# Robust & Säker IoT

## Bilaga 2
## Rutin och handledning för Risk- och sårbarhetsanalys (RSA)

**2020-03-01**

**Ver 1.0**

# INNEHÅLLSFÖRTECKNING


**1. Inledning 3**

**2. Referenser 3**

2.1 Referensdokument 3

2.2 Revisionshistorik 3

**3. Omfattning och syfte 3**

3.1 Omfattning 3

3.2 Syfte 3

**4. Avgränsningar 3**

**5. Återkommande RSA 4**

**6. Planerade förändringar 4**

**7. Sekretess 4**

**8. Revidering och ansvar 4**

**9. Handledning risk- och sårbarhetsanalys 5**

9.1 Allmänt 5

9.2 Förberedelser 5

9.2.1 Analysgrupp 5

9.2.2 Lokal och utrustning: 6

9.2.3 Tidsplanering 6

9.3 Metod för RSA 6

9.3.1 Inför genomförandet 7

9.3.2 Metodens delar 7

9.4 Riskhantering och kontinuitetsplanering 11

9.4.1 Riskhantering 11

9.4.2 Kontinuitetsplanering 11

**10. Bilaga 2.1, Verktyget Risk- och sårbarhetsanalys 12**

# 1. INLEDNING

Detta dokument utgör en rutin och en handledning för Risk- och sårbarhetsanalyser (RSA) avseende IoT ekosystem

# 2. REFERENSER

## 2.1 Referensdokument

Nedanstående referensdokument ska upprättas innan arbetet med risk-och sårbarhetsanalyser genomförs.

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

## 2.2 Revisionshistorik

| Utgåva | Datum | Handläggare | Beskrivning |
|---|---|---|---|
| Ver 1. | 2020-02-05 | J Persson | Första utgåva |
| | | | |

# 3. OMFATTNING OCH SYFTE

## 3.1 Omfattning

Analyserna ska omfatta:

- Identifiering av samtliga relevanta hot mot det aktuella IoT ekosystemet.
- Kvalificerad bedömning av konsekvenserna i händelse av att identifierade risker inträffar
- Kvalificerad bedömning av sannolikheten för att identifierade risker inträffar.
- Kvalificerad sammanvägd bedömning av sannolikheten för att identifierade risker inträffar och de konsekvenser det kan medföra om de inträffar (riskbedömning).
- Åtgärdsförslag för hantering av identifierade risker

Vid genomförande av riskanalyser ska utförarna beakta erfarenheter från tidigare inträffade incidenter.

## 3.2 Syfte

Syftet med risk- och sårbarhetsanalyserna är att minska sårbarheten i verksamhetens IoT-system.

# 4. AVGRÄNSNINGAR

Risk- och sårbarhetsanalyserna i detta dokument avser inte:

- drift- och förvaltningsorganisationens interna system och resurser.

## 5. ÅTERKOMMANDE RSA

Minst en gång per år ska det göras en översyn och bedömning av och om förändringar i omvärld och/eller tekniska miljöer påverkar IoT-systemet och därmed behovet av förnyade risk- och sårbarhetsanalyser. Denna riskbedömning ska vara en avvägning mellan vad som kan inträffa, vilka konsekvenser detta kan få och hur troligt det är att det sker. Riskbedömningen ska vara skriftlig. Det ska upprättas en löpande tidplan för återkommande RSA.

## 6. PLANERADE FÖRÄNDRINGAR

Vid förändringar i verksamhetens IoT-systemet ska det genomföras en riskbedömning. Denna riskbedömning ska vara en avvägning mellan vad som kan inträffa vad gäller funktionell påverkan, vilka konsekvenser detta kan få och hur troligt det är att det sker.
Metoden för riskbedömningen är den samma som för återkommande RSA med tillägget att riskbedömningen ska vara skriftlig och finnas tillgänglig innan förändringen genomförs.
Utförande tekniker eller beställare ansvarar för att en riskbedömning genomförs.

