencefordele i en tid, hvor fokus på IT-sikkerhed og beskyttelse af kritiske data øges verden over. Derfor skal Danmark være det land i Europa, hvor borgerne har størst tillid til, at virksomhederne behandler deres data sikkert.

Virksomhedsrådet for IT-sikkerhed anbefaler på den baggrund, at der opstilles følgende vision for IT-sikkerheden og håndteringen af data i dansk erhvervsliv:

VIRKSOMHEDSRÅDETS VISION

Dansk erhvervsliv skal være anerkendt som en troværdig og attraktiv samarbejdspartner med et højt niveau af IT-sikkerhed og ansvarlig datahåndtering.

Indsatsområder

Hvis visionen skal realiseres, og Danmark skal være anerkendt som en troværdig og attraktiv samarbejdspartner med et højt niveau af IT-sikkerhed og ansvarlig datahåndtering, kræver det en målrettet indsats på flere fronter.

Det er først og fremmest virksomheden selv, som har ansvar for at have styr på sin IT-sikkerhed og datahåndtering – uanset virksomhedens størrelse og om virksomhedens IT er outsourcet eller ej, men erhvervs- og brancheorganisationer og det offentlige spiller også en vigtig rolle, hvis visionen skal nås.

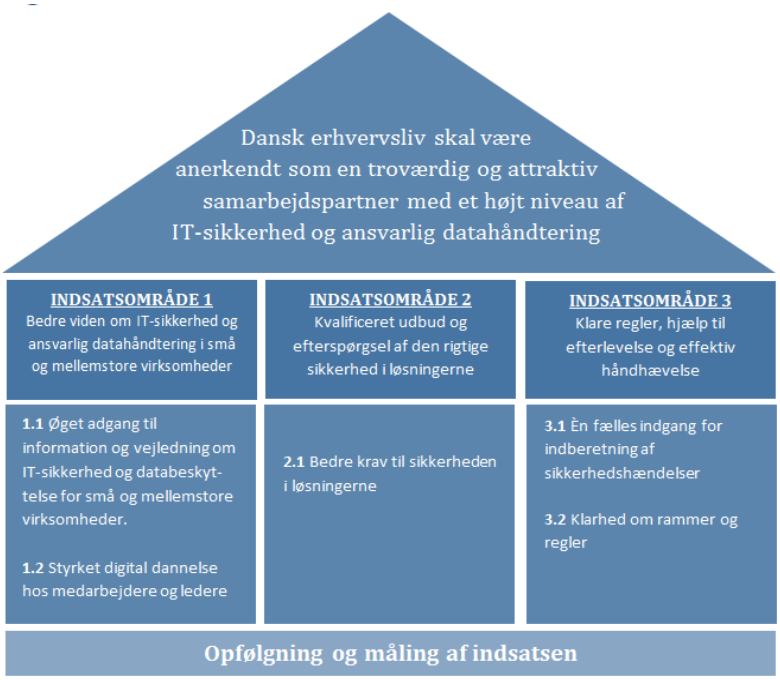
Virksomhedernes opmærksomhed og kapacitet til at sikre sine digitale systemer og kritiske data skal øges. Det omfatter øget viden om aktuelle trusler og hensigtsmæssige tekniske forholdsregler såsom installation af antivirus og back-up løsninger, men også øget viden hos ledelse og medarbejdere om potentielle sårbarheder og relevante forholdsregler og processer.

Samtidig skal rammerne for virksomhederne være på plads. Virksomhederne skal have adgang til et velfungerende marked med leverandører af IT-sikkerhedsprodukter og -tjenester, som også er rettet mod og efterspurgt af små- og mellemstore virksomheder.

Endelig skal virksomhederne møde klare reguleringsmæssige rammer, der er lette at efterleve, og som giver virksomhederne færrest mulige byrder. Og der skal være offentlige myndigheder, som kan bistå med at afdække trusselsbilledet, efterforske hændelser og sikre en effektiv og gennemsigtig håndhævelse af reglerne.

