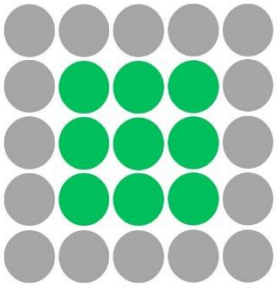

Robust & Säker IoT

Vägledning för Robust och Säker IoT

2020-03-01

Ver 1.0

INNEHÅLLSFÖRTECKNING

1. INLEDNING

1.1 Bakgrund

Samhällets beroende av tjänster baserade på lösningar, utrustningar och system för Internet of Things (IoT) ökar i en allt snabbare takt. IoT finns i många delar av samhället: i hemmet, i offentlig verksamhet och inom industrin. Beroendet till IoT gör att hanteringen av utrustningar och system för IoT, och den infrastruktur som de kopplas upp till, måste vara robust och säker. Detta gäller även tillverkningen av utrustning samt leveranskedjan till slutanvändaren.

Det finns ett behov av en vägledning som kan stödja aktörerna i att höja säkerhetsnivån i IoT. Minimikraven i denna vägledning är menade som stöd att få en grundläggande nivå gällande IoT-säkerhet. För att veta om dessa grundläggande krav är tillräckliga behöver dock varje aktör genomföra riskbedömning och analyser för att beakta rättsliga krav och verksamhetsbehov för att få underlag om vilka ytterligare säkerhetsåtgärder som behöver införas.

Dokumentet har utarbetats av Svenska Stadsnätsföreningen i samarbete med nedanstående organisationer:

- Digital Nordix AB
- EkoT Konsult
- IoT Open
- Knowit
- RAD Data Communications
- Rejlers Sverige AB
- STF Ingenjörsutbildning AB
- Umeå Energi AB
- Utsikt Bredband AB
- Vinnergi AB

Vi tackar MSB för värdefulla synpunkter kring vägledningen om cybersäker, formalia, nomenklatur och processarbete.

1.2 Robust & Säker IoT

Begreppet Robust & Säker IoT i denna vägledning innebär att IoT-enheterna och den infrastruktur som de kopplas till ska ha genomgått en analys av minimikraven för IoT-säkerhet samt en riskbedömning för att erhålla en för tillämpningen anpassad tillgänglighet och säkerhetsnivå.

1.3 Syfte

Vägledningen innehåller minimikrav avseende åtgärder för robusthet och säkerhet för IoT. Enskilda systemägare tillämpar vägledningen efter egna instruktioner, processer och byggbeskrivningar och kan ha krav som är högre eller krav som inte framgår här.

Syftet med vägledningen är att:

- Definiera branschgemensamma begrepp och uttryck.
- Beskriva hur ENISA (European Union Agency for Cybersecurity) definierar säkerhetsområden, säkerhetskategorier och IoT hot för IoT- lösningar.
- Beskriva minimikrav avseende säkerhetsåtgärder för IoT-lösningar.
- Beskriva en metod samt tillhandahålla verktyg för analys av minimikrav avseende säkerhetsåtgärder för IoT.
- Beskriva en metod samt tillhandahålla verktyg för riskhantering.
- Utgöra underlag för utbildning, kompetensutveckling och fortbildning.

- *Utgöra underlag för en eventuellt framtida certifiering eller motsvarande av systemleverantörer som tillhandahåller IoT.*
- Utgöra tekniskt stöd vid upphandling.

1.4 Målgrupp

Vägledningen riktar sig till aktörer som i olika roller utvecklar, levererar, tillhandahåller, underhåller och driftar utrustningar, tjänster och system för IoT-tillämpningar. Vägledningen riktar sig också till aktörer som bedriver utbildning inom IoT området samt till aktörer som svarar för upphandling och kravställning på tjänster och utrustning.

1.5 Om vägledningen / Standarder

Vägledningen utgår från standarder och regelverk inom de olika delområden som berörs i vägledningen till exempel:

- ENISA Good practices for IoT and Smart Infrastructures.
- ENISA Baseline Security Recommendations for IoT.
- MSB 245, 2011 MBS:s vägledning för risk- och sårbarhetsanalyser.
- MSB 2017–1554 NCS3 Studie – IoT-relaterade risker och strategier.
- ISO/IEC 30141 Internet of Things Reference architecture.
- ISO/IEC 15408–1:2009 Generella säkerhetsmodeller.
- ISO/IEC TR 15446:2017 Vägledning för produktion av skyddsprofiler och säkerhetsmål.
- ISO/IEC 31010:2019 Risk management - Risk assessment techniques.

1.6 Identifierade brister och utmaningar inom IoT enligt ENISA

För att belysa de utmaningar som IoT-branschen har att hantera redovisas de brister och risker som framkommit när ENISA har genomfört en GAP-analys av ekosystem för IoT (Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures[1]). Analysen omfattar sex områden och en koncentrerad beskrivning av problemen inom respektive område redovisas nedan.

1: Fragmentering i befintliga säkerhetsmetoder och regler.

För närvarande finns det ingen gemensam EU-omfattande strategi för IoT-säkerhet. Inte heller intressenterna inom ekosystemet för IoT har någon gemensam modell för IoT-säkerhet. Majoriteten av experterna på området anser att avsaknaden av etablerade säkerhetsramar och den omfattande mängd överväganden man måste ta ställning till är ett hinder för utvecklingen av IoT-säkerhet. Av dessa anledningar tillämpar aktörerna inom området egna modeller när de implementerar IoT-säkerhet vilket ytterligare bromsar utvecklingen mot etablerade standarder på området.

2: Brist på medvetenhet och kunskap.

Det finns en kunskapsbrist när det gäller utvecklingen och tillämpningen mot uppkopplade, och av varandra beroende, enheter och system. Dessa brister kan bero på att det finns brister när det gäller grundläggande terminologi (taxonomi) och en objektiv bedömning av behovet av säkerhet. Då även de som anskaffar utrustningen i många fall har en bristande kunskap om IT-säkerhet innebär det ofta att förbättringar genom aktiv kravställning och uppgraderingar inte införs i den takt som behövs.

3: Osäker design och / eller utveckling

Studier som genomförts av ENISA pekar på följande brister avseende design och utveckling av IoT-komponenter och system:

- Vid design tas ingen hänsyn till säkerhetsrelaterade faktorer.
- Ingen hänsyn tas till ”säkerhet genom design” eller ”integritet genom design”, vare sig i den egna utrustningen eller lösningen eller hos tredjepartsaktörer.
- Dåligt skydd för kommunikation, både intern och extern sådan.
- Brist på stark autentisering och dålig behörighetshantering.
- Ingen validering eller signering vid uppdatering av firmware.
- Programuppdateringar utan serververifiering och verifiering av filförtroende.
- Brist på härdning, det vill säga att oönskad eller osäker funktionalitet är inaktiverad samt att standardinställningar och standardlösenord ändras.

4: Bristande interoperabilitet mellan olika IoT-enheter, plattformar och ramverk

Många IoT-enheter och lösningar med IoT kopplas ihop med system som kan anses vara kritisk informationsinfrastruktur1. Som tidigare nämnts har de flesta företag och tillverkare, på grund av bristen på en gemensam utgångspunkt, till exempel i form av reglering, sitt eget arbetssätt när de utformar IoT-enheter. Detta orsakar interoperabilitetsproblem mellan utrustning från olika tillverkare. Det orsakar också uppkomsten av flera olika säkerhetsmodeller, oförenliga koncept och taxonomier osv.

5: Brist på ekonomiska incitament

Många av IoT-tillverkarna och leverantörerna anser vanligtvis att funktionalitet och användbarhet är mycket viktigare än att implementera säker design och programmering. Det ekonomiska intresset finns inte för högre säkerhet då det är en uppfattning att det inte finns någon direkt avkastning på investeringar för högre säkerhet. Detta beror i sin tur på svårigheten att bedöma den ekonomiska effekten av hypotetiska säkerhetsbrister jämfört med alternativkostnaden att hantera sårbarheterna.

6: Brist på korrekt produktlivscykelhantering

I allmänhet saknas säkerhetsåtgärder från enheternas konstruktionsfas till deras efterföljande utveckling. Det finns ett behov av en korrekt produktlivscykelhantering för de olika enheterna i en föränderlig miljö, där enheterna och nätverken är sammankopplade och i de flesta fall anslutna till Internet, där de utsätts för många och olika hot. IoT-system består av en mängd olika enheter och om dessa lämnas utan säkerhetsuppdateringar görs hela systemet sårbart. IoT utökar den globala exponeringen och det är allas ansvar att hantera riskerna. De olika enheterna och produkterna måste utvecklas på ett säkert sätt för att konsekvent, och genom hela deras livslängd, tillhandahålla den lösning som de skapades för.

Denna vägledning hanterar i varierande omfattning samtliga områden ovan utom 5: *Brist på ekonomiska incitament.*

[1] Critical information infrastructure: ICT systems that are Critical Infrastructures for themselves or that are essential for the operation of Critical Infrastructures (telecommunications, computers/software, Internet, satellites, etc.); ENISA https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii

2. DEFINITIONER, FÖRTYDLIGANDEN OCH FÖRKORTNINGAR

2.1 IoT-system en översikt

ENISA definierar IoT som ett system av sammankopplade sensorer och ställdon vilket möjliggör intelligent beslutsfattande.

Schematisk bild över komponenterna/tillgångarna (assets groups) i ett IoT-system.

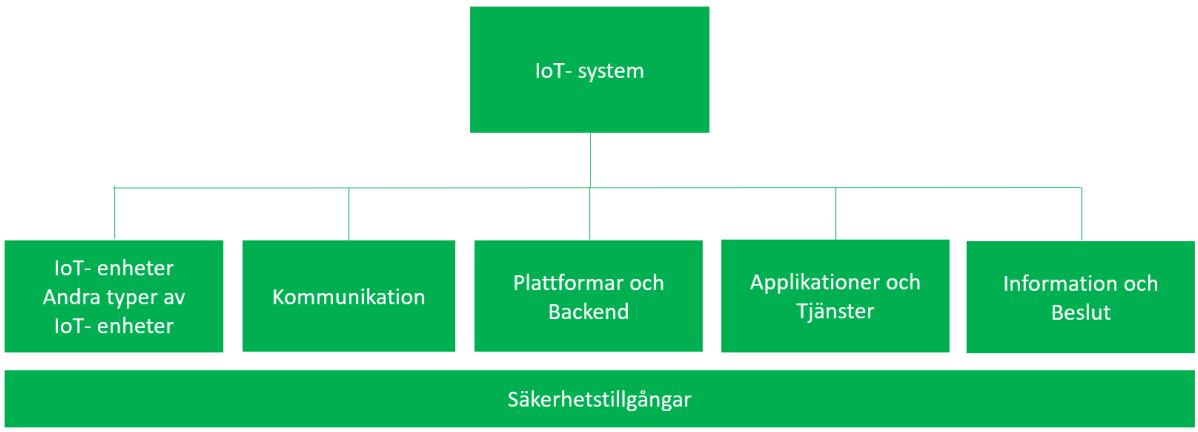

Bild Schematisk bild över komponenter i ett IoT- system

IoT-enhet

Enhet som interagerar med fysiska enheter och andra digitala enheter i ett IoT-system genom att avkänna och aktivera funktioner i dessa. Observera att en IoT-enheten är en fysisk enhet såväl som en digital enhet - detta är viktigt då vissa av de fysiska egenskaperna hos IoT-enheten spelar en roll vid användningen inom ett IoT-system, såsom dess läge, eller dess rörelse och acceleration. En IoT-enhet använder ett eller flera nätverk för att kommunicera med andra enheter. En IoT-enhet har en nätverksanslutning och exponerar en eller flera slutpunkter och kan innehålla beräkningskapacitet samt kan ibland användas för lokal lagring, IoT-enheter utgörs av:

- Sensor
  IoT-enhet som detekterar och/eller mäter händelser i en fysisk enhet och som sedan omsätter resultatet till digitalt data som representerar mätningen och som kan överföras över ett nätverk. Sensorns digitala utgång för mätning kan skilja sig mycket från den ursprungliga fysiska mätningens miljö och kan orsaka en betydande tidsfördröjning beroende på bearbetningen av data inom enheten. Ett exempel kan vara identifiering av en persons identitet från en övervakningskamera. **En sensor är en specialisering av en IoT-enhet**.

- Ställdon (eng. Actuator)
  IoT- enhet som har möjlighet att göra förändringar i den fysiska miljön. Ställdonet styr en fysisk händelse, till exempel varvtalet på en pump.

- Strömförsörjning (Infrastruktur)
  Strömförsörjer en IoT- enhet och dess interna komponenter. Spänningskällan kan vara extern och kabelansluten eller utgöras av ett batteri integrerad i IoT-enheten.

Andra typer av IoT-enheter

- *Enheter med gränssnitt mot andra IoT-enheter.*
  Enheter vars syfte är att fungera som gränssnitt eller aggregator mot andra IoT-enheter i ett specifikt IoT-system.
  Enheter använda av användare som gränssnitt för att interagera med IoT-enheter.

- *Enheter för hantering av andra IoT-enheter*
  Enheter speciellt utformade för att hantera andra IoT-enheter, kommunikationsnät etc.

- *Inbäddade system*
  Enheter som har möjlighet att själva behandla data. De inkluderar inbäddade sensorer och/eller ställdon, nätfunktioner för anslutning direkt till Molntjänster, minnesfunktioner och möjlighet att hantera programvara.

Kommunikation

- *Passiv Infrastruktur*
  Ledningsnät: fiber-, koppar- och koaxialkablar.

- *Aktiv Infrastruktur (Kommunikationsnät)*
  Kommunikationsnät som medger att olika noder i ett IoT-system kan utbyta data och information över en datalänk. Det finns olika typer av kommunikationsnät beroende på tillämpningsområde vilket bland annat inkluderar (W)LANs, (W)PANs, PAN:s och (W)WANs.
  - Routers
    Nätkomponenter som skickar datapaket mellan olika kommunikationsnät i IoT Ekosystemet.
  - Gateways
    Noder som används som gränssnitt mot andra kommunikationsnät i IoT miljön som använder andra typer av protokoll. Gateways kan innehålla protokolltransformering, funktioner för isolering av fel etc. för att stödja system-interoperabilitet.

- *Protokoll*
  Definierar regler för hur kommunikation mellan IoT-enheter ska utföras över en specifik kommunikationskanal. Det finns många olika protokoll för trådlös alternativt trådbunden kommunikation. Exempel på kommunikationsprotokoll för IoT är ZigBee, MQTT, CoAP, BLE, etc.