## 7. SEKRETESS

Risk- och sårbarhetsanalyserna 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, drift och förvaltning av analyserade tillgångar och förbindelser.

## 8. REVIDERING OCH ANSVAR

Risk- och sårbarhetsanalysen revideras en gång per år eller då väsentliga förändringar gjorts i det elektroniska kommunikationsnätet och/eller de elektroniska tjänsterna. Systemägaren ansvarar för att detta görs.

# 9. HANDLEDNING RISK- OCH SÅRBARHETSANALYS

## 9.1 Allmänt

Risk- och sårbarhetsanalysen skall tydliggöra orsaker till och verkan av olika typer av händelser som kan påverka IoT-systemets funktionalitet negativt. Syftet är att ökad medvetenhet om de egna riskerna, sårbarheterna och förmågan att motstå dessa samt ge underlag för vilka eventuella förbättringsåtgärder som kan vidas för förbygga störningar och avbrott.

Riskanalyser kan göras i många olika situationer och på många olika nivåer. För en verksamhet som helhet, för en särskild informationstillgång, för en specifik applikation, för en serverhall, för en verksamhetsprocess och så vidare. Denna handledning fokuserar på IoT-systemet.

Det finns många olika metoder för att göra en riskanalys och det är till stor del ett hantverk som helt enkelt måste utföras av de personer som vet hur IoT-systemet är anlagd, hur drift och underhåll sköts samt har kunskaper om förvaltningen av IoT-system. Att ha goda kunskaper om omgivningarna och de risker som dessa kan utgöra för IoT-systemet funktionalitet är också viktigt när en riskanalys görs.

## 9.2 Förberedelser

För att resultaten av risk- och sårbarhetsanalyserna skall bli bra och leda till korrekta förebyggande åtgärder och förbättringsåtgärder krävs förberedelser.

### 9.2.1 Analysgrupp

En analysledare ska utses som sedan leder den analysgrupp som sätts samman för att genomföra risk och sårbarhetsanalysen.

Analysledaren bör ha vetskap om:

- Hur verksamheten och analysobjektet 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 exempelvis vara tekniker, säkerhetssamordnare, ekonomer och jurister.

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 riskanalys 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 risk- och sårbarhetsanalysen är:

- Författningskrav, föreskrifter och andra styrande dokument som direkt kan påverka riskanalysen
- Statistik som underlättar analysgruppens bedömning
- Liknande riskanalyser som kan vara av stort värde för arbetet
- Allmänna hotbilder som kan vara till stöd och hjälp för att identifiera hot
- Dokument och dokumentation som beskriver aktuella tillgångar och förbindelser.

### 9.2.2 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.

### 9.2.3 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.

Exempel på tidsschema för analysen:

- Inledning med presentation av deltagarna 5-10 minuter
- Genomgång och beskrivning av metoden 10-20 minuter
- Beskrivning av valt analysobjekt 10-30 minuter
- Genomgång av hotlista, lägg till, ta bort, beskriv 30-60 minuter
- Riskbedömning – konsekvens och sannolikhet 120-240 minuter
- Framtagning av åtgärdsförslag 30-60 minuter
- Sammanställning av rapport 60-240 minuter

Tidsschema för en RSA, kan vara mycket varierande beroende på objektet och analysgruppens ambitionsnivå.

## 9.3 Metod för RSA

Metoden som presenteras i det här dokumentet beskriver hur man systematiskt identifierar olika oönskade händelser, bedömer hur troligt det är att händelserna inträffar, bedömer de omedelbara negativa konsekvenserna, analyserar det elektroniska kommunikationsnätets och tjänsternas sårbarheter samt bedömer förmågan att hantera olika påfrestningar.
Metoden bygger på kraven i 27001-standarden och på underlag från MSB (Myndigheten för Samhällsskydd och Beredskap).

