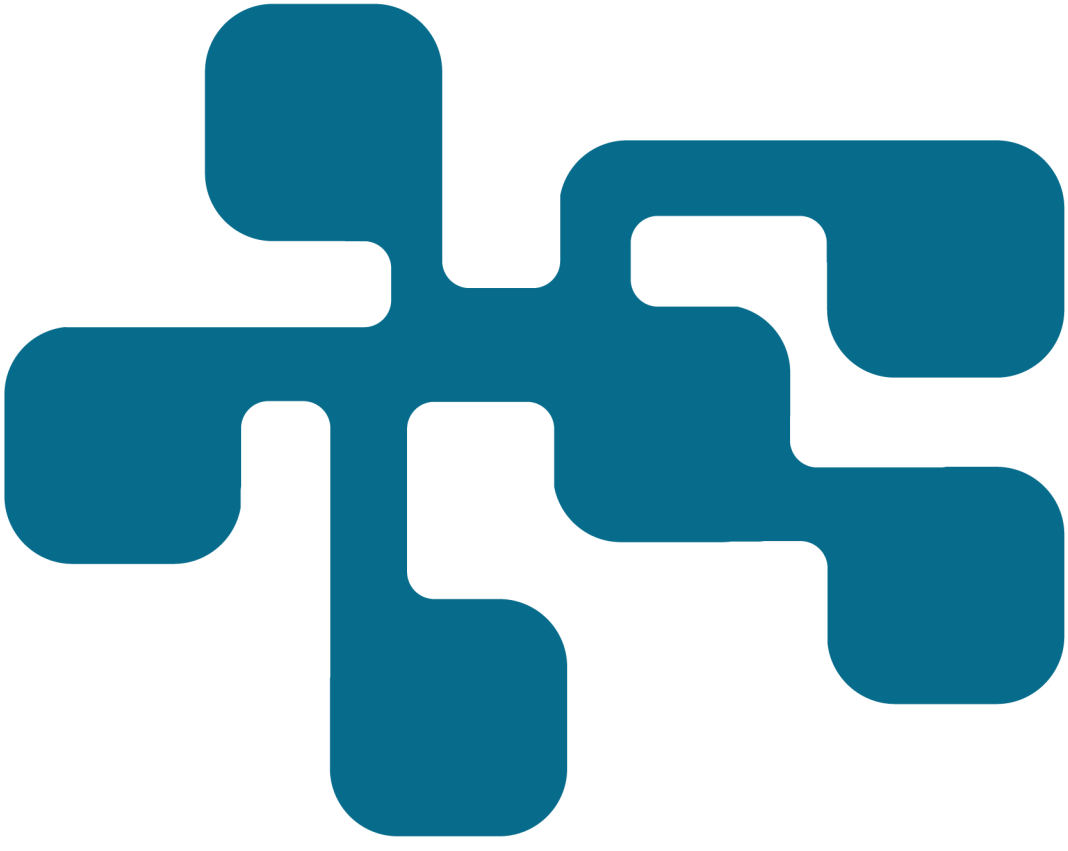
NCS3 Studie – IoT-relaterade risker och strategier

Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem

VIDAR HEDTJÄRN SWALING, JESSICA JOHANSSON FOI



FOI-R--4591--SE
MSB 2017-1554 April 2018
ISSN 1650-1942

Vidar Hedtjärn Swaling, Jessica Johansson

NCS3 Studie – IoT-relaterade risker och strategier

Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem

Titel	NCS3 Studie – IoT-relaterade risker och strategier
Title	NCS3 Study – IoT related risks and strategies
Rapportnr	4591
Månad	April
Utgivningsår	2018
Antal sidor	62
ISSN	1650-1942
Kund	MSB
Forskningsområde	5. Krisberedskap och samhällssäkerhet
FoT-område	Ej FoT
Projektnr	E13607
Godkänd av	Lars Höstbeck
Ansvarig avdelning	Försvarsanalys

Sammanfattning

Denna studie identifierar och analyserar risker relaterade till Internet of Things (IoT), samt föreslår strategier för att motverka och begränsa dem. Strategierna riktas i första hand till MSB och andra myndigheter.

Till grund för analysen ligger en studie av vetenskapliga skrifter. Analysen görs med hjälp av ett ramverk baserat i riskanalytisk metod. De element som ingår i ramverket är *skyddsvärden*, *sårbarheter*, *attackvektorer*, *risker* och *strategier*. Attackvektorerna beskrivs på en djupare teknisk nivå än de andra delarna och har därför lagts i en bilaga.

Slutsatserna är att MSB i sitt IoT-säkerhetsarbete särskilt bör:

1. Verka för en riskhantering där förebyggande insatser riktas mot
    a. sårbarheter såsom bristfällig hantering av lösenord samt fysisk exponering
    b. informationsstöld och sekretessbrott, eftersom de kan vara ett första steg i en attacksekvens som i värsta fall hotar samhällsviktiga funktioner.
2. Förespråka ett konservativt förhållningssätt i termer av ”security by design”, t.ex. att produkter ska levereras med säkra lösenord samt att enheter inte ska vara uppkopplade i onödan.
3. Prioritera ordinärt IT- och ICS-säkerhetsarbete eftersom det är i dessa domäner som de relevanta konsekvenserna manifesteras.
4. Verka för transparens inom IoT där syftet med uppkopplingen kommuniceras och där information om händelser och sårbarheter kan delas utan att kommersiella incitament äventyras.

MSB bör också försöka bidra till en aktuell bild av vilka de potentiella sårbarheterna *faktiskt* är, vilka av dessa som *faktiskt* exploateras, som *faktiskt* leder till allvarliga konsekvenser och *vilka aktörer* det är som drabbas eller på annat sätt är involverade i attackerna.

Nyckelord: Internet of Things, attackvektorer, risker, strategier, myndigheter.

Summary

This study identifies and analyses risks related to the Internet of Things (IoT) and proposes strategies for countering them. The strategies, although primarily directed to MSB (Swedish Civil Contingencies Agency) and other authorities.

The analysis is based on a study of the scientific literature and proceeded using a risk assessment framework. The elements included are *protection values*, *vulnerabilities*, *attack vectors*, *risks*, and *strategies*. The attack vectors are described at a deeper technical level and have been placed in an appendix.

The conclusion is that MSB should:

1. Strive to attain risk management that directs preventative efforts against:
    a. vulnerabilities such as poor password management as well as physical exposure;
    b. information theft and other breaches of confidentiality, since these can be the first steps in an attack sequence that in the worst case threatens critical societal functions;
2. Recommend a conservative attitude, in terms of "security by design", so that products are delivered with secure passwords, and that units should not be connected unnecessarily.
3. Prioritise ordinary IT and ICS security work because it is in these domains that the relevant consequences are manifested.
4. Strive for transparency within IoT, where the purpose of being connected is communicated, and where information about incidents and vulnerabilities are shared without jeopardising commercial incentives.

MSB should also try to contribute to a current overview of the potential vulnerabilities and which of them are *actually* exploited and *actually* result in serious consequences; as well as *which actors* are involved in, the attacks.

Keywords: Internet of Things, attack vectors, risks, strategies, authorities.

Innehållsförteckning

1 Inledning

Internet of Things (IoT) är ett begrepp som används för att beskriva att allt fler föremål, både för privat och industriellt bruk, utrustas med möjligheten att anslutas till internet och andra nätverk.

Anslutningen kan ge fördelar och skapa många nya tjänster, men innebär också många utmaningar. Exempelvis har lösningarna ofta låg säkerhet med otillräckligt skydd mot obehörigt användande. Incitamentet att sälja IoT-enheter i stora volymer till relativt låga anskaffningskostnader begränsar också möjligheterna att skapa god säkerhet. Detta kan exempelvis leda till att föremålen utnyttjas för användning i så kallade botnät.

Utvecklingen inom IoT och digitalisering går mycket fort och det finns behov av att fördjupa kunskapen om den problematik som detta medför.

Denna studie har utförts av Totalförsvarets forskningsinstitut (FOI) på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB) inom ramen för NCS3[1].

1.1 Syfte och mål

Syftet med studien är att ge underlag för fortsatt agerande utifrån MSB:s uppdrag inom informations-, IT- och ICS-säkerhet vad gäller risker förknippade med utvecklingen inom IoT.[2]

Målet med studien är att inventera, sortera och sammanställa de risker med IoT som beskrivs i svenska och internationella studier och utifrån dessa beskriva möjliga sätt för MSB att verka för ökad säkerhet.

Ambitionen är att dra slutsatser som är relevanta för ett någorlunda moget IoT, det vill säga teknologier som det finns spår av idag men som förväntas blomma ut under de närmaste 10–20 åren. Analysen har alltså relevans idag, men kan förväntas blir än mer relevant framöver.

[1] NCS3: Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet.

[2] ICS: Industrial Control System, ibland även IACS (Industial Automation and Control Systems), SCADA (Supervisory Control and Data Aquisition) eller OT (Operational Technology).

1.2 Avgränsningar

För att begränsa studiens omfattning har vi gjort följande avgränsningar:

- Analysen är kvalitativ vilket betyder att vi inte kommer att analysera sannolikheter och skadekostnader (det vill säga konsekvensers värde, se avsnitt 3.2) i någon betydande utsträckning.
- Vi kommer inte att närmare identifiera specifika instanser av riskerna, det vill säga bakomliggande hotbilder eller vilka specifika strukturer som IoT-händelser ytterst kan skada.
- I studien förutsätts att hot finns i form av exempelvis professionella hackergrupper hos främmande makt, och att de händelser som dessa hot utlöser kan leda till allvarliga konsekvenser för samhället, i form av strömavbrott, trafikolyckor, driftstopp och liknande.
- Analysen fokuserar på samhällsrisker, det vill säga händelser på samhällsnivå med större eller allvarligare konsekvenser. Risker för enskilda individer berörs i begränsad utsträckning.
- Analysen fokuserar på antagonistiska händelser såsom hackerattacker, och inte på händelser som utlöses av mänskligt felhandlande eller andra slumpmässiga händelser (såsom mjukvarufel och naturolyckor). De strategier som föreslås kan dock vara relevanta även för sådana händelser.
- De studier som i första hand tas som utgångspunkt för analysen är vetenskapliga studier och artiklar samt policydokument från myndigheter och branschorgan.

1.3 Målgrupp

Studien vänder sig i första hand till personer inom MSB som arbetar med cyberrelaterade frågor kopplade till IT och ICS, i huvudsak personer med anknytning till NCS3 och CERT-SE[3]. Studien bör också kunna vara intressant för personer med ett allmänt intresse av kris- och riskhantering och samhällets beroende av tekniska system.

[3] CERT-SE (CERT: Computer Emergency Response Team) är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. Verksamheten bedrivs vid Myndigheten för samhällsskydd och beredskap (MSB).

1.4 Disposition

Rapporten är huvudsakligen disponerad med utgångspunkt i den tillämpade metoden. Efter ett bakgrundskapitel (kap. 2), där de teoretiska och tekniska utgångspunkterna beskrivs, och ett metodkapitel (kap. 3), följer i tur och ordning redovisningar av *skyddsvärden* (kap. 4), *sårbarheter* (kap. 5), *attackvektorer* (kap. 6 och bilaga 1), *risker* (kap. 7) och *strategier* (kap. 8). I det avslutande kapitlet (kap. 9) förs en diskussion och dras ett antal slutsatser.

2 Bakgrund

I detta kapitel beskriver och definierar vi till att börja med de viktigaste analytiska begreppen. Därefter ger vi en begreppslig såväl som teknisk bakgrund till IoT.

2.1 Hot, risk och andra begrepp

Hot och *risk* är begrepp som är problematiska och som ofta blandas ihop. Risk används i dagligt tal även med betydelser motsvarande konsekvens eller sannolikhet.[4] Eftersom vi vill använda oss av termerna hot och risk är det viktigt att vi är tydliga med vad vi menar med dem och för detta behövs definitioner. De definitioner vi har valt är hämtade från Hallberg m.fl.[5]

- Hot: *En möjlig, oönskad händelse med negativa konsekvenser*.
- Risk: *Kombinationen av sannolikhet för att ett givet hot realiseras och därmed uppkommande skadekostnad*.[6]

Risk är det avgjort mest centrala begreppet i vår analys eftersom risken är ett indirekt mått på värdet av att vidta någon åtgärd, eller snarare alternativkostnaden för att inte göra något. Det är alltså med avseende på risken som en åtgärd, eller en strategi, kan definieras. Den specifika åtgärden kan sedan sättas in mot hotet eller konsekvensen, beroende på om det är sannolikheten för den oönskade händelsen eller konsekvenserna av den som ska minskas.

Notera att det inte på förhand går att uttala sig om huruvida en händelse är ett hot, en konsekvens eller något där emellan. En händelse kan vara en konsekvens, som i sin tur är ett hot om en ny händelse, etc. Det hela handlar om vad som tas som utgångspunkt, och vad analysen har i fokus. En oönskad händelse ska vi förstå som att en teknisk eller socioteknisk struktur angrips med avsikt att orsaka någon form av skada på samhället. Det kan röra sig om attacker med *IoT som mål*, det vill säga attacken på IoT antas i sig vara skadlig, eller med *IoT som medel*, det vill säga tekniken utnyttjas för att skada andra strukturer.

Begrepp som vid sidan av risk kommer att dominera denna framställning är *sårbarhet*, det vill säga vad i en struktur som är mottagligt för en attack, samt *attackvektor*, det vill säga det sätt på vilket angreppet utförs och vilken struktur (teknisk eller samhällelig) som angreppet riktas mot. Vi kommer även att prata

[4] Hallberg, m.fl. (2015).
[5] Ibid. Enligt författarna harmonierar dessa med definitioner som ges av Försvarsmakten och Swedish Standards Institute (SIS).
[6] I samtliga de dokument som åberopas av Hallberg m.fl. (2015) har risk innebörden av sannolikhet i kombination med konsekvens.

om *skyddsvärden* eftersom det är utifrån att något är värt att skydda som det är meningsfullt att prata om oönskade händelser och konsekvenser.

