Digital

VEJLEDNING

Sikkerhed i Internet of Things

DI Digital
1787 København V.
3377 3377
digital.di.dk
digital@di.dk

DI Digital – et branchefællesskab i Dansk Industri for virksomheder inden for it, tele, elektronik og kommunikation

Udgivet af: DI Digital

Redaktion: Henning Mortensen

ISBN: 978-87-7144-066-9

0.011.15

Digital

VEJLEDNING

Sikkerhed i Internet of Things

BAGGRUND

Internet of Things er opkobling til internettet af fysiske ting, som har fået indbygget computere, der gør tingene intelligente. Når der indbygges computere i ting, får disse ting en helt ny værdi for brugerne og virksomhederne.

Tingene kan f.eks. fjernstyres eller afgive data, som brugerne kan tage beslutninger på baggrund af. Tingene kan også i nogle sammenhænge styre sig selv på helt nye måder uden menneskelig interaktion. De helt store gevinster opnår man, når tingene kan tale sammen og understøtte hinanden.

For virksomheder er der også mange gevinster ved Internet of Things. For det første kan et produkt erobre markedsandele ved at blive videreudviklet med ny teknologi. For det andet kan der opbygges helt nye forretningsmodeller i form af services ovenpå selve produktet. For det tredje opsamles der typisk en lang række data fra de intelligente produkter. Disse data kan bruges til dels at give en bedre service - f.eks. i samspil med andre data - eller til at videreudvikle produktet yderligere.

Det er vigtigt, at danske virksomheder innoverer deres produkter med ny teknologi, således at danske produkter kan fastholde og udbygge deres markedsposition. Hermed bidrager man til økonomiske gevinster for virksomhederne og vækst og arbejdspladser i det danske samfund. Faktisk er det en risiko for danske virksomheders overlevelse, hvis de ikke løbende følger den teknologiske udvikling og innoverer deres produkter med ny teknologi.

Når tingene gøres intelligente og kobles på internettet opstår der ikke blot muligheder, men også helt nye risici. Det er derfor vigtigt at have fokus på sikkerheden, når man gør sine produkter intelligente. Der findes en lang række tilfælde eller demonstrationer af uretmæssig kontrol med Smart TV, Netværksdiske, SmartPhones, insulinpumper, pacemakere, biometriske låse, elmålere, biler og intelligente produktionssystemer. Der er dermed en risiko for, at det, der skulle være godt for brugerne og virksomhederne, kan blive rigtig skidt for begge parter, hvis sikkerheden ikke er designet rigtigt med ind i det intelligente produkt.

Denne vejledning giver en række gode sikkerhedsråd, som de produktansvarlige i virksomhederne bør tage med i deres overvejelser, når der indbygges intelligens i produkterne. I vejledningens bilag 1, findes desuden en lille intuitiv risikovurdering, som den sikkerhedsansvarlige og den produktansvarlige i samarbejde kan anvende for på overordnet plan at fastslå, hvor vigtigt det er at inddrage anbefalin-

gerne fra denne vejledning i deres arbejde. Det er ultimativt virksomhedens direktion, der har ansvaret for, at virksomhedens produkter har det fornødne sikkerhedsniveau. I vejledningens bilag 2 findes derfor en liste af råd, som virksomhedens direktion bør forholde sig til. Det er tanken, at den produktansvarlige kan forelægge listen for sin direktion.

PROCESSER TIL AT HÅNDTERE SIKKERHED

Producenter af intelligente produkter skal have processer på plads, som håndterer sikkerheden i produkterne og de mobile apps og backend databaser, som produkterne kommunikerer med.

Generelt er det vigtigt, at producenten har processer på plads til at håndtere alle aspekter af deres informationssikkerhed. Man kan tage udgangspunkt i en sikkerhedsstandard som f.eks. ISO27001, der adresserer det administrative it-miljø og NIST 800-82, som adresserer produktionsmiljøet. Der findes ikke en samlet standard til at håndtere produkters informationssikkerhed - givetvis fordi produkter er meget forskellige.

Mange af de procedurer, som skitseres i de ovenfor nævnte standarder, kan imidlertid overføres på produkters informationssikkerhed. Det gælder f.eks. risikovurdering, dataklassifikation, adgangskontrol, penetrationstests og opdateringsrutiner. Disse standarder er kendte af virksomhedens sikkerhedsfolk. Det vil derfor være naturligt at inddrage den sikkerhedsansvarlige i sikkerhedsarbejdet med produkter.

RISIKOVURDERING

Producenterne skal foretage en risikovurdering af de mulige trusler, de kan stå overfor, når de gør deres produkter intelligente.

Først og fremmest skal man vurdere, hvilke konsekvenser det kan have, hvis et produkt kompromitteres. Vurderingen skal gå på selve produktet, men også på de øvrige elementer der indgår i produktet - f.eks. inklusive kommunikation af datastrømme til produktet fra mobile apps eller opdateringsservere og fra produktet til backend databaser hos producenten selv eller hos tredjeparter.

Herefter skal man vurdere, hvilke trusler produktet og de afledte systemer står overfor. For at få en inspiration til at vurdere truslerne kan der henvises til OCTAVE-terminologien for trusler, som omfatter menneskelige trusler, systemmæssige trusler og trusler udenfor virksomhedens kontrol[1]. For hver trussel skal man desuden estimere sandsynligheden for, at den opstår.

Endelig skal man identificere de sikkerhedstiltag, man har iværksat, som skulle kunne imødegå de identificerede trusler og konsekvenser.

---

[1] DI har gennemgået i sikkerhedsvejledningen, Trusler mod virksomhedens it-sikkerhed, http://di.dk/Virksomhed/Produktion/IT/itsikkerhed/Sikkerhedformindrevirksomheder/Pages/Truslermodvirksomhedensit-sikkerhed.aspx.

Man står herefter tilbage med et risikobillede af produktet. Det er en forretningsmæssig vurdering, hvilke sikkerhedstiltag der skal afsættes ressource til at iværksætte, for man kan aldrig nå fuldstændig sikkerhed. Ledelsen skal acceptere de mulige konsekvenserne for risici, man ikke har adresseret.

Der findes i ISO27015 en udmærket gennemgang af, hvordan man laver risikovurderinger.

Det er også centralt, at risikovurderingen ikke bliver for snæver. I en række sammenhænge er der fysiske konsekvenser af modifikationer - tilsigtede end ondsindede - af intelligente it-systemer. Der er risiko for, at modifikationerne f.eks. kan resultere i, at produktionsmaskiner kører, mens der er personale på dem, som så kan komme til skade, eller at der sker overspænding i installationerne med skade for servicepersonale til følge. Ligeledes kan modifikationerne resultere i skade på trafikanter eller personer med indopererede intelligente apparater. Denne trussel bliver mere markant, hvor der foretages fjernadgang til systemerne, og hvor den, der håndterer disse, dermed ikke har kontrol med det fysiske miljø. For at undgå at risikovurderingerne bliver for snævre, kan det overvejes, om der skal laves flere risikovurderinger, således at ovenstående forhold også bliver opfanget.

For at kunne CE-mærke sit produkt vil der normalt være krav om, at der laves en skriftlig risikovurdering i forhold til sikkerhed for personer/husdyr/værdier. Det er uden for denne vejlednings fokus, og er derfor ikke medtaget her.

DATAKLASSIFIKATION

Producenter af intelligente produkter bør vurdere, om der behandles data - og i givet fald hvilke data - i produktet. Data bør klassificeres efter deres følsomhed.

Data, der ved første øjekast kan virke uskyldige - f.eks. dagligt forbrug af strøm - kan vise sig at være følsomme - f.eks. fordi et fald i brugen af strøm kan indikere, at man er på ferie, og at hjemmet står tomt. Klassifikationen bør tage udgangspunkt i, hvilke skade der kan ske for ejeren af produktet og producenten ved at data eksponeres. I statsministeriets sikkerhedscirkulære[2] er der defineret fire niveauer, men mindre kan også gøre det.

Data kan også vurderes ud fra, hvem der skal have adgang til data og bruge dem i de videre processer. Nogle data skal brugerne have adgang til, andre skal producenter have adgang til (f.eks. data om vedligehold og tilstand), og andre skal måske videregives til tredjeparter (f.eks. forbrug aflæst af måler).

Centralt i denne forbindelse er det også at vurdere, hvor data skal placeres. I nogen sammenhænge vil data ligge bedst i produktet og blive aflæst lokalt. I andre tilfælde vil det være hensigtsmæssigt at lægge data op på en central server, så de kan bruges til service af forskellig art.