### 9.3.1 Inför genomförandet

Erfarenheterna visar att metodiken inte är det svåra med en analys, utan administrationen. Därför är det väldigt viktigt att följa upp att deltagarna är förberedda och har satt av tid för analysen.

Innan genomförandet av risk- och sårbarhetsanalyser måste man också fastställa vissa utgångspunkter som skall ligga till grund för det fortsatta analysarbetet. Sammanfattningsvis bör risk- och sårbarhetsanalysens utgångspunkter klargöra:

**Roll och ansvarsområde**

Systemägaren och förvaltningsansvariga för analysobjekten samt, beroende av analysobjekt, experter som tekniker, säkerhetssamordnare, ekonomer och jurister.

**Avgränsningar och perspektiv**

Det är även viktigt att förstå begreppen risk och sårbarhet för att kunna sätta korrekta avgränsningar och utgå från ett korrekt perspektiv. Följande definitioner används i Risk-och Sårbarhetsanalysen. Risk = Osäkerhetens effekt på mål
Riskanalys = Process för att förstå riskens natur och för att avgöra risknivån.
Sårbarhet = Kritiskt beroende av en tillgång eller brist i skyddet av en tillgång exponerad för hot.
Resulterande sårbarhet = Sårbarheter som återstår efter införande av skyddsåtgärder

### 9.3.2 Metodens delar

När analysgruppen är samlad genomförs analysen med hjälp av följande steg som beskrivs mer utförligt under respektive punkt samt i kapitel 9.4.

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

#### *9.3.2.1 Välj och beskriv analysobjekt*

Det första steget i arbetet med en risk- och sårbarhetsanalys är att välja och beskriva objektet för analysen, beskrivningen skall vara kortfattad men tydlig nog för andra att förstå utanför analysgruppen.

Aktuella objekt utgörs av definierade tillgångar och förbindelser för IoT-systemet.

#### *9.3.2.2 Identifiera hot*

Ett viktigt moment är att identifiera de hot som finns mot analysobjekten. På ENISA finns det en översikt av hot som baserar sig på ENISA Baseline Security Recommendations for IoT Tabellen är en god utgångspunkt för det vidare arbetet och har med de allra flesta hot som är relevanta också för ett IoT ekoinfrastruktur.

Utifrån IoT-systemets omfattning görs ett urval av vilka hot som kan anses relevanta och dessa ska sedan till ligga grund för risk- och sårbarhetsanalyserna. Urvalet av bashot bör göras för varje nytt analysobjekt. Se figur 1 *Tabell bashot* nedan.

Vill man själv indentifiera hoten kan man använda sig av "brainstorming" där varje deltagare på en lapp skriver ner hot som kan inträffa eller saker som redan har hänt. Alla hot samlas sedan in och gås igenom.

Det är viktigt att deltagarna försöker beskriva hoten så att alla förstår. Det blir då lättare att bedöma risken i kommande steg. Alla måste förstå och vara överens om innebörden i hoten.

När man arbetar med identifiering av hot bör man tänka på följande:

- Lyssna extra noga på de personer som arbetar aktivt med den berörda verksamheten.
- Vad har hänt som kan hända igen?
- Fokusera på hoten – undvik att tänka i lösningar!
- Undvik för långa diskussioner om det befintliga skyddet.
- Låt alla komma till tals.
- Experter måste tänka på att tala så att alla förstår.

***Gruppering av hot***

Med hjälp av analysledaren ska gruppen försöka beskriva hoten på ett strukturerat sätt. Målet är att gruppera liknande hot med varandra, ta bort dubbletter och förtydliga vissa hot om det behövs.

