Handbok för framtagning av cybersäkra IoT-produkter

Revisionshantering

Detta är första versionen av handboken (utgiven 2023) och den kommer att uppdateras med jämna mellanrum.

Styrgrupp:

Magnus Svensson/Thorbjörn Ebefors, Smartare Elektroniksystem

Maria Månsson, Smartare Elektroniksystem

Olle Bergdahl, IoT Sverige

Processledare och huvudskribent:

John Lindström, Smartare Elektroniksystem

Deltagande företag och organisationer:

AFRY

Atlas Copco industrial technique AB

Eskilstuna Elektronikpartner AB

IoT Sverige

Luleå tekniska universitet (LTU)

Nexus AB

Prevas AB

RISE

SKR

SSF Stöldskyddsföreningen

Strainlabs AB

Svensk Elektronik

T2Data AB

Uppsala universitet

Weop AB

Xertified AB

Upphovsrätt

Disclaimer

Denna handbok är skriven baserad på den samlade kunskap och erfarenhet arbetsgruppen har inhämtat under sina år i branschen. Trots att vi har gått igenom materialet noggrant ett flertal gånger kan vi inte garantera att det inte har smugit sig in felaktigheter och alla som använder sig av innehållet i handboken gör det på eget ansvar. Arbetsgruppen tar inte på sig något ansvar för fel eller skador som uppstår inom de områden den här handboken omfattar.

Redigering: Maria Bergenheim och Kristin Blom, IoT Sverige

Formgivning: Zellout

Tryck: By Wind

ISBN: 978-91-985741-3-5

Förord

Smartare Elektroniksystem är ett strategiskt innovationsprogram inom ramen för Vinnova, Formas och Energimyndighetens gemensamma satsning på strategiska innovationsområden. Programmets mål är att stödja den svenska industrin för hållbar utveckling och konkurrenskraft i världsklass. Under arbetet med framtagning av agendan för programmet lyftes tre huvudutmaningar fram som de viktigaste för att klara framtidens krav. Dessa var spetskompetens, kompetensförsörjning och en effektiv värdekedja. För varje utmaning tillsattes ett råd, och det är i Värdekedjarådet som arbetet med handböcker har initierats. Den första handboken ”Smartare elektronikhandboken” finns och används sedan några år och har rönt mycket uppskattning. Handböckerna förvaltas av Branschorganisationen Svensk Elektronik. Denna publikation Handbok för framtagning av cybersäkra IoT-produkter har tagits fram i samarbete mellan Smartare Elektroniksystem och Internet of Things Sverige (IoT Sverige).

De olika värdekedjor som involveras i framtagningen av IoT-produkter är komplexa. Många aktörer är inblandade och bidrar på olika sätt till den cybersäkra IoT-produkt som sätts på marknaden. Ett nära samarbete mellan objektsägare och användare hos kunder är viktigt. Liksom ett nära samarbete kring utveckling, tillverkning, test, underhåll/service och support. Det krävs för att leverera innovativa, konkurrenskraftiga, tillförlitliga och cybersäkra IoT-produkter. Med andra ord måste tillförlitlighet, cybersäkerhet liksom producerbarhet och underhållbarhet vara inkonstruerade i produkten. Just gränssnittet mellan objektsägare hos kund, utveckling, forskning, produktion och underhåll/service har konstaterats vara särskilt utslagsgivande för hur framgångsrik produkten blir över hela dess livscykel. Effektiv samverkan ger lägre produktions- och underhållskostnader över livscykeln, snabbare ”time to market” och högre kvalitet samt cybersäkerhet.

Handbok för framtagning av cybersäkra IoT-produkter har tagits fram av en arbetsgrupp med representanter från företag och organisationer som bidragit med sina kunskaper och erfarenheter. Den har avgränsats till att fokusera på vad som krävs för att ta fram cybersäkerhetsrelaterade livscykelkrav till produktchefer, utvecklingsansvariga och underhållsansvariga innan tillverkningsunderlag ska tas fram. Denna handbok i kombination med Smartare Elektronikhandboken 2.0 möjliggör effektiv kunskapsöverföring mellan de aktiva parter som samarbetar för att ta fram en cybersäker IoT-produkt för hela dess livscykel.

Detta är första versionen av handboken och vi tar gärna emot idéer till förbättringar och utökningar inför nästa version.

Vi hoppas att du finner handboken användbar i ditt dagliga arbete. Den är skriven av tekniker för tekniker, men vi tror att även icke-tekniker kan hitta delar som är av värde då vi inkluderat den affärsmässiga och bitvis legala sidan av IoT-produkters framtagning.

Sprid gärna denna handbok bland dina leverantörer och kunder!

Handboken finns att ladda ner från:
www.smartareelektroniksystem.se och
www.svenskelektronik.se

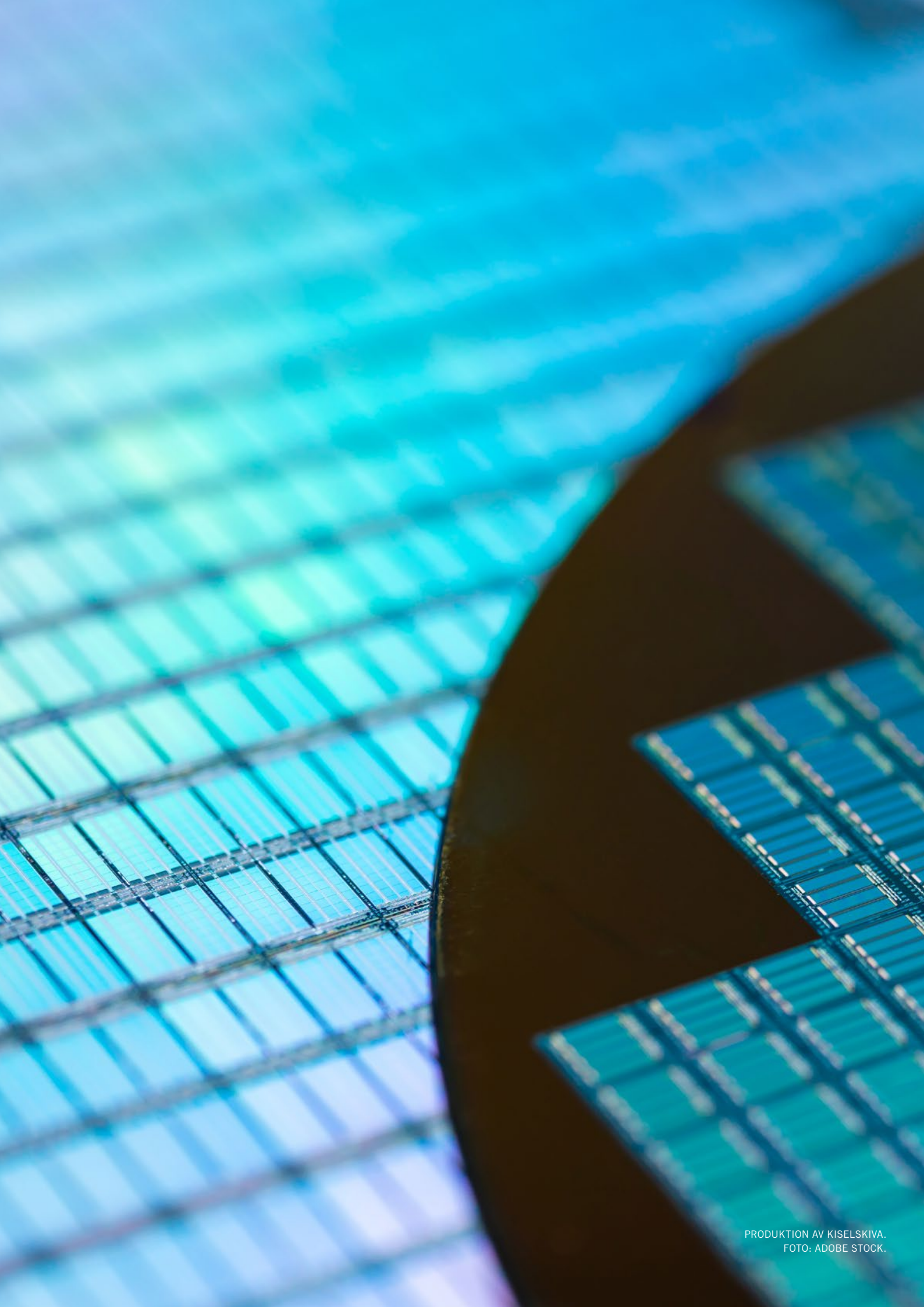
Med vänliga hälsningar,
Arbetsgruppen bakom Handboken för framtagning av cybersäkra IoT-produkter.

Sammanfattning

Handboken för framtagning av cybersäkra IoT-produkter ämnar ge stöd till både primära och sekundära intressenter, då den tar ett grepp över hela livscykeln och då naturligt inbegriper de intressenter och parter som ingår eller medverkar i värdekedjan från början till slut. Att tänka över hela livscykeln gör att kravinsamling och design kräver bredare och djupare kunskaper om både hur användare hos kunder kommer använda en IoT-produkt liksom teknik från sensornivå till molntjänster. Dessutom tillkommer olika holistiska krav där cybersäkerhet ingår om det inte redan delvis finns med i de funktionella krav som produktägare och användare ställer. Vidare behövs goda kunskaper om hur data och information, som genereras i och runt en IoT-produkt, kan användas för att skapa värde genom olika funktioner och tjänster. Dessutom behöver en IoT-produkt troligen kunna, på ett effektivt och cybersäkert vis, övervakas och underhållas samt optimeras över tid. För detta behöver data och information från IoT-produkten kunna extraheras ut och exempelvis uppdateringar, uppgraderingar, omkonfigurationer och optimeringar göras både lokalt och på distans. Till detta behövs en god kunskap om hur kontexterna där IoT-produkterna skall användas i drift och en förståelse för hur cybersäkerhet och IT- samt OT-infrastrukturer tillåter data att skickas ut och in samt hur eventuella externa uppkopplingar kan göras utifrån. Ledningen hos leverantörer och andra intressenter i en IoT-produkts värdekedja kan behöva ta reda på och röja olika hinder ur vägen för att ovan skall kunna ske så att IoT-produkten ska kunna skapa ett bra värde för alla inblandade.

Om IoT-produkter skapar cybersäkerhetsproblem, eller risker i den kontext där de används, lär de inte bli långvariga oavsett hur bra de är. Om det dessutom inte går att sätta upp ett skydd runt dem (runt den IPR och data/information som genereras eller finns i dem) blir det ännu troligare med en kortare livslängd. Samtidigt, att behöva sätta upp ett skydd runt dem på grund av otillräcklig inbyggd cybersäkerhet gör att kostnaden och komplexiteten hos användare ökar. Att behöva sätta upp ett skydd runt omkring försvårar även hur data kan skickas ut och in tillika hur eventuella uppkopplingar utifrån kan göras. Således är det mycket som behöver tänkas över och en förståelse för hela livscykeln och objektsägares IT- och OT-miljöer är nödvändig. Tilläggas bör att det är stor skillnad mellan IoT-produkter avsedda för bruk i hemmet jämfört med användning i professionella miljöer och kritiska infrastrukturer. IoT-produkter avsedda för bruk i hemmet behöver dock ha en tillräckligt bra nivå av cybersäkerhet för att inte skapa onödiga risker. En ytterligare skillnad är att i hemmen är även att den förväntade kunskapsnivån lägre för att kunna göra tillräckligt cybersäkra installationer och konfigurationer.

Handboken handlar om de processer som är relaterade till framtagning av själva IoT produkten, med fokus på hårdvara och inbyggd mjukvara. Något som inte tas upp i handboken är behov av cybersäkerhetsrelaterade strukturer och processer hos tillverkare och andra intressenter eller parter i värdekedjan som hjälper till att hantera en IoT-produkt under dess livscykel. Här kan förutom vidareutveckling, support, service och underhåll även behövas backup/återläsning av data som lagras centralt, incidenthantering (incident response planning), återställningshantering (disaster recovery planning) och kontinuitetsplanering (business continuity planning) om IoT-produkten har server- eller molntjänstdelar som påverkar driften och tillgängligheten eller lagrar data och information. Ju mer kritiska tillämpningar och högre tillgänglighetskrav som objektsägare hos kunder har, desto robustare och motståndskraftiga behöver dessa strukturer och processer vara i händelse av cyberattacker eller driftstörningar.



PRODUKTION AV KISELSKIVA.
FOTO: ADOBE STOCK.

Innehåll

1. Inledning

Idén till handboken har uppkommit i samband med att publikationen Smartare Elektronikhandboken 2.0, har arbetats fram samtidigt som omvärlden tyvärr blivit alltmer full av hot mot IoT-produkter. Dessa båda handböcker ska ses som komplement till varandra och läs gärna båda två innan nya projekt av IoT-produkter dras igång. IoT står för Internet of Things, på svenska sakernas internet. I denna handbok använder vi termen IoT genomgående.

I boken kommer följande definition av "IoT-produkter" att användas: till IoT-produkter räknar vi kollektivt in intelligenta och uppkopplade enheter som kommunicerar och skickar data över Internet. Enheterna är utrustade med processorer, sensorer och mjukvara på så vis att de kan uppfatta sin omgivning, kommunicera med den och således skapa ett situationsanpassat beteende för att kunna bidra och skapa smarta, attraktiva och hjälpfulla omgivningar/miljöer, produkter och tjänster.[1]

Om vi återgår till behovet för handboken så behöver vi allt säkrare IoT-produkter på grund av en ökande aktivitet från hobbyhackers, professionella hackers samt statsunderstödda underrättelseorganisationer vars syfte är att stjäla information, tjäna pengar eller störa verksamheter (till exempel kritisk infrastruktur eller kommuner och regioner) i andra länder.[2] Detta faktum går inte att bortse från och vi får helt enkelt anpassa oss och våra IoT-produkter till situationen. Nedan finns några scenarier för olika miljöer där IoT-produkter kan användas och vad som kan hända om inte IoT-produkterna säkras upp:

Hemmet – vid en cyberattack kan till exempel uppkopplade frysar, spisar, värmesystem, TV och datorer sluta fungera eller låsas. I flerbostadshus kan gemensamma system såsom fastighetsautomation (styrning av VA/värme/el/ventilation/lås med mera) påverkas och i värsta fall sluta fungera. Även bilar och trädgårdsutrustning är numera i hög grad uppkopplade och behöver vara cybersäkra för att inte orsaka fysiska skador eller bränder på grund av medveten överbelastning av komponenter eller system.

På jobbet i kontorsmiljö – förutom att datorer, olika IT-system och nätverk kan sättas ur spel så kan även hissar, kontorets lås-/larmsystem och fastighetens automation påverkas. Konferensrummets utrustning kan avlyssnas och andra samtal spelas in/avlyssnas med hjälp av mikrofoner som finns i datorer, mobiler eller konferensutrustning.

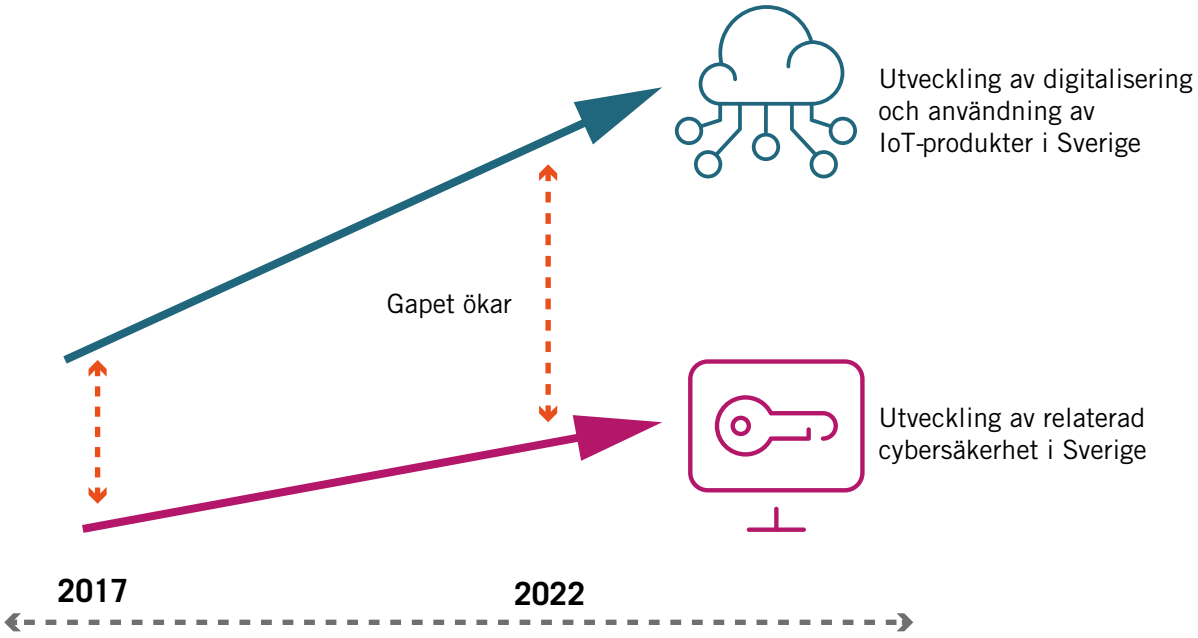
På jobbet i produktions- och distributionsmiljöer – ofta sitter IT-miljön (kontor/administration) ihop med OT[3]-miljön (produktion/distribution) och dessa samverkar då det som ska göras ofta bestäms och administreras via IT-miljön och sedan skickas det till OT-miljön där det sker beställd produktion/distribution. En OT-miljö, som oftast har många IoT-produkter, kan likt en IT-miljö påverkas av cyberattacker i olika former och få driften störd, kvaliteten på det som produceras påverkad eller helt stoppad drift. Tyvärr kan OT-miljön ofta negativt påverkas om IT-miljön är under cyberattack då ingen ny beställningsdata skickas in och ingen produktions-/distributionsdata tas emot tillbaka igen, och kan på så vis även stoppas efter ett tag när beställningsdata är slutfört och ingen ny finns att köra vidare med. Det finns även exempel när produktionsutrustning förstörts eller kraftigt påverkats i samband med cyberattacker. Vissa produktions-/distributionsmiljöer tål inte längre stopp för då fastnar eller stelnar "saker" i långa rörsystem eller annan utrustning, som sen behöver rensas eller bytas ut. Dessa saker kan vara till exempel förstadier till pappersmassa, plaster eller mat. Det finns ytterligare miljöer som liknar vanliga OT-miljöer såsom inom hälso- och sjukvården

[1] http://www.swedishembeddedaward.se/register-to-compete/definition-of-iot/#:~:text=IoT%2C%20the%20Internet%20of%20Things%2C%20is%20a%20collective,that%20communicate%20and%20deliver%20data%20across%20the%20Internet.
[2] https://www.sakerhetspolisen.se/publikationer.html Se årsrapport 2020 och 2021
[3] OT – Operational Technology – att jämföra med IT – Information Technology

men där kallas de inte OT utan MT.[4] I fortsättningen kommer vi dock använda begreppet OT för alla dessa miljöer då grundprincipen är densamma för miljöerna.

Kritiska infrastrukturer[5] (produktion/distribution av energi, VA, telekommunikationer, vägar/järnväg/broar/flyg, livsmedelsproduktion/distribution med mera) – likt ovan i produktions-/distributionsmiljöer finns ofta en behövd samverkan mellan IT- och OT-miljöerna. Skillnaden här är att ett stopp i dessa OT-miljöer snabbt får en väldigt stor inverkan på samhället i stort och många av dessa OT-miljöer är (förhoppningsvis) gjorda för att kunna köras vidare även utan en IT-miljö med hjälp av reservrutiner. Om till exempel energiproduktion/distribution ligger nere under mer än 2–3 dagar kommer påverkan att bli mycket stor då avsaknad av el och elektronisk kommunikation påverkar nästan allt i förlängningen. Vissa av dessa OT-miljöer är så känsliga att de inte ens är uppkopplade utan använder egna nätverk eller publika nätverk med hög säkerhet.

Således finns tyvärr ett alltmer ökande behov av cybersäkra IoT-produkter för att allt från hem till kritisk infrastruktur ska fungera och vara tillgängligt över tid. Figur 1 beskriver att den ökande



FIGUR 1 – ÖKANDE GAP MELLAN SNABBT ÖKANDE DIGITALISERING OCH ANVÄNDANDE AV IOT-PRODUKTER JÄMFÖRT MED TAKTEN PÅ RELATERAD UTVECKLING AV CYBERSÄKERHET.

[4] MT – Medical Technology

[5] MSB definierar samhällsviktig verksamhet där kritiska infrastrukturer används enligt: https://www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/samhallsviktig-verksamhet/vad-ar-samhallsviktig-verksamhet/

takten av digitalisering i kombination med ökad användning av IoT-produkter inte hinns med i den takt som relaterad cybersäkerhet utvecklas. Gapet blir hela tiden större tyvärr, men boken kommer ta upp en del positiva faktorer som kan hjälpa till att vända utvecklingen så att gapet minskar över tid i stället för att öka.

Smartare Elektroniksystem har tillsammans med ett flertal aktörer sedan flera år tillbaka skapat råd till elektronikbranschen hur elektronik kan utvecklas och produceras av flera aktörer tillsammans i värdekedjor. De senaste råden finns i form av Smartare Elektronikhandboken 2.0 där fokus ligger på gränssnittet mellan utveckling och produktion för att ge effektiv samverkan i värdekedjan som ger bättre produkter med högre kvalitet, lägre produktionskostnader och snabbare time-to-market. Nu ser vi ett behov att utöka råden med en Handbok för framtagning av cybersäkra IoT-produkter, då IoT-produkterna är en viktig del av digitaliseringen av vårt samhälle och ekonomi där både ting och människor är ihopkopplade, kan kommunicera och rapportera om sin status samt omgivning1. Genom denna handbok, som kompletterar innehållet i Smartare Elektronikhandboken 2.0, kommer hela IoT-branschen att kunna höja nivån på cybersäkerheten i produkterna redan från början. Vidare ska cybersäkerheten kontinuerligt kunna förbättras under hela livscykeln genom en bra grund- och vidaredesign samt ett genomtänkt underhållsförfarande där uppdateringar och förbättringar kan ske över tid. I takt med att cybersäkerhet förbättras kommer kvaliteten på IoT-produkter samtidigt att förbättras genom nya krav och ökad testning.

Handbokens primära intressenter, vilka beskrivs mer i sektion 1.1, är:

- Konstruktörer och utvecklare (hård- och mjukvara), projektledare, testare, dokumentatörer
- Beställare
- Produktägare
- Produktchef
- Objektägare

Sekundära intressenter för handboken är:

- Tillverkare
- Installatörer
- Utförare av underhåll, service och support samt optimeringstjänster
- Återvinnare
- Myndigheter – som själva är användare och eventuellt även har tillsynsansvar

Samspel och kommunikation mellan intressentgrupperna är essentiellt för att IoT-produkter ska kunna bli framtagna liksom cybersäkra. Alla inblandade behöver förstå att om inte cybersäkerhet, liksom alla andra krav som påverkar livscykelhanteringen av en IoT-produkt, är med så kommer det i långa loppet uppstå: högre kostnader, svåra problem med cybersäkerheten och onödig friktion mellan objektsägare hos kunder och leverantörer. Då det ligger i intressentgruppers intresse att så inte blir fallet, behöver de samarbeta om kravbilden för att möjliggöra en rationell livscykelhantering åt alla inblandade parter och intressenter. Någon av intressentgrupperna behöver sätta sig in i vilka olika lagar och regleringar som gäller samt vilka branschstandarder och best practises som är lämpliga att använda. De sekundära intressentgrupperna behöver även de blandas in i relativt tidigt skede. De behöver hållas informerade och utbildas så att de under sin del av livscykeln kan hantera IoT-produkten korrekt och tillse att dess cybersäkerhet är rätt uppsatt och konfigurerad. Ett bra sätt att behålla samspel och kommunikation är att dokumentera allt som är viktigt.

Fokus och avgränsningar för handboken kommer att vara:

- Handboken avser att adressera en IoT-produkts hela livscykel och cybersäkerhetskrav vid framtagningen av en ny IoT-produkt för att livscykeln ska kunna vara lång och driftsäker.

FABRIKSARBETARE MONTERAR KRETSKORT FÖR HAND.
FOTO: ADOBE STOCK.

PROGRAMMERING AV MJUKVARA.
FOTO: ADOBE STOCK.

- Ge handfasta råd/checklistor/standarder/metoder/best practises som kan läsas av elektronik- och mjukvaruutvecklare (samt deras chefer) som inte själva är säkerhetsexperter. Tyngden kommer vara mot T:et i IoT-produkterna.
- En lagom nivå handfasta råd med praktisk nivå och struktur, rörande cybersäkerhet för utveckling av IoT-produkter, som ska vara lätta att läsa och ta till sig.
- Olika IoT-produkter varierar i omfattning och gränser, från lokalt uppkopplad med begränsad lokal funktion till uppkopplad att skicka data till moln som används för optimering av IoT-produktens funktion samt den process som den verkar i. Handboken kommer adressera detta, liksom hur löpande underhåll av hårdvara och lokal mjukvara samt inställningar kan ske på ett rationellt och cybersäkert vis.

På sidan 82 finns förklaringar till fackuttryck och förkortningar rörande IoT-produkter.

1.1 Intressenter

Det ingår många intressenter i de värdekedjor som IoT-produkter utvecklas och senare används i. Nedan är några av dessa intressenter, som kan ha större eller mindre påverkan på kraven och utformningen av en IoT-produkt, beskrivna. Fokus ligger på de intressenter (eller aktörer) som deltar från första början till dess att livscykeln är slut och IoT-produkterna återvinns. Primär målgrupp är designers och konstruktörer samt utvecklare av hård- och tillhörande mjukvara. Nedan beskrivs även ett antal sekundära intressenter.

1.1.1 Primära intressenter

1.1.1.1 Konstruktörer och utvecklare, projektledare, testare, dokumentatörer och konsulter

När en IoT-produkts framtagning har kommit så långt att en kravbild finns behövs en lämplig grupp för att ta fram IoT-produkten. Ofta lånas öppen källkod och design in, vilket snabbar på

men samtidigt måste tillräcklig kompetens finnas för att kunna utveckla och bedöma om eventuell öppen källkod och design är säker och tillämplig att faktiskt användas. Delintressenterna här beskrivs kort nedan:

Konstruktörer och utvecklare av hård- och mjukvara – konstruktion och utveckling av hårdvara och kod, samt användning av hårdvara och kod utvecklade av andra, innebär att förutom att rätt funktionalitet (utifrån kravspecifikationen) skall bli till, behöver den även bli cybersäker. Det är inte helt lätt, kräver kontinuerlig utbildning och att följa med i utvecklingen av cyberattacker och generell cybersäkerhet. Att tro att detta inte behövs kommer leda till IoT-produkter som rent av kan vara farliga eller som ingen vill ha när detta kommer fram. Vid användning av öppen design eller källkod innebär det normalt att utvecklingsgruppen manuellt behöver gå igenom och använda verktyg för att se till att inget oälkommet har planterats in. Detta bör göras när nya versioner kommer och kan vara ett stort arbete om mycket öppen design eller källkod används. Även hårdvarukomponenter, chips i olika varianter och färdiga kretskort som köps in behöver testas och granskas så att de bara gör det som de skall och inte har fått något extra tillskott (framför allt om de tillverkats utom EU/USA i låglöneländer eller i länder med icke demokratiskt styrelseskick). Utvecklare av både hård- och mjukvara behöver bli bättre på att testa det som de utvecklar och där även ha med tester för cybersäkerhet och gärna automatisera detta så att det går lätt och snabbt att göra alla tester efter en ändring. Automatisering av utvecklingstesterna och användning av testsviter och/eller testriggar förenklar testning av andras och eget.

Utvecklare av tjänster, processer och andra nödvändiga stödjande strukturer – omfånget av en IoT-produkt kan variera från i princip nästan bara en produkt med garanti till att vara baserad på mycket mer avancerad och värdeskapande affärsmodell i botten. Utvecklare av hård- och mjukvara kan säkert bidra och kanske rent av utveckla de tjänster och processer som behövs likt de grundstrukturer som krävs för att dessa ska fungera över tid. Dock skiljer sig utveckling av tjänster och processer lite från hård- och mjukvara, så andra kompetenser kan löna sig att använda här liksom att det krävs en helhetsförståelse för hela livscykeln och värdekedjan samt deras kommande utveckling åren framöver. Till stöd för tjänster och processer kan en blandning av färdiga verktyg användas och kompletteras med egenutvecklade i de underliggande och stödjande strukturer som behövs. Några exempel på tjänster och processer som kan genomföras på plats, från distans eller mix av dessa: support, service, underhåll, utbildningar (för egen personal, kunder och andra i värdekedjan), och "fleet management" (se mer om detta i kapitel 7) med övervakning och andra värdeskapande och effektiva funktioner eller tjänster. En bra självhjälp vid problem, med FAQ, instruktioner och videos samt virtuell/utökad verklighet, som kan konsumeras via webben eller en app kan vara värdefullt för att spara tid både för egen del och för användare.

Projektledare – projektledaren får i vanliga fall ansvar att ta fram en IoT-produkt som utgår från en kravspecifikation och förväntat är att det levereras önskat slutresultat, som håller en bestämd cybersäkerhets- och kvalitetsnivå, med hjälp av tilldelade resurser vid ett visst datum. Till sin hjälp har projektledaren i övrigt exempelvis produktchef och andra relevanta delar i värdekedjan.

Testare – testare behöver inte bara göra testfall för grundfunktionaliteten, vilken självklart skall testas igenom gärna i kombination av automatiserade tester och manuella där inte automatisering går, utan även ha kunskap och förmåga att göra testfall för cybersäkerhet. Testare bör även genomföra olika former av penetrationstester, tester av tillgänglighet/prestanda och vilken information som kan extraheras genom att göra olika grepp såsom felaktiga inloggningar. Hackarna, som kan angripa en IoT-produkt, använder en flora av enkla till mycket avancerade verktyg som

även testarna bör ha kännedom om och rent av ha ett avskärmat labb där dessa verktyg används för att prova att knäcka eller ta sig in en IoT-produkt. Detta ger bra förståelse för hur testfall skall utformas och hur vanliga cyberattacker går till.

