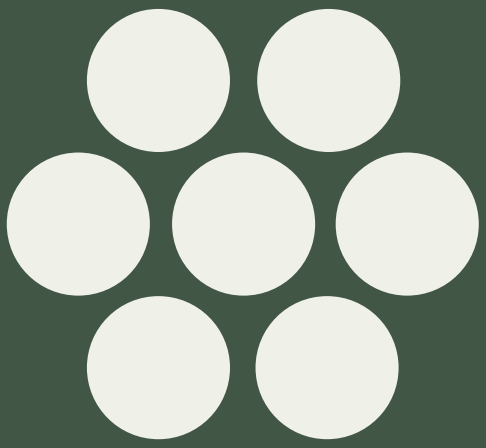
Vägledning för Robust & säker IoT

Huvuddokument

Version 2.0



Robust digital infrastruktur

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.

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.
- Förstå 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 / Lagrum

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

- ENISA Good practices for IoT and Smart Infrastructures Tool
- Guidelines for Securing the Internet of Things
- ENISA Baseline Security Recommendations for IoT
- MSB:s stöd i risk- och sårbarhetsanalys
- MSB1523 2020 IoT-relaterade risker
- ISO/IEC 3014:2024 Internet of Things Reference architecture
- ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection
- ISO/IEC TR 15446:2017 Vägledning för produktion av skyddsprofiler och säkerhetsmål.
- Gällande lag om Elektronisk kommunikation samt dess förordning

1.6 Identifierade brister och utmaningar inom IoT

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). 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 mjukvaran.
- 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 informationsinfrastruktur[1]. 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 taxonomi osv.

[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

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 område 5: *Brist på ekonomiska incitament*.

1.7 Riktlinjer för att säkra IoT

Sammanfattning av slutsatserna från analysen av *god praxis och standarder kap 5 i ENISAS Guidelines for Securing the Internet of Things.* Slutsatserna tar formen av riktlinjer som representerar rekommendationer på hög nivå och en ingångspunkt till den utökade uppsättningen av god praxis.

1: Skapa bättre relationer mellan aktörer

Denna riktlinje fokuserar på att lösa säkerhetsproblem som uppstår från kommunikationsproblem och relationer i leveranskedjan. Dessa problem kan vara onda till sin natur eller ha sitt ursprung i missförstånd eller brist på samordning. Några problematiska exempel som kan identifieras inkluderar fel i design på grund av bristande synlighet i de komponenter som levereras av leverantörer, eller överproduktion av en produkt utanför gränserna för ett etablerat avtal.

God praxis att överväga:

- Prioritera att arbeta med leverantörer som kan ge cybersäkerhetsgarantier.
- Arbeta med att förbättra transparensen i leveransförmågan.
- Utveckla innovativa modeller för att skapa förtroende.
- Inför synen på säkerhet i leveranskedjan som en kontinuerlig process.
- Främja antagandet av servicenivåer som kräver konkreta säkerhetsåtgärder.

Mest relevanta standarder:

- ISO/IEC 27001: Krav för ett informationshanteringssystem för informationssäkerhet (ISMS).
- ISO 27036: Informationssäkerhet för leverantörsrelationer.

2: Cybersäkerhetsexpertisen bör vidareutvecklas

Medlemmar från alla delar av en organisation (t.ex. ingenjörer, tekniker, ledning och marknadsföring) kan vara benägna att försumma säkerhetsträning och utbildning, felaktigt anta att "det kommer inte att hända mig eller min organisation". Men säkerhetsproblem tenderar att vara genomgripande och allvarliga, och som sådana måste bristen på kunskap inom detta område adekvat hanteras. Det bör också noteras att ytlig säkerhetskunskap kan leda till en falsk trygghetskänsla och kan utgöra ett hot. Brister i utbildning, brist på standardprocedurer och begränsad övervakning har vanligtvis en direkt korrelation till betydande säkerhetshål i senare skeden av produkten.

God praxis att överväga:

- Underhåll och utbilda en kvalificerad och skicklig personal.
- Främja en kultur som fokuserar på ett riskbaserat tillvägagångssätt.
- Främja IoT-säkerhetsmedvetenhet för användare.

Mest relevanta standarder:

- NIST 8276: Praxis inom cyberförsörjningskedjans riskhantering.