[2] Statsministeriets sikkerhedscirkulære: https://www.retsinformation.dk/Forms/R0710.aspx?id=20965.

Såfremt nogle af de data, der behandles, kan anses for at være personoplysninger, skal man være opmærksom på lovkrav, jvf. nedenfor.

PRIVACY

Personoplysninger skal beskyttes i henhold til lovgivningen, og producenter af intelligente produkter kan desuden med fordel vurdere, hvordan de opnår tillid hos brugerne, når produkterne opsamler personoplysninger (hvad enten de lagres eller ej, og hvad enten den lagring i så fald sker i produktet eller sker udenfor produktet f.eks. på centrale servere).

Beskyttelse af personoplysninger er indenfor EU reguleret i Lov om behandling af personoplysninger, som stammer fra EU direktivet 95/46/EF. Reglerne er under forandring, og det forventes, at ny lovgivning kommer på plads primo 2016 med virkning fra 2018. Manglende opfyldelse af denne lovgivning, vil kunne medføre meget store bøder.

Lovgivningen påpeger bl.a., at det skal præciseres, hvem der har ansvar for, at personoplysninger behandles (dataansvarlig), og hvem der eventuelt behandler dem på den dataansvarliges vegne (databehandler). Data må kun anvendes til på forhånd definerede formål, og man må kun indsamle de oplysninger, man har brug for. Data skal være præcise, og den, data vedrører (datasubjektet), skal i de fleste sammenhænge gives adgang til data og have mulighed for at få dem rettet. Der skal indhentes samtykke for behandlingen af data fra datasubjektet. Yderligere er der en række følsomme data, som slet ikke må behandles af private. Der er krav til, at data skal behandles sikkert. Desuden er der regler for videregivelse til tredjeparter. Endelig skal data slettes, når der ikke længere er brug for dem. Hvis producenten er dataansvarlig, er det producenten, der har ansvaret for, at reglerne efterleves.

Udenfor EU gælder andre nationale regler. Selv om nogle af de principper, der gør sig gældende i Europa, også gælder andre steder i verden, er det relevant at sikre sig, at man ikke overtræder national lovgivning ved behandling af personoplysninger. Et af de forhold, man især kan være opmærksom på, er, at der i en række lande gælder, at personoplysningerne ikke må forlade landet eller skal forblive i landet i kopi (forced data localization). Et andet forhold, man skal være opmærksom på, er, i hvilket omfang national lovgivning kan gøre, at direktøren bliver gjort personlig ansvarlig for efterlevelse af regler om beskyttelse af personoplysninger.

Jo tidligere det vurderes, om et planlagt design af et intelligent produkt kan efterleve lovens krav jo bedre. Opfyldelse af lovgivningen er obligatorisk, men ofte kan det være nyttigt at se på behandling af personoplysninger fra datasubjektets synspunkt. Har virksomheden håndteret dette fornuftigt, vil brugernes tillid til løsningen forøges.

En metode, til at vurdere om et produkt har en fornuftig beskyttelse af persondata, er ved at gennemløbe en privacy impact assessment, PIA. En PIA formulerer en række spørgsmål, som skal besvares på forskellige stadier af udviklingen og implementeringen af it-systemer. En PIA er teknologineutral og kan derfor med fordel bruges i mange forskellige sammenhænge. En PIA bidrager desuden til at skabe overensstemmelse med lovgivningen, men kan sjældent stå alene. Der findes et utal

af PIA-skabeloner, og nogle af dem er meget komplicerede og omfattende. DI har lavet en skabelon, som med fordel kan anvendes[3].

Som et led i en PIA bør producenten gøre sig klart, hvilke data der løber til og fra produktet, hvor de løber hen, og hvem der har adgang til dem til hvilke formål. Dette kaldes en dataflowanalyse. Der findes en skabelon for dataflowanalyse i DI's PIA-vejledning.

DI forventer at udgive en vejledning, som går mere i dybden med behandling af personoplysninger, når den endelige reviderede lovgivning foreligger - formodentlig i 2016.

STANDARDER, MILJØPÅVRIKNINGER OG COMPLIANCE

Der findes en række sektorspecifikke standarder, som virksomhederne indenfor en given sektor skal opfylde. Disse standarder er skrevet for at sikre, at produkter generelt fungerer som tilsigtet i det miljø, som det er meningen, de skal bruges i. I denne sammenhæng vil der dermed med sikkerhed også menes generel forbrugersikkerhed for, at produktet virker som tilsigtet - og altså ikke 'kun' cybersikkerhed. Dette kan f.eks. være for at sikre, at produktets trådløse forbindelse ikke bliver blokeret af anden radiokommunikation, eller at sikre at produktet ikke begynder at fryse og ikke reagerer på tastetryk. Disse standarder er harmoniserede og kan dermed bruges til at demonstrere compliance med de europæiske direktiver, og dermed kan produktet blive CE mærket. Eksempler på sådanne sektor specifikke standarder under f.eks. EMC direktivet er EN 50121-4 for elektronik til signaler for tog eller EN 60601-1-2 for medicoteknisk udstyr. Hvis der derfor laves IoT produkter til disse sektorer, skal disse standarder efterleves for at sikre funktionaliteten og lovligheden af produktet, og det er vigtigt at tage dette i betragtning under udviklingen af softwaren.

Det er dog ikke alle påvirkninger fra miljøet, der bliver fanget af sådanne tests op i mod standarderne. Dette skyldes, at testen kun er lavet, så den fanger de fleste fejl i de fleste miljøer. Derfor er der også udviklet standarder, som definerer metodikker, hvor disse ekstreme påvirkninger kan afdækkes og derved sikre et mere robust produkt. Det er ikke et krav at benytte sådanne standarder, men investeringen gives ofte godt igen i form af besparelser på tilbagekaldelser og reklamationer. Et eksempel på en sådan standard er f.eks. IEC 62506.

IEEE, ETSI, CEN og flere andre standard organisationer har udgivet mange standarder omkring sikkerhed for trådløse protokoller, men det er vigtigt at være opmærksom på, at dette ofte ligger indbygget i teknologien. I relation til cybersikkerhed kan det anbefales at være bekendt med ISO 27005, som adresserer, hvordan risiko kan håndteres af udviklere. Samtidigt kan ISO/IEC TR 13335-4 levere guidelines til, hvordan man styrer IT sikkerhed og vælger safeguards. Det amerikanske institut NIST har udgivet SP 1800, som er en serie om best practise omkring cybersikkerhed.

---

[3] DI's skabelon for Privacy Impact Assessment: http://di.dk/Virksomhed/Produktion/IT/itsikkerhed/personoplysninger/Pages/DIsskabelonforPrivacyImpactAssessment.aspx.

COMMON CRITERIA CERTIFICERING

Virksomheden skal overveje om den ønsker en Common Criteria certificering, som har til formål at demonstrere, at et produkt efterlever nogle på forhånd definerede sikkerhedskriterier.

Certificering er en ganske udbredt måde at demonstrere, at ens produkter efterlever nogle fastlagte kriterier. På sikkerhedsområdet findes der masser af forskellige standarder. Der er dog særlig en standard, som er rettet mod certificering af it-udstyr og it-løsninger og det er Common Criteria (CC), som er en ISO standard (ISO 15408)[4].

Formålet med CC er at verificere, at et produkt er sikkert, fordi det efterlever nogle tekniske sikkerhedsfunktionaliteter. For at sikre dette, må produktet følge visse krav i løbet af sin udvikling, omend der ikke er krav til udviklingsprocessen som sådan. Tilsvarende må produktet kunne give brugeren den fornødne vejledning og den sikkerhedsfunktionalitet, som det lover. Ideen er, at produkter, som kan CC certificeres, har højere sikkerhed (i betydningen: efterlever det de lover) end produkter, der ikke er CC certificeret. CC certificering er primært ment som en måde at kunne sammenligne sikkerhed mellem produkter. På den måde kan man vælge at øge sikkerheden ved kun at efterspørge produkter, der efterlever certificeringen.

Certifikatet udstedes til et konkret produkt eller en konkret løsning. Den internationale gensidige anerkendelse af certifikaterne sker via deltagelse i Common Criteria Recognition Agrement (CCRA), som Danmark har tiltrådt i 2006. Producenten udpeger en Commercial Licensed Evaluation Facility (CLEF), som gennemgår en proces for produktet. Resultatet af denne præsenteres for en certificeringskomite, som så udsteder certifikatet[5].

I praksis forløber processen som følger:

- En producent eller en kunde identificerer et produkt, som man gerne vil certificere. Dette produkt kaldes for Target of Evaluation (TOE).