Dokumentatör – dokumentatörer behöver även de kunna och förstå aktuell cybersäkerhet för en IoT-produkt. Om inte cybersäkerhet ingår som grundfunktionalitet kan förslagsvis ett extra kapitel eller appendix läggas till manualer för att beskriva hur arkitekturen är uppsatt och hur cybersäkerhet skall appliceras runt om och i IoT-produkten, då denna normalt verkar i uppkopplade miljöer med många andra ting och system. Bra kan vara att ha med vilken cybersäkerhetsfunktionalitet som finns, hur den installeras och konfigureras korrekt, uppdateras och hur det går att verifiera att cybersäkerhetsfunktionaliteten är korrekt uppsatt och fungerar. Till det sista kan särskilda procedurer eller skript behöva tas fram och beskrivas.

Konsulter – för att stärka upp utvecklingsgrupperingar anlitas ofta konsulter inom utveckling av hårdvara, mjukvara, testning, dokumentation eller projektledning med mera. Då dessa kan röra sig mellan flera kunder, som är leverantörer av IoT-produkter eller relaterat och kan vara konkurrenter, behövs vissa saker styras upp för att skydda intellektuella rättigheter, patentidéer och mönster (IPR) samt tillse att cybersäkerheten inte påverkas negativt när de är med i projekt eller löpande arbete. Således behöver avtal om sekretess, IPR och cybersäkerhet upprättas och instruktioner för hur cybersäkert arbete ska ske då konsulter, liksom egna anställda, ofta sitter på annan plats (såvida inte det är ett krav att vara på plats). I avtalet bör det även ingå att konsulterna ska ha god kunskap om cybersäkerhet och framför allt inom utveckling av IoT-produkter.

Övriga – inom utvecklingsgrupperingar finns många olika roller och personalkategorier inblandade, allt ifrån CEO, CTO, utvecklingschefer, programledning, projektledning, till säljare som tar in kravbild samt städare och förvaltare av kontor som rör sig i lokaler där utveckling sker. För dessa behöver cybersäkerhet samt skydd av IPR och sekretess styras upp likväl som för direkt inblandade konsulter.

1.1.1.2 Beställare

Det är inte alltid lätt att förutse hur en IoT-produkt kommer att användas även om en viss användning förskrivs. Möjligheter att lösa nya problem, och även gamla problem, som var utanför tankeramen till idén kommer alltid att dyka upp och hjälpa till att vidareutveckla en IoT-produkt. Att lyssna och prata med delintressenter hos beställare (kunder) med jämna mellanrum är alltid bra för att uppdatera sig om vad behoven är, hur IoT-produkten används, vad som kan förbättras och vad som eventuellt saknas. Hos beställaren kan det finnas ett antal olika delintressenter som är inblandade, varav inte alla alltid kan och förstår hur en IoT-produkt skall användas liksom vilka krav dess omgivning ställer. I sådana lägen kan det vara bra att kunna erbjuda hjälp och ställa frågor som får fram det som behövs för IoT-produkten och dess framtida användning.

Delintressenter hos en beställare:

Inköpare – ofta har inte dessa all specialkunskap som behövs och följer en inköpsprocess. Här behövs ibland lite hjälp så att cybersäkerhetskrav kommer med redan från början då det kan vara både svårt och dyrt att lösa detta senare. Tyvärr blir det nästan heller aldrig lika bra som om de rätta kraven är med från början. En möjlig utveckling av inköpsprocesser är att tillse att kompetens inom IT, OT samt cybersäkerhet är med i processen redan från tidig början för att undvika svåra eller dyra problem senare.

Funktions-/processägare – dessa arbetar ute i verksamheter och har ansvar att saker och ting sker med hjälp av olika former av utrustning där IoT-produkter kan ingå eller IoT-produkter kan ingå som övervakning så att funktionen/processen

FÖRNYBARA ENERGIKÄLLOR ÄR VIKTIGA I FRAMTAGANDET AV IOT.
FOTO: ADOBE STOCK.

fungerar som den skall. Exempel på både styrning av funktion/process och övervakning är sensorer och kameror.

Teknik-/utvecklingsavdelning – kunder har ofta en teknik-/utvecklingsavdelning som bygger upp produktions- och distributionslinjer och anpassar teknik så att den fungerar inom dessa. De som arbetar här har ofta god förståelse för både verksamhet och teknik, vilket gör dem till viktiga delintressenter att diskutera med.

Drift och underhåll/service – de som arbetar på drift och underhåll/service är de som håller på mest med IoT-produkterna då detta oftast är den längsta fasen under en IoT-produkts livscykel. Här finns god förståelse om hur en IoT-produkt på ett effektivt sätt kan sättas i och tas ur drift, uppdateras/uppgraderas, ändras, omkonfigureras, samt allmänt underhållas. Att göra detta enkelt och effektivt (till exempel med hjälp av "fleet management" funktioner) gör att en IoT-produkts livscykelkostnad för en kund blir intressant vid en jämförelse med eventuellt konkurrerande IoT-produkter och lösningar som saknar detta.

Således är det en bra idé att tala med flera olika delintressenter hos kunder då alla har sin pusselbit att bidra med. Här kan goda idéer till att få ned den totala livscykelkostnaden för kunder erhållas.

1.1.1.3 Produktägare

Produktägaren, det vill säga företaget som äger IoT-produkten, är den som sätter IoT-produkten på marknaden och har ansvar för att bland annat CE-märkning finns och att alla lagkrav uppfylls.

1.1.1.4 Produktchef

På leverantörssidan för en IoT-produkt är det en bra idé att ha någon som ansvarar för produktens kravhantering (och kanske fler liknande produkter i en produktfamilj) under deras livscykler och på så vis är produktägarens förlängda arm. Ett tydligt ansvar med tydliga befogenheter att hantera IoT-produkten gör det lättare att få med rätt krav från början och sen lägga till nya krav på resan till slutet av livscykeln. Vanligt är att en produktchef håller i kravinsamlingen och strategisk utvecklingsplanering (någon form av "roadmap") samt verkar som en sammanhållande kraft mellan kunder, utveckling, säljare och andra intressenter. Vanligt är att kravspecifikationen till utvecklingen ägs och sköts av produktchefen.

1.1.1.5 Objektägare

På beställarsidan finns ibland objektägare som är ansvariga eller har budgetansvar för till exempel IoT-produkter och andra tillgångar som finns i produktions- och leveransmiljöer. Dessa har efter att inköpet och installationen är klar ett förvaltningsansvar tills IoT-produkten rangeras ut eller övergår till någon annan objektägare. Dessa arbetar ofta nära funktions-/processägare, som har ett större ansvar, för att tillse att det som skall åstadkommas gör det med rätt kvalitet och tillgänglighet. Objektägare har inte alltid cybersäkerhet för ögonen, men de blir alltmer tvungna att ha det i form av planering för åtkomst inifrån och utifrån, redundans, backup/återställning, loggning med mera.

1.1.2 Sekundära intressenter

Ingen kedja är starkare än dess svagaste länk. Om flertalet sekundära intressenter är inblandade i värdekedjorna behöver både fysisk säkerhet och cybersäkerhet avtalas och följas upp med jämna mellanrum då dessa annars kan innebära en väsentlig riskexponering. Nedan finns ett antal potentiella sekundära intressenter, varav en del ibland finns hos leverantören om denne håller i hela vertikalen och horisontalen till kund. Vanligt är att ett flertal externa parter agerar som sekundära intressenter.

1.1.2.1 Tillverkare

Vid tillverkning i egen regi och egna fabriker är det enklare att hålla en bra cybersäkerhet runt

produktionsmiljön samt skydda informationen som behövs för att tillverka hela eller delar av IoT-produkten. En IoT-produkt kan vara enkel eller mer komplicerat uppbyggd och var gränsen går till så kallade cyberfysiska system är oklart. Hur som helst behöver produktionsmiljön skyddas så att: det som är i den behålls konfidentiellt, det inte går att ändra i produktionsprocess och produktionsparametrar utan att ha behörighet för detta samt att produktionsprocesserna fungerar utan störningar och avbrott då dylika förutom att påverka antalet som produceras även kan negativt påverka kvaliteten hos det som produceras. Fysisk säkerhet runt produktionsanläggningen behöver även vara tillräckligt bra så inte inbrott och stölder kan ske liksom sabotage av eltillförsel, ventilation eller vattenledningar.

Vid utkontrakterad tillverkning behöver både fysisk säkerhet och cybersäkerhet uppfylla de krav som internt ställs. Det är skillnad om standardkomponenter utkontrakteras jämfört med om det finns IPR i form av hårdvarulösningar, mjukvara eller kunskap om produktionsprocessen som önskas skyddas. Således kanske inte viss tillverkning skall ske utanför betrodda produktionsanläggningar eller i länder utanför EU/USA där politiska påtryckningar eller inblandning innebär risk för IPR.

En säkerhets- och cybersäkerhetsbedömning kan vara på sin plats att göras åtminstone årligen för att tillse att tillverkningen sker på önskat vis vad gäller fysisk säkerhet samt cybersäkerhet. Utkontrakterad tillverkning innebär också att den externa tillverkaren i sin helhet bör utvärderas med jämna mellanrum inom ramen för inköps- eller leverantörsbedömningsprocesserna.

1.1.2.2 Distributör

Efter tillverkningen kan en IoT-produkt distribueras ut helt eller delvis i egen regi, eller helt eller delvis genom extern distributör eller distributionslösning. För enkla IoT-produkter är detta inte så komplicerat men för de som efter den initiala distributionen även kan ha reservdelar/komponenter eller mjukvara och manualer som

RÄTTIGHETER OCH LEGALA FRÅGOR ÄR CENTRALA GENOM HELA PRODUKTIONSPROCESSEN ÄNDA FRAM TILL SLUTANVÄNDAREN. FOTO: ADOBE STOCK.

ska uppgraderas kan man behöva fundera lite så att detta hålls fysiskt skyddat så gott det går liksom att ingen obehörig kan ändra i vare sig IoT-produkten, reservdelar/komponenter eller mjukvara eller manualer. Att lägga till virus eller annat till mjukvaruuppdateringar eller manualer (om det är exekverbara filer i någon form) kan skapa stora problem för objektsägare hos kunder och leverantören (vare sig de bärs ut manuellt med hjälp av servicepersonal eller laddas ned från en molntjänst eller portal). Till distributionen av hårdvara, mjukvara och manualer behövs processer som säkerställer att inget ovälkommet följer med.

Vidare kan tilläggstjänster finnas till IoT-produkter, i form av underhåll, service och support samt optimeringstjänster varav en del utförs på plats och en del från distans eller med hjälp av data som skickas ut till exempelvis en molntjänst för ändamålet. Om dessa tjänster inbegriper egen personal eller extern distributör/utförare liksom om den eventuella molntjänsten är hos extern molntjänstleverantör, så behövs även här cybersäkerhetstänk och eventuellt även fysiskt säkerhetstänk. Se mer om detta nedan.

1.1.2.3 Installatör

Om inte slutkunden eller leverantören gör installation så används ofta externa installatörer. Likt distributörer behöver dessa ha god fysisk säkerhet och eventuellt även cybersäkerhet om de har små lager hos sig och sköter installationsarbeten med dessa liksom även har mjukvara i egen portal eller molntjänst. Installatörerna behöver fortlöpande utbildning i IoT-produkten och dess installation, konfigurering och driftsättning samt ett generellt säkerhetsmedvetande (där både fysisk säkerhet och cybersäkerhet ingår). Om IoT-produkterna skall installeras i känslig verksamhet eller i processer som kräver väldigt hög tillgänghet, behöver installatörerna tillse att igen annan än de har åtkomst till IoT-produkterna eller deras olika komponenter. Vidare behöver installatörer även veta vad de skall göra när de tar bort gamla IoT-produkter och ersätter med nya eller andra lösningar. Då behöver eventuell känslig data, konfigurationer och styrdata tas bort så att det inte ger någon annan information om vad IoT-produkten använts till, hur miljön där de suttit ser ut och även information om nätverk samt IP-adresser. Vissa IoT-produkter kan behöva destrueras helt om det inte går att säkerställa att känslig data och konfigurationer med mera är helt borttaget. En produktchef eller objektägare kan med fördel prata med dessa om hur installation, konfiguration och driftsättningar kan förbättras.

1.1.2.4 Utförare av tilläggstjänster – underhåll, service och support samt optimeringstjänster

Vanligt förekommande tilläggstjänster inom värdekedjor är att till IoT-produkterna tillhandahålla support, service och underhåll samt optimering av hård-/mjukvara och processer som IoT-produkterna verkar i. Även tilläggstjänster som vidareutveckling av processer och integrationer med andra lösningar är vanligt förekommande. Bland dessa delintressenter finns ofta bra idéer om vad som kan förbättras hos en IoT-produkt då dessa är de som praktiskt hanterar IoT-produkten under den längsta fasen i livscykeln och ser brister och möjliga förbättringar samt kan jämföra med andra leverantörers IoT-produkter och lösningar. Vid service och underhåll, när en del av IoT-produkter byts ut, behöver det säkerställas att ingen känslig data eller annan information, likt för installatörerna, åker med utan tas bort innan kassation. En produktchef eller objektägare kan med fördel prata med dessa hur det operativa kan förbättras.

Tilläggstjänster kan utföras på plats och en del även från distans. Om det sker på plats måste det säkerställas att inte virus eller annan skadlig kod kan föras in och utförarna behöver då tillsammans med kundens användare komma överens om hur processerna skall vara cybersäkrade. I många fall får inte externa bärbara datorer, USB-diskar eller mobiltelefoner användas för att ta in filer och annat utifrån utan andra procedurer behövs. Kundens personal behöver även hålla koll på att utförarna bara gör det som de

skall och inte samlar in data eller annan information från konkurrenters utrusning runt i kring eller om processer och processparametrar de inte skall ha tillgång till. Alltmer av det som tidigare gjordes på plats görs nu från distans genom att ha externa uppkopplingar, såsom högnivå eller lågnivå VPN, vilket sparar tid och kostnader då reseavstånden ofta är långa och tiden det tar för utförandet inte är så lång. Kunden behöver då ha bra kontroll över vilka som släpps in och göra detta på ett eget valt standardiserat vis och där uppkopplingarna är tidsbegränsade, aktiva enbart under "normal" arbetstid och helst tas bort om de inte varit aktiverade under en viss tid. För akuta problem kan man ha snabbaktivering av konton med kort livslängd. Vanligt är att leverantörer samlar data i en central molntjänst för att kunna hjälpa olika delintressenter hos kunden med analyser av processer, optimera dem och inställningar av processparametrar, se tecken på slitage och underhållsbehov eller utbytesbehov av utrustning. Vidare sker ofta underhåll av mjukvara och omkonfigureringar vid ändringar på detta sätt. En del kunder vill dock beroende på: vem som äger denna data, vem som får göra vad med det, och vem som får ha tillgång till, ha en serverlösning lokalt på plats i sitt eget datacenter (on-premise) och inte använda en molntjänst eller leverantörens centrala server. Ägandeskap och åtkomst till data kommer att bli alltmer viktiga i framtiden och ägande eller nyttjanderätten till data blir ofta centralt i datadrivna affärsmodeller. Således behöver det även vara god fysisk säkerhet och cybersäkerhet där data lagras, vare sig det är lokalt eller i en molntjänst alternativt i server hos leverantören.

1.1.2.5 Återvinnare

En IoT-produkt behöver kunna återvinnas helt eller i hög grad när dess fysiska livscykel är slut. En instruktion för hur detta skall gå till behöver finnas med i manualen liksom på eventuella förpackningar. När en IoT-produkt lämnas in för återvinning behöver den förberedas och tömmas på data och information samt vissa delar eventuellt förstöras fysiskt. Detta behövs för att inte svårraderade minnen eller delar som har högt IPR-intresse skall hamna hos konkurrenter eller de som vill göra intrång. I så fall kan de behöva rivas sönder eller krossas. Att tänka på i en eventuell nödvändig destruktion är att underlätta för återvinnaren. Detta kan göras genom att ha en tydlig instruktion och där även hänvisa till objektägares och användares regler för hantering av data och information mot slutet av livscykeln. Se även sektion 3.5 och kapitel 8 för mer om detta. Normalt har objektägare och användare en process för återvinning och om avsteg från normal process och rutin behövs så behöver detta tas upp. Att tänka på är att om en IoT-produkt läggs i en allmän hög på en återvinningsstation så upphör kontrollen över den och vid behov kan andra arrangemang med mer skyddad mellanlagring på återvinningsstationen eller på annan plats vara nödvändig.

1.1.2.6 Myndigheter – som själva är användare och/eller har tillsynsansvar

Myndigheter kan ha en dubbel roll i sammanhang där IoT-produkter används. De kan själva vara användare i olika former av kritiska infrastrukturer samt att de kan vara tillsynsmyndigheter med revision/granskning av cybersäkerhet hos olika aktörer där IoT-produkter används i processer. Således behövs goda kunskaper i cybersäkerhet både där IoT-produkter används samt för de kontexter där tillsyn skall göras. Exempel på tillsynsmyndigheter är Livsmedelsverket (vattenproduktion), PTS, Elsäkerhetsverket och MSB medan exempel på de som använder IoT-produkter är Trafikverket (vägnät, järnväg, farleder), Swedavia (flygplatser), kommuner (vägnät, vatten- och avlopp, fastigheter, äldrevård) och regioner (sjukvård och fastigheter med mera).

1.2 Att certifiera en IoT-produkt eller ej…

En fråga som många ställer sig är vad för skäl det finns att certifiera en IoT-produkt? Några uppenbara skäl är om det finns lagkrav, till exempel GDPR och CE-märkning inom EU (samt kom-

mande Cyber Resilience Act och Cybersecurity Act), eller branschkrav som förväntas för att kunna sälja IoT-produkten. Även Storbritannien, som är en stor marknad i Europa men utanför EU, kommer ha UKCA-märkning för produkter från 31 december 2024 likt EU:s CE-märkning. Mer att läsa om dessa branschkrav finns i punktlistan nedan. Sedan kan vissa kundsegment ha olika krav på sig och mer eller mindre vara tvungna att köpa certifierade produkter för att på ett någorlunda enkelt sätt kunna påvisa att de uppfyller krav i nästa led exempelvis mot en tillsynsmyndighet eller sina kunder. Även styrelser och ägare har börjat vakna och börjar certifiera sina egna organisationer med till exempel ISO 27001 eller IEC 62443. Vidare behöver de även se över vad den utrustning, IoT-produkter och programvaror som de själva använder och tillverkar/säljer har för certifieringar. Således har en viss proaktivitet börjat slå igenom och tanken är att detta ska ge fördelar i affärsutveckling och senare försäljning för att inte tidigt bli utsållad eller diskvalificerad på grund av för låg bevisad cybersäkerhetnivå.

Att certifiera en IoT-produkt kostar både tid, arbetsinsats och pengar. Således bör detta tänkas igenom så att det ska ge mer värde ut än det som stoppas in. Det kan vara bra att innan man påbörjar något förhöra sig med kollegor i branschen eller med de som gör certifieringar inom aktuell standard vilka kostnader och tid som vanligen behövs för ett dylikt certifieringsprojekt.

Att certifiera en IoT-produkt kan ha vissa fördelar då vissa saker kan minimeras eller helt slippa göras. Exempel på dylika saker är kunders frågebatterier inför inköp eller kvalificering, då de själva kan se eller få enkel information om vilken eller vilka certifieringar som IoT-produkten har. Här kan mellan 10–100 timmar sparas varje gång då tyvärr kundernas frågebatterier inte är likadana. Vidare ger en bra och lämplig standard en kvalitetsstämpel och tydlig bild av cybersäkerhetsstatusen vid lyckad certifiering.

Några exempel på cybersäkerhetsstandarder som IoT-produkter kan certifieras mot är inom följande branscher:

- **Konsument** – ETSI TS 103 645/TS 103 701, ETSI EN 303 645, SSF 1120-1
- **Intelligenta städer och fastigheter** – SKR:s Informationsäkerhet inom fastighetsområdet & IoT, Arkitekturgemenskapens Referensarkitektur för IoT (till smart stad och digitala tvillingar)
- **Industri** – IEC 62443 3-3, 4-1 och 4-2
- **Marina tillämpning med klassningsförfarande** – DNV-RU-SHIP Pt.6 Ch.5 och Lloyd's Register Cyber Safe for marine (är bägge baserad på IEC 62443 3-3)
- **Hälso- och sjukvård** – IEC 81001-5-1, MDCG 2019–16 (medicintekniska enheter)
- **Mat och livsmedel inklusive vattenproduktion/ distribution** – IEC 62443 3-3, 4-1 och 4-2
- **Finans** – PCI-DSS
- **Fordon** – ISO 21434
- **Kommuner, regioner samt statligt** – SKR/RISE (KLASSA för IoT), SSNF Robust och säker IoT (stadsnät i Sverige), Traficon (finska transport och kommunikationsnät)
- **Kritisk infrastruktur** – IEC 62443 3-3, ISO 27019
- **Generellt:**
  - ISO/IEC 27400 (IoT säkerhet och integritet), SSF 1120 (stöldskydd runt uppkopplade enheter), SSF3523 (digitala lås), ioXt Alliance (certifieringsprogram för säkra IoT-produkter), IEC 62443 3-3
  - EU Cybersecurity Act är ett ramverk med krav för att certifiera produkter inom cybersäkerhet
  - EU Cyber Resilience Act ställer krav på cybersäkerheten i en produkt under hela dess livscykel

- EU Radio Equipment Directive (RED) som kommer gälla för alla IoT-produkter som kan kommunicera elektroniskt per augusti 2024-
- ISO 27017/18 (säkerhet i molnmiljöer då data från IoT-produkter ofta sparas där)
- ISO 27032 (riktlinjer för Internet säkerhet)

I handboken kommer vi att hålla några standarder, som är bra och tillför stöd i en IoT-produkts livscykel, lite i handen och använda dem framför allt i kapitel 3 och kravanalysen där.

1.3 Regelverk och lagkrav

EU:s NIS-direktiv, Directive on Security of Network and Information Systems, blev svensk lag 2018 och kommer att uppdateras till "NIS2" senast 2024. I grunden ställer direktivet krav på att verksamheter som levererar tjänster som är viktiga för samhället har ett systematiskt risk- och säkerhetsarbete där eventuella säkerhetsincidenter ska rapporteras och hanteras. Det nuvarande direktivet ställer krav på ganska uppenbara verksamheter inom exempelvis hälsovård, dricksvatten, digital infrastruktur med mera. Det nya direktivet utökar omfattningen rejält och inkluderar även fjärrvärme, avfallshantering, avlopp, livsmedel, "kemikalier" samt en lång rad branscher inom tillverkande industri. Samordnat med NIS2 kommer även en rad andra nya och uppdaterade regelverk från EU (se exempel i figur 2). I flera av fallen finns också direkta kopplingar mellan de olika regelverken. Det är viktigt att göra en rejäl regelverksanalys för att skapa en enad bild av den kravmassa man står under.

Några viktiga exempel som kompletterar NIS2 är:

- **CER** – Critical Entities Resiliency Directive. Krav på verksamheter som bedriver samhällsviktiga verksamheter. Ett stort överlapp finns med NIS2.
- **DORA** – Digital Operational Resilience Act. Krav på tålighet inom finansvärlden.
- **CRA** – Cyber Resilience Act. Krav på teknisk utrustning som har många beröringspunkter med NIS. Mycket relevanta kopplingar till IoT.
- **RED** – Radio Equipment Directive. Primärt gällande kravställning på utrustning som innehåller någon form av radio-teknik.
- **MDR/IVDR** – EU förordningar för Medicintekniska produkter och Medicintekniska produkter för in vitro-diagnostik.
- **Maskindirektivet** – krav som säkerställer att maskiner i alla former inte är farliga att använda. Kommer framöver att adressera cybersäkerhet, användning av AI och flera andra tekniska utmaningar inom området.

Av dessa är sannolikt främst NIS2, CRA och RED applicerbara på användning av IoT-teknik inom väldigt många områden. I de fall där IoT används som en del av någon form av maskin kommer även Maskindirektivet vara relevant att ta hänsyn till. Medicintekniska produkter är strängt reglerade med höga säkerhetskrav. NIS2 och de andra regelverken sätter mycket fokus på att skapa säkerhet i leverantörskedjorna. Verksamheter, som exempelvis omfattas av NIS2, förväntas därmed ställa motsvarande krav på sina leverantörer. I praktiken kan detta innebära att alla verksamheter som förväntar sig att sälja produkter och tjänster till NIS2-organisationer behöver anpassa sig till kraven även om den egna verksamheten i sig själv inte omfattas av kravtexterna. Andra krav som NIS2 trycker på är incidentberedskap, tålighet mot störningar, samverkan med tillsynsmyndigheter, sårbarhetshantering, förmåga att mäta effektiviteten i säkerhetsarbetet, ledningens ansvar och behovet av kompetens på ledningsnivå.

NIS2 har utrymme för sanktionsavgifter för verksamheter som inte sköter sig med upp till 2% av global omsättning eller 10 MEUR.

2. Hotbild mot IoT-produkter, risker samt principer

Nedan kommer vi att benämna IoT-produkter och den data och information och annat som behöver skyddas i olika miljöer för "tillgångar". Dessa tillgångar kan då finnas inom ramen för själva IoT-produkten eller i direkt närhet och påverkas av IoT-produktens funktion eller möjlighet att genomföra någon form av cyberattack genom. I sektion 2.1 beskrivs mer om detta.

IoT-produkter kan användas och används på långt fler ställen än man initialt kan tänka sig. I handboken kommer vi till största delen adressera IoT-produkter med följande användningsområden även om det självklart finns många fler såsom flyget, rymden och i det militära:

Hemmet (uppkopplad hemelektronik från smarta fastighetsautomationssystem och lås-/larmsystem, brödrostar, kyl/frys, TV, spelplattformar, klockor, till moderna uppkopplade fordon).

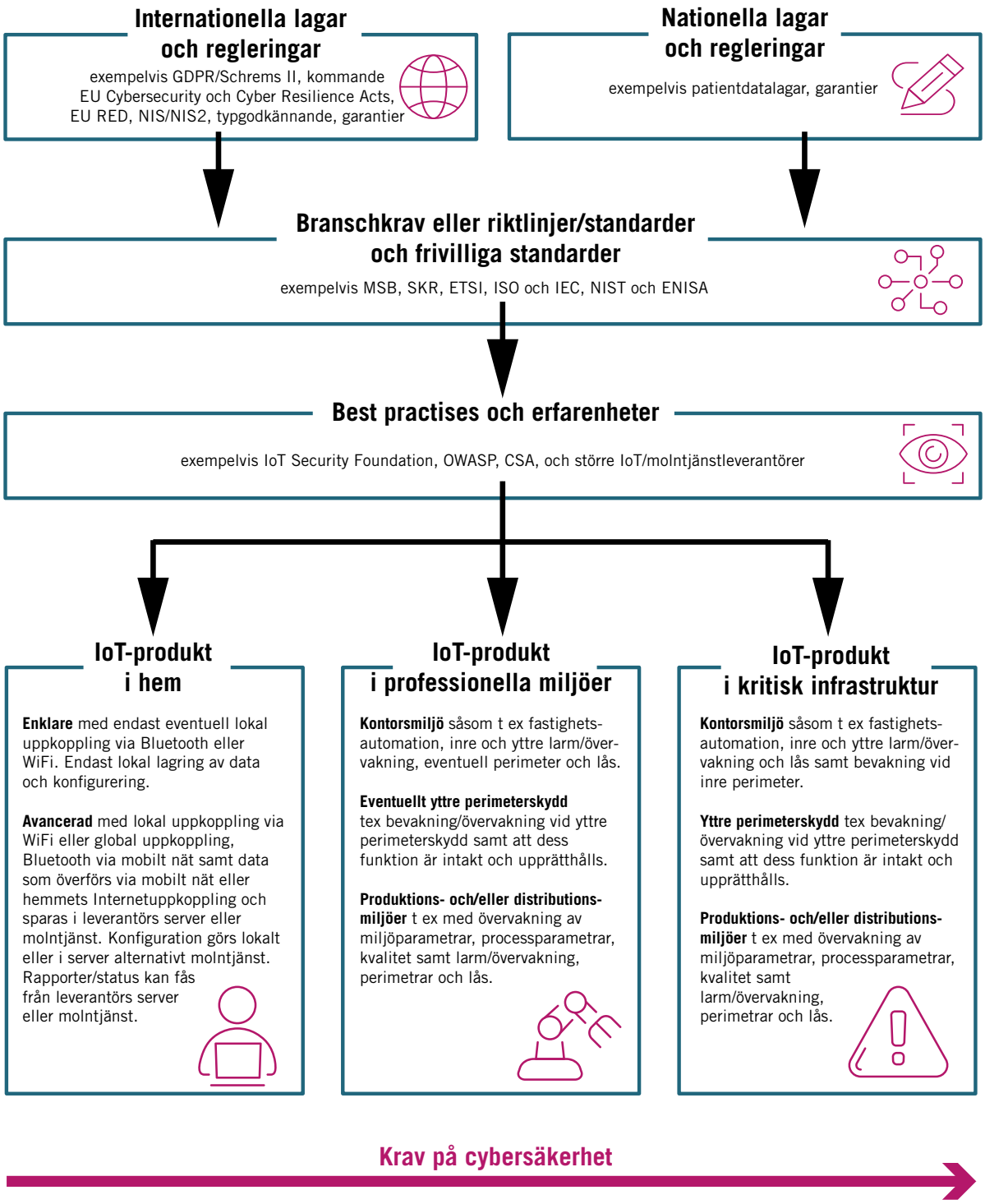
Professionella miljöer (fastighetsautomationssystem och lås-/larmsystem, industriell produktion/distribution, marina miljöer med funktion inom drift av fartyg eller plattformar, hälso- och sjukvård från akutvårds- till äldrevårdsprocesser, livsmedelsproduktion och -distribution, från avstånd manuellt körda eller helt autonoma uppkopplade fordon som används i olika transportprocesser, med mera).