2.2 IoT i teori och praktik

Det interaktiva eller kommunicerande kylskåpet är ett så vanligt förekommande exempel på vad IoT är att det kanske rentav för många blivit själva sinnebilden av IoT, eller *sakernas internet* som det ofta kallas. Andra applikationer som ofta lyfts fram handlar om självkörande bilar och tillämpningar inom sjukvården. Eftersom det troligen inte finns någon bortre gräns för hur och i vilka sammanhang IoT kan tillämpas samtidigt som utvecklingen hela tiden går framåt, kanske det är viktigare att förstå vad som gör något till en IoT-sak snarare än att kunna ge många exempel på sådana saker.

I en presentation av Östen Frånberg från Luleå Tekniska Universitet konstateras att det bara är att lägga till prefixet ”smart” så blir en vanlig sak en IoT-sak. Om en manuell termostat kan slås av och på, och en digital termostat kan programmeras att göra detsamma, så kan *den smarta termostaten* sköta detta själv baserat på interaktion med andra apparater.[7] Med hjälp av denna analogi kan vi föreställa oss många olika tillämpningar av IoT, och även se dess eventuella potential för framtiden.

2.2.1 Ett förslag till definition

Internet myllrar av olika mer eller mindre genomarbetade försök att definiera och beskriva Internet of Things. På webbplatsen *Postscapes*[8] görs ett försök att sammanställa olika definitioner för att visa på den stora bredden (och kanske förvirringen) och för att identifiera gemensamma nämnare. Det konstateras att begreppet IoT förekommer i allt från marknadsföringsmaterial till titlar på vetenskapliga artiklar. I djungeln av relaterade begrepp hittar vi *physical internet, ubiquitous computing, ambient intelligence, machine to machine (M2M), industrial internet, web of things, connected environments, smart cities, spimes, everyware, pervasive internet, connected world, wireless sensor networks, situated computing, future internet and physical computing.*

På webbplatsen *Den digitala resan*[9] konstateras att IoT är ett samlingsbegrepp för den utveckling som innebär att maskiner, fordon, gods, hushållsapparater, kläder och andra saker samt varelser (inklusive människor), förses med små inbyggda sensorer och datorer som kan kommunicera med sin omvärld och som

[7] Frånberg 2014.
[8] Postscapes 2018.
[9] Den digitala resan 2015.

därmed kan skapa ett situationsanpassat beteende och anpassade miljöer, varor och tjänster.

Något liknande anförs av Wikipedia[10], där sakernas internet beskrivs som ”alla föremål (hushållsapparater, personliga accessoarer, maskiner, fordon och byggnader) som har inbyggda elektroniska delar (sensorer, processorer, etc.), internetuppkoppling (fysiskt eller trådlös), en unik och identifierbar adress och som utbyter data.”

En tredje beskrivning, snarlik de föregående men något mer koncis, hittar vi hos Tritech, ett av flera företag som specialiserat sig på att utveckla ”tjänster för det uppkollade samhället”.[11] Tritech beskriver IoT som ”ett världsomspännande nätverk av uppkopplade objekt som är unikt adresserbara och baseras på standardiserade kommunikationsprotokoll.”[12]

Kamrani m.fl. gör ett försök att hitta en mer allmängiltig och entydig definition.[13] Enligt Kamrani m.fl. är det en utmaning att begreppet IoT spänner över många olika forskningsområden inom såväl teknik som humaniora och samhällskunskap. Utgångspunkten är dock enkel – IoT syftar på fysiska enheter och apparater (eng. devices) som är kopplade till internet.[14] Kamrani m.fl. påpekar att även om IoT-enheter ofta är små anordningar som innesluter en trådlös transmissionskanal gäller detta inte allt som kallas IoT. Mer karaktäristiskt är enligt Kamrani m.fl. att systemen åtminstone till viss del är *inbyggda* (eng. embedded) *och styr något i sin omgivning*. Den definition som enligt Kamrani m.fl. bäst inkluderar även denna aspekt är den som återfinns i en skrift från U.S. Department of Homeland Security:

”The term IoT refers to the connection of systems and devices with primarily physical purposes (e.g. sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the internet) via interoperable protocols, often built into embedded systems.”[15]

Det vill säga, ungefär, *fysiskt mätande, avläsande eller påverkande system och enheter som via interoperabla protokoll, ofta implementerade i inbyggd elektronik, sammankopplas med informationsnätverk.*

[10] Wikipedia 2018a.
[11] Tritec 2018.
[12] Ibid.
[13] Kamrani m.fl. 2016, s. 7.
[14] Ibid.
[15] Department of Homeland Security, 2016.

2.2.2 IoT-arkitektur

I diskussionen om olika möjliga attacker mot, eller med hjälp av, IoT använder många författare den fysiska arkitekturen som utgångspunkt. IoT-arkitekturen kan åskådliggöras på lite olika sätt, men ofta delas den in i tre lager.[16] Lagren kallas vanligen för *perceptionslagret* (eng. perception layer), *överföringslagret* (eng. transmission layer) och *applikationslagret* (eng. application layer).[17]

I **perceptionslagret** samlas data om den omgivande miljön in med hjälp av bland annat sensorer, kameror, GPS, laserscannrar och RFID-taggar.[18] Den insamlade informationen kan röra bland annat ljud, ljus, mekanik, kemi, elektricitet och geografisk lokalitet. Utrustningen i perceptionslagret kan samla in data som behövs för exempelvis övervakning och spårning samt för att tolka information från den fysiska omgivningen.[19] I perceptionslagret kan också samarbete mellan noder i lokala nätverksdomäner ske. Sensorerna kan generera data i realtid, som sedan aggregeras och analyseras i applikationslagret. [20]

I perceptionslagret kan det också finnas ställdon. De kan åstadkomma förändringar i den fysiska miljön genom exempelvis mekaniska rörelser eller genom att styra elektriska funktioner. Ställdonen kan till exempel slå av och på brytare till lampor, fläktar, radiatorer och annan utrustning samt reglera flöden genom ventiler och pumpar. Detta kan göras genom direkta kommandon från användaren via applikationslagret, men lika gärna automatiskt baserat på insamlad information.

I **överföringslagret** sker utbyte och bearbetning av data mellan perceptionslagret och applikationslagret. Överföringen av data kan ske genom lokala nätverk och över internet.[21] De kommunikationsprotokoll som används är dels vanliga standardprotokoll som Bluetooth, Wi-Fi, 4G, 5G, UMTS, RC5, IRDA och ZigBee, dels protokoll som har utvecklats för att motsvara behoven av strömsnålhet, lång räckvidd och begränsad beräkningskapacitet. Bland dessa senare kan nämnas 6LoWPAN, RFID, NFC, Sigfox och LoraWAN.[22] Dessa protokoll används vanligen för att överföra data till en IP-stack för vidare kommunikation över internet. Lagret består av såväl mjukvara för

[16] Se t.ex. Ashibani & Mahmoud 2017, Kumar m.fl. 2016, Mahmoud m.fl. 2016 och Shifa m.fl. 2016.
[17] Perceptionslagret kallas ibland även för sensorlagret *(sensor layer)* och igenkänningslagret *(recognition layer).* Överföringsslagret kan även kallas nätverkslagret *(network layer)* eller transportlagret *(transport layer).* Se t.ex. Ashibani & Mahmoud 2017, samt av dem angivna referenser.
[18] Ashibani & Mahmoud 2017.
[19] Ibid.
[20] Ibid.
[21] Ibid.
[22] Sethi & Sarangi 2017.

nätverkskommunikation som av fysiska komponenter (t.ex. servrar) som gör det möjligt för apparaterna att kommunicera.[23]

I **applikationslagret** bearbetas den mottagna informationen och kommandon utfärdas till de fysiska enheterna.[24] Data från flera olika källor kan läggas samman och många gånger är det mycket stora mängder data som behöver bearbetas. För detta, samt för att styra de uppkopplade apparaterna, kan molntjänster, mellanprogramvara (eng. middleware) och data mining-algoritmer användas.

[23] Kumar m.fl. 2016.
[24] Ashibani & Mahmoud 2017.

3 Metod

I denna studie ska vi inventera, sortera och sammanställa de risker med IoT som beskrivs i svenska och internationella studier och utifrån dessa beskriva möjliga sätt för MSB att verka för en ökad säkerhet. I detta kapitel redovisar vi hur vi har gått tillväga.

3.1 Litteraturstudie

För att hitta vetenskaplig litteratur som beskriver IoT-relaterade risker gjordes en sökning i databasen Scopus. För att hitta artiklar med ett brett innehåll valde vi att söka på översiktsartiklar. Den söksträng som användes var: (*”internet of things”) and (vulnerab* or risk* or secur* or threat*) and (survey or review)*. Sökningen gav totalt 335 träffar, varav 322 stycken var på engelska.[25] Efter en genomgång av dessa publikationers rubriker bedömde vi att 48 stycken kunde innehålla beskrivningar av hot och risker på en övergripande nivå. Dessa artiklars sammanfattningar lästes igenom varpå 15 artiklar valdes ut för att läsas igenom i helhet. Ur åtta av dessa artiklar hämtades information som användes som det huvudsakliga underlaget till identifieringen av attackvektorer och risker (kapitel 6 och 7). Artiklarna utgörs till största delen av konferensbidrag, men också artiklar från vetenskapliga tidskrifter. Utöver detta har sökningar gjorts på enskilda termer och begrepp och då har sökningarna gjorts bredare än enbart i vetenskapligt publicerad litteratur.

Sökningar på internet har också gjorts på svenska och engelska på ”IoT”, ”Internet of Things” eller ”sakernas internet”, tillsammans med exempelvis ”hot”, ”säkerhet”, ”risk” och ”sårbarhet”. För att hitta exempel på strategier för att motverka riskerna med IoT har sökorden ovan även kompletterats med sökord som ”strategy” och ”mitigation”. Sökningar har också gjorts på enskilda organisationers webbplatser, exempelvis Enisa och NIST.[26]

Den vetenskapliga litteratur som vi har studerat har varit fokuserad på tekniska aspekter, ofta på en ganska detaljerad nivå. Andra källor är mer svepande och tar ibland upp konsekvenser på ett mer övergripande samhälleligt plan. Dessa källor kommer ofta från företag som producerar hårdvara eller mjukvara, som exempelvis Microsoft och Ericsson, eller konsultfirmor som tillhandahåller olika typer av säkerhetslösningar.

[25] Sökningen gjordes 2017-04-20
[26] https://www.enisa.europa.eu respektive https://www.nist.gov.

3.2 Analys

Utgångspunkten i analysen är de risker som identifieras i litteraturstudien. Vad som kallas risker i litteraturen sammanfaller emellertid inte alltid med vår definition av risk (se avsnitt 2.1). Således har vi stött på litteratur som använder termen risk för sådant som kanske snarare är ett hot, en konsekvens eller en allmänt oönskad händelse, eller vice versa, termerna hot och konsekvens används om sådant som skulle kallas risk enligt vår definition. Genom att genomgående hålla oss till våra definitioner av hot och risk får vi en konsistent analys.

Övriga riskrelaterade begrepp som är viktiga för analysen har vi valt att definiera utifrån ett ramverk som beskriver hur de olika begreppen hänger samman.

Vårt ramverk utgår ifrån en generisk riskanalysmodell liknande den som brukar illustreras i bow-tie-diagram.[27] Modellen beskriver övergripande följande logik:

- För att något ska vara en risk krävs en konsekvens med avseende på något *skyddsvärt*.
- Risken uppstår också i närvaro av ett *hot* och en *attackvektor*, det vill säga ett sätt på vilket hotet kan realiseras.
- Möjligheten för ett antagonistiskt hot att realiseras i ett tekniskt system beror av systemets inneboende *sårbarheter*.

De intressanta konsekvenserna är med andra ord de som uppstår genom att ett hot genom någon attackvektor i kombination med en sårbarhet påverkar något av skyddsvärdena.

Konsekvensutvecklingen från påverkan på skyddsvärden vidare till andra samhällskonsekvenser kan sedan göras mer eller mindre detaljerad. I denna studie kommer samhällskonsekvenser att beskrivas översiktligt, med några typexempel kopplat till de olika skyddsvärdena. Det viktiga är att vi kan troliggöra att attacker kan leda till konsekvenser och att vi har en begreppsapparat som gör det principiellt möjligt att identifiera de allvarligaste kombinationerna, det vill säga de viktigaste samhällsriskerna. Sådana risker beskrivs övergripande i kapitel 7. Riskerna kopplas sedan till strategier för hur de på olika sätt kan motverkas och begränsas.

I tabell 1 beskrivs ramverket och dess olika modellelement (vilka också svarar mot varsitt kapitel i rapporten) samt de kategorier som dessa element bryts ned i eller analyseras genom.

[27] Bow-tie-diagrammet är en av de mer etablerade modellerna i riskanalyssammanhang. Det rekommenderas i ISO/IEC 31010:2009 och beskrivs där som ”a simple diagrammatic way of describing and analysing the pathways of a risk from causes to consequences”. ISO/IEC 31010:2009, sid. 66.

Tabell 1: Ramverket med dess element, hämtade från riskanalytisk metod, och de kategorier som dessa element bryts ned i eller analyseras genom.

Modellelement	**Kategorisering**	**Kommentar**
Skyddsvärden (kap. 4)	Sekretess	Kategoriseras utifrån element i CIA-triaden (se kapitel 4).
	Riktighet	
	Tillgänglighet	
Sårbarheter (kap. 5)	Komplexitet	Kategoriseras utifrån generella egenskaper med riskpåverkan (egen tematisering).
	Designförutsättningar	
	Exponering	
Attackvektorer (kap. 6)	Perceptionslagret	Kategoriseras utifrån de olika lagren i arkitekturmodellen.
	Överföringslagret	
	Applikationslagret	
Risker (kap. 7)	Sekretess	Kategoriseras utifrån element i CIA-triaden (jfr skyddsvärden).
	Riktighet	
	Tillgänglighet	
Strategier (kap. 8)	Tillverkare och integratörer	Kategoriseras utifrån typer av aktörer.
	Systemutvecklare	
	Importörer och distributörer	
	Systemägare och användare	
	Myndigheter	
Diskussion/slutsatser och vad MSB kan göra (kap. 9)		Diskussion och slutsatser utifrån identifierade risker samt DHS:s principer.

4 Skyddsvärden

I en riskanalys är det viktigt med en definition av vad som är *skyddsvärt* eftersom det är utifrån att något är värt att skydda som det är meningsfullt att prata om oönskade händelser och konsekvenser.