Plattform och backend

Plattform(ar), IoT-middleware placerat i ”molnet” eller i eget datacenter

- Hantering/management av Enheter och Kommunikationsnät
  Hanteringen/management av IoT-systemets enheter och kommunikationsnät inkluderar uppdatering av mjukvara för OS, firmware och applikationer. Det omfattar också spårning och monitorering av enheter och kommunikationsnät, insamling och lagring av loggar som i ett senare skede kan användas för diagnostik.

- Enhetsanvändning
  Övergripande uppföljning av IoT- systemets enheter och kommunikationsnät för att förstå aktuellt status, användarmönster, prestanda etcetera

Backend

- Web-baserade tjänster
  Detta är tjänster inom World Wide Web, vilka stödjer ett web-baserat gränssnitt för web-användare eller för web-anslutna applikationer. Detta innebär att web-teknologi kan användas inom IoT för Människa till Maskin-kommunikation (H2M) och för Maskin till Maskin-kommunikation (M2M).

- Moln-infrastruktur och tjänster
  Inom IoT, kan moln-backend användas för att aggregera och processa data från spridda enheter och för att stödja beräkningskapacitet, lagring, applikationer, tjänster etcetera.

Applikationer och tjänster

- Program för användartillämpningar.
- Leverans-API (Application Programming Interface).
- Dataanalys och visualisering.
  Efter att data har samlats in och processats kan den framtagna informationen analyseras och visualiseras för att identifiera nya mönster (eng. pattern), effektivisering av drift etc.

Säkerhetstillgångar

- Denna grupp omfattar tillgångar som är specifikt fokuserade på säkerheten för IoT-enheter, kommunikationsnät och information. Tillgångarna inkluderar främst Brandväggar, Brandväggar för Web Applikationer (WAF), programvara för skydd av cloud access (cloud access security broker/CASB*), system för intrångsskydd (Intrusion Prevention System/IPS**) och system för hantering av autentisering/rättigheter.

  * **CASB** (cloud access security broker) är en lokal eller molnbaserad programvara, mellan användare av moln-tjänster och moln-applikationer, som monitorerar alla aktiviteter och säkerställer säkerhetspolicys. En CASB kan tillhandahålla flera olika tjänster, inklusive men inte begränsat till monitorering av användaraktiviteter, varning till administratörer om potentiellt farliga åtgärder, säkerställer efterlevnaden av säkerhetspolicyn, och skyddar automatiskt mot skadlig programvara.

  * **IPS** (Intrusion Prevention System) är en datasäkerhetsanordning som övervakar nätverk och/eller systemaktiviteter för att upptäcka skadligt beteende och som kan reagera och blockera dessa aktiviteter i realtid. Ett nätverksbaserat IPS (NIPS) söker efter skadlig kod eller attacker. När en attack upptäcks kan NIPS:en kasta bort dess paket medan andra paket får passera som vanligt.

Information

- I vila
  Information lagrad i databaser i moln-backend eller i enheterna själva.
- Under överföring
  Information skickad eller förmedlad genom kommunikationsnätet mellan IoT-komponenter.
- Under användning
  Information använd av en application, tjänst eller i en IoT-komponent generellt.

Beslutshantering av data

- Mining
  Detta refererar till algoritmer och tjänster för att processa insamlat data och transformera denna till en definierad struktur för framtida användning genom big data teknologier för att upptäcka mönster i mycket stora datamängder.

- **Databehandling**
  Tjänster som underlättar behandlingen av insamlat data i avsikt att få fram användbar information som kan användas för att implementera regler och logik för beslutsfattande och för automatiseringsprocesser. AI kan användas för att lära av användningen av information över tid.

2.2 Definitioner och förtydliganden

Attributbaserad åtkomstkontroll Attribute-based access control (ABAC)
I denna metod bestäms tillgången till en resurs av en samling av flera attribut. Den betraktar användarattribut (subjektattribut), resursattribut (objektattribut) och miljöattribut. Attribut är egenskaperna hos användare, resurser och miljö.

Beslut-trigger (Beslutsutlösare)
En beslut-trigger är ett villkorat uttryck som utlöser en åtgärd. En beslut-triggers utgång(ar) kan kontrollera ställdon och transaktioner.

Buggjägarprogram (eng. Bug bounty)
Ett koncept för en överenskommelse som erbjuds av många webbplatser och programutvecklare där individer kan få erkännande och kompensation för rapportering av sårbarheter eller fel.

Chain of trust
Metod för att validera varje komponent av hårdvara och programvara från ändenheten upp till rotcertifikatet. Det är avsett att se till att endast pålitlig programvara och hårdvara kan användas samtidigt som flexibiliteten bibehålls.

Chain of trust boot- loader
Metod för att säkerställa att exekverad kod kommer från en pålitlig källa. Det skapar en fullständig kedja av förtroende, från en hårdvaruskyddad rot av förtroende till bootloader, till bootpartitionen och andra verifierade partitioner inklusive system, leverantör och eventuella oem-partitioner. Under uppstart av enheten verifierar varje steg integriteten och äktheten i nästa steg innan överlämnandet för drift.

Cross-Site Request Forgery (CSRF),
Cross-Site Request Forgery (CSRF) är en attack som tvingar en slutanvändare att utföra oönskade åtgärder på en webbapplikation där de för närvarande är autentiserade.

Cross-Site Scripting (XSS),
Cross-Site Scripting (XSS) attacker är en typ av injektion, där skadliga skript injiceras på annars godartade och pålitliga webbplatser.

Cybersäkerhet
Sammanfattar metoder och åtgärder för att tekniskt skydda Informations-och kommunikationssystem.

End-of-life (EoL)
Termen indikerar att produkten är i slutet av dess livslängd (från leverantörens synvinkel) och att en leverantör slutar marknadsföra, sälja eller uppdatera produkten, samt slutar att tillhandahålla reservdelar och reparationer.

End-of-support (EoS)
Termen hänvisar till en situation där ett företag upphör med stöd för en produkt eller tjänst. Detta tillämpas vanligtvis på hårdvaru- och mjukvaruprodukter när ett företag släpper en ny version och slutar stödet för tidigare versioner.

Förvaltning av informationstillgångar (eng. Asset Management)
Ett sammanhållet och strukturerat arbetssätt för förvaltning av IoT-tillgångar under hela deras livscykel.

Hashfunktion
En funktion som gör om någon sorts data till ett relativt litet heltal som kallas hashsumma, hashvärde eller kondensat. Används på samma sätt som en kontrollsumma, dvs. genom att jämföra hashsumman som anges med den hashsumma som själv räknas fram går det att avgöra om det skett någon förändring i det data som kontrolleras.

Informationssäkerhet

Ett bra informationssäkerhetsarbete är en förutsättning för effektiv och korrekt informationshantering. Därför måste informationen skyddas enligt tre perspektiv:

- tillgänglighet - att den alltid finns när vi behöver den
- riktighet - att vi kan lita på att den är korrekt och inte manipulerad eller förstörd
- konfidentialitet - att endast behöriga personer får ta del av den

Arbetet med informationssäkerhet omfattar att införa och förvalta administrativa säkerhetsåtgärder så som policys och riktlinjer, tekniska säkerhetsåtgärder såsom brandväggar, autentiseringslösningar och kryptering samt fysiska säkerhetsåtgärder i form av skal- och brandskydd.

Lightweight encryption
Ett undersegment som är avsett för olika resurskontrollerade enheter. Kärnan i lättviktiga krypteringssystem är att använda mindre minne, mindre datorresurser och mindre kraft eller energi för att tillhandahålla säkerhetslösning för resursbegränsade enheter.

Molntjänster
IT-tjänster som tillhandahålls över Internet, i synnerhet funktioner som traditionellt sköts på egna datorer men genom tjänsten sköts av någon annan. Det kan till exempel handla om tillämpningsprogram, serverprogram och lagring av data.

Multifaktorautentisering (MFA)
En metod för åtkomstkontroll där användare endast beviljas åtkomst efter att framgångsrikt ha presenterat flera separata bevis för en autentiseringsmekanism – vanligtvis inom minst två av följande tre kategorier: kunskap (något de vet), innehav (något de har) och inneboende (något de är).

Packet-Sniffing
En metod för att samla och logga några eller alla paket som passerar genom ett datornätverk, oavsett hur paketet adresseras. På detta sätt kan varje paket, eller en definierad delmängd paket, samlas för ytterligare analys.

Principen om minsta behörighet [principle of least privilege (POLP)]
Principen om minsta privilegium (POLP) är ett viktigt begrepp inom datorsäkerhet och innebär att man begränsar åtkomsträttigheter för användare till de bara minsta behörigheter som de behöver för att utföra sitt arbete.

Priviligierad kod
Tillfälligt tillgång till kod som man normalt inte skulle ha rätt att köra.

Reverse engineering
Också känt som demontering, är tekniken att ifrån en färdig produkt ta fram detaljerade ritningar och specifikationer på hur produkter fungerar. Ordet syftar alltså på att arbetssättet är omvänt jämfört med hur en ingenjör vanligen arbetar. När det handlar om datorprogram används ofta uttrycket dekompilering.

Rollbaserad åtkomstkontroll (role-based access control (RBAC)
I denna metod bestäms tillgången till en resurs av användarens roll. Administratörer i organisationen tilldelar roller till användarna. Det innebär att en uppsättning användare kan ha tillgång till att läsa filer, medan en annan uppsättning användare kan ha tillgång till skrivfiler etcetera ska implementeras.

Root of Trust
En enhets Root of Trust är den punkt där autentiseringen startar och som sedan sträcker sig genom varje lager. För mer kritiska IoT-applikationer är en hårdvarubaserad Root of Trust en viktig byggsten för att säkra IoT-slutpunkter och tjänster.

Salt
Ett slumpmässigt tillägg till ett lösenord som gör det svårare för en lösenordstjuv att lista ut det riktiga lösenordet.

Snooping
Snooping, i säkerhetssammanhang, innebär obehörig åtkomst till en annan persons eller företags data. Metoden liknar avlyssning men är inte nödvändigtvis begränsad till att få tillgång till data under överföringen.

SQL Injection and HTML Injection
SQL Injection används inte bara för att dumpa en databas eller för att logga in utan giltiga användaruppgifter. Många webbapplikationer, som Wordpress, lagrar webbplatsinnehållet i en databas. Om en angripare får skrivåtkomst till databasen kan han sätta in skadlig kod som sedan kommer att ges för alla användare.

Säkerhetsskydd och sekretess
Hanteringen av säkerhetsskydd och sekretess regleras genom nedanstående lagar och förordningar.

- ***Säkerhetsskydd***
  Säkerhetsskyddslagen (2018:585) gäller för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (Säkerhetsskyddslagen kompletteras med Säkerhetsskyddsförordning 2018:658).
  Med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet* mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter. Den som bedriver säkerhetskänslig verksamhet ska utreda behovet av säkerhetsskydd (säkerhetsskyddsanalys avseende Informationssäkerhet, Fysisk säkerhet, Personsäkerhet). Säkerhetsskyddsanalysen ska dokumenteras.
  Med säkerhetsskyddsklassificerade uppgifter avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig.
  Säkerhetsskyddsklassificerade uppgifter ska delas in i säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet. Indelningen i säkerhetsskyddsklasser ska göras enligt följande:

  1. kvalificerat hemlig vid en synnerligen allvarlig skada,
  2. hemlig vid en allvarlig skada,
  3. konfidentiell vid en inte obetydlig skada, eller
  4. begränsat hemlig vid endast ringa skada.

Säkerhetsskyddsavtal. Statliga myndigheter, kommuner och regioner som avser att genomföra en upphandling och ingå ett avtal om varor, tjänster eller byggentreprenader ska se till att det i ett säkerhetsskyddsavtal anges hur kraven på säkerhetsskydd ska tillgodoses av leverantören.

* Säkerhetskänslig verksamhet är verksamhet som är av betydelse för Sveriges säkerhet eller som Sverige har förbundit sig att skydda genom internationella åtaganden. Det kan till exempel handla om verksamheter inom totalförsvaret, rättsväsendet, energi- eller vattenförsörjningen, telekommunikationer eller transportsektorn.

- ***Sekretess***
  Offentlighets- och Sekretesslag (2009:400) (OSL) berör myndigheter och personer vars yrkesutövning är i det allmännas tjänst eller det som annars kan kallas offentlig sektor. OSL reglerar sekretess både genom att de anställda beläggs med tystnadsplikt gällande interna förhållanden men även begränsning i utgivande av handlingar. OSL gäller även för juridiska personer så som aktiebolag och handelsbolag där kommun eller landsting har ett stort inflytande. Dessa juridiska personer är att jämställa med en myndighet. Därmed regleras tystnadsplikt, sekretess samt brott mot detta för anställda inom offentlig sektor i första hand genom lag.

  Gällande privat sektor är det istället enskilda lagar exempelvis lag (1990:409) om skydd för företagshemligheter (FHL), rättsprinciper och klausuler i anställningsavtal som tillsammans spelar en avgörande roll.

Åtkomstkontroll
Se:
- Attributbaserad åtkomstkontroll
- Rollbaserad åtkomstkontroll

Tvåfaktorautentisering (även känd som 2FA)
Ett sätt att bekräfta användarens begärda identitet genom att använda en kombination av två olika komponenter. Tvåfaktorsautentisering är en typ av multifaktorautentisering.

2.3 Förkortningar

5Vs	volume, velocity, veracity, variability, and variety
ABAC	Attribute-based access control (ABAC), Policy-based access control
API	Application programming interface
ASD	Application & Service Domain
BSS	business support systems
CM	Conceptual Model
EOL	End-of-Life
FQDN	fully qualified domain name
HMI	human machine interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	heating, ventilation and air conditioning
IaaS	infrastructure as a service
ICT	information and communication technologies
IoT	Internet of Things
IoT RA	Internet of Things Reference Architecture
LAN	local area network
LOB	line of business
MQTT	Message Queuing Telemetry Transport
OMD	Operation & Management Domain

OSS	operational support systems
OTA	Over-the air, uppdatering av firmware
PaaS	platform as a service
PED	Physical Entity Domain
PII	personally identifiable information
POLP	Principle of Least Privilege
QoS	quality of service
RA	Reference Architecture
RAID	Resource Access & Interchange Domain
RBAC	Role based access control
RFID	radio-frequency identification
RM	Reference Model
SaaS	software as a service
SCD	Sensing & Controlling Domain
UML	Universal Modelling Language
UD	User Domain
URI	uniform resource identifier
UUID	universally unique identifier(a 128-bit number used to identify information in computer systems)

3. IOT REFERENSMODELL OCH ROLLER

Vägledningen baseras på nedanstående generiska referensmodell för ett IoT-system.