Kritisk infrastruktur (inom samhällsviktig verksamhet).[6]

I professionella miljöer och kritisk infrastruktur anses IoT-produkter av många idag tyvärr vara ett av de största hoten mot hela verksamheten. Således är det av stor vikt att IoT-produkter framöver får en god, eller mycket god, nivå på cybersäkerhet så att den här stämpeln kan arbetas bort.

Figur 2 visar hur övergripande lagkrav till frivilliga bra idéer och erfarenheter påverkar en IoT-produkt förutom de krav som objektägare hos kunder och leverantören själv eller olika intressenter i värdekedjan ställer. IoT-produkterna är grovt indelade i grupper för hem, professionella miljöer och kritisk infrastruktur – och självklart finns fler grupper. Att det finns fler är dock inte poängen här utan att förstå att det inte bara finns krav som utgår från objektägare hos kunder samt att det finns olika grupper eller typer av IoT-produkter från enkel till avancerad samt uppkopplad utåt eller inte. Vidare skiljer sig kraven på cybersäkerhet och tillgänglighet/motståndskraft markant mellan hem, professionella miljöer och kritisk infrastruktur. Således får en kund vara beredd på att betala mer för IoT-produkter avsedda för professionella miljöer eller kritisk infrastruktur än de som finns i hem. Att installera IoT-produkter avsedda för hem, bara för att de är "billiga" och "löser problemet enkelt", i de andra nämnda miljöerna är ingen god idé och lär dessutom inte bli särskilt billigt eller värdeskapande i längden.

[6] Se till exempel: https://soff.se/samhallssakerhet/vad-ar-samhallsviktig-verksamhet/



FIGUR 2 – PÅVERKAN AV INTERNATIONELLA OCH NATIONELLA LAGAR OCH REGLERINGAR, BRANSCHKRAV/RIKTLINJER/STANDARDER SAMT BEST PRACTISES OCH ERFARENHETER PÅ IOT-PRODUKTER I HEMMET, PROFESSIONELLA MILJÖER OCH KRITISKA INFRASTRUKTURER.

DET FINNS MÅNGA TILLGÅNGAR I HEMMET SOM BEHÖVER SKYDDAS PÅ OLIKA SÄTT.
FOTO: ADOBE STOCK.

2.1 Vad vill/behöver man skydda för tillgångar?

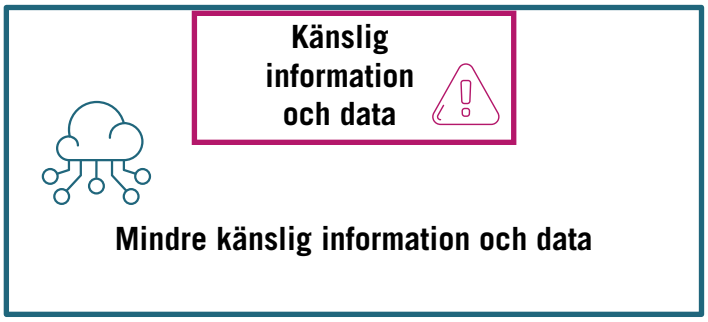
I sektion 3.2 beskrivs olika områden, eller snarare konsekvenser, som vanligen diskuteras när tillgångar ska skyddas: konfidentialitet, integritet, tillgänglighet, förtroende och spårbarhet. Det finns fler men dessa räcker bra till att börja med. Dessa kan vara bra att ha i sinnet när man funderar och kartlägger vilka tillgångar, som finns i IoT-produkterna eller deras närhet, och som behöver skyddas för att undvika sannolika konsekvenser. Nedan tar vi upp några exempel på tillgångar som målas upp kortfattat.

Tillgångar i hemmet

Vad finns för olika tillgångar som är värt att skydda i hemmet? Förutom att inte kunna förstöra själva hemmet genom att skapa eldsvådor och översvämningar har vi data om de som bor där via mikrofoner/högtalare och kameror och som önskas hållas konfidentiella och integriteten intakt. Under kalla delen av året behöver el- och värmesystem fungera så att inte vattenledningar fryser sönder och orsakar vattenskador och under hela året behöver vatten- och avlopp, ventilation samt gärna elsystemet och internetuppkoppling med mera också fungera. Dåligt skyddad utrustning för internetuppkoppling kan ge tillgång till olika system och eventuella sensorer som finns inkopplade, information om nätverkets utformning, och således det mesta som är uppkopplat i hemmet. Om en frys och kyl, som inte är skyddade så vatten kan läcka ut, stängs av och detta inte märks så kan vattenskador uppstå liksom om en sämre brödrost eller spis hålls igång kontinuerligt kan brand uppstå. Vidare kan det analyseras fram om de boende är hemma eller inte med hjälp av data från vatten- och elmätare samt kylskåp ifall de inte är skyddade. Detta kan i värsta fall föranleda ovälkommet besök när man inte är hemma. Har man ett oskyddat larmsystem så kan det testas om det är aktiverat, vilken svarstid olika sensorutslag eller ett larm har, och om sensorer fungerar, eller rent av kan stängas av när så önskas. Det finns många fler exempel på varför IoT-produkter eller lösningar, som ofta kallas smarta produkter, i hemmet behöver vara både fysiskt säkra och cybersäkrade.

Tillgångar i professionella miljöer

I professionella miljöer finns många skyddsvärda tillgångar såsom data om: olika processer där IoT-produkten används samt processparametrar och inställningar/recept, fastigheter och deras stödsystem, nätverks utformning och vilken utrustning som finns där. Vidare kan en mängd detaljerad information finnas om verksamhetens processer, vad som eventuellt produceras och distribueras och hur detta sker. Det sistnämnda kan vara antingen öppen IPR eller sådant man önskar hålla hemligt gentemot konkurrenter. Vidare är det för många verksamheter av stort intresse att produktions- och distributionsprocesses fungerar utan störningar så att det som produceras håller önskad kvalitet och inte får med något extra som inte skall vara där (oönskad mjukvara, komponent eller annan ingrediens). Även information om hur tillverknings- och distributionsprocesser fungerar, eller inte fungerar, kan ge information som kan vara marknadspåverkande och således anses skyddsvärd. Felaktigt installerade och konfigurerade IoT-produkter är en stor oro för många i professionella miljöer och om de även helt saknar vettig cybersäkerhetsfunktionalitet, och är helt beroende av cybersäkerhetsnivån i nätverket runt, så borde detta föranleda att cybersäkerheten som helhet görs både tillräcklig och uthållig över tid. Kopplat till IoT-produkter och hur en verksamhets processer fungerar kan även förtroendet för leveransförmåga och varumärke få sig en törn hos objektägare hos kunder, leverantörer och eventuella granskande myndigheter. En törn av förtroendet klarar de flesta men man kan kortsiktigt tappa försäljning. Ett större ras i förtroende kan bli desto svårare klara av i långa loppet.



FIGUR 3 – EXEMPEL PÅ VILKEN INFORMATION OCH DATA SOM KAN VARA KÄNSLIG OCH SÄRSKILT BEHÖVA SKYDDAS I FÖRHÅLLANDE TILL HELA MÄNGDEN INFORMATION OCH DATA.

Tillgångar i kritiska infrastrukturer

I kritiska infrastrukturer finns ännu fler skyddsvärda tillgångar och dessa måste oftast skyddas enligt nationella skyddslagar och måste ha adekvat skyddsnivå. Förutom högintressant data och information om processerna, anläggningar och nätverk är i många fall högsta prioritet att kritiska infrastrukturer fungerar med väldigt hög tillgänglighet (oftast dygnet runt), att inte deras processer och recept/inställningar kan ändras av ej auktoriserade personer och självklart att allt detta hålls konfidentiellt på rätt nivå.

Figur 3 visar behovet av att kartlägga till exempel vilken information och data som är känslig och särskilt behöver skyddas. Likaså kan ett behov finnas att kartlägga i vilka verksamhetsprocesser, system och tjänster som det måste upprätthållas hög tillgänglighet och integritet. IoT-produkter ingår oftast som en del i något större.

Sammanfattningsvis så bör alla, från hem till kritisk infrastruktur, fundera över vilka deras skyddsvärda tillgångar är. Vanligt är dock olika former av: data och information, att olika former av utrustning och processer är driftsäkra med hög tillgänglighet, objektägare hos kunder och partners förtroende och varumärken med mera. För en leverantör av IoT-produkter gäller det att förstå sina kunders kontexter och utveckla ett adekvat skydd i form av instruktioner och processer i kombination med funktionalitet för att uppnå önskad nivå på säkerhet och cybersäkerhet. Att förstå vilka lagar och regulatoriska krav som berör direkt eller indirekt blir framöver ett måste då det kan få stor påverkan för vad som behöver skyddas eller upprätthållas. En del nya strukturer och processer kan bli nödvändiga att ta fram.

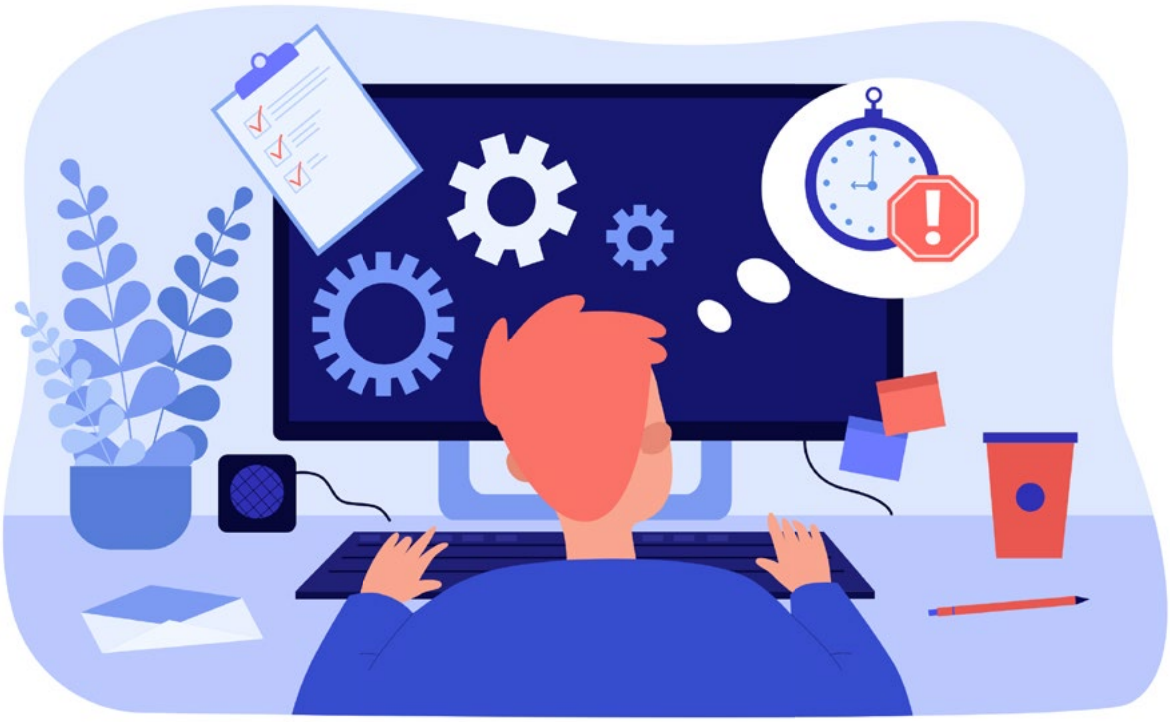
2.2 Svagheter eller sårbarheter

Tillgångar kan ha svagheter och sårbarheter redan från början eller så kan dessa uppkomma efterhand när dåligt utformade uppdateringar eller kombinationer av omständigheter upptäcks. Svagheterna och sårbarheterna kan finnas i hårdvaran, dess eventuella “firmware”, operativsystem och den kod eller applikationer som körs ovanpå detta. Vidare kan olika processer som används för att sköta en IoT-produkt skapa svagheter eller sårbarheter med genom att öppna upp med otillräckligt bra externa uppkopplingar utåt, såsom till exempel hög- eller lågnivå VPN (Virtual Private Network – krypterad tunnel från en punkt till en annan), eller att inte uppdateringar eller underhåll på plats sker med virus- och malware-kontrollerad mjukvara och utrustning. Det är oftast lättare att i efterhand, när svagheter eller sårbarheter upptäcks, åtgärda dessa i olika former av mjukvaror än hårdvara.

I hemmet är det tyvärr vanligt med ett nästan oskyddat eller dåligt utformat skydd av utrustning runt Internetuppkoppling samt dålig

uppdelning av nät (segmentering) för fastighets-automation, barn, arbete, larm med mera. En korrekt uppdelning av nätet försvårar spridning av virus och malware och kan förutom bättre säkerhet även ge IoT-produkter bättre bandbredd ifall detta behövs. I hemmet uppdaterar de flesta IoT-produkterna sig själva om detta ställs in när de installeras och konfigureras, men annars behöver deras eventuella mjukvara uppdateras med jämna mellanrum manuellt. Vidare är det tyvärr inom IoT-produkter för hemmabruk vanligt med dålig design av eller initial avsaknad av cybersäkerhet i hårdvara, firmware eller den mjukvara som körs ovanpå detta. Något som börjar bli bättre, men inte ännu är bra, är ett tvingande att ändra standardkonfigurationer och standardlösenord vid installationsprocessen. Om inte dessa ändras är det tyvärr enkelt, att om IoT-produkten kan kommas åt av obehöriga, ta över och använda den till oönskade aktiviteter. Dessa aktiviteter kan vara att ställa till med: allmän oreda; utpressa genom att kryptera data, information och system; göra system och IoT-produkterna oåtkomliga; användas i så kallade "botnets" och medverka i DDOS-attacker på Internet mot till exempel banker, finansiella lösningar som SWISH och BankID eller webbplatser för exempelvis bokning av tågbiljetter. Om det i hemmet finns IoT-produkter, som är oskyddade, och innehåller mikrofoner/högtalare och kameror är det en god idé se till att dessa inte innehåller svagheter eller sårbarheter så de kan användas för att samla information om de som bor där och se om de är hemma eller ej.

Mycket av det som gäller för hemmet gäller även professionella miljöer och kritiska infrastrukturer. I dessa är det dock ännu viktigare att se till att inte öppna upp onödiga svagheter eller sårbarheter genom antingen dåligt utformad funktionalitet och cybersäkerhetsnivå i en IoT-produkt eller i de nätverk och uppkopplingar utåt som behövs samt olika processer som genomförs vid installation, konfiguration och senare support, underhåll ända till avinstallationen. I dessa miljöer är det viktigare än i hemmet att även skydda så



DET FINNS MÅNGA TILLGÅNGAR I HEMMET SOM BEHÖVER SKYDDAS PÅ OLIKA SÄTT.
FOTO: ADOBE STOCK.

att inte information om nätverken, där IoT-produkterna verkar, läcker ut genom dålig design eller cybersäkerhetsnivå. Den informationen kan sedan användas vid cyberattacker.

TIPS! Vid intresse att se mer om svagheter, sårbarheter och vad som faktiskt är exponerat utåt mot Internet kan till exempel webbläsaren TOR användas tillsammans med olika sökverktyg som Shodan (men då från en dator ej inkopplad i nät som skall vara säkrade). Här kan lätt ses, inom olika geografiska områden och kategorier, utrustning som till synes är exponerad, eventuellt oskyddad och möjlig att koppla upp sig mot. Här hittas mängder med webkameror, sensorer och fastighetsautomationssystem med mera. Tyvärr finns många bra och billiga verktyg tillgängliga för olika former av hackers både på vanliga Internet och Darknet. Se mer om detta nedan.

En generell svaghet för många IoT-produkter är att deras dokumentation i form av användarhandledning med installation och konfiguration inte innehåller något om hur cybersäkerheten runt omkring IoT-produkten bör se ut liksom hur IoT-produkten bör installeras och konfigureras samt underhållas för att vara cybersäkrad så gott det går. Ett tips är att lägga in detta antingen i användarmanualen eller göra ett extra appendix på slutet. En enkel tumregel är att ju lägre cybersäkerhetsnivå en IoT-produkt har desto högre cybersäkerhetsnivå behöver den ha runt sig.

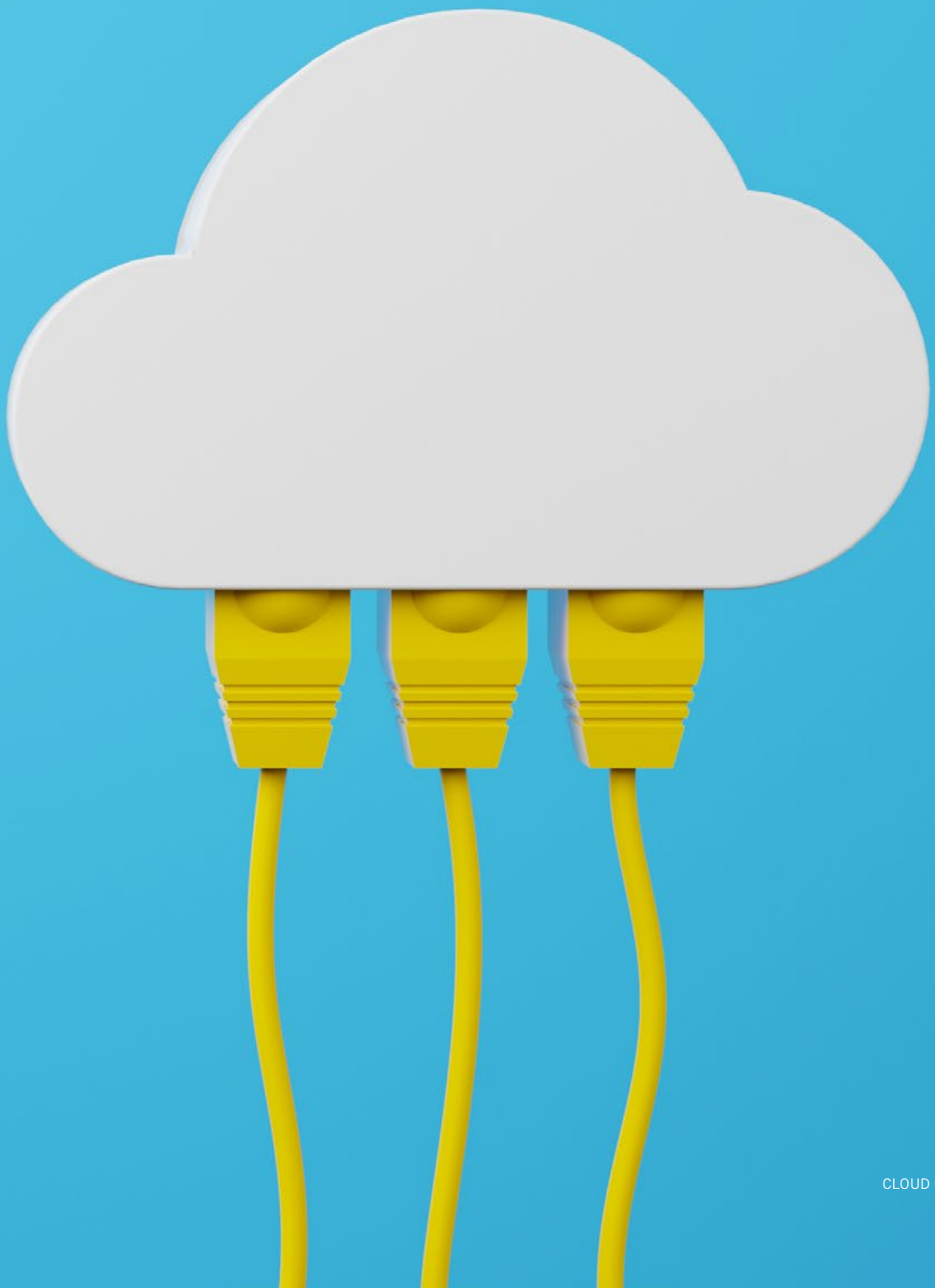
2.3 Vanliga hot

Ofta delas hot in i mindre illasinnade, såsom hobby hackers, samt mer illasinnade som professionella hackers och statliga aktörer vars syfte är att tjäna pengar, stjäla information och IPR, störa eller förstöra verksamheter. Tyvärr har de senare två aktörstypernas aktivitet samt grad av sofistikation ökat väsentlig under de senaste fem åren och ser ut bli än värre. Cyberattacker eller intrångsförsök sker dygnet runt och har till stor del automatiserats för att storskaligt se var aktörerna kan komma in och vad de där kan uträtta. De gör sedan en (affärs)plan och beroende på syfte en turordning för vad som ska attackeras eller infiltreras för informationsinsamling över tid. Tyvärr har både professionella hackare och statliga aktörer ofta goda kunskaper och ligger före många av IoT-produktleverantörer liksom leverantörer av ingående operativsystem med mera.

Ett annat hot från främst professionella hackers eller statliga aktörer är att ta sig in i antingen en IoT-produkts utvecklingsmiljöer eller någonstans i dess distributionskedja för att i någon form av lämplig programkod eller hårdvarukomponent göra tillägg som gör att aktörerna senare kan ta sig in i de miljöer som IoT-produkterna verkar i när deras kod finns distribuerad dit. En benämning på detta är “supply-chain-attack”. Ett annat sätt att få in oönskad kod är genom användning av öppen källkod (olika ramverk), som inte gåtts igenom ordentligt innan ny kod har lagts till de som ansvarar för öppna källkoden. Här bör även ursprunget och vilka som är ansvariga för öppna källkoden granskas och godkännas innan den används. Det är väldigt svårt för de som skall använda IoT-produkterna att hitta tecken på den här typen av attack, särskilt om programvarupaket from IoT-produktleverantören är signerade och allt ser okay ut i tester innan installation då dessa antingen kan vara tidsaktiverade eller bara öppnar ett fönster utåt och låter aktörerna bestämma när och vad som skall ske. För öppen design av hårdvara föreligger samma problematik och allt bör gås igenom innan det används.

Ett annat hot är den egna personalen (eller inhyrda konsulter) och de som är inblandade i hela värdekedjan runt en IoT-produkt till dess att den är avinstallerad och utrangerad. Oftast är det misstag eller för låg kunskapsnivå som gör att svagheter och sårbarheter uppstår och finns kvar samt att dessa inträffar vid olika aktiviteter runt IoT-produkten. Mer sällan är det att missnöjd personal medvetet stör verksamheter, saboterar eller stjäl data, information eller annan IPR och säljer till aktörer. Tyvärr händer detta dock även om det förstnämnda med misstag från egna anställda (eller inhyrda konsulter) är vanligare.

I övrigt finns flera hot och detta behöver tänkas igenom grundligt och beskrivas noggrant i en riskanalys.



CLOUD COMPUTING CONCEPT.
FOTO: ADOBE STOCK.

Tröskeln för hoten är låg och det är relativt billigt att hyra in hackers eller köpa tid i molntjänster eller bot nets avsedda för att hacka eller störa verksamheter. Vidare kostar hackerverktyg från någon dollar till tusentals dollars - allt beroende på vad de kan åstadkomma. Dessa verktyg kan köpas på Internet, Darknet eller från firmor som är specialiserade och säljer dylika verktyg till allt ifrån polis, underrättelsetjänster och de som i övrigt kan betala för sig. Detta gör att förhållandet till att göra en attack jämfört med vad den kan ställa till med är att en väldigt liten kostnad kan skapa stor påverkan/kostnad/förlust. I övrigt behöver ägare av IoT-produkter, eller ägare av verksamheter där IoT-produkter används, tillse att inte deras IoT-produkter är med i bot nets eller andra dylika kampanjer.

Vidare finns det IoT-produkter som är inkopplade i olika nätverk men som inte kommunicerar utåt av sig själva och de som kommunicerar utåt liksom de som installeras i så kallade isolerade öar och inte är inkopplade på nätverket där de används. Dessa som finns i öar kan ibland ha uppkoppling i form av en mobil uppkoppling utåt som används för att skicka data, hämta uppdateringar eller support och underhåll från distans. Här kan man fundera över om man ska ha en process för att öppna upp åtkomst utifrån så att inte ständig åtkomst utifrån finnes. Vanligt är att sätta "problematisk" utrustning i öar då de är gamla, ej uppdaterade eller har alltför låg cybersäkerhetsnivå för att få sitta på verksamhetens nätverk. En sårbarhet som kan utnyttjas av olika aktörer är support, service eller underhåll av IoT-produkterna och här hitta hur icke auktoriserade ändringar eller virus och malware kan fås in. Processerna för support, service och underhåll behöver gås igenom så att inte dessa öppnar upp för detta och alltid tillse att de uppdateringar, komponenter och reservdelar som förs in i en miljö är kollade innan liksom den eventuella utrustningen (till exempel speciellt utrustade bärbara datorer och USB-minnen eller diskar) och som inte underhåll eller IT hos kunden tillhandahåller är ren. Här är det alltså IoT-produktleverantörerens egen, eller värdekedjans, personal och konsulter som måste ha en eller flera cybersäkrade processer och utrustning.

2.4 Riskanalys och hantering av riskerna

Vad gäller riskanalys, som vanligen innebär att skatta sannolikheten och påverkan av hur en tillgång med dess svagheter/sårbarheter kan utnyttjas inom hotbilden, behöver den involvera flertal parter i värdekedjan. Initialt är troligen IoT-produktens utvecklingsorganisation mest inblandad då de behöver inom ramen för sin utvecklingsprocess göra en riskanalys och då förslagsvis även försöka förstå hur resten av värdekedjan påverkar och använder IoT-produkten. Troligtvis leder detta till flera funktions- och cybersäkerhetskrav samt testfall för produktchefen att beakta. Efter en tids användning av en ny IoT-produkt börjar resten av värdekedjan lära sig mer om vad som fungerar och inte samt vad som kan förbättras. Således bör lämpliga parter som håller på med installation, konfiguration, support, service och underhåll involveras liksom flera intressenter hos kunden (där IoT-produkten används). Hos professionella kunder samlar vanligen objektsägare, förvaltningsledare och OT-säkerhetsansvariga ihop vad som kan förbättras utifrån faktiskt utfall och riskanalyser genomförda där. Produktchefen hos IoT-produktleverantören kan lämpligen se till att samla ihop dessa erfarenheter och förbättringsidéer och omvandla dem till krav för fortsatt vidareutveckling.
För både professionella och privatkunder kan användargrupper vara på sin plats, så att man undviker att missnöjda kunder eller andra parter lägger ut detta på Internet för att inget händer. En del leverantörer betalar dem som delger allvarliga buggar och svagheter och inte lägger ut dem i olika grupper på Internet eller Darknet och säljer dem där istället.

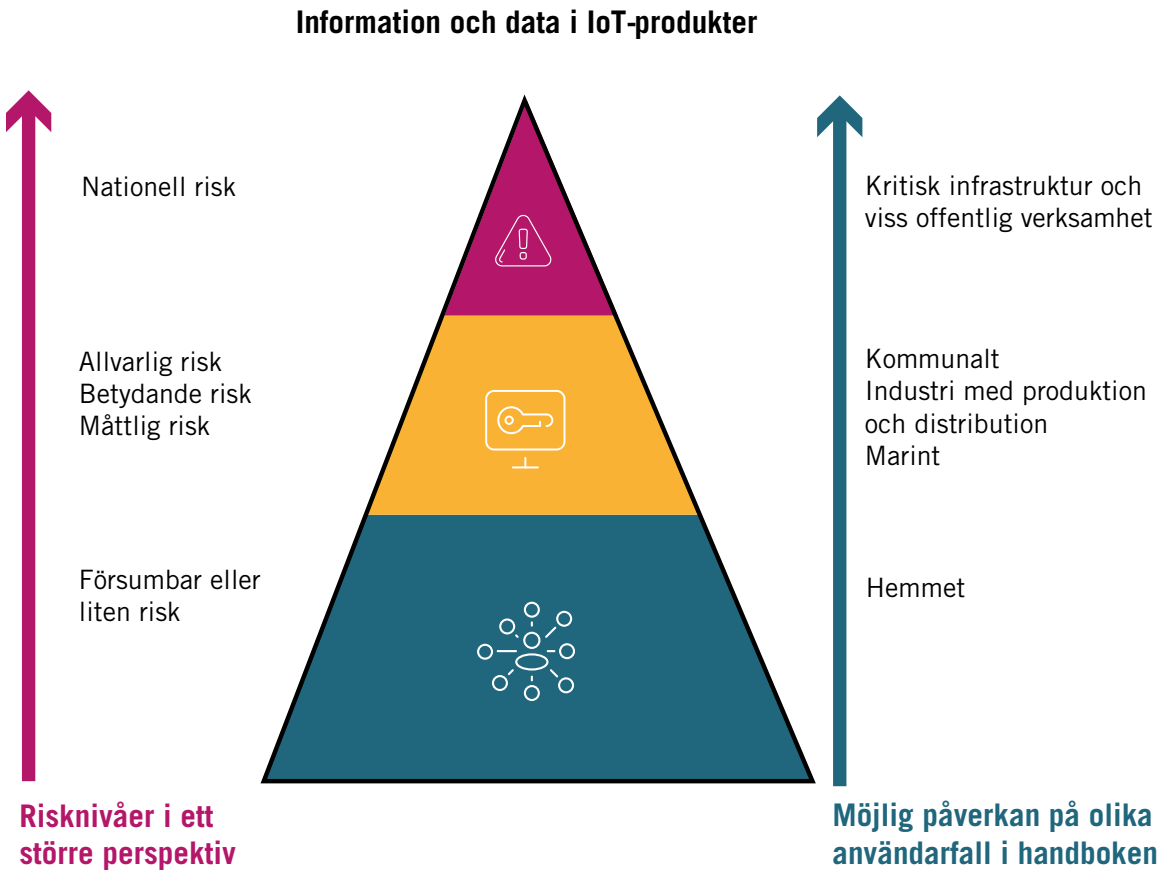
Figur 4 ger ett exempel på hur olika verksamheters information och data i IoT-produkter kan ses i risknivåer och grovt vilken möjlig påverkan som exponering av dessa kan ge i ett större

perspektiv. Riskernas möjliga påverkan på till exempel tillgänglighet eller integritet är inte med i figur 4.