Vi kommer här att betrakta elementen i den så kallade CIA-triaden som skyddsvärden. CIA-triaden är en modell som ofta används för att vägleda arbetet med informationssäkerhet inom en organisation. C står då för confidentiality (sekretess), I för integrity (riktighet) och A för availability (tillgänglighet).

Denna kategorisering anses relevant även för IoT. Det betyder att vi diskuterar risker med utgångspunkt i konsekvenser som äventyrar *sekretess*, *riktighet* eller *tillgänglighet*, eller en kombination av dessa.

Sekretess (C) innebär att ett system ska kunna säkerställa att endast behöriga användare får tillgång till information. **Riktighet** (I) betyder att ett system ska kunna garantera att dess information är komplett och inte har ändrats på ett otillåtet sätt. Med **tillgänglighet** (A) menas att ett system ska säkerställa att informationen är tillgänglig när den behöver användas av behöriga användare.[28]

Både vad gäller informationssäkerhet i stort och vad gäller IoT så diskuteras ibland om dessa tre kategorier är tillräckliga för att beskriva alla relevanta mål för säkerhetsarbetet.[29] Kategoriseringen lanserades på 1970-talet och har sitt ursprung i ett fokus på de tekniska aspekterna av IT-system.[30] Sedan dess har flera försök gjorts att komplettera den med ett bredare och mer socioteknisk perspektiv. Det finns emellertid ingen konsensus om vilka skyddsvärden som borde finnas med för att få en heltäckande bild och vissa författare anser att de kan sorteras in inom den vanliga CIA-triaden, som en del av antingen sekretess, riktighet eller tillgänglighet, eller som en kombination av dessa.[31]

I denna rapport kommer vi att hålla oss till den vanliga CIA-triaden eftersom vi anser att den är tillräckligt detaljerad för att vi ska kunna göra en meningsfull åtskillnad mellan olika slag av konsekvenser.

[28] Mohsen Nia & Jha 2016.
[29] Se t.ex. Mohsen Nia & Jha 2016.
[30] Samonas & Coss 2014.
[31] Samonas & Coss, 2014.

5 Sårbarheter

För att en risk ska uppstå måste det finnas ett hot och ett sätt på vilket hotet kan realiseras. Möjligheten för ett antagonistiskt hot att realiseras i ett tekniskt system beror dels av attackvektorn (det sätt på vilket systemet angrips), dels av systemets inneboende sårbarheter och brister samt hur systemet exponeras. En stor poäng med riskanalyser är att de identifierar vilka attackvektorer och sårbarheter som är involverade i händelsekedjor som är sannolika och/eller leder till svåra konsekvenser. Riskerna kan sedan elimineras genom att antingen sårbarheten byggs bort eller att hotfaktorer på olika sätt motverkas.

Det är till syvende och sist sårbarheter i enskilda system som kommer att exploateras vid en attack, det vill säga bli måltavla eller inkörsport för någon typ av handling med antagonistiska motiv. För IoT, som teknologi betraktad, går det inte att peka ut konkreta sårbarheter. Däremot kan generella egenskaper hos IoT-enheter som i sin tur medför potentiella sårbarheter i specifika instanser pekas ut. Till viss del är teknikens egenskaper intimt förknippade med dess användning, det vill säga de sätt som den används på eller är tänkt att användas på. Detta eftersom användningen i mångt och mycket bestämmer hur tekniken exponeras. Exponeringen är i sin tur en förutsättning för att en sårbarhet ska kunna utnyttjas.

I detta avsnitt gör vi ett försök att kartlägga de egenskaper hos IoT som påverkar riskbilden och därmed, i specifika instanser, kan utgöra viktiga sårbarheter. Framställningen tar sin utgångspunkt i en jämförelse med klassisk IT-säkerhet och är till stora delar baserad på Kamrani m.fl. 2016.[32] Egenskaperna är grupperade enligt vad vi uppfattar som grundläggande karaktäristika för IoT – stor komplexitet, speciella designförutsättningar och hög exponering.

5.1 Komplexitet

De egenskaper som sorterar under *komplexitet* utgörs av mängden uppkopplade enheter samt heterogeniteten hos dessa, det vill säga att de i olika aspekter är mycket olika.

[32] Kamrani m.fl. påtalar att IoT är nära besläktat med informations- och kommunikationsteknologi och IoT-relaterade risker därför i stora drag liknar de som hanteras inom konventionell IT-säkerhet. (Kamrani m.fl. 2016, sid. 8)

5.1.1 Antalet uppkopplade enheter

Antalet uppkopplade IoT-enheter är redan stort och flera bedömare förväntar sig att det kommer att växa i snabb takt under de närmaste åren.[33] Enligt Kamrani m.fl. kommer riskerna i sin tur att öka ännu snabbare eftersom antalet kommunikationsvägar ökar snabbare än antalet uppkopplade noder.[34]

5.1.2 Heterogenitet

Jämfört med dagens datornätverk förväntas IoT bli långt mer heterogent ifråga om tillverkare, mjukvaruplattformar och kommunikationsprotokoll. Eftersom det finns en stor variation av uppgifter som en nod kan ha så uppstår också många olika typer av datainnehåll och dataformat. Detta innebär utmaningar vad gäller kompatibilitet och att det blir svårare att upprätthålla den systemförståelse som krävs för att hålla systemet säkert.[35] Jing m.fl. framhåller också att det ofta inte finns något operativsystem i IoT-enheterna, utan att dessa bara innehåller enkla inbäddade program.[36]

5.2 Designförutsättningar

I kategorin *designförutsättningar* samlar vi egenskaper som har att göra med hur IoT-enheterna är konstruerade och hur de fungerar.

5.2.1 Säkerheten får inte plats

IoT-enheter är ofta batteridrivna och tillgången på ström därmed en starkt begränsande faktor. Generellt sett har de också liten processorkraft och minne jämfört med konventionella nätverksenheter. Dessa begränsningar gör att det kan bli svårt att tillämpa tillräckligt bra säkerhets- och anonymiseringslösningar.[37] Vad gäller IoT finns det i allmänhet bara utrymme att använda enkla algoritmer för att uppnå bättre säkerhet eftersom beräkningskraft och elförbrukning behöver balanseras mot varandra.[38]

[33] Enligt en uppskattning från konsultfirman Gartner (2017) så fanns det 6,4 miljarder uppkopplade IoT-enheter år 2016. Vid utgången av år 2017 så tror de att den siffran kommer att ha växt till 8,4 miljarder för att år 2020 vara upp i 20,4 miljarder.
[34] Kamrani m.fl. 2016, s. 8.
[35] Ibid.
[36] Jing m.fl. 2014.
[37] Kamrani m.fl. 2016, s. 9.
[38] Jing m.fl. 2014.

5.2.2 Osäker kommunikation

I mobilt internet används säkerhetsprotokoll som är näst intill omöjliga att använda i de resursbegränsade IoT-noderna. IoT-noder kommunicerar därför generellt via långsammare och mindre säkra trådlösa media.[39]

5.2.3 Design utan säkerhetstänk

IoT-enheter är ofta inte designade med tanke på säkerhet vilket betyder att de kan innehålla många sårbarheter men också att det inte alltid är möjligt att ”patcha” dem, det vill säga mjukvarufel som upptäcks kan inte alltid korrigeras i efterhand. IoT-enheter tillverkas dessutom ofta av mindre företag som inte har samma resurser att lägga på kvalitetssäkring som större företag (t.ex. att felsöka mjukvara innan den släpps ut på marknaden).[40]

5.3 Exponering

Under kategorin *exponering* samlar vi egenskaper som i första hand rör enheternas användning.

5.3.1 Oövervakade enheter kan lättare manipuleras

Servrar och arbetsstationer är ofta skyddade rent fysiskt, i ett serverrum, en kontorsbyggnad eller liknande, medan persondatorer och mobila enheter skyddas i ägarens närvaro. I ett IoT-nätverk kan däremot de ingående komponenterna finnas på obevakade platser, vilket gör fysiskt skydd svårt.[41]

IoT-nätverk kan dessutom vara dynamiska i den meningen att enheterna kan ”komma och gå”.[42] Detta i kombination med att IoT karaktäriseras av kommunikation över flera olika protokoll, svaga (ofta fabriksinställda) lösenord samt att enheterna i många fall aldrig stängs ner gör traditionella IT-säkerhetslösningar otillräckliga.[43]

5.3.2 Överallt och inuti allt

Det påpekas ofta att IoT förväntas bli ”ubiquitous and pervasive” (ungefär ”överallt och inuti allt”). Uppkopplade enheter kommer att bäras av oss och integreras i världen omkring oss. De kommer att samla in data och kommunicera

[39] Jing m.fl. 2014.
[40] Schneier 2017c..
[41] Ibid. s. 8.
[42] Ibid. s. 9. Med referens till Bugeja m.fl. 2016.
[43] Ibid. s. 9. Med referens till Bugeja m.fl. 2016.

och interagera med andra enheter utan vårt tillstånd och ibland utan att vi är medvetna om det, eftersom vi inte äger dem (till exempel övervakningskameror i offentliga miljöer).[44] Informationen kan bland annat röra var människor befinner sig geografiskt, deras hälsotillstånd och deras levnadsvanor. Eftersom det många gånger saknas säkerhetsfunktionalitet i IoT kan en antagonist relativt enkelt extrahera och avslöja människors personliga data.[45]

5.3.3 Osäkra lösenord

Något som kan bli ett stort problem med IoT, och som i viss mån kopplar både till design och komplexitet (avsnitt 5.1 och 5.2 ovan), är att individer tenderar att använda samma inloggningsuppgifter för alla ändamål samt att fabriksinställda lösenord ofta är kända eller enkla att knäcka samt att de dessutom sällan byts ut av användaren.[46]

[44] Kamrani mfl. 2016, s. 9.
[45] Jing mfl. 2014.
[46] Stafford 2016.

6 Attackvektorer

I detta kapitel tillsammans med bilaga 1 redovisas exempel på möjliga angrepp uppdelade på respektive lager i den tredelade modell som beskrivs i avsnitt 2.2.2. Anledningen till att attackvektorerna beskrivs separat i en bilaga är att en detaljerad förståelse av olika attackvektorer inte är nödvändig för att förstå kopplingen mellan risker och strategier. Det går heller inte att entydigt koppla en viss attackvektor till ett specifikt bakomliggande hot (vem som attackerar och med vilken målsättning) eller en specifik samhällskonsekvens. I detta kapitel ges därför endast en översikt över attackvektorer (se tabell 2), medan de i bilagan beskrivs mer detaljerat för den läsare som önskar fördjupa sig, och för fortsatt arbete inom exempelvis CERT-SE. I bilagan tas även möjliga motåtgärder mot de olika attackerna upp.

Tabell 2: Översikt över IoT-relaterade attacker och attackvektorer.

Attacker mot	Attackvektorer
Perceptionslagret Attacker i perceptionslagret riktar sig mot beräkningsnoder, RFID-taggar, direkt mot kommunikationen eller mot beräkningar som utförs i utkanten av nätverket (s.k. edge computing).	- Hårdvarutrojaner - Sidokanalsattacker och avlyssning - Invasiva attacker och hårdvarumanipulation - Replikering/kloning av noder och RFID-taggar - Denial of Service (DoS) - Injicering av data eller paket - Störning av maskininlärning - Störsändning
Överföringslagret Attacker i överföringslagret har ofta att göra med någon form av dataläckage. En angripare kan fånga upp ett meddelande, modifiera det och sedan skicka det vidare, eller dra nytta av fjärraccess i nätverk med många anslutna nätverksnoder för att generera överbelastning.	- Loopar - Maskhål - Slukhål - Störsändning - Denial of Service (DoS) - Avlyssning - Passiv övervakning - Identitetsstöld - Injicering av felaktig information
Applikationslagret Stora mängder användarinformation samlas i detta lager och här kan attacker få till följd att data skadas och att information hamnar i orätta händer.	- Buffertöverskridande - Skadlig kod - Informationsfusion - Nätfiske (phishing) - Denial of Service (DoS) - Social manipulation

7 Risker

I detta avsnitt sammanfattas och kommenteras riskerna med IoT, i första hand risker med allvarliga konsekvenser på samhällsnivå. Vi har följt CIA-modellen som introducerades i kapitel 4. Det betyder att vi diskuterar riskerna med utgångspunkt från konsekvenser som äventyrar ett eller flera av skyddsvärdena *sekretess*, *riktighet* och *tillgänglighet*.

Generellt kan sägas att det inom det traditionella arbetet med IT-säkerhet har fokuserats mycket på sekretess. När det gäller IoT har det argumenterats för att riktighet och tillgänglighet blir viktigare.[47] Attacker sker dock ofta i flera steg och därför drabbar ofta en och samma attack flera av elementen i CIA-modellen. När en angripare har lyckats göra intrång i en IoT-enhet kan denne sedan försöka ta sig vidare in i andra enheter kopplade till det nätverk som enheten är uppkopplad mot. Där kan angriparen sedan få ytterligare tillgång till uppgifter, manipulera data och införa skadlig kod.

Samhällsviktiga sektorer som dricksvattenförsörjning, energiförsörjning, livsmedelsdistribution och kommunikationer är alla beroende av IT-system och industriella styrsystem för sina funktioner. Systemen har ofta anslutningar till internet och bygger åtminstone delvis på IoT-produkter, vilket gör att de riskerar att utsättas för cyberangrepp.[48] Intrång i sådana system kan ställa till med stor skada för samhället.

7.1 Risker med avseende på sekretess

Risker med avseende på sekretess handlar om att information kommer i orätta händer. Det kan gälla information som ger tillgång till tekniska system, individers personuppgifter eller företagshemligheter. Stöld av information kan vara ett första led i en attack som innebär att information ändras eller görs otillgänglig, eller att utrustning eller processer störs eller skadas. Motivet kan till exempel vara att skaffa ett affärsmässigt övertag genom utpressning, att påverka attityder hos befolkningen eller att utsätta befolkningen för direkt fara.

7.1.1 Stöld av systeminformation

Stöld av information underlättas genom användning av IoT-enheter som språngbräda in i andra, mer traditionella IT-system.[49]

[47] Anderson 2017.
[48] Eidenskog & Kamrani 2017.
[49] Martin Karresand (FOI), personlig kommunikation 2017-08-28.