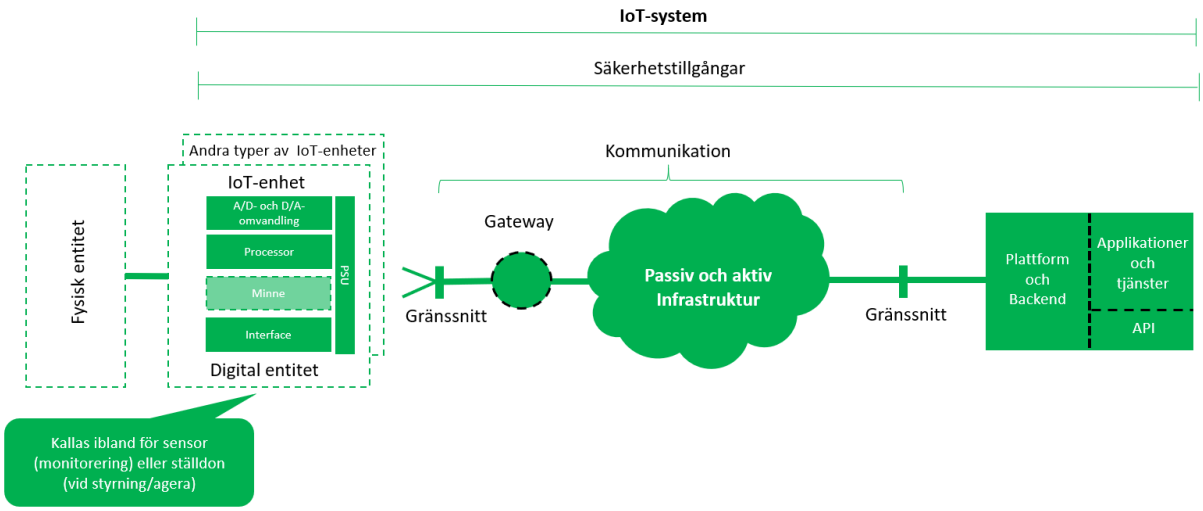

Bild Generisk Referensmodell för ett IoT-system.

Inom ramen för referensmodellen positionerar sig aktörerna inom IoT marknaden i olika roller som, till exempel, utvecklare, tillverkare, leverantör av produkter och tjänster, integratör o.s.v.

Nedan redovisas IoT-systemets komponenter samt de aktörsroller som omfattas av denna vägledning. Komponenterna beskrivs under kapitel *Definitioner, Förtydliganden och Förkortningar*.

3.1 IoT-systemet

- Omfattar grundläggande komponenter enligt avsnitt 3.2–3.7.

Roller för hantering av IoT-system

- *Utvecklar (till exempel design, arkitektur, integration, konfiguration)*
- *Levererar IoT-system*
- *Systemägare. Har det övergripande ansvaret för tillhandahållandet av IoT-system avseende administration, förvaltning, säkerhet och drift.*

3.2 IoT-enheter

- *Sensorer (datainhämtning)*
- *Ställdon (styrning)*
- *Strömförsörjning*

Roller för hantering av IoT-enheter

- *Utvecklar och tillverkar IoT-enheter*
- *Levererar IoT enheter*

3.3 Andra typer av IoT-enheter

- *Enheter med gränssnitt mot andra IoT-enheter*
- *Enheter för hantering av andra IoT-enheter*
- *Inbäddade system*

Roller för hantering av Andra typer av IoT-enheter

- *Utvecklar och tillverkar Andra typer av IoT-enheter*
- *Levererar Andra typer av IoT enheter*

3.4 Kommunikation

- *Passiv infrastruktur*
- *Aktiv infrastruktur*
- *Protokoll*

Roller för hantering av Kommunikation

- *Utvecklar kommunikationsnät och tjänster*
- *Levererar kommunikationsnät och tjänster*
- *Tillhandahåller, underhåller och driftar kommunikationsnät och tjänster*

3.5 Plattform och backend

- *Web-baserade gränssnitt*
- *Moln-Infrastruktur och tjänster*
- *Hantering av enheter och kommunikationsnät.*

Roller för hantering av Plattformar och backend

- *Utvecklar och ”tillverkar” funktionsplattformar med backendfunktioner*
- *Levererar plattformar med backendfunktioner*
- *Tillhandahåller, underhåller och driftar funktionsplattformar med backendfunktioner*

3.6 Applikationer och tjänster

- *Program för användartillämpningar*
- *Leverans-API*
- *Dataanalys och visualisering*

Roller för hantering av Applikationer och tjänster

- *Utvecklar och ”tillverkar” IoT-applikationer och IoT- tjänster*
- *Levererar IoT-applikationer och IoT- tjänster*
- *Tillhandahåller, underhåller och driftar IoT-applikationer och IoT- tjänster*

3.7 Säkerhetstillgångar

- *Brandväggar*
- *Säkerhetsprogram*

Roller för hantering av Säkerhetstillgångar

- *Utvecklar och tillverkar säkerhetstillgångar*
- *Levererar säkerhetstillgångar*

4. METOD FÖR KRAVANALYS OCH RISKHANTERING

Den övergripande metoden för kravanalys och riskhantering avseende IoT-tillämpningar redovisas nedan:

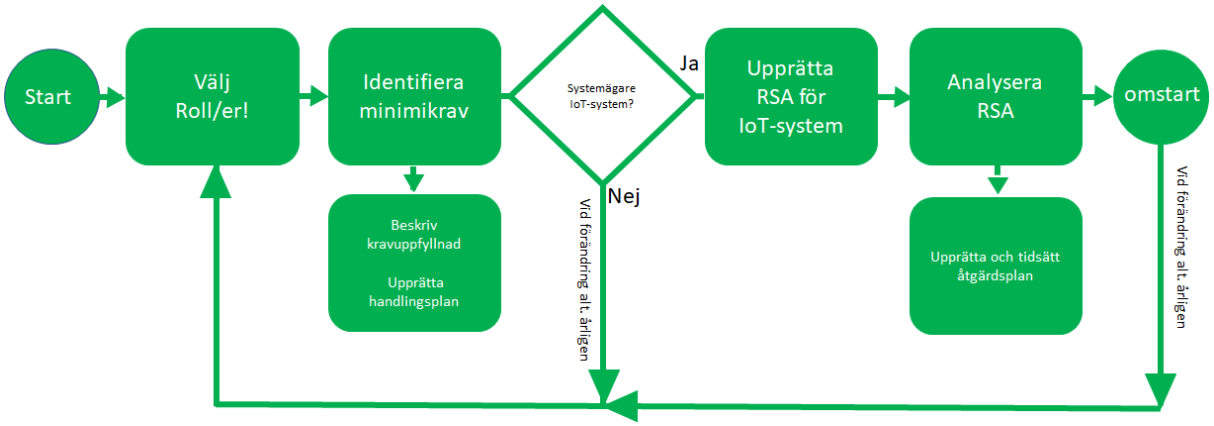

Bild Metod för kravanalys och riskhantering

Övergripande beskrivning av metoden steg för steg:

1. Aktören definierar vilken typ av IoT – Roll/er som är tillämplig samt genomför en ändamålsbaserad bedömning av den säkerhet och integritet som speglar olika säkerhetsnivåer kopplat till systemets/enhetens tillämpning (till exempel blåljus/kris, hemautomatisering).

2. Minimikraven för den valda rollen analyseras i enlighet med *Bilaga 1. Rutin och handledning, Kravanalys Robust & Säker IoT.*

3. Aktören upprättar en beskrivning över lösningarna för uppfyllda krav samt upprättar och tidsätter en handlingsplan för att åtgärda avvikelser mellan befintligt läge och minimikraven.

4. Är den valda rollen Systemägare genomförs en riskanalys och riskbedömning i enlighet med Bilaga 2. *Rutin och handledning, RSA Robust & Säker IoT*. **Observera att verksamhetens art, t. ex hantering av samhällskritiska funktioner, kan ställa högre krav på säkerhet än de som är angivna som minimikrav i *Bilaga 1.1 Verktyg Kravanalys Robust & Säker IoT***

5. Aktören ska minst en gång per år analysera risken för att förändrade säkerhetshot kan påverka säkerheten i IoT- systemet och därmed behovet av en förnyad kravanalys.

6. Inför planerade verksamhets- och/eller tekniska förändringar ska aktören göra en översyn och bedömning av om förändringarna påverkar säkerheten i IoT- systemet och därmed behovet av en förnyad kravanalys.

Anm. En Aktör som har rollen att tillhandahålla allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster ska även vidta åtgärder enligt **5 kap. 6 b § lagen (2003:389)** om elektronisk kommunikation.

5. SÄKERHETSOMRÅDEN OCH KATEGORISERING

För att kunna hantera hot, sårbarheter och riskanalys så arbetar man med säkerhetsområden och kategorisering. Till dessa kopplas sedan fundamentala och kompletterande säkerhetsåtgärder baserade på kravanalyser och riskbedömningar. De säkerhetsområden och kategorier som används i denna vägledning är de av ENISA utarbetade områden.

5.1 Säkerhetsområden

Säkerhetsområdena enligt ENISA, *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures,* utgörs av:

1. **Styrning av säkerheten i informationssystem och riskhantering (Information System Security Governance & Risk Management)**
   Innehåller säkerhetsåtgärder avseende riskanalys, policy, ackreditering, indikatorer och revision samt säkerhetsresurser för informationssystem.

2. **Systemhantering (Ecosystem Management)**
   Innehåller säkerhetsåtgärder avseende kartläggning av ekosystem och ekosystemrelationer.

3. **IT-säkerhetsarkitektur (IT Security Architecture)**
   Innehåller säkerhetsåtgärder avseende systemkonfiguration, förvaltning av tillgångar, systemseparering, trafikfiltrering och kryptografi.

4. **Administration av IT-säkerhet (IT Security Administration)**
   Innehåller säkerhetsåtgärder avseende administrationskonton och administrationsinformationssystem.

5. **Identitets-och åtkomsthantering (Identity and access management)**
   Innehåller säkerhetsåtgärder avseende autentisering, identifiering och åtkomsträttigheter.

6. **Underhåll av IT-säkerhet (IT security maintenance)**
   Innehåller säkerhetsåtgärder avseende underhållsrutiner för IT-säkerhet och fjärråtkomst.

7. **Fysisk- och miljömässig säkerhet (Physical and environmental security)**
   Innehåller fysisk säkerhet och miljöfaktorers påverkan på driftsäkerhet.

8. **Loggning (Detection)**
   Innehåller säkerhetsåtgärder avseende detektering, loggning och loggkorrelation och analys.

9. **Hantering av datasäkerhetsincidenter (Computer security incident management**)
   Innehåller säkerhetsåtgärder avseende analys och hantering av informationssystemets säkerhetsincidenter samt incidentrapport.

10. **Driftsäkerhet (Continuity of Operations**)
    Innehåller säkerhetsåtgärder för hantering av kontinuitet och katastrof.

11. **Krishantering (Crisis Management)**
    Innehåller säkerhetsåtgärder avseende krishanteringsorganisation och process.

5.2 Kategorier

Säkerhetkategorier enligt ENISA, *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures,* utgörs av:

- Säkerhetspolicys (PS)
- Organisation, personal och processmätvärden (OP)
- Tekniska åtgärder (TM)

Policys

Avser policys som riktar sig mot informationssäkerhet och syftar till att göra den mer konkret och robust. Policys ska vara tillräckliga för organisationens verksamhet och ska innehålla väl dokumenterad information. I det här sammanhanget har good practice används som utgångspunkt.
När säkerhets- och integritetsskydd hänför sig till design bör säkerhetsåtgärderna återspegla de särdrag och det sammanhang där IoT-enheten, eller systemet, kommer att användas. Därför kan säkerhet genom design hänvisa till olika specifikationer när en IoT-enhet används i hemmiljö, jämfört med en IoT-enhet i en kritisk infrastruktur.

Säkerhetspolicy

En säkerhetspolicy är ett skriftligt dokument i en organisation som beskriver hur man ska skydda organisationen mot hot, inklusive datasäkerhetshot och hur man hanterar situationer när de inträffar. En säkerhetspolicy måste identifiera alla företagets tillgångar såväl som alla potentiella hot mot dessa tillgångar

IT (IoT)-säkerhetspolicy

En IT-säkerhetspolicy identifierar regler och procedurer för alla individer som får tillgång till och använder en organisations IT (IoT)-tillgångar och resurser. Målen för en IT(IoT)-säkerhetspolicy är att bevara konfidentialitet, integritet och tillgänglighet av system och information som används av en organisations medlemmar

Organisation, personal och processmätvärden

Alla organisationer ska ha organisatoriska kriterier för hantering av informationssäkerhet.
Personalpraxis ska främja god säkerhet, säkerställa hanteringen av processer och en säker hantering av information i organisationen.
Organisationer bör se till att entreprenörer och leverantörer är ansvariga för givna funktioner.
I händelse av en incident i organisationens säkerhet ska organisationen vara förberedd med tydliga roller för ansvar, utvärdering och åtgärder.

Tekniska åtgärder

För att minska sårbarheten i ett IoT-system ska säkerhetsåtgärder och god praxis implementeras och omfatta systemets tekniska element.
Tekniska mätvärden ska ge nödvändiga indata för de tekniska åtgärder som krävs för att bevara och skydda informationssäkerheten.
Vid tillämpning av dessa tekniska åtgärder bör man ta hänsyn till särdragen i IoT-ekosystemet. Det innebär till exempel att vid ett stort antal involverade enheter och produkter kan vissa åtgärder behöva utföras med specialiserade arkitektoniska komponenter, till exempel gateways.

6. GENERELLA KRAV

Utöver de minimikrav som anges i tabell 1 MINIMIKRAV IoT-SYSTEM omfattar vägledningen också ett antal generella krav på den personal och de företag som är engagerade i att arbeta med planering, upphandling, projektering, leverans och drift av IoT-lösningar.

