Robust & Säker IoT

Bilaga 1
Rutin och handledning, Kravanalys Robust och Säker IoT

2020-03-01

Ver 1.0

INNEHÅLLSFÖRTECKNING

1. INLEDNING

Detta dokument utgör en rutin och en handledning för analys av minimikrav för Robust och Säker IoT.

2. REFERENSER

2.1 Referensdokument

Nedanstående referensdokument ska finnas tillgängligt innan arbetet med analysen genomförs.

Referens	Dokumentnummer, datum
Omvärldsanalys	
Dokumentation av samtliga tillgångar och kritiska komponenter	

2.2 Revisionshistorik

Utgåva	Datum	Handläggare	Beskrivning
Ver 1.	2020-02-03		Första utgåva

3. OMFATTNING OCH SYFTE

3.1 Omfattning

3.2 Syfte

Syftet med Kravanalysen är att IoT- aktörer ska kunna identifiera de minimikrav som är kopplade till aktörens roll inom ett IoT-system samt att fastställa erforderliga åtgärder för att hantera identifierade avvikelser.

4. AVGRÄNSNINGAR

Analysen i detta dokument avser inte:

- fysisk säkerhet
- drift- och förvaltningsorganisationens interna system och resurser.

5. ÅTERKOMMANDE KRAVANALYS

Minst en gång per år ska det göras en översyn och bedömning av om förändrade säkerhetshot påverkar säkerheten för komponenter/IoT- systemet och därmed behovet av en förnyade säkerhetsåtgärder. Översynen ska vara skriftlig. Det ska upprättas en löpande tidplan för återkommande säkerhetsåtgärder

Komponentansvarig eller systemägaren ansvarar för att översynen genomförs.

6. PLANERADE FÖRÄNDRINGAR

Det ska finnas en etablerad formell process för att hantera och dokumentera alla förslag till ändringar i verksamheten.
Inför planerade verksamhets- och/eller tekniska förändringar ska det göras en översyn och bedömning av om förändringarna påverkar säkerheten i IoT- systemet och därmed behovet av en förnyade säkerhetsåtgärder. Översynen ska vara skriftlig och finnas tillgänglig innan förändringen genomförs.

Utförande tekniker eller beställare ansvarar för att översynen genomförs.

7. SEKRETESS

Kravanalyserna ska säkerhetsklassats som ”Intern”. Intern innebär att informationen endast ska vara tillgänglig för dem som behöver informationen för att kunna fullfölja sina åtaganden rörande ägandeskap samt drift och förvaltning.

8. GENOMFÖRANDET AV KRAVANALYSEN

8.1 Allmänt

Kravanalysen ska användas för att säkerställa att Aktören i sin IoT-roll uppfyller minimikraven för IoT-säkerhet samt för att identifiera förbättringsåtgärder för att förbättra förmågan att hantera informationsrelaterade hot.

8.2 Förberedelser

För att resultaten av Kravanalysen ska bli bra och leda till korrekta åtgärder krävs förberedelser.

8.2.1 Analysgrupp

En analysledare ska utses som sedan leder den analysgrupp som sätts samman för att Kravanalysen.

Analysledaren bör ha vetskap om:

- Hur verksamheten fungerar på ett övergripande plan
- Hur och analysobjektet (komponent/system) fungerar på ett övergripande plan
- Hur metoden fungerar
- Vilka som bör ingå i analysgruppen
- Vilket underlag som behövs för analysen
- Vilket resultat som förväntas

Experter av olika slag kan behövas i gruppen, det kan exempelvis vara Komponent-/Systemägare och IT-säkerhetsexperter.

Storleken på analysgruppen kan variera men bör inte vara fler än åtta deltagare eftersom det kan vara svårt att hantera.

En dokumentationsansvarig bör utses och är den som håller i pennan eller IT-stödet, och som måste kunna metoden och de hjälpmedel som används vid analysen.

Inför en Kravanalys är det viktigt att ha tillgång till den information som behövs för att lösa uppgiften. Analysledarens uppgift är att se till att medlemmarna i analysgruppen har förberett sig för detta och har tagit reda på alla nödvändiga fakta.