Genom till exempel tjuvlyssningsattacker och nätfiske (eng. phishing) kan obehöriga personer skaffa sig tillgång till information om exempelvis användarnamn, kryptonycklar och lösenord. Med hjälp av dessa uppgifter kan de sedan ta sig in i datorsystem och utföra flera olika typer av attacker. Det kan handla att ändra eller ta bort information eller att sprida skadlig kod.

7.1.2 Stöld av information om individer

Mängden data som samlas in om människor växer ständigt och även om känsliga uppgifter skulle rensas bort eller anonymiseras finns en risk att till synes harmlös information från olika källor kan kombineras på ett sätt som gör att känsliga uppgifter ändå kan kopplas till enskilda individer.[50] Informationen kan handla om var vi befinner oss geografiskt, vårt hälsotillstånd och våra beteendemönster.[51, 52]

Att information om människor läcker ut till obehöriga kan vara ett problem i sig. Detta behöver dock inte bara vara en olägenhet för de enskilda individerna utan kan även leda till problem på en mer samhällsövergripande nivå. Ett exempel kan vara att en antagonist påverkar en samhällsfunktion på något sätt och sedan observerar hur samhället reagerar för att därefter kunna förbättra nästa angrepp.[53]

Personer som har viktiga befattningar i samhället kan utsättas för riktade angrepp som bland annat utnyttjar IoT-enheter. Sådana angrepp genomförs oftast med hjälp av välinformerad och sofistikerad social manipulation kombinerat med tekniska angrepp.[54] För att lyckas behöver angriparen ha goda kunskaper om sin måltavla och för detta ändamål samlas information in från flera olika källor. Att få tillgång till den stora mängd information som potentiellt kan finnas i IoT-enheter kan vara mycket värdefullt i sådana sammanhang.[55]

Vissa typer av IoT-enheter kan också användas för avlyssning. Det rör sig bland annat om IP-kameror, datorer, smartphones, smarta klockor, trådlösa headsets och enheter för röststyrning av hem. Genom den ökande användningen av sådana apparater ökar också möjligheten för en angripare att skaffa sig information via dessa.[56] Det öppnar också för möjligheten att skapa kopior av produkter från kända märken, t.ex. smarta klockor, där angriparen kan använda enheten för att tjuvlyssna, stjäla information och övervaka användarens aktiviteter.[57]

[50] Kamrani m.fl. 2016, s. 9.
[51] Ibid.
[52] Eidenskog & Kamrani 2017
[53] Martin Karresand (FOI), personlig kommunikation 2017-08-28.
[54] Eidenskog & Kamrani 2017.
[55] Ibid.
[56] Eidenskog & Kamrani 2017. Se även Zunnurhain 2016.
[57] Zunnurhain, 2016.

7.1.3 Spionage

Det är inte bara information om individer som riskerar att hamna i orätta händer. Genom den ökande användningen av IoT-enheter inom företag och myndigheter öppnas också nya möjligheter till exempelvis industrispionage och underrättelseinhämtning.

7.2 Risker med avseende på riktighet

Risker med avseende på riktighet innebär att viktig information manipuleras på ett otillåtet sätt. Eftersom många IoT-enheter är sårbara för angrepp finns risken att en angripare lyckas ta sig in i dem för att modifiera deras funktion. I riktighetsfallet handlar det om att de fås att fungera på andra sätt än vad som är avsett.

En viktig konsekvens av att riktigheten i data och kod angrips är att tilliten till systemen skadas. Användarna vågar helt enkelt inte lita till att de fungerar som de ska och att de levererar riktiga uppgifter.

7.2.1 IoT som mål för angrepp

Bilar blir i allt högre utsträckning utrustade med funktioner som Bluetooth, inbyggd GPS, automatisk start via telefonen och stöd för olika appar. Forskare har bland annat kunnat visa att det genom att ta sig in i en app som kommunicerar med en bil har gått att lokalisera den för att sedan låsa upp den och fjärrstarta den.[58] Forskare har också på distans lyckats installera skadlig kod på en enhet kopplad till en bils interna nätverk och senare kunnat stänga av bilens motor under körning.[59]

Pacemakers och pumpar för att dosera medicin till patienter finns bland den sjukvårdsutrustning som har visat sig sårbara för angrepp.[60]

Attackerna i ovan nämnda exempel kan ställa till med besvär eller hota liv på individnivå, men om de skalas upp till att drabba många liknande IoT-utrusningar samtidigt så kan det leda till problem även på samhällsnivå, t.ex. i tillämpningar som smarta hem, smarta hus, smarta elnät eller smarta städer.[61]

[58] Se t.ex. Zunnurhain 2016.
[59] Se t.ex. Zunnurhain 2016.
[60] Se t.ex. Zunnurhain 2016 och Moe 2016.
[61] Martin Karresand (FOI), personlig kommunikation 2017-08-28.

7.2.2 IoT för att förstärka angrepp

Genom att bygga upp ett så kallat botnät kan en angripare skaffa sig stora mängder datorkraft. Ett botnät består av en samling internetanslutna enheter, till exempel persondatorer, servrar, mobila enheter och numera i allt högre utsträckning IoT-enheter, som har infekterats och styrs med hjälp av skadlig programvara. Angreppet sker i det fördolda och användaren märker oftast inte av att en enhet har blivit infekterad.

Den skadliga programvaran, själva ”boten”, sprider sig över internet genom att söka efter sårbara och oskyddade datorer att infektera. Typiskt letar den efter gamla versioner av operativsystem som kanske inte har blivit säkerhetsuppdaterade på länge, men även IoT-enheter är ofta mycket lätta byten eftersom de kan ha fabriksinställda lösenord, är svåra eller omöjliga att uppdatera, ständigt är påslagna och åtminstone i framtiden förväntas finnas i mycket stort antal.[62]

Botnät kan även användas för att kringgå spam- och överbelastningsfilter som delvis bygger på att de kan känna igen vilka datorer som skickar mycket stora mängder e-post eller andra meddelanden. Med hjälp av ett botnät går det också snabbare att gissa lösenord till användarkonton på internet. Det är numera möjligt att hyra tid på ett botnät genom kriminella organisationer.[63]

7.3 Risker med avseende på tillgänglighet

Risker med avseende på tillgänglighet innebär i praktiken att viktig information eller viktiga system görs otillgängliga för behöriga användare. Detta sker typiskt genom att botnät används för överbelastningsattacker, eller i utpressningsattacker där antagonisten krypterar innehållet i en dator och sedan kräver en lösensumma för att ta bort krypteringen igen (så kallad ransomware). Liksom angrepp mot riktigheten i ett system börjar angrepp mot tillgängligheten ofta med någon form av inledande sekretessöverträdelse, för att rekrytera botnät eller för att ta sig in i den dator eller det system som ska tas som gisslan.

7.3.1 IoT som mål för angrepp

Som vi har berört ovan så kan IoT-enheter utsättas för direkta angrepp i syfte att göra dem obrukbara eller få dem att fungera felaktigt. Hur stor skadan av detta blir beror på vad det är för typ av enhet som angrips och hur många enheter som drabbas. Om ett kylskåp angrips så kan det ställa till med stort besvär för det hushåll som drabbas, men på samhällsnivå märks det inte. Om en stor mängd

[62] Martin Karresand (FOI), personlig kommunikation 2017-08-28.
[63] Schneier 2017a.

kylskåp drabbas samtidigt mitt i sommaren så kanske konsekvenserna blir kännbara även på samhällsnivå.[64]

IoT-enheter som är kopplade till ställdon och kontrollsystem kan orsaka fysisk skada.[65] I fall då en enhet motsvarar en avgörande komponent i ett system som ska tillhandahålla en samhällsviktig funktion räcker det att sätta den ur spel för att orsaka effekter på samhällsnivå.

En utpressningsattack kan innebära att en motståndare gör en enhet obrukbar tills ägaren betalar lösen eller utför en viss handling. Hittills har det varit vanliga datorer som har utsatts för detta, men det finns experter som anser att utpressningsattacker i framtiden kommer att drabba även IoT-produkter.[66] Det finns också forskare som har visat hur det skulle kunna gå till, bland annat på en smart termostat. Liksom många IoT-relaterade angrepp utnyttjar mjukvara för utpressningsattacker ofta svagheter i gamla, dåligt designade eller bristfälligt underhållna system.

7.3.2 IoT för att förstärka angrepp

Botnät kan, som nämndes ovan, användas för att åstadkomma massiva angrepp, däribland överbelastnings- och utpressningsattacker som kan ge allvarliga tillgänglighetsproblem. Sådana DoS- eller DDoS-attacker (Denial of Service respektive Distributed Denial of Service) kan drabba viktiga system som transport-, energi- och stadsinfrastruktur.[67] Det förekommer att politiska grupper använder sig av överbelastningsattacker för att släcka ner webbplatser som de ogillar.[68]

Ett känt exempel på ett omfattande botnät är Mirai. Det bestod till stora delar av IoT-enheter. Mirai var inriktat på att rekrytera IoT-enheter genom att logga in på dem med deras fabriksinställda användarnamn och lösenord. Mirai användes vid de uppmärksammade överbelastningsattackerna mot den stora namnserverleverantören Dyn den 21 oktober 2016. Attackerna ledde till att flera stora webbplatser i Europa och Nordamerika blev otillgängliga i perioder under dagen.

[64] Martin Karresand (FOI), personlig kommunikation 2017-08-28.
[65] Kamrani mfl. 2016, s. 9.
[66] T.ex. Schneier 2017b och Dickson 2016.
[67] Ibid.
[68] Schneier 2017a.

8 Strategier

Det råder stor entusiasm kring de nya möjligheter som IoT skulle kunna erbjuda. Säkerhetsriskerna med IoT får dock inte så stor uppmärksamhet som de kanske skulle behöva ha.[69]

Många av sårbarheterna i IoT-enheter skulle kunna minskas om redan erkänd säkerhetspraxis tillämpades, men av flera orsaker saknar många produkter ändå grundläggande säkerhetsfunktioner. Bland annat kan det vara oklart vem som ska ta ansvar för säkerhetsåtgärder när ett företag står för utformningen av en produkt, ett annat företag står för delar av mjukvaran, ett tredje hanterar det nätverk som enheten ska kopplas in i och ett fjärde företag driftsätter produkten. Problemet förvärras av att det inte finns några heltäckande och allmänt erkända internationella regler och standarder för IoT-säkerhet. En annan bidragande orsak kan vara att leverantörer och underleverantörer saknar incitament att ta tillräcklig hänsyn till säkerhetsaspekter, eftersom det inte är de som måste bära kostnader som kan uppstå till följd av den bristande säkerheten. I vissa fall kan det också vara så att medvetenhet om säkerhetsfrågorna är otillräcklig.[70]

Denna rapport syftar primärt till att föreslå strategier för MSB att hantera olika IoT-relaterade risker. Eftersom MSB är en koordinerande och rådgivande myndighet bör dessa strategier tas fram baserat på vad som är de olika IoT-beroende aktörernas förutsättningar och utmaningar. Microsoft har gjort en sammanställning av best practices när det gäller IoT-säkerhetsarbete som tar hänsyn till de olika aktörsnivåernas specifika förhållanden.[71] USA:s departement för inrikes säkerhet, U.S. Department of Homeland Security (DHS), som kan sägas vara MSB:s systerorganisation i USA, har i sin tur tagit fram ett antal grundläggande principer för IoT-säkerhetsarbete.[72]

Vår tanke är att en fusion av dessa två sammanställningar kan utgöra en robust strategi för MSB att agera utifrån. Strategin måste givetvis, där så krävs, anpassas till svenska förhållanden.

För att organisera sitt sätt att tänka kring IoT-säkerhet föreslår DHS att aktörerna ska göra följande:[73]

- Bygga in säkerhet redan i designfasen.
- Verka för säkerhetsuppdateringar och sårbarhetshantering.
- Bygga på beprövad praxis.

[69] Department of Homeland Security 2016, s. 2.
[70] Ibid. s. 3.
[71] Microsoft Azure 2018.
[72] En i stort sett överensstämmande bild ges av ENISA 2017.
[73] Department of Homeland Security 2016, s. 4.

- Prioritera säkerhetsåtgärder utifrån potentiell påverkan.
- Verka för transparens inom IoT.
- Ansluta enheter genomtänkt och med försiktighet.

Dessa principer är riktade till utvecklare, tillverkare, tjänsteleverantörer och aktörer med ett övergripande säkerhetsansvar inom samhällsviktig verksamhet, industri och statlig styrning. Dessa är ungefär samma aktörer som representeras i Microsofts best practice-dokument.[74]

Nedan följer en sammanställning av de åtgärder och strategier som tas upp för respektive aktörskategori i dokumenten från DHS och Microsoft.

8.1 Tillverkare och integratörer av hårdvara

Det finns en lång rad åtgärder som tillverkare och integratörer kan vidta för att öka säkerheten i sina produkter. En princip som återkommer är *security by design*, det vill säga att säkerhetsåtgärder har vidtagits redan i designfasen. Samtliga strategier och åtgärder som föreslås nedan kan ses som tillämpningar av den principen:

- Hårdvara, såsom integrerade kretsar och processorer, kan ha inbyggda säkerhetsattribut som stödjer t.ex. kryptering och anonymitet.[75] Det går även att göra enheter motståndskraftiga mot fysisk manipulation. Det kan exempelvis innebära att enheter förses med USB-portar bara om det är helt nödvändigt, eller att mekanismer som kan detektera fysisk manipulation byggs in.[76]
- Mjukvaran i en apparat bör kunna säkerhetsuppdateras på ett säkert sätt. Det kan ske genom att enheter konstrueras med säkra vägar för uppdatering och att nya mjukvaruversioner verifieras med kryptografiska metoder.[77] Nytillverkade enheter bör även förses med det senaste operativsystemet utifrån vad som är ekonomiskt och tekniskt försvarbart.[78] Detta ger viss garanti för att kända sårbarheter har åtgärdats. Vidare bör tillverkare erbjuda säkerhetsuppdateringar under hela produktens livslängd.
- Viktigt är också att utrustningen har designats med viss tolerans mot avbrott eller fel hos andra enheter. Enheter bör utformas med en sund

[74] Microsoft Azure 2018.
[75] Department of Homeland Security 2016, s. 6.
[76] Microsoft Azure 2018.
[77] Microsoft Azure 2018.
[78] Department of Homeland Security 2016, s. 6.

felhantering så att kaskadfel undviks.[79] Det är också bra om IoT-enheter utformas så att de kan fortsätta att fungera även om anslutningen till internet eller olika molntjänster störs.[80] För att begränsa angreppsytan kan funktionaliteten hos IoT-enheter begränsas så att de bara kan utföra det de är avsedda för och inte lägga till onödiga kringfunktioner.

