Titel	Cybersikkerhed i produkter
GTS-institut	DELTA
Kontaktperson	Christian Skytt, +45 72 19 44 23, csk@delta.dk

0. Sammenfatning

I 2020 forventes det, at ca. 50 milliarder produkter er forbundne til internettet. De store fordele i at forbinde produkter online medfører dog tilsvarende en sårbarhed overfor potentielt misbrug. Da produkter i dag kan tilgås og distribueres over hele verden, skabes der i globaliseringens navn en sikkerhedsrisiko for såvel producenten, forbrugeren og potentielt for nationer. DELTA vil udvikle og tilbyde services, som assisterer udviklere og sikrer, at produkter lever op til gældende sikkerhedsstandarder.

1. Markeds- og samfundsbehov

I dag taler vi om sikkerhed på hjemmesider, overtagelse af Pc'er/mobiltelefoner og uhindret adgang til data i større systemer. Men hvad sker der, når 50 milliarder produkter er sluttet til internettet i 2020? Det skønnes allerede i dag, at 70 % af alle elektriske apparater er styret via software/services[1] samtidig med, at 80 % af den digitale infrastruktur er privatejet[2]. Truslen mod spionage, hacking, terror og fjendtlig overtagelse af apparater og infrastruktur bliver endnu mere reel i takt med, at flere enheder bliver koblet til cyberspace – og dermed adgang til at gøre fysisk skade på mennesker og samfund. Misbrugte eller forkert sensordata kan skabes ikke bare via hacking, men ved fysisk sabotage, som kan give uoverskuelige konsekvenser i sikkerhedskritiske anvendelser.

Tidligere var det kun blandt fagfolk, at sikkerhed havde betydning. Nu er relevansen nået helt ud til forbrugerne i dagligdagen fx fjernsyn, som overvåger samtaler[3], via sundhedsudstyr[4] og i biler[5], som alle kommer på nettet og kan overtages. Samtidigt optager det i stigende grad industrien[6], hvor truslen er erkendt og stigende[7]. Hvis ikke produkter (og infrastruktur) er robuste mod misbrug, kan det have vitale følger for den daglige drift, men også deres markeds tillid. Markedet begynder at efterspørge/stille krav om sikkerhed i produktet[8], men det forventes, at der over en 2-5 årig periode også bliver stillet krav til cybersikkerhed i produktet. (Konkret ONS/FDA, EU Direktiv, NATO, Digitaliseringsstyrelsen, nyt 27001 direktiv).

Det vil i særdeleshed være den produktudviklende del af dansk industri, som er målgruppe for aktiviteten. Primært virksomheder, som allerede eller i perioden sætter deres produkter på internettet. Dernæst de relaterede aktører hertil, fx dem som leverer netværks- og IT-løsninger, systemdesignere og SW udviklere, som er i berøring med såvel infrastruktur og produkter, fx energisektoren og andre store infrastrukturer, som gøres intelligente. Industrifokus vil især rettes mod særligt sikkerhedskritiske produktkategorier, fx medico, energi, forsyning, infrastruktur, militær/space, automotive.

I Danmark er der stort fokus på, at infrastruktur og IT-løsninger skal være sikre. Men der findes kun få løsninger og viden omkring, hvordan udviklingen af produkter gøres sikre. Det er her DELTA kan udvikle den teknologiske service igennem udvikling, formidling og opbygning af rådgivnings/test ydelser, som kan hjælpe virksomheder med at udvikle produkter, der lever op til internationale krav om øget sikkerhed. De færreste virksomheder har interne ressourcer til at kunne løfte en så videntung opgave, og særligt for SMV-segmentet er denne opgave uoverskuelig.

[1] Kilde: Præsentationer fra FE og industrimøder
[2] Hollands NSCC Elly van den Heuvel.
[3] http://www.b.dk/nationalt/smart-tv-overvaager-dine-samtaler
[4] http://www.informationweek.com/healthcare/security-and-privacy/hackers-outsmart-pacemakers-fitbits-worried-yet/d/d-id/1113000
[5] http://www.computerworld.dk/art/233077/bmw-efter-sikkerhedshul-derfor-kunne-2-2-millioner-biler-hackes
[6] http://www.version2.dk/artikel/nsa-aflytninger-i-tyskland-tvang-it-ivaerksaettere-til-traeffe-dyr-beslutning-86199
[7] http://www.business.dk/digital/nsas-spionprogrammer-gemt-dybt-nede-paa-de-fleste-harddiske
[8] Et eksempel på klare sikkerhedsmæssige krav fra Digitaliseringsstyring (27. nye initiativer), Carsten Møller Jensen