Gode rammebetingelser er ikke mindst af stor betydning for de små- og mellemstore virksomheder, som typisk har færre ressourcer og kompetencer in-house til at håndtere IT-sikkerhed og kritiske data. Virksomhedsrådet for IT-sikkerhed anbefaler på den baggrund, at der sættes ind på følgende områder:

Anbefalinger fra Virksomhedsrådet for IT-sikkerhed



1. Bedre viden om IT-sikkerhed og ansvarlig datahåndtering i små og mellemstore virksomheder

Mange virksomheder mangler i dag viden om aktuelle cybertrusler, potentielle konsekvenser af cyberangreb og relevante tiltag til at beskytte deres IT-systemer og data. Det gælder ikke mindst små- og mellemstore virksomheder uden egen IT-afdeling. Samtidig er meget af den information og vejledning, der i stigende grad bliver tilgængelig for virksomhederne, skrevet i et relativt teknisk sprog, som kan være svært tilgængelig for ledere og medarbejdere uden særlige IT-sikkerhedsfaglige kundskaber.

Virksomhedsrådet anbefaler på den baggrund, at der iværksættes en indsats for at styrke små- og mellemstore virksomheders adgang til information og vejledning om IT-sikkerhed og ansvarlig datahåndtering. Informationen skal være lettilgængelig, i øjenhøjde og målrettet virksomhedernes behov, så den kan omsættes til konkret handling. Det skal løfte virksomhedernes bevidsthed og viden om samt kapacitet til at imødegå IT-sikkerhedstrusler.

Der er endvidere brug for, at ledere og medarbejderes grundlæggende viden om IT-sikkerhed og ansvarlig datahåndtering løftes. Virksomhedsrådet anbefaler derfor, at den generelle digitale dannelse styrkes gennem hele det danske uddannelsessystem og i den løbende efteruddannelse af ledere og medarbejdere.

2. Kvalificeret udbud og efterspørgsel af den rigtige sikkerhed i løsningerne

Det er de færreste virksomheder, der i en stadig mere avanceret digital virkelighed selv besidder alle de nødvendige kompetencer, der skal til for at sikre et robust og tilstrækkeligt sikkerhedsniveau. Det er derfor centralt at virksomhederne – ikke mindst de små- og mellemstore – har kapaciteten til at efterspørge den rette sikkerhed i løsningerne og derved understøtter et velfungerende marked af leverandører af digitale ydelser.

Virksomhedsrådet anbefaler derfor, at der tages tiltag, der understøtter små og mellemstore virksomheder i en kvalificeret efterspørgsel efter IT-sikkerhedsprodukter og – services fra deres leverandører, som matcher deres behov.

3. Klare regler, hjælp til efterlevelse og effektiv håndhævelse

Klar og gennemsigtig lovgivning, der ikke er unødvendigt byrdefuldt at efterleve, er et vigtigt fundament for dansk erhvervslivs konkurrenceevne. I disse år skærpes de europæiske regler i forhold til bl.a. håndtering af persondata og informationssikkerhed. Det stiller nye krav til dansk erhvervsliv. Virksomhedsrådet anbefaler, at der er fokus på at sikre, at reglerne er lette at efterleve for danske virksomheder, og at håndhævelsen af reglerne er gennemskuelig og rimelig. Samtidig skal der tages tiltag for at styrke virksomhedernes adgang til vejledning om de nye regler.

IT-sikkerhed er et område i kontinuerlig forandring. Cybertruslerne udvikler sig hele tiden og angrebene bliver mere og mere avancerede. Samtidig er det et område præget af mørketal om det faktiske antal af angreb og hændelser. Virksomheder og andre organisationer er meget tilbageholdende med at give informationer om hændelser, bl.a. pga. frygt for deres omdømme. Virksomhedsrådet anbefaler derfor, at der gennemføres årlige undersøgeler af, hvilke og hvor mange hændelser danske virksomheder oplever.