För att göra riskanalys finns enkla till komplicerade metoder att använda. Att använda en enkel metod är ett bra sätt att starta och sedan kan den utvecklas vidare om behövs. Det finns många böcker och standarder/vägledningar om metoder för riskbedömning/hantering såsom: ISO-27005 och 31000, NIST risk management framework och CIS risk assessment method. Bland det viktigaste är dock, oavsett metod som väljs och används, att involvera alla parter som kan bidra. Tyvärr är det vanligt att endast få parter deltar och då blir inte riskbilden korrekt. Riskanalys behöver göras regelbundet (i början av varje utvecklingsprojekt hos IoT-produktleverantörer och minst årligen hos kunden) och oftare om världen runt, det vill säga riskbilden, snabbt förändras till det sämre.

2.5 Principer för cybersäker design av IoT-produkter

Det finns principer för många saker inom design och utveckling av produkter generellt liksom mer specifikt IoT-produkter. Design-for-x eller x-by-design-tänket har funnits länge inom framför allt mekanisk produktutveckling och har utvecklats i takt med att mer krävande affärsmodeller har tagit mekaniska produkter till att bli IoT-ifierade eller omvandlade till mer omfattande cyberfysiska system eller ännu större system. Exempel på dylika affärsmodeller är: produkter med löst



FIGUR 4 – INFORMATION OCH DATA I IOT-PRODUKTER. RISKNIVÅER FÖR OLIKA ANVÄNDARFALL (SE KAPITEL 9) SETT I ETT STÖRRE PERSPEKTIV.

RISKANALYS BEHÖVER GÖRAS REGELBUNDET OCH OFTARE NÄR OMVÄRLDENS RISKBILD SNABBT FÖRÄNDRAS TILL DET SÄMRE.
FOTO: ADOBE STOCK.

kopplade tjänster, produkter med integrerade tjänster, PSS (Product-Service Systems) och funktioner eller funktionella produkter, vilka torde vara av intresse för många IoT-produktleverantörer med. För cybersäkerhet har EU och ENISA sedan ett antal år tillbaka lanserat principerna security-by-design och privacy-by-design. Grundtankarna i dessa två är att säkerhetskrav skall komma med redan från tidig början (då annars cybersäkerheten blir dyr och resultatet oftast sämre likaså) samt att personlig information (som bearbetas, lagras och/eller kommuniceras) ska vara skyddad redan från start till slutet på livscykeln för personliga informationen inom systemet. Mycket av detta berör generell mjukvara, men IoT-produkter är i högsta grad aktuella de med.

I övrigt finns fler designprinciper som kan vara av intresse, såsom Stallings och Brown[7] förespråkar för att minska attackytorna hos nätverk, mjukvara, människor och via fysisk access. Stallings och Brown lyfter fram 13 principer med bland annat: minsta rättighetsnivån, separation av rättigheter (så att man bara kan göra ett visst antal saker som en användare och även så att vissa åtgärder kräver minst två inblandade), minsta antal gemensamma mekanismer, isolering, inkapsling, modularisering, använda lager/nivåer samt öppen design. Zero-trust-modellen, som blir allt mer använd, behöver även den beaktas, och innebär i korthet att varje del i ett system ska ha sin egen tillräckliga säkerhetsnivå och inte behöva vara beroende eller lita på andras säkerhetsnivå. Således gäller "never trust, always verify" och att ingen skall lita på något annat/annan innan verifiering skett. En IoT-produkt kan med fördel delas in i (betrodda) zoner, beroende på vilka komponenter som ingår och hur samt varifrån olika åtkomster sker, för att skapa en separering och kunna upprätthålla god tillgänglighet och skydda data. Kapitel 3 kommer att ta upp mycket av detta och om kravspecifikationen i IoT-produktutveckling tar in lämpligt innehåll från kapitel 2 och 3 kommer båda principerna att vara beaktade. Ett flertal av de standarder som finns i kapitel 3 beaktar åtminstone security-by-design.[8]

En inte helt ny men annan princip eller paradigm, är micro-services paradigm, som fått en renässans när många leverantörer av IoT-produkter eller större system upptäckt att ha all kod i en eller några klumpar inte är särskilt effektivt då det gör att kostnader för underhåll och testningen blir både onödigt dyr och tidskrävande då all kod behöver testas igenom vid även bara mindre ändringar. För att minska detta problem har så kallade "containers" eller liknande börjat användas där man lägger små enskilda micro-services (lätt utbytbara och väl avgränsade tjänster) som samverkar med andra dylika via tydligt specificerade protokoll och gränssnitt. De som har tänkt lite längre här har även lagt in gemensam grundfunktionalitet för cybersäkerhet, administration och "fleet management" i en underliggande plattform som alla micro-services använder. Tänket här är alltså att om man ändrar i en micro-service så behöver bara den testas ordentligt liksom att den fungerar med de andra via uppgjorda gränssnitt. Således kan man undvika att behöva testa all kod, det vill säga alla micro-services, när man ändrat i en eller ett par stycken. Om den underliggande plattformen ändras föreligger dock först ett testbehov för den och sen eventuellt även ett för micro-services beroende på vad som ändrats. Men, att fortsätta utveckla IoT-produkter och ha all mjukvara i en eller några klumpar är inte en effektiv och lönsam väg framåt. Detta kommer hämma innovationshastigheten och binda upp resurser till ingen större nytta alls. Det finns många dylika plattformar för IoT och automation och det svåra är nog att välja vilken som är bra nu och i framtiden. Om koden skrivs på ett bra sätt går det självklart att byta plattform och att ha en gemensam sådan ger potentiellt fina skaleffekter för en utvecklingsorganisation då kunskaper och automatiserade testsviter kan återanvändas till nya projekt och IoT-produkter.

För hårdvaran finns liknande tankegångar som för mjukvaran att, när möjligt och rimligt, bryta ned konstruktioner i utbytbara moduler och komponenter som har väl definierade gränssnitt och standardiserad funktionalitet (kompabilitet).

[7] Stallings, W. och Brown, L., Computer Security: Principles and Practice, 4th edition, Pearson, USA, 2018.
[8] https://www.enisa.europa.eu/news/enisa-news/how-to-implement-security-by-design-for-iot

3. Inför starten av ett nytt projekt

Handboken tar hela livscykeln för en IoT-produkt i beaktande, vilket påverkar kravanalysen och den eventuella infrastruktur och processer samt strukturer som behövs runt en IoT-produkt. En hel del behöver tänkas igenom innan starten av ett nytt projekt och redan från ett tidigt skede i livscykeln. Om inte detta tänks igenom ordentligt så kan måhända initiala utvecklings/projektkostnaden ser bra ut medan hela livscykelkostnaden och lönsamheten för IoT-produkten inte ser så bra ut.

I korthet handlar följande kapitel om:

- Tidigt skede med affärsutveckling, idéer och konceptframtagning
- Kravanalys – funktionella och ”holistiska” krav, lagar/regleringar, branschstandarder och frivilliga standarder, best practises, designprinciper (se sektion 2.3) med mera
- Ledningens ansvar för att ge förutsättningar som behövs
- Utvecklingsmiljö och utvecklingsprocess
- Dokumentation
- Testning
- Underhållbarhet över tid
- Kvalitetsnivå
- Industrialisering
- Utveckling
- Efter utveckling – underhåll/service/uppdateringar och support samt optimering (oftast längsta fasen) samt utbildningspaket
- Uppföljning av IoT-produkten under dess livscykel (ofta lång fas)
- Vid slutet av livscykeln

3.1 Tidigt skede – affärsutveckling, idéer och konceptframtagning

I ett tidigt skede är det affärsmässiga, planeringen och tidiga beslut runt en IoT-produkt känsliga och vissa saker bör hållas hemliga och skyddade. Detta berör inte direkt en IoT-produkts slutliga cybersäkerhetsnivå men väl starten för att nå dit. Således bör information och skisser/ritningar samt anteckningar som berör affärsutvecklingen, idéerna som kläcks och blir till koncept och slutligen urval med en konceptframtagning där eventuella prototyper eller demonstratorer görs för utvärdering, hållas väl skyddade och inom en mindre krets innan nästa steg påbörjas.

Cybersäkerhet krävs således i en organisations IT-miljö och utvecklingsmiljö för att i tidigt skede skydda det som berör:

- Tidig affärsutveckling och lite senare affärsutveckling med affärsmodelltänk
- Idégenerering, konceptgenerering och val av koncept att gå vidare med
- Konceptframtagning – skydd av idéer, skisser och ritningar samt affärsplaner
- Prototyper eller demonstratorer
- Skydda tidig kravanalys (som genereras ur prototyp), samt skydda erfarenheterna av kravanalyserna

Här gäller det för övrigt att de inblandade inte pratar öppet utan tänker på hur de hanterar informationen ovan vid besök hos kunder, resor, i bilen på väg hem från jobbet vid handlingsstopp, eller i kollektivtrafiken på väg till eller från

jobbet. Här kanske även informationen skall vara krypterad och skyddad både inom organisationens miljöer liksom om den bärs med i bärbara datorer, mobiler och USB-diskar eller e-postas.

3.2 Kravanalys
– insamling av funktionella och holistiska krav från intressenter, lagar/regleringar, branschstandards med mera

Det finns ett antal generella och styrande cybersäkerhetskrav på högre nivå, CIA+TP som beskrivs nedan, vilka kan ha påverkan på hela IoT-produktens utformning och anpassning till omständigheter under dess livscykel. Mer specifikt behöver IoT-produktutvecklaren förstå vilken kontext, processer och data/information som kommer vara med under användningen. Här kan man fråga användare hos kunderna vilken tillgänglighetsklassning de kommer att ha på IoT-produkten och vilken informationssäkerhetsklass data/informationen som finns i den. Exempel på data/informationsklasser är: öppen, intern, konfidentiell, strikt konfidentiell samt om persondata eller data/information om kritisk infrastruktur/rikets säkerhet kommer vara med i bilden.

CIA + TP:

- **C (Confidentiality)** – vad behöver skyddas/hållas hemligt och hur?
- **I (Integrity)** – hur ska oauktoriserade ändringar i IoT-produkten eller dess data motverkas?
- **A (Availability)** – vad krävs för tillgänglighet, robusthet och resiliens (dvs. kunna klara av att fungera trots problem)?
- **T (Trustworthiness)** – vad krävs för att upprätthålla kunders, omvärldens och den egna organisationens förtroendet för IoT-produkten?
- **P (Provenance)** – spårbarhet (proveniens) för den data/information som finns i IoT-produkten och sen eventuellt förs över till andra system för lagring eller analys? Även konfigurationer och inställningar av IoT-produkten kan beröras här. Ändringar i IoT-produktens hård- och mjukvara behöver också kunna spåras i respektive utvecklingsmiljöer genom att "tagga koden" och ha versionsnumrering etc.

I IT-miljöer brukar generellt ovan rangordnas i prioritet enligt CIA medan i OT-miljöer och kritiska infrastrukturer rangordnas som AIC och TP hängas på dessa på slutet. Således är det av intresse att veta om IoT-produkten skall användas i något som liknar en IT- eller OT-miljö alternativt kritisk infrastruktur.

Vad gäller den data/information som kommer genereras i eller runt en IoT-produkt och som finns värde i att kunna använda för analys eller förädla på annat sätt i olika tilläggstjänster eller funktioner rörande underhåll/övervakning/optimering, kan det vara bra att först reda ut det affärsmässiga, legala och kontraktuella.

Affärsmässiga, legala och kontraktuella aspekter:

- Vem kommer att äga den data som finns i produkten?
- Var kommer denna data lagras? Finns det legala eller andra aspekter att tänka på?
- Vad får denna data användas till?
- Vem får använda vilken data och när?

Beroende på utfallet ovan är det ändå rekommendationen att separera olika typer av data så ovan frågeställningar är lättare att upprätthålla och bädda inför framtida affärsutveckling (när alla förstår möjligheterna med användning av data till olika ändamål).

Ett exempel på separation är:

- Personrelaterade data (med anledning av exempelvis GDPR inom EU). Om detta hålls separerat är det mycket enklare att utveckla funktionalitet för att följa upp så att olika lagar och regleringar följs.

CYBERSÄKERHETSTÄNKANDET BÖRJAR REDAN NÄR MAN BÖRJAR PLANERA EN NY PRODUKT OCH ÄR INGET MAN LÖSER ENBART I SLUTANVÄNDARFASEN. FOTO: ADOBE STOCK.

- Process- och kvalitetsrelaterad data som berör de aktiviteter eller processer där IoT-produkten används. Dessa data kan till exempel användas för att kunna optimera processers funktion och kvalitetsutfall (genom mätningar på input och output från delprocessteg och/eller hela processer).
- Underhållsrelaterad data som berör slitage och underhållsbehov av IoT-produkten samt dess omgivning och som samlas in via sensorer, kameror, räknare med mera. Dessa brukar IoT-produktleverantören kunna använda i tilläggstjänster liksom samla information om sin "fleet" och kunna se om det finns generella problem och svagheter som behöver designas bort i framtida produktutveckling eller korrigeras genom bättre underhållsprocesser etc. Även att kunna sänka belastning eller göra skyddsstopp är funktionalitet som kan behövas så att inte ett fullständigt haveri inträffar.

3.2.1 Branschstandarder och standarder som kan vara användbara och ge vägledning till cybersäkerhetskrav

Lagar och regleringar kan ge tvingande krav medan andra är mer frivilliga eller krav från den bransch en organisation verkar inom. Alla dessa kan ge upphov till generella och fysiska säkerhetskrav liksom cybersäkerhetsrelaterade krav. En del fysiska säkerhetskrav kan vara relaterade till cybersäkerhetskrav genom att en IoT-produkt till exempel kan behöva ha ett yttre skalskydd eller vara inlåst och ej kunna manipuleras via fysiska åtgärder på plats utan att ha tillträde och auktorisation för det. Vidare finns en mängd olika best practises, som kan tillföra sånt som andra redan upplevt och det är onödigt att genomgå den hårda vägen, vilka kan ge bra och tänkvärda embryon till cybersäkerhetskrav för den egna IoT-produkten. Nedan finns en översiktlig sammanställning som kan vara en god start och

ge högnivåorientering. Alla produktutvecklingsgrupper behöver dock göra sin hemläxa och ta reda på vad som gäller för sin IoT-produkt och de kontexter och branscher som är aktuella.

Vad är det som reglerar en IoT-produkt?

- **Produktregler och lagar** – CE-märkning inklusive exempelvis RED och andra typgodkännanden samt förlängd garanti. Det är ofta olika krav i EU, USA, Australien och Asien.
- **Lagar säkerhet/cybersäkerhet**
  - GDPR (och Schrems II) eller liknande lagar i olika världsdelar
  - Kommande EU Cyber Resilience Act (cybersäkerhetskrav på produkter genom hela livscykeln)
  - Kommande EU Cybersecurity Act (ramverk för cybersäkerhetscertifiering)
  - Patientdatalagar
  - Nationella säkerhetsskyddslagar
  - NIS/NIS2-direktivet från EU för samhällsviktiga/kritiska och digitala tjänster
  - FN:s Resolution MSC.428(98) för marin/sjöfart
  - Lag 2018:1174 rörande informationssäkerhet för samhällsviktiga och digitala tjänster
- **Branschstandarder** – exempel är följande:
  - ETSI TS 103 645/TS 103 701 (IoT säkerhet för konsumenter)
  - ISO/IEC 27018 (skydd av personuppgifter i molntjänster)
  - Hälso- och sjukvård - IEC 81001-5-1, MDCG 2019-16 (medicinteknska enheter)
  - PCI-DSS (skydd av kontokortsuppgifter)
  - SSF 1120-1 (IoT – uppkopplade enheter – krav och provning)
  - SSF 3523 (digital låsenhet - klassning, krav och provning)
  - IEC 62443 3-3 (för automations/kontrollsystem i diverse olika branscher)
  - ISO 21434 (cybersäkerhet i fordon)
  - ISO/IEC 30141:2018 (Referensarkitektur för IoT)
  - ISO/IEC 27400 (IoT säkerhet och integritet)
  - NIST Cybersecurity for IoT
  - IMO:s MSC-FAL.1/Circ.3 riktlinjer för cybersäkerhet i marina miljöer/sjöfart (för klassade farkoster och plattformar). DNV-RU-SHIP Pt.6 Ch.5 och Lloyd's Register Cyber Safe for marine (utgår båda från IMO:s riktlinjer och är bägge baserade på ovan IEC 62443 3-3)
  - MSB:s rekommendationer för industriella kontrollsystem samt IoT och cyberfysiska system (kritisk infrastruktur). Livsmedelsverkets rekommendationer, som utgår från MSB:s ditto, används vid tillsyn av tillverkning och distribution av t.ex. dricksvatten
  - ENISA:s rekommendationer om IoT/moln/kritiska infrastrukturer och utveckling av dessa (industri och kritisk infrastruktur)
  - SKR:s/RISE:s KLASSA för IoT
  - SKR:s Informationsäkerhet inom fastighetsområdet & IoT
  - SKR:s Informationssäkerhet i fastighetsorganisationen
  - SKR:s Vägledning för IoT-tjänster
  - ioXt Alliance (certifieringsprogram för säkra IoT-produkter)
  - SSNF:s Robust och säker IoT (stadsnät)
  - Traficon (finska transport och kommunikationsnät)
- **Best practices med mera** – exempel är följande:
  - GOV.UK (Consumer IoT Security)
  - IoT Security Foundation – sök på global webbplats under "Publications"
  - OWASP IoT Verification Standard (råd för att utveckla säker programvara och de vanligaste bristerna som utnyttjas av hackers)

- Cloud Security Alliance (moln och IoT) – sök på globala webbplatsen under "research"
- IBM (moln och IoT) – sök på global webbplats efter best practices och andra råd
- Microsoft (moln och IoT) - sök på global webbplats efter topp-10 listor och best practices
- Google (moln och IoT) – sök på global webbplats efter best practices
- IoT Security Insititute (för smarta städer och kritisk infrastruktur)

3.2.2 Praktiska funktionella och miljörelaterade krav med bäring på cybersäkerhet

Funktionella och miljörelaterade krav på en IoT-produkt har ibland ingen relation till annat och kan då ses som fristående och blir då lite enklare att hantera. Det finns dock många av dessa krav som har relationer till annat och då till exempel cybersäkerhet. För att enklare klara av dessa senare relationer kan som tidigare nämnts tankegångar om modularisering, användning av standardiserade komponenter och micro-services vara till hjälp när man bryter ned dessa kraven.

Funktionella krav har med vad IoT-produkten behöver kunna göra och helst bör dessa vara praktiska och väl utformade så hanteringen under livscykeln blir effektiv och livscykelkostnaden så optimerad som möjligt. Att göra funktionella krav som i praktiken blir komplicerade och dyra senare, till exempel att service och underhåll inte är genomtänkt, gör att många kunder och deras användare kommer att dra sig för att köpa mer eller ersätta IoT-produkter vars livscykel är slut från den leverantören. Ett dåligt exempel på detta är nya bilar där det i många fall knappt går att byta en lampa själv.

Olika praktiska funktionella och miljörelaterade krav är till exempel:

Driftsmiljö – driftsmiljö påverkar utformningen av en IoT-produkt både vad gäller utvändigt skydd kombinerat med cybersäkerhet. En tuff industriell miljö ställer sina krav liksom om en IoT-produkt kommer finnas mer eller mindre obevakad och oskyddad i drift utomhus, inne eller utomhus i hemmiljöer. Således kan likväl fysiska angrepp som cyberattacker leda till otillgänglighet eller förstörelse i utsatta miljöer. Fysisk åtkomst kan även leda till risk för cyberattacker genom att koppla in sig genom oskyddade gränssnitt eller att kunna skruva bort en lucka och få åtkomst till kontakter eller kunna byta ut ett minneskort där.

Hårdvarukrav – ofta finns även i vad som kan tyckas vara säkra miljöer ett behov av att skydda IoT-produkten från fysiskt intrång/åverkan alternativt vara öppningsbar. Det minsta som kan tänkas behövas är att exempelvis ha ett sigill eller klisterlapp på eventuella öppningsbara luckor över minneskort och insida med kontakter. Ett alternativ är att rekommendera att IoT-produkten bör installeras i helt kontrollerad miljö med lås runt (såsom i låst rum eller bur/skåp). Att bara ha en enkel plastkåpa som enkelt kan forceras och det tar lång tid innan något intrång upptäcks är tyvärr inte ovanligt. Här kan man ha en inbyggd funktion som larmar och eventuellt tar IoT-produkten ur drift vid fysiskt intrång eller åverkan (om den kan användas som väg in för vidare cyberattacker). IoT-produkter som är oskyddade och utsatta bör sitta i ett nätverk som helst inte är inkopplat i huvudnätverk. Exempel på dylika är uppkopplade motorvärmare och yttre larmsystem, yttre elektroniska låssystem utan bevakning med mera.

Miljörelaterade – det är tänkvärt att se över möjligheten att kunna byta ut slitna delar i hårdvara eller fräscha upp dem igen så det går att fortsatt använda (så kallad "re-furbishing" eller "re-manufacturing") i IoT-produktens resterande livscykel. När den primära livscykeln är slut för en IoT-produkt går det ofta att hitta en ny livscykel i andra sammanhang med lägre krav, för att undvika avveckling och skrotning (så kallad "re-purposing" eller "down-cycling"). Dock bör IoT-produkten tömmas och rensas på data och information samt konfiguration innan den

avvecklas från en livscykel och eventuellt fortsätter sitt liv i en ny.

Informationsflöden – under livscykeln kommer en mängd data och information troligen flöda genom IoT-produkten och det bör tänkas igenom var och hur dessa skall lagras samt då hanteras cybersäkert. Tidigare nämndes ett förslag på att dela upp data och information som berör personuppgifter, process och kvalitetsdata, samt underhåll och "fleet management" för att underlätta transparens rörande: vem som äger data, vem som får göra vad med data när och hur. Användning av molntjänster och leverantörens egen lagring gör detta mer komplicerat att komma överens om än om lagringen sker hos användare hos kunden i ett datalager eller lokal server. Hur som helst finns mycket intressant affärsutveckling att göra nu och framöver med data och information, varför detta kan vara bra tänka igenom extra mycket.

Interoperabilitet och kompatibilitet – hur behöver IoT-produkten passa in i olika objektägares användarmiljöer och vilka krav kan dessa komma att ställa på designen? Detta kan innebära följande för designen: hur vi får ut data/information genom nätverk och brandväggar, hur ska data/information lagras/delas säkert, vilka dataformat och kommunikationsprotokoll behövs, ska data/information kunna exporteras till olika format förutom att backup och återställning (import) ska kunna göras enkelt, hur ska de som behöver eventuellt kunna koppla upp sig utifrån – och vilken funktionalitet behöver de ha tillgång till, med mera.

Kunnande i driftsmiljö – om IoT-produkten är enkel så bör kunnandet i driftmiljön klara av den efter lite utbildning. Om IoT-produkten och dess funktion är mer komplex så kan det finnas behov av extrahjälp från leverantören eller någon annan i värdekedjan. Då kan man tänka igenom, beroende på kontext, om support och service kan ske från distans via cybersäker uppkoppling eller om det behöver ske på plats. Även utbildningar kan vara bra att ha. Vidare kan externa vara med på cybersäker videolänk eller att en virtuell/utökad verklighetsmiljö (VR/AR) tas till hjälp iför att prova och träna med innan åtgärder sker på riktigt.

Cybersäkerhet i distributionskedjan – hur ska IoT-produkten och dess delar kunna enkelt och effektivt distribueras till användare hos kunder vid första leverans och sen under fortsatt livscykel utan att IoT-produktens fysiska eller logiska innehåll komprometteras? Tänk igenom detta och säkerställ att IoT-produkten eller reservdelar och komponenter är intakta vid ankomst till kund och användare.

Effektiv installation, konfiguration och driftsättning – här kan mycket tid och resande sparas om detta tänks igenom. Denna process, som oftast har flera steg, behöver vara cybersäker. Tänk igenom om det går att automatisera delar eller hela steg genom att utveckla så kallade "fleet management" funktioner med plug-and-play, autokonfiguration av lokala inställningar och nätverksuppkopplingar utifrån färdiga centrala inställningar som hämtas, och automatisk eller manuell driftsättning. Det går att göra väldigt mycket här och kostnadsbilden för en kund och användare med många IoT-produkter blir mycket attraktiva om detta finns automatiserat. Fördelen med central styrning, eller "fleet management", är att det blir färre fel och enklare att ändra många snabbt vid behov.

Cybersäkerhet under eventuell drift och underhållsfas – IoT-produkten behöver vara designad för att på ett cybersäkert vis kunna driftas och underhållas till dess att livscykeln tar slut. Normalt sett krävs data och information om process och kvalitetsutfall samt underhållsbehov för att göra detta någorlunda optimerat, men IoT-produkten behöver också designas så detta sen kan utföras effektivt på plats eller från distans (det som går att göras på håll) i kombination med det som automatiserats.

Cybersäkerhet vid slut av livscykel – IoT-produkten och dess beståndsdelar behöver vid någon punkt kunna skrotas och tas bort utan att IPR, data och information (inställningar, recept/programmering, annan driftsinfo såsom IP-adresser med mera) läcker ut till obehöriga. Här kan med fördel en "fleet management" funktion för detta finnas så att när den stängs ned och tas ur drift så görs även borttagning av IPR, data och information. Om sedan en fysisk destruktion behövs måste bestämmas av kundens policys och användaren, men leverantörer bör ha med en instruktion om hur detta bäst görs såvida inte det finns ett så kallat producentansvar för återvinning och destruktion. Vid producentansvar bör det finnas en instruktion så att destruktionen blir väl genomförd.

3.2.3 Generella cybersäkerhetskrav för IoT-produkter

Varje IoT-produkt och de kontexter där de kommer användas ställer specifika krav på cybersäkerheten. Detta behöver analyseras och diskuteras med kunder och användare samt att världen runt omkring förstås då allmän hotbild, krigstillstånd, lagar och regleringar påverkar detta. För att få en viss inblick i vad som kan kallas generella cybersäkerhetskrav, kommer vi använda den struktur som standarden IEC 62443 del 3-3 och dess säkerhetsnivå 1 (av 4 och där 4 är högsta) har. En bransch som kommer ha tvingande krav för kritiska och miljöpåverkande "komponenter och system" som baseras på detta är sjöfart/marint med klassningskrav. Detta gäller för kontrakterade nybyggnationer och installationer från 1-jan 2024.[9] Det är inte helt otroligt att andra branscher även på land kommer att ta efter och i annan transport, luft och rymd finns redan vissa reglerade cybersäkerhetskrav.

I IEC 62443 del 3–3 och dess lägsta säkerhetsnivå 1, som enkelt kan uttryckas berör cybersäkerheten i "komponenter", finns ett antal grupper med krav som påvisas nedan. Observera att detta enbart är ett exempel för att visa vad som faktiskt redan finns framtaget, för främst professionella miljöer, och vad som kan certifieras mot

[9] Se på webben om IACS UR E26/E27 - https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/

SYSTEMADMINISTRATION UTFÖRS AV EN SPECIALIST.
BILD AV EN IT-TEKNIKER SOM GÖR INSPEKTIONER I ETT DATACENTER.
FOTO: ADOBE STOCK.

om behov finns för det. För mer kritiska miljöer kan de ännu mer krävande säkerhetsnivåerna 2–4 vara aktuella. I Sverige finns för olika branscher vägledningar och kravsamlingar (se till exempel MSB:s och SKR:s skrifter i kapitel 10 och sektion 3.2.1) som kan ge bra grund. Nedan kan man läsa om innehållet i säkerhetsnivå 1 och sen betänka vad som är relevant för sammanhanget och vad som behövs i vilket fall.

