DANSK ERHVERV
Børsen
1217 København K

www.danskerhverv.dk
info@danskerhverv.dk
T. + 45 3374 6000

Erhvervsstyrelsen

Til: Winn Nielsen; winnie@erst.dk

Cc. Center for Cybersikkerhed; lartho@cfcs.dk

Den 17. februar 2020

Svar på høring om indhentning af forslag til indsatser i det kommende EU-program for cybersikkerhedscertificering

Dansk Erhverv har modtaget høring om indhentning af forslag til indsatser i det kommende EU-program for cybersikkerhedscertificering og har følgende kommentarer.

Generelle bemærkninger

Dansk Erhverv hilser EUs øgede fokus på it-sikkerhed velkomment, lige som vi tidligere har bakket op om Kommissionen forslag om at et frivilligt certificeringssystem i EU.

Større tillid til de digitale produkter på markedet er en afgørende forudsætning for fortsat forretningsudvikling og økonomisk vækst. De seneste års store it-sikkerhedshændelser, som har ramt både større og mindre virksomheder, samt de mange datalæk hvor mange privatpersoners data er blevet offentliggjort, har vist, at der er behov for et løft af it-sikkerheden på tværs af samfundet. Derfor er EU's cybersikkerhedscertificering et velkomment og nødvendigt tiltag, som kan bidrage til, at virksomheder og borgere får bedre mulighed for at beskytte sig mod it-kriminalitet.

Generelt vil det være centralt, at en fælleseuropæiske certificering understøtter allerede igangsatte aktiviteter i de europæiske lande. I Danmark har Dansk Erhverv m.fl. taget initiativ til en mærkningsordning for it-sikkerhed til virksomheder, og flere andre europæiske lande har udviklet en række nationale tiltag. Det er centralt, at en fælleseuropæisk cybercertificering ikke underminerer de nationale indsatser.

Sikkerheden i teleinfrastrukturen er en topprioritet for teleselskaberne, så uafhængige sikkerhedstest af komponenter, der indgår i teleinfrastrukturen, hilses velkommen.

Det synes helt naturligt, at der på EU-niveau sættes en standard for hvad og hvordan, der skal testes. For mindre lande som Danmark synes det dog ikke optimalt, både ud fra et økonomisk og kompetencespørgsmål, at test nødvendigvis skal ske nationalt – det synes mere naturligt, at der i EU er få testcentre, hvor kompetencerne bedre kan vedligeholdes. Fastholdes det, at test kan/skal ske nationalt, bør der etableres et samarbejde mellem test-faciliteterne for at sikre en optimal udnyttelse af ressourcer og kompetencer.

Teleindustrien har som udgangspunkt et ønske om at behandle alle leverandører ens og vælge produkter ud fra sikkerhed, teknologi og økonomi – for at skabe de bedste produkter for samfund og kunder. Som følge heraf bør det defineres hvilke typer af udstyr, der skal testes, uafhængig af leverandør og oprindelse – herved kan teleselskaberne afgøre hvilke yderligere risici der skal mitigeres.

Specifikke bemærkninger
Mht. specifikke bemærkninger har Dansk Erhverv følgende:

Product lifecycle
Netkomponenter i teleinfrastrukturen har typisk en lang levetid, så "Product lifecycle" er vigtig at medtage uafhængigt af produktområde. Det må antages at procestiden i certificeringsprogrammet (Common Criteria-baseret) kan være længerevarende, så det er vigtigt at finde en metode for implementering af udstyr, der endnu ikke er certificeret, så den teknologiske udvikling ikke begrænses unødigt.

Internet of Things (IoT)
Internetforbudne apparater findes alle vegne både i virksomheder og i private hjem og vinder stadig større udbredelse. De åbner mulighed for nye og smartere produkter og tjenester, som rummer ikke mindst store potentialer for den grønne dagsorden. Det er dog tale om et broget og umodent marked, hvor der indimellem er store udfordringer med sikkerheden. Det gælder fx produkter, som ikke kan sikkerhedsopdateres, eller som efter en kort periode ikke længere supporteres af producenten, eller som er udstyret med et *default passwords* m.v., som gør dem sårbare. Konsekvensen kan være at kriminelle misbruger teknologien til at få adgang til et netværk, ligesom inficerede IoT-enheder kan indlemmes i *botnets* og bruges til at udføre DDoS-angreb.

Derfor er IoT et oplagt område at give et sikkerhedsmæssigt løft, og som et certificeringsparadigme bør dække. Dansk Erhverv ser gerne, at producenter der bruger ressourcer på it-sikkerhed og står bag deres produkter og tjenester opnår en konkurrencefordel på markedet ved at dokumentere at man efterlever nogle kriterier for it-sikkerhed. En certificering kan på den måde være med til at flytte markedsandele.

Security by Design (SbD)
SbD – og hertil kan tilføjes *Security by Default* – bør være standard i alle digitale produkter. Her er det dog nødvendigt at en certificering stiller eventuelle krav på en måde, som gør dem forenelige med innovation og udvikling i it-branchen.

Andet
Et område, som ikke er nævnt specifikt i høringsbrevet, men som Dansk Erhverv mener er helt centralt er hensynet til køberen af fx et IoT-produkter dvs. både erhvervs- og privatkunder. En certificering vil kun have den ønskede effekt, hvis det er muligt for både privat- og erhvervskunder at gennemskue 1) et produkts sikkerhedsniveau, og 2) hvordan det niveau passer ift. den konkrete risiko, som følger af produktets anvendelseskontekst.

F.eks. vil det være naturligt at stille større sikkerhedskrav i IoT-produkter, som bruges i brancher, der er udsat for en høj grad af industrispionage, end det vil være for fx

Videre vil det være nødvendigt at afklare, om certificeringen kun skal dække et minimumsniveau af sikkerhed, som alle produkter og services indenfor en given kategori skal leve på til, eller om der vil være tale om en certificering med flere niveauer.

Med venlig hilsen

Christian von Stamm Jonasson