Opfølgning og måling af indsatsen

Virksomhedsrådet anbefaler derudover, at der inden for hvert af de tre indsatsområder fremadrettet skal være et skarpt fokus på effekterne af de konkrete tiltag, der bliver igangsat for at opfylde visionen. Det kræver, at der opstilles klare og relevante målepunkter, der i højere grad end i dag gør det muligt løbende at følge udviklingen inden for IT-sikkerhed og ansvarlig datahåndtering i dansk erhvervsliv samt at indsatsen kontinuerligt tilpasses til den hastige digitale udvikling.

INDSATSOMRÅDE 1
Bedre viden om IT-sikkerhed og ansvarlig datahåndtering i små og mellemstore virksomheder

Dansk erhvervsliv står overfor et voksende trusselsbillede. Center for Cybersikkerhed vurderer, at truslen fra cyberspionage og cyberkriminalitet mod danske virksomheder er meget høj[1] – og der er ikke noget, der tyder på, at den vil falde i fremtiden. I takt med, at cyberkriminalitet bliver mere avanceret og dansk erhvervsliv står overfor et trusselsbillede, der bliver ved med at udvikle sig, stiger behovet også for at styrke de små og mellemstore virksomheders viden omkring IT-sikkerhed og databeskyttelse.

De små og mellemstore virksomheder er i stigende grad opmærksomme på vigtigheden af at ruste sig mod brud på IT-sikkerheden. Men vidensniveauet på området blandt ledere og medarbejdere er fortsat begrænset.

1.1 Øget adgang til information og vejledning om IT-sikkerhed og databeskyttelse for små og mellemstore virksomheder

Mange små og mellemstore virksomheder har ikke grundlæggende kendskab til, hvilke cybertrusler de er mest udsat for, de konsekvenser et cyberangreb kan medføre eller hvordan de beskytter deres IT-systemer eller forretningskritiske data mest effektivt imod et trusselsbillede, som er i konstant udvikling.

Den eksisterende trusselsinformation og vejledning til at styrke informationssikkerheden kan for små og mellemstore virksomheder ofte opleves for teknisk svær at forstå og ikke tilstrækkelig handlingsanvisende. Samtidig kommer en del af informationen fra aktører, der kan have en kommerciel interesse i at overvurdere truslerne. Tilsvarende kan det være svært at orienterer sig i, hvor man skal gå hen for at få viden på området, da information ligger spredt mange steder.

1 Center for Cybersikkerhed "Cybertruslen mod Danmark" februar 2017

Derfor er der behov for at styrke virksomhedens viden og kapacitet til at ruste sig bedst mod sikkerhedshændelser. Det handler især om at øge virksomhedernes viden om aktuelle trusler, deres kapacitet til at identificere sårbarheder, som trusler skaber i deres organisation samt øge deres beredskab, så de er rustet mod brud på sikkerheden. Virksomhederne skal derfor have:

Denne viden skal formidles i øjenhøjde til virksomhederne og være differentieret, således at den er brugbar for både virksomheder, der stort set ikke har arbejdet med IT-sikkerhed og virksomheder, som allerede er i gang. Adgangen til disse informationer og værktøjer skal være lettilgængelig og overskuelig for virksomhederne. Det kan ske ved at samle den relevante viden, hvor virksomhederne naturligt søger information. Der kan søges inspiration fra Norge og Storbritannien, hvor viden om informationssikkerhed og ansvarlig datahåndtering er samlet hos henholdsvis Norsk Senter for Informasjonssikring (NorSIS) og National Cyber Security Centre. Informationen kan med fordel indgå på den fællesoffentlige myndighedsportal virk.dk, hvor virksomhederne allerede færdes i dag.