- Hvis initiativet til at få certificeret et produkt ligger hos kunderne (i bred forstand, f.eks. også staten og standardiseringsorganisationer), opstiller de nogle krav til, hvilken sikkerhed produktet skal efterleve. Disse krav beskrives i en Protection Profile (PP)[6].

- Hvis initiativet til at få certificeret et produkt ligger hos producenten beskriver han de sikkerhedsforanstaltninger, der er indbygget i produktet i et Security Target (ST). Såfremt initiativet kommer fra kunderne, vil det altid være nyttigt for producenten at sikre, at hans ST som minimum indeholder

[4] For en introduktion til CC, se: http://en.wikipedia.org/wiki/Common_Criteria. Den samlede CC kan findes her: http://www.commoncriteriaportal.org/.
[5] http://www.rycombe.com/cc.htm.
[6] Konkrete eksempler på Protection Profiles lavet for den amerikanske regering kan findes her: http://www.niap-ccevs.org/pp/.

de krav, der er fremsat i de mest anvendte PP – ellers kan hans produkt ikke efterleve kundernes krav.

- Indholdet i ST og PP består som oftest af en præcisering af TOE, en beskrivelse af relevante sikkerhedsproblemer/trusler, nogle målsætninger for sikkerheden (der kan være tilknyttet truslerne 1:1) tillige med en beskrivelse af målsætningerne formuleret formelt som:

    4a. Security Functional Requirements (SFRs), som beskriver den sikkerhedsfunktionalitet, der skal ligge i produktet – f.eks. hvem må få adgang til at gøre hvad med produktet. Denne beskrivelse skal være formel i betydningen teknisk og gerne følge tekniske standarder på området.

    4b. Security Assurance Requirements (SARs), som beskriver hvilke tiltag, der skal være taget for at sikre, at produktet faktisk har den sikkerhedsfunktionalitet, som det hævder, at det har. I praksis stiller SAR krav om, at der skal kontrolleres for hvordan produktet er udviklet, hvilken vejledning man kan få til implementering og drift af produktet, tests af produktet, sårbarhedsanalyse af produktet og lifecycle support af produktet.

- Verifikationen af SAR kan foregå med forskellige niveauer af grundighed kaldet Evaluation Assurance Level (EAL). Der findes syv niveauer af dette. Ved at vælge et højere niveau af EAL får man altså ikke et sikrere produkt, men et produkt som, der er bedre sikkerhed for, efterlever det, der er blevet evalueret for. Det er ganske usædvanligt at have kommercielle produkter, som er certificeret på mere end niveau fire. De højeste grader af certificering findes til produkter og løsninger, som har en meget begrænset funktionalitet og anvendelsesområde, eller til virksomheder og organisationer, der har særlig strenge krav til sikkerhed – f.eks. forsvarsindustrien.

CC specificerer ikke selv en detaljeret udviklingsmodel, som skal følges. I stedet angives de generelle sikkerhedskrav, der bør opfyldes. Disse bør opstilles inden udviklingsprocessen påbegyndes, således at man er sikker på at give en rimelig sikkerhedsfunktionalitet, og således at man kan give den funktionalitet, som er efterspurgt af markedet.

Det skal bemærkes, at på det danske marked er efterspørgsel af CC-certificeringer ganske minimal. Det skal også fremhæves, at CC-certificeringer er så specifikke, at de kun gælder konkrete konfigurationer af et produkt. Hvis produktet omkonfigureres, gælder CC-certificeringen ikke nødvendigvis længere. Endelig skal det fremhæves, at CC kan være ganske tungt at arbejde med særligt for mindre og mellemstore virksomheder. Desuagtet er CC-certificeringer et godt bud på at få arbejdet med sikkerheden i sine intelligente produkter – og få demonstreret at sikkerheden er på plads overfor omverdenen.

Foruden CC, som er en generel certificering, findes der også mere snævre certificeringer eller udstedelse af mærker m.v., der har til formål at demonstrere, at sikkerheden i større eller mindre grad er blevet afprøvet. F.eks. laver CompTIA og ViaFo-

rensics en undersøgelse af, om mobile applikationer efterlever visse på forhånd definerede krav[7]. Det kan betale sig at undersøge, om der findes tilsvarende tiltag i den branche, som virksomheden hører til.

PATCH MANAGEMENT

Producenten bør sikre, at de intelligente produkter løbende kan opdateres i takt med at der opdages fejl i softwaren.

Al software har fejl. Så længe produktet er isoleret og ingen forsøger at udnytte disse fejl, kan konsekvenserne være begrænsede. Men når produktet er online ændres risikobilledet. Derfor er det nødvendigt at sikre, at produkterne løbende kan opdateres i takt med at fejl opdages.

Der skal laves procedurer for, hvordan software kan opdateres løbende. Strategien afhænger i høj grad af produktet, og af hvordan produktet forbinder sig til internettet. Det er vigtigt, at det ikke kun er produktet selv, som opdateres. Også mobile apps og backend databaser skal opdateres, i det omfang disse er tilknyttet produktet.

Opdateringen skal ske på en sådan måde, at uvedkommende ikke kan give sig ud for at være en opdateringsservice og på den måde downloade skadelig kode til produktet eller de applikationer, som er tilknyttet produktet. Dette sikres typisk gennem krypterede forbindelser og udveksling af hemmelige nøgler, som styrer, hvem der må få adgang til at opdatere.

Opdatering kan i en række tilfælde ske automatisk. Det er imidlertid vigtigt, at brugerne kan gives mulighed for at vælge, om de vil opdatere, da en opdatering kan give kompatibilitetsproblemer med anden software, som produktet eventuelt kommunikerer med.

Man opdaterer typisk på baggrund af ny funktionalitet eller kendte sårbarheder. Det kan i en række sammenhænge være nyttigt at lave en decideret sårbarhedsdatabase over alle kendte sårbarheder i produktet med tilhørende versionsnumre. Databasen kan gøres tilgængelig for brugerne med tilhørende opdateringer.

LIFE CYCLE MANAGEMENT

Producenter af intelligente produkter bør tænke på, hvordan de kan skabe sikkerhed i hele produktets livscyklus.

Producenterne bør være meget specifikke om, hvilken garanti-/supportperiode forbrugerne kan forvente. Mange produkter lever meget længere end garantien eller serviceaftalen tilsiger. Kunderne har været vant til at bruge produktet, til det ikke virker mere. Det forhold, at produktet er intelligent og koblet på nettet, ændrer ikke brugernes forventninger. Men sikkerheden ændres betydeligt for kunderne, hvis de bruger et produkt, som ikke længere supporteres af virksomheden, og dermed ikke opdateres sikkerhedsmæssigt. Desuagtet, at virksomheden juridisk kan skrive sig ud af et ansvar, bør virksomheden overveje, i hvilket omfang der opstår et imagetab

[7] http://www.comptia.org/news/pressreleases/11-12-15/New_Secure_Mobile_App_Developer_Credential_Planned_by_CompTIA_and_viaForensics.aspx.

hos brugerne, hvis noget går galt med et produkt efter udløb af garanti/serviceaftale.

Producenten bør med andre ord tænke på sikkerheden som noget, der skal tilknyttes hele produktets livscyklus. I produktets supportperiode skal det være muligt at opdatere produktets sikkerhed i takt med, at der opdages nye sårbarheder, eller i takt med at underliggende platforme ændres (f.eks. styresystemer under en mobil app). Når garanti-/supportperioden udløber, bør producenten kunne sætte kunderne i stand til at isolere produktet (fjerne online-funktionalitet), hvis de måtte ønske det, således at produktets sikkerhedsrisici reduceres til et minimum.

Det skal overvejes, om produktet efter en periode skal isoleres efter udløb af garanti-/supportperioden som standard. I en række sammenhænge vil en sådan strategi være tvivlsom - særligt hvis kunderne bruger produktet i samspil med andre produkter.

Overvejelserne er særlig relevante for produkter, som er vanskeligt tilgængelige (f.eks. nedgravet under vej, indstøbt i fundament eller indbygget i tag eller hulmur) og dermed grænsende til umulige at erstatte med et nyt produkt med en ny garanti/serviceperiode.

AFHÆNGIGHED AF EKSTERNE LEVERANDØRER

Producenter af intelligente produkter skal gøre sig klart, i hvilket omfang de er afhængige af eksterne leverandører og stille sikkerhedsmæssige krav til disse.

Eksterne partnere kan være en stor fordel, fordi de typisk har specialiserede kompetencer, som producenten ikke er i besiddelse af. Hvis man vælger en ekstern leverandør til at skrive sin software, er det vigtigt, at man får adgang til kildekoden, og at man får lavet et uafhængigt kvalitetstjek af koden.