Innehåll i säkerhetsnivå 1:

- Identifiering av användare
- Autentiseringsnivåer och vilken nivå på autentisering som olika användargrupper eller roller har (användare med rätt att enbart se, användare med rätt att ändra, administratör). Vidare kan administration från ett osäkert eller externt nät kräva två- eller multifaktorinloggning.
- Identifiering och autentisering av mjukvaruprocesser och enheter
- Användarhantering
- Användargrupper/roller
- Kunna ändra och styra autentiseringsmetod
- Kunna styra trådlös access
- Krav på att kunna ändra styrka/längd i lösenord och hur lösenord vid inloggningar ska synas eller ej
- Kunna styra hur ej lyckade inloggningsförsök hanteras (hur många får göras, temporär låsning eller ej, att bara adminkonton låses och behöver låsas upp, styra läng på timeouts innan nya inloggningsförsök kan göras efter ett visst antal har gjorts under en viss tidsperiod)
- Kunna styra och ändra systemmeddelanden
- Kunna tillåta eller ej tillåta access från ej betrodda/osäkra nätverk

- **Styrning och kontroll av användning:**
  - Krav på auktorisation (vad de har rättigheter att göra) för mänskliga användare enligt princip om uppdelning av ansvar och minsta möjliga rättigheter
  - Kontroll/styrning av trådlös användning
  - Kontroll/styrning av eventuell användning av portabla och mobila enheter (i uppkoppling mot IoT-produkten eller dess nätverk)
  - Kunna begränsa användning av farlig mobil kod (till exempel java script, ActiveX, PDFer med mera)
  - Kunna låsa sessioner (tidsbaserad eller användarstyrd)
  - Kunna avsluta eventuella uppkopplingar från distans (per tid, inaktivitet, eller från användare som till exempel trycker på knapp)
  - Kunna manuellt godkänna eventuella uppkopplingar från distans samt kunna avbryta dylika
  - Kunna ha auditloggning (tidsstämplade, vad är relevant och behövs loggas enligt krav från lag, standarder eller objektägare hos kunder)
  - Ha tillräckligt lagringsutrymme för auditloggar (beror på mängd och tidsdräkt)
  - Kunna styra vem som får komma åt auditloggar och se till att de är skyddade (och inte kan ändras av vem som helst)
  - Åtgärder vid fel på auditloggning – vad skall göras och vad måste göras för att påkalla uppmärksamhet?
  - Tidsstämpling av varje enskild logg
- **Systemintegritet:**
  - Integritetsskydd av kommunikation i nät som ej är tillräckligt skyddade (så ej det som kommuniceras kan ändras utan att det märks)
  - Skydd mot skadlig kod (överallt eller på ingångs-/utgångspunkter)
  - Kunna verifiera att säkerhetsfunktionalitet fungerar (det vill säga ha funktioner, procedurer, script eller liknande som kan köras för att påvisa att det fungerar som det ska)

- Validering av indata
- "Fail-to-safe"-funktionalitet om normal drift ej fungerar på grund av en cyberattack (och då kan återgå till ett felsäkert tillstånd)
- Ha integritetsskydd av sessioner (till exempel med unika sessions-ID för varje session)

- **Datakonfidentialitet:**
  - Skydd av kommunikationens och lagringens konfidentialitet (med hjälp av kryptering)
  - Aauktorisation för åtkomst/läsning
  - Krav på uppdaterade och tillräckliga krypteringsalgoritmer, nyckellängder, certifikat samt processer för hantering av nycklar och certifikat
  - Möjlighet att kunna uppgradera algoritmer och nycklar med mera om/när högre krav kommer
- **Begränsa dataflöden:**
  - Kunna ha segmenterade nät (logiskt/fysiskt eller bägge) där IoT-produkten skall driftas
  - Kunna ha zonskydd med möjlighet att övervaka och kontrollera kommunikationen vid segmentets gräns (kompartimentalisering) och ha "deny-by-default and allow by exception" samt skall vara möjligt att kunna manuellt stoppa kommunikation mellan olika zoner liksom möjlighet att kunna köra i "island mode"
  - Kunna hindra "peer-to-peer" kommunikation eller liknande lösningar (bara godkänd kommunikation inom lösning och in/ut ur segment)
  - Kunna ha partitionering av applikation/tjänster/data (för att få oberoende och skyddade zoner)
- Svarstider vid händelser:
  - Kunna ha auditloggar som ska kunna läsas (read only) av auktoriserade användare (människa eller verktyg)
- **Tillgänglighet till resurser:**
  - Kunna ha skydd mot DOS-attacker eller liknande problem – IoT-produkten skall kunna fungera i begränsad utsträckning även under en dylik attack
  - Resurshantering – IoT-produkten ska kunna reservera tillräckliga systemresurser till säkerhetsfunktioner för att förhindra att alla resurser är upptagna/maximalt utnyttjade av övrig funktionalitet
  - Backup-funktionalitet – backup av all kritiska data och auditloggar ska kunna göras utan att påverka normal drift (samt lagras på plats som är tillgänglig men ej on-line, det vill säga "de-linked")
  - Funktionalitet för återställning och återstart – IoT-produkten skall kunna återställas och återstartas till ett känt säkert tillstånd efter avbrott eller fel
  - Vid höga krav på tillgänglighet ha nödström (det vill säga ha mer än en strömkälla tillgängligt och även likaså mer än ett uttag för strömkabel) – och ett byte av strömkälla skall inte påverkar IoT-produktens säkerhetsfunktionalitet
  - Kunna konfigurera och ändra inställningar av nätverk och säkerhetsnivå – IoT-produkten skall kunna konfigureras (via gränssnitt) så dess nätverks- och säkerhetsparametrar överensstämmer men rekommenderade nivåer från leverantören (kan ske lokalt eller centralt via molntjänst)
  - Tillämpa minsta möjliga funktionalitetsprincipen – onödiga funktioner/tjänster, portar, protokoll med mera skall göras oanvändbara (disablas), förbjudas eller tas bort från IoT-produkten

Om IoT-produkten har, eller ansluter till, en molntjänst eller server på annat ställe som används för datalagring, "fleet management", uppdateringar, rapportfunktion, optimeringsfunktion med mera, tillkommer fler krav för att skydda dessa. Om dessa finns tillgängliga via

Internet kan man få en överblick på cybersäkerhetskrav och risker från Cloud Security Alliance, Microsoft, IBM med flera.

Vidare kan det finnas behov av att kunna styra vilka mjukvaror som får exekvera på IoT-produkten (enheten) via secure eller trusted boot och ”chain of trust” från hårdvara, via operativsystem och till appar. I sådana fall kan det vara viktigt att ytterligare härda sin plattform genom så kallad “Secure boot”. Det är en metod som är utformad för att säkerställa att en enhet endast kör pålitlig programvara. Detta görs genom att verifiera integriteten hos programvaran som laddas under uppstartsprocessen. Secure boot implementeras vanligtvis som en del av en IoT-produkts uppstartsmjukvara, och den fungerar genom att använda kryptografiska nycklar för att verifiera äktheten av programvaran som laddas. Nycklarna lagras helst säkert i en hårdvarumodul (till exempel en ”trusted platform module” (TPM)). När IoT-produkten startas kontrollerar uppstartsmjukvaran (boot firmware) signaturen för starthanteraren (bootloader) mot de lagrade nycklarna. Om signaturen är giltig tillåts starthanteraren köras. Starthanteraren upprepar sedan denna process för operativsystemet och all annan programvara som laddas. Secure boot hjälper till att förhindra att skadlig programvara läses in på en IoT-produkt, eftersom den säkerställer att endast pålitlig programvara kan köras. Detta kan hjälpa till att skydda mot skadlig programvara, bootkits och andra typer av hot som är beroende av att kunna exekvera kod på en enhet (IoT-produkten).

Det finns som sagt var en hel del redan färdigt att fundera över och bestämma vad som är aktuellt för IoT-produkten som skall utvecklas (eller förbättras om befintlig). Man behöver inte själv komma på allt och man kommer långt genom att läsa igenom och fundera över det som redan finns skrivet.

3.3 Ledningens ansvar – vilka saker behöver redas ut?

Vissa saker behöver ledningen hos organisationen som utvecklar IoT-produkten ta ansvar för och tillse att de som är med i värdekedjan är med på (vilket inkluderar kunder och deras

CYBERSÄKERHETSKONCEPT IDENTITETSSTÖLD, CYBERBROTTSLIGHET PÅ INTERNET. FOTO: ADOBE STOCK.

användare) för att IoT-produkten ska kunna fungera bra på både kort och lång sikt med god cybersäkerhetsnivå. Det är svårt för en utvecklingsgrupp att jobba med många parter i en värdekedja om krav som går över organisationers gränser, så här behöver ledningen reda ut detta för att undvika dyra och osäkra överraskningar senare.

Vissa krav påverkar alla inblandade, och kallas ibland holistiska krav som skär rakt igenom, och innebär att viss infrastruktur behöver finnas eller befintlig göras interoperabel eller kompatibel samt att vissa processer och uppsättningar av tillgångar/utrustning behöver göras på standardiserat vis. Exempel på tillgångar/utrustning är då IoT-produkten, molntjänst(er), certifikatinfrastruktur med rotcertfikat och revokeringslistor, "federering" av användaridentiteter (kunna använda en identitet för att logga in på flera ställen såvida organisationerna litar på varandra och lägger till användaren hos sig också) och access med mera.

Ledningen behöver även börja tänka mer i total livscykelkostnad istället för initial utvecklingskostnad. Detta gör att kravinsamling, beslut och design kan ge högre initial kostnad men betala sig tillbaka ordentligt senare i IoT-produktens livscykel. De långsiktiga besparingarna kan då komma från att IoT-produkten redan har förberetts och att ledningen har tänkt till inför framtida utveckling och arkitekturbeslut. Användning av designprinciper i kravanalysen kan bidra till ett bättre totalt resultat.

3.4 Cybersäker utvecklingsmiljö och utvecklingsprocess

Två bra frågor att ställa sig är:

- Vad har vi för IPR som är skyddsvärd?
- Varför ska vi anstränga oss och utveckla IoT-produkter om andra bara kan förstöra allt sen genom att ta ritningar, underlag, beskrivningar av tjänster och processer eller strukturer, koden eller plantera in virus eller elak kod alternativt design?

Om frågorna ovan är relevanta behöver fler frågor ställas och de berör vad som ingår i utvecklingsmiljön (utveckling, test och dokumentation) och vem som får komma åt vad och sen göra vad med:

- Vem ska få komma åt olika delar i utvecklingsmiljön (på plats eller från distans) och använda vilka verktyg?
    - Vilka ska få komma åt utvecklingsmiljön och vilka verktyg får de använda i den?
    - Behöver alla kunna komma åt programkoden, hårdvarudesign eller tjänstdesign, om sitter utanför organisationens nät, utanför arbetstid 8-19 på vardagar?
    - Ska man kunna komma åt utvecklingsmiljön från andra länder än Sverige (och det går att öppna upp särskilt för ett tag vid behov)?
    - Vilka har rätt att checka ut all kod och vilka kan checka in kod i "huvudträdet" eller göra ändringar i ritningar?
    - Krav på "code review" eller "design review" innan kod, ritningar eller tjänste- och processbeskrivningar får checkas in i huvudträdet.

- Behövs specifikt skydd av utvecklingsdokumentation och annat material som produkt-/tjänste-/processdokumentation, IPR/ritningar, produktionsprocess/metod (om klassas som konfidentiellt eller strikt konfidentiellt)?
- Vad finns för cybersäkerhetskrav på samarbetsverktyg – kommunikation och delning av dokument med mera, skyddsnivå för dokument, krav på autentiseringsnivå med mera?
- Det behöver göras ett val av lämplig utvecklingsprocess/metodik för problemet som skall lösas samt att få med cybersäkerhet från första början till slutet. Man bör dock ha en utvecklingsprocess som ser till att ha en bra kravbild innan man kör igång utvecklingen så att man undviker dyra misstag. Kravbilden kommer liksom i de flesta projekt säkerligen utvecklas under gången och någon form

av ändringshantering behöver finnas med i processen. Att använda samma utvecklingsprocess/metodik till alla problem ger kanske inte bästa slutresultatet, så det kan vara bra att ha kunnande och erfarenhet av flera särskilt för IoT-produkter som potentiellt involverar hårdvara, mjukvara, tjänster, processer, moln, kommunikation och dataanalys.

- Vad skall ställas för krav på utvecklingsprocessen/metodiken? Den bör kunna ha med ett flertal parallella delprocesser och ändå samtidigt koordinera dessa så de inte går i otakt och en delprocess stänger designrummet för de andra på grund av designval som de gör. Här kan man tänka att ha ett antal parallella delprocesser för: hårdvara, mjukvara (lokal och i moln/hostad), tjänster och processer (allt från support/underhåll till optimeringstjänster baserade på data), "management of operation" (bygga upp de strukturer och infrastruktur som IoT-produkten behöver ha för att fungera på lång sikt och även förbättra prestanda och tillgänglighet). Bra är att få med det som är relevant från start och undvika dåliga (eller omöjliga) påbyggnader senare.
- Vilka krav ställs på utvecklings-/testmiljö och val av testdata i övrigt?

Det är alltid på sin plats att styra upp både fysisk säkerhet och cybersäkerhet runt utvecklingsmiljöer. Att utveckla något och lägga mycket tid och medel för att sen se någon annan komma ut med något liknande väldigt nära inpå är inte särskilt upplyftande och särskilt inte om man vet att det är vi som utvecklat och bekostat det.

De som utvecklar tjänster, processer och andra strukturer som behövs kan med fördel använda samma utvecklingsmiljö som de som utvecklar hård- och mjukvara, för att få kontroll på access, behörigheter, vem som får göra ändringar, versionshantering och backup på allt som tas fram.

3.5 Dokumentationskrav – olika handledningar och manualer

Att ha med cybersäkerhet i dokumentationen för IoT-produkter behövs och missas i många fall. Detta är även nödvändigt om en IoT-produkt skall certifieras, men en god idé i alla kontexter från hem till kritisk infrastruktur.

En bra och väl avvägd dokumentation för cybersäkerhet kan innehålla:

- IoT-produktens funktion beskriven. Ha en bra bild över "hela systemet" och hur cybersäkerheten (och eventuell fysisk säkerhet runt i kring) skall vara uppsatt på schematiskt vis. Vilka roller kommer logga in var och vad kommer de utföra?
- Rekommendera cybersäkring av driftsmiljö hos kund och användare – hur kan den se ut? Behövs det ett eget fysiskt och logiskt nätverkssegment med relevant skydd (brandvägg/gateway med databuffring) eller är det bara en delkomponent i annat system?
- Vad gäller om IoT-produkten inte körs i en rekommenderad miljö – ansvarsfrågor?
- Hur görs en cybersäker installation, konfiguration och driftsättning?
- Hur ska data eventuellt skickas ut?
- Behöver kunden och användare göra brandväggsöppningar (vilka portar, protokoll m.m. behövs) och vilka krav på autentisering och säker kommunikation ställer IoT-produkten? Detta är bra att dokumentera och förklara. Om tvåfaktorsautenticering eller annan form av multifaktorsautentisering är ett krav för till exempel administratörer så kan detta kräva att det görs en installation eller faktorer köps in.
- Hur kan man verifiera att IoT-produktens cybersäkerhet är rätt uppsatt och konfigurerad – finns det en särskild funktion, procedur eller annat sätt att verifiera? Detta är för övrigt ett vanligt krav i många certifieringar.

EN BRA DOKUMENTATION AV CYBERSÄKERHETEN GER BÄTTRE STÖD VID INSTALLATION, KONFIGURATION OCH UPPDATERINGAR AV IOT-PRODUKTER.
FOTO: ADOBE STOCK.

- Kommer support och underhåll ske på distans via Internet eller annat nätverk? Går det bygga in underhålls/uppdateringsfunktion i IoT-produkten, som initieras när IoT-produkten kopplar upp sig mot till exempel en molntjänst och lämnar data, samt då även hämtar konfigurationsändringar? Ett annat alternativ är att ha en ha VPN-uppkoppling utifrån som är godkänd av kundens policys.
- Ska cybersäkert underhåll/service ske på plats? Det gäller att inte kompromettera cybersäkerheten och föra in virus eller malware vid uppdatering av mjukvara eller som kommer in om en extern bärbar dator, mobil eller USB-disk ansluts. Här behövs processer (som ser till att inga virus eller malware kommer med) och utbildning av de servicetekniker som utför underhåll och service på plats.

Således, att ha en bra dokumentation med cybersäkerheten beskriven ger bättre stöd vid installation, konfiguration och uppdateringar under livscykeln. Dessutom slipper supporten många frågor och kan spara tid över till det som kräver en supportteknikers fulla uppmärksamhet.

Vid slutet av livscykeln, eller dess användning hos en kunds objektägare, så behövs instruktioner för hur IPR och annan information/data kan tömmas och ersättas med till exempel fabriksinställningar eller intetsägande innehåll. Det är även bra om det finns en funktion för detta och att den som utför detta får en bekräftelse på att IPR och informationen verkligen är borttagen och ersatt med annat. Till detta behöver det finnas en instruktion för hur eventuell återvinning skall göras. Observera att detta gäller alla ställen där IPR och information finns lagrad, vilket inte bara inkluderar själva IoT-produkten utan även molntjänster eller serverdelar och olika steg i överföring av data. Användare hos en kund har troligen en IT- och OT-policy som reglerar hur de ska rangera ut och avveckla olika tillgångar från IT- och OT-miljöer. Ibland krävs destruktion av minnen och diskar och andra delar, med högt IPR-intresse från konkurrenter och andra parter, helt och hållet.

TESTNING AV EN IOT-PRODUKT ÄR VIKTIG BÅDE FÖR FUNKTIONENS SKULL OCH ATT CYBERSÄKERHETSNIVÅN ÄR BRA.
FOTO: ADOBE STOCK.

3.6 Testkrav

Testning av en IoT-produkt är viktig både för funktionens skull och att cybersäkerhetsnivån är bra. Det går att planera, beroende utifrån kompetens och kunnande, så att utvecklare och testare samarbetar och att vissa saker byggs in i utvecklings- och testmiljön (vilket kan kräva en hel del utveckling). Således kan olika former av automatiserade tester och testriggar med mera krav som bör ingå i kravspecifikationen redan från början, och att dessa sedan är fortsatt med under livscykelns vidareutveckling och förfinas och byggs vidare. Vidare bör funktionella krav liksom cybersäkerhetskrav vara testbara.

Olika typer av tester behöver sättas samman för att få en slutligt bra IoT-produkt. Nedan finns ett antal exempel på möjliga testkravsgrupper, vilka kan vara bra att utveckla i en testspecifikation och plan för att få till en så bra täckning som möjligt:

- Planering och översikt av testtäckning – kommer IoT-produkten att innehålla olika konfigurationer av hårdvara, mjukvara, och eventuell molntjänst/server eller andra tillhörande tjänster?
    - Hur stor testmatris behövs för att få bra täckning?
    - Portering till olika plattformar – skiljer sig plattformarna eller är de snarlika?
- Funktionstest
- Testning och genomgång av eventuella tillkommande tjänster, processer och strukturer
- Tester för att tillse att funktionerna (och tjänster, processer och strukturer) är cybersäkra
- Prestanda och skalbarhet
- Dokumentationstest – är dokumentationen komplett och korrekt
- Testautomation – testsviter för cybersäkerhet, funktionella krav samt prestanda/skalbarhet/överbelastning
- Testriggar – vad behövs för att effektivt kunna utföra testerna? Kan testriggar ha färdiga konfigurationer som automatiskt kan ställas in?
- Penetrationstest – gärna med hjälp av extern part – kan vara en bra idé att göra med jämna mellanrum för att se om IoT-produktens cybersäkerhet kan forceras i de olika miljöer den kommer finnas i
- Sårbarhetsskanning av exponerade delar i IoT-produkten och eventuell molntjänst med mera – behöver göras över tid regelbundet och inte bara en gång
- Regressionstester efter buggrättningar/ändringar. Vid användning av testautomation och testriggar går detta mycket snabbare

Penetrationstester och sårbarhetsskanningar bör vid upptäckt av problem generera ett krav till utveckling eller hanteras på annat vis via underhållsuppdateringar. Att på ett bra sätt automatisera testningen gör att testning går snabbt, man kan köra den många gånger och i stället använda testare till att fokusera på testning som är svår att automatisera. Detta gör att man kan få en bra testtäckning och hinner göra mycket tester under en utvecklingsprocess. Om en organisation använder en plattform för att bygga IoT-produkter på, så kan en del av testarna fokusera och testa plattformens grundfunktioner så att de som testar IoT-produkterna kan fokusera på dessa och inte underliggande plattformen. Det finns flertal bra publikationer att läsa om utveckling av säkra gränssnitt och API:er samt de stora molnföretagens och OWASPs top-10-listor ger både utvecklare och testare bra indata till testfall och automatiserade tester genom de vanligaste problemen, svagheterna och cyberattacker som sker.

3.7 Underhållbarhet över tid
– planering för uppdateringar, uppgraderingar och migrationer

Den oftast längsta fasen i en IoT-produkts livscykel är när den är installerad och driftsatt hos kunders användare ända tills den avinstalleras och eventuellt avvecklas eller får ett fortsatt liv någon annan stans. Att ha en IoT-produkt som på ett effektivt och cybersäkert vis går att ge support, underhålla och uppdatera är inte bara en konkurrensfördel utan ren självbevarelsedrift om värdekedjan skall kunna vara lönsam och IoT-produktens totalkostnad intressant för alla. För att klara av detta kan ett utbildningspaket behöva utvecklas för både internt och externt bruk. Utbildning för externt bruk åt användare hos kunder kan ju även ses om en tilläggstjänst. Om det är en hög omsättning på anställda blir utbildningspaket ännu viktigare.

Att underhålla något är inte helt enkelt och behöver tänkas igenom så det blir både effektivt och cybersäkert för den kontext som är aktuell. Om IoT-produktens arkitektur har både hårdvara, mjukvara i olika former och nivåer, ingående mjukvaruplattform, en molntjänst/server och olika typer av tjänster och processer som kan vara manuella eller automatiserade och utföras på plats eller från distans, så innebär det en viss komplexitet och krav på underhållbarhet.

För att få IoT-produkten att fungera väl under sin livstid behöver man antingen från början tillse att den har tillräcklig kapacitet i hårdvara vad gäller processorkraft, minne och lagring för att kunna lägga till och uppgradera firmware, operativsystem, plattformar och paket som används, open-source som växer och applikationskod. Nya utökade krav på cybersäkerhet, vilka tillkommer med jämna mellanrum, leder med stor sannolikhet till att hårdvaran kommer behöva klara mer eller ansenligt mer än från början. Ett alternativ är att i hårdvaran ha utbytbara moduler, men då återstår problemet att ha tillräckligt av dessa utbytesmoduler när de sen väl behövs. Många tillverkare slutar efter några år göra gammalt för att fortsätta med nytt. Detta behöver planeras för och att köpa in en hårdvara som precis klarar sig i början kommer troligen att skapa mer problem och kostnader än om man hade tagit i lite mer från början.

Till inspiration, från framför allt mekanisk/elektronik produktutveckling, finns tanken om “design for maintenance” tillsammans med en mängd andra dylika “design for X”-koncept såsom “design for manufacturing”. Om det är svårt och komplext att planera och genomföra underhåll och uppdateringar så kommer det bli onödigt dyrt och IoT-produkten tappa i konkurrenskraft. Är underhåll och uppdateringar lätt och snabbt att utföra så blir ju även stillestånd kortare (om det inte finns redundans som ger kontinuerlig drift).

Något som ofta glöms bort i tidig IoT-produktutveckling är data och information som genereras och sparas under lång tid. Vilket dataformat ska användas, hur ska man kunna ta ut data och flytta det till en annan leverantörs molntjänst/server om objektägare hos kunden (det vill säga avtalsparten) äger denna data och i framtiden önskar flytta det? Att då komma och kräva extra betalt kommer inte ge pluspoäng eller snälla kommentarer när kollegor i branscher träffas och diskuterar på mässor och konferenser. Har IoT-produkten däremot bra dylika funktioner för migration från ett dataformat till annat och att de går ta ut data och flytta över (med hjälp av meta-data) till annan miljö - då lär beröm ges.

3.8 Kvalitetsnivå och vad påverkar denna

En IoT-produkts kvalitetsnivå påverkas av många saker i förhållande till de förväntningar användare hos kunder har och till vilket pris den säljs för. I handboken är en IoT-produkts livscykel central och därför bör man tänka att kvaliteten behöver kunna hållas på en bra nivå, över användarens förväntan, ända tills livscykeln är slut. Alltså är inte kvalitetens nivå efter installation och driftsättning det avgörande om den snabbt faller undan på grund av dålig underhållbarhet och

ineffektivt eller för sent underhåll och uppdateringar. Cybersäkerheten, som är nära kopplad till underhåll och ibland tidskritiska uppdateringar, är en del i kvalitetsnivån och ifall cybersäkerheten är för låg så diskvalificeras användningen i många kontexter.

Även ett svagt ägandeskap hos objektsägare och ingen underhållsbudget i kundens förvaltning påverkar kvalitetsnivån snabbt på en IoT-produkt (ifall den har behov av underhåll och uppdateringar med mera). Det finns tyvärr många IoT-produkter och andra produktionstillgångar som lever ett kärvt liv med dålig uppmärksamhet och omtänksamhet och förfaller snabbt och kan då orsaka störningar i produktions- eller distributionsprocesser alternativt annan typ av verksamhet. Likaså kan en försummad IoT-produkt innebära att sårbarheter finns kvar länge och i värsta fall utnyttjas av någon form av hot och orsakar störningar, läckage av data eller oönskad kryptering av data/information med mera.

På samma vis som en objektsägare inte tar hand om en IoT-produkt kan en produktchefs svaga ägandeskap snabbt förpassa en IoT-produkt från att vara ett premiumval till att vara bland de på sista plats när inköp skall göras och som enbart kan konkurrera med ett lågt pris.

3.9 Industrialiseringskrav

Att industrialisera, eller förbereda en IoT-produkt för mer eller mindre storskalig produktion, och sen ha resterande värdekedja som behövs för att tillföra värde till användare hos kunder är inte helt lätt. Det är faktiskt ganska svårt att göra helt rätt från början och det gäller att prova sig fram tills det blir helt bra. I denna delen kommer det finns många led och tillfällen där en IoT-produkt är blottlagd från sitt innersta, och detta behöver styras upp med hårda krav på både fysisk säkerhet, cybersäkerhet och att tekniker och produktionsarbetare är pålitliga. Om det är många inblandade så är detta inte lätt och frågan som man behöver ställa sig är vad som en organisation ska göra själv och vad andra i en värdekedja kan göra bättre och effektivare utan att riskera den IPR som tagits fram och nu skall ut till användare hos kund i slutlig form. Om för många har tillgång till något känsligt eller hemligt så är det inte så länge till oftast. Ytterligare frågor är om värdekedjan kan vara utanför Sverige och EU av både säkerhets- och cybersäkerhetsskäl samt beroenden till leveranser som kan bli fördröjda och på så vis skapa stora leveransproblem.

I kravanalysen bör det finnas med någon form av “design for manufacturing”-krav så att IoT-produkten är så rättfram och enkel att tillverka, sätta ihop, samt kvalitetstesta efter (innan slutgodkännande) exempelvis i en testrigg och/eller testsvit. Att manuellt testa ett fåtal såsom exempelvis 3 av 1000 är inte en bra strategi utan bättre automatisera testning så att alla testas istället. Då vet man att allt som går till användare hos kund är OK. Vid små handgjorda volymer är inte automatiseringen lika viktigt som vid stora volymer där en rationell och enkel tillverkning ofta skapar mindre defekter och således mindre kassation eller tidskrävande efteroperationer för att rätta till felen. Onödig komplexitet i tillverkning och testning kostar pengar för alla och att förenkla och automatisera ger klara fördelar och är ett måste om konkurrenter gör det.

4. Process för att som leverantör ta till sig kravbilden, få en korrekt kravbild och sen kunna verifiera kraven

I föregående kapitel finns en mängd olika grupper av krav och även specifika potentiella krav att vara medveten om och se ifall de kan tillföra något relevant och användbart. Att samla ihop krav på ett slumpmässigt vis ökar risken för att viktiga saker missas. Att ha en tydlig strukturerad process hos leverantörer (och resten av värdekedjan) som med jämna mellanrum ger en bra återkoppling till hur IoT-produkten lever upp till deras och användarnas hos kunder förväntningar är nödvändigt. Att samla in en fullständig kravbild är inte helt lätt och detta framgår ju med all tydlighet i förra kapitlet då många saker behöver tas hänsyn till och prioriteringar blir nödvändiga då vanligen antalet krav överskrider det som är möjligt få med i en utvecklingscykel. Därför är en process för strukturerad kravinsamling nödvändig och att krav som inte kommer med nu sparas och inte faller bort utan är med i processen även inför nästa större utvecklingsiteration eller mindre uppdatering/patch. För att hjälpa en produktchef och alla som arbetar med IoT-produktens utveckling kan med fördel en "road map" göras för till exempel kommande tre årens utveckling där stora krav eller ändringar visas på en tidslinje. Denna road map behöver vara dynamisk och uppdateras beroende på vad som händer i teknikutvecklingen, egen vision för IoT-produkten, hos kunders användare och i omvärlden, samt kommuniceras med viktiga intressenter i värdekedjan regelbundet så de är med i planeringsförfarandet och vet vad som kan väntas. Detta kan även underlätta budgetallokering och inköpsplanering hos kunders objektägare.

Återkoppling och verifiering

Vissa branscher har utvecklat ramverk, processer eller instruktioner (och kan även ha särskilda lagar eller regleringar) för att detta ska gå smidigare och om mottagarna är en homogen grupp så kan dessa även hjälpa till med återkoppling och verifiering på road map och kravbilden då och då. Olika metoder för att få återkoppling och verifiering finns – allt från fokusgrupper med nuvarande användare, användargruppmöten med jämna mellanrum till möten med strategiskt viktiga kunder samt potentiella kunder. Exempel på användbara ramverk tas upp på sidan 80 – se bland annat för kommuner, regioner och stat samt marina användare. Troligen kommer fler branscher att göra liknande för att skapa gemensamma kravprocesser och lyfta kvaliteten på dessa. Vidare har MSB gjort en vägledning för kritiska infrastrukturer som är på rätt hög nivå men behöver vara med i bilden om detta är målgrupp för IoT-produkten. EU:s ENISA har också gjort ett antal matnyttiga vägledningar om cybersäkerhet inom IoT och automationssystem samt kritisk infrastruktur som är läsvärda för både privat och publik sektor.

Ramverk och annat i all ära, men det som behövs är ett ordentligt och gediget arbete av produktchef med flera inblandade för att ta till sig hela kravbilden och sen sålla och prioritera i den med ett tidsperspektiv framåt. Det finns inga genvägar, men däremot kan hjälp att förstå hela bilden fås bland annat med hjälp av denna handbok. Det är oftast bra att ha en gemensam process, för att få struktur, med flera inblandade som har olika ingångar när krav samlas in för att få en så bra helhetsbild som möjligt. Ensamma hjältar, oavsett om en process används eller ej, får det tufft och de hinner inte träffa alla som behöver träffas och få uppslag till kravbilden.

Offentlig upphandling

För offentlig verksamhet innebär att upphandla IoT-produkter med eventuella tillhörande tjänster att lagen om offentlig upphandling (LOU) tillämpas över en viss av EU bestämd beloppsnivå eller den egna lägre nivån som verksamheten själv bestämt. En upphandling som görs enligt LOU blir i och med sin natur svårare för leverantörer av IoT-produkter då en tät dialog med inköpare och de som faktisk skall installera och använda IoT-produkten blir svår och långsam. Således kan en nödvändig återkoppling och verifiering av kravställningen blir svår att genomföra på ett rationellt och effektivt vis inledningsvis. När väl en IoT-produkt är upphandlad och skall fortsätta att vidareutvecklas är dessa initiala barriärer inte med längre utan en tät och bra dialog kan föras mellan parterna, och alltså kan detta vara bra ha med i upphandling och avtal att så skall ske. Det är till synes lättare med standardprodukter än för mer specialiserade och där vidareutveckling behöver göras hos leverantören för att möta kraven i upphandlingen. I och med den ofta tyngre processen som LOU kräver så orkar inte alltid tyvärr mindre och små leverantörer av IoT-produkter vara med, vilket gör att större leverantörer har en fördel. Mindre och små leverantörer kan dock gå samman eller vara underleverantörer för att minska sin egen ansträngning vad gäller själva processen.

För mer konkreta exempel på kravbilder och bakgrunder i olika användarfall – se kapitel 9, på sidan 68.