3: Inbyggd säkerhet eller säkerhet som standard

Design av IoT-enheter kräver noggrann planering och riskhantering. Beslut som tas i början av processen påverkar hur enkelt det blir att underhålla enheterna senare. Det finns mycket att tänka på eftersom IoT-enheter ofta har speciella begränsningar, som till exempel begränsade resurser. Flexibilitet är önskvärd men en välplanerad strategi är viktig. Kundkrav bör vara huvudfokus för säkerhetsbedömning. Att inte prioritera cybersäkerhet i IoT-massprodukter kan fördröja antagandet av säkerhetsteknologier.

God praxis att överväga:

- Inför princip för inbyggd säkerhet i enheter.
- Etablera och förbättra datainsamling, mätteknik och datahantering.
- Nyttja ny teknik för säkerhetskontroll och revision.
- Etablera och förbättra planering och hantering av uppgradering på enheter och system.
- Inför mekanismer för fjärruppdatering.
- Använd och utvärdera hotmodeller för IoT-leverantörskedjan.

Mest relevanta standarder

- ISO 20243: Mildring av uppsåtliga och förfalskade produkter.

4: Ta ett omfattande ansvar att införa säkerhet

Säkerhetshoten inom IoT är ofta lokaliserade längs leveranskedjan, vilket är kritiskt med tanke på den ökade spridningen av enheter och deras vanliga användning i offentliga miljöer och autonom drift. Data och design måste genomgå noggrann analys och validering från olika perspektiv.

Data och design kan analyseras och valideras från flera perspektiv, och mänskligt ingripande bör övervakas noggrant när det är möjligt. Kostnaden för att reagera på en säkerhetsincident är vanligtvis högre än kostnaden för att proaktivt hantera problemet.

God praxis att överväga:

- Identifiera tredjepartsprogramvara.
- Upprätta en omfattande testplan.
- Implementera fabriksinställningar som använder säkerhet som standard.
- Erbjud säkerhetsuppdateringar under en bestämd period, som kan motsvara enhetens eller produkten livscykel.
- Integrera processer för hantering av säkerhetsavfall.
- Använd säkra tekniker för borttagning av data.
- Använd hårdvarumekanismer för intern validering.
- Integrera identitetshanteringssystem för IoT-enheter.
- Införliva en stark grund av förtroende.
- Integrera autentiseringsmekanismer i kretsar.
- Överväg cybersäkerhetsmöjligheter som introduceras av samarbete mellan hårdvara och mjukvara.
- Dokumentera arbete, enhetsuppdateringar, nätverksförändringar och säkerhetsaktiviteter i samband med arbetsprocessen.

Mest relevanta standarder:

- ISO 11889: Trusted Platform Module (TPM).
- IETF RFC 8520: Manufacturer usage description (MUD).
- IEEE 802.1AR-2018: Säker enhetsidentitet för lokala och metropolnätverk.
- ISO 20243: Mitigating maliciously tainted and counterfeit products.

5: Använd existerande standarder och goda praxis

Etablerade normer, tidigare erfarenheter och juridiska riktlinjer är grundläggande för IoT-leveranskedjans framgång. Organisationer bör anpassa bästa metoder till sina behov och samarbeta för att främja säkerhetsstandarder. Det är viktigt att agera innan regleringar tvingas fram av regeringar. Genom att tillämpa säkerhetsstandarder minskas risken för attacker vid varje steg i kedjan.

God praxis att överväga:

- Utveckla eller anpassa standarder för IoT-leverantörskedjan.

Mest relevanta standarder:

- GSMA SAS-UP: Säkerhetsackrediteringssystem för UICC-produktion.
- CMU SPL: Säkerhets- och integritetsmärkning

2. Definitioner, förtydliganden och förkortningar

2.1 IoT-system en översikt

ENISA definierar Internet of Things (IoT) som en avancerad uppsättning teknologier och hänvisar till ett brett ekosystem där sammankopplade enheter och tjänster samlar in, utbyter och bearbetar data för att dynamiskt anpassa sig till ett sammanhang. Schematisk bild över komponenterna/tillgångarna (assets groups) i ett IoT-system.