I en række sammenhænge vil man være afhængig af eksterne leverandørers software. Det gælder f.eks., når man skal have sin mobile app til at køre på et mobilt styresystem, når app'en skal placeres i en app-store, eller når data skal placere i en backend database. Der kan være vanskeligheder forbundet med at blive optaget i en app-store, og man skal være opmærksom på betalingsmodellen for at blive optaget. Man skal desuden holde øje med de opdateringer, der foretages af denne software, da der kan opstå konflikter i forhold til virksomhedens egne programmer. Endelig bør man være opmærksom på, om nogle af de fejl, der findes i denne software, kan gøre producentens egne programmer sårbare.

Nogle af leverandørerne af software kan kræve, at der ikke kører sikkerhedsprogrammer på deres software. Formålet er at sikre, at fremmede programmer ikke gør skade på softwarens funktionalitet og tilgængelighed. Det gør sig især gældende indenfor produktionssoftware. Man skal være opmærksom på, om leverandøren stiller sådanne krav og vurdere sin risiko herved.

Når indkøberne indgår i et samarbejde med en ekstern leverandør, er det vigtigt at have processer på plads, som sikrer, at de rette krav stilles. Kravene kan bl.a. omfatte:

1. Software - f.eks. styresystem, kompatibilitet og eventuelle krav til andet særligt software
2. Krav til hardware
3. Netværksteknologier - f.eks. trådløse teknologier, IPv6-kompatibilitet og åbne porte
4. Sikkerhedsteknologier - f.eks. indlejrede firewalls, opdatering af produktet eller styresystemet og antivirus
5. Service level agreement (SLA) og herunder kontinuitet i service
6. Fjernadgang for leverandøren
7. Behov for at indgå non-disclosure agreement.

Foruden de krav som stilles til leverandøren, skal den, der har ret til at foretaget indkøbet hos producenten, også være bevidst om sikkerhedskravene i egen organisation.

FØLG MED I TRUSSELSBILLEDET

Producenter af intelligente produkter bør følge med i trusselsbilledet og identificere, hvilke metoder hackere tager i brug for at få adgang til virksomhedens produkter eller tilsvarende produkter.

Virksomheden kan lære rigtig meget af hackernes angrebsformer. Ved at følge med i diverse hacker fora kan man også få en early warning af om der er noget i gærde, som retter sig mod virksomheden.

Desuden er det vigtigt at forsøge at sætte sig i hackernes sted og spørge sig selv om der er noget de kan vinde ved at hacke netop virksomhedens produkt. Typisk er hackerne ude efter at tjene penge (f.eks. hacking som service eller afpresning), ude efter at opnå et politisk eller idealistisk formål, ude efter at ramme en bestemt person eller institution, som har produktet installeret eller blot ude efter at hacke for at se, om det kan lade sig gøre, og de dermed kan få prestige i hackermiljøet. Det er altså en ganske bred kreds af motiver, man skal beskytte sig imod.

Har man ikke selv ressourcer eller kompetencer til en sådan overvågning, kan det betale sig at købe den som en service hos en sikkerhedsleverandør.

FORSIKRING

Producenter af intelligente produkter bør undersøge, om de kan forsikre sig mod konsekvenserne af sikkerhedsmæssige risici, som man af tekniske eller ressourcemæssige årsager ikke har adresseret.

Uanset hvor gode udviklings- og sikkerhedsprocesser man har baseret sin produktion på, vil der altid være en restrisiko for, at noget utilsigtet kan ske med produktet. I den forbindelse er det en god ide at undersøge, om man kan forsikre sig mod denne restrisiko.

HÅNDTERING AF HENVENDELSER VEDRØRENDE KOMPROMITTERING

Producenter af intelligente produkter bør have en proces på plads til at håndtere henvendelser, der drejer sig om sikkerhed i produkterne.

Denne type henvendelser skal betragtes som en værdifuld kanal til at få viden om produktet, som man ikke havde i forvejen.

Det må forventes, at en række brugere vil manipulere med produktet enten med det formål at opnå ny funktionalitet, eller med det formål at teste om sikkerheden har et niveau, som er i overensstemmelse med deres individuelle forventninger.

Den første gruppe kan det være nyttigt at holde tæt til virksomheden med det formål at få ideer til fremtidig udvikling af produktet. Flere virksomheder har med fordel faciliteret brugerfora med det formål at opnå brugerdreven innovation.

Den anden gruppe vil typisk henvende sig til virksomheden og fortælle, at de har opdaget en sårbarhed, som de mener bør repareres. Typisk vil denne gruppe give virksomheden et tidsrum til at rette op på fejlen inden den vil blive publiceret på en hackerkonference eller i et teknologisk online forum. Det er aldrig en god ide at møde sådanne henvendelser med advokater og forbud. Det vil blot give personen et incitament til at gå til pressen med det samme. Istedet bør teknisk kompetente henvendelser mødes med teknisk kompetente udviklere, som forstår problemstillingen og kan gøre noget ved den.

UDVIKLINGSPROCESSEN

Producenter af intelligente produkter bør sikre sig, at udviklingsprocessen på bedst mulig måde bidrager til at designe sikkerhed ind i produktet fra starten af.

Der findes ganske mange forskellige modeller for softwareudvikling. Hastighed, fleksibilitet og omkostningseffektivitet har været klare drive for udviklingen af nogle af de nyere modeller. Nogle modeller anskuer udvikling som en struktureret lineær proces, hvor der indledningsvist er grundig planlægning og ét procestrin gøres færdigt inden det næste påbegyndes. Andre modeller er mere iterative og baserer sig på prototyper eller delkomponenter af det samlede system, som hver især løber alle procestrin igennem inden de udvides og udvides til at omfatte det samlede system.

Nogle af de nyere tendenser er at lave agil udvikling af software, hvor der arbejdes i tværfunktionelle teams, der løbende giver feedback til projektet, som løbende udvikler produktet på baggrund af denne feedback.

Der er fordele og ulemper ved de forskellige modeller. I forhold til sikkerhed er det således tvivlsomt, om man kan sige, at én model er bedre end andre. Men noget af det man med sikkerhed kan sige er, at hvor programmering foregår i par mellem programmører, der reviewer hinandens kode, har man en reduktion af mulige fejl. Desuden kan man også sige at jo flere gange et produkt gennemløber tests af forskellige faggrupper med forskelligt fokus, jo mindre sandsynligt er det, at man oplever fejl. Jo bedre procedurer for ændringer i produktet (change management) der er fastlagt, jo mere kan man reducere risikoen for introduktion af nye fejl i forbindelse med ændringer. Man kan desuden forbedre sin udviklingsproces ved på forhånd at fastlægge nogle sikkerheds krav (security targets), som der udvikles efter (a la Common Criteria). Og endelig jo mere grundige eksterne tests man får lavet, jo bedre kan man identificere fejl inden produktet frigives.

PROGRAMMERINGSFEJL

Producenter af intelligente produkter bør være særligt opmærksomme på og lære af de kendte fejl, der typisk opstår i programmeringsprocessen for software og firmware i produkter og omkringliggende services.

Der vil altid være fejl i programmer. Man kan reducere fejl ved at sikre, at udviklingen af produkter strømlines efter bestemte modeller. Desuden kan få lavet et code review, hvor koden på forskellig vis gennemgås for fejl. Mange af de fejl, der opstår, ses imidlertid igen og igen, og derfor kan man med fordel lære af de fejl, som allerede er begået.

Fejlene ligger i det indlejrede system i produktet, i mobile apps der kommunikerer i produktet og i backend databaser, som modtager data fra produktet. Hertil kommer, at der også kan være fejl i det software, som de nævnte systemer kører på, men det er i et vist omfang udenfor virksomhedens kontrol.

Der findes flere lister over typiske fejl på nettet, og her skal kun fremhæves tre:

SQL-injection
SQL-kommandoer bruges bl.a. til at få input fra (en bruger af) et program og kommunikere dette input videre til en database, hvor det skal bruges til et givent formål. Programmøren har forventet, at der gives en type bestemt input - f.eks. bogstaver ved angivelse af navn eller tal ved angivelse af alder. Hvis der ikke er lavet en validering af, at input er som programmøren forventer, og at alt andet input neutraliseres, kan en ondsindet person give et input, der bliver fortolket som SQL-kode. Dette kan modificere en back-end database og i værste fald give brugeren ret til at køre programkode i databasen og overtage kontrollen med den. Problemet er som oftest relateret til hjemmeside programmering, men flere og flere systemer bruger webinterfaces til at interagere med deres produkter, hvorfor dette kendte problem er relevant i stadig flere sammenhænge.