***Figur 1**. Tabell över bashot.*

| Bashot som baserar sig på ENISAs framtagna hotbild för IoT ekosystem | |
|---|---|
| **Grupp** | **Hot** |
| **Nefarious activity / abuse** | IoT communication protocol hijacking |
| | DDoS |
| | Attacks on privacy |
| | Modification of information |
| | Network reconnaissance |
| | Replay of messages |
| | Malware |
| | Exploit Kits |
| | Targeted attacks |
| | Counterfeit by malicious devices |
| | Man, in the middle |
| | Interception of information |
| | Session hijacking |
| | Information gathering |
| **Failures / Malfunctions** | Third parties failures |
| **Damage / Loss (IT Assets)** | Software vulnerabilities |
| | Data / Sensitive information leakage |
| **Disaster** | Natural Disaster |
| | Environmental Disaster |
| **Physical attacks** | Device destruction (sabotage ) |
| | Device modification |
| **Outages** | Loss of support services |
| | Failure of system |
| | Network Outage |
| | Failures of devices |
| | Nytt hot här! |

### *9.3.2.3 Klassificeringsmodell*

För att kunna bedöma risken med ett hot görs en sammanvägning av konsekvensen av att hotet inträffar och en bedömning av sannolikheten för att hotet inträffar. För att göra detta krävs att kriterierna för konsekvenser och sannolikhet definieras och beskrivs så att alla i analysgruppen förstår och är överens om innebörden.

Sannolikheten anger hur troligt det är att hotet kommer att inträffa enligt följande kategorier med exempel på definitioner av kriterierna:

- **Mycket låg**
  *Händelsen förväntas inte inträffa under den närmaste 20 åren alternativ En gång på 20 år eller obefintlig sannolikhet att händelsen inträffar över huvud taget.*

- **Låg**
  *Händelsen förvänts inte inträffa under närmaste 10 åren alternativt En gång på 10 år eller mycket sällan.*

- **Medel**
  *Händelsen kan inträffa alternativt En gång på 5 år eller sällan.*

- **Hög**
  *Händelsen kommer med stor sannolikhet att inträffa alternativt årligen eller regelbundet,*

- **Mycket hög**
  *Händelsen kommer nästan säkert att inträffa alternativt Mer än en gång per år eller ofta.*

Konsekvensen är ett mått på hur mycket verksamheten skadas om hotet blir verklighet. Påverkan kan exempelvis vara direkt eller indirekt, ekonomisk eller medmänsklig. Modellen innehåller följande fem nivåer med exempel på definitioner av kriterierna:

- **Mycket låg**
  *Om händelsen inträffar är det osannolikt att händelsen får negativa konsekvenser eller försumbar skada.*

- **Låg**
  *Om händelsen inträffar är det möjligt att händelsen får negativa konsekvenser eller måttlig skada.*

- **Medel**
  *Om händelsen inträffar är det närmast säkert att händelsen får negativa enklare konsekvenser och kan vara en måttlig skada.*

- **Hög**
  *Om händelsen inträffar är det sannolikt att händelsen får negativa konsekvenser kan vara en betydande skada.*

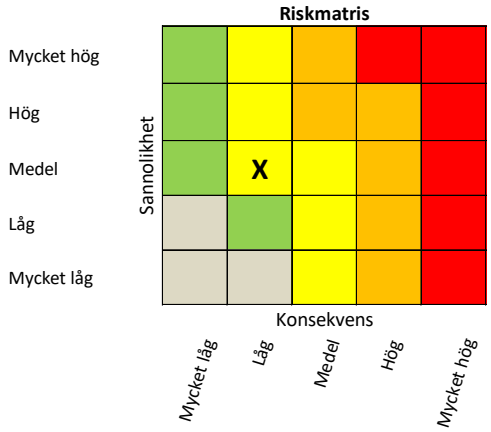
- **Mycket hög**
  *Om händelsen inträffar är det närmast säkert att händelsen får negativa konsekvenser kan vara en allvarlig skada.*

Definitionerna av konsekvens och sannolikhet är ett riktmärke och kan förändras, och det är viktigt att gruppen går igenom definitionerna och ändrar om det behövs. Eventuella förändringar ska dokumenteras och tas med i slutrapporten.