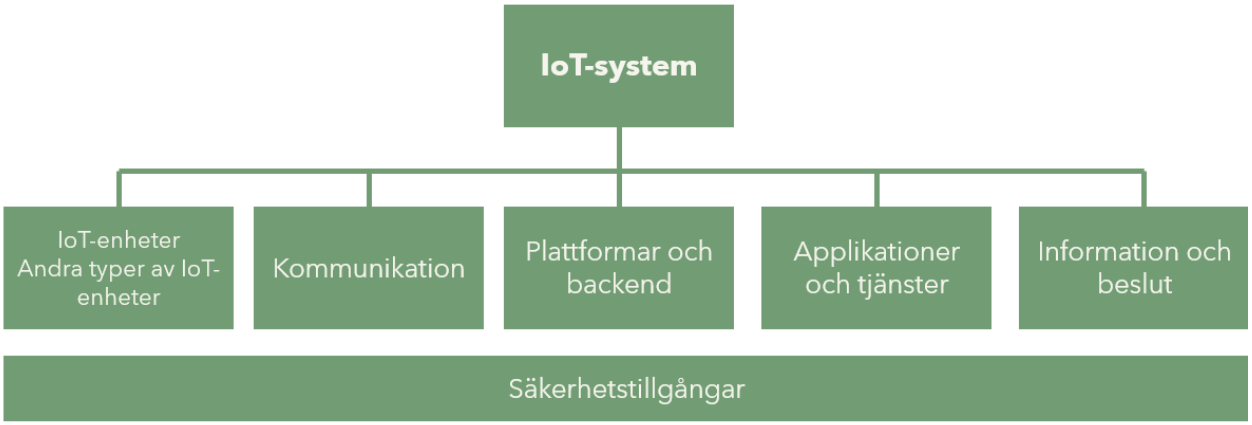


Bild Schematisk bild över komponenter i ett IoT- system

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, IoTenheter 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. Ett exempel kan vara identifiering av en persons identitet från en övervakningskamera.

- 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 eller system 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 autentiseringsmetod som kräver att användaren tillhandahåller två eller fler oberoende verifieringsfaktorer för att få tillgång till en resurs, till exempel en applikation eller ett konto:

- något användaren vet (ett lösenord)
- något användaren har (en säkerhetsbricka)
- något användaren har (mobilapp för generering av engångslösenord)
- något användaren är (biometrisk verifiering)

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 delmängdpaket, samlas för ytterligare analys.

Principen om minsta behörighet [principle of least privilege (POLP)]

En säkerhetsprincip som innebär att användare och system endast ska tilldelas de minsta nödvändiga behörigheterna och åtkomsträttigheterna för att utföra sina arbetsuppgifter eller åstadkomma sitt syfte.

Reverse engineering

Att arbeta baklänges från den färdiga produkten för att få insikter som gör det lättare att förstå hur den fungerar.

Rollbaserad åtkomstkontroll (role-based access control (RBAC)

En säkerhetsmodell där användare tilldelas behörigheter baserat på deras roll eller ansvarsområde inom en organisation.

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

Slumpmässigt genererad tillägg av data som läggs till vid hashning av lösenord för att öka säkerheten.

Sekretess
Gällande Offentlighets- och sekretesslagen (OSL) innehåller regler om myndigheters hantering av allmänna handlingar, tystnadsplikt för anställda på myndigheter och begränsningar i rätten att ta del av allmänna handlingar.

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

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

- Säkerhetsskydd handlar om att skydda information och verksamheter som är av betydelse för Sveriges säkerhet mot spionerі, sabotage, terroristbrott och vissa andra hot. Säkerhetsskydd handlar också om att skydda verksamhet som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd.

Denna vägledning tar inte upp dessa lagrum. Mer information om säkerhetskydd finns på säkerhetspolisens hemsida samt gällande lag och förordningar till Säkerhetsskyddslagen, Säkerhetsskyddsförordningen, Säkerhetspolisens föreskrifter om säkerhetsskydd samt Post- och telestyrelsens föreskrifter om säkerhetsskydd.