VIKTIGT MED BRA STRUKTUR PÅ KRAVSTÄLLNINGEN AV CYBERSÄKRA IOT-PRODUKTER.
FOTO: ADOBE STOCK.

5. Cybersäker utveckling

Själva utvecklingen av IoT-produkt är bara en liten, men väldigt viktig återkommande fas, i en IoT-produkts livscykel. Vanligen blir det flera utvecklingscykler, för att göra förbättringar och hantera problem, med regelbundna nya versioner och uppdateringar/patchar så länge IoT-produkten genererar intäkter och går att underhålla och vidareutveckla. När inte så är läget längre brukar leverantören antingen göra det mycket dyrare att ha underhållsavtal på övertid eller göra en plan för avveckling av IoT-produkten som produktägare eller produktchef kommunicerar ut till objektsägare hos kunderna.

I utvecklingen så kan en mer komplex IoT-produkt innehålla ett antal olika delar såsom tidigare nämnt hårdvara, mjukvara på olika nivåer ("firm ware", operativsystem, applikationer, databaser med mera ovanpå), molntjänster/servers, manuella eller automatiserade tjänster som utförs på plats eller från distans samt olika processer och strukturer. Självklart kan mer ingå, men detta ställer krav på utvecklingsprocessen så att den koordinerar flera ofta parallella utvecklingsprocesser med vissa delar som behöver ha lös eller väldigt nära integration. Om inte dessa koordineras eller har tydliga kontrakt eller standardiserade gränssnitt hur de skall passa ihop eller fungera tillsammans så kommer problem sannolikt att uppstå, resultatet bli mindre bra, samt kostnaden driva iväg utan att värde skapas. Fotot nedan visar en utvecklingsmiljö med olika mät- och testverktyg för IoT-produkter med fokus på hårdvaru- och mjukvaruintegration.

Förutom att ovan behöver fungera på ett effektivt sätt så behöver det även vara cybersäkert, för varför ska vi anstränga oss och satsa massa medel om någon annan bara kan ta idéer, ritningar, mönster, kod, dokumentation, övrig IPR och patentarbete med mera eller lägga in saker i det som sen stjäl data, stör eller förstör hos kunders användare? En utvecklingsmiljö behöver skyddas och till vilken skyddsnivå beror på vad som finns i den och självklart hur mycket det kostar samt vilken vinst som kan genereras. En IoT-produkt som kan dra in någon miljon jämfört med några miljarder är det viss skillnad på, liksom om den skall köras i hemmet eller i kritiska infrastrukturer. En analys behöver göras vad som behöver skyddas, vilka är svagheter, hot och riskerna (se sektionerna 3.4-3.6 tidigare). Utifrån detta kan sen en cybersäker utvecklingsmiljö tas fram med segmenterade nät, kryptering av kommunikation och data, accesskontroll, multifaktorautentisering och auktorisation för vad som får göras av olika roller eller om vissa moment behöver utföras tillsammans med andra. Ibland delas utvecklingsmiljöer upp för att bättre kunna skydda olika delar men detta kräver då bra koordination och kontrakt/gränssnitt till de andra delarna.

Hur som helst så är detta bara den enkla delen och den svårare återstår i form av att arbeta på ett cybersäkert vis genom att inte avslöja hemligheter till icke behöriga samt inte öppna upp svagheter eller sårbarheter genom misstag och dåligt cybersäkerhetsmedvetande. IPR i form av kod, dokument, manualer och ritningar bör ha ett ordentligt skydd och bara kunna kommas åt och ändras på kontrollerat vis av behöriga, och i vissa fall bara låta ändringar kunna göras efter en genomgång (av programkod eller ritningar).

För att åstadkomma ovan behövs till exempel:

- Utbilda utvecklingsteamen i cybersäkerhet och cybersäker utveckling – veta hur man skyddar sin IPR och utvecklar cybersäker design, kod, kunna göra testfall för cybersäkerhet och automatiserade testsviter/testriggar med säkerhetstestfall i (här kan till exempel OWASPs listor ge en bra startpunkt tillsammans med andra dylika).

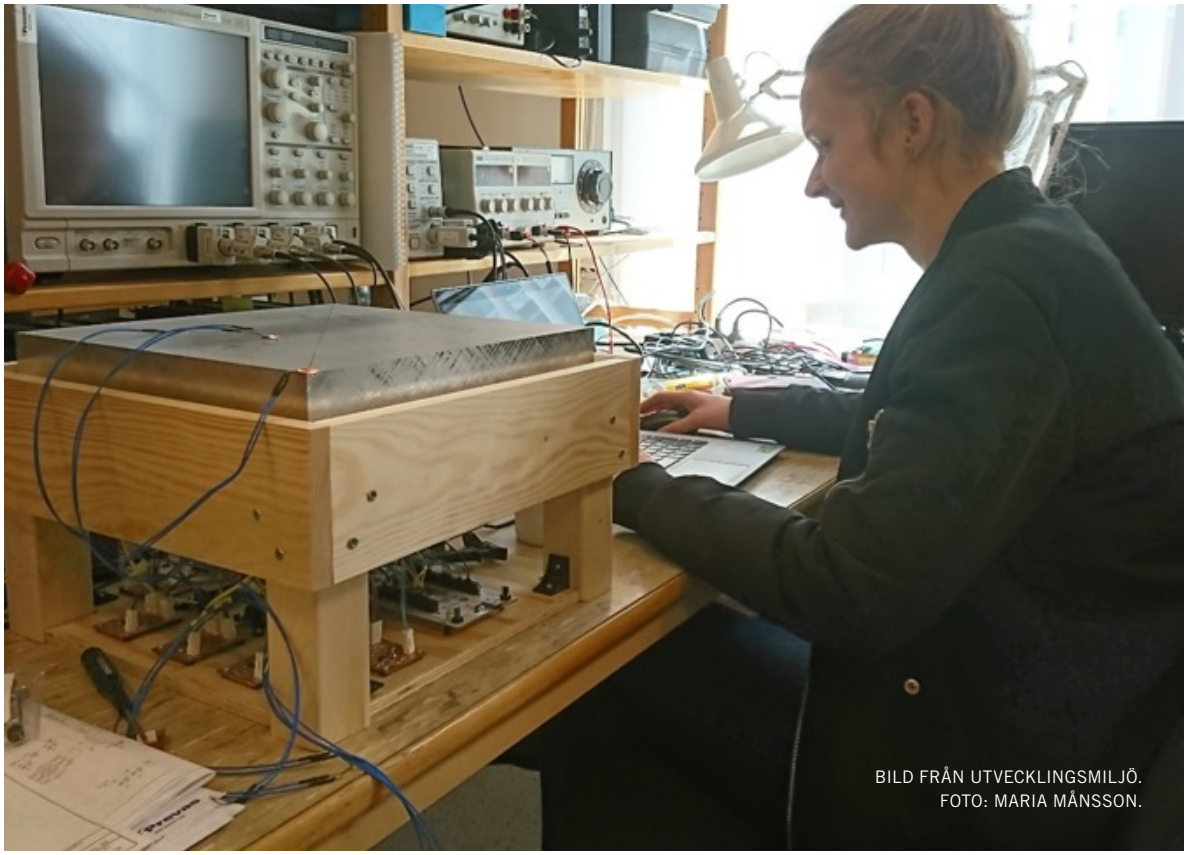


BILD FRÅN UTVECKLINGSMILJÖ.
FOTO: MARIA MÅNSSON.

- Se till att ha kontroll på vilka krav eller begränsningar som finns i eventuell open source eller öppen design licenser som används, och lagra kopior av dem lokalt för framtida bruk om de försvinner från Internet och så att man har kontroll på vilken version som är med. Licenserna för dessa måste vara kompatibla med den eventuellt egna licensieringsformen så inga överraskningar dyker upp senare.
- Effektiv testning av funktionella och holistiska krav (cybersäkerhet, digitalt bevarande, kvalitet/stabilitet, tillgänglighet, användbarhet) då dessa ofta hänger ihop när de holistiska skär igenom allt – kräver en god teknisk bredd och förståelse av testkrav (se tidigare i handboken) och skalbarhet av testningen. Här behövs funderas över hur det kan göras mycket tester med få personer inblandade med hjälp av smarta testmatriser och automatisering av tester (testsviter, testriggar och testrobotar med mera för att gå igenom alla testfallen och prestanda/belastningstester). Självklart bör även säkerhetstestningsverktyg införlivas i den automatiska testningen, vilket gör att mer säkerhetstester genomförs under hela utvecklingen. Vissa tester kan köras under nattetid eller i andra tidszoner för att korta ned den totala testtiden i kalenderdagar – vilket gör hela utvecklingsprocessen snabbare.
- Ha cybersäkrade utvecklingsverktyg och genomgångna design, ramverk, bibliotek eller open source som används. Dessa designer och ramverk bör analyseras och testas innan de stoppas in och används och även övervakas över tid då ofta kvaliteten går ned och innehållet får fler bidragstagare över tid (vilket ökar risken för att dålig och farlig kod kommer in i kodbasen). Detta är en inte

helt lätt och grannlaga uppgift över tid – och behöver därför ha resurser tilldelade. Kartlägg bakgrund till open source och open design som används i form av historik, hur mycket uppdateringar som sker och av vem, sker utveckling och förbättringar kontinuerligt eller är den "död".

- Ha en cybersäkrad testmiljö som ingen utomstående kan ändra i och få testresultat se bra ut även om inte är det.
- Ha cybersäkrade samarbetsverktyg för delning av dokument och kommunikation samt möten.

Ovan kommer till en början ge lite mer arbete och kostnader än om man struntar i cybersäkerheten och att öka effektiviteten i testningen samt täckningen av testfallen, men oftast har en organisation igen detta merarbete och kostnader flerfalt senare under en IoT-produkts livscykel. Dessutom går själva tänket och strukturen ofta att återanvända till liknande IoT-produkter.

Om det hittas brister eller fel i open source, mjukvarukomponenter eller öppen design för hårdvara så bör detta rapporteras in så det kan bli rättat. Många leverantörer av komponenter, open source- och öppen-design-projekt tar emot hittade brister och kan till och med ha belöningar i vissa fall.

MOLNBASERADE CYBERSÄKERHETSLÖSNINGAR.
FOTO: ADOBE STOCK.

6. Efter utveckling

– cybersäker support, service, underhåll och ytterligare stödprocesser och tjänster

En kostnadsdrivare och potentiellt hål i cybersäkerheten är om support, service, underhåll, ytterligare stödprocesser och tjänster som optimering av hårdvara, mjukvara och driftsprocesser är ogenomtänkta och kunskapen om målmiljöerna där IoT-produkterna kommer finnas i drift är låg. En leverantör av IoT-produkter kan behöva ha några olika alternativ så att de vanligaste driftsmiljöerna klaras av och därutöver får specialanpassningar med hjälp av konsulter göras. Några saker att tänka på är hur ska vi göra det nämnda – allt på plats, mixat på plats och från distans, eller mesta delen från distans utom byten av hårdvara och eventuellt annat mekaniskt underhåll? Se sektion 3.7 tidigare för lite kravförståelse.

Det kan vara på sin plats att ge objektsägare och användare hos kunder en rekommendation för cybersäker driftsmiljö så att de förstår vikten av detta ifall deras kunskap om området är låg och mer fokuserad på endast verksamhetsprocesserna. Detta bör påbörjas redan under affärsutveckling/försäljning och skapar normalt sett inte problem utan tvärt om signalerar ansvarstagande och professionalism. De som döljer detta eller mörkar det för objektägare och användare hos kunden kommer skapa problem för dem som senare ska ta hand om allt som kommer efter utvecklingsfasen i livscykeln. I IoT-produktens dokumentation (se sektion 3.5 för mer krav och idéer för detta) så kan det med fördel finnas cybersäkerhet inlagt i löpande texten eller mer samlat i ett appendix. Utöver själva uppsättningen är det bra att visa hur cybersäkerheten kan verifieras, vilket kan göras med instruktioner, procedurer eller små program som kan distribueras med IoT-produkten. Att ha bilder som gärna knyter an till vedertagna standarder och riktlinjer för cybersäkerhet underlättar för alla inblandade i sammanhanget. Att tänka på är att om en IoT-produkt har ett eget nät eller nätsegment som kopplas ihop med större nät hos kundens användare kan det större nätet antingen ha samma (eller högre) skyddskrav som IoT-produkten eller så behöver någon form av skydd (eller "kontroller" som det även kallas) sättas emellan. Även vilken kommunikation och dess skydd som får/måste finnas, vad och vem som får ha åtkomst samt vad de med åtkomst får göra behöver åtminstone styras upp (se exempel på kravbild i sektion 3.2.3).

Kommande EU Cyber Resilience Act kommer med stor sannolikhet att ställa krav på att övervaka och kontinuerligt övervaka ifall de IoT-produkter (eller erbjudanden där sådana ingår) som framtagits är eller blir sårbara. Följden av detta är krav på att under hela livscykeln göra uppdateringar för att rätta till sårbarheter och att dessa uppdateringar kan distribueras på ett cybersäkert vis och installeras säkert likaså.

Att hålla uppsikt över en IoT-produkt, eller kanske hel flotta av IoT-produkter som finns ute hos kunder, är något som blir allt vanligare antingen för kravinsamling (och se vad som fungerar och inte fungerar) och/eller som tilläggstjänst för prediktivt eller tillståndsbaserat underhåll och optimeringar. Som tidigare nämnts kan det vara bra att skilja på dessa data och den data som berör hur IoT-produkterna används och eventuella process- samt kvalitetsdata som även kan fångas upp. Att få tillbaka dessa data, som då kan användas i "fleet management" funktioner och ge översikt om det finns svagheter i design, enskilda komponenter, helhetstänket eller ofta förekommande fel (som tillverkningsfel från viss fabrik eller för hård hantering), är en viktig del i både cybersäkerhet men även att mer

specifikt förstå stabilitet/robusthet, tillgänglighet och vad som slits eller går sönder vid olika typer av användning i varierande miljöer. Det är inte säkert att en IoT-produkt har samma slitage och underhållsbehov om de används i en konstant fuktig miljö i en dammig gruva jämfört med i en omväxlande utomhusmiljö vid väg eller järnväg. Här gäller det att tänka igenom vad för data och olika grupper av data som kommer genereras och kan användas för att skapa värde för användaren hos kunden och även hos aktörerna i tillhörande värdekedjan. Utifrån detta kan en informationsmodell göras och sen behöver det funderas över hur överenskommelse eller avtal med objektsägare hos kund och övriga i värdekedjan skall se ut, vem som äger all data eller olika grupperna av data, var det får lagras och processas, vem som får använda vilken data och till vad mer mera. Detta är oftast mycket svårt att göra i efterhand – och bör med fördel göras tidigt. Nästa steg är att kunna få ut data från en IoT-produkt på ett effektivt och cybersäkert vis till dit det ska för att lagras och processas för olika ändamål. Om data, ändrad konfiguration eller optimering skall hämtas tillbaka, kan det ju göras i en kommunikationskanal som öppnas av IoT-produkten när den skickar data utåt (vilket då underlättar att hålla en bra och enkel cybersäkerhet och mindre uppkopplingar initierade utifrån). Data från en IoT-produkt kan utifrån behov och cybersäkerhetskrav samt vad objektägaren hos kunden accepterar lagras allt ifrån i IoT-produkten (kräver då en hel del RAM-minne och disk eller minneskort), i en näraliggande (lokal) server hos objektägaren, i en server hos leverantören eller annan part i värdekedjan eller kanske rent av i en molntjänst. Om man vill använda en extern molntjänst, som driftas av till exempel Microsoft eller Amazon, behöver cybersäkerheten sättas upp korrekt och verifieras med jämna mellanrum samt tillämpliga lagar, regleringar och rekommendationer ses över så allt är okay på dessa

MÄNNISKOR SOM SKYDDAR PRIVAT INFORMATION MED ANTIVIRUSPROGRAM.
FOTO: ADOBE STOCK.

KODDATA PÅ MONITOR.
FOTO: ADOBE STOCK.

fronter innan man börjar användningen av molntjänsten. Tyvärr är det alltför många molntjänster som har hål i sin cybersäkerhet beroende på felaktig uppsättning och konfiguration samt att cybersäkerheten inte verifieras kontinuerligt.

Vidare behöver det även i designsfasen funderas över och undersökas hur support, service, underhåll och omkonfigurationer samt andra fleet-management-funktioner kan göras på ett cybersäkert vis, samt om allt måste göras på plats, delat på plats och från distans, eller om en majoritet (utom det som måste göras fysiskt vad gäller underhåll och reparationer) kan göras från distans. Bra är att rita upp hur dessa processer ser ut och eventuellt samverkar och behöver dela data. Något som underlättar är om processen att distribuera och hämta samt installera uppdateringar och uppgraderingar för mjukvara kan ske smidigt och automatiserat (utan att få med virus och malware). En del kunder har troligen en testmiljö som alla uppdateringar och uppgraderingar provkörs i, allt från en vecka till sex månader, innan det får distribueras ut och installeras. En del tillåter att operativsystem och firmware uppdateras utan tester om leverantören av dessa är betrodd och har en bra historia bakom sig utan missöden. Men, det är som sagt bra att ta reda på fakta om detta och rita upp de processer som behövs.

Om en kunds policys inte tillåter uppkopplingar utifrån blir det mer komplicerat, men möjligheter är ju att då hämta data, konfigurationsändringar och mjukvaror med mera i samma kommunikationskanal som data sänds ut i. Om inte detta går behöver mer göras på plats och då behöver rutiner finnas för att inte virus och malware kommer med i mjukvaror eller utrustning som förs in hos objektägaren hos kunden. Objektägaren bestämmer hur data eventuellt får skickas ut, och det kan vara bra att ha till exempel tre olika sätt/vägar detta kan göras på om en eller två av dessa inte är OK för objektägaren. Att ha en kontinuerlig uppkoppling utåt för att skicka data är oftast inte acceptabelt såvida inte det krävs väldigt snabba reaktioner. Det är heller inte möjligt i vissa miljöer om de inte har kontinuerlig uppkoppling utan bara med jämna mellanrum.

Olika mellansteg och buffringar av data (till exempel använda en buffrande gateway med brandväggsfunktionalitet ovanför IoT-produkten eller ha buffring i IoT-produkten inbyggd) samt olika dataöverföringsmekanismer (exempelvis FTP, säker epost, IoT-hubb, lokala eller globala datalager som exporterar data efter filtrering och godkännande, "mobilt") och säker överföring (exempelvis SFTP/FTPS, SMIME/PGP, HTTPS (XML/JSON), secure MQTT, secure OPC-UA,

SMS, eller annan skyddad överföring) över olika typer av nät och topologier kan behövas för att få till en robusthet och inte tappa data på vägen. Vanligt förekommande industriella protokoll[10] för insamling av data och/eller styr- och reglerfunktionalitet är Profinet, Profibus, Modbus, OPC/OPC-UA med flera. OPC-UA utvecklas mer och mer vad gäller cybersäkerhet och har även en informationsmodell som hjälper till att standardisera för utvecklare och objektägare hos kunder. Ju färre mellansteg och buffringar med mera – desto bättre och enklare är det att upprätthålla driftsäkerhet och cybersäkerhetsnivån. Alla mellanlagringar och buffringar behöver övervakas så att om stopp uppträder att detta kan upptäckas snabbt. Ofta brukar kunderna i känsliga miljöer inte vilja ha mobil kommunikation via SIM-kort då detta kan öppna för cyberattacker, vilket bör framgå i deras policys. I sådana fall måste det säkerställas att IoT-produkten är i en egen ö eller att kommunikation bara kan gå utåt.

Om det är OK att ha kontrollerade uppkopplingar, som initieras utifrån, så behöver dessa uppfylla kundens olika policyer och standarder för cybersäkerhet (troligen både för IT och OT då uppkopplingarna med stor sannolikhet kommer passera både IT- och OT-miljöer). Det bästa är att kunna använda kundens standard för externa uppkopplingar och inte låsa sig till någon specifik egen lösning. Om IoT-produkten sedan kan nås direkt efter att ha kommit genom kundens lösning eller har en gateway eller brandvägg med en extra VPN-uppkoppling eller liknande så brukar det gå att lösa. Kunder brukar ha begränsningar på hur en extern uppkoppling kan och får ske. Begränsning är nödvändiga och det bör även snabbt gå att stänga ned en extern uppkoppling helt eller för en specifik användare eller grupp av användare.

Vanliga parametrar för konfiguration av externa uppkopplingar utifrån, vilka kan vara bra veta om som leverantör av IoT-produkter, är:

- Krav på genomgången process för identifiering av användare och uppsättning av konto (“enrolment”) och eventuellt även krav på att ha genomfört godkänd kurs i cybersäkerhet för att få koppla upp sig utifrån
- Tidsbaserad åtkomst (när på dygnet och vilka veckodagar åtkomst får ske)
- Autentiseringsnivå (lösenord, certifikat, tvåfaktors- eller multifaktorsautentisering)
- Auktorisation (vad användaren får göra och med vad)
- Ska åtkomsten vara på låg- eller högnivå – vad behövs för att utföra det som skall då lågnivååtkomst är betydligt svårare att begränsa (ofta kallat IPSEC VPN) jämfört med högnivååtkomst (ofta kallat SSL VPN). Många lösningar för externa uppkopplingar utifrån har ofta dessa två olika delar och att bara ha lågnivååtkomst är inte att rekommendera, vilket leverantörer av IoT-produkter bör vara medvetna om och inte göra sig beroende av att ha en dylik utan att det även ska fungera med en högnivååtkomst
- Cybersäkerhetsnivå på enheten som används vid uppkoppling (så kallad “end-point-security”)
- Åtkomsterna bör vara tidsbegränsade och ska behöva förnyas efter 1–12 månader. Om de inte förnyas så ska de direkt automatiskt inaktiveras och tas bort (så inte gamla åtkomstkonton finns kvar)
- Ska om allt ovan är OK en extern uppkoppling kunna etableras eller ska den godkännas och öppnas varje gång (till exempel genom att kundens användare behöver klicka i en ruta och godkänna) samt även närhelst kunna avbryta en aktiv uppkoppling utifrån?
- Tidsbegränsning av uppkopplade sessioner – vanligt är maxtid på 30–60 minuter innan en session automatiskt kopplas ned såvida inte annat behövs. Att kunna ha en obegränsat lång session är riskfyllt för alla inblandade

[10] Några olika exempel samlade i sammanfattning av böcker: https://www.sciencedirect.com/topics/computer-science/industrial-protocol

7. Uppföljning av IoT-produkten under dess livscykel

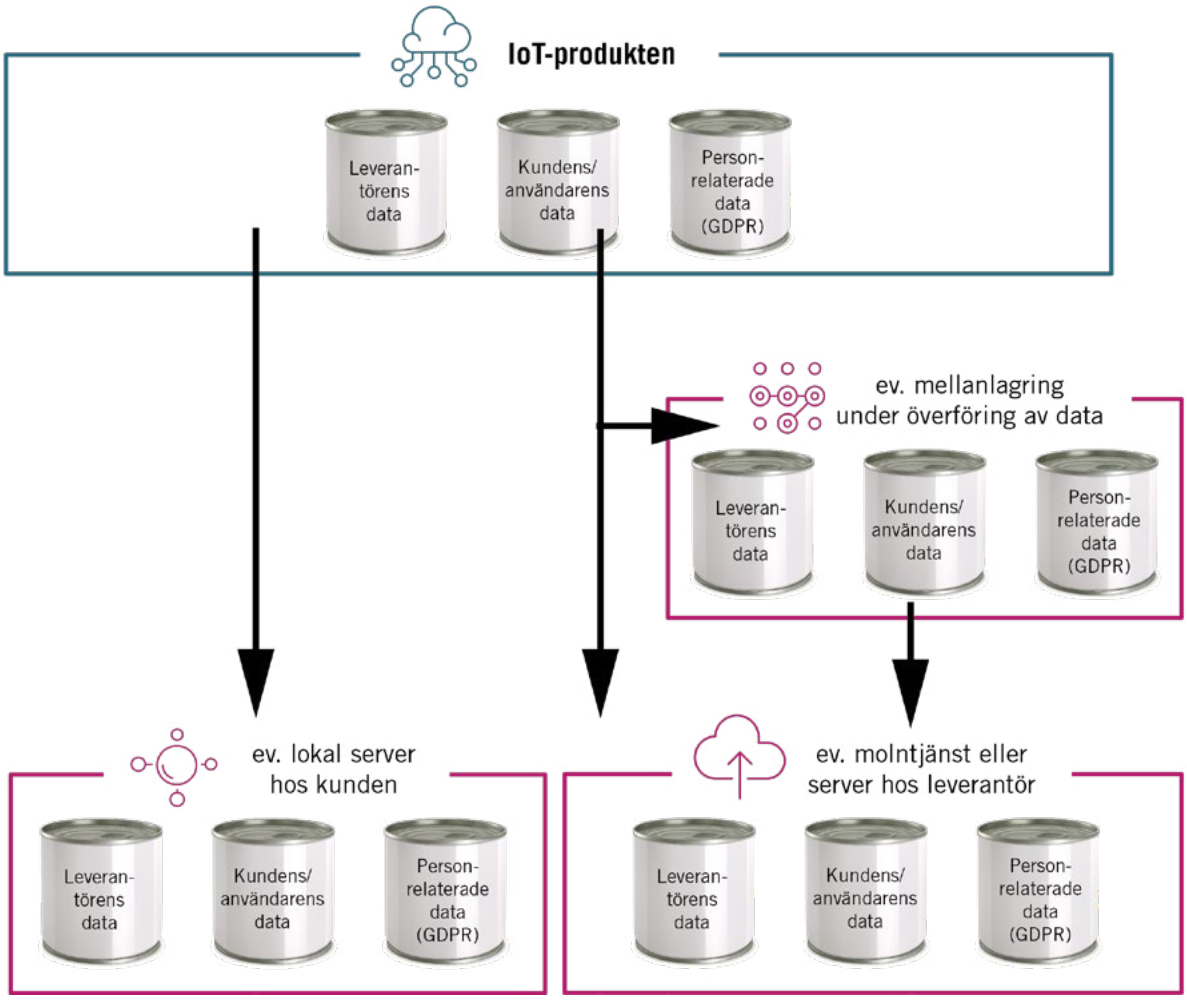
Även om det nämnts tidigare i handboken så är uppföljningen av en IoT-produkts allmänna status och underhållsbehov så pass viktig att den får ett eget kapitel. För att som leverantör, eller om det är en annan intressent i värdekedjan som tar ansvar, kunna följa upp en IoT-produkt över lång tid så behövs vissa förutsättningar finnas. En förutsättning är att klara ut med objektägare hos kunder att få ut det data som behövs och att det får användas i detta syftet. Detta görs lämpligen genom att först göra en informationsmodell och kartläggning av de processer där data skall användas innan ett kontraktsförslag eller annan överenskommelse ges till objektägaren. Det är då lättare att förklara vilken data som behövs och för vilket syfte så att objektägaren ser värdet med detta och inte reagerar på att "deras data" skall tas ut. Process- och kvalitetsdata är en annan sak som även där tilläggstjänster för övervakning av processer (processparametrar) och kvalitetsnivåer (toleranser på ingående material, mätningar under eller efter olika processteg och toleranser på utgående resultatet) samt optimering med mera kan erbjudas om det finns tillgång till denna data. I Figur 6 finns ett exempel där olika grupper av data delats upp och leverantören äger det gröna (relaterat till uppföljning och status på IoT-produkten), objektägaren eller lämplig annan intressent hos kunden äger det blåa (relaterat till process och kvalitet) samt det som finns i röda är personrelaterad data som behöver hanteras enligt GDPR inom EU och andra motsvarande lagar för skydd av personlig integritet i USA, Indien, Kina, Australien med flera.

Uppdelning av data

Ett förslag som tidigare nämnts är att tydligt dela upp olika grupper av data, som sparas i IoT-produkten innan de eventuellt skickas vidare, antingen i olika tabeller eller rent av olika databaser. Enklast är nog att använda olika tabeller då en IoT-produkt troligen inte har processorkapacitet att driva alltför många processer parallellt. Andra faktorer som påverkar här är kostnad för eventuella licenser, om det praktiskt är vettigt och om det finns sådana krav från objektägare hos kunder. Vem som äger vilken data, får göra vad med det och vad det får användas till behöver regleras i kontrakt eller annan överenskommelse mellan säljare och objektsägaren eller annan lämplig intressent hos kunden. En uppdelning gör det även möjligt att ha olika säkerhetsnivåer (med exempelvis kryptering) för de olika grupperna data samt även hårdare kunna styra vem som får ha åtkomst till vilken data och hur.

Molntjänster och servrar

På molntjänst eller serversidan (lokal hos kundens drift eller hos leverantören) så behöver en del saker tänkas igenom. Är det okej att blanda olika kunders data i samma databas och tabeller (ofta kallat "one-tier" eller "multi-tenant") eller behöver alla eller vissa kunder ha en egen instans i molntjänsten eller serverparken (om den finns hos leverantören)? Det senare kallas ofta "multi-tier" eller "single-tenant" lösning och ökar komplexitet och kostnad för drift och licenser, men om kundens objektägare kräver det och betalar för sig så kan det behövas.



FIGUR 5 – EXEMPEL PÅ UPPDELNING AV DATA I IOT-PRODUKTEN, LOKAL SERVER ELLER EVENTUELLA MELLANLAGRINGSSTEG UNDER ÖVERFÖRING OCH MOLN-/SERVERSIDAN DÄR LEVERANTÖREN ÄGER UPPFÖLJNINGSDATA, OBJEKTÄGARE HOS KUNDEN ÄGER PROCESS- OCH KVALITETSDATA, OCH PERSONRELATERAD DATA HÅLLS ISÄR FRÅN ÖVRIG DATA.