Buffer overflow
Når der gives et input fra (en bruger af) et program, har programmøren typisk haft en forventning om en given maksimal længde på dette input. Hvis en ondsindet person giver et input, som er længere end forventet, og dette input ikke neutraliseres, er der risiko for at programmet går ned, eller risiko for at der kan køres programkode, som kan give den ondsindede person kontrol med programmet. Problemet forværre af, at det ikke kun er inputfelter fra brugere, som er i spil, men også buffere af forskellig længde i selve programmet, som kan blive overfyldt ved kopiering fra en buffer til en anden.

Cross site scripting
De fleste websider genereres dynamisk, således at indholdet skifter over (kort) tid. Hvis en hacker får givet et input til en webserver og denne webserver ikke analyserer indholdet og neutraliserer eventuel skadelig kode, inden inputtet gives som output til en dynamisk hjemmeside, kan en brugers produkt blive inficeret af webserveren.

For en mere grundig liste over typiske fejl, kan der henvises til Open Web Application Security Project[8].

PENETRATIONS- OG SÅRBARHEDSTESTS

Producenter af intelligente produkter bør for at identificere mulige sårbarheder teste sikkerheden i deres intelligente produkter og angribe det udefra, som om de selv var hackere.

Test af produkter er et helt almindeligt kendt fænomen. Den mest oplagte test er at se, om produktet virker efter hensigten. Andre tests kommer også jævnligt på tale – f.eks. test af slitage, test af produktionsforløbet, test af kvaliteten, test af brugervenligheden og test af design og emballage. Det er nødvendigt systematisk at føje tests af sikkerheden til denne gruppe af tests. Der er flere forskellige typer af sikkerhedstests[9]:

I IT-verdenen har man i mange år brugt de såkaldte penetrationstests. Penetrationstest er en metode, hvor man simulerer angreb fra personer med ondsindede hensigter, som forsøger at få adgang til it-systemet. Der testes f.eks. for potentielle sårbarheder som følge af fejl på hardware, konfigurationsfejl eller programfejl i softwaren. Der kan også testes for om de tilstrækkelige korrigerende foranstaltninger er til stede og virker.

Det er vigtigt, at penetrationstests gennemføres på både netværkslaget og applikationslaget.

Penetrationstests på netværkslaget er typisk semiautomatiserede skanninger, som kortlægger, hvor der kan sendes informationer ind i eller ud af virksomheden/produktet. Resultatet af denne type skanninger vil ofte være en liste over åbne porte og eventuelle sårbarheder, der kan udnyttes direkte.

Penetrationstests på applikationslaget er, som det fremgår af ordet, test af et program. Det er typisk en mere manuel proces, hvor testeren leder efter typiske programmeringsfejl som f.eks. sql injections eller cross site scripting eller logiske fejl, som f.eks. systematisk forkert henvisning til en modtager. Disse fejl er gennemgået under Programmeringsfejl i denne vejledning.

En delmængde af penetrationstests kaldes også sårbarhedsskanninger. Hen skanner man automatisk efter tilstedeværelsen af en række kendte sårbarheder enten på netværkslaget eller applikationslaget.

Der findes også tests der er rettet mod trådløs kommunikation. Her kan man teste om et produkt kan kommunikere via forskellige trådløse teknologier[10] – f.eks.

---

[8] https://www.owasp.org/index.php/Main_Page.
[9] En glimrende oversigt over de forskellige sikkerhedstests kan findes i NIST SP 800-115, http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf. En mere abstrakt og digert værk er The Open Source Security Testing Methodology Manual, OSSTMM 3, http://www.isecom.org/mirror/OSSTMM.3.pdf.
[10] En glimrende introduktion til de forskellige trådløse teknologier og deres karakteristika kan findes på Wikipedia: http://en.wikipedia.org/wiki/Compari-

GPRS, UMTS, WI-FI (IEEE 802.11x), WiMax, Blutooth, ZigBee, og Z-Wave – og ikke mindst om der i tilknytning til disse er sårbarheder.

Endelig anvendes der ofte fysiske penetrationstests, som har til formål at se, om uvedkommende via f.eks. social engineering kan snyde sig forbi receptionen eller forbi "hunde og hegn" og få adgang til produktet, der hvor det er placeret.

Den typiske penetrationstest forløber i henhold til NIST som følger:

- Planlægningsfase
  I denne fase defineres testens målsætning, omfang og ledelsen accepterer reglerne for gennemførsel af testen.

- Analysefasen
  I denne fase indsamles forskellige informationer om det, der skal skannes, og der gennemføres skanninger af porte og services m.v., så man kan se, f.eks. hvilke porte man kan kommunikere på og hvilke versioner af hvilken software, der kører på systemet. Herefter gennemføres der en sårbarhedsskanning af den information, man indledningsvis har fået indsamlet. På denne baggrund har man en oversigt over, hvor man eventuelt kan slå til og angribe systemet.

- Angrebsfasen
  I denne fase gennemføres det egentlige angreb. Man vil forsøge at få adgang til systemet, herefter vil man forsøge at få stadig større privilegier på systemet og gerne opnå at kontrollere det. Endelig vil man undersøge, om man via systemet kan få adgang til andre systemer, tillige med at man vil installere forskellige værktøjer, der gør, at man kan bevare kontrol med systemet.

- Afrapportering
  Undervejs i hele processen indsamles der data. Disse vil i den afsluttende fase blive opsummeret således, at systemets ejer kan se, hvilke sårbarheder der findes, hvilken risiko for udnyttelse der er i sårbarhederne og endelig gode råd til hvordan disse kan afhjælpes.

I den finansielle sektor er penetrationstests så populære, at det er gjort obligatorisk at foretage penetrationstests hos virksomheder, der håndterer betalinger via kreditkort[11]. Anvendelsen af penetrationstests vil i nogle sammenhænge følge af lovgivning. I USA stiller HIPAA sikkerhedsreglerne krav om at der foretages penetrationstest. Man kunne godt have en forventning om, at der i stigende grad vil blive stillet krav gennem lovgivning, branchemæssig selvregulering eller bare krav fra

---

son_of_wireless_data_standards. Som det kan ses anvendes de til forskellige formål, der bl.a. er bestemt af deres rækkevidde, hastighed og kommunikationsfrekvens.

[11] Payment Card Industries Security Standards kan findes her: https://www.pcisecuritystandards.org/security_standards/documents.php. Det er krav 11.3, der vedrører penetrationstests.

kunderne om at der er gennemført en (årlig[12]) penetrationstest, og hvilke resultater testen gav.

At gennemføre en troværdig penetrationstest kræver særlig uddannet personale. Det anbefales for langt de fleste producenter at hyre en ekstern samarbejdspartner ind. Både for at sikre sig den tilstrækkelige faglige viden og for at sikre sig at den, der tester, er uafhængig af producenten. Producenten kan dog med fordel sætte sig ind i området og blive en bedre sparringspartner for den, der skal gennemføre testen. Det kan bl.a. ske ved at sætte sig ind i nogle af de metodikker, der anvendes ved gennemførsel af penetrationstests. I særdeleshed kan det betale sig at læse NIST SP800-115, pp. 5-2 – 5-6[13].

ADGANGSSTYRING

Producenter af intelligente produkter bør styre, hvem der kan få adgang til hvilken funktionalitet hvorfra i de intelligente produkter.

Adgangen til udstyret er helt afgørende for, hvem der kan foretage ændringer på det. Producenten skal tage stilling til, hvem der skal have adgang til produktet, hvad de skal have adgang til i produktet, og hvordan de skal kunne få adgang.

Typisk vil brugeren skulle have adgang til produktet. Brugeren har desuden i mange sammenhænge brug for at kunne delegere adgang til produktet til familie eller kolleger. Hertil kommer, at producenten, i takt med at produkterne er online, også kan have brug for adgang. Endelig vil visse tredjeparter, som leverer særlige services til produktet, måske have brug for adgang.

Erfaringen viser, at brugeren ikke altid har adgang til hele produktet, idet visse services ofte bliver skjult for brugeren. Disse services bruges som regel til at servicere produktet - f.eks. sikre at servicemedarbejdere kan se logfiler, konfigurere de mest avancerede indstillinger i produktet eller har adgang til et interface, hvorfra der kan tilføjes ny funktionalitet.