6.1 Personalens kvalifikationer

Personal med goda kunskaper om hantering av lokala förutsättningar är en viktig förutsättning vid planering och projektering av lösningar för IoT. Uppdragsgivaren (t.ex. nätägare, upphandlare, beställare) ska säkerställa att egen personal, ombud eller inhyrd personal, samt utvalda leverantörer, har tillräckliga kvalifikationer och kunskap om IoT och dess lösningar samt olika teknologiers funktion, samt kompetens att genomföra behovsanalysen och att kravställa eventuella entreprenader.

6.2 Leverantörens kvalifikationer

Leverantör av personal, kompetens eller hårdvara inom området IoT ska förutom den tekniska kompetens som krävs enligt ovan, även ha förmåga, förståelse och kunskap att ställa rimliga krav på de parametrar som beskrivs i denna vägledning. Uppdragsgivaren bör vid val av leverantören väga in flera aspekter, exempelvis förmåga att möta krav på geografisk leveransförmåga, närhet till anläggning för relevanta inställelsetider, support- och driftförmåga. Krav bör ställas på leverantörens förmåga till utbyte/reparationer enligt systemägarens och/eller upphandling, och i förhållande till på IoT- systemet ställda tillgänglighetskrav.

Man bör även överväga krav på långsiktighet, miljö och nyttjande av naturresurser vid val av material och metoder.

7. MINIMIKRAV IOT-SYSTEM

Minimikraven avseende säkerhet för ett IoT-system redovisas i tabell 1. MINIMIKRAV IoT-SYSTEM nedan. Minimikraven anges per kategori definierade i avsnitt 5.2 Kategorier. I minimikraven anges det säkerhetsområde som kravet avser. För varje krav anges den roll som är ansvarig för hanteringen av åtgärden. Varje minikrav börjar med ett index som härstammar från ENISAS beteckningar alternativ alternativt med MKx för kompletterande krav baserat på bland annat MSB förhandsutgåva av vägledning för Grundläggande it-säkerhetsåtgärder.

I tabellen används följande beteckningar för definierade IoT-roller:

R1 – Roller för IoT enheter
Utvecklar och tillverkar IoT-enheter
Levererar IoT enheter

R2 – Roller för andra typer av IoT-enheter
Utvecklar och tillverkar andra typer av IoT-enheter
Levererar andra typer av IoT enheter

R3 – Roller för funktionsplattformar och backend
1. Utvecklar och ”tillverkar” funktionsplattformar med backendfunktioner
Levererar plattformar med backendfunktioner
2.Tillhandahåller, underhåller och driftar funktionsplattformar med backendfunktioner

R4 – Roller för applikationer och tjänster
1. Utvecklar och ”tillverkar” IoT-applikationer och IoT- tjänster
Levererar IoT-applikationer och IoT- tjänster
2. Tillhandahåller, underhåller och driftar IoT-applikationer och IoT- tjänster

R5 – Roller för IoT- system
1. Utvecklar (till exempel design, arkitektur, integration, konfiguration)
Levererar IoT-system
2. Systemägare (juridiska ägare eller nyttjare av systemet och ansvarig för lagefterlevnad, exempelvis GDPR, elsäkerhet, säkerhetsklassning, frekvensanvändning etcetera)

R6 – Roller för kommunikation
1. Utvecklar kommunikationsnät och tjänster
Levererar kommunikationsnät och tjänster
2. Tillhandahåller, underhåller och driftar kommunikationsnät och tjänster

R7 – Roller för Säkerhetstillgångar
Utvecklar och tillverkar säkerhetstillgångar
Levererar säkerhetstillgångar

För tabellen gäller att om en roll har ansvar för att hantera ett minimikrav så markeras detta med rollens indexnummer (R1-R7) i aktuell rollkolumn (R1-R7), Gäller kravet endast en underroll till huvudrollen så markeras det med rollens huvudindex samt underrollens indexnummer, exempelvis R6.2.

För att hantera ett minimikrav kan det ibland krävas att andra roller har implementerat funktioner/delfunktioner för att möta kraven men detta hanteras inte i detta dokument då dessa funktioner/delfunktioner är lösningsberoende.

Minimikraven är inarbetade i en matris *Bilaga 1.1 Verktyg, Kravanalys Robust & Säker IoT* som aktuell organisation ska använda vid analys av tillämpliga krav för IoT i respektive verksamhet. Handhavande och metod för kravanalysen redovisas i *Bilaga 1. Rutin och handledning, Kravanalys Robust & Säker IoT.*

TABELL 1. MINIMIKRAV IOT SYSTEM

7.1 Säkerhetspolicy (PS)

Avser policys (se kapitel 5.2 Kategorier) som riktar sig mot informationssäkerhet och syftar till att göra den mer konkret och robust. Policys ska vara tillräckliga för organisationens verksamhet och ska innehålla väl dokumenterad information. I det här sammanhanget har good practice används som utgångspunkt.
När säkerhets- och integritetsskydd hänför sig till design bör säkerhetsåtgärderna återspegla de särdrag och det sammanhang där IoT-enheten, eller systemet, kommer att användas. Därför kan säkerhet genom design hänvisa till olika specifikationer när en IoT-enhet används i hemmiljö, jämfört med en IoT-enhet i en kritisk infrastruktur.

Roller -- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.

7.1.1 Säkerhet genom design		R1	R2	R3	R4	R5	R6	R7
Säkerhetsområde 3: *IT-säkerhetsarkitektur.*	GP-PS-05: Arkitekturen ska utformas i segment/delar som kapslar in/isolerar element i händelse av attacker.	R1	R2	R3	R4	R5	R6	R7
Säkerhetsområde 2: *Systemhantering.*	GP-PS-02: Möjligheten att integrera olika Säkerhetspolicyer (inkl. roller och ansvar) och tekniker för en konsekvent säkerhetskontroll av olika enheter och användarnät i ett IoT-system ska säkerställas.			R3.2	R4.2	R5.2	R6.2	
Säkerhetsområde 6: *Underhåll av IT-säkerhet.*	GP-PS-06: IoT hårdvarutillverkare och IoT programvaruutvecklare ska implementera testplaner för att verifiera att en produkt som installeras i ett system fungerar som förväntat. Testplanerna ska också omfatta felaktig beteende t. ex handhavandefel. *Kommentar: Penetrationstester hjälper till för att identifiera felaktig inmatningshantering, bypass försök vid autentisering och för övergripande säkerhetsstatus.*	R1	R2	R3.1			R6.1	R7
Säkerhetsområde 6: *Underhåll av IT-säkerhet.*	MK 1: Använd separata miljöer för utveckling, testning och produktion så att operativa verksamhetsprocesser och produktionsdata inte påverkas vid fel i utvecklings- och testprocessen.	R1	R2	R3.1	R4.1	R5	R6.1	R7
Säkerhetsområde 3: *IT-säkerhetsarkitektur.*	GP-PS-04: Vid utformning av lösningar för energibesparing ska säkerheten inte äventyras.	R1	R2			R5		
	GP-PS-03: Vid utformningen av säkerhetslösningar ska risken för människors säkerhet vägas in.	R1	R2	R3.1	R4.1	R5	R6.1	R7
Säkerhetsområde 2: *Systemhantering.* **Säkerhetsområde 3:** *IT-säkerhetsarkitektur.*	GP-PS-01: Säkerheten för hela IoT-systemet ska hanteras genom ett konsekvent förhållningssätt enligt kapitel *Analysprocessen* under hela livscykeln. *Kommentar: Detta görs på alla nivåer av enhet/applikationsdesign och utveckling samt omfattar också säkerhetsaspekterna under utveckling, tillverkning och implementering.*					R5		
Säkerhetsområde 6: *Underhåll av IT-säkerhet.*	GP-PS-07: IoT programvaruutvecklare ska genomföra kodgranskning under implementationen, detta bidrar till att minska buggar i en slutlig version av en produkt. *Kommentar: Underlag som visar hur kvalitét under utveckling och implementation säkerställs ska kunna redovisas.*	R1	R2	R3	R4	R5	R6	R7

Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
7.1.2 Sekretess genom design		**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 1: *Styrning av säkerheten i informationssystem och riskhantering.*	GP-PS-09: Konsekvensbedömningar baserat på nedanstående tre frågor ska utföras innan nya applikationer implementeras: 1. Var är IoT applikationernas geografiska placering (rättsliga begränsningar och kulturell miljö). 2. För vilket ändamål (omfattning). 3. För vilket scenarier (företags-/organisationskrav)			R3	R4	R5		
	GP-PS-08: Sekretess och riskhantering ska vara en vägledande princip när man utformar och utvecklar IoT-system och ska utgöra en integrerad del av systemet.					R5		R7
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
7.1.3 Förvaltning av anläggningstillgångar - Asset Management		**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 3: *IT-säkerhetsarkitektur.* .	GP-PS-10: Viktiga tillgångarna (dvs. Gateways, Endpoint-enheter, hemnätverk, roamingnät, serviceplattformar, programvara, etc.) som ingår i en IoT-tjänst ska identifieras, verifieras och förtecknas. Detta ska hanteras i ett system för förvaltning och konfigurationskontroll. *Kommentar: Verktygen för detta bör vara automatiserade och centrala.*			R3	R4	R5	R6	
	MK 2: Det ska finnas en förteckning över den hård- och mjukvarvara som är godkänd för användande i verksamheten. Förteckningen inkluderar ägarskap för tillgångarna.					R5		
	MK 3: För att ha kontroll över var verksamhetskritisk information hanteras ska dataflödet inom IoT-systemet och mellan systemdelar identifieras och dokumenteras.					R5		
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
7.1.4 Risker och hot, Identifiering och bedömning		**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 3: *IT-säkerhetsarkitektur.*	MK 4: Överväg noga riskerna vid utkontraktering och prioritera ökad säkerhet för inloggningar till externa tjänster (t. ex molntjänster).					R5		
Säkerhetsområde 1: *Styrning av säkerheten i informationssystem och riskhantering.*	GP-PS-11: En end-to-end identifiering och bedömning av risker och hot (RSA) som inkluderar såväl interna- som tredjepartsleverantörer, där det är möjligt, ska genomföras. *Kommentar: Riskbedömning bör göras löpande, eftersom komponenter i leveranskedjan ersätts, tas bort eller uppgraderas.* *Riskbedömningsproceduren bör initieras med att man först svarar på tre grundläggande frågor:* 1. Var är IoT applikationernas geografiska placering 2. För vilket ändamål (omfattning) 3. För vilket scenarier (företags-/organisationskrav) *Kommentar: Utvecklare och tillverkare bör inkluderas i riskbedömningsprocessen, vilket kommer att skapa öppenhet och göra det möjligt för dem att bli medveten om eventuella svagheter.*					R5		R7
Säkerhetsområde 1: *Styrning av säkerheten i informationssystem och riskhantering.* **Säkerhetsområde 3:** *IT-säkerhetsarkitektur.*	GP-PS-12: Den avsedda användningen och miljön för en given IoT-enhet ska vara identifierad. *Kommentar: Detta kommer att hjälpa utvecklare och tillverkare att bestämma de lämpligaste tekniska egenskaperna för IoT-enhetens funktion och de säkerhetsåtgärder som krävs samt att underlätta felhantering eller begäran om förbättringar effektiv.*					R5		

7.2 Organisation, personal och processmätvärden (OP)								
Alla organisationer ska ha organisatoriska kriterier för hantering av informationssäkerhet. Personalpraxis ska främja god säkerhet, säkerställa hanteringen av processer och en säker hantering av information i organisationen. Organisationer bör se till att alla inblandade intressenter och leverantörer är ansvariga för givna funktioner. I händelse av en incident i organisationens säkerhet ska organisationen vara förberedd med tydliga roller för ansvar, utvärdering och åtgärder.								
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
7.2.1 End-of-life support		**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 6: *Underhåll av IT-säkerhet.*	GP-OP-03: Det ska finnas en funktion för att hämta patchar/buggfixar för kända sårbarheter fram till slutdatum för en produkts livscykel. *Kommentar: På grund av den begränsade livscykeln för många IoT-enheter kan kritiska, offentligt kända säkerhets- eller sekretessfel utgöra en risk för att användarna använder föråldrade enheter.*	R1	R2	R3	R4	R5	R6	R7
	GP-OP-01 A: Det ska finnas en strategi för End of Life (EOL) och End of support (EOS) för IoT-produkter. *Kommentar: Införandet av patchar/buggfixar och uppdateringar kommer efter en tid att upphöra för vissa IoT-enheter.*	R1	R2	R3	R4	R5	R6	R7
	GP-OP-01 B: Det ska finnas en produktavvecklingsplan för att hantera End of Life (EOL) och End of Support (EOS) för att säkerställa att tillverkare och kunder är medvetna om de risker som finns för en enhet efter utgångsdatumet. End of Support (EOS) ska hanteras med hänsyn till när det är lämpligt att avveckla en IoT-enhet och eventuellt byta ut denna mot en av en nyare generation.	R1	R2	R3	R4	R5	R6	R7
	GP-OP-02: Tiden för hur länge uppdateringar och patchsupport löper efter produktgarantins utgång ska anges. *Kommentar: Sådana upplysningar bör anpassas till den förväntade livslängden hos anordningen och kommuniceras med kunden.*	R1	R2	R3	R4	R5	R6	R7
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
7.2.2 Beprövad lösning		**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 3: *IT-säkerhetsarkitektur.*	GP-OP-04: Beprövade lösningar, dvs välkända kommunikationsprotokoll och kryptografiska algoritmer, erkända av standardiseringsorgan, etcetera ska användas. *Kommentar: Vissa proprietära lösningar, såsom anpassade kryptografiska algoritmer, bör undvikas.* *Rent proprietära tillvägagångssätt och standarder begränsar driftskompatibiliteten. Beakta därför möjligheten till att välja alternativa leverantörer för komponenter i en systemlösning.*	R1	R2	R3	R4	R5	R6	R7
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
7.2.3 Hantering av säkerhetsproblem och / eller incidenter		**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 3: *IT-säkerhetsarkitektur.* **Säkerhetsområde 6:** *Underhåll av IT-säkerhet.*	GP-OP-06: Det ska finnas en funktion för att informera intressenter om avslöjade sårbarheter, patchar och rättelser samt säkerhetsmetoder för att ta itu med identifierade sårbarheter. *Kommentar: Funktionen bör involvera utvecklare, tillverkare och tjänsteleverantörer och inkludera information om eventuella sårbarheter som rapporterats till ett Computer Security Incident Response Team (CSIRT).*	R1	R2	R3	R4	R5	R6	R7
Säkerhetsområde 6: *Underhåll av IT-säkerhet.*	GP-PS-08: Det ska finnas en offentliggjord process för sårbarhetsrapporter. Ex. Bug Bounty-program för att identifiera sårbarheter som företagens egna interna säkerhetsgrupper kanske inte fångar upp.	R1	R2	R3	R4	R5	R6	R7

