Anbefaling:

En mærkningsordning for it-sikkerhed

Virksomhedsrådet for IT-SIKKERHED

Virksomhedsrådet for IT-sikkerhed anbefaler

Der skal etableres et mærke for it-sikkerhed, der signalerer, at en virksomhed har implementeret it-sikkerhedsforanstaltninger, som beskytter mod de mest almindelige sikkerhedshændelser.

Mærket skal:

- være frivilligt
- have små og mellemstore virksomheder som primær målgruppe
- reducere virksomhedernes risiko for it-sikkerhedshændelser – herunder ved hjælp af medarbejder-awareness
- hjælpe kunder, aftagere, forbrugere og samarbejdspartnere med at vælge virksomheder, der har styr på it-sikkerhed og ansvarlig dataanvendelse
- kickstarte virksomhedernes arbejde med it-sikkerhed, så rejsen mod endnu bedre og mere avancerede tiltag bliver lettere og mere overskuelig
- være en ramme for dialog om it-sikkerhed mellem kunder, leverandører, medarbejdere og alle øvrige samarbejdspartnere
- være et skridt i den rigtige retning mod efterlevelse af krav til virksomheders datasikkerhed i leverandøraftaler
- samtænkes med andre relevante initiativer, og udvikles i samarbejde med relevante parter

Baggrund:

SMV'erne har ikke godt nok styr på it-sikkerheden

Flere tilfælde af bredt omtalte og omkostningsfulde it-sikkerhedsbrud har betydet, at mange større danske virksomheder er begyndt at forbedre deres it-sikkerhed. Samtidig stilles der i dag lovmæssige krav til it-sikkerheden i forsyningsvirksomheder og udbydere af digitale tjenester i NIS-direktivet, mens den danske regering med Den nationale strategi for cyber- og informationssikkerhed har stillet krav til de samfundskritiske sektorer.

Udfordring
Mange danske virksomheder, herunder særligt SMV'er, har ikke implementeret basale it-sikkerhedsforanstaltninger og er derfor unødigt sårbare over for de mest almindelige it-sikkerhedshændelser.

Disse indsatser er vigtige og afgørende for Danmarks sikkerhed. Men en meget stor del af dansk erhvervsliv består af små og mellemstore virksomheder, som også er sårbare over for it-sikkerhedshændelser. En undersøgelse fra 2018 viste for eksempel, at fire ud af ti små og mellemstore virksomheder ikke har et passende it-sikkerhedsniveau i forhold til deres risikoprofil (DELOITTE/ERHVERVSSTYRELSEN: *IT-sikkerhed og datahåndtering i danske SMV'er*). Der er derfor behov for en fokuseret indsats for at løfte it-sikkerhedsniveauet i danske SMV'er.

Løsning:

Et mærke for IT-sikkerhed

Heldigvis kan mange danske virksomheder reducere deres risiko for it-sikkerhedshændelser betydeligt, hvis de får styr på de mest grundlæggende it-sikkerhedstiltag. Derfor anbefaler Virksomhedsrådet for IT-sikkerhed, at der etableres en frivillig mærkningsordning for it-sikkerhed, der kan give virksomhederne et incitament til at påbegynde arbejdet med it-sikkerhed. Langt de fleste it-sikkerhedshændelser er nemlig nemme at dæmme op for, og med den basale it-sikkerhed på plads, er det Virksomhedsrådets vurdering, at virksomhederne kan imødegå op til 90 procent af it-sikkerhedshændelserne.

Formål
Et mærke for it-sikkerhed skal gøre det lettere for virksomhederne at strukturere deres arbejde med it-sikkerhed og opnå et basalt it-sikkerhedsniveau, såvel som guide kunder, aftagere og forbrugere til at vælge de virksomheder, der har styr på it-sikkerhed og dataanvendelse.

Mærket kan samtidig hjælpe virksomhederne på vej mod ansvarlig dataanvendelse samt skabe gennemsigtighed om it-sikkerhed og dataanvendelse

i virksomhederne og dermed i fremtiden blive en konkurrencefordel.

Mærkets indhold, organisation, pris og certificeringsproces mv. fastlægges senere i samarbejde med relevante parter. Virksomhedsrådet anser det dog som vigtigt, at medarbejder-awareness inkluderes i mærkets krav. Andre indholdskrav kunne være back-up eller løbende opdatering.

Et frivilligt mærke målrettet SMV'er

Mærket skal være *frivilligt*, så der ikke stilles unødige krav til virksomheder, der allerede er langt med it-sikkerhedsarbejdet. Dermed målrettes mærket de danske virksomheder – særligt blandt SMV'erne – der ikke arbejder med it-sikkerhed, eller dem, som søger en mere struktureret tilgang til it-sikkerhedsarbejdet. Mærkets indholdskrav skal derfor balanceres, så det ikke bliver for omfattende og omkostningstungt at implementere og opnå, men så det samtidig fører til en betydelig reduktion i virksomhedernes risiko. Administrative byrder i forbindelse med mærket skal minimeres.

Et signal til kunder, aftagere, forbrugere og samarbejdspartnere

Med mærket kan virksomhederne signalere til kunder, aftagere, forbrugere og samarbejdspartnere, at de har forholdt sig til it-sikkerhed og ansvarlig dataanvendelse. På den måde kan mærket, i tillæg til at hjælpe virksomhederne på vej med it-sikkerhedsarbejde, være efterspørgselsdrevet og blive en indgang til og ramme for dialogen om it-sikkerhed, for eksempel mellem virksomheder og deres leverandører. Og dermed også på sigt blive et konkurrenceparameter.