I det omfang producenten selv eller tredjeparter har adgang til data fra produktet, bør det vurderes om nogle af disse data er personoplysninger og falder ind under Lov om behandling af personoplysninger. I givet fald skal der sikres compliance med loven. Der bør også foretages en vurdering - f.eks. en Privacy Impact Assessment, som er omtalt i denne vejledning - af om adgangen til data påvirker brugernes tillid til produktet. I givet fald kan man eventuelt separere adgangene således at producenten kun har systemadgang uden at kunne se data og at tredjeparten evt. kun kan se anonymiserede data. Det afhænger helt af produktet, hvad der giver mening.

producenten skal fastlægge hvordan den tekniske adgang til produktet skal ske og hvilke rettigheder der skal følge med. Adgangsstyring foregår typisk således at en bruger identificerer sig med et brugernavn og et password. Produktet autentificerer

[12] En pacemaker eller et intelligent vindue installeres for at holde i mange år. Det nytter ikke noget kun at teste én gang. Trusselsbilledet og de ondsindedes metoder udvikler sig løbende og en sårbarhed, der ikke blev opdaget eller ikke kunne udnyttes for et år siden er måske højaktuel i dag.
[13] http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

brugeren ved at vurderer om den fremlagte identifikation er troværdig. På baggrund af autentifikationen autoriserer produktet så brugere til at have forskellige rettigheder til produktet eller dele heraf. Rettighederne opdeles typisk i læseadgang, skriveadgang, redigering og sletning.

Autorisationen er helt afgørende for sikkerheden i produktet. Selv om det er let at administrere, bør der ikke forefindes et standardbrugernavn og password, som giver adgang til produktet eller dele heraf. Sådanne bliver altid før eller siden afsløret og lagt på internettet.

I stedet bør der etableres brugernavn og password og gerne kombineret med et engangspassword. Der kan alternativt foretages en egentlig udveksling af krypteringsnøgler over en krypteret VPN-forbindelse.

Adgangen til udstyret kan desuden begrænses via firewall og black- og whitelister, som gennemgås i denne vejledning, således at det kun er godkendt udstyr, der får adgang til produktet.

Der er til en vis grad en sammenhæng mellem adgangskontrol, kryptering og udveksling af nøgler, som også gennemgås i denne vejledning.

KLASSISKE SIKKERHEDSTILTAG

Producenter af intelligente produkter bør overveje, om det kan betale sig at installere små sikkerhedspakker på produktet, som man kender det fra fra PC'er, tablets og SmartPhones.

Sikkerhedspakkerne kan indeholde firewall, antivirus, logning, intrusion detection, lister over godkendt software og DDoS prevention. Sikkerhedspakkerne vil blokkere de mest almindeligt forekomne og ofte tilfældige angreb på produktet. Nogle af disse gennemgås i flere detaljer nedenfor.

WHITELISTS OG BLACKLISTS

Producenter af intelligente produkter bør overveje, om de af sikkerhedsmæssige årsager skal begrænse adgangen til produktet gennem white- og blacklists.

Som nævnt flere steder skal producenten være opmærksom på, at det intelligente produkt typisk kommunikerer med andre produkter - f.eks. en SmartPhone - eller indgår i et netværk med flere andre produkter - f.eks. et trådløst netværk i hjemmet. Disse andre produkter kan være sårbare.

Typisk vil en bruger have en række produkter, som han i varierende grad har tillid til. For at få mest muligt ud af disse produkter kobles de på det samme netværk, så produkterne kan kommunikere med hinanden. Hvert produkt bliver altså trusted på netværket. Det produkt, som har den svageste sikkerhed - f.eks. et ældre produkt, som ikke længere supporteres - vil måske kunne give adgang til de øvrige produkter på netværket og er dermed det svageste led. Producentens gode sikre produkt bliver dermed koblet sammen med et eller flere usikre produkter, som det skal kommunikere med.

Producenten står dermed i et dilemma: På den ene side skal brugerne jo have lov til at bruge det udstyr, de har erhvervet sig. På den anden side går det ud over producentens omdømme hos brugeren, hvis et af brugerens øvrige produkter på netværket ødelægger producentens produkt, idet det næppe er gennemskueligt for brugeren, hvad der er sket.

Virksomheden kan forsøge at håndtere problemet ved at etablere blacklists og whitelists.

Blacklists er en liste over services eller adresser på netværket eller internettet, som produktet ikke må kommunikere med. Alle services og adresser, som ikke står på listen, kan der dermed kommunikeres med.

Whitelists er en liste over services eller adresser på netværket eller internettet, som produktet gerne må kommunikere med. Alle services og adresser, som ikke står på listen, kan der dermed ikke kommunikeres med.

Whitelists er dermed langt mere restriktive end blacklists.

Man kan desuden kombinere de to lister, således at man får tre udfaldsrum: Der er nogle services og adresser, som produktet aldrig må kommunikere med. Der er nogle services og adresser, som kan få begrænset adgang til at kommunikere - f.eks. læseadgang. Der er nogle services og adresser, som kan få fuld adgang - f.eks. ret til at konfigurere produktet.

Hvis man vælger at arbejde med black- og whitelists er det vigtigt, at man sørger for at vedligeholde listerne løbende. Der skal også overvejes fordele og ulemper ved at brugeren selv får adgang til at påvirke udformningen af listerne.

SEGMENTER OG ZONER

Producenter af intelligente produkter bør overveje, om det intelligente produkt bør anbefales placeret på sit eget segment på et netværk.

Udfordringen med at håndtere andre usikre produkter på netværket kan også løses på en anden måde. Man kan ved at opsætte en lokal firewall sørge for, at produktet alene får lov til at sidde på et separat segment af netværket - f.eks. et private VLAN. På den måde kan man tillade, at der etableres en dedikeret forbindelse fra produktet ud på internettet, og man kan tillade at enkelte af brugerens produkter får adgang til dette netværk - f.eks. en SmartPhone, som kan bruges til at konfigurere og læse data fra produktet. Omvendt kan de øvrige produkter brugeren er i besiddelse ikke nødvendigvis få adgang til produktet, fordi de ikke har adgang til det pågældende netværkssegment. Der skal også overvejes fordele og ulemper ved, at brugeren selv får adgang til at ændre i konfigurationen af netværksindstillingerne.

KRYPTERING

Producenter af intelligente produkter bør overveje, i hvilket omfang autentifikation, data og kommunikation skal krypteres.

Generelt er der god grund til at se på forskellige anvendelser af kryptering, hvoraf lokal parring gennem udveksling af nøgler, som gennemgået nedenfor, er ét eksempel. Krypteringsteknikker kan bruges til at kryptere kommunikation, så data ikke

kan læses af uvedkommende, mens det transporteres. Lagrede data kan krypteres. Kryptering kan bruges til at autentificere, hvem der forsøger at få adgang til produktet og autorisere, hvad de får adgang til. Desuden kan kryptering bruges i forbindelse med autentifikation, hvor man skal fremvise en nøgle for at dokumentere, hvem man er.

Generelt er det meget svært at implementere kryptering på en sikker måde. Der er f.eks. en del eksempler på at browsere ikke har benyttet TLS/SSL korrekt. Det må anbefales, at virksomheden tager kontakt til leverandører med speciale i dette område, hvis man ønsker at arbejde med kryptering i sine produkter.

UDVEKSLING AF NØGLER

Producenter af intelligente produkter bør overveje, om kommunikation med det intelligente produkt bør sikres gennem lokal parring og udveksling af nøgler mellem trustede apparater.

I en række tilfælde er produktet ikke koblet på netværk eller internet men kommunikerer istedet med apparater i sin nærhed via andre trådløse teknologier. Det kan være en vigtig sikkerhedsparameter, at kun bestemte computere kan kommunikere med produktet. Et oplagt eksempel er pacemakere. Det vil være nyttigt, hvis kun lægen, hospitalet og pacemakerens ejer kan kommunikere med pacemakeren, men ikke andre. På den måde kan det sikres, at uvedkommende ikke kan sidde i et tog og hacke sine medpassagerers pacemakere. Alle virksomheder bør overveje, om deres produkt er af en sådan karakter, at det kan medføre skade på produktet eller skade for ejeren, hvis uvedkommende kan få adgang til at kommunikere med produktet.

Der findes en række løsninger, som sikrer, at alene to på forhånd bestemte parter kan kommunikere med hinanden. Alle disse løsninger er på en eller anden måde baseret på kryptering[14].

Produkterne skal lære, hvilke computere de må kommunikere med og samtidig vide, at det er forbudt at kommunikere med alle andre computere end dem, der eksplicit er tilladt. På den måde kan man opnå sikkerhed for, at uvedkommende ikke kommunikerer med ejerens sensorer og målere.