Säkerhetsområde 9: *Hantering av datasäkerhets-incidenter.*	GP-PO-07: Medverka i forum för informationsdelning för att själv rapportera sårbarheter och för att få aktuell och kritisk information om aktuella cyberhot och sårbarheter från offentliga och privata partners.	R1	R2	R3	R4	R5	R6	R7
Säkerhetsområde 6: *Underhåll av IT-säkerhet.*	GP-OP-05: Det ska finnas en process för analys och hantering av säkerhetsincidenter. För varje händelse ska det finnas ett svar på: 1. arten och omfattningen av händelsen 2. hur man ska ta kontroll över situationen 3. hur man ska kommunicera med användarna 4. hur man säkerställer en snabb och effektiv hantering av informationssäkerhetsincidenter.	R1	R2	R3	R4	R5	R6	R7
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
	7.2.4 Personalresurser, säkerhetsträning och medvetenhet	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 1: *Styrning av säkerheten i informationssystem och riskhantering.*	GP-OP-10: Utbildningsaktiviteter för personalen ska dokumenteras och följas upp.					R5		
	GP-OP-09: Personalpraxis ska främja integritet och säkerhet och personal ska utbildas i god integritet och säkerhetspraxis för säker användning av systemen, och till att inse att teknisk kompetens inte nödvändigtvis motsvarar säkerhetskompetens.					R5		
	GP-OP-11 A: Cybersäkerhetsroller och ansvar för all personal ska vara infört.					R5		
	GP-OP-11 B: Personliga åtaganden i enlighet med definierade säkerhetsbehov för ett projektgenomföranden ska användas.					R5		
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
	7.2.5 Tredjepartsrelationer	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 1: *Styrning av säkerheten i informationssystem och riskhantering.* **Säkerhetsområde 1:** *Styrning av säkerheten i informationssystem och riskhantering.*	GP-OP-12: Data som behandlas av en tredje part ska skyddas genom ett databehandlingsavtal med tredjepartsleverantören. *Kommentar: Vid överföring av data bör ansvaret för att skydda data också införas och efterlevnaden verifieras.*					R5		
	GP-OP-13 A: För att kunna dela en persons personuppgifter med tredje part ska personen givit sitt samtycke, utom då det krävs för, och är begränsat till, hantering av produktfunktioner eller service.					R5		
	GP-OP-13 B: Kräv att en tredjeparts tjänsteleverantör använder samma policyer, inklusive att hålla sådana uppgifter i förtroende- och med anmälningskrav för eventuella förluster av data och / eller obehörig åtkomst.					R5		
	GP-OP-14: IoT-hårdvarutillverkare och IoT-programvaruutvecklare ska anta riskhanteringspolicyer för cyberförsörjningskedjor. Cybersäkerhetskrav ska kommuniceras till leverantörer och partners.	R1	R2	R3	R4		R6.1	R7

7.3 Tekniska åtgärder (TM)								
För att minska sårbarheten i ett IoT-system ska säkerhetsåtgärder och god praxis implementeras och omfatta systemets tekniska element Tekniska mätvärden ska ge nödvändiga indata för de tekniska åtgärder som krävs för att bevara och skydda informationssäkerheten. Vid tillämpning av dessa tekniska åtgärder bör man ta hänsyn till särdragen i IoT-ekosystemet. Det innebär till exempel att vid ett stort antal involverade enheter och produkter kan vissa åtgärder behöva utföras med specialiserade arkitektoniska komponenter, till exempel gateways. För att minska sårbarheten i det tekniska systemet ska säkerhetsåtgärder och god praxis implementeras och omfatta systemets tekniska element. Tekniska mätvärden ska ge nödvändiga indata för de tekniska åtgärder som krävs för att bevara och skydda informationssäkerheten. Vid tillämpning av dessa tekniska åtgärder bör man ta hänsyn till särdragen i IoT-ekosystemet. Det innebär till exempel att vid ett stort antal involverade enheter och produkter kan vissa åtgärder behöva utföras med specialiserade arkitektoniska komponenter, till exempel gateways.								
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
	7.3.1 Hårdvara säkerhet	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 9: *Hantering av datasäkerhets-incidenter.*	GP-TM-02: Hårdvara som innehåller säkerhetsfunktioner för att stärka enhetens skydd och integritet ska användas t.ex. specialiserade säkerhetschips/coprocessors [System-on-a-Chip (SoC)] som integrerar säkerhet på transistornivå, inbäddade i processorn, som understödjer: 1. Chain of trust boot-loader som autentiserar operativsystemet innan det laddas, 2. operativsystem Chain of Trust som autentiserar applikations-programvara innan den laddas, 3. en säker startprocess för maskinvara och låsning av kritiska delar av minnet, 4. skyddat minne (NVM / RAM / Cache) för att undvika otillåten access till enhetens data (Eng. Snooping) och dekompilering (Eng. Reverse engineering), 5. kryptering och anonymitet, 6. slumptalsgenerator (Random Number Generator- RNG), 7. detektering av manipulation, 8. miljöövervakning och intern kontroll, 9. en tillförlitlig exekveringsmiljö, 10. en säker kodhämtning och exekvering (integritetskontroller), 11. kod- och datasignaturer, byggda under sammanställning och lagras och verifieras under körning, 12. en pålitlig lagring av enhetsidentitet och autentiseringsmedel, inklusive skydd av nycklar i vila och vid användning, 13. skydd mot privilegierad åtkomst till säkerhetskänslig kod samt 14. skydd mot lokala och fysiska attacker kan täckas via funktionell säkerhet.	R1	R2	R3			R6	R7
Säkerhetsområde 3: *IT-säkerhetsarkitektur.* **Säkerhetsområde 7:** *Fysisk- och miljömässig säkerhet.*	GP-TM-01: Det ska finnas en hårdvarubaserad, oföränderlig Root of Trust. *Kommentar: Root of Trust är en pålitlig hårdvarukomponent som alla säkra funktioner i ett datorsystem är beroende av. Den innehåller bland annat en betrodd exekveringsmiljö, nycklarna som används för kryptografiska funktioner och möjliggör en säker startprocess.*	R1	R2	R3			R6	R7
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
	7.3.2 Förtroende och integritetshantering	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 3: *IT-säkerhetsarkitektur.*	GP-TM-04 A: Kod ska vara kryptografiskt signerad för att säkerställa att den inte har manipulerats efter att ha skrivits in som säker för enheten. Endast signerad kod ska användas.	R1	R2	R3	R4	R5	R6	R7
	GP-TM-04 B: Realtidsskydd (Eng.Run-time) ska vara implementerat och exekverings-övervakning ska användas för att säkerställa att skadliga attacker inte skriver över kod efter att den har laddats.	R1	R2	R3	R4	R5	R6	R7

	Kommentar: Mätning av startprocessen möjliggör detektering av manipulering av värd-operativsystemet och programvaran, så att skadliga förändringar i enheternas beteende kan detekteras. Det gör det möjligt att upptäcka starttid av skadlig programvara för åtkomst till enheten (Eng.rootkits), virus och maskar.							
Säkerhetsområde 5: *Identitets-och åtkomsthantering.*	GP-TM-05 A: Installationen av programvara i system i drift ska övervakas, för att förhindra att inte autentiserad programvara och/eller filer kan installeras.	R1	R2	R3	R4	R5	R6	R7
	GP-TM-05 B: I händelse av att produkten är avsedd för att tillåta obehörig programvara, ska sådan programvara endast köras med begränsade behörigheter och/eller med en testmiljö som isolerar otestade kodändringar och direkta experiment i produktionsmiljön (Eng. Sandbox).	R1	R2	R3	R4	R5	R6	R7
Säkerhetsområde 9: *Hantering av datasäkerhets-incidenter.*	GP-TM-03: Startprocessen ska initiera de viktigaste hårdvarukomponenterna och starta operativsystemet. Förtroende (Eng.Trust) måste etableras i startmiljön innan något förtroende för någon annan programvara eller ett exekverbart program kan hävas, så den uppstartade miljön måste verifieras och beslutas vara i ett kompromisslöst tillstånd.	R1	R2	R3	R4	R5	R6	R7
Säkerhetsområde 9: *Hantering av datasäkerhets-incidenter.* **Säkerhetsområde 10:** *Driftsäkerhet*. **Säkerhetsområde 11:** *Krishantering.*	GP-TM-06: Efter att ett driftavbrott har inträffat, eller om en uppgradering inte har lyckats, ska det finnas en funktion för att återställa systemet till ett tillstånd som är känt för att vara säkert.	R1	R2	R3	R4	R5	R6	R7
Säkerhetsområde 2: *Systemhantering.*	GP-TM-07 A: Tillförlitliga och betrodda protokoll och mekanismer ska användas för att representera och hantera förtroende och förtroenderelationer.	R1	R2	R3	R4	R5	R6	R7
	GP-TM-07 B: Varje kommunikationskanal ska ha en tillförlitlighet som står i proportion till de säkerhetsberoende som den stöder (dvs hur mycket den är betrodd av andra komponenter för att utföra sina säkerhetsfunktioner).				R4	R5	R6	
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
	7.3.3 Stark default säkerhet och sekretess	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 1: *Styrning av säkerheten i informationssystem och riskhantering.* **Säkerhetsområde 3:** *IT-säkerhetsarkitektur.*	GP-TM-08: Alla tillämpliga säkerhetsfunktioner ska vara aktiverade som standard. *Kommentar: Alla oanvända tjänster och protokoll samt osäkra funktioner bör avaktiveras som standard. En stark säkerhetskontroll bör vara något användaren avsiktligt måsta inaktivera.*	R1	R2	R3	R4	R5	R6	R7
Säkerhetsområde 5: *Identitets-och åtkomsthantering.*	GP-TM-09: Det ska finnas funktioner och rutiner som gör det svårt att knäcka en enhets individuella standardlösenord. *Kommentar: Användarnamn och lösenord för IoT-enheter som tillhandahålls av tillverkaren ändras sällan av användaren och är lätta att knäcka, och ett svårt standardlösenord är fortfarande en svaghet om den används för mer än en enhet.*	R1	R2	R3	R4	R5	R6	R7
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
	7.3.4 Dataskydd och regelansvar (GDPR)	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 1: *Styrning av säkerheten i informationssystem och riskhantering.*	GP-TM-14: Användare av IoT-produkter och tjänster ska kunna utöva sina rättigheter avseende information, tillträde, radering, rättelse, dataöverförbarhet, begränsning av bearbetning, invändning mot bearbetning samt rätten att inte utvärderas på grundval av automatisk bearbetning.					R5.2		

	GP-TM-13: IoT-intressenter ska följa EU: s allmänna dataskyddsförordning (GDPR). Det komplexa nätverket av intressenter kräver en exakt fördelning av det lagliga ansvarat mellan dem när det gäller behandlingen av individernas personuppgifter, med utgångspunkt i särdragen i deras respektive uppgifter.					R5.2		
	GP-TM-11: Personuppgifter ska enbart användas för de angivna ändamål för vilka de samlades in. Ytterligare behandling av personuppgifter ska vara kompatibel med angivet ändamål och de registrerade ska vara välinformerade.					R5.2		
	GP-TM-10: Personuppgifter ska samlas in och behandlas rättvist och lagligt. Rättvisa principer kräver särskilt att personuppgifter aldrig ska samlas in och behandlas utan den registrerades samtycke.					R5.2		
	GP-TM-12: Data som samlas in och behålls ska minimeras. Många IoT-intressenter behöver bara aggregerade data och behöver inte det obearbetade data som samlas in av IoT-enheter. Involverade aktörer ska ta bort obearbetade data så snart de har extraherat de data som krävs för aktuell databehandling. *Kommentar: Som princip bör radering ske vid närmaste punkt för datainsamling av rådata (till exempel på samma enhet efter bearbetning).*					R5.2		
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
	7.3.5 Systemsäkerhet och tillförlitlighet	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 7: *Fysisk- och miljömässig säkerhet.*	GP-TM-15: IoT-enheter ska utformas och byggas så att driftstörningar inte leder till en större störning av systemet, skada eller avbrott i säkerhetskritiska processer, som kan påverka leveransen av en tjänst (till exempel energi, gas, värme eller vatten) eller orsaka en oacceptabel risk för fysisk skada på person eller miljö.	R1	R2					
Säkerhetsområde 10: *Driftsäkerhet*.	GP-TM-17: Viktiga funktioner ska fortsätta att fungera även vid avbrott i kommunikationen och kontinuerlig negativ påverkan från komprometterade enheter eller molnbaserade system. En förlust av kommunikationen får inte äventyra enhetens integritet, och IoT-enheter ska fortsätta att fungera även vid fel i molnets back-end.					R5		
Säkerhetsområde 9: *Hantering av datasäkerhets-incidenter.* **Säkerhetsområde 10:** *Driftsäkerhet*.	GP-TM-16: Det ska finnas mekanismer för säkerhetskopiering och för självdiagnos och självreparation för återställning efter fel, funktionsfel eller komprometterade tillstånd.					R5		
	MK 5: Säkerhetskopiering och återställning ska testas periodiskt.					R5.2		
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
	7.3.6 Säker programvara / firmware uppdatering	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 9: *Hantering av datasäkerhets-incidenter.* **Säkerhetsområde 10:** *Driftsäkerhet*.	MK 22: Endast godkänd programvara ska få köras (Vitlistning) och makron ska vara inaktiverade.	R1	R2	R3	R4	R5	R6	R7
Säkerhetsområde 9: *Hantering av datasäkerhets-incidenter.* **Säkerhetsområde 10:** *Driftsäkerhet*.	MK 23: Säkerhetsuppdateringar ska genomföras så fort det går.	R1	R2	R3	R4	R5	R6	R7