Anbefaling 1.1
Øget adgang til information og vejledning om IT-sikkerhed og databeskyttelse for små og mellemstore virksomheder

Virksomhedsrådet for IT-sikkerhed anbefaler, at der i samarbejde med erhvervs- og brancheorganisationer iværksættes en samlet indsats for, at små og mellemstore virksomheder har nem adgang til målrettet og relevant information om IT-sikkerhed og databeskyttelse.
Indsatsen skal have fokus på:

- Løbende formidling af viden om aktuelle nationale og internationale trusler. Trusselsinformationen skal være let forståelig og kombineres med handlingsanvisende vejledning.
- Udvikling af konkrete redskaber og vejledninger, der udbygger de eksisterende værktøjer som Sikkerhedstjekket og PrivacyKompasset. Det kan fx være udviklingen af et tjek, der er målrettet specifikke funktioner som fx HR, bogføring, markedsføring og lign.
- Et katalog over eksisterende standarder for informationssikkerhed og tekniske løsninger, der med fordel kan anvendes til at højne IT-sikkerhed og databeskyttelse, og vejledning til virksomheder om at vælge de løsninger, der passer til deres risikoprofil.
- Overblik og vejledning om gældende lovgivning samt information om, hvor man som virksomhed kan henvende sig ved tvivlsspørgsmål.

1.2 Styrket digital dannelse hos medarbejdere og ledere

En meget stor del af de sikkerhedshændelser, som virksomhederne oplever, opstår, fordi ledere og medarbejdere ikke har en tilstrækkelig viden om, hvordan de navigerer sikkert digitalt.

Sikkerhedshændelserne kan skyldes bevidste skadelige handlinger fra medarbejdere såsom tyveri af data eller bevidst installering af skadeligt software. Ofte skyldes brudene dog ubevidste handlinger, hvor en medarbejder utilsigtet klikker på en såkaldt phishing-mail og dermed utilsigtet downloader skadelig software eller udløser et ransomware angreb.

Medarbejdernes brug af virksomhedens IT-udstyr til private formål øger også risikoen for utilsigtede hændelser, fx når hackere udnytter en sårbarhed i et downloadet spil på arbejds-pc, -tablet eller -telefon.

Undersøgelser peger på, at 30 pct. af danske virksomhedsledere ser deres egne medarbejdere som den største trussel mod deres IT-sikkerhed.[2] De fleste medarbejdere ved godt, at de skal skifte password regelmæssigt og forholde sig kritisk til mails, der kan være forsøg på phishing. Alligevel er det de færreste, der rent faktisk gør det. Der er derfor behov for at øge den grundlæggende digitale indsigt og forståelse for digitale risici hos ledere og medarbejdere på alle niveauer.

Det kræver en langsigtet indsats startende allerede i folkeskolen. Der eksisterer allerede en række gode initiativer, herunder CodeX som udbydes til en række folkeskoler, der sætter fokus på digital tryghed hos eleverne. Initiativerne er ofte båret af ildsjæle og endnu ikke bredt implementeret på tværs af uddannelser. Det er derfor vigtigt, at der støttes op om allerede igangsatte initiativer, og at de udbredes til en bredere kreds.

Digital dannelse stopper ikke i folkeskolen. En efteruddannelsesindsats med fokus på både grundlæggende kurser i IT-sikkerhed og ansvarlig datahåndtering samt mere specialiserede kurser skal fremme, at også nuværende medarbejdere bliver kvalificeret til at agere sikkert digitalt og får den nødvendige viden om ansvarlig digital færden.

I Storbritannien har regeringen igangsat en række initiativer, der kan søges inspiration i, herunder The Cyber Security Challenge og The Cyber School Programme. Formålet med programmerne er at øge bevidstheden samt opfordre og inspirere unge mennesker til en karriere indenfor IT-sikkerhed og ansvarlig datahåndtering.

---

[2] PWC "Cybercrime Survey" 2016.