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, patchar m.m.
PaaS	platform as a service
PED	Physical Entity Domain

3. IoT Referensmodell och roller

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

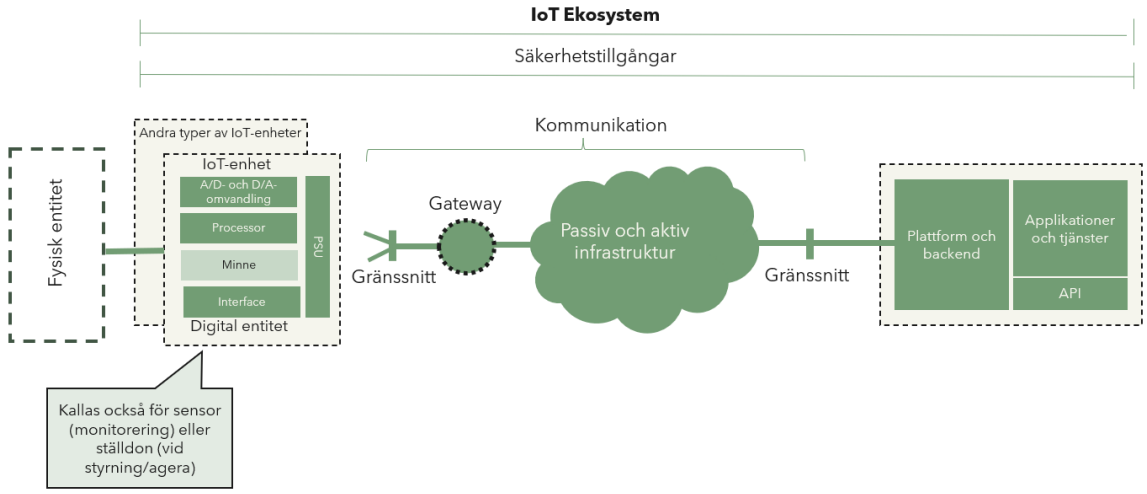


Bild Generisk Referensmodell för ett IoT-system.

Säkerhet inom IoT-systemet handlar om att ge enkel åtkomst till data för de i organisationen som behöver det för att göra sitt jobb bättre, men samtidigt skydda uppgifterna genom att förhindra tillgång till informationen av utomstående som inte ska se, ändra eller ta bort den. Det är viktigt att separera/segmentera verksamhetssystem IT från OT och IoT-systemet. I verksamhetssystem hanteras information och i OT-system hanteras funktion och data.

Ett tydligt gränssnitt definieras och kan också därför kontrolleras mellan IT- och OT/IoT-system. Gränssnittet kan vara en brandvägg, datadiod eller både och. Ett sätt att skapa dessa ”ö”-ar av säkerhetsdomäner är att använda sig av Purdue-modellen, *Se Bilaga 2 Purude-arbetsblock-säkerhetspåret Robust & säker IoT v2.0*.

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/actuator (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*
- *Fysiska åtkomstkontroller: Detta inkluderar säkerhetssystem såsom passerkort, biometriska läsare och säkerhetsvakter som reglerar åtkomsten till fysiska lokaler och resurser.*
- *Krypterad kommunikation*
- *Policyer och riktlinjer*
- *Säkerhetskopiering*

Roller för hantering av Säkerhetstillgångar

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

4. Kravanalys och riskhantering

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

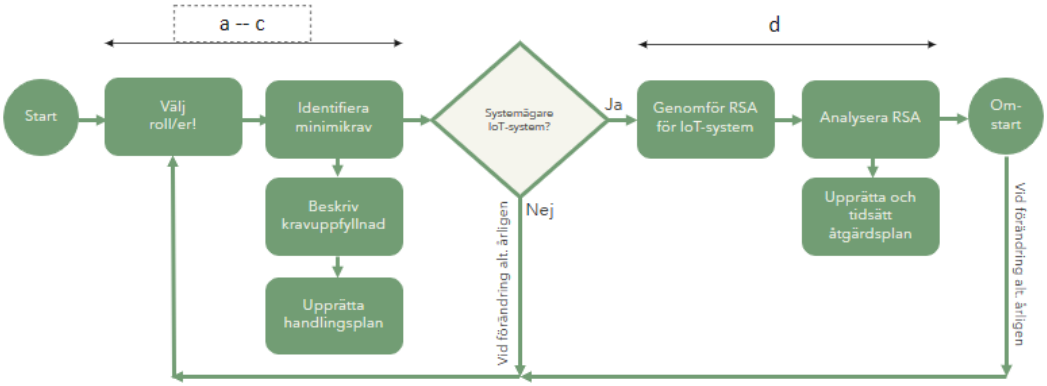


Bild Metod för kravanalys och riskhantering

Övergripande beskrivning av metoden steg för steg:

a) 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).

b) Minimikraven för den valda rollen analyseras i enlighet med *Bilaga 1. Rutin och handledning, Kravanalys 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*

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

d) Är den valda rollen Systemägare genomförs en riskanalys och riskbedömning i enlighet med kapitel 8.3 Hot, risk-och sårbarhetsanalys.

e) 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.

f) 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.