Säkerhetsområde 3: *IT-säkerhetsarkitektur.*	GP-TM-19 A: Automatiska uppdateringar av fast programvara ska vara aktiverade som standard. (Policyfråga).					R5.2		
	GP-TM-19 B: En enhet kan erbjuda ett alternativ som inaktiverar automatiska uppdateringar av fast programvara och med krav på autentisering. Erbjuds en automatisk uppdateringsmekanism för fast programvara så ska enheterna konfigureras för att kontrollera om det finns regelbundna uppdateringar av firmware.	R1	R2	R3	R4	R5	R6	R7
	GP-TM-20 A: Automatiska uppdateringar av fast programvara ska inte ändra nätverksprotokollens gränssnitt på ett sätt som är oförenligt med tidigare versioner.	R1	R2	R3	R4	R5	R6	R7
	GP-TM-20 B: Uppdateringar och korrigeringsfiler ska inte ändra användarinställda inställningar, säkerhets- och / eller sekretessinställningar utan användaranmälan.	R1	R2	R3	R4	R5	R6	R7
	GP-TM-20 C: Användare ska ha möjlighet att godkänna eller avvisa uppdateringar.	R1	R2	R3.2	R4.2	R5.2	R6.2	R7
Säkerhetsområde 3: *IT-säkerhetsarkitektur.* **Säkerhetsområde 4:** *Administration av IT-säkerhet.* **Säkerhetsområde 5:** *Identitets-och åtkomsthantering.* **Säkerhetsområde 6:** *Underhåll av IT-säkerhet.*	GP-TM-18: Innan en uppdateringsprocess påbörjas ska följande kontrolleras: 1. att enhetens programvara / firmware, dess konfiguration och dess applikationer har möjlighet att uppdateras OTA (Over The Air), 2. att uppdateringsservern är säker, 3. att uppdateringsfilen överförs via en säker anslutning, 4. att filen inte innehåller känsliga data (t.ex. hårdkodade uppgifter), 5. att filen är signerad av en auktoriserad tillitsenhet och krypterad med hjälp av accepterade krypteringsmetoder samt 6. att uppdateringspaketet har sin digitala signatur, signeringscertifikat och signaturcertifikat, verifierat av enheten innan uppdateringsprocessen börjar. *Kommentar: Att inte ha byggt in OTA-uppdateringsfunktioner (Over The Air) innebär att enheterna utsättas för hot och sårbarheter under hela livslängden.*			R3.2	R4.2	R5.2		
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
	7.3.7 Autentisering	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 4: *Administration av IT-säkerhet.* **Säkerhetsområde 5:** *Identitets-och åtkomsthantering.*	GP-TM-25: Inloggningsförsök ska skyddas mot "brute force" (en metod för att hitta exempelvis lösenord genom att pröva alla möjliga kombinationer) och/eller andra misstänksamma inloggningsförsök (till exempel automatiserade inloggningsrobotar etcetera) genom att låsa eller inaktivera användar- och supportkonton (er) efter ett rimligt antal ogiltiga inloggningsförsök. *Kommentar: Alternativt får användaren vänta en viss tid för att logga in igen efter ett misslyckat försök. Detta skydd bör också övervägas för nycklar som lagras i enheter.*	R1	R2	R3	R4	R5	R6	R7
Säkerhetsområde 5: *Identitets-och åtkomsthantering.*	GP-TM-24: Autentiseringsuppgifter, inklusive men inte begränsade till användarlösenord, ska vara Saltade, Hashed och / eller krypterade.	R1	R2	R3	R4	R5	R6	R7
	GP-TM-26: Lösenordsåterställning eller återställningsmekanismen ska vara robust och inte ge en angripare information som avser ett giltigt konto. Detta gäller också för viktiga uppdaterings- och återhämtnings-mekanismer.	R1	R2	R3	R4	R5	R6	R7
	GP-TM-21 A: Utformningen av autentiserings- och auktoriseringssystemen (unika per enhet) ska baseras på identifierade hotmodeller på systemnivå.					R5		
	GP-TM-21 B: Enheterna ska innehålla mekanismer för att på ett tillförlitligt sätt kunna verifiera sina backend-tjänster och för att stödja applikationer.	R1	R2	R3	R4		R6	R7

	GP-TM-22: Standardlösenord och standardanvändarnamn, ska ändras efter den ursprungliga inställningen, svaga, inga eller tomma lösenord är inte tillåtna.			R3.2	R4.2	R5.2	R6.2	
	GP-TM-23: Godkännandemekanismer ska använda starka lösenord eller personliga identifikationsnummer (PIN-koder). *Kommentar: Möjligheten att använda Tvåfaktorsautentisering (2FA) eller Multifaktorautentisering (MFA) som Smartphones, Biometrics, etcetera och certifikat bör övervägas.*	R1	R2	R3	R4	R5	R6	R7
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
	7.3.8 Tillstånd	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 5: *Identitets-och åtkomsthantering.*	MK 6: Det ska finnas ett dokumenterat arbetssätt med tydliga processer och rutiner för att förvalta användarkonton, roller och behörighet. Arbetssättet behöver inkludera hur ansvaret för förvaltningen ser ut.			R3.2	R4.2	R5.2	R6.2	
	MK 7: De olika användarkategorier som finns i verksamheten ska kartläggas och definieras för att fastställa behovet av regelbunden uppföljning och kontroll av dessa.			R3.2	R4.2	R5.2	R6.2	
	MK 8: Ansvar och ansvarsområden som står i konflikt med varandra åtskiljs så att ingen enskild person kan få tillgång till, ändra eller använda tillgångar utan tillstånd eller upptäckt.			R3.2	R4.2	R5.2	R6.2	
Säkerhetsområde 3: *IT-säkerhetsarkitektur.*	GP-TM-28 A: Firmware för enheter ska utformas för att isolera Priviligierad kod, processer och data från de delar av den fasta programvaran som inte behöver åtkomst till dem.	R1	R2	R3.1	R4.1		R6.1	R7
	GP-TM-28 B: För att minimera risken för att kompromitterad kod får tillgång till säkerhetskänslig kod och / eller data ska enhetshårdvara tillhandahålla ett isoleringskoncept.	R1	R2	R3.1	R4.1		R6.1	R7
Säkerhetsområde 5: *Identitets-och åtkomsthantering.*	GP-TM-27 A: Administratörsrättigheterna och behörigheterna för tillåtna åtgärder för ett visst system ska begränsas (t.ex. kan informationsägaren eller databasadministratören bestämma vem i en grupp av onlineanvändare som kan uppdatera en delad filåtkomst).			R3.2	R4.2	R5.2	R6.2	
	GP-TM-27 B: Regelverk för Åtkomstkontroll och finkorniga auktorisationsmekanismer - såsom Attributbaserad åtkomstkontroll (ABAC) eller Rollbaserad åtkomstkontroll (RBAC) - för att utföra privilegierade åtgärder, åtkomst till filer och kataloger, applikationer, etc. ska implementeras. Använd Principen om minst behörighet (POLP): Programmen måste fungera på lägsta möjliga privilegienivå.			R3.2	R4.2	R5.2	R6.3	
Säkerhetsområde 5: *Identitets-och åtkomsthantering.*	MK 9: Använd automatiserade och centrala verktyg för att styra åtkomst och behörigheter samt till att hålla en aktuell översikt av alla de konton och dess behörigheter som de har över tid. Godkännande av behörigheter/användarrättigheter måste kunna spåras till en ansvarig person och när i tiden ändringar av rättigheten skedde.			R3.2	R4.2	R5.2	R6.2	
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
	7.3.9 Tillgångskontroll – fysisk skydd	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 7: *Fysisk- och miljömässig säkerhet.*	GP-TM-31 A: Eftersom vissa enheter, Gateways etc. måste hanteras på distans snarare än att manövreras manuellt på plats ska åtgärder för att detektera och hantera manipulering vidtagas.			R3.2	R4.2	R5.2	R6.2	
	GP-TM-31 B: Detektering och reaktion på manipulering av hårdvara ska inte förlita sig på nätverksanslutning. *Kommentar: Manipulering av hårdvara innebär att en angripare har fysisk kontroll över enheten under en viss tid. I stort sett kan manipulering av hårdvara ske vid någon av de olika perioderna i en enhets livscykel.*			R3.2	R4.2	R5.2	R6.2	

	GP-TM-33 A: Enheter ska endast ha de nödvändiga fysiska externa portarna (till exempel USB) som är nödvändiga för dess funktion. *Kommentar: I allmänhet låser man ned fysiska portar till bara vara betrodda anslutningar.*	R1	R2	R3.1	R4.1	R5	R6.1	R7
	GP-TM-33 B: Test / debug-lägena ska vara säkra, så att de inte kan användas för att komma åt och skada enheterna.	R1	R2	R3.1	R4.1		R6.1	R7
Säkerhetsområde 1: *Styrning av säkerheten i informationssystem och riskhantering.*	GP-TM-30: Det ska finnas en ändamålsbaserad bedömning av säkerhet och integritet som speglar de olika säkerhetsnivåer som definierats för systemets/enhetens tillämpning (till exempel blåljus/kris, hemautomatisering).					R5		R7
Säkerhetsområde 1: *Styrning av säkerheten i informationssystem och riskhantering.* **Säkerhetsområde 5:** *Identitets-och åtkomsthantering.*	GP-TM-29: Dataintegritet och konfidentialitet ska hanteras genom Åtkomstkontroll. Har någon/något fått tillstånd att få tillgång till särskilda processer är det nödvändigt att tillämpa den definierade Säkerhetspolicyn. *Kommentar: Effektiviteten och styrkan av åtkomstkontrollen beror på huruvida åtkomstkontrollbesluten är korrekta (till exempel hur säkerhetsreglerna konfigureras) och styrkan i åtkomstkontrollens tillämpning (t ex design av mjukvaru- eller hårdvarusäkerhet).*					R5		
Säkerhetsområde 7: *Fysisk- och miljömässig säkerhet.*	GP-TM-32: Enheten ska inte enkelt kunna demonteras och datalagringsmediet ska vara krypterat i vila och inte enkelt kunna tas bort. *Kommentar: Det bör finnas mekanismer för att styra säkerhetsinställningar för en enhet, till exempel fjärrlåsning eller radering av innehåll på en enhet om enheten har stulits.*	R1	R2	R3.1	R4.1		R6.1	R7
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
	7.3.10 Kryptografi	**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 3: *IT-säkerhetsarkitektur.*	GP-TM-36: Enheter ska byggas så att de är kompatibla med Lightweight kryptering och säkerhetsteknik (inklusive säker identifiering, säker konfiguration etc.) som ena sidan kan användas för resursbegränsade enheter	R1	R2	R3.1	R4.1		R6.1	R7
	GP-TM-35: Kryptografiska nycklar ska hanteras säkert. *Kommentar: Kryptering är bara lika robust som förmågan hos det krypteringsbaserade system att hålla krypteringsnyckeln gömd. Kryptografisk nyckelhantering innefattar nyckelgenerering, distribution, lagring och underhåll.*	R1	R2	R3	R4	R5	R6	R7
	GP-TM-34: En korrekt och effektiv användning av kryptografi ska användas för att skydda sekretess, äkthet och / eller integritet av data och information (inklusive kontrollmeddelanden) både vid överföring och i vila. Se till att det är korrekt val av standard, starka krypteringsalgoritmer och starka nycklar. Inaktivera osäkra protokoll. Robustheten för implementationen ska verifieras.			R3.2	R4.2	R5	R6.2	R7
	GP-TM-37: Det ska finnas stödbara skalbara nyckelhanteringssystem i de fall kryptografi används i lösningen. *Kommentar: Det måste anses att små sensornoder inte kan tillhandahålla alla säkerhetsfunktioner eftersom de har många systembegränsningar. Således kan den avkända data som överförs via infrastrukturnätverk inte ha stark kryptering eller säkerhetsskydd.*	R1	R2	R3.2	R4.2	R5	R6.2	R7

Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
7.3.11 Säker och betrodd kommunikation		**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 3: *IT-säkerhetsarkitektur.*	GP-TM-39: Kommunikationssäkerheten ska tillhandahållas med hjälp av moderna standardiserade säkerhetsprotokoll, till exempel TLS för kryptering.			R3	R4	R5	R6	
Säkerhetsområde 2: *Systemhantering.*	GP-TM-42 A: Lita inte på mottagna data och verifiera alltid sammankopplingar.			R3	R4	R5.2	R6.2	
	GP-TM-42 B: Det ska finnas funktioner för att upptäcka, identifiera och verifiera / autentisera enheter som ansluts till nätverket innan förtroende upprättas. Bevara integriteten för tillförlitliga lösningar och tjänster. *Kommentar: En enhet mäter exempelvis sin egen integritet som en del av uppstart, men validerar inte dessa mätningar - när enheten begär anslutning till ett nätverk innebär det att en integritetsrapport skickas för fjärrvalidering. Om validering misslyckas avbryts anslutningen och enheten avgränsas för åtgärd.*			R3	R4	R5	R6	
Säkerhetsområde 3: *IT-säkerhetsarkitektur.*	GP-TM-45: Specifika portar och / eller nätverksanslutningar för selektiv anslutning ska vara inaktiverade. *Kommentar: Om det behövs, ge användarna riktlinjer för att utföra denna process vid den slutliga implementeringen.*			R3.2	R4.2	R5	R6.2	
	MK 10: Automatisk portscanning ska göras regelbundet mot alla servrar som bedöms vara centrala och ska jämföras mot godkänd konfiguration. Om förändringar upptäcks, och som inte är en del av verksamhetens godkända konfiguration, bör det loggas, rapporteras automatiskt och gås igenom manuellt. *Kommentar: Portskanning mot enkla komponenter med liten kapacitet i buffert kan vara vanskligt och ska därför användas restriktivt. Det kan av enheten uppfattas som en DDoS attack och enhetens funktionalitet kan bli hotad.*			R3.2	R4.2	R5	R6.2	
	GP-TM-38: De olika säkerhetsaspekterna för informationen - sekretess, integritet, tillgänglighet och äkthet – ska garanteras under överföringen i nätverket och vid lagringen i IoT-applikationen eller i molnet, med hjälp av datakrypteringsmetoder för att minimera nätverkshot, såsom återspelning, avlyssning och Packet sniffing.			R3.2	R4.2	R5	R6.2	
	GP-TM-46: För att minska risken för automatiska attacker ska det ska finnas möjlighet att kontrollera trafiken, hastighet/mängd som skickas eller tas emot av ett nätverk.					R5	R6	
Säkerhetsområde 2: *Systemhantering.* **Säkerhetsområde 3:** *IT-säkerhetsarkitektur.*	GP-TM-43 A: IoT-enheter ska vara restriktiva istället för tillåtande vid kommunikation.					R5		
	GP-TM-43 B: IoT-enheter ska inte förlita sig enbart på nätverksbrandväggen för att begränsa kommunikationen, eftersom vissa kommunikationer mellan enheterna i IoT-systemet kanske inte går igenom brandväggen. *Kommentar: När det är möjligt bör enheter inte nås via inkommande anslutningar som standard.*					R5		
Säkerhetsområde 3: *IT-säkerhetsarkitektur.*	GP-TM-41: Dataintegritet ska garanteras för att möjliggöra tillförlitligt datautbyte. *Kommentar: Data lagras ofta, cachas och bearbetas av flera noder. inte bara skickad från punkt A till punkt B. Av dessa skäl bör data alltid undertecknas samt ange när och varifrån data hämtas och lagras.*			R3	R4	R5	R6	
Säkerhetsområde 3: *IT-säkerhetsarkitektur.* **Säkerhetsområde 5:** *Identitets-och åtkomsthantering.*	GP-TM-40: Autentiseringsinformation (Eng. credentials) t.ex. lösenord, token, eller certifikat ska inte exponeras vid intern eller extern nätverkstrafik.	R1	R2	R3	R4	R5	R6	R7