Anbefaling 1.2.
Styrket digital dannelse hos medarbejdere og ledere

Virksomhedsrådet for IT-sikkerhed anbefaler, at der iværksættes en målrettet indsats med fokus på digitale kompetencer. Indsatsen skal have fokus på:

- Ledelses- og bestyrelsesuddannelse i IT-sikkerhed og ansvarlig datahåndtering, der skal gøre virksomhedslederne bevidste om vigtigheden af at have fokus på disse temaer og skabe en sikkerhedsbevidst kultur i virksomheden.
- Efteruddannelse og kvalifikationsløft af medarbejdere på tværs af faggrupper med fokus på både grundlæggende viden om ansvarlig digital færden samt på efter- og videreuddannelse af eksperter.
- Ændring af medarbejdere og lederes adfærd i forhold til IT-sikkerhed og ansvarlig datahåndtering. Der kan gennemføres konkurrencer om at udvikle initiativer, der kan fremme en mere hensigtsmæssig IT-sikkerhedsadfærd, fx gennem brug af nudging-metoder.
- Støtte op om og udbrede allerede igangsatte initiativer, der har fokus på digital dannelse i folkeskolen og på ungdomsuddannelser.

INDSATSOMRÅDE 2
Kvalificeret udbud og efterspørgsel af den rigtige sikkerhed i løsningerne

Et effektivt servicelag, der både kan rådgive virksomheder om risikostyring og ansvarlig anvendelse af data samt levere de nødvendige løsninger, er en forudsætning for, at danske virksomheder kan forbedre deres IT-sikkerhed og datahåndtering og derved drive en robust digital forretning. Samtidig skal det være let og overskueligt for virksomhederne at vurdere, hvilke leverandører der lever op til nationale og internationale krav til datasikkerhed.

2.1 Bedre krav til sikkerheden i løsningerne

Det er de færreste virksomheder, der selv besidder alle de nødvendige kompetencer, der skal sikre et robust og tilstrækkeligt sikkerhedsniveau. Derfor outsourcer mange særligt mindre og mellemstore virksomheder også en stor del af deres IT. I 2016 blev funktioner relateret til IT-sikkerhed og databeskyttelse i 65 pct. af danske virksomheder primært udført af eksterne leverandører, men kun 39 pct. stiller krav til virksomhedens leverandører vedr. IT-sikkerhed[3]. I sidste ende er det dog virksomheden selv, der skal tage ansvar for sine egne data og derfor er der behov for bedre redskaber til leverandørstyring så virksomhederne bliver i stand til at stiller de nødvendige krav vedr. sikkerheden til deres leverandører.

For at kunne indgå i en kvalificeret dialog med leverandører af digitale ydelser og IT-sikkerhedsløsninger er det væsentligt, at danske virksomheder er bevidste om trusselsniveauet, deres egen risikoprofil og potentielle sårbarheder og dermed, hvad der er et passende sikkerhedsniveau for deres forretning.

Det kræver, at virksomhedernes kapacitet til at efterspørge de relevante løsninger understøttes. Derfor skal virksomhedernes nærmeste rådgivere (bl.a. revisorer, advokater og finansielle rådgivere) i højere grad blive i stand til at oplyse virksomhederne om, hvilke opmærksomhedspunkter de bør have i forhold til IT-sikkerhed og ansvarlig datahåndtering, samt hvor virksomhederne kan få konkret rådgivning og hjælp. Samtidig skal virksomhederne have adgang til let og overskuelige viden om indhold og værdien af nationale og internationale standarder og mærkninger, som de kan efterspørge hos potentielle leverandører.

[3] Danmarks Statistik "Virksomhedernes IT-anvendelse" 2016

I Storbritannien har National Cyber Security Centre en sektion på deres hjemmeside dedikeret til leverandører af sikkerhedsløsninger. Her kan virksomheder få et overblik over, hvilke leverandører der er certificeret, og hvem der kan hjælpe med hvilke problemstillinger.