Nödvändig information inför Kravanalysen är:

- Författningskrav, föreskrifter och andra styrande dokument som direkt kan påverka Kravanalysen.
- Statistik som underlättar analysgruppens bedömning
- Liknande kravanalyser som kan vara av värde för arbetet
- Allmänna hotbilder som kan vara till stöd och hjälp för att identifiera hot
- Dokument och dokumentation som beskriver aktuellt objekt.

8.2.2 Lokal och utrustning:

- Bra om det finns en skrivtavla och/eller blädderblock.
- Bra om det finns datorstöd och projektor.
- Välj gärna en lokal med bra miljö där ni kan arbeta ostört.
- Tryck upp eller skriv upp begrepp och definitioner synligt i lokalen.
- Tryck upp eller rita matrisen i en lämplig storlek.

8.2.3 Tidsplanering

Ta fram en realistisk tidsplan inför analysarbetet. Vissa delar kan visa sig ta längre tid än beräknat, men det är ändå viktigt att ha ett ”grundschema” att falla tillbaka på för att säkert bli klar i tid.
Avsätt tid för flera korta pauser men se till att deltagarna inte springer iväg och jobbar med annat under pauserna. Analysgruppens fokusering är helt avgörande för resultatet.

Tidsschema för en Kravanalysen kan vara mycket varierande beroende på Aktörens roll och omfattningen av objektet.

8.2.4 Roller och ansvarsområde

Klargör roller och ansvarområden för deltagarna.

8.2.5 Avgränsningar och perspektiv

Fastställ avgränsningar och ur vilket perspektiv Kravanalysen ska genomföras

8.2.6 Omfattningen av analysobjektet.

Beskriv omfattning och funktion hos analysobjektet.

8.4 Kravanalys

Säkerhetsarbetet i enlighet med vägledningen omfattar nedanstående steg:

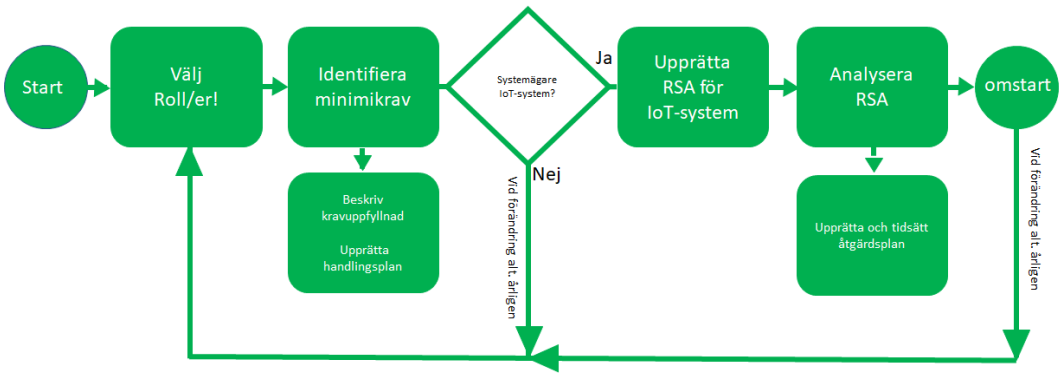

Bild Metod för kravanalys och riskhantering

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. Är den valda rollen Systemägare genomförs en riskanalys och riskbedömning i enlighet med *Bilaga 2. Rutin och handledning, RSA Robust &Säker IoT*.

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.

8.5 Sammanfattning och rapport

Resultatet tas om hand av analysledaren som sammanställer en slutgiltig rapport. Förutom själva analysresultatet är det viktigt att rapporten innehåller all tänkbar information, alla avsteg som gruppen har gjort från analysobjektet och eventuella nya definitioner. Rapporten kan också omfatta annan viktig information, till exempel styrdokument, produktbeskrivningar och ritningar som är värdefulla för resultatet.

Det är viktigt att skriva en bra och kortfattad sammanfattning som på ett enkelt sätt beskriver de avvikelser som analysgruppen funnit. Sammanställningen ska även innehålla eventuella förslag till åtgärder och rekommendationer till den som ska fatta besluten.

Den färdiga slutrapporten ska ut på "remiss" till deltagarna som skall ges möjlighet att ge sina synpunkter.