5. Säkerhetsområden och kategorisering

Notera:
För en komplett förteckning av säkerhetsområden, kategorisering samt specifika krav *Bilaga 1.1 Verktyg, Kravanalys Robust & Säker IoT v2.0*

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

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 ekosystem-relationer för IoT.

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 administrations-informationssystem.

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 drift-säkerhet.

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

Säkerhetskategorier 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 bäst praxis använts 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 (IoT)-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, riktighet och tillgänglighet av system och information som används av organisationsmedlemmar.

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 RDI Bilaga 1.1 Verktyg, Kravanalys Robust & Säker IoT v2.0* 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 (till exempel 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 *Bilaga 1.1 Verktyg, Kravanalys Robust & Säker IoT v2.0*. 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.

Notera:
För en komplett förteckning av säkerhetsområden, kategorisering samt specifika krav se *Bilaga 1.1 Verktyg, Kravanalys Robust & Säker IoT v2.0*

8. Hot och riskhantering

8.1 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.

8.2 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.

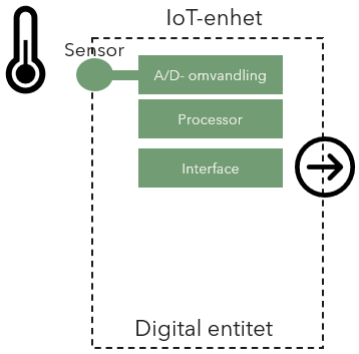


Bild: IoT-enhet för mätning av temperatur

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 IoTenhetens actuator.

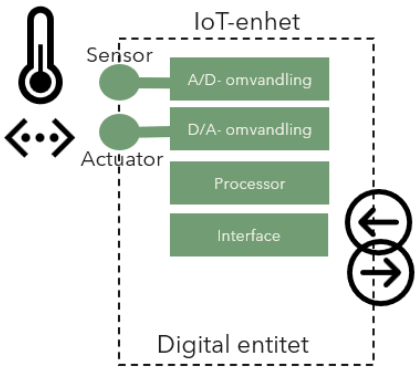


Bild: IoT-enhet inte autonom

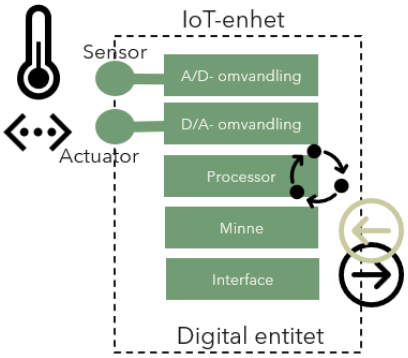


Bild: IoT-enhet autonom

Detta scenario höjer säkerhetskraven på IoT-enheter och andra komponenter i ekosystemet avsevärt. IoTenheterna 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 sp**rinklersystem 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. IoTenheter har en tendens att bli många och därför blir sårbarheten extra stor vid brister i säkerheten.

8.3 Hot, risk- och sårbarhetsanalys (RSA)

För identifiering av hot som påverkar IoT systemet och för genomförandet av en Risk- och sårbarhetsanalys hänvisas till Bashot Telekom som finns att hämta på https://www.ssnf.org/branschstod/robust-digital-infrastruktur/

Följande dokument ska användas:

- Instruktion för RSA inom telekom
- Presentation för RSA inom telekom
- RSA Robust och säker IoT

Metoden för RSA beskriver hur man systematiskt identifierar olika oönskade händelser, bedömer hur troligt det är att händelserna inträffar, bedömer de omedelbara negativa konsekvenserna, analyserar nät-och informationsbehandlingstillgångarnas sårbarheter samt bedömer förmågan att hantera olika påfrestningar.

Metoden bygger på kraven i ISO 27001-standarden och på underlag från MSB (Myndigheten för Samhällsskydd och Beredskap).