#### *9.3.2.4 Riskanalys*

När alla kriterier för sannolikheter och konsekvenser är bestämda ska analysgruppen bedöma risken (konsekvensen och sannolikheten) för ett hot, t.ex genom att använda en Konsekvens- och sannolikhetsmatris (fig 2) där man med färger indikerar allvarlighetsgraden av att ett hot inträffar, från grönt (acceptabel risk till röd (måste åtgärdas). Matrisens resultat kan senare att ligga till grund för bland annat prioriteringen av olika åtgärder.

**Figur 2**. Konsekvens- och sannolikhetsmatris



#### *9.3.2.5 Sammanställning och rapport*

Resultatet tas sedan 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 risker 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.

## 9.4 Riskhantering och kontinuitetsplanering

### 9.4.1 Riskhantering

Med riskanalysen som utgångspunkt görs en bedömning om risken ska begränsas med skyddsåtgärder eller om den ska accepteras och hanteras i kontinuitetsplanen. Förslag på åtgärder ska dokumenteras i ett dokument, ***Åtgärdsplan riskanalys,*** där en riskansvarig anges samt om möjligt en uppskattad kostnad för respektive åtgärd.

Det finns två sätt att arbeta med åtgärderna.

**Alternativ 1: Riskerna ska hanteras senare**

Ett alternativ är att riskerna inte ska mötas med några åtgärder ännu utan man förbereder sig endast genom att dokumentera på vilket sätt hotet ska hanteras om det skulle inträffa, det vill säga en kontinuitetsplanering, se avsnitt 9.4.2. Men om deltagarna har bra förslag på åtgärder kan man ändå dokumentera dem.

**Alternativ 2: Riskerna ska hanteras nu**

Det andra alternativet går ut på att ta hand om riskerna på en gång. Den framtagna matrisen visar vilka hot som är allvarligast – de med högst sannolikhet och störst konsekvenser. Med den informationen som utgångspunkt är det sedan dags att diskutera eventuella åtgärdsförslag och prioritetsordningen för dem. Analysgruppen tar fram ett förslag på lämpliga åtgärder och anger i vilken ordning de bör hanteras.

Beslut om genomförande av åtgärd bör föregås av en riskhanteringsprocess, d.v.s. att bedöma på vilket sätt identifierade risker skall hanteras i verksamheten.

Först efter att en bedömning av kostnaden för genomförande av åtgärder har vägts mot kostnaden för att hantera ett inträffat hot bör beslut tas.

### 9.4.2 Kontinuitetsplanering

Om beslut fattas om att inte vidta åtgärder skall en kontinuitetsplan upprättas för minimera effekterna om hotet skulle inträffa.

# 10. BILAGA 2.1, VERKTYGET RISK- OCH SÅRBARHETSANALYS

Detta avsnitt beskriver handhavandet av ett verktyg för risk- och sårbarhetsanalys (Bilaga 2.1 Verktyg RSA-mall Robust & Säker IoT) som kan användas för att dokumentera analysarbetet samt för stöd under genomförandet. Nedan följer en handledning i användandet av verktyget.

### Arbetsgång

#### *Analysobjekt*

Starta med att identifiera och prioritera de objekt som ska analyseras.