Om man fokuserar på uppföljningen av en IoT-produkt och den data som rör allmän status och underhållsbehov så finns, om de kontraktuella ramarna med objektägaren hos kunden tillåter, fina möjligheter att kunna hitta krav till nya versioner eller generationer av en IoT-produkt. Detta görs genom att se vad som fungerar och inte och ifall det finns fel som uppträder ofta och härrör till samma rotproblem i en IoT-produkt. Vid sådana fynd kan produkt- och objektsägare, tillsammans med utvecklingsgrupp och andra lämpliga intressenter, analysera vad som behöver göras för att få till en mer värdeskapande och hållbar IoT-produkt. Ibland kan det vara instruktioner eller utbildning för installatörer och användare som behövs snarare än designförändringar, ifall dessa skadar IoT-produkten genom alltför hårda handgrepp eller om den placeras på fel ställen. Även begränsningar för användningen kan ibland vara lösningen så att en produkt inte har sönder sig själv genom olika moment eller rörelser. Uppföljningen behöver ske på ett strukturerat vis och de data som kommer in kunna analyseras på ett effektivt sätt. Här kan även data som kommer från de som utför support, service, underhåll och reparationer samlas in för att komplettera det som kommer från IoT-produkten. För att enklare kunna analysera de data som människorna genererar så är det bra att ha en applikation där data kan grupperas in i standardiserade grupper

och områden, vilket sedan kan kompletteras med fritext. Att endast ha fritextrapporter blir väldigt arbetskrävande då dessa kräver arbete med katalogisering och harmonisering tillika någon form av gemensam mätbarhet eller skala (normalisering) att ha till analyser och jämförelser.

Uppföljningen av IoT-produkter går att dra några steg längre och bara fantasin och den egna utvecklingsgrupperingens förmåga begränsar. Uppföljningen kan utökas med till exempel självtester och självdiagnoser som körs med jämna mellanrum för att kolla att alla komponenter, all mekanik, alla funktioner och toleranser är som de ska och inom ramarna. Som komplement till det mer fysiska och funktionella kan med fördel automatiserade och inbyggda testsviter användas för att säkerställa att IoT-produktens cybersäkerhetsnivå är OK eller inte. Även procedurer som människor utför kan lösa dessa saker, men om möjligt är det bättre att automatisera i så hög grad som möjligt. Den data och resultat som genereras av självtester, självdiagnoser och testsviter eller procedurer behöver tas om hand, lagras och kunna användas för analyser och uppföljning.

Ett möjligt nästa steg är om tillgänglighetskraven är extrema liksom om det är svårt att fysiskt komma åt en IoT-produkt för människor. Då kan koncepten med självläkande eller självreparerande IoT-produkter eller delkomponenter vara aktuella, vilket kan kompletteras med redundans, om det är extremt svårt komma åt IoT-produkten fysiskt (om den är inbyggd i strukturer, är långt under vattenyta, är i luften eller rymden). Att fundera på är om det går att ha robotar eller drönare (unmanned aerial vehicle - UAV) som kan hjälpa till med reparation och service eller underhåll ifall inte människor kan vara på plats eller det är farligt. Troligen kommer vi få se mer av sådant i framtiden.

Fleet management

Fleet management som koncept utvecklas allt mer och framför allt där mer avancerade affärsmodeller används och det krävs att leverantörssidan kan (be)hålla koll på vad som sker med det som finns hos kundens användare. Här kanske det inte är en IoT-produkt som säljs utan en produkt integrerad med tjänster, ett Product-Service System, eller en funktion som sålts med kontraktsparametrar såsom: abonnemang/prenumeration, utlovad tillgänglighetsnivå, utlovad ökad produktivitetsnivå, eller riskdelning och intäktsdelning från IoT-produktens värdeskapande överstiger viss förbättring. För att klara detta behövs förutom att kunna övervaka och följa upp även en effektivisering av det mesta så det kan ske från distans förutom då fysisk service och underhåll (även benämnt MRO – "maintenance, repair and overhaul"). Även återbruk efter återställande (kallas även "remanufacturing" eller "refurbishment") av delar eller hela produkter blir intressant här för att bli lönsammare och samtidigt påverka miljön mindre. Troligen växer fleet-management-funktionerna fram allt eftersom behovet och möjligheter upptäcks, och nedan finns några exempel på potentiella fleet-management-funktioner för uppföljning och administration samt konfiguration från distans.

Exempel på potentiella fleet-management-funktioner:

- **Hos leverantör eller annan lämplig intressent förbereda installation och initial konfiguration, antingen för enskild IoT-produkt eller för en grupp av dylika för plug-and-play.** Detta innebär att IoT-produkten behöver vara medveten om vissa saker redan från början när den kommer till kundens driftmiljö, efter en förberedande installation/konfiguration hos leverantören eller annan intressent i värdekedjan, rörande var den skall koppla upp sig för att kunna hämta ned fullständig installation och konfiguration (på ett både cybersäkert och automatiskt vis).

- **Administration och konfiguration från avstånd** – kunna från centralt håll ändra inställningar och annan konfiguration i en eller grupp av IoT-produkter och initiera ändringen. Här kan även uppdateringar och uppgraderingar initieras, och bör vara kopplat till de olika "asset management" funktionerna nedan.

- **Tömning av data och avinstallation** – kunna från avstånd, vid slutet av användningen i

kundens driftmiljö eller slutet på hela livscykeln, tömma IPR och data från alla delar där sådant finns (det vill säga i IoT-produkten, eventuella mellanlagringsstationer av data vid överföringar samt i moln eller serverdelar). Här bör det kunna styras om det är för en IoT-produkt, en grupp av dessa, en/flera/alla hos en viss kund, en grupp av kunder eller alla som finns i flottan. Det senaste bör en ensam administratör inte kunna göra själv dock utan 2–3 personer med adekvat behörighet bör krävas så inte misstag eller sabotage sker. Verifiering att allt är klart är även det en oftast mycket önskvärd funktion. Se mer om detta i nästkommande kapitel.

- **IoT-produktens funktion bör kunna begränsas vid allvarliga problem** ("graceful degradation") och minska belastning eller i värsta fall automatiskt kunna stängas ned för att undvika allvarliga och dyra haverier. Ibland behöver beslut om detta tas av människor beroende på vilken kontext som är aktuell, men en hög nivå av automatisering av dessa beslut kan spara dyra utgifter eller i värsta fall behov att köpa en helt ny. Problem som leder till detta behöver då i tidigt skede skickas till fleet management och användare/driften hos kunden som får ta beslut om hur det hanteras eller om en temporär ersättning görs till den nuvarande är redo igen.
- **Insamling av synpunkter och klagomål från de som använder IoT-produkten hos kunder** – om det inte finns annan kanal till produktchefen via till exempel webbplats, social media eller användargrupper för insamling av synpunkter och klagomål, så är även detta en potentiell funktion för fleet management då dessa kan generera nya krav eller ge förbättringsidéer samt möjliggöra att åtgärda rena felaktigheter eller otydligheter. Här kan det vara bra att ha en standardiserad inmatning för olika områden och funktioner (med normaliserade mätdata/uppskattningar) med möjlighet till fritextbeskrivning, så att detta går att matcha och jämföra med det som kommer från support, service och underhåll.
- **Asset management** – kunna hålla koll på vad en kund har och var IoT-produkterna finns installerade. Ett övergripande asset management system bör vara kopplat mot nedanstående möjliga system/funktioner för "change/configuration/obsolescence management" då asset management är överordnat dessa:
  - **Change management** – spara data om planering, genomförande och resultat av ändringar i IoT-produkter ute i drift (till exempel omkonfigurationer och inställningar samt kontext där driftas).
  - **Configuration management** – spara konfigurationsdata för att veta vilken hårdvara och komponenter som finns i varje IoT-produkt och vilka versioner av mjukvara med mera, när uppdateringar har skett från vad till vad. Detta kan spara mycket tid och underlätta inför planering av uppdateringar och patchningar samt sökningar vid exempelvis cyberattacker då vissa mjukvarukomponenter eftersöks (ett exempel är "log4j" och liknande som inträffat).
  - **Obsolescence management** – innebär planering av lager och lagernivåer för reservdelar/komponenter samt mjukvaror och hur länge fysiska reservdelar/komponenter och gamla versioner av mjukvaror behöver lagras. Detta är dyrt och binder kapital som man ej vet om blir framtida affär av och kan dessutom även ta mycket plats (vilket kostar i fysiskt lagerutrymme). Det går att göra detta till en bra och lönsam affär om man hanterar det rätt.

För att kunna få en bra överblick och beslutsunderlag behövs någon form av sammanställning av vad status är, vad som händer och om det finns akuta saker att ta hand om. Till fleet management kan en så kallad "cockpit" eller "management view" göras vilken kompletterar de mer detaljrika "operator views" för de som kontinuerligt övervakar och löser problem inom flottan av IoT-produkter.

8. Vid slutet (eller ny fortsättning) på livscykeln

– cybersäker utrangering och förstörande av data/information i IoT-produkten och eventuella molntjänster med mera

Det är svårt för leverantören av en IoT-produkt att innan eller i början av livscykeln kunna förutse hur den verkliga användningen blir liksom av vilka användare. Att förutse nya användningsområden och möjliga förlängningar av olika slag, som dyker upp och ger nya möjligheter antingen för affärer eller socialt och ekologiskt ansvarstagande, är även det väldigt svårt. Det är inte ovanligt att objektägare hos kunder vill förlänga avtalstider och support, service och underhåll långt längre än leverantören önskar på grund av att IoT-produkten fungerar och skapar värde i miljöer där nyinvesteringar görs när saker och ting går sönder eller innebär alltför hög risk eller fara. Att förlänga livscykeln och erbjuda support, service och underhåll för en IoT-produkt innebär dock en påfrestning för organisationen och vanligen höjs priset till objektägare för att avspegla detta och kompensera för ökade kostnader och mindre fokus på nyare IoT-produkter.

I takt med att världens resurser används upp alltmer har olika former av tidigare, kanske lite i skymundan, tankar och koncept börjat bli alltmer vedertagna bland leverantörer och värdekedjor som inbegriper någon form av fysisk produkt eller system. För att, i hopp om att förbättra resursanvändningen, och även öka hållbarheten i flera olika perspektiv, finns nedan några möjliga typer av förlängning för en IoT-produkts livslängd. Detta benämns ofta som cirkulär ekonomi och den senaste tiden har termen elliptisk ekonomi[11], där livscykelns användningsfas förlängs ytterligare för att minska påfrestningen av jordens resurser, börjat dyka upp.

För att åstadkomma nedan behöver även det funderas över vad som krävs för (nya/ändrade) affärsmodeller, hur ska vanlig och cybersäkerhetsinfrastruktur se ut, samt vilka kunskaper och utbildningspaket som behövs.

Exempel på åtgärder för att förlänga livslängden på en IoT-produkt:

- **Tillämpning av "plus-1 strategi"**, vilket innebär att någon eller några funktioner tillförs och annat lyfts lite så IoT-produkten lever vidare och kan säljas ytterligare några år och skapa värde hos objektägare hos kund och speciellt hos leverantören som kan förlänga försäljningen företrädesvis hos redan nöjda objektägare. Denna strategi är vanlig hos till exempel biltillverkare där vissa modeller sålts med hjälp av strategin upp till 20 år eller mer.
- **Tillämpning av "remanufacturing" eller "refurbishment"** och förlänga livscykel genom att byta ut eventuella slitna delar eller delkomponenter vilket kan kombineras med att uppgradera vissa delar eller komponenter som behövs för att förbättra IoT-produktens funktion framöver. En annan liknande variant, som kallas "re-conditioning", innebär mer att rengöra, städa upp, eventuellt laga/byta ytskikt samt testa att allt är OK än att byta ut eller uppgradera delar (även om detta även ingår hos en del när de säger re-conditioned).

[11] https://www.ltu.se/research/Framtidsomraden/creaternity/Aktuellt/Elliptisk-ekonomi-annu-mer-hallbar-an-cirkular-1.224542

Re-conditioned är vanligt förekommande i samband med försäljning av till exempel bättre begagnade server-datorer, nätverksutrustning, bilar och mobiltelefoner.

- **Tillämpning av "repurposing"**, vilket innebär att använda IoT-produkten till annat än det som ursprungligen var tänkt och där en äldre IoT-produkt fortvarande fungerar bra.
- **Tillämpning av "downcycling"** där IoT-produkten kan användas vidare på marknader eller kontexter med lägre krav eller där betalningsförmågan inte är lika stor (till exempel i utvecklingsländer) men kanske affärsvolymen ändå är intressant.

Ovan kräver att, likt vid slutet på livscykeln, att en IoT-produkt töms på IPR och information och ersätts med fabriksinställning eller annat intetsägande innehåll. Fotot visar hur en del av en process för återvinning av elektronik och metaller kan se ut där IoT-produkter ska vara tömda på IPR och annan känslig information innan de matas in i processen.

Vid verkliga slutet på livscykeln så är det bra om det i dokumentationen finns instruktioner för hur IoT-produkten och dess beståndsdelar ska avvecklas/skrotas/tas om hand/återvinnas utan att IPR och data/information (inställningar, recept/programmering, annan driftsinfo såsom IP-adresser med mera) läcker ut till obehöriga. Således behöver allt som nämns ovan kunna tömmas på IPR och data/information samt tömningen kunna verifieras.

Observera att tömningen gäller alla ställen där IPR och data/information finns lagrad, vilket inte bara inkluderar själva IoT-produkten utan även molntjänster eller serverdelar och olika mellanlagringssteg i överföring av data. I molntjänster och serverdelar kan det vara bra att ha funktion för att ta bort all IPR och data/information som bara berör en IoT-produkt, en grupp av IoT-produkter, en kund, en grupp av kunder, eller alla kunder vid komplett avveckling.

ÅTERVINNING AV ELEKTRONIK OCH METALLER.
FOTO: ADOBE STOCK.

9. Användardfall

Att förstå och kunna ta till sig en fullständig kravbild i ett tidigt skede och dessutom innan en IoT-produkt börjat användas och erfarenheter från riktig drift finns är svårt. För att underlätta detta är det ofta en bra idé att göra några användarfall för att ge en bättre förståelse bland alla som är med i utvecklingsprocessen för vad som skall tas fram. Kapitel 9 kan ses som en fortsättning av kapitel 4 för dem med intresse att få en generell bild av några vanliga användarfall. Inför utvecklingsprojekt kan det vara bra att ha med ännu mer än nedan rörande användningen av IoT-produkten.

9.1 Användarfall med konkreta exempel

Nedan finns fem olika användarfall som sträcker sig från hem till olika professionella miljöer. Användarfallens syfte är att ge bättre förståelse för att kontextens krav på cybersäkerheten i IoT-produkter inte är lika. Ju mer cybersäkerhet som behövs, desto större kostnad för att utveckla, testa och göra eventuella certifieringar samt senare under IoT-produktens livscykel vidareutveckla och underhålla kommer det att bli.

En gemensam struktur för användarfallen har använts för att göra det lättare att jämföra mellan dem. **Strukturen finns nedan och användarfallen följer därefter:**

- Organisationstyp – kort beskrivning
- Verksamhet – introduktion av verksamheten som bedrivs för att förstå kravbilden för IoT-produkter. Kraven kan komma från: kunder/användare, lagar/regleringar, branschstandards och andra intressenter
- Typ av IoT-produkter och hur de används
- Krav på cybersäkerhet runt IoT-produkterna
- Övrigt – här finns vad som kan vara intressant men inte tas upp i ovan punkter

9.1.1 Användarfall – hemmet

- **I hemmet så sträcker sig användarfallet vanligen från lägenheter i flerfamiljshus till radhus och villor samt fritidsstugor.** Hemmen får allt högre standard och detta gäller även infrastruktur i form av Internetanslutningar via fiber, kabel-TV- eller mobilnät. Många hushåll har låg cybersäkerhetsmognad och kunskaper om hur hemmet kan nå en hygiennivå för cybersäkerhet.
- **I hemmet spenderar många en hel del tid av sin tid och där används många olika uppkopplade produkter, maskiner och system.** Det finns en del krav på att de skall vara återvinningsbara, energisnåla och cybersäkra. Förutom vanliga elsäkerhetskrav och typgodkännande med CE-märkning finns numera även till exempel GDPR, IoT-säkerhet för konsumenter (ETSI TS 103 645/TS 103 701) samt kommande EU Resilience och Cybersecurity Acts med krav på hygiennivå av cybersäkerhet för digitala konsument- och professionella produkter.
- **I hemmen byts äldre och ointelligent hemelektronik, maskiner samt system ut mot allt mer smarta och uppkopplade IoT-produkter** såsom: kylskåp, tvättmaskiner, brödrostar, babymonitorer, TV och mediautrustningar, smarta klockor med pulsmätare och GPS, mobiltelefoner, hemdatorer/paddor, spelkonsoler, Alexa- eller Nest-liknande enheter från Amazon/Google/Apple, uppvärmnings-/kylnings- och fastighetsautomationssystem, lås- och larmsystem, bilar och belysning. Dessa allt smartare IoT-produkter används för att öka bekvämligheten, kunna övervaka och styra funktioner från distans eller med automatik (till exempel energikostnadsstyrning), kunna se status på lås- och larmsystem plus vattenläckagevarningar – i allmänhet förenkla vardagslivet där det går. I vissa fall kan någon

I HEMMET SPENDERAR MÅNGA EN HEL DEL TID AV SIN TID OCH DÄR ANVÄNDS MÅNGA OLIKA UPPKOPPLADE PRODUKTER, MASKINER OCH SYSTEM.
FOTO: ADOBE STOCK.

INGENJÖR.
FOTO: SHUTTERSTOCK.

form av e-hälsa eller hemsjukvård även ske i hemmet, och till hjälp använda sensorer och trygghetslarmsystem. Då är förutom personliga integriteten även tillgängligheten av stor vikt att upprätthålla.

- I hemmet finns en hel del att tänka på vad gäller cybersäkerhet och vad de boende önskar skydda. Vanligtvis finns en hel del personliga data, som bara berörda bör kunna komma åt, vilket även gör att man i sina mobiler bör tänka över vilken information som appar snappar upp och eventuellt delar med andra liksom andra sensorer, mikrofoner och kameror. I hygiennivån på cybersäkerheten så behövs ett skydd mot cyberintrång, gärna i flera nivåer/lager från Internetanslutningen och inåt, för att förhindra att någon kan: förstöra IoT-produkterna, se om de boende är hemma, kunna se i larmkameror, kunna öppna lås eller slå av larmsystem, kunna sprida krypteringsvirus eller använda IoT-produkterna i botar. I hygiennivån ingår vid Interanslutningen att ha en lagom kompetent brandvägg/router och gärna segmentera eller dela upp nätverken samt stärka upp enskilda mer känsliga IoT-produkter såsom larm, bil, mobil, datorer, fastighetsautomation med mera. Anti-virus och malware lösningar bör komplettera en lokal brandvägg där det går, och bör åtminstone finnas i datorer, paddor, mobiler och andra IoT-produkter som klarar detta kapacitetsmässigt. Vid ökade krav på tillgänglighet, vid e-hälsa eller hemsjukvård men även för larm och övervakningssystem, så kan extra åtgärder behövas vad gäller cybersäkerhetsnivån liksom att kanske ha dubblerad Internetanslutning via fiber/kabel-TV och mobilt. I övrigt är en så kallad härdning bra att göra, vilket innebär att ta bort eller inaktivera tjänster som inte skall användas liksom begränsa kommunikation bara till de portar som trafik behöver gå igenom. Här vore det bra om leverantören redan gjort härdningen och man istället får öppna upp vid behov. Det stora problemet för hemmen är kostnadsnivån, då bra cybersäkerhet kostar, vilket gör att många i allmänhet lägger för lite pengar på att få till en hygiennivå samt sen inte underhåller nivån tillräckligt. Ett annat problem är om leverantören inte har utvecklat tillräcklig nivå av cybersäkerhet, för den blir sällan bättre eftersom. Bra är att ha automatik påslagen för att göra uppdateringar och få in cybersäkerhetsuppdateringar snabbt samt att man får någon form av varning om allt inte verkar stå rätt till.

- I övrigt behövs vanlig cyberhygien och basala kunskaper i vad man inte bör göra, till exempel att klicka på okända länkar, öppna bifogade filer som inte är anti-viruskollade, inte gå på intrångsförsök/bedrägerier som kan initieras via telefon, SMS eller e-post med länkar. Vidare bör vid varje nytt inköp eller ominstallation av en IoT-produkts grundinställningar innebära obligatoriska ändringar av enhetsnamn, användarkonton, lösenord och nätverksadresser/masker. Ofta går det dessutom att ställa in en relativt hög säkerhetsnivå, men detta kan kräva att grundinställningarna gås igenom, efter att ha läst instruktioner, och ökas för exempelvis kryptering och autentisering.

9.1.2 Användarfall – industri med produktion och distribution

- Inom tillverknings- och processindustrier finns oftast någon form av administrativ miljö (IT) och en annan miljö där produktion sker (OT). Även distributionsprocesser är ibland ihopkopplade tillsammans med OT-miljön för tillverkningen, men oftast helt eller delvis separerade. Tidigare har i många fall bara IT-miljön varit ihopkopplad med Internet, men numera är många OT-miljöer också uppkopplade och möjliga att komma åt utifrån. Vissa miljöer har fortvarande ingen eller dålig uppkoppling, men de blir allt färre. Cybersäkerhetsmognaden har i vissa delar av industriföretag varit god sedan tidigare. Dock så mognaden nu stärkas upp hos de flesta anställda och industriföretagen behöver organisera sin cybersäkerhet både för IT- och OT-miljöerna då de oftast sitter ihop.
- Många företag med produktion har sina processer igång utanför ordinarie kontorstider och kör ofta flerskift eller dygnet runt med endast stopp i produktionen under någon eller ett par veckor per år. Ju mer kontinuerlig drift desto svårare är det att ändra i produktionen och då behöver alla ändringar eller nyinstallationer planeras väl så att allt hinns med under stoppet och sen går igång smidigt utan störningar. Allt vanligare blir att leverantörer och konsulter, av effektivitetsskäl, behöver kunna koppla upp sig från utsidan för att utföra tjänster. Även data behöver i allt högre grad kunna delas från IoT-produkter både internt och utåt. Det finns en hel del krav på IoT-produkter att ha god hållbarhet för miljön de används i, ha robust och stabil funktion, liksom att de skall vara återvinningsbara, energisnåla och cybersäkra. Förutom vanliga arbetsmiljökrav, elsäkerhetskrav och typgodkännande med CE-märkning finns numera även GDPR och kommande EU Cybersecurity Act med krav på hygiennivå av cybersäkerhet för digitala konsument- och professionella produkter.
- I produktionen finns en mängd IoT-produkter, till exempel sensorlösningar, för övervakning och styrning av processer och produktionsutrustning. Vidare finns vanligtvis även bevakningslarm/låssystem, fastighetsautomation för ventilation/värme/kyla, underhållssystem som bevakar tillstånd hos produktionsutrustning, mätningssystem för upplag av råvaror, lagersystem med streckkoder för färdiga produkter med mera. Även i distributionsprocesser används IoT-produkter för att hålla ordning på var produkter är och att deras kvalitet upprätthålls (exempelvis fuktighet, kyla eller rätt temperatur). I distributionsmiljöer är oftast den fysiska säkerheten sämre och därför kan detta behöva tänkas igenom ordentligt. Produktions- och distributionsmiljöer kan vara tuffa för IoT-produkter både vad gäller fysiskt skydd (miljöskydd för vatten/smuts/damm/kyla/värme, tåla smällar och fysiska intrångsförsök för att kunna koppla in sig i nätverk via IoT-produkten) och cybersäkerhet.
- I en industri finns en hel del information både i IT- och OT-miljöerna som är skyddsvärd. Då det mesta av värdet skapas i produktionsmiljön och det är viktigt att den fungerar bra, så är tillgängligheten, robustheten och stabiliteten i produktionsprocesserna oftast det viktigaste. Vidare behöver integriteten i processerna hållas hög så att de inte varierar, har stopp

och avbrott, och att det som kommer ut på slutet håller en jämn och önskad kvalitetsnivå. Information finns i stora mängder i en produktionsprocess, varav en hel del kan vara hemlig i form av processkunnande och implementationer, metoder, recept/mönster, programmeringar med mera. Även att kunna veta om en produktionsprocess går eller inte kan vara värdefullt. IoT-produkter i form av sensorer, mätutrustningar och system, övervakningssystem, underhållssystem behöver således ha ett gott fysisk skydd i kombination med en minsta gemensam hygiennivå på cybersäkerhet. Finns det svaga områden så är det där problem oftast uppstår. I hygiennivån brukar man först dela upp nätverken i IT och OT och vidare dela upp OT-miljön i mindre segment så att olika processavsnitt isoleras och skyddas från annat och bara godkänd kommunikation får gå emellan dessa segment. Utöver detta ingår en hel del för att se till att användare bara kan göra det som de skall (och inte mer), ha kontroll på externa uppkopplingar och hur data delas säkert med rätt parter, övervakning av nät, patchrutiner, incidenthantering, backuptagning och återställningsrutiner etc. Tyvärr har många IoT-produkter dålig cybersäkerhetsnivå och den är heller inte möjlig att uppgradera eller byta ut på ett rationellt vis, vilket föranleder att dessa då inte får kopplas in i OT-näten utan får bli öar.

Hantera tredjepart

Ett annat problem är att hantera tredjepartsleverantörer och -konsulter som rör sig i OT-miljön och tillse att de inte tar med sig virus/malware eller kopplar in "saker" utan att ha tillstånd från säkerhetsansvarig för detta. I distributionsmiljöer finns ofta IoT-produkter som är utsatta och kan användas för att ta sig in i nätverk och sprida virus/malware. Således behöver man skydda dessa fysiskt, ha kontroll på vem som kan kommunicera med dem, liksom tänka över hur cybersäkerheten skall upprätthållas över tid och vad som händer när IoT-produkterna kanske slängs tillsammans med emballage i en publik sopcontainer. I övrigt är en så kallad härdning av IoT-produkter bra att göra, vilket innebär att ta bort eller inaktivera tjänster som inte skall användas liksom hårt begränsa kommunikation från/till bara till de portar, applikationer och protokoll som trafik behöver gå igenom. Här vore det bra om leverantören redan gjort härdningen, som del i grundinställningen, och man istället får öppna upp vid behov under installationen. Grundkonfigurationer för härdningar kan med fördel användas. Det stora problemet för industrin är ofta avsaknad av tillräcklig kompetens och organisation samt tydliga regler, vilket kan skapa cybersäkerhetsproblem i OT-miljön som följd. Ett annat problem är att cybersäkerheten i OT-miljöer ofta är underinvesterad till skillnad från i IT-miljön, vilket egentligen är rätt konstigt då värdet genereras i OT-miljön. Ett annat, dock mindre problem, är leverantörernas funktionsgarantier som ofta kräver att uppgraderingar och patchar ska godkännas innan de kan installeras och då detta nästan alltid släpar efter rätt länge orsakar svagheter.

- I övrigt behövs en hög cyberhygien och kunskaper i vad man inte bör göra, till exempel att inte stoppa in mobiltelefoner i USB-uttag, inte använda okontrollerade media (USB-diskar), inte installera okontrollerad mjukvara, inte klicka på okända länkar eller öppna bifogade filer som inte är anti-viruskollade, inte gå på så kallad "social engineering" som kan initieras via telefon för att komma åt inloggningsuppgifter. Vidare bör varje nytt inköp eller ominstallation av en IoT-produkt innebära att dess grundinställningar tvingar obligatoriska ändringar av enhetsnamn, användarkonton, lösenord och nätverksadresser/masker. Säkerhetsnivån skall ställas in så den är på samma eller över hygiennivån.

9.1.3 Användarfall – marint

- Inom marina industrier, med fartyg och plattformar samt hamnar, finns oftast någon form av administrativ miljö (IT) och en annan miljö där produktion sker (OT). Här skiljer sig produktionen från landbaserad industri då den ofta finns i ekologiskt känsliga områden vilket

INDUSTRIELL TEKNIK KONCEPT. KOMMUNIKATIONSNÄTVERK. FABRIKSAUTOMATION.
FOTO: SHUTTERSTOCK.

då även delar av följande distributionsprocesser gör. Distributionsprocesser är ibland ihopkopplade tillsammans med OT-miljön för tillverkningen, till exempel om det finns pipelines från en olje-/gasplattform, men vanligen är att de är separerade genom att ha fartyg som fraktar och har sin helt egna IT/OT-miljö (som dock kan vara uppkopplade och dela data med mera). Tidigare har i många fall bara IT-miljön varit ihopkopplad med Internet, men numera är vissa OT-miljöer också uppkopplade (men kräver då hög cybersäkerhet beroende på verksamhet). Cybersäkerhetsmognaden har i vissa delar av marina industrier varit god sedan tidigare och nu behövs den stärkas upp hos de flesta anställda och företagen behöver organisera sin cybersäkerhet både för IT- och OT-miljöerna.

- Många marina industrier har drift igång dygnet runt med endast stopp i produktionen under någon eller ett par veckor per år. Ju mer kontinuerlig drift desto svårare är det att ändra i produktionen och då behöver alla ändringar eller nyinstallationer planeras väl så att allt hinns med under stoppet och sen går igång smidigt utan störningar. Allt vanligare blir att leverantörer och konsulter, av effektivitetsskäl, behöver kunna få ut data för planering av åtgärder och optimeringar (alternativt även koppla upp sig från utsidan för att utföra tjänster). Således behöver data i allt högre grad kunna delas från marina IoT-produkter både internt och utåt, men detta kräver uppkoppling vilket inte alltid är tillgängligt och kan dessutom ha låg bandbredd och vara väldigt dyr om det sker via

CYBERSÄKERHETSRISKANALYTIKERTEAM MINSKAR RISKERNA.
FOTO: ADOBE STOCK.

satellit. Mobil täckning blir allt bättre men fungerar fortvarande inte på många platser. IoT-produkter för marint bruk har en hel del krav på god hållbarhet för miljön de används i, på robust och stabil funktion, liksom att de skall vara återvinningsbara, energisnåla och cybersäkra. Förutom vanliga arbetsmiljökrav, elsäkerhetskrav och typgodkännande finns numera även FN:s och IMO:s krav på cybersäkerhet (om klassade, baserade på IEC 62443 3-3), GDPR och kommande EU Cybersecurity Act med krav på hygiennivå av cybersäkerhet för digitala konsument- och professionella produkter. För fartyg som åker världen runt finns ännu fler lagrum att ta hänsyn till liksom fysisk säkerhet och cybersäkerhet i hamnar, så att inget ovälkommet hamnar ombord.