- Enheterna måste ha ett bra lösenordsskydd. Istället för att tillhandahålla ett fabriksinställt osäkert standardlösenord som användaren behöver ändra till något säkrare, kan produkter levereras med ett unikt och säkert lösenord som användaren vid behov kan ändra till något annat, eventuellt mindre säkert, lösenord.[81] Detta är inte minst viktigt för att undvika att IoT-enheter rekryteras till botnät, något som är ett ständigt överhängande hot.[82]

Det finns många fler åtgärder som kan vidtas vid produktionen av IoT-enheter.[83] Beroendet av många lättillgängliga lågprislösningar på både hård- och mjukvarusidan kan göra det svårt att få en korrekt bild av den resulterande säkerhetsnivån när en uppkopplingsbar enhet sätts samman. I många fall utnyttjas dessutom paketlösningar som bygger på öppen källkod vilket försvårar härledning av de ingående komponenternas ursprung.[84]

8.2 Systemutvecklare

Systemutvecklingen, det vill säga utvecklingen av de färdiga IoT-lösningarna, innebär integration av olika hårdvaru- och mjukvarukomponenter samt anpassning och konfigurering av dessa till specifika ändamål. Utvecklaren har stora möjligheter att utforma IoT-lösningen från grunden, använda kommersiella komponenter och göra anpassningar av öppen källkod.[85]

När mjukvara utvecklas är det viktigt att säkerhetstänkandet genomsyrar alla steg i processen, inklusive val av plattformar, programspråk och verktyg. Om öppen källkod används är det viktigt att välja mjukvara som underhålls kontinuerligt och i en version där kända säkerhetsbrister har åtgärdats.[86]

[79] Ibid.
[80] BITAG 2016.
[81] Department of Homeland Security 2016, s. 6.
[82] Ibid.
[83] Se exempelvis BITAG 2016.
[84] Department of Homeland Security 2016, sid. 11.
[85] Microsoft Azure 2018.
[86] Många sårbarheter finns t.ex. i applikationsgränssnittet (API) genom att applikationer tillåts anropa även sådana delar av ett bibliotek (funktioner, datatyper, variabler mm.) som inte krävs för en specifik uppgift. Ibid.

Utvecklare bör också ha en livscykelstrategi för systemet och kommunicera rimliga förväntningar till både tillverkare och användare. Detta inkluderar att påtala riskerna med att utnyttja en lösning bortom dess supportade livslängd.[87]

8.3 Importörer och distributörer

De flesta produkter som importeras och saluförs för användning i Sverige kommer från tillverkare i andra länder. Importörer och säljare kan ställa krav på att IoT-produkterna ska hålla en godtagbar säkerhetsnivå, till exempel enligt de rekommendationer som ges i föregående avsnitt.

8.4 Systemägare och användare

När en IoT-lösning har utvecklats ska den tas i drift i den tilltänkta miljön. Det betyder att enheter kopplas ihop och att olika lösningar i mjukvara eller molntjänster driftsätts. Till att börja med måste IoT-utrustningen installeras på ett säkert sätt. Om den dessutom placeras på en offentlig plats eller i ett oövervakat utrymme så behöver möjligheterna att fysiskt manipulera den minimeras. Enheterna ska heller inte vara uppkopplade i onödan. Ibland kan det istället räcka att med lokal kommunikation mellan enheter alternativt att de inte kan kommunicera alls.[88]

Även om säkerhetshänsyn har tagits i designfasen kommer många brister och sårbarheter inte att upptäckas förrän utrustningen har tagits i drift. Genom säkerhetsuppdateringar, övervakning och underhåll kan sådana sårbarheter hanteras, och därmed begränsas potentiella konsekvenser av angrepp.

Om möjligt bör program som skyddar mot virus och annan skadlig kod installeras. För att upptäcka intrång bör händelser i systemet loggas och analyseras, exempelvis genom de molntjänster som skapats specifikt för detta ändamål. Autentiseringsuppgifter bör skyddas genom starka lösenord. Systemanvändare bör också göras uppmärksamma på riskerna med nätfiske (eng. phishing) och social manipulation (eng. social engineering).

Det är också viktigt att tillämpa ett *djupförsvarstänkande*, det vill säga att säkerhet implementeras i olika abstraktionslager, ytterst med verktyg på användarnivå för att skydda mot angrepp från exempelvis insiders. Djupförsvarstanken är särskilt relevant i de fall säkerhetsuppdateringar inte är möjliga eller otillräckliga för hantering av en specifik sårbarhet.

Användare av IoT-utrustning bör vara delaktiga i olika plattformar för informationsdelning. Dels för att rapportera sårbarheter, dels för att erhålla

[87] Department of Homeland Security 2016, s. 8.
[88] Se Schneier 2017c.

aktuell information om hot och sårbarheter från offentliga och privata aktörer. Leverantörer bör också förse användarna med information om avsikten med olika nätverksanslutningar. All uppkoppling måste ske medvetet och med kunskap om de risker som uppkopplingen medför. Direkt internetuppkoppling bör inte vara nödvändigt för kritiska funktioner i en IoT-enhet, särskilt inte i industriella sammanhang.

8.5 Myndigheter

Aktörerna som beskrivs tidigare i kapitlet kan alla vidta åtgärder för att minska riskerna med IoT, men åtgärder behöver även vidtas på en mer övergripande nivå. Det kan ske i olika former, bland annat som statlig reglering, initiativ från branschen (exempelvis standarder), riktade utbildnings- och informationsinsatser från myndigheter samt samverkan mellan branschen och myndigheterna. Initiativ av detta slag pågår bland annat i USA där DHS presenterat fyra övergripande strategier som de anser att den amerikanska myndighetssfären bör kraftsamla kring.[89]

- Koordinera myndigheterna så att de tillsammans med aktörer kan hitta sätt att minska riskerna med IoT.
- Bygga upp en medvetenhet om riskerna med IoT hos aktörerna.
- Identifiera och föreslå incitament för att förbättra IoT-säkerheten.
- Bidra till utvecklingen av internationella standarder för IoT.

Dessa strategier är mycket generella och antas här ha relevans även för svenska förhållanden. Nedan går vi igenom dessa i tur och ordning och ger med utgångspunkt hos DHS exempel på vad de kan innebära i praktiken.

8.5.1 Aktörsgemensamma aktiviteter för att hitta sätt att förbättra säkerheten i IoT

DHS anger att de kommer att fortsätta arbeta tillsammans med andra myndigheter och med samarbetspartners inom industrin för att hitta sätt att förbättra säkerheten inom IoT och för att öka kunskapen om nya tekniker som kan användas för att motverka risker med IoT.

Här följer ett axplock av de förslag som ges:

- Det bör finnas en gemensam policy för att offentliggöra information om sårbarheter, med tillhörande praxis för hantering av dem. Rapporter om sårbarheter kan exempelvis samlas in från olika forskar- och

[89] U.S. Department of Homeland Security 2016.

hackergrupper av ett Computer Security Incident Response Team (CSIRT) såsom CERT-SE. Som exempel nämns bland annat så kallade ”bug bounty”-program, som bygger på crowdsourcing-metoder för att identifiera sårbarheter som företags interna sårbarhetsanalysmetoder inte fångar upp.

- Myndigheter kan delta i olika plattformar för informationsdelning för att få aktuell och kritisk information om vanligt förekommande cyberhot och sårbarheter. Exempel på sådana plattformar är DHS:s *National Cybersecurity and Communications Integration Center* (NCCIC), mellanstatliga och sektorsspecifika informationsdelnings- och analyscenter (ISACs) samt informationsdelnings- och analysorganisationer.
- Utvecklare och tillverkare bör kunna ta fram en lista med kända hård- och mjukvarukomponenter utan att göra patentintrång eller andra avkall rörande immateriella rättigheter. En sådan lista kan vara ett värdefullt verktyg för andra aktörer för att förstå och hantera riskerna samt åtgärda potentiella sårbarheter baserat på inträffade händelser.
- Riskbedömningar bör genomföras över hela försörjningskedjan, med hänsyn till såväl interna risker som risker kopplade till tredjepartsleverantörer, där detta är möjligt.
- Det bör genomföras ”red team”-övningar, där systemutvecklare aktivt försöker gå förbi nödvändiga säkerhetsåtgärder i systemen. Den resulterande åtgärdsanalysen bör utgöra underlag till prioriteringar vad gäller var och hur ytterligare säkerhetsåtgärder ska införlivas.

8.5.2 Ökad medvetenhet om riskerna med IoT

För att höja kunskapen i säkerhetsfrågor, om vilka risker som finns och hur olika aktörer kan bemöta dem så kan MSB, länsstyrelser, sektorsansvariga och andra myndigheter hålla utbildningar, övningar och andra typer av träffar.[90] Sådana aktiviteter kan behöva skräddarsys för att passa olika aktörsgrupper eller sektorer, men det kan också vara värdefullt med gruppöverskridande aktiviteter där olika aktörer, till exempel leverantörer och användare, kan träffa varandra.

Även om det inte finns expertkunskap inom den egna organisationen, så behövs tillräckliga kunskaper för att kunna ställa rätt krav på de tjänster som köps in utifrån. Utöver utbildningar i syfte att öka beställarkompetensen så behöver det tas fram råd om vilka krav som bör ställas på säkerhet när tjänster som inbegriper IoT ska upphandlas.

[90] Detta är författarnas anpassning av DHS:s rekommendationer till svenska förhållanden.

Medvetandehöjande åtgärder kan också behöva riktas mot konsumenter för att öka kunskapen om hur riskerna med IoT kan minskas.

8.5.3 Incitament för förbättrad IoT-säkerhet

Incitamenten för olika aktörer att bidra till höjd säkerhet i IoT behöver stärkas. Idag är det ofta oklart vem som ansvarar för säkerheten i en viss produkt eller ett visst system. Kostnaden för bristande säkerhet bärs också sällan av de som har bäst förutsättningar att höja säkerheten.

DHS framhåller ett antal mekanismer som både kan höja säkerheten och stödja banbrytande innovation. Bland dessa kan nämnas skadeståndsansvar, cyberförsäkringar, frivillig certifiering samt lagar och regler i största allmänhet.

Regler som syftar till att åstadkomma en acceptabel lägstanivå vad gäller säkerhet bör införas. Många IoT-produkter säljs på en global marknad och ett sådant regelverk bör om möjligt tas fram inom ramen för internationella samarbeten. Ett sätt är att införa en internationell märkning av produkter som liknar den CE-märkning som är ett krav för att få sälja vissa produkter inom EU.[91] I avsaknad av internationellt överenskomna regler kan svenska myndigheter kräva att de produkter som säljs i landet håller en viss säkerhetsnivå. Sådana nationella regler finns bland annat i Storbritannien, Frankrike och Nederländerna.[92]

Förutom bindande regler kan frivilliga standarder och certifieringar användas. Utgångspunkt kan tas i den internationella standarden ISO/IEC 15408 *Common Criteria for Information Technology Security Evaluation* (ofta kallad *Common Criteria* eller *CC*). I Sverige är det certifieringsorganet för IT-säkerhet, CSEC, som har ansvar för opartisk granskning av produkters IT-säkerhet enligt denna standard.[93] Standarden är internationellt erkänd och anses vara obligatorisk för IT-produkter i kritiska infrastrukturer i flera länder.[94] Den tillämpas inom sektorer som försvar, finans, sjukvård, transport och kommunikation.

Europeiska kommissionen har föreslagit att ett ramverk för certifiering av IoT-produkter ska tas fram.[95] Enligt förslaget ska certifieringskraven antas av

[91] Se Eidenskog och Kamrani 2017.
[92] European Commission 2017.
[93] Sveriges Certifieringsorgan för IT-Säkerhet (CSEC) etablerades efter ett regeringsbeslut år 2002. CSEC är en oberoende enhet inom Försvarets materielverk (FMV) som representerar Sverige inom den europeiska organisationen SOGIS-MRA. Organisationen bygger på ömsesidigt erkännade av certifikat enligt Common Criteria som ges ut av medlemsländerna. CSEC utfärdar licenser till företag som utför granskningar enligt standardens regler samt utövar tillsyn över dessa företag och stöttar dem i granskningsarbetet. Se FMV 2016.
[94] http://www.fmv.se/Verksamhet/CSEC---Sveriges-Certifieringsorgan-for-IT-Sakerhet/. [Läst 2018-03-18]
[95] European Commission 2017.

kommissionen, men vara frivilliga att följa. Syftet med certifieringen är att få enhetliga regler för den europeiska marknaden för att på så sätt undvika att fragmentering och handelshinder uppstår som en följd av att olika länder har egna regler. Kommissionen föreslog även att ENISA får utökat ansvar och resurser så att de därmed blir EU:s cybersäkerhetsmyndighet, bland annat med ansvar för att ta fram certifieringen.

8.5.4 Utveckling av standarder för IoT

Myndigheter har goda möjligheter att delta i utvecklingen av standarder via arbetsgrupper inom olika standardiseringsorgan, branschorganisationer och lobbygrupper. Detta kan vara ett bra sätt att styra implementeringen av många av de strategier och principer som föreslås i denna rapport. DHS påpekar vikten av att åstadkomma konsistenta och internationellt erkända IoT-standarder, och inte bara sådana som är anpassade efter en specifik sektor eller ett specifikt lands förhållanden eftersom IoT i sig är del av ett globalt ekosystem.

9 Diskussion och slutsatser

I denna rapport har framkommit ett flertal strategier och åtgärdsförslag som är direkt relevanta för MSB i rollen som säkerhetskoordinerande och rådgivande myndighet. Även om avsnitt 8.5 är det som är mest direkt riktat till MSB, bör även andra aktörers särskilda utmaningar vara av intresse för att MSB på ett konstruktivt sätt ska kunna stötta dessa aktörer. Därmed är hela kapitel 8 relevant.