En kickstarter til arbejdet med it-sikkerhed

Mærket skal sikre, at virksomhederne bliver fortrolige med grundlæggende terminologi og metodik inden for it-sikkerhed. Det gør det lettere senere hen at arbejde videre mod endnu bedre it-sikkerhed, for eksempel i form af mere omfattende standarder og certificeringer. Det kan således bidrage til at sænke kognitive barrierer i forhold til it-sikkerhed, og opbygge virksomhedernes tro på, at området er til at gå til. Mærket skal således være en lettere måde at gøre det nødvendige på.

Et første skridt mod efterlevelse af leverandørkrav om datasikkerhed

Med GDPR-lovgivningens indførelse har virksomheder fået pligt til at risikovurdere sine partnere og leverandører, når der indgår persondata i en aftale. Et mærke for it-sikkerhed kan hjælpe virksomhederne med at tage et skridt i den rigtige retning, når de skal efterleve andre virksomheders krav om datasikkerhed hos deres leverandører. Det vil i praksis reducere risikoen for, at mindre virksomheder uden styr på it-sikkerheden, fravælges som leverandører til større virksomheder. Et løft af it-sikkerhedsniveauet kan også hjælpe virksomhederne på vej med de generelle sikkerhedskrav i GDPR.

Et løft af Danmarks it-sikkerhed

Endelig vil et løft af SMV'ernes it-sikkerhed styrke det danske samfunds generelle modstand mod kritiske it-sikkerhedshændelser, idet SMV'erne leverer produkter og ydelser til de samfundskritiske sektorer, store virksomheder og myndigheder. Hvis det lykkes for en stor del af SMV'erne at løfte deres it-sikkerhedsniveau, er Danmark derfor kommet langt i kampen mod it-kriminelle.

Konstruktion:

Et bredt funderet mærke samtænkt med andre tiltag og ordninger

For at sikre, at en mærkningsordning giver reelle resultater for erhvervslivet, anbefaler Virksomhedsrådet, at mærkets konstruktion og indhold udvikles i samarbejde med relevante parter, herunder myndigheder, brancheorganisationer, Industriens Fond og Dansk Standard. Det skal blandt andet gøre mærket relevant for virksomhederne, og skabe en relation til andre initiativer såsom sikkerdigital.dk og sikkerhedstjekket.dk.

En sådan samtænkning skal sikre, at it-sikkerhed og ansvarlig dataanvendelse bliver enkelt og nemt for virksomhederne at forholde sig til. Det skal også sikre, at der er en naturlig overgang fra simple råd og vejledninger over et it-sikkerhedsmærke og til de mere omfattende internationale standarder og rammeværker.

Figur 1

Kompleksitet i it-sikkerhedsarbejdsformer ift. en virksomheds modenhed

Det er altså vigtigt, at mærket etableres i relation til eksisterende arbejdsformer som sikkerhedstjekket.dk, ISO27001 og NIST-rammeværket, som vist på figur 1 herover. Figuren illustrerer, at jo mere moden og fortrolig en virksomhed bliver med it-sikkerhedsarbejdet, jo mere komplekse arbejdsformer og redskaber kan den tage i brug. Det kan også ses, hvordan et nyt it-sikkerhedsmærke kan udfylde gabet i kompleksitet mellem sikkerhedstjekket.dk og ISO27001.

Mærket kan desuden udvikles med inspiration fra lignende, internationale mærkningsordninger, såsom det britiske Cyber Essentials, der er beskrevet herunder.

Case: Cyber Essentials

Cyber Essentials er et britisk mærke for it-sikkerhed, der skal beskytte virksomheder mod de mest almindelige cyberangreb. Mærkningsordningen har to niveauer: »Cyber Essentials« og »Cyber Essentials Plus«. Der var i 2017 udstedt mere end 9000 mærker.

Med mærket signalerer virksomheden til kunder, at den arbejder med at sikre sin it og data samtidig med, at virksomheden får opbygget et tillidsbaseret forhold til en it-leverandør. Nogle lokale og nationale myndigheder kræver, at virksomheder skal have mærket, hvis de skal indgå kontrakter med det offentlige. Virksomheder, der har opnået mærket, kan søges frem på en database på Cyber Essentials hjemmeside.

Mærket stiller krav om, at alle enheder og al software i virksomhedens it-infrastruktur skal leve op til fem tekniske krav:

1. Brug af firewall
2. Brug af de mest sikre indstillinger
3. Kontrol af brugeradgang til data og enheder
4. Beskyttelse mod virus og andet malware
5. Løbende opdatering af enheder og software

Et »Cyber Essentials«-mærke koster ca. £300 for en virksomhed, mens »Cyber Essentials Plus«-mærket koster ca. £1300.

Kilde: https://www.cyberessentials.ncsc.gov.uk

Medlemmer af Virksomhedsrådet for IT-sikkerhed

Tom Engly (formand)
koncernsikkerhedschef, Tryg

Ann Harkjær Frederiksen
Økonomichef, Svend Frederiksen Maskinfabrik A/S

Annette Falberg
Branchedirektør, DI Handel

Benjamin Nordentoft Vejgaard
Områdedirektør, Security Services, KMD

Charlotte Pedersen
Director, PwC

Claus Bak Petersen
CEO, Auditdata A/S

Henning Mortensen
CISO/CPO, Brødrene A&O Johansen A/S

Ingrid Colding-Jørgensen
Director, Global Information Security Management, Novo Nordisk

Jacob Herbst
CTO, Dubex

Lars Ramkilde Knudsen
Professor, DTU Compute og Dencrypt

Max Gersvang Sørensen
Advokat, LIGA Advokatpartnerselskab

Merete Søby
Managing Director, Hitachi Vantara

Michael Busk-Jepsen
Digitaliseringsdirektør, Finans Danmark

Rasmus Theede
CEO, Sparkle Security