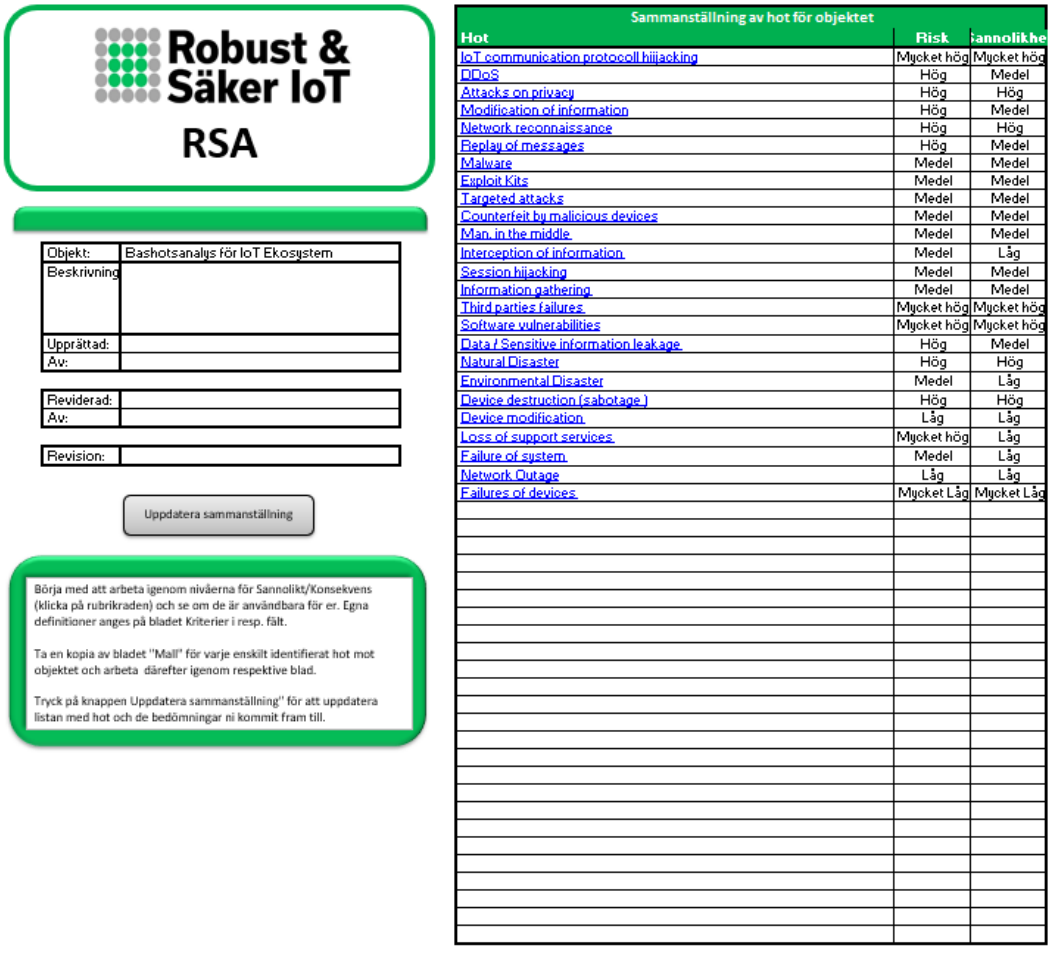
#### *Arbetsdokument*

Gör en kopia av Bilaga 2.1, *Verktyg RSA* för varje objekt som ska analyseras.

#### *Fliken Sammanställning*

Under fliken Sammanställning ska valt objekt beskrivas, det ska också framgå när den är upprättad och vem som har upprättat den.  Det finns också fält för revideringsdatum, vem som reviderat dokumentet samt ett revisionsnummer.

**Figur 3**. Fliken sammanställning



***Fliken Kriterier***

Se över kriterierna under fliken ”Kriterier” och kontrollera att de är relevanta. Uppdatera vid behov. Under arbetes gång kan definitionerna för kriterierna hämtas genom att dubbelklicka på Konsekvens eller sannolikhet i riskmatrisen.

***Fliken Bashot***

I verktyget är varje hot listad i fliken ”Bashot”. För varje sådant bashot är det sedan upplagt en separat flik som hanteras i enlighet med rubriken ***Analysera hot*** nedan.