2. Ny teknologisk serviceydelse, kompetence og teknologi

I samarbejde med videnpartnere og industrien vil der efter aktivitetsperioden kunne udbydes følgende eksempler på teknologiske services:

- Rådgivning om enklere/værdiskabende implementering af ISO 27001 i mindre og umodne virksomheder.
- Rådgivning om best practice for udvikling af sikre elektronikprodukter (cybersikkerhed, privacy, datasikkerhed, hacking).
- Efteruddannelse af virksomheder i forhold til Cybersikkerhed i produkter.
- Etablering af Nordisk Screening Center for Produktcybersikkerhed for udveksling af viden og best practice.
- Udbud af anerkendt sikkerhedstjek i samarbejde med Digitaliseringsstyrelsen.
- Udbud af risiko assesments.
- Rådgivning om nationale og internationale standarder for sikkerhed.
- Service for "Extreme Product Hacking" – netværk af antihackere, som kan finde produktets svage sider.

Lignende ydelser findes på IT-området, men eksisterer i dag ikke i Danmark på produktsiden, bl.a. da der endnu ikke er fuldt udviklede standarder. Forankringen i GTS-nettet vil være medvirkende til at sikre en national og uvildig tilstedeværelse af viden og services. Netop emnet taget i betragtning, er der brug for fortrolighed, neutralitet og uafhængighed for at have dialogen med virksomheder, da det kan have vital betydning for virksomhedens tillid i markedet og konkurrenceevne, hvis det rygtes, at de er svage på cybersikkerhed.

Videnmedarbejdere med sikkerhedskompetence er en mangelvare. DTU[9] uddanner i dag 20 nye dimittender om året – og totalt set 40-100 på landsplan. Disse bliver opslugt af myndigheder, større virksomheder og internationale konsulentvirksomheder. Det er ikke nok til, at mindre danske virksomheder kan få adgang til viden på en økonomisk tilgængelig måde og dermed en barriere for vækst og innovation.

3. Centrale aktiviteter

For at etablere dette serviceudbud skal der gennemføres følgende centrale elementer af videnopbygning, -hjemtagning og –formidling:

- Deltage i lovgivning og standardisering, hvoraf der skabes viden om implementérbare sikkerhedslovgivninger.
- Etablering af lokalt testcenter for cybersikkerhed i produkter (i samarbejde med EU's Research C©enter i Milano og ENISA).
- Formidle viden og kompetencer i samarbejde med Center for Dansk Cybersikkerhed (fokus på avancerede cybersikkerhedsudfordringer).
- Implementering af sikkerhedsprocesser i produktudvikling igennem testforløb for at skabe demonstrationscases for mindre virksomheder.
- Formidle, påvirke og nationalt samarbejde omkring åbne standarder for sikkerhed i forhold til Nationale, NATO og EU direktiver på vej.
- Etablering af National Council a la hollandsk model på tværs af produktudviklere, universiteter og myndigheder.
- Implementere ny viden i uddannelsesforløb på både universiteter og tekniske skoler, da der i dag er for få uddannede med kompetencer inden for cybersikkerhed.

4. Mulige samarbejdspartnere

- Offentlige sikkerhedstjenester fx FE, PET, Center for Cybersikkerhed og Digitaliseringsstyrelsen er centrale for de krav, som i fremtiden vil blive stillet.
- Branche og interesseorganisationer fx DI ITEK, Dansk Erhverv, Atlantsammenslutningen og Innovationsnetværket CFIR er centrale samarbejdspartnere for at nå ud til industrien og afdække behov og problemstillinger.

[9] DTU Compute

- Myndigheder fx Erhvervsstyrelsen, Sikkerhedsstyrelsen og andre vil skulle implementere krav og blive mødt med behov fra industrien.
- Internationale sikkerhedsorganisationer, fx FDA, EU's Research Center i Milano vil være vigtige for videnhjemtagning.
- Rådgivende og andre virksomheder som beskæftiger sig med sikkerhed: fx COPITS, Siscon vil være sparringspartnere i udvikling af sammenhængende rådgivningsydelser.
- Uddannelsesinstitutioner, fx DTU Compute, SDU og Forsvarsakademiet har forskningsaktiviteter på dette felt.

DELTA, Venlighedsvej 4, 2970 Hørsholm, Danmark. Tlf. +45 72 19 40 00, www.delta.dk