Anbefaling 2.1.: Bedre krav til sikkerheden i løsningerne

Virksomhedsrådet for IT-sikkerhed anbefaler, at der skal gøres en aktiv indsats for at styrke små og mellemstore virksomheders efterspørgsel efter IT-sikkerhedsløsninger. Der bør sættes ind på følgende områder:

- Løft af viden inden for IT-sikkerhed og datahåndtering hos små og mellemstores virksomheders primære rådgivere, herunder revisorer, advokater og finansielle rådgivere, gennem efter- og videreuddannelse.
- Virksomhederne skal med udgangspunkt i en konkret risikovurdering blive mere kvalificerede indkøbere. Det skal ske via Sikkerhedstjekket.dk, der skal udbygges med bedre redskaber til leverandørstyring, fx standardkontrakter, standardbilag og spørgeguides.
- Fremme brugen af internationale og nationale standarder og mærkningsordninger for IT-sikkerhed og ansvarlig datahåndtering, der skal gøre det let og overskueligt at vurdere om potentielle leverandører har sikkerheden i orden.

INDSATSOMRÅDE 3
Klare regler, hjælp til efterlevelse og effektiv håndhævelse

Klare reguleringsmæssige rammer og en effektiv håndhævelse, der er gennemskuelig og ikke unødigt byrdefuld at leve op til, er forudsætninger for, at virksomhederne kan fokusere deres ressourcer på dels at løse deres sikkerhedsudfordringer effektivt og dels at udnytte de digitale vækstmuligheder bedst muligt.

Der tages i disse år en række reguleringsmæssige initiativer som modsvar til stigningen i sikkerhedshændelser. I maj 2018 træder persondataforordningen i kraft. Forordningen indeholder bl.a. krav om øget dokumentation og krav til virksomhedernes tekniske og organisatoriske set-up, samt bestemmelser om, at tilsynsmyndighederne kan udstede administrative bøder på op til 20.000.000 euro eller 4 pct. af omsætningen ved overtrædelse af forordningens bestemmelser.

Endvidere vil det kommende NIS-direktiv, der også skal være implementeret senest i maj 2018, introducere et krav om anmeldelse af sikkerhedshændelser, som strækker sig ud over persondataforordningens krav om anmeldelse af brud på den personlige datasikkerhed til private virksomheder i sektorerne for finansielle ydelser, energi, transport, sundhed, vand og digital infrastruktur med mere end 50 ansatte. Direktivet fastlægger sikkerhedskrav for operatører af digitale serviceudbydere (onlinemarkedspladser, søgemaskiner og cloudbaserede IT-ydelser).

Persondataforordningen forpligter organisationer til at rapportere et brud, når risikoen for privatlivets fred for de dataregistrerede er høj, mens NIS-direktivet, kræver at operatører anmelder til myndighederne, hver gang en sikkerhedshændelse (enhver hændelse, der har en aktuel, kritisk effekt på netværks- og informationssystemers sikkerhed) har en betydelig indflydelse på leveringen af deres ydelser.

3.1 Én fælles digital indgang for indberetning af sikkerhedshændelser

En konsekvens af de reguleringsmæssige initiativer er, at danske virksomheder skal indberette og anmelde sikkerhedshændelser til forskellige myndigheder.

Persondataforordningen stiller krav til alle typer virksomheder om indberetning af databrud til Datatilsynet, og implementering af NIS-direktivet indeholder krav om indberetning af alvorlige sikkerhedshændelser til en relevant myndighed. Det betyder, at en større del af erhvervslivet, herunder også små og mellemstore virksomheder, vil blive underlagt krav om at indberette sikkerhedshændelser. Det er ressourcekrævende for den enkelte virksomhed at overskue, hvor man indberetter, og hvad der skal indberettes. Det kan medføre, at virksomhederne ikke nødvendigvis altid indberetter og anmelder, hvilket kan være til skade for både virksomheden og samfundet, da tilbageløb af viden om trusselsbilledet er vigtig for at vurdere og bekæmpe truslerne. Virksomhederne giver samtidig udtryk for, at de sjældent modtager tilbagemeldinger fra myndighederne om, hvad der sker med de oplysninger de indberetter, herunder hjælp til hvordan de kan arbejde med at forebygge lignende hændelser.