De olika stegen i en riskanalys omfattar följande steg:

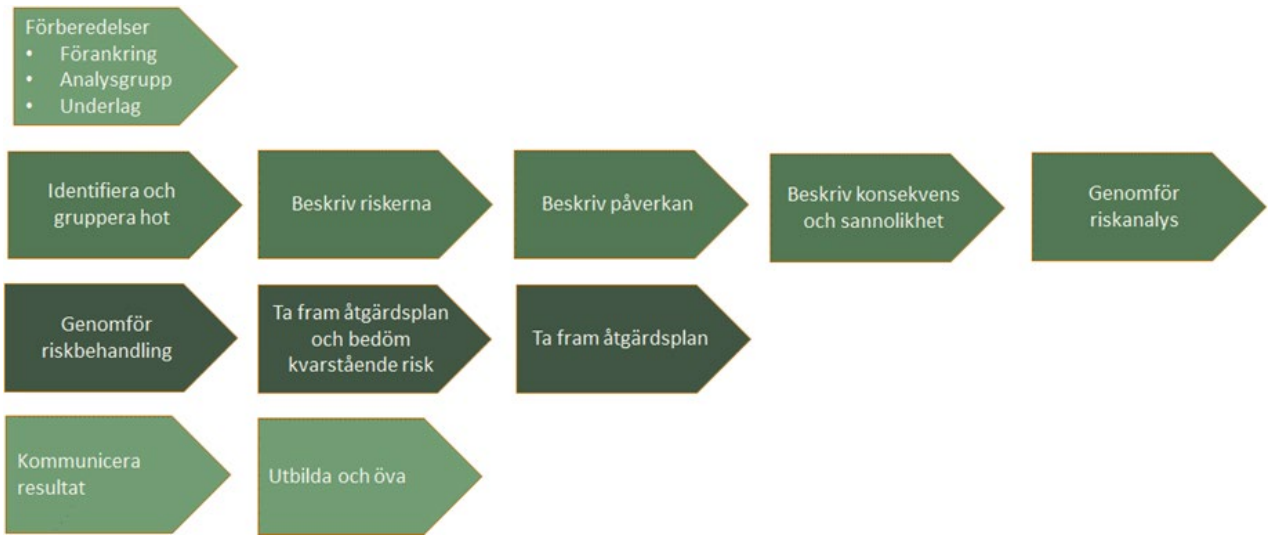


Bild: RSA-metoden

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.

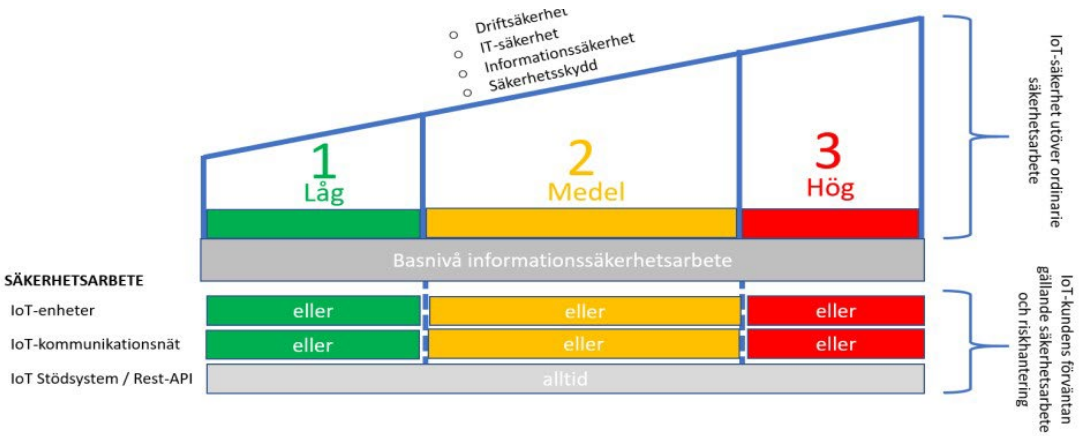


Bild: Riskskala IoT

9. Bilagor

Bilaga 1 Rutin och handledning, Kravanalys Robust & Säker IoT v2.0

Bilaga 1.1 Verktyg, Kravanalys Robust & Säker IoT v2.0

Bilaga 2 Purude-arbetsblock-säkerhetspåret Robust & säker IoT v2.0