Produkter er, når de leveres fra producenten, i en fødselstilstand, hvor de ikke har nogen ejere. Fra det øjeblik, hvor de tændes for første gang af den nye bruger, er der risiko for, at ondsindede forbipasserende kan overtage kontrol med dem. For at imødegå denne trussel må produktet ud over en wi-fi adgang fødes med en "location-limited side channel" – f.eks. Near Field Communication[15], som har ekstremt

---

[14] Anbefalingerne i dette afsnit er fortrinsvist baseret på Frank Stajano og Ross Andersons "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", http://www.cl.cam.ac.uk/~fms27/papers/1999-StajanoAnd-duckling--att.pdf og Dirk Balfanz, D. K. Smetters, Paul Stewart og H. Chi Wongs "Talking To Strangers: Authentication in Ad-Hoc Wireless Networks", http://www.isoc.org/isoc/conferences/ndss/02/papers/balfan.pdf.

[15] Standard for radiokommunikation på korte afstande, specificeret i ISO/IEC 18092 / ECMA-340 og ISO/IEC 21481 / ECMA-352.

kort rækkevidde eller et fysisk interface som f.eks. en USB-indgang[16]. På den måde kan det sikres, at det virkelig kun er f.eks. ejerens SmartPhone (og andre computere i tilstrækkelig fysisk nærhed), der kan kommunikere med enheden.

Når brugeren skal installere sit nye produkt og konfigurere det med sin SmartPhone, sker der en første udveksling af kommunikation i form af kryptografisk information mellem de to parter via den såkaldte "location-limited side channel".

Både produktet og SmartPhonen antages at have deres egen offentlige og private nøgle. Nøgleparret har den funktion, at de kan bruges til at kryptere eller dekryptere en besked. Hvis en person, Bob, vil sende en besked til en anden person, Alice, kan Bob kryptere sin besked med Alices offentlige nøgle. Herefter er det kun Alice, der kan læse beskeden ved at dekryptere den med sin private nøgle. Nøglerne genereres på en sådan måde, at selv med kendskab til den offentlige nøgle er det indenfor næsten uendelig tid umuligt at gætte den private nøgle.

Sikkerheden ligger i tre elementer: For det første vil det være meget vanskeligt grænsende til umuligt for en ondsindet person at komme så fysisk tæt på produktet, at han vil kunne udveksle nøgler med den via sin egen SmartPhone i den "location limited side channel"[17]. For det andet ville ejeren opdage, at noget var galt, hvis der allerede var en anden part, der havde kontrol med produktet. For det tredje vil en ondsindet person, der forsøger at få adgang til sensoren via wi-fi, ikke kunne kommunikere med denne, da han ikke har SmartPhonens private nøgle, og derfor ikke kan dekryptere det budskab sensoren sender, som er krypteret med den offentlige nøgle fra ejerens SmartPhone.

Man kan derfor vælge at anvende mere simple former for kryptering end selve nøglerne. Der kan være tale om certifikater, eller der kan være tale om kortere udgaver af nøglerne kaldes kryptografiske hash-funktioner. Man kan også lave en gruppenøgle, således at man fra sin SmartPhone kan kommunikere med en flerhed af produkter på én gang.

PRODUKTETS SIKKERHEDSTILSTAND

Producenter af intelligente produkter bør overveje, om det intelligente produkt skal kunne rapportere sin egen sikkerhedstilstand til de trustede apparater, som kommunikerer med det.

Producenten kan installere et hardwaremodul i sit produkt, som sikrer at produktet kan rapportere om sin sikkerhedstilstand - herunder i særdeleshed rapportere at

---

[16] Se f.eks. WirelessHART, http://www.hartcomm.org/protocol/wihart/wireless_technology.html.

[17] Anvendes der NFC, vil man på større afstande med det rette udstyr potentielt set kunne aflytte kanalen, men sandsynligheden for at dette skulle ske er meget lille. Se en diskussion af dette i Ernst Haselsteiner og Klemens Breitfuß: "Security in Near Field Communication (NFC)", http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf. Det kan eventuelt overvejes om ejeren skal kunne tænde og slukke for den "location limited side channel" via sin wi-fi-forbindelse, så den kun står åben i de meget korte tidsrum, hvor der skal tilføjes nye computere til muligheden for at kommunikere med sensoren.

der ikke er blevet pillet ved konfigurationen. Dette sker ved at installere et Trusted Platform Module, TPM[18], som følger standarden, ISO/IEC 11889.

TPM kan generere krypteringsnøgler, begrænses disse brug, generere tilfældige tal, skabe hash værdier for software og hardware konfigurationen, så man kan verificere at den ikke er blevet ændret, kryptere data og kryptere data på en sådan måde at de kun kan dekrypteres når TPM sættes i stand til det.

Tanken bag TPM er at skabe tillid til digitale produkter ved at etablere et højt sikkerhedsniveau. Ulempen ved TPM er at producenter, der anvender TPM, har udbredt kontrol med produktet og herunder kan bestemme at ikke bare usikre services men også konkurrerende services ikke må interagere med produktet.

UBRUGT FUNKTIONALITET

Producenter af intelligente produkter bør overveje, om komponenters overskudskapacitet bør utilgængeliggøres.

Nar det bygges produkter bruges der typisk standardkomponenter med standardfunktionalitet, som kan masseproduceres for at holde omkostningerne nede. Det betyder at en række komponenter i produktet indeholder ekstra funktionalitet, som ikke benyttes af produktet - f.eks. ekstra lagerplads eller ekstra instruktioner i chips.

Producenten bør overveje om den ekstra kapacitet der findes i standardkomponenterne i produktet skal gøres utilgængelige ved at fylde dem eller gøre dem uaddresserbare. Ved at gøre dette sikrer man, at de ikke kan bruges til ondsindede formål.

SEPARATION AF SERVICES

Producenter af intelligente produkter skal overveje, om man kan forbedre det intelligente produkts sikkerhed ved at separere nogle af de services, som kører i produktet, således at de ikke kan kommunikere med hinanden.

Når et produkt udvikles tænkes der ofte i at produktets enkelte dele skal fungere sammen. Der er grund til at producenten overvejer om det er mest hensigtsmæssigt at alle dele af systemet kan kommunikere med hinanden. I mange sammenhænge vil det være mere sikkert at vurdere, hvilke komponenter som har et formål med at kommunikere med hinanden, og så sikre at produktets øvrige dele ikke kan kommunikere med hinanden. Årsagen er at hvis der findes en fejl i en del af softwaren kan denne fejl måske få indflydelse på andre vigtigere dele af softwaren, hvis der ikke er sket en separation.

UAFHÆNGIGE LEVERANDØRER

Producenter af intelligente produkter skal overveje, om det kan være relevant at søge hjælp til at sikre produktet hos uafhængige eksterne leverandører.

Det er de færreste virksomheder, som selv er i besiddelse af stærke kompetencer indenfor alle de forskellige sikkerhedsdiscipliner, som nævnes i denne vejledning.

---

[18] Overblik over TPM: https://en.wikipedia.org/wiki/Trusted_Platform_Module.

Det skal derfor overvejes, i hvilket omfang det kan være relevant at søge disse kompetencer udenfor virksomheden. Fordelene ved at bruge eksterne leverandører er bl.a., at man kan være sikker på at få fat i stærkt specialiserede og altid opdaterede kompetencer og desuden får en uafhængig vurdering af sikkerheden i produktet.

TJEKLISTE

I takt med at produkter gøres intelligente, kommer online og bliver en del af et Internet of Things er der stigende behov for at der er styr på sikkerheden. DI har skrevet vejledningen "Sikkerhed i Internet of Things", som skal hjælpe danske virksomheder med at håndtere sikkerhedsudfordringerne. Vejledningen er en ikke-udtømmende bruttoliste af råd om løsninger, som virksomhederne kan tage med i deres overvejelser, når de udvikler intelligente produkter, som kobles på internettet.

- **Processer til at håndtere sikkerhed**
  Producenter af intelligente produkter skal have processer på plads, som håndterer sikkerheden i intelligente produkter og de mobile apps og back-end databaser, som produkterne kommunikerer med.

- **Risikovurdering**
  Producenter af intelligente produkter skal lave en risikovurdering af de mulige trusler, de kan stå overfor, når de gør deres produkter intelligente.

- **Dataklassifikation**
  Producenter af intelligente produkter bør vurdere, om der behandles data og i givet fald hvilke data, der behandles i produktet. Data bør klassificeres efter deres følsomhed.

- **Privacy**
  Personoplysninger skal beskyttes i henhold til lovgivningen, og virksomhederne kan desuden med fordel vurdere, hvordan de opnår den bedste tillid hos brugerne, når de anvender personoplysninger.

