Internet of Things må ikke blive til Internet of Insecure Things

by Anika Lüdeke Dueholm - tirsdag, april 05, 2016

http://perspektiv.tdc.dk/internet-of-things-maa-ikke-blive-til-internet-of-insecure-things/

Internet of Things må ikke blive til Internet of Insecure Things

Internet of Things inviterer så meget til innovation og forretningsudvikling, at sikkerhedshensyn risikerer at blive skubbet i baggrunden – eller helt glemt – når man udvikler sine løsninger. Det må ikke ske, siger TDC-ekspert og forklarer her, hvilke to nøgleopgaver man som sikkerhedsansvarlig skal fokusere på.

Det kan være fristende at lukke øjnene og tage et hovedspring ud i de mange forretningsmuligheder, der byder sig til i den nye IoT-virkelighed. For der er stort set ingen grænser for, i hvilket antal og hvorhenne man kan koble sensorer på enheder, mennesker og maskiner og derigennem opnå ny indsigt.

Men netop fordi Internet of Things ofte bevæger sig på ubetrådt grund, rejser det en række fundamentale it-sikkerhedsspørgsmål. Svarene på de spørgsmål skal ligge indlejret i en virksomhed eller organisations IoT-løsninger, *før* løsningerne går i luften. Ellers risikerer man at komme på kant med loven.

Nye enheder, nye risici

Den opfordring kommer Brian Krogh Jensen med. Han er afdelingschef i Enterprise Architects, Solution Sales i TDC Erhverv.

“Analysehuset Gartners seneste forudsigelse lød på, at der ville være 6.4 milliarder aktive forbundne enheder i 2016. I 2020 estimerer Gartner, at samme tal hedder 20.8 milliarder aktive enheder. Tallene fortæller, at markedet i disse år bliver oversvømmet af nye internetforbundne enheder.”

“I sig selv er det en enorm interessant udvikling. Vi kan slet ikke begribe det fulde potentiale i den nye IoT-virkelighed endnu. Men – og det er et stort men – med så mange nye spillere på markedet med så mange nye produkter vil det også øge risikoen for sikkerhedsbrud,” siger Brian Krogh Jensen.

Fra gummidæk til sikkerhedspatching

Sikkerhed og Internet of Things er mange ting. Det er blandt andet privacy-hensyn og beskyttelsen af virksomheds- eller personfølsomme informationer. Det er dataintegritet og beskyttelsen mod datamanipulation. Og så er det den mere traditionelle beskyttelse mod hackere og andre ubudne gæster.

> Hvis man som virksomhed har været vant til at producere gummidæk, termovinduer eller græsslåmaskiner, så tænker man ikke nødvendigvis i disse baner, når man designer og fremstiller sit produkt

“Hvis man som virksomhed har været vant til at producere gummidæk, termovinduer eller græsslåmaskiner, så tænker man ikke nødvendigvis i disse baner, når man designer og fremstiller sit produkt. Og man har heller ikke nødvendigvis det rette mandskab til at håndtere eksempelvis opdatering af firmware, patching og generel netværkssikkerhed,” siger Brian Krogh Jensen.

Lige så mange muligheder Internet of Things tilbyder, lige så mange sikkerhedsovervejelser følger der med. Den virkelighed vil være ny for mange, der pludselig bliver en lille del af en stor IoT-økonomi.

Hacking af en bilvask

Sikkerhedsfirmaet Kaspersky Lab har allerede givet eksempler på, at umiddelbart harmløse IoT-løsninger kan hackes og dermed misbruges. Kaspersky Lab har blandt andet vist, at det kan lade sig gøre at hacke en bilvask, et politiovervågningssystem og et fitnessarmbånd.

Og hvad kan man så bruge det til? Jo, man kan eksempelvis manipulere maskinerne i bilvasken, så de ødelægger bilerne i stedet for at rengøre dem. Man kan koble sig op på politiets videoovervågningssystem og forurette stor skade – eller bare kigge med i det skjulte. Og man kan bruge menneskers fitness-armbånd til at bekræfte deres geografiske position i realtid.

I 2013 meldte sikkerhedsfirmaet Proofpoint, at de havde opdaget det første IoT-botnet. Ifølge Proofpoint bestod mere end 25 pct. af botnettet af Smart TV’s, babyalarmer og andre husholdningsenheder.

To fokuspunkter

Som virksomhed eller organisation er der særligt to hensyn, man skal tage stilling til, når man designer IoT-løsninger, siger Brian Krogh Jensen.

“For det første skal man stille krav til de IoT-komponenter, der skal indgå i løsningen. Der bliver produceret sensorer og netværksudstyr meget billigt og i meget varierende kvalitet rundt omkring i verden. Det er virksomhedens ansvar, at komponenterne lever op til nogle basale sikkerhedskrav.”

> Man må aldrig slække på sikkerheden i jagten på forretningsgevinster. Heller ikke selvom alt er nyt og spændende i IoT.

“Når man har de ønskede komponenter og skal strikke sin specifikke løsning sammen, skal man for det andet lægge sikkerhedskrav ned over løsningen i forhold til dataprotokoller, dataintegritet og privacy-hensyn. Løsningen skal med andre ord drives forsvarligt,” siger Brian Krogh Jensen.