Säkerhetsområde 3: *IT-säkerhetsarkitektur.*	GP-TM-44 A: Obehöriga anslutningar till enheten eller andra enheter som produkten är ansluten till, och på alla nivåer i protokollen, ska förhindras.	R1	R2	R3	R4	R5	R6	R7
	GP-TM-44 B: IoT-enheter ska meddela och/eller begära en användarbekräftelse när de initialt integreras, kopplas ihop och/ eller ansluts till andra enheter, plattformar eller tjänster.	R1	R2	R3	R4	R5	R6	R7
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
7.3.12 Säkra gränssnitt och nätverkstjänster		**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 2: *Systemhantering.* **Säkerhetsområde 3:** *IT-säkerhetsarkitektur.*	GP-TM-48: Protokoll ska utformas för att säkerställa att om en enda enhet är komprometterad, så ska denna inte kunna påverka övriga systemenheter.	R1	R2	R3.1	R4.1		R6.1	R7
Säkerhetsområde 4: *Administration av IT-säkerhet.*	GP-TM-53: Ett felmeddelande ska ge/visa endast den korta informationen användaren behöver - den får inte avslöja känslig information som kan utnyttjas av en angripare, till exempel ett fel-ID, en version av webbservern etc.	R1	R2	R3.1	R4.1		R6.1	R7
Säkerhetsområde 3: *IT-säkerhetsarkitektur.*	GP-TM-52: Användarsessionen i webbgränssnittet ska vara helt krypterad från enheten till backend-tjänsterna, och de ska inte vara mottagliga för ”Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), SQL Injection and HTML Injection” etc.			R3.1	R4.1	R5	R6.1	R7
Säkerhetsområde 2: *Systemhantering.* **Säkerhetsområde 5:** *Identitets-och åtkomsthantering.*	GP-TM-49: Samma hemliga nyckel ska undvikas i en hel produktfamilj, eftersom tillgång till nyckeln för en enda enhet skulle räcka för att avslöja resten av produktfamiljen. *Kommentar: Alla enheter bör ha egengenererade nycklar. Om det finns flera enheter med samma nyckel finns det risk för att det kan få kaskadeffekter om ett visst segment av IoT-systemet slås ut vilket skulle kunna generera en skadlig påverkan på resten av IoT-systemet.*	R1	R2	R3.1	R4.1	R5	R6.1	R7
Säkerhetsområde 3: *IT-säkerhetsarkitektur.*	GP-TM-51: En DDoS-resistent och lastbalanserad infrastruktur ska implementeras för att skydda tjänsterna mot DDoS-attacker som kan påverka enheten själv eller andra enheter och/eller användare i det lokala nätverket eller andra nätverk.					R5		
Säkerhetsområde 3: *IT-säkerhetsarkitektur.*	GP-TM-50: Endast nödvändiga portar ska vara öppna och tillgängliga.	R1	R2	R3	R4	R5	R6	R7
Säkerhetsområde 1: *Styrning av säkerheten i informationssystem och riskhantering.*	GP-TM-47: Nätverkselement ska delas upp i separata komponenter (risksegmentering) för att hjälpa till att isolera säkerhetsbrott och minimera den totala risken. *Kommentar: Nätverk kan delas in i separata delnätverk för att öka prestanda och förbättra säkerheten.*					R5	R6	
	MK 23. Segmentera nätverken och filtrera trafiken mellan nätverken.					R5	R6	
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
7.3.13 Säker in- och utmatning		**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 3: *IT-säkerhetsarkitektur.* **Säkerhetsområde 4:** *Administration av IT-säkerhet.*	GP-TM-54: Validering av att data är säker för användning ska ske vid inmatning (validering) och utmatning (filtrering) av data. *Kommentar: Säkerhet är ett problem för Besluts-triggers (skadlig kod eller generella fel). Andra problem kan vara indirekt manipulering av ingångsvärden till Besluts-triggers genom att manipulera eller begränsa ingångsvärdena. Tillförlitlighet är ett problem för Beslut-triggers (generella brister). Beslut-triggers kan vara inkonsekventa, självmotstridiga och ofullständiga. Att förstå hur skadliga data sprids för att påverka Beslut-triggers är avgörande. Underlåtenhet att åtgärda fel i Beslut-triggers i tid kan få oönskade konsekvenser.*	R1	R2	R3	R4		R6	R7

Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
7.3.14 Loggning		**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
	MK 11: Det ska finnas en rutin för logghantering.					R5		
Säkerhetsområde 8: *Loggning.*	GP-TM-55: Det ska finnas ett loggningssystem som registrerar händelser som rör användarautentisering, hantering av konton och åtkomsträttigheter, ändringar av säkerhetsregler och systemets funktion. Loggarna måste också bevaras under angiven tid i varaktigt lagringsutrymme och kunna återvinnas via en autentiserad anslutning.	R1	R2	R3.2	R4.2	R5	R6.2	R7
	MK 12: Loggar ska vara konfigurerade så att de skickas centralt och analyseras.	R1	R2	R3.2	R4.2	R5	R6.2	R7
	MK 13: Alla system som loggas ska synkroniseras mor samma tidkälla och tidszon.	R1	R2	R3.2	R4.2	R5	R6.2	R7
	MK 14: Det ska finnas tillräcklig behörighetsstyrning för att ta del av innehållet i loggar. Loggar ska skyddas mot obehörig förändring.			R3.2	R4.2	R5	R6.2	
	MK 15: Loggningsinställningar och loggningsdata ska valideras.			R3.2	R4.2	R5	R6.2	
	MK 16: Synkronisera loggar mot minst två referenstidskällor så att aktiviteter förses med en korrekt tidsstämpel och kan läsas av kronologiskt.			R3.2	R4.2	R5	R6.2	
	MK 17: Loggarna ska arkiveras och signeras digitalt med jämna mellanrum för att bevara riktigheten i loggarna.			R3.2	R4.2	R5	R6.2	
	MK 18: Loggar ska använda ett standardiserat format så att de enkelt kan läsas av tredje parts logganalysverktyg.	R1	R2	R3.2	R4.2	R5	R6.2	R7
	MK 19: Behovet av loggning av metadata och/eller innehåll bör vägas mot användarens respektive verksamhetens behov av skydd för konfidentialitet och bör beskrivas.					R5		
Roller --- R1- IoT enheter **R2**- Andra typer av IoT-enheter **R3**- Funkpl. & backend **R4**- App. & tjänster **R5**- IoT- syst **R6**- Komm. **R7**- Säktill.								
7.3.15 Övervakning och revision		**R1**	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**
Säkerhetsområde 1: *Styrning av säkerheten i informationssystem och riskhantering.* **Säkerhetsområde 6:** *Underhåll av IT-säkerhet.*	GP-TM-57: Regelbundna granskningar och översyner av säkerhetskontrollerna ska utföras för att säkerställa att kontrollerna är effektiva. Penetrationstest ska utföras minst två gånger per år. *Kommentar: Granskningen av säkerhetsrelaterade händelser samt övervakning och spårning av systemavvikelser är viktiga inslag i efterhandsanalysen och för återställning efter ett säkerhetsrelaterade fel.*			R3.2	R4.2	R5	R6.2	
Säkerhetsområde 8: *Loggning.*	GP-TM-56: Det ska genomföras en regelbunden övervakning för att verifiera en enhets beteende, upptäcka skadlig kod och upptäcka integritetsfel.			R3.2	R4.2	R5	R6.2	
Säkerhetsområde 8: *Loggning.*	MK 20: Det ska finnas ett automatiserat system för övervakning av konfiguration som verifierar alla externt testbara element och som varnar när obehöriga ändringar förekommer. Detta inkluderar funktionalitet för att övervaka ändringar i brandväggskonfiguration (t ex öppning av nya portar), nya administrativa användare och nya tjänster som körs i ett system.			R3	R4	R5		
Säkerhetsområde 8: *Loggning.*	MK 21: Automatiska verktyg för att säkerställa att kritiska systemfiler inte har ändrats ska användas. Kontrollerna bör identifiera misstänkta systemändringar såsom ändringar av ägare och behörigheter för filer eller kataloger, användning av alternativa dataströmmar som kan användas till att dölja illasinnade aktiviteter samt införande av extra filer till mappar som är avsedda för operativsystemet. Upptäckt av sådant kan indikera på skadlig kod som angripare lämnat eller filer som är felaktigt lagda vid batch- distributionsprocesser			R3	R4	R5		

8. ÖVERSIKT AV IOT- HOT

I tabellen nedan redovisas bashot mot IoT- systemen. Bashoten ligger till grund för genomförandet av Risk- och sårbarhetsanalyser. Bashoten är utarbetade och kategoriserade av ENISA.

Notis: Hot kopplade till Social engineering (manipulering av människor så att de lämnar ifrån sig konfidentiell information eller manipulerar IoT-systemet negativt) definieras inte i dessa bashot.

Översikt av IoT- hot		
Hotkategori	**Bashot (- *Systemdel*)**	**Beskrivning**
Skadlig aktivitet/Missbruk Nefarious activity / Abuse	**Skadlig kod (Malware)** *- IoT enheter* *- Övriga IoT enheter* *- Plattformar och Backend*	Programvaror som är utformade för att utföra oönskade och obehöriga åtgärder i ett system utan användarens samtycke, vilket resulterar i skada, korruption eller stöld av information. Påverkan kan vara hög.
	Kod som utnyttjar svagheter (ExploitKits) *- IoT enheter* *- Övriga IoT enheter*	Kod utformad för att dra fördel av en sårbarhet för att få tillgång till ett system. Detta hot är svårt att upptäcka och i IoT-miljöer varierar dess påverkan från hög till avgörande beroende på de berörda tillgångarna.
	Målinriktade attacker *- Infrastruktur* *- Plattformar och Backend* *- Information*	Attacker utformade för ett specifikt mål, som har pågått under en lång tidsperiod och genomförts i flera steg. Huvudmålet är att förbli dold och att få så mycket känslig data / information eller kontroll som möjligt. Medan effekterna av detta hot är medium, är det vanligtvis mycket svårt att upptäcka dem och det tar lång tid.
	Skador genom förfalskade enheter *- IoT enheter* *- Övriga IoT enheter* *- Infrastruktur*	Detta hot är svårt att upptäcka eftersom en förfalskad enhet inte lätt kan skiljas från originalet. Dessa enheter har vanligtvis bakdörrar och kan användas för att utföra attacker mot andra IKT-system i miljön.
	Överbelastningsattacker (DDoS) - IoT enheter - Övriga IoT enheter - Plattformar och Backend - Infrastructure	Flera system attackerar mot enda mål för att överbelasta det och få det att krascha. Detta kan göras genom att göra många anslutningar, överbelasta en kommunikationskanal eller spela upp samma kommunikation om och om igen
	Attack mot användarnas integritet *- IoT enheter* *- Övriga IoT enheter* *- Plattformar och Backend* *- Information*	Detta hot påverkar både användarnas integritet och exponeringen av nätverkselement för obehörig personal.
	Manipulering av information *- IoT enheter* *- Övriga IoT enheter* *- Plattformar och Backend* *- Information*	I detta fall är målet inte att skada enheterna, utan att manipulera informationen för att orsaka kaos eller få ekonomiska vinster.
Avlyssning/ Uppfångande/ Kapning Eavesdropping / Interception / Hijacking	**Mannen i mitten (Man, in the middle)** *- Information* *- Kommunikation* *- IoT enheter*	Aktiv avlyssningsattack, där angriparen fångar upp och vidarebefordrar meddelanden från ett offer till ett annat, för att få dem att tro att de pratar direkt med varandra
	Kapning av IoT kommunikationsprotokoll *- Information* *- Kommunikation* *- IoT enheter* *- Beslutsfattande*	En inkräktare tar kontroll över en befintlig kommunikationssession mellan två eheter i nätverket. Inkräktaren kan fånga upp känslig information, inklusive lösenord. Kapningen kan använda aggressiva tekniker som att tvinga fram frånkoppling eller ett förnekande av tjänst.
	Avlyssning av information *- Information* *- Kommunikation* *- IoT enheter*	Obehörig avlyssning (och ibland modifiering) av en privat kommunikation, till exempel telefonsamtal, snabbmeddelanden, e-postkommunikation