Virksomhederne bør ikke skulle bruge unødig tid og ressourcer på at gennemskue, til hvilken myndighed og hvad der skal indberettes. Dette gælder særligt de lovpligtige indberetninger, men også anmeldelser til politiet.

Anbefaling 3.1
Én fælles digital indgang for indberetning af sikkerhedshændelser:

Virksomhedsrådet for IT-sikkerhed anbefaler, at det bliver gjort nemt og enkelt for virksomhederne at indberette sikkerhedshændelser til det offentlige. Indsatsen skal have fokus på:

- At der på tværs af myndigheder etableres én fælles digital indgang for virksomhederne for indberetning af sikkerhedshændelser.
- At det særligt gælder de lovpligtige indberetninger, men samtidig muliggør en smidig anmeldelse til politiet. Det er dog vigtigt, at det tydeliggøres, når der er tale om anmeldelser til politiet.
- At indgangen giver virksomhederne letforståelig og handlingsorienteret information tilbage om forebyggelse og håndtering af hændelser, jf. anbefaling 1 om styrket information.
- At indgangen placeres på Virk.dk, som allerede i dag er den digitale indgang for virksomheder i forhold til indberetninger til det offentlige.

3.2 Klarhed om rammer og regler

I disse år skærpes de europæiske regler i forhold til bl.a. håndtering af persondata og indberetning af IT-sikkerhedshændelser. Det stiller nye krav til dansk erhvervsliv. Det er vigtigt, at lovgivningen og håndhævelsen heraf gøres så klar og gennemsigtig som mulig, så den ikke er unødvendigt byrdefuld for virksomhederne at efterleve.

Mange virksomheder oplever, at de mangler konkret og handlingssorienteret information og vejledning om, hvordan reguleringen skal fortolkes og implementeres. Denne usikkerhed risikerer at udgøre en hæmsko for øget digitalisering og brug af data.

Det er endvidere væsentligt, at der er en ensartet implementering af europæisk lovgivning om IT-sikkerhed og ansvarlig datahåndtering for at sikre ensartede rammevilkår i EU.

Når kommende lovgivning inden for IT-sikkerhed og datahåndtering skal implementeres, er det vigtigt, at der er tværministeriel koordination, og der sikres fleksibilitet i forhold til den teknologiske udvikling, således at der i højere grad sigtes på rammelovgivning og regulering af formål frem for brugen af teknologier. Ligeledes er det vigtigt, at unødige danske særregler undgås.

Der er allerede igangsat en række initiativer, der skal skabe klarhed omkring fortolkningen af gældende og kommende lovgivning inden for IT-sikkerhed og datahåndtering, herunder den kommende persondataforordning. Det er vigtigt, at vejledning - både i form af skriftlige vejledninger og muligheden for at få svar i konkrete tvivlstilfælde – prioriteres højt, så virksomheder har adgang til det rette niveau af viden og vejledning om gældende og kommende lovgivning fra den rette myndighed. Derfor opfordrer Virksomhedsrådet for IT-sikkerhed til, at der i det offentlig prioriteres de nødvendige ressourcer til at gennemføre en vejledningsindsats overfor de små og mellemstore virksomheder, der matcher virksomhedernes behov.

Hvis ansvarlig datahåndtering skal være et fremtidigt konkurrenceparameter, er det samtidig væsentligt, at håndhævelsen af lovgivningen styrkes og gøres mere gennemsigtig.