- I produktionsprocesser finns en mängd IoT-produkter för övervakning och styrning av processer, produktionsutrustning och framdrift. Vidare finns vanligtvis även styrning/navigation och kommunikation, fysisk säkerhet (varningar, evakuering, släckning med mera), bevakningslarm/låssystem, automation för ventilation/värme/kyla, underhållssystem som bevakar tillstånd hos produktionsutrustning och framdrift, mätningssystem för last och tankar med mera. Även i distributionsprocesser används IoT-produkter likt i produktionsprocesser men också för att hålla ordning på var produkter är och att deras kvalitet upprätthålls (till exempel tryck, fuktighet, kyla eller rätt temperatur om de måste hållas inom visst intervall). I distributionsmiljöer är oftast den fysiska säkerheten varierande beroende på ålder hos fartyg, och kan behöva förbättras så icke behöriga får tillgång till IT och OT. Produktions- och distributionsmiljöer kan vara tuffa för marina IoT-produkter både vad gäller fysisk tålighet/skydd (miljöskydd för vatten/smuts/damm/kyla/värme, tåla smällar, sabotageverksamhet och fysiska intrångsförsök för att kunna koppla in sig i nätverk via IoT-produkten) och cybersäkerhet.
- I en marin industri finns en hel del information både i IT- och OT-miljöerna som är skyddsvärd, och då det mesta av värdet skapas genom produktions/distributionsmiljön när den fungerar bra så är tillgängligheten, robustheten och stabiliteten i dessa processer oftast det viktigaste. Vidare behöver integriteten i processerna hållas hög så att de inte varierar, har stopp och avbrott, och att det som kommer ut på slutet håller en jämn och önskad kvalitetsnivå. Stora variationer i produktionsprocesser kan innebära fara på flera vis. Information finns i stora mängder i en produktionsprocess, varav en hel del kan vara hemlig i form av processkunnande och implementationer, metoder, recept/mönster, programmeringar med mera. Att veta om en produktions-/distributionsprocess fungerar eller inte kan vara värdefullt om det kan påverka till exempel aktiekurser. IoT-produkter i form av sensorer, mätutrustningar och system, övervakningssystem, driftsystem, styrnings/navigations/planeringssystem och kommunikation, underhållssystem behöver således ha ett gott fysisk skydd i kombination med en godkänd nivå på cybersäkerhet. Nivån varierar beroende på verksamhet och vilken klassning ett fartyg eller plattform har, men dessa är oftast betydligt högre än vad som krävs i landbaserad industri. I grundnivån brukar man först dela upp nätverken i IT och OT och vidare dela upp OT-miljön i mindre segment så att olika processavsnitt isoleras och skyddas från annat och så att bara godkänd kommunikation får gå emellan dessa segment. Utöver detta ingår en hel del för att se till att användare bara kan göra det som de skall (och inte mer), ha kontroll på externa uppkopplingar och hur data delas säkert med rätt parter, övervakning av nät, patch-rutiner, incidenthantering, backuptagning och återställningsrutiner. Tyvärr har många äldre befintliga IoT-produkter dålig cybersäkerhetsnivå och den är heller inte möjlig att uppgradera eller byta ut på ett rationellt vis, vilket föranleder att dessa då inte får kopplas in i

OT-näten utan får bli öar. Från januari 2024 kommer hårdare krav att införas och således kan en mängd äldre IoT-lösningar då behöva bytas ut samt inte få installeras i kontrakterade nybyggen. Ett annat problem är att hantera en mängd tredjeparts leverantörer och konsulter som rör sig i OT-miljön och tillse att de inte tar med sig virus/malware eller kopplar in "saker" utan att ha tillstånd från säkerhetsansvarig för detta.

I distributionsmiljöer finns även där ofta marina IoT-produkter som är utsatta och kan användas för att ta sig i nätverk och sprida virus/malware. Således behöver man skydda dessa fysiskt, ha kontroll på vem som kan kommunicera med dem, liksom tänka över hur cybersäkerheten skall upprätthållas över tid och vad som händer när IoT-produkterna slutligen avvecklas. I övrigt är en så kallad härdning av marina IoT-produkter nödvändigt att göra, vilket innebär att ta bort eller inaktivera tjänster som inte skall användas liksom hårt begränsa kommunikation från/till bara till de portar, applikationer och protokoll som trafik behöver gå igenom. Här behöver leverantören göra härdningen, som grundinställning, och vid behov får man öppna upp under installationen. Grundkonfigurationer för härdningar kan med fördel användas för att undvika mänskliga fel. Det stora problemet för marina industrin är ofta avsaknad av tillräcklig kompetens och organisation samt implementerade lokala regler, vilket kan skapa cybersäkerhetsproblem i OT-miljön som följd. Ett mindre problem är leverantörernas funktionsgarantier som ofta kräver att uppgraderingar och patchar ska godkännas innan de kan installeras och då detta nästan alltid släpar efter orsakar det svagheter.

- I övrigt krävs en hög cybernivå och kunskaper i vad man inte bör göra, till exempel inte stoppa in mobiltelefoner i USB-uttag, inte använda okontrollerade media (USB-diskar), inte installera okontrollerad mjukvara, inte klicka på okända länkar eller öppna bifogade filer som inte är anti-viruskollade etcetera. Vidare bör vid varje nytt inköp eller ominstallation av en marin IoT-produkts grundinställningar innebära obligatoriska ändringar av enhetsnamn, användarkonton, lösenord och nätverksadresser/masker. Säkerhetsnivån skall ställas in så den är på samma eller över krävda grundnivån (som bestäms av eventuell klassning)

9.1.4 Användarfall – kommunalt (med påverkan av lagen om offentlig upphandling – LOU)

- Kommuner i Sverige har en verksamhet med stor spännvidd och varierande omfattning, varav vissa verksamhetsdelar har stor likhet med kritisk infrastruktur, industri och sjukvård medan andra är mer administrativt orienterade. Ett fåtal kommuner är riktigt stora medan fler är medelstora och de flesta små med från endast några tusen till tio tusen invånare. Det låga invånarantalet i en kommun, och ifall den ligger i glesbygd, har ofta en negativ inverkan på möjligheter att hitta god kompetens inom områdena IT, OT och IoT-produkter liksom cybersäkerhet i allmänhet. En del områden är större cybersäkerhetsmässiga utmaningar än andra, till exempel skolan där i princip alla elever är uppkopplade numera liksom offentliga platser som bibliotek, sporthallar, bussar och torg med kommunalt publika WiFi-uppkopplingar.
- En kommun är ofta uppdelad i nämnder för olika förvaltningsområden, och vanligt förekommande områden är: kommunal service, skola, social omsorg, fritid, kultur, miljö och byggande, digitalisering, statsbyggnad, räddningstjänst och hamn eller liknande. Ytterligare kan det finnas även val- och överförmyndarnämnder. Inom statsbyggnad finns ofta ett tekniskt kontor som håller på med fastigheter, trafikstyrning/trafikljus, VA och eventuellt IT (såvida det inte är en egen fristående funktion inom en kommun). I de övriga nämnderna finns ett ansvar för skola, bibliotek, sporthallar, äldrevård och andra boenden, lokaltrafik med buss och spårvagn med mera som alla har sin IT-, OT, eller MT

RÄTTVISA. DOMARKLUBBA.
FOTO: SHUTTERSTOCK.

(medicinteknik) infrastruktur med IoT-produkter på många ställen. I en kommun är ofta gränserna till vad som kan klassas som kritisk infrastruktur lite otydliga i underliggande infrastrukturen och borde få lite mer omsorg. I sammanhanget räknas till exempel dricksvattenproduktion och avloppshantering (VA), energiproduktion/distribution, trafik, räddningstjänst och sjukvård (äldrevård) in i det som är mer kritiskt. Även större trafikleder, flygplatser och hamnar med större logistisk påverkan landar i samma kategori. Beroende på en kommuns storlek, och verksamhetens påverkan på samhället omkring i stort, så kan en del av det kritiska som just nämnts lyda under olika nationella säkerhetsskyddslagar och riktlinjer från MSB och Livsmedelsverket med flera myndigheter. I flera av en kommuns olika nämnder finns mycket personlig och känslig information, vilket kräver en hög nivå av cybersäkerhet. Således behöver hänsyn tas till bland annat GDPR, eventuellt EU:s NIS/NIS2 och kommande Cybersecurity Act.

- I och med spännvidden på verksamheten i en kommun finns IoT-produkter på väldigt många ställen beroende på digitaliseringsnivån i kommunen. Många IoT-produkter används på liknande vis som i industri och kritisk infrastruktur för att övervaka och styra, vilket även är fallet för fastighetsautomation (ventilation, värme, kyla), övervakning/lås/larmsystem där behövs. I sjukvård/äldrevård finns även övervakning av patienter, utrustning för distanssjukvård (vilket lär öka mer och mer), trygghetslarm och annat som gör att sjukvård/äldrevård kan genomföras i hemmet allt längre upp i åldrarna hos en kommuns invånare. Således finns många IoT-produkter i en kommuns verksamhet och fler lär det bli framöver såvida cybersäkerheten i dessa håller måttet.
- Vanliga problem i kommuner som har mindre eller större bäring på cybersäkerhet och användning av IoT-produkter är nödvändig kompetens, tuffa och prioriterade budgetar, LOU som motverkar deltagande från en del potentiella leverantörer samt verksamhetens vida omfattning. Vad gäller små och medelstora kommuner så är oftast det största problemet att få tag på rätt kompetens. Användning av konsulter kan lösa det kortsiktigt och på grund av pandemins framtvingade digitalisering är det numera lite enklare att få hjälp på distans. Små kommuner med en liten budget har vanligen 2–3 personer på IT-avdelningen som förutom att de skall sköta alla +100 system även skall klara cybersäkerhet och allt annat operativt. Ekvationen går helt enkelt inte ihop på ett bra vis. För att hitta vägar framåt har en del näraliggande kommuner börjat samarbeta och delar system

och kompetens. Större kommuner har oftast större tillgång till kompetens och konsulter. LOU gör tyvärr även i större kommuner att många mindre IoT-produktleverantörer inte är intresserade.

- I övrigt behöver kommuner följa med det allmänt ökade kravet på högre cybersäkerhet, då de hanterar både känslig information samt till viss del kritisk infrastruktur. Således behövs en generell höjning av nivån på cybersäkerhet och då även för IoT-produkter som används i verksamheterna. En viss variation i kraven finns såklart beroende på verksamhet och om IoT-produkterna är inkopplade i egna mindre fristående nätverk alternativt i IT- eller OT-nät. Kritiskt för kommuner är att se över rekrytering och att säkerställa tillgång till cybersäkerhetskompetens samt den kompetens som krävs runt IoT-produkter. Användningen av IoT-produkter lär öka mycket inom närmaste 20–30 åren när gammal infrastruktur sakta byts ut och mer övervakning med olika former av sensorer görs. Tidigare nämndes att små och mindre kommuner med fördel kan samarbeta och dela på system och personal/kompetens. Då gäller det att komma överens och gärna samordna IoT-produkter och cybersäkerhet för att lättare kunna skaffa behövd kompetensnivå.

9.1.5 Användarfall – kritisk infrastruktur

- Kritiska infrastrukturer har många likheter med både industrin och marint (se tidigare användarfallen) men har ännu mer betydelse för samhället och klassas därför som kritiska. Viss del av vanlig industri och marin industri påverkar självklart samhället och kan vid längre avbrott orsaka stora störningar, framför allt om komponent/varuproduktion, matproduktion och logistikkedjor störs ut ordentligt. De verksamheter som inom EU:s NIS-direktiv klassas som kritiska infrastrukturer skiljer sig från USA då vi har sju sektorer jämfört med sexton. EU:s sju sektorer inbegriper idag följande (som troligen kommer att utökas med fler närmaste åren): banker, infrastruktur för finansiella marknader, digital infrastruktur, energi, hälsovård/sjukhus, distribution av dricksvatten och transporter. I USA finns även kemiindustri, kritisk tillverkningsindustri, matproduktion och jordbruk, samt blåljustjänster, vilka torde vara av intresse även inom EU.
- De flesta kritiska infrastrukturer med produktion och distribution har sina processer igång dygnet runt med endast möjligheter till kortare stopp i produktionen och distributionen. Vissa kan ha kortare stopp, såsom

HÖGSPÄNNINGSLEDNING.
FOTO: SHUTTERSTOCK.

vattenproduktion när vattentornen är fulla tills de behöver fyllas på igen medan avloppsrening samt eldistribution behöver kunna fortgå kontinuerligt. Ju mer kontinuerlig drift desto svårare är det att ändra i produktionen och distributionen, och då behöver alla ändringar eller nyinstallationer planeras väl så att allt hinns med under stoppet och sen går igång smidigt utan störningar. Anställda kan av effektivitetsskäl behöva kunna koppla upp sig från utsidan för att utföra arbetsmoment och kontrollera att allt går bra. Vad gäller tredje parter så bör dessa inte få koppla upp sig utifrån utan mycket tunga skäl för det. Data behöver i allt högre grad kunna delas från IoT-produkter både internt och utåt. Det finns en hel del krav på IoT-produkter och ha god hållbarhet för miljön de används i, ha robust och stabil funktion, liksom att de skall vara återvinningsbara, energisnåla och ordentligt cybersäkra. Förutom säkerhetsskyddslagar så finns vanliga arbetsmiljökrav, elsäkerhetskrav och typgodkännande med CE-märkning. Utöver dessa finns även ENISAs och MSBs riktlinjer, Livsmedelsverkets riktlinjer, GDPR, NIS/NIS2 och kommande EU Resilience och Cybersecurity Acts med krav på hygiennivå av cybersäkerhet för digitala konsument- och professionella produkter.

- IoT-produkterna i kritiska infrastrukturer liknar mycket de som används i industrin och marint men de har ofta ännu mer utmaningar i distributionsprocesser på grund av att de är exponerade och svåra att skydda fysiskt då omfattningen är stor och ofta spänner över stora geografiska områden. Tyvärr har sabotageverksamhet blivit en realitet att ta med. Fysiska kraven och cybersäkerhetskraven är således i grunden högre än i vanliga industrin och marint och dessa hanteras ofta genom högre fysisk säkerhet i produktionen, hårdare gränsdragningar i behörigheter, starkare separation och härdning av nät och produktionsutrustning inkluderande i IoT-produkterna. För distributionsprocesserna behövs ofta övervakning och intrångsdetektering både fysiskt och cybermässigt. Övervakning behövs för distributionsprocesserna och nätens funktion för att kunna kontrollera att de fungerar (det vill säga är tillgängliga). Om de fallerar så behöver man snabbt kunna lokalisera problemen och åtgärda dessa.
- Kraven på cybersäkerheten i och runt IoT-produkter i kritiska infrastrukturer är högre, eller betydligt högre, jämfört med i industrin. Grundnivån på cybersäkerheten måste vara god och inga svaga punkter eller områden ska finnas. Det stora problemet för kritiska infrastrukturer är ofta avsaknad av tillräckligt mycket personal med kompetens och säkerhetsskyddsklass och ibland även otydliga lokala regler, vilket gör att det kan bli cybersäkerhetsproblem i OT-miljön som följd på grund av omfattningen och behov av kontinuerlig förbättring. En tillräcklig budget är ofta ett problem det med. Ett mindre problem är leverantörernas funktionsgarantier som ofta kräver att uppgraderingar och patchar ska godkännas innan de kan installeras och då detta nästan alltid släpar efter så orsakar det svagheter. I och med kontinuerlig drift så behöver en del redundans finnas, och på så vis kan uppdateringar ske kontrollerat utan avbrott eller vid väl valda tillfällen. IoT-produkter behöver vara så enkla och snabba att uppdatera eller ändra i som möjligt.
- I övrigt krävs en mycket hög cybersäkerhetsnivå och kunskaper i vad man inte bör göra, till exempel att inte stoppa in mobiltelefoner i USB-uttag, inte använda okontrollerade media (USB-diskar), inte installera okontrollerad mjukvara, inte klicka på okända länkar eller öppna bifogade filer som inte är anti-viruskollade etc. Vidare bör varje nytt inköp eller ominstallation av en IoT-produkts grundinställningar innebära obligatoriska ändringar av enhetsnamn, användarkonton, lösenord och nätverksadresser/masker. Säkerhetsnivån skall ställas in så att den är på samma eller över krävda grundnivån. Om inte IoT-produkter uppfyller kraven kommer de inte bli använda i kritiska infrastrukturer, vilka det finns många av och dessutom är omfattande.

10. Lästips

– ramverk/standarder, referenser och parlör

Nedan finns listor med lästips inom ramverk/standarder, nya EU lagar/regleringar samt referenslitteratur för dem som vill fördjupa sig inom olika områden.

Ramverk och andra relevanta skrifter som kan vara av intresse för att förstå hur IoT-produkten kommer att passa in i den större cybersäkerhetsbilden:

- Konsument/hemmasäkerhet
  - ETSI TS 103 645/TS 103 701 (www.etsi.org)
  - För uppkoppling av fastighetsautomation – se nedan rörande "generellt till OT-miljöer" och MSB:s skrift
  - NIST Cybersecurity for IoT rörande Consumer IoT Products (https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/consumer-iot-cybersecurity)
- Generellt framför allt för IT-miljöer
  - CIS controls framework (https://www.cisecurity.org/)
  - ISO/IEC 27001/2/5/17/18/19/32 med flera (www.iso.org)
- Generellt till OT-miljöer
  - MSB:s rekommendationer för cybersäkerhet i industriella kontrollsystem, cyberfysiska system och IoT (flertal olika publikationer finns på MSB:s webbplats www.msb.se)
  - MSB:s skrift om cybersäkerhet vid uppkoppling av fastighetsautomation, 2015, https://www.msb.se/sv/publikationer/fastighetsautomation--cybersakerhet-inom-fastighetsautomation/
  - NIST standards (gäller för offentlig verksamhet i USA men innehåller bra generella råd även för andra) – Cybersecurity Framework, SP 800-213, NISTIR 8228, NISTIR 8259, SP 800-30/53/73/82/171 och flertal publikationer i 800-serien (som hittas på www.nist.gov och mer specifikt på https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program)
  - ENISA – EU:s cybersäkerhetscentrum har många moln- och IoT-säkerhetsrelaterade publikationer på sin hemsida (www.enisa.europa.eu)
  - ISO/IEC 27019 rörande informationssäkerhet för processkontroll i energiproduktion och överföring (hittas på https://www.iso.org/standard/68091.html)
  - IEC 62443 (del 3-3 är troligen av mest intresse – https://www.en-standard.eu/)
  - ISA95/98 och automationspyramiden samt Purdue-modellen (https://www.isa.org/)
- Marina miljöer
  - IMO:s riktlinjer för marina miljöer MSC-FAL.1/Circ.3 och Resolution MSC.428(98) – finns ihopsatta i ramverk av bland annat DNV (DNV-RU-SHIP Pt.6 Ch.5), LLoyd´s Register (Cyber Safe for marine) och American Bureau of Shipping (Cybersafety program)
- Mer generell IoT-säkerhet (och även för data som hamnar i en molntjänst)
  - IoXt Alliance standard for IoT Security – https://www.ioxtalliance.org/
  - ISO/IEC 27018 (skydd av personuppgifter i molntjänster – www.iso.org)

  - PCI-DSS (skydd av kontokortsuppgifter https://www.pcisecuritystandards.org/)
- Kommun, region och stat – IoT i olika miljöer
  - Robust & Säker IoT: Vägledning för Robust och Säker IoT ver 1.0, Svenska Stadsnätsföreningen (SSNF), 2020, https://www.ssnf.org/nat-i-varldsklass/avtal/nyhet-avtal-robust--saker-iot-version-1.0/#:~:text=V%C3%A4gledning%20f%C3%B6r%20Robust%20%26%20S%C3%A4ker%20IoT%20beskriver%20ett,Webbinarium%20om%20avtalet%20f%C3%B6r%20robust%20och%20s%C3%A4ker%20IoT
  - Stödmaterial till Klassa, flertal publikationer från SKR med flera, https://klassa.skr.se/sidor/stodmaterial
  - Klassa för IoT, SKR och RISE, 2020, https://webbutik.skr.se/skr/tjanster/rapporterochskrifter/publikationer/klassaforiot.65074.html
  - Informationssäkerhet inom fastighetsområdet & IoT, SKR, 2022, https://webbutik.skr.se/skr/tjanster/rapporterochskrifter/publikationer/informationssakerhetinomfastighetsomradetiot.65014.html
  - Informationssäkerhet i fastighetsorganisationen, SKR, 2022, https://skr.se/skr/tjanster/rapporterochskrifter/publikationer/informationssakerhetifastighetsorganisationen.66960.html
  - Referensarkitektur för IoT (till smart stad och digitala tvillingar), Arkitekturgemenskapen (kommuner och regioner), 2022, https://inera.atlassian.net/wiki/spaces/AR/pages/2753593356/Referensarkitektur+f+r+IoT
  - NIS-direktivet (finns information om detta på EU:s och MSB:s webbplatser https://digital-strategy.ec.europa.eu/en/policies/nis-directive och https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/)
- Hälso- och sjukvård
  - MDCG 2019-16 – Guidance on Cybersecurity for medical devices
  - IEC 81001-5-1 – Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product life cycle
- Bil/fordonssäkerhet
  - ISO 21434 (www.iso.org)

Några (kommande) regleringar och direktiv på EU-nivå:

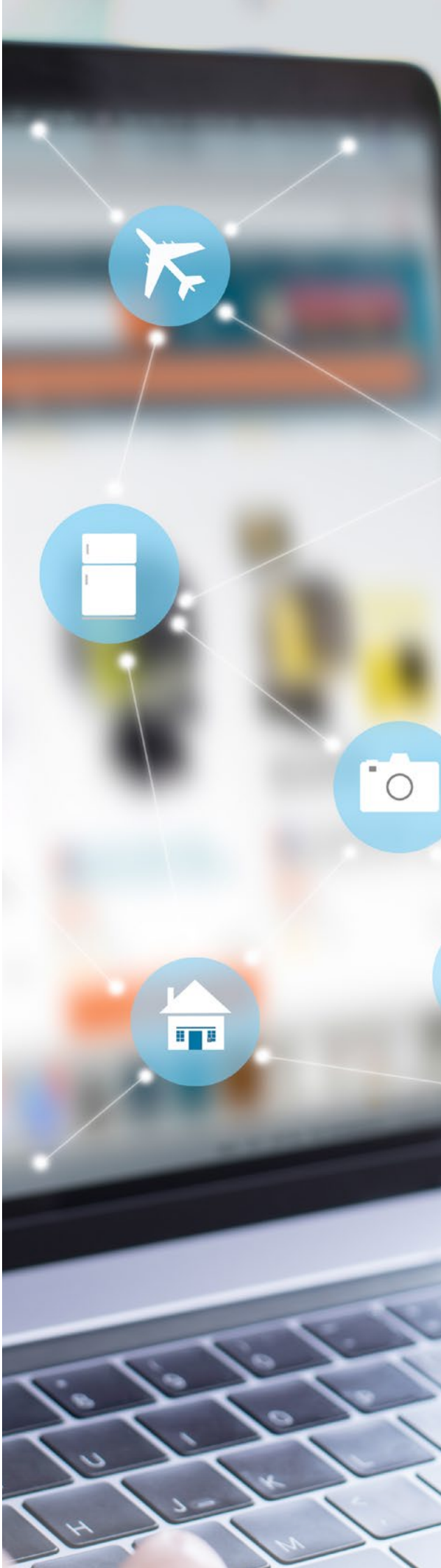
- EU Cybersecurity Act, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
- EU Cyber Resilience Act, https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
- EU Radio Equipment Directive (RED), https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en

Referenslitteratur:

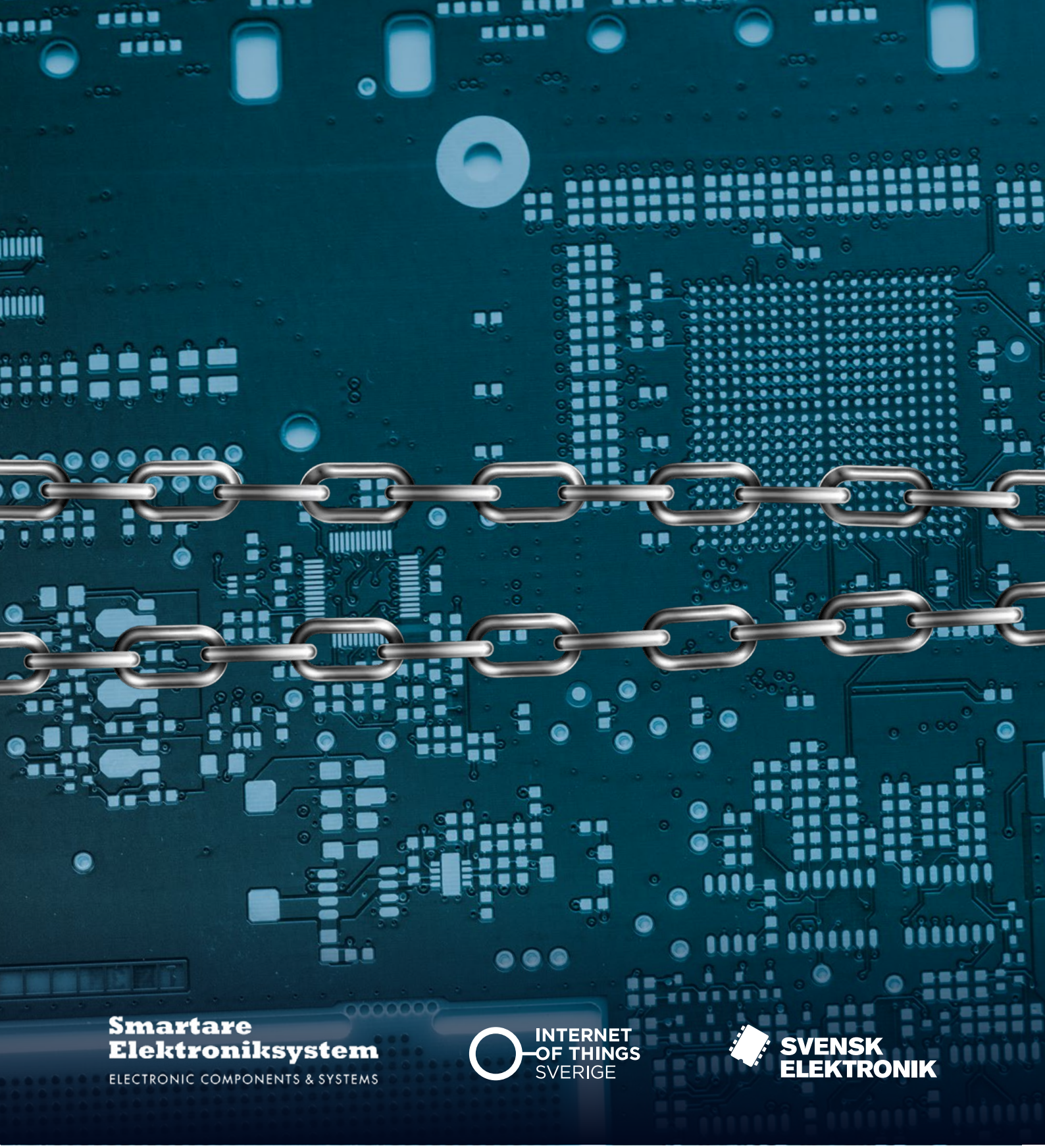
- Securing IoT and Big Data Next Generation Intelligence, 1st Ed., Edited by Vijayalakshmi Saravanan, Alagan Anpalagan, T. Poongodi, Firoz Khan, ISBN 9780367432881, CRC Press, USA, 2021
- IoT Security and Privacy Paradigm, 1st Ed., Edited by Souvik Pal, Vicente García Díaz, Dac-Nhuong Le, ISBN9780429289057, CRC Press, USA, 2020
- IoT Automation: Arrowhead Framework, Edited by Jerker Delsing, CRC Press, Boca Raton, USA, 2017
- Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and other Industrial Control Systems, 2nd Ed., Eric D. Knapp, Joel Thomas Langill, Syngress/Elsevier, MA, USA, 2014

Parlör med fackuttryck:

- **VA** – vatten och avlopp, finns i de flesta hus/byggnader och normalt har kommunerna en stor infrastruktur för produktion och distribution av rent dricksvatten samt rening av ihopsamlat avloppsvatten innan det återförs till naturen.
- **IT** – informationsteknologi, används överallt men ofta i hemmet och på kontor för administrativa göromål.
- **OT** – operationell teknologi, används i till exempel produktions- och distributionsmiljöer i industri och kritisk infrastruktur. Ibland är OT-enheter liknande de som används i IT, och i framtiden tros mycket av IT och OT börja konvergera rent teknologimässigt även om funktionen skiljer dem åt. Inom OT kan det finnas höga krav på snabbhet, det vill säga realtid, och tillgänglighet blandat med sådant som inte är tidskritiskt.
- **MT** – medicinsk teknik, används inom hälso- och sjukvård och liknar OT men har ofta ännu mer (tids)kritiska tillämpningar och krav på prestanda och tillgänglighet.
- **Fleet management** – om det finns flera IoT-produkter installerade hos olika kunder benämns ofta dessa för flotta (fleet). För att kunna hålla koll på och övervaka, samt till viss del sköta dessa från avstånd, så kan ett så kallat fleet-management-system eller -funktioner utvecklas och användas. Ett sådan system kan effektivisera och öka snabbhet till eventuella åtgärder som behöver göras alternativt be kundens användare/drift sänka belastningsnivå eller stoppa vid tecken på allvarliga problem innan ett haveri uppstår.



DET FINNS MÅNGA RAMVERK/STANDARDER, NYA LAGAR OCH REGLERINGAR ATT HÅLLA KOLL PÅ NÄR DET GÄLLER CYBERSÄKERHET OCH IOT-PRODUKTER.
FOTO: ADOBE STOCK



Med stöd från:

VINNOVA

Energimyndigheten

FORMAS

STRATEGISKA
INNOVATIONS-
PROGRAM

smartareelektroniksystem.se
svenskelektronik.se

ISBN: 978-91-985741-3-5
PRIS: 374 SEK EXKL. MOMS