Nedan lyfter vi fram några saker som vi utifrån det samlade materialet tror är särskilt viktiga för MSB att ta med sig i det fortsatta säkerhetsarbetet. Framställningen ska ses som ett försök att förankra de principer som DHS föreslår (se punktlistan i början av kapitel 8) i den riskbild som vi har presenterat i kapitel 4–7.

Det finns väsentligen två vägar att eliminera risker, dels att minska sannolikheten för en händelse, så kallade *förebyggande åtgärder/strategier*, dels att mildra konsekvenserna, så kallade *konsekvenslindrande åtgärder/strategier*.

Principen om att **verka för säkerhetsuppdateringar och sårbarhetshantering** harmonierar med en strategi för förebyggande riskhantering. Denna måste i sin tur fokusera antingen på sårbarheterna i sig eller på attackvektorerna som utnyttjar dem:

- *Förebyggande avseende sårbarheter*: Brister i hanteringen av IoT-enheter som det tydligt går att göra något åt är svaga lösenord och för stor fysisk exponering. Den stora mängden IoT-enheter med bristande skydd (dåliga lösenord, svagt fysiskt skydd mm.) utnyttjas för att exempelvis skapa botnät som skannar av IT-utrustning. Heterogeniteten i IoT-beståndet gör det svårt att hålla koll på att enheterna inte utsätts för angrepp. Inom dessa områden har MSB en möjlighet att göra en riktad insats, exempelvis mot tillverkare och ägare av kameraövervakningssystem.
- *Förebyggande avseende attackvektorer*: Det kan noteras att många attackvektorer utgör eller kräver någon form av informationsinhämtning eller sekretessbrott (det senare om informationen är känslig eller hemlig). Sådan information kan användas direkt för exempelvis utpressning, men angrepp mot riktighet och tillgänglighet sker många gånger först i ett andra steg, med effekter i samhällsviktiga funktioner som tänkbar följd. Sådana angrepp skulle därmed kunna förhindras om själva informationsinhämtningen eller sekretessbrottet förhindrades, det vill säga att attacken kvävs i sin linda.

Även principerna om att **bygga in säkerhet i designfasen** (”security by design”) och **genomtänkt och försiktig anslutning** är väsentligen av förebyggande

karaktär. De kan också ses som uttryck för *ett konservativt förhållningssätt till risk* – lösenord ska vara säkra som standard, och om nödvändigt kunna ändras till något enklare och eventuellt mindre säkert, inte tvärtom. På motsvarande sätt ska en enhet inte levereras med några andra uppkopplingar än de som är nödvändiga för dess grundläggande funktion och syfte. Inte minst inom industriella tillämpningar gäller att enheter *inte ska vara uppkopplade i onödan.*

När det gäller konsekvenslindrande åtgärder så handlar det mycket om vanlig IT- och ICS-säkerhet eftersom IoT ofta utnyttjas för att ta sig in i IT- och ICS-system. Konsekvenserna av de flesta IoT-angrepp realiseras med andra ord i IT- och ICS-domänerna. En vettig strategi torde därmed vara att stärka det ordinära IT- och ICS-säkerhetsarbetet i samhällsviktig verksamhet för att säkerställa att *om* ett intrång lyckas så begränsas kanske ändå konsekvenserna. DHS:s princip om att **bygga på beprövad praxis** samt att **prioritera säkerhetsåtgärder utifrån potentiell påverkan** harmonierar med en sådan strategi. Rent konkret kan de konsekvenslindrande åtgärderna handla om att öka robustheten genom att redundans byggs in och genom robust hantering av feltillstånd i viktig utrustning.

Principen om att **verka för transparens** kan tolkas i termer av att syftet med att en enhet är uppkopplad tydligt ska kommuniceras till användarna. Det kan också betyda att information om händelser och sårbarheter ska kunna delas av många utan att detta äventyrar grundläggande kommersiella incitament. Några av de förslag som ges handlar om att bygga upp certifieringsmöjligheter, regelverk och standarder samt att stärka möjligheterna att ställa aktörer till svars för IoT-händelser. Det gäller att skapa incitament så att ”säkerhet lönar sig”. Genom att se säkerhet som ett attribut hos nätverksuppkopplade enheter har det hävdats att både tillverkare, leverantörer och tjänsteleverantörer ges en möjlighet till marknadsdifferentiering.[96] Den rörelse mot garanterat IoT-fria produkter som har gjort sig gällande under de senaste åren kan ge incitament till IoT-produkter där säkerhetsrelaterade aspekter på olika sätt är tagna i beaktande. Här finns säkerligen utrymme för flertalet tekniska certifieringar där MSB kan vara en viktig part som rådgivare, medkonstruktör och granskare.

Slutligen bör MSB bidra till en aktuell bild av de specifika instanserna av de generella sårbarheter som har tagits upp i denna rapport, det vill säga vilka de potentiella sårbarheterna *faktiskt* är. På samma sätt gäller att MSB bör bidra till kunskapen om vilka av dessa som *faktiskt* exploateras, som *faktiskt* leder till allvarliga konsekvenser och *vilka aktörer* det är som drabbas eller på annat sätt är involverade i attackerna.

[96] Department of Homeland Security 2016, s. 5.

9.1 Avslutande sammanställning – vad kan MSB göra?

I denna studie har en mängd olika sätt att närma sig IoT-säkerhetsrelaterade frågor presenterats. I det fortsatta arbetet för stärkt IoT-säkerhet föreslås MSB:

1. Verka för en riskhantering där förebyggande insatser riktas mot
    a. sårbarheter såsom bristfällig hantering av lösenord samt fysisk exponering
    b. informationsstöld och sekretessbrott, eftersom dessa kan vara första steget i en attacksekvens som i värsta fall hotar samhällsviktiga funktioner.
2. Förespråka ett konservativt förhållningssätt i termer av ”security by design”, t.ex. att produkter levereras med säkra lösenord som vid behov kan göras mindre säkra, samt att enheter inte ska vara uppkopplade i onödan.
3. Prioritera ordinärt IT- och ICS-säkerhetsarbete inom samhällsviktig verksamhet. Detta eftersom IoT ofta utnyttjas som en språngbräda in i dessa domäner och det alltså är där som de relevanta konsekvenserna manifesteras.
4. Verka för transparens inom IoT där syftet med uppkopplingen kommuniceras från leverantör till brukare och där information om händelser och sårbarheter kan delas av många utan att grundläggande kommersiella incitament äventyras.

Dessa rekommendationer harmonierar med DHS:s principer för ökad säkerhet i IoT.

Slutligen bör MSB försöka bidra till en aktuell bild av vilka de potentiella sårbarheterna är, vilka av dessa som *faktiskt* exploateras, som *faktiskt* leder till allvarliga konsekvenser och *vilka aktörer* det är som drabbas eller på annat sätt är involverade i attackerna.

Referenser

Anderson, R. (2017). *Internet of Things Problems – Computerphile*. Videoklopp tillgängligt på: https://www.youtube.com/watch?v=PLiE0Nr8VOE. Besökt 2017-12-28.

Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers and Security, 68*, 81-97.

Atamli, A. W., & Martin, A. (2014). Threat-based security analysis for the internet of things. Paper presented at the *Proceedings - 2014 International Workshop on Secure Internet of Things, SIoT 2014*, 35-43.

Billure, R., Tayur, V. M., & Mahesh, V. (2015). Internet of things - A study on the security challenges. Paper presented at the *Souvenir of the 2015 IEEE International Advance Computing Conference, IACC 2015*, 247-252.

BITAG (2016). *Internet of Things (IoT) Security and Privacy Recommendations.* A broadband internet technical advisory group technical working group report. A Uniform Agreement Report Issued: November 2016.

Bugeja, J., Jacobsson, A., & Davidsson, P. (2016). On privacy and security challenges in smart connected homes. In *European Intelligence and Security Informatics Conference (EISIC)*, 172-175, IEEE Computer Society, 2016.

Cherdantseva, Y., Hilton, J., Rana, O., & Ivins, W. (2016). A multifaceted evaluation of the reference model of information assurance & security. *Computers and Security, 63*, 45-66.

cisco (2014). *The Internet of Things Reference Model.* Tillgänglig på: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf. Besökt 2017-02-12.

Computer Sweden (2017). *Totalsträckskryptering*. IT-ord. Tillgänglig på: https://it-ord.idg.se/ord/totalstrackskryptering/ Besökt 2017-11-09.

Den digitala resan (2015). *Vad är Internet of Things?* Tillgänglig på: http://dendigitalaresan.se/vad-ar-internet-of-things/ Besökt 2018-02-25.

Department of Homeland Security 2016. *Strategic principles for securing the Internet of Things (IoT).* Version 1.0 November 15, 2016.

Dickson, B. (2016). *The IoT ransomware threat is more serious than you think.* Tech Talks 2016-08-22. Tillgänglig på: https://bdtechtalks.com/2016/08/22/the-iot-ransomware-threat-is-more-serious-than-you-think/.

Eidenskog, D., & Kamrani, F. (2017). Internet of Things – en IT-säkerhetsmässig mardröm. I Hull Wiklund, C., Faria, D., Johansson, B., & Öhrn-Lundin, J. (red.). *Strategisk utblick 7. Närområdet och nationell säkerhet.* FOI-R--4454--SE, Stockholm.

ENISA (2017). *Baseline Security Recommendations for IoT – in the context of Critical Information Infrastructures.* European Union Agency For Network And Information Security. November 2017.

European Commission (2016). *Advancing the Internet of Things in Europe. Accompanying the document Communication from the Commission to the European parliament the Council, the European economic and social committee of the regions: Digitising European Industry. Reaping the full benefits of a Digital Single Market.* Commission staff working document.

European Commission (2017). *Cybersecurity. EU agency and certification framework.* State of the Union 2017. Factsheet on the EU Cybersecurity Agency. Tillgänglig på: http://europa.eu/rapid/attachment/IP-17-3193/en/Cybersecurity-EU%20agency%20and%20certification%20framework.en.pdf. Besökt 2018-02-13.

FMV (2016). *CESC*. Web-plats. Tillgänglig på: https://www.fmv.se/sv/Verksamhet/CSEC---Sveriges-Certifieringsorgan-for-IT-Sakerhet/. Besökt 2018-02-13.

Frånberg, Ö. (2014). *Grunden för loT är en referensarkitektur.* Presentation vid IoT-seminarium hos Ericsson i Kista 26 oktober 2014. Tillägänglig på: http://docplayer.se/8275629-Iot-utblick-26-oktober-ericsson-kista-osten-franberg-iot-direktor-lulea-tekniska-universitet-centrum-for-distansoverbryggande-teknik.html. Besökt 2018-02-13.

Gartner (2017). *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016.* Newsroom. Press Release 2017-02-07. Tillgänglig på: https://www.gartner.com/newsroom/id/3598917. Besökt 2017-10-02.

Hallberg, J., Bengtsson, J., & Karlzen, H. (2015). *Bedömning av sannolikhet och konsekvens för informationssäkerhetsrisker - En studie av vikt.* Totalförsvarets forskningsinstitut, FOI-R--4152--SE, Linköping.

IEC 31010:2009. *Risk management -- Risk assessment techniques.* International Organization for Standardization.

Jing. Q., Vasilakos, A.V., Wan, J., Lu, J., & Qui, D. (2014) Security of the Internet of Things: perspectives and challenges. *Wireless Netw. 20:2481-2501.*

Kamrani, F., Wedlin, M., & Rodhe, I. (2016). *Internet of Things: Security and Privacy Issues.* Totalförsvarets forskningsinstitut, FOI-R—4362—SE, Linköping.

Karresand, M. (FOI), personlig kommunikation via e-post 2017-08-28.

Khan, W. Z., Aalsalem, M. Y., Khan, M. K., & Arshad, Q. (2017). When social objects collaborate: Concepts, processing elements, attacks and challenges. *Computers and Electrical Engineering, 58*, 397-411.

Kumar, S. A., Vealey, T., & Srivastava, H. (2016). Security in internet of things: Challenges, solutions and future directions. Paper presented at the *Proceedings of the Annual Hawaii International Conference on System Sciences, 2016-March* 5772-5781.

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2016). Internet of things (IoT) security: Current status, challenges and prospective measures.

Microsoft Azure 2018. *Internet of Things security best practices*. Web-sidor och nedladdningsbart document. Tillgänglig på: https://docs.microsoft.com/en-us/azure/iot-suite/iot-security-best-practices. Besökt 2018-02-12.

Moe, M. (2016). Go Ahead, Hackers. Break My Heart. Wired 2016-03-14. Tillgänglig på: https://www.wired.com/2016/03/go-ahead-hackers-break-heart/. Besökt 2017-12-06.

Mohsen Nia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. *IEEE Transactions on Emerging Topics in Computing, PP*(99).

Nastase, L. (2017). Security in the Internet of Things: A Survey on Application Layer Protocols. *21st International Conference on Control Systems and Computer Science.*

Postscapes (2018). *Internet of Things Infographic. What Is The "Internet of Things"?* Tillgänglig på https://www.postscapes.com/what-exactly-is-the-internet-of-things-infographic/ Besökt 2018-02-25.

Samonas, S. & Coss, D. (2014). The CIA strikes back: redefining confidentiality, integrity and availability in security. *Journal of Information System Security*. 2014, 10;3, 21-45.

Schneier, B. (2017a). *Botnets of Things*. MIT Technology Review March/April 2017. Tillgänglig på: https://www.schneier.com/essays/archives/2017/03/botnets_of_things.html. Besökt 2018-02-12.

Schneier, B. (2017b). *The next ransomware attack will be worse than WannaCry.* The Washington Post 2017-05-17. Tillgänglig på: https://www.washingtonpost.com/posteverything/wp/2017/05/16/the-next-ransomware-hack-will-be-worse-than-the-current-one/?utm_term=.bccfef3b8f75. Besökt 2018-02-12.

Schneier, B. (2017c). *Click Here to Kill Everyone.* New York Magazine 2017-01-27. Tillgänglig på: https://www.schneier.com/essays/archives/2017/01/click_here_to_kill_e.html. Besökt 2018-02-13.