Virksomhederne oplever, at bevisbyrden ved meget kompliceret IT-kriminalitet ofte ligger hos dem selv, og at der er begrænset hjælp at hente hos myndighederne. Samtidig er det ofte uigennemsigtigt for virksomhederne, hvad der sker med en sag efter anmeldelse. Begge forhold kan afholde virksomheder fra at indberette hændelser, hvilket kan være til skade for såvel virksomhederne selv som klarheden om de aktuelle trusler og hændelser.

Anbefaling 3.2
Klare og enklere regler og effektiv håndhævelse

Virksomhedsrådet anbefaler, at reglerne inden for IT-sikkerhed og datahåndtering skal være lette at efterleve for danske virksomheder og håndhævelsen af reglerne skal være gennemskuelig og rimelig. Der bør sættes ind på følgende områder:

- Opstilling af målsætninger for politiets arbejde i forhold til IT-kriminalitet, herunder løbende rapportering om anmeldelser samt offentliggørelse af opklaringsprocenter
- Ved udarbejdelse af ny lovgivning indenfor det digitale område sigtes på rammelovgivning og regulering af formål frem for brugen af teknologier.
- Udarbejdelse af konkret handlingsanvisende vejledning i persondataforordningen. Vejledningen kan med fordel opdeles efter konkrete emner og arbejdsopgaver og tage udgangspunkt i, hvad andre virksomheder har gjort i specifikke situationer.

Opfølgning og måling af indsatsen

De ovenstående anbefalinger er Virksomhedsrådets bud på, hvordan udfordringerne i forhold til IT-sikkerhed og ansvarlig datahåndtering kan håndteres. IT-sikkerhedsområdet er dog et område i kontinuerlig forandring, hvor angrebstyper og hændelser ændrer sig konstant. Samtidig er antallet af hændelser, hvor der sker brud på IT-sikkerheden steget betydeligt over de seneste år. Men viden om, hvor meget antallet af hændelser faktisk er steget, og hvilke typer hændelser der oftest rammer virksomhederne, er behæftet med stor usikkerhed.

Usikkerheden skyldes, at virksomheder og andre organisationer ofte ønsker at undgå opmærksomhed om konkrete hændelser og derfor ikke anmelder eller rapporterer, når de oplever brud på IT-sikkerheden. Det resulterer i store mørketal, der gør det svært at følge udviklingen i IT-sikkerhedshændelser, og derved også at fastslå om tiltag, der skal styrke IT-sikkerheden erhvervslivet, virker eller ej.

For at få en bedre indsigt i, hvilke typer sikkerhedshændelser virksomhederne typisk oplever, er der brug for et bedre og mere retvisende vidensgrundlag. Samtidigt er der brug for, at der kontinuerligt følges op på de igangsatte initiativer for at sikre, at de fungerer efter hensigten. Endeligt er der brug for, at IT-sikkerhed og ansvarlig datahåndtering prioriteres i internationale fora for at sikre en optimal videndeling.

Anbefaling
Opfølgning og måling af indsatsen

Virksomhedsrådet anbefaler, at det fremadrettede arbejde med IT-sikkerhed og ansvarlig datahåndtering bygger på konkret og opdateret viden. På den baggrund bør følgende aktiviteter igangsættes:

- I forbindelse med Danmarks Statistiks undersøgelse af IT-anvendelse i virksomhederne bør der fokuseres på udviklingen i danske virksomheders IT-sikkerhed.
- For at muliggøre internationale sammenligninger, bør der gennemføres internationale undersøgelser af virksomheders IT-sikkerhed og ansvarlig datahåndtering fx i regi af OECD.
- For at sikre, at de igangsatte initiativer fungerer efter hensigten, skal der opstilles klare og relevante målepunkter, der i højere grad end i dag gør det muligt løbende at følge udviklingen inden for IT-sikkerhed og ansvarlig datahåndtering i dansk erhvervsliv.