- **Standarder og compliance**
  Der findes en række sektorspecifikke standarder, som producenterne af intelligente produkter indenfor forskellige sektoren skal opfylde.

- **Common Criteria certificering**
  Producenter af intelligente produkter skal overveje, om de ønsker en Common Criteria certificering, som har til formål at demonstrere at softwaren er sikker fordi den efterlever nogle på forhånd definerede sikkerhedskriterier.

- **Patch management**
  Producenter af intelligente produkter bør sikre, at de intelligente produkter løbende kan opdateres i takt med at der opdages fejl i softwaren.

- **Life cycle management**
  Producenter af intelligente produkter bør tænke på, hvordan man kan skabe sikkerhed i hele det intelligente produkts livscyklus.

- **Afhængighed af eksterne leverandører**
  Producenter af intelligente produkter skal gøre sig klart, i hvilket omfang de er afhængige af eksterne leverandører og stille sikkerhedsmæssige krav til disse.

- **Følg med i trusselsbilledet**
  Producenter af intelligente produkter bør følge med i trusselsbilledet og identificere, hvilke nye metoder hackere tager i brug for at få adgang til virksomhedens produkter eller tilsvarende produkter.

- **Forsikring**
  Producenter af intelligente produkter bør undersøge, om de kan forsikre sig mod konsekvenserne af sikkerhedsmæssige risici, som man af tekniske eller ressourcemæssige årsager ikke har adresseret.

- **Håndtering af henvendelser vedrørende kompromittering**
  Producenter af intelligente produkter bør have en proces på plads til at håndtere henvendelser, der drejer sig om sikkerhed i produkterne.

- **Udviklingsprocessen**
  Producenter af intelligente produkter bør sikre sig, at udviklingsprocessen på bedst mulig måde bidrager til at designe sikkerhed ind i produktet fra starten af.

- **Programmeringsfejl**
  Producenter af intelligente produkter bør være særligt opmærksomme på og lære af de kendte fejl, der typisk opstår i programmeringsprocessen.

- **Penetrations- og sårbarhedstests**
  Producenter af intelligente produkter bør for at identificere mulige sårbarheder teste sikkerheden i deres intelligente produkter og angribe det udefra, som om de selv var hackere.

- **Adgangsstyring**
  Producenter af intelligente produkter bør styre, hvem der kan få adgang til hvilken funktionalitet hvorfra i de intelligente produkter.

- **Klassiske sikkerhedstiltag**
  Producenter af intelligente produkter bør overveje, om det kan betale sig at installere små sikkerhedspakker på produktet, som man kender det fra PC'er, tablets og SmartPhones.

- **Whitelists og blacklists**
  Producenter af intelligente produkter bør overveje, om de af sikkerhedsmæssige årsagen skal begrænse adgangen til det intelligente produkt gennem white- og blacklists.

- **Segmenter og zoner**
  Producenter af intelligente produkter bør overveje, om det intelligente produkt bør placeres på sit eget segment på netværket.

- **Kryptering**
  Producenter af intelligente produkter bør overveje, i hvilket omfang autentifikation, data og kommunikation bør krypteres.

- **Udveksling af nøgler**
  Producenter af intelligente produkter bør overveje, om kommunikation

med det intelligente produkt bør sikres gennem lokal parring og udveksling af nøgler mellem trustede apparater.

- **Produktets sikkerhedstilstand**
  Producenter af intelligente produkter bør overveje, om det intelligente produkt skal kunne rapportere sin egen sikkerhedstilstand til de trustede apparater, som kommunikerer med det.

- **Ubrugt funktionalitet**
  Producenter af intelligente produkter bør overveje, om komponenters overskudskapacitet bør utilgængeliggøres.

- **Separation af services**
  Producenter af intelligente produkter skal overveje, om man kan forbedre det intelligente produkts sikkerhed ved at separere nogle af de services, som kører i produktet, således at de ikke kan kommunikere med hinanden.

- **Uafhængige leverandører**
  Producenter af intelligente produkter skal overveje, om det kan være relevant at søge hjælp til at sikre produktet hos uafhængige eksterne leverandører.

BILAG 1: INTUITIV RISIKOVURDERING

1. Er produktet intelligent, men uden forbindelse til sin omverden?
2. Er produktet koblet på et lokalt netværk eller internettet?
3. Kommunikerer produktet trådløst?
4. Afleverer produktet data til en central database?
5. Kan uvedkommende have en interesse i at aflure data fra produktet?
6. Kan nogen have en interesse i at ændre de data, som produktet afgiver?
7. Kan nogen have en interesse i, at produktet ikke kan aflevere sine data?
8. Kan der være nogen, der har en interesse i at produktet holder op med at virke?
9. Er det hensigten at brugeren kan kommunikere med produktet via SmartPhone, tablet, SmartTV, PC eller tilsvarende?
10. Er det hensigten at andre på forhånd definerede personer end brugeren kan kommunikere med produktet (f.eks. en remote servicemedarbejder)?
11. Hvis uvedkommende får kontrol med produktet kan det så gøre skade på produktet, andre produkter eller brugere?
12. Hvis uvedkommende får kontrol med produktets data kan det så gøre skade på produktet, andre produkter eller brugere?

"Ja" til spm. 1, men "Nej" til resten => Du behøver ikke have fokus på produkters sikkerhed lige nu.

"Ja" til spm. 2, men "Nej" til spm. 3-12 => Du behøver ikke have stort fokus på produkters sikkerhed lige nu.

"Ja" til mindst et af spm. 3-8, men "Nej" til spm. 9-12 => Du bør arbejde med produkters sikkerhed, som led i udviklingen af dine intelligente produkter. Du kan få inspiration til arbejde i DI's vejledning om Sikkerhed i Internet of Things.

"Ja" til mindst af spm. 9-12 => Det er meget vigtigt for din forretning, at du har styr på sikkerheden i dine intelligente produkter. Du kan få inspiration i DI's vejledning om Sikkerhed i Internet of Things.

BILAG 2: VIRKSOMHEDENS DIREKTION

Det er helt afgørende for danske virksomheders forretningspotentiale, at de udvikler deres produkter og indbygger intelligens og online kommunikation i dem. På alle områder kommer flere og flere ting online og afgiver data til løbende service og beslutningsunderstøttelse. Vi er godt igang med at få et Internet af Ting - og om få år bliver det et internet af alle ting.

Der er forretning i at få tingene online, og der er endnu mere forretning i at udnytte alle de data, som tingene kan indsamle og afgive. På baggrund af de nye online intelligente produkter vil helt nye disruptive forretningsmodeller opstå.

Når ting bliver intelligente og kommer online, er der en række nye risici, som skal håndteres. Vi har allerede set eksempler på, at de nye online intelligente produkter kan hackes - f.eks. biler, SmartPhones, insulinpumper, pacemakere, NAS-diske, elmålere og intelligente produktionssystemer. Nogle produkter er kommet for hurtigt online, uden at der har været tænkt nok på at få sikkerheden på plads. Det er dyrt, når en hel serie biler skal kaldes ind til service worldwide, og der sker et betydeligt imagetab i samme forbindelse. Det er derfor vigtigt, at man håndterer risikoen fornuftigt fra starten.

Det er ledelsen i virksomheden, som har ansvaret for sikkerheden i virksomheden - herunder også i virksomhedens online intelligente produkter.

DI anbefaler, at ledelsen håndterer produkternes sikkerhed ved at sørge for, at følgende forhold er på plads i virksomheden:

- **Sikkerhedsansvarlig og sikkerhedsorganisation**
  Der skal udpeges en sikkerhedsansvarlig og oprettes en sikkerhedsorganisation. Sikkerhedsmedarbejderne skal fungere tværfagligt i organisationen og medvirke til at sikre det administrative netværk, produktionsnetværket og udviklingen af virksomhedens online intelligente produkter.

- **Procedurer for sikkerhed i produktudvikling m.v.**
  Der skal udarbejdes overordnede politikker med uddybende retningslinjer for sikkerhedsarbejdet i organisationen. Ledelsen skal mindst årligt godkende de overordnede politikker og have forelagt et review af deres aktualitet og deres efterlevelse.

- **Compliance med standarder og lovgivning**
  Ledelsen skal mindst gennem et årligt review sikre, at virksomhedens håndtering af data og udvikling af produkter er i overensstemmelse med lovgivningen og relevante standarder.

- **Forelægges og godkender dokumentation for at der er foretaget de fornødne tests**
  De online intelligente produkter skal udvikles efter fastsatte retningslinjer - herunder sikkerhedsretningslinjer. Produkterne skal løbende testes, således at det dokumenteres, at produkterne har det fastlagte og accepterede sikkerhedsniveau.