Sethi, P., & Sarangi, S.R. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*, vol. 2017, 1-25.

Sherasiya, T., & Upadhyay, H (2016) Intrusion Detection System for Internet of Things. IJARIIE Vol-2 Issue-3 2016.

Shifa, A., Asghar, M. N., & Fleury, M. (2016). Multimedia security perspectives in IoT. Paper presented at the *2016 6th International Conference on Innovative Computing Technology, INTECH 2016*, 550-555.

Stafford, C. (2016). *IoT security issues and vulnerabilities.* 2016-12-15. Tillgänglig på http://searchcompliance.techtarget.com/video/IoT-security-issues-and-vulnerabilities, Besökt 2018-03-20.

Tritec (2018). *Internet of Things.* Tillgänglig på: http://tritec.se/erbjudande/internet-of-things/. Besökt 2018-02-25.

Wikipedia (2017). *Buffertöverskridning*. Tillgänglig på: https://sv.wikipedia.org/wiki/Buffert%C3%B6verskridning. Besökt 2017-11-06.

Wikipedia (2018a). *Sakernas internet.* Tillgänglig på: https://sv.wikipedia.org/wiki/Sakernas_internet Besökt 2018-02-25.

Wikipedia (2018b). *Radio Frequency Identification.* Tillgänglig på: https://sv.wikipedia.org/wiki/Radio_Frequency_Identification. Besökt 2018-03-20.

Zhao, K., & Ge, L. (2013). A Survey on the Internet of Things Security. Paper presented at the 2013 *9th International Conference on Computational Intelligence and Security, INTECH 2013*, 663-667.

Zunnurhain, K. (2016). Vulnerabilities with Internet of Things. Paper presented at the *International Conference of Security and Management, SAM'16*, 83-88.

Bilaga 1: Attackvektorer och motåtgärder

I denna bilaga redovisas exempel på möjliga angrepp och motåtgärder uppdelade på respektive lager i den tredelade modell som presenterades i avsnitt 2.2.2. Motåtgärderna tas primärt med för att ge bakgrund och perspektiv åt attackvektorerna, inte för att de skulle utgöra goda strategier för exempelvis MSB.

Många av beskrivningarna av attacker och motmedel för perceptionslagret är hämtade från en artikel av Mohsen Nia och Jha.[97] Den utgår i sin tur från en sjudelad modell av IoT, hämtad från Cisco.[98] Vi har inte hittat några lika detaljerade genomgångar av attacker och motmedel i överföringslagret och applikationslagret och därför beskrivs dessa mer översiktligt.

I många fall finns inga etablerade svenska översättningar av de engelska termerna, och ibland är det de engelska termerna som används även i svenskt tal och skrift. I de fall då det råder tveksamheter kring vilken term som är mest gångbar i svenskt språkbruk anges även den engelska termen.

B1.1 Attacker mot perceptionslagret

Perceptionslagret motsvaras av *edge-side layer* i Mohsen Nia och Jhas modell. Det delas in i de tre underkategorierna *edge nodes*, *kommunikation* och *edge computing*.

- Edge nodes består av **beräkningsnoder** (eng. computing nodes**),** till exempel RFID-läsare eller sensorer, och **RFID-taggar**.
- **Kommunikation** består av alla komponenter som möjliggör överföring av information eller kommandon mellan enheter och komponenter i perceptionslagret.
- **Edge computing**, även kallat fog computing, utför enklare bearbetning av data som minskar belastningen på högre nivåer och ger snabbare respons. Många realtidsapplikationer behöver utföra beräkningar så nära utkanten av nätverket som möjligt. Hur mycket bearbetning som sker här beror på vilken datorkraft som finns tillgänglig från serviceleverantörer, servrar och beräkningsnoder. Vanligtvis är det enkel signalbearbetning och inlärningsalgoritmer som används.

[97] Mohsen Nia & Jha 2016
[98] Se Mohsen Nia & Jha 2016 och cisco 2014.

B1.1.1 Attacker mot beräkningsnoder

Nedan beskrivs attacker mot beräkningsnoder (eng. computing nodes), exempelvis RFID-läsare och sensorer.

- **Hårdvarutrojaner**: En hårdvarutrojan (eng. hardware trojan) är en skadlig modifiering av en integrerad krets som ger angriparen möjlighet att använda kretsen och dess funktionalitet för att komma åt data eller program som finns på den.[99]
- **Sidokanalsattacker och avlyssning**: Alla noder kan avslöja kritisk information under normal användning även när de inte använder trådlös kommunikation för att överföra data. Ett exempel är den elektromagnetiska signaturen som noden sänder ut. Även kommunikationskanaler kan avlyssnas. På så sätt kan en angripare komma åt användarnamn och lösenord och annan kontrollinformation, exempelvis delade nätverkslösenord eller identifikationsuppgifter för noder. Med hjälp av denna information kan angriparen sedan exempelvis sätta upp obehöriga noder i systemet.[100]
- **Invasiva attacker och hårdvarumanipulation**: Enheter som är placerade på oskyddade platser, till exempel utomhus, kan angripas fysiskt. Angripare med fysisk tillgång till enheter kan exempelvis extrahera krypterad information, manipulera kretsar, modifiera programvara eller byta operativsystem. Fysiska attacker kan förstöra enheten permanent och syftet är ofta att utvinna information för användning vid ett senare tillfälle.[101]
- **Replikering av noder**: Angriparen tillför en ny nod till en befintlig uppsättning noder genom att kopiera och använda en annan nods identifikationsdata. På så sätt kan angriparen skaffa sig tillgång till delade kryptonycklar samt slå ut legitima noder. Angriparen kan dessutom lätt föra in fel, injicera falska data, styra nätverket eller dirigera inkommande paket åt fel håll.[102] Den falska nodens aktiviteter kan leda till minskad prestanda i nätverket och om de övriga noderna i systemet dräneras på batterikraft kan konsekvenserna bli desamma som vid en överbelastningsattack.[103]
- **Denial of service**: Denial of service (DoS) innebär att en tjänst är otillgänglig för en behörig användare. DoS kan exempelvis uppnås

[99] Mohsen Nia & Jha 2016, Shifa m.fl. 2016.
[100] Mohsen Nia & Jha 2016.
[101] Mohsen Nia & Jha 2016, se även Billure m.fl. 2016, Mahmoud m.fl. 2016, Shifa m.fl. 2016 och Atamil & Martin 2014.
[102] Mohsen Nia & Jha 2016.
[103] Ashibani & Mahmoud 2017 och Mahmoud m.fl. 2015.

genom att angriparen skickar en mängd meddelanden i syfte att överbelasta enheter, för att på så sätt hindra dem från att utföra sina vanliga sysslor, kommunicera med andra enheter eller för att dränera dem på batterikraft.[104] Det kan också ske genom att enheten stjäls, att dess programvara manipuleras eller genom att dess kommunikationskanal störs.[105]

B1.1.2 Attacker mot RFID-taggar

RFID är en teknik för att läsa information på avstånd från transpondrar och minnen.[106] I sin enklaste form kan en RFID-tagg sända ut ett unikt nummer några decimeter. I ett något mer avancerat utförande har taggen ett inbyggt minne som det går att skriva till flera gånger, men minnet är ändå väldigt begränsat. Nedan ges exempel på attacker mot RFID-taggar.

- **Avlyssning**: Nästan alla RFID-taggar har unika identifikationsuppgifter som olovligen kan avläsas av en RFID-läsare som placeras i närheten av taggen. Informationen kan sedan användas som ingångsvärden i exempelvis kloning (se nedan).[107] Vissa taggar innehåller information om den produkt som de är fästa på, och gör det möjligt att exempelvis läsa av vilken medicinsk utrustning som en person har med sig eller på sig.[108] Själva avläsningen kan även ge direkt tillgång till känslig information som exempelvis kreditkortsnummer.[109]
- **Kloning**: RFID-taggar kan kopieras och förfalskas i syfte att ge angriparen tillträde till fysiska platser med begränsat tillträde eller tillgång till bankkonton och känslig information.[110]
- **Återuppspelning**: I en återuppspelningsattack blir kommunikationssignalen mellan RFID-taggen och läsaren uppfångad för att spelas upp vid varje förfrågan från läsaren. På så sätt reproduceras taggens innehåll.[111]

[104] Mohsen Nia & Jha 2016, Ashibani & Mahmoud 2017, Shifa m.fl. 2016, Stout & Urias 2016 och Mahmoud m.fl. 2015.
[105] Atamli & Martin 2014.
[106] Wikipedia 2018.
[107] Mohsen Nia & Jha 2016 och Kumar 2016.
[108] Mohsen Nia & Jha 2016, Atamli & Martin 2014.
[109] Mohsen Nia & Jah 2016, Kumar m.fl. 2016.
[110] Mohsen Nia & Jha 2016, Shifa m.fl. 2016, Stout & Urias 2016 och Atamli & Martin 2014.
[111] Shifa m.fl. 2016 och Mahmoud m.fl. 2015.

B1.1.3 Attacker mot kommunikationen

Nedan beskrivs attacker mot kommunikationen i perceptionslagret, det vill säga alla komponenter som möjliggör överföring av information eller kommandon mellan enheter och komponenter i perceptionslagret. Det kan röra sig om att föra in felaktig data, att på olika sätt störa kommunikationen eller att avlyssna information.

- **Injicering av paket**: En angripare kan injicera felaktiga paket i kommunikationslänkar på tre olika sätt.[112]
    - Genom att tillföra nya paket till nätverkskommunikationen och få dessa att accepteras som legitima.
    - Genom att fånga in befintliga paket, manipulera dem och sedan skicka dem vidare.
    - Genom att paket som tidigare har spelats in återuppspelas. Ett system som inte håller reda på tidigare paket eller tidigare tillstånd i systemet kan vara sårbart för denna typ av attack.
- **Routingattacker**: Attacker som påverkar hur meddelanden dirigeras kan användas för att vilseleda, feldirigera eller för att ta bort paket. I den enklaste typen av attack ändras routing-informationen genom att routing-loopar eller falska felmeddelanden genereras. Det finns även flera andra sätt, där Mohsen Nia och Jha[113] listar följande:
    - *Black hole*: En skadlig nod attraherar all trafik i nätverket genom att avisera att den kan erbjuda den kortaste vägen till destinationen i nätverket. Angriparen kan sedan bearbeta paketen eller ta bort dem.[114]
    - *Grey hole*: Ungefär samma som black hole, men här attraheras endast utvalda paket.
    - *Worm hole*: Paket som hittas på en plats förs till en annan plats.
    - *Hello flood*: Noder måste markera sin närvaro för sina grannar genom att sända ut en så kallad ”Hello packet”-hälsningssignal. En skadlig nod kan sända ut en stark hälsningssignal för att få alla andra noder i nätverket att tro att den är en granne.

[112] Mohsen Nia & Jha 2016. Ashibani & Mahmoud 2017 tar upp denna typ av attack under överföringslagret.
[113] Mohsen Nia & Jha 2016. Ashibani & Mahmoud 2017 och Shifa mfl 2016 tar upp denna typ av attack under överföringslagret.
[114] Se även Billure mfl 2016.

- *Sybil*: Angriparen använder en nod med falsk identitet för att rösta ut legitima noder ur systemet.

- **Sidokanalsattacker**: Avancerade verktyg används för att fånga upp och bearbeta kommunikation så att information kan utvinnas ur olika mönster, även om informationen i sig är krypterad. Det kan till exempel röra sig om tiden mellan två på varandra följande paket (så kallad timing attack), vilket frekvensband kommunikationen sker på och hur den är modulerad. Sådana icke-invasiva attacker är mycket svåra att upptäcka och således också svåra att skydda sig mot.[115]
- **Störsändning** (eng. spoofing): Radiosignaler kan sändas ut i syfte att störa kommunikationen. Genom sådan störning kan också batteridränering åstadkommas då enheten gång på gång försöker sända sitt meddelande.[116]

B1.1.4 Attacker mot ”edge computing”

Nedan beskrivs attacker mot edge computing, även kallat fog computing, det vill säga beräkningar som utförs i utkanten av nätverket.

- **Injicering av data**: Otillräcklig validering av indata kan möjliggöra injektion av fientlig indata. Angriparen kan sedan exempelvis stjäla data, manipulera databasers innehåll eller gå runt autentisering.[117]
- **Sidokanalsattacker**: Angriparen kan använda information som läckt ut från andra komponenter, exempelvis servrar, för att attackera sidokanaler. Mångordiga felmeddelanden kan till exempel innehålla information som är användbar för angripare.[118]
- **Störning av maskininlärning**: Maskininlärningsmetoder som används i IoT kan angripas, exempelvis genom att träningsdata manipuleras vilket i sin tur ändrar träningsprocessens resultat.[119]

B1.2 Möjliga motåtgärder i perceptionslagret

I detta avsnitt presenteras några möjliga motåtgärder mot attacker i perceptionslagret. Den mest fullständiga genomgång av motåtgärder som vi har

[115] Mohsen Nia & Jha 2016.
[116] Billure m.fl. 2016.
[117] Mohsen Nia & Jha 2016, Ashibani & Mahmoud 2017, Kumar m.fl. 2016, Stout & Urias 2016 och Atamli & Martin 2014.
[118] Mohsen Nia & Jha 2016.
[119] Mohsen Nia & Jha 2016.

hittat finns hos Mohsen Nia och Jha och detta avsnitt bygger i sin helhet på deras framställning.[120]

B1.2.1 Motåtgärder för attacker mot beräkningsnoder

Nedan listas några tänkbara motåtgärder för attacker mot beräkningsnoder.