Översikt av IoT- hot (fortsättning)		
Hotkategori	**Bashot (-** ***Systemdel*** **)**	**Beskrivning**
Avlyssning/ Inhämtning/ Kapning Eavesdropping / Interception / Hijacking	**Informationsinsamling** *- Information* *- Kommunikation* *- IoT enheter*	Få tillgång till intern information om nätverket: anslutna enheter, använt protokoll etc.
	Upprepning av meddelanden *- Information* *- IoT enheter* *- Beslutsfattande*	Den här attacken använder en giltig dataöverföring genom att repetetivt skicka den, alternativt försena den, för att manipulera eller krascha enheten som utgör målet för attacken.
	Skanning av nätverk (Network reconnaissance) *- Information* *- Kommunikation* *- IoT enheter* *- Infrastruktur*	Få tillgång till intern information om nätverket: anslutna enheter, använda protokoll, öppna portar, tjänster som används osv
	Sessionskapning *- Information* *- Kommunikation* *- IoT enheter*	Stöld av en dataförbindelse genom att agera som en legitim värd med avsikten att stjäla, ändra eller radera överförd data.
Driftavbrott Outages	**Fel i system** *- IoT enheter* *- Plattformar och Backend* *- Övriga IoT enheter*	Hot om fel i programvarutjänster eller applikationer
	Avbrott i nätverk *- Infrastruktur* *- Kommunikation*	Avbrott eller fel i nätverket, antingen avsiktligt eller oavsiktligt. Beroende på det berörda nätverkssegmentet och den tid som krävs för att återhämta sig, är vikten av detta hot från hög till kritisk.
	Fel på enheter *- IoT enheter*	Hot om fel eller fel på hårdvara
	Förlust av supporttjänster *- Alla tillgångar*	De supporttjänster som krävs för en korrekt drift av informationssystemet är inte tillgängliga.
Skada/ Förlust Damage / Loss (IT Assets)	**Läckage av Data/Känslig information** *- IoT enheter* *- Övriga IoT enheter* *- Plattformar och Backend* *- Information*	Känslig information avslöjas, avsiktligt eller inte, för obehöriga parter. Betydelsen av detta hot kan variera mycket beroende på typen av data.
Fel/Störningar Failures / Malfunctions	**Sårbarhet i programvara (Software vulnerabilities)** *- IoT enheter* *- Övriga IoT enheter* *- Plattformar och Backend* *- Infrastruktur* *- Applikationer och tjänster*	De vanligaste IoT-enheterna är ofta sårbara på grund av svaga / standardlösenord, programvarufel och konfigurationsfel, vilket utgör en risk för nätverket. Detta hot är vanligtvis kopplat till andra, som exploateringssatser (exploit kits), och det anses vara kritskt.
	Tredje parts fel (Third parties failures) - IoT enheter - Övriga IoT enheter - Plattformar och backend - Infrastruktur - Applikationer och tjänster	Fel på ett aktivt element i nätverket orsakat av felkonfiguration i ett annat element som har direkt relation till det aktiva elementet.
Katastrof Disaster	**Naturkatastrofer** *- IoT enheter* *- Övriga IoT enheter* *- Plattformar och Backend* *- Infrastructure*	Detta inkluderar händelser, t.ex.översvämningar, kraftig vind, kraftiga snöbyar och jordskred, som fysiskt kan skada enheterna.
	Miljökatastrof *- Övriga IoT enheter* *- Plattformar och Backend* *- Infrastruktur*	Katastrofer i IoT-utrustningens implementeringsmiljöer som orsakar problem med deras driftskompatibilitet.
Fysiska attacker Physical attacks	**Enhetsmodifiering** *- Kommunikation* *- IoT enheter*	Förlust av en enhet genom att inkräktaren till exempel dragit fördel av dålig konfiguration av portar eller utnyttjat de som lämnas öppna
	Sabotage av enheter *- IoT enheter* *- Övriga IoT enheter* *- Plattformar och Backend* *- Infrastruktur*	Händelser som stöld av enheter, bombattacker, vandalism eller sabotage kan skada enheter

9. RISKHANTERING

9.1 Allmänt

IoT- Ekosystemen skiljer sig från allmän säkerhet genom att funktionen hos en enhet, IoT-enheten, är helt avgörande för systemets avsedda funktion. En och samma IoT- enhet kan också användas på flera olika sätt och i olika miljöer med varierande hot och risker.

För att exemplifiera detta används en temperaturgivare som utgångspunkt. Temperaturgivare är en IoT-enhet med en sensor för att mäta temperatur. Denna givare kan användas på rätt så många olika sätt ur ett IoT-perspektiv.

1. **Temperaturgivare för att mäta endast temperaturmätning**
   Ex. badtemperatur på publika bad till allmänheten

2. **Temperaturgivare för att mäta temperatur i kritiska anläggningar**
   Ex. Tempsenor i ställverk för eldistribution för upprätthållande av robust driftmiljö

3. **Temperarutgivare i fastigheter för att reglera komfortvärme**

4. **Temperaturgivare i fastigheter för att reglera komfortvärme men och för att mäta en eskalerad temperaturökning under kort tid för att identifiera en möjlig brand kopplat till ett larmsystem**

När dessa fyra scenarier appliceras på det konceptuella IoT- Ekosystemet fås följande kritiska komponenter och funktioner att hantera ur ett säkerhetsperspektiv.

9.2 SCENARIOR

Scenario 1, 2 och 3

I Scenario 1, 2 och 3 är det en ”sensor” som mäter den fysiska entiteten temperatur och översätter den till ett digitalt format för hantering.

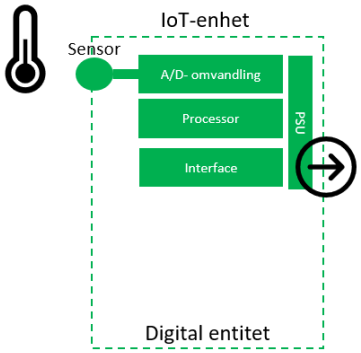

Bild: IoT-enhet för mätning av temperatur

Scenario 1 – Enkel användning av sensor

Scenario 1 kräver i princip ingen kryptering av data eller annan typ av informationssäkerhet än grundläggande stöd. Fokus här ligger på driftsäkerhet då tempgivaren befinner sig i vattnet. Om data manipuleras eller på något sätt hindras att behandlas så är riskkonsekvensen låg, då information till allmänheten blir bristfällig men inget mer händer.

Scenario 2 - Beslutstöd med hjälp av sensor
I scenario 2 kommer mätt temperatur från givaren att användas som en del i ett stöd för att verifiera rätt driftmiljö i en kritisk anläggning. Med detta som utgångspunkt så krävs det att data skickat från IoT-enheten kan valideras som korrekt från IoT-enheten till API-gränssnittet. Då faller flera säkerhetsaspekter in i bilden. IoT-enheten måste ha möjlighet till att skicka krypterat data genom IoT kommunikationsnät. IoT-stödsystem måste ha krav på dekryptering, loggning och behörighetsrutiner, likaså REST-API: t. Säkerhetskraven kan till och med kräva att IoT Ekosystem är skilt från annan IoT och får då ses som ett proprioritärt IoT Ekosystem för kritiskt system och driftdata.

Scenario 3 – Kombinationsfunktion av sensor
Scenario 3 är en hybrid mellan 1 och 2. Risken för manipulerat data är medelmåttig eftersom IoT-stödsystem transporterar data till ett tredjepartsystem som använder data från sensor som en del i ett större beslutfattande om att reglera värme i t ex ett hus. Värdet i sig själv är inte avgörande för beslutet men det ökar kvaliteten i fall det är rätt. Därför behövs inte krypterad trafik men däremot intrångsskydd till IoT-enhet, kommunikationsnät, IoT-stödsystem samt Rest-API. Ekosystemet kan dela resurser med andra IoT-enheter.

Scenario 4 – Kritisk funktion av sensor
I scenario 4 är det också en ”sensor” som mäter den fysiska entiteten men också en ”actuator” som skickar en signal till ett brandlarm. Sättet att hantera exempelvis en kraftig temperaturökning kan göras på två sätt. Ett autonomt system i IoT-enheten som själv avgör om actuatorn ska skicka signal till brandlarmet, alternativ att temperatur mäts och skickas vidare till IoT stödsystem för beslut om att skicka signal till brandlarm via IoT-enhetens actuator.

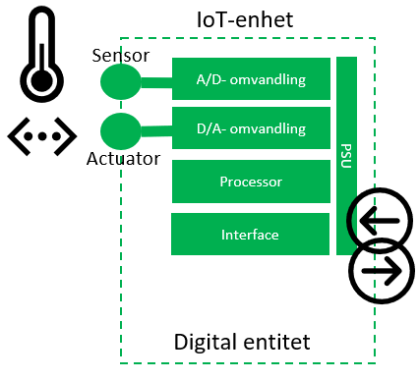

Bild: IoT-enhet inte autonom

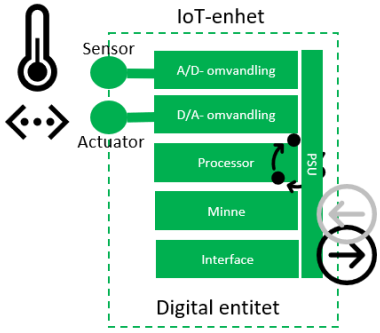

Bild: IoT-enhet autonom

Detta scenario höjer säkerhetskraven på IoT-enheter och andra komponenter i ekosystemet avsevärt. IoT-enheterna i sig själv är mer kompetenta och likvärdig en dator som går att använda för olika typer av cyberattacker. Manipulering eller nefarious aktivitet, dvs aktivitet som har till syfte att påverka andra saker. Ex köra igång ett brandlarm och sprinklersystem genom att påverka sensorn värde. Dessa IoT-enheter måste i sin design ha mekanismer för att identifiera och stoppa sådana odåd.

Dessa fyra exempel utgör en beskrivning över hur en och samma IoT-enhet kan baserat på vad de ska åstadkomma med applikationen eller applikationerna skapa olika utmaningar gällande säkerhet. Det är därför extra viktigt när det handlar om IoT att ta hänsyn till hela IoT-ekosystemet vid en säkerhetsanalys. IoT-enheter har en tendens att bli många och därför blir sårbarheten extra stor vid brister i säkerheten.

9.3 Metod för riskanalys

De olika stegen i en riskanalys omfattar följande steg:

- Välj och beskriv analysobjekt
- Identifiera hot
- Gruppera ock klassificera hot
- Genomför en riskanalys
- Sammanställning och rapport
- Handlingsplan – åtgärdslista
- Riskhantering enligt åtgärdsplan
- Kontinuitetsplanering

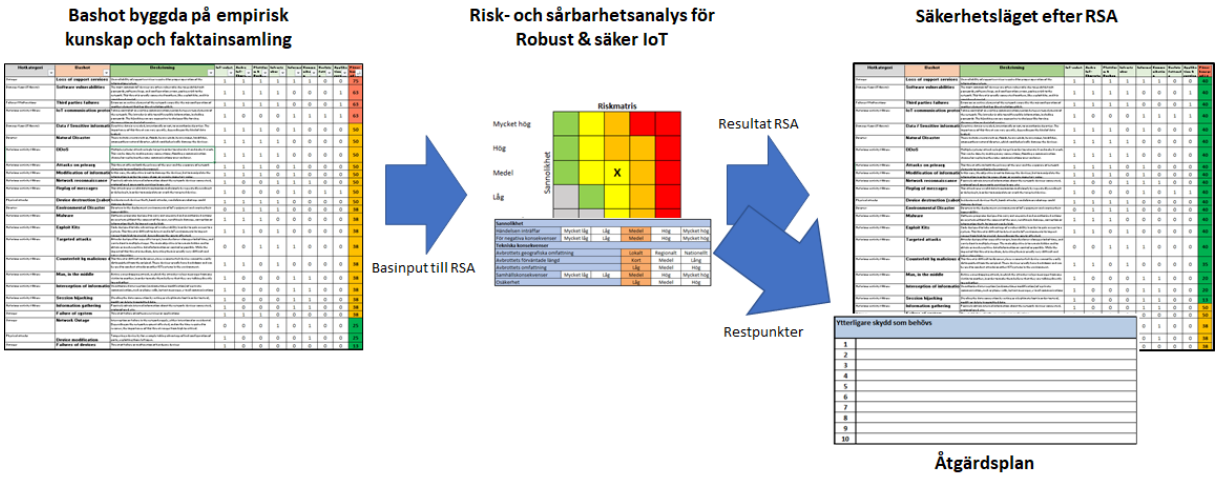

Bild: Översikt riskanalys

IoT-säkerhetsarbetet måste koordineras med det ordinarie säkerhetsarbetet och ses som en nödvändig komplettering för att kunna erbjuda IoT-relaterade tjänster. Bilden nedan beskriver en riskskala med tre nivåer som går att tillämpa för att förstå arbetet kring varje implementering av funktioner i sitt IoT ekosystem. IoT-kundens verksamhet/krav är alltid utgångspunkten och avgör säkerhetsrisk och nivå på säkerhetskrav.

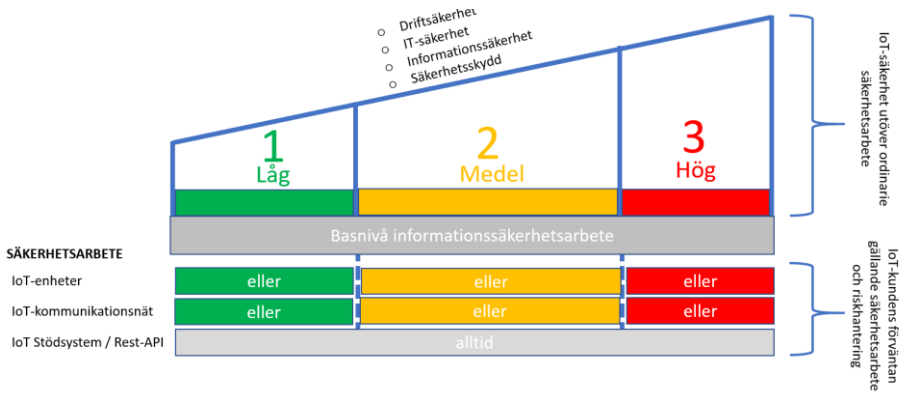

Bild: Riskskala IoT

För genomförandet av en Risk- och sårbarhetsanalys hänvisas till:

- Bilaga 2; Rutin och handledning för Risk- och sårbarhetsanalys
- Bilaga 2.1; Verktyg RSA- mall Robust & Säker IoT

10. LAGRUMMET

Inom ramen för arbetet med vägledningen har nedanstående lagar och förordningar identifierats som styrande dokument för de organisationer som tillhandahåller IoT-lösningar.

Lag (2003:389) om elektronisk kommunikation: 5 kap. 6 b § samt 6 kap. 3 §
Lagen om elektronisk kommunikation (2003:389) kravställer att det finns ett strukturerat och kontinuerligt informationssäkerhetsarbete för en aktör som handhar allmänt kommunikationsnät.

Förordning (2003:396) om elektronisk kommunikation: 34 a §, 34 b § samt 37 §

PTSFS 2014:1
PTS föreskrifter om allmänna råd om skyddsåtgärder för behandlade uppgifter: 3 §

PTSF 2015:2
Driftsäkerhetsföreskriften

BILAGA 1. RUTIN OCH HANDLEDNING, KRAVANALYS ROBUST OCH SÄKER IOT

BILAGA 1.1 VERKTYG, KRAVANALYS ROBUST OCH SÄKER IOT

BILAGA 2. RUTIN OCH HANDLEDNING, RSA ROBUST OCH SÄKER IOT

BILAGA 2.1 VERKTYG, RSA- MALL ROBUST OCH SÄKER IOT

BILAGA 3. REFERENSER ROBUST OCH SÄKER IOT