- **Analys av sidokanalssignaler**: Genom att analysera sidokanalssignaler som tid, energiförbrukning och temperatur kan både hårdvarutrojaner och skadlig programvara (inbyggd och tillagd) upptäckas. Signalerna analyseras för att upptäcka om en enhet beter sig onormalt. En betydande ökning av energiförbrukningen kan till exempel tyda på ett skadligt program har installerats på en enhet.
- **Aktivering av trojaner**: Det finns olika sätt att medvetet aktivera trojaner i syfte att upptäcka och eliminera dem. Trojanerna identifieras genom analys av skillnaden i beteenden, output och sidokanalsläckage mellan en trojanfri och en trojaninfekterad krets.
- **Policy-baserad intrångsdetektering** handlar om att ett system detekterar brott mot viktiga policyer, exempelvis avvikande förfrågningar till en nod som skulle kunna leda till batteridränage och liknande.
- **Ändring av hårdvara**: Enligt Mohsen Nia & Jha är ändringar i hårdvaran ett av de effektivaste sätten att skydda sig mot fysiska angrepp, sidokanalsattacker och trojaner. Här är några exempel på sådana ändringar:
    - *Manipulationsskydd och självförstörelse*: Noder kan designas på ett sätt som gör det svårare att bryta sig in i dem. En annan möjlighet är att använda en självförstöringsmekanism som löser ut om noden angrips fysiskt.
    - *Minimering av informationsläckage*: För att minska risken för informationsläckage över sidokanalen kan slumpmässiga fördröjningar och avsiktligt brus läggas till. Andra möjligheter är att använda mjukvara med konstant exekveringstid (eng. constant execution path code), förbättra cache-arkitekturen eller skärma av elektroniska kretsar.
    - *Integrering av hårdvara som inte går att klona* (physically unclonable function, PUF): PUF är en funktion som genererar brus i en integrerad krets. PUF:ar möjliggör unik identifiering

[120] Avsnittet är baserat på Mohsen Nia & Jha 2016.

och autentisering samt detektion av trojaner (eftersom dessa påverkar signalen).

B1.2.2 Motåtgärder för attacker mot RFID-taggar

Mohsen Nia och Jha ger ett antal exempel på vad som kan göras när det gäller attacker mot RFID-taggar, men påpekar också att de är svåra att skydda helt på grund av deras inneboende egenskaper.

- **Avstängningskommando**: Vid produktionen av en RFID-tagg kan en funktion läggas in som gör att RFID-läsaren kan stänga av taggen eller försätta den i viloläge. Detta för att den inte längre ska kunna överföra någon information.
- **Isolering**: Ett sätt att skydda taggars integritet är att isolera dem från elektromagnetiska signaler. Detta kan göras genom att innesluta dem i ett material som blockerar elektromagnetiska signaler.
- **Anonyma taggar**: RFID-taggarna kan tilldelas anonyma identiteter som skyddas av kryptering. Taggarna ska dock inte ha fasta anonyma identiteter för då kan de ändå vara sårbara för spårning.
- **Estimering av avstånd**: RFID-taggen ges förmåga att läsa av avståndet till läsaren och bara avge sin information inom en viss radie.
- **Lokal brandvägg**: En brandvägg kan implementeras i enheter som har tillräcklig beräkningskapacitet för att stödja en sådan, exempelvis en mobiltelefon. Med brandväggen kan sofistikerade regler sättas upp, exempelvis att taggen inte ska avge sin information om den inte befinner sig i närheten av en viss geografisk punkt.
- **Kryptografiska metoder**: Mohsen Nia och Jha tar upp tre typer av kryptografiska metoder.
    - *Kryptering*: Fullständig kryptering är vanligen resurskrävande och därför har sådan inte varit så utbredd i RFID-taggar som behöver hålla låg kostnad.
    - *Hash-baserad kod*: Taggen förblir låst tills den öppnas med en kod som skickas från läsaren. För att undvika spårning är det bra om koden ändras på ett för angriparen oförutsägbart sätt.
    - *Enkla kryptografiska protokoll*: Flera kryptografiska protokoll som inte är så resurskrävande har föreslagits för användning i RFID-taggar. Dessa protokoll kan användas för autentisering av taggar, men kan knäckas av en resursstark angripare.

B1.2.3 Motåtgärder för attacker mot kommunikationen

Här följer några förslag på motåtgärder för attacker mot kommunikationen i perceptionslagret.

- **Tillförlitlig routing**: En egenskap hos IoT-nätverk, som gör det svårt att införa säkra routingprotokoll är att mellanliggande noder eller servrar kan kräva direkt access till ett meddelandes innehåll innan de skickar det vidare.
- **Intrångsdetektering**: Med hjälp av intrångsdetekteringssystem (eng. intrusion detection system, IDS) kan routingattacker upptäckas. De flesta intrångsdetekteringssystem är utvecklade för trådlösa sensornätverk eller för vanliga datornätverk, men numera finns även metoder som är inriktade på IoT.
- **Kryptografiska metoder**: Kryptografiska metoder är effektiva, men för IoT behövs metoder som inte kräver så mycket batterikapacitet, processorkapacitet och minne. Sådana är under utveckling. Dock saknas fortfarande krypteringsmetoder med publika nycklar som passar för IoT-enheter med begränsade resurser.
- **Dölja trafikmönster**: Tekniker för att dölja trafikmönster, så kallad de-patterning, kan skydda mot sidokanalsattacker genom att falska paket tillsätts, vilka ändrar trafikmönstret för att vilseleda en angripare.

B1.2.4 Motåtgärder för attacker mot ”edge computing”

Även angrepp mot beräkningarna i perceptionslagret går i viss mån att skydda sig mot.

- **Tester**: Innan uppdateringar och andra funktioner implementeras i kritiska system kan beteendet hos hela systemet (med routrar, edge-noder och servrar med mera) undersökas genom att olika angrepps-scenarier identifieras och simuleras.
- **Detektion av avvikelser**: Med olika metoder kan avvikelse i form av datapunkter som inte hör till det rätta datasetet upptäckas. Detta kan användas för att skydda mot attacker mot maskininlärning och riktighet.
- **Intrångsdetektering**: Intrångsdetekteringssystem kan upptäcka en skadlig nod som försöker införa ogiltig information i systemet eller som bryter mot regler.

B1.3 Attacker mot överföringslagret

I överföringslagret sker utbyte och bearbetning av data mellan perceptionslagret och applikationslagret. Överföringen kan ske på olika sätt, men ofta används internet. Attacker i det här lagret har ofta att göra med någon form av *dataläckage*, exempelvis genom att det tranmissionsmedium som används vid trådlös kommunikation är öppet. Sådana attacker kan fånga upp ett sänt meddelande, modifiera det och sedan skicka det vidare. Angripare kan också dra nytta av mekanismer för fjärraccess i nätverk med många anslutna nätverksnoder för att generera överbelastning.[121] Nedan följer några exempel på attacker mot överföringslagret.

- **Loopar**: Routing-angrepp kan, som nämndes ovan, ge upphov till loopar som får till följd att meddelanden fördröjs.[122]
- **Maskhål** (eng. wormhole) erbjuder falska vägar genom ett nätverk som alla paket skickas genom.[123]
- **Selektiv vidarebefordran** (eng. selective forwarding) innebär att en angripen nod slänger vissa paket, medan vissa utvalda paket skickas vidare.[124]
- **Slukhål** (eng. sinkhole): En falsk bästa väg att nå andra noder tillkännages av den angripna noden, vilket gör att paket kommer på avvägar. Denna attack kan användas som ett led i andra attacker som selektiv vidarebefordran och störsändning.[125]
- **Störsändning** (eng. spoofing) innebär att angriparen blockerar den trådlösa kanalen mellan sensornoden och basstationen. Detta kan göras genom att en signal eller brus med samma frekvens förs in. Detta kan leda till DoS.[126]
- **DoS-attack**: I överföringslagret kan DoS skapas genom att angriparen orsakar massiv indata-trafik eller avsiktligt blockerar kommunikationskanaler.[127]
- **Avlyssning**: Genom avlyssning kan angriparen fånga upp information som skickas genom nätverket.[128]

[121] Stycket baserat på Ashibani & Mahmoud 2017.
[122] Ashibani & Mahmoud 2017 och Shifa m.fl. 2016.
[123] Ashibani & Mahmoud 2017.
[124] Ashibani & Mahmoud 2017.
[125] Ashibani & Mahmoud 2017.
[126] Ashibani & Mahmoud 2017.
[127] Shifa m.fl. 2016, Mahmoud m.fl. 2015 och Kumar m.fl. 2016.
[128] Shifa m.fl. 2016.

- **Passiv övervakning**: En angripare kan observera och analysera en IoT-enhets trafik över nätverket i realtid och ändra identifikationsreglerna samt märka ut vissa aktiviteter.[129]
- **Identitetsstöld**: En angripare kan ”sniffa” autentiseringsinformation som lösenord, produktkod (EPC-kod) eller upplåsningsmetod för en enhet.[130]
- **Injicering av felaktig information**: En angripare kan föra in falska data och på så sätt få systemet att agera felaktigt eller farligt.[131]

B1.4 Möjliga motåtgärder i överföringslagret

Dataöverföring mellan enheter kan medföra risker som har sitt ursprung i att enheter som är anslutna till ett nätverk inte är kompatibla med varandra. För att komma tillrätta med dessa risker räcker det inte att använda konventionella protokoll som utvecklats för internet, även om dessa kan ge ett visst skydd.[132]

Enheterna bör ha möjlighet att upptäcka onormala beteenden eller situationer som kan påverka systemets säkerhet. För detta behövs robusta överföringsprotokoll och programvaror som kan upptäcka intrång.[133] Gemensamma standarder föreslås ofta som ett sätt att hantera mångfalden av apparater, programvaror och protokoll som kan ingå i ett system.[134]

Det är önskvärt att ett nätverk ska kunna fortsätta att fungera även om vissa noder slås ut eller stjäls. Det ska också gå lätt att lägga till nya noder utan att nätverket störs. Självläkande nätverk är ett nytt forskningsområde inom IoT.[135]

En viktig fråga när det gäller säkerheten i överföringslagret är hur enheter kopplar upp sig mot varandra eller mot ett nätverk. I de fall då uppkoppling görs peer-to-peer, det vill säga att kommunikationen sker direkt mellan noder utan att först passera en basstation, kan otillåten nod-access behöva motverkas genom tekniker för autentisering eller auktorisering. Datasäkerheten kan behöva stärkas genom mekanismer för autentisering och hantering av krypterade nycklar, liksom kryptering av överförd information.[136]

Wi-Fi är trådlösa nätverk med en mängd olika tillämningar. Det är ett så kallat centriskt nätverk där kommunikationen mellan noderna sker genom fasta bryggor

[129] Shifa m.fl. 2016.
[130] Shifa m.fl. 2016.
[131] Kumar m.fl. 2016.
[132] Ashibani & Mahmoud 2017 och Mahmoud m.fl. 2015.
[133] Ashibani & Mahmoud 2017.
[134] Mahmoud m.fl. 2015.
[135] Billure m.fl. 2015
[136] Ashibani & Mahmoud 2017 och Mahmoud m.fl. 2015.

(accesspunkter). Enheterna kan koppla upp sig och kommunicera trådlöst med varandra över internet via Wi-Fi-nätverken. För att motverka angrepp i centriska nätverk kan olika mekanismer för accesskontroll och nätverkskryptering användas.[137]

B1.5 Attacker mot applikationslagret

Enligt Ashibani och Mahmoud är de viktigaste frågorna för applikationslagret att förhindra otillåten access och att privata uppgifter avslöjas. Stora mängder användarinformation samlas i detta lager och här kan attacker få till följd att data skadas och att information hamnar i orätta händer.[138] Här följer några exempel på attacker mot applikationslagret.

- **Bufferöverskridande**: Vid buffertöverskridning försöker programmet spara mer information i en buffert än vad som får plats. Ofta skrivs data då över, vilket kan leda till störningar, krascher eller orsaka säkerhetshål, beroende på vilken data som skrivs över, vad den skrivs över med och hur situationen hanteras av programvaran.[139] Angriparen kan utnyttja dessa svagheter för att iscensätta andra attacker.[140]
- **Skadlig kod**: Användarapplikationen kan utsättas för olika typer av skadlig kod, som virus, maskar och trojaner, vilket kan orsaka skada och få nätverket att sakta ner. [141] Skadlig programvara kan införas vid exempelvis programuppdateringar.[142]
- **Informationsfusion**: IoT-applikationer kan innehålla många personliga och konfidentiella uppgifter, som till exempel var ett objekt befinner sig, individers beteenden och deras sociala relationer eller en organisations historiska data. Information från flera källor kan läggas samman för att dra slutsatser om personer och organisationer. Denna information kan sedan användas för kriminella aktiviteter eller säljas vidare.[143]
- **Nätfiske (phishing)**: Angriparen skickar till synes legitima meddelanden till användare från övertagna enheter för att få tillgång till identifikations- och inloggningsuppgifter eller för att introducera skadlig kod i mottagarens system.[144]

[137] Ashibani & Mahmoud 2017.
[138] Ashibani & Mahmoud 2017.
[139] Wikipedia 2017.
[140] Ashibani & Mahmoud 2017.
[141] Ashibani & Mahmoud 2017 och Kumar m.fl. 2016.
[142] Shifa m.fl. 2016.
[143] Shifa m.fl. 2016.
[144] Shifa m.fl. 2016.

- **DoS**: Applikationslagret innehåller olika typer av programvaror som kan utsättas för överbelastningsattacker.[145]
- **Social manipulation** (eng. social engineering): Genom social manipulation kan IoT-användare luras att utföra handlingar eller avslöja konfidentiell information. Ett exempel på detta är nätfiske (se ovan). [146]

B1.6 Möjliga motåtgärder i applikationslagret

Olika applikationer har olika behov av säkerhetslösningar. Ashibani och Mahmoud tar upp följande:[147]

- **Kryptering**: Vid totalsträckskryptering (eng. end-to-end) är det bara sändare och mottagare som kan läsa meddelandena i klartext. Routrar, switchar eller annan nätverksutrustning som meddelandet passerar på väg mellan avsändare och mottagare vidarebefordrar meddelandet utan att dekryptera det.[148]
- **Intrångsdetektering**: Intrångsdetekteringssystem kan känna igen signaturer av välkända attacker och identifiera otillåten nätverksaktivitet (mänsklig eller maskinell).[149]
- **Autentisering och auktorisering av användare**: Olika autentiserings- och auktoriseringsmekanismer finns för att försäkra sig om att inga obehöriga användare eller enheter får tillgång till information.

[145] Shifa m.fl. 2016.
[146] Nastase 2017, Shifa m.fl. 2016,
[147] Ashibani & Mahmoud 2017.
[148] Computer Sweden 2017.
[149] Sherasiya & Upadhyay 2016.

Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

www.msb.se