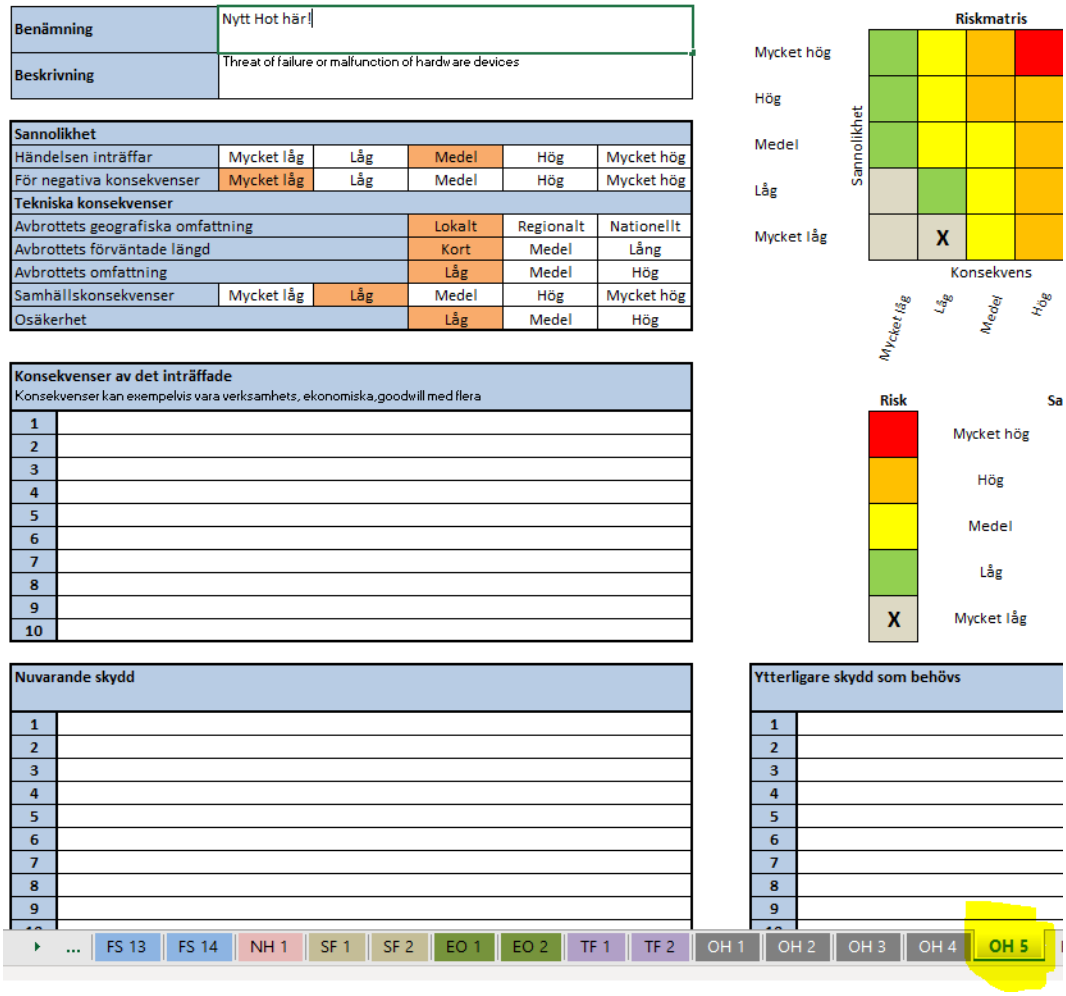
Gå igenom och ta bort de hot/flikar som inte är relevanta för analysen, dokumentera ändringar och tillägg under fliken ”Bashot” och gå därefter till fliken ”Sammanställning” klicka på knappen **Uppdatera sammanställning** varvid kolumnen *Sammanställning av hot för objekten* uppdateras.

För att skapa ett nytt bashot så lägger du till en rad (Figur 4) med hjälp av ”Infoga” i Excel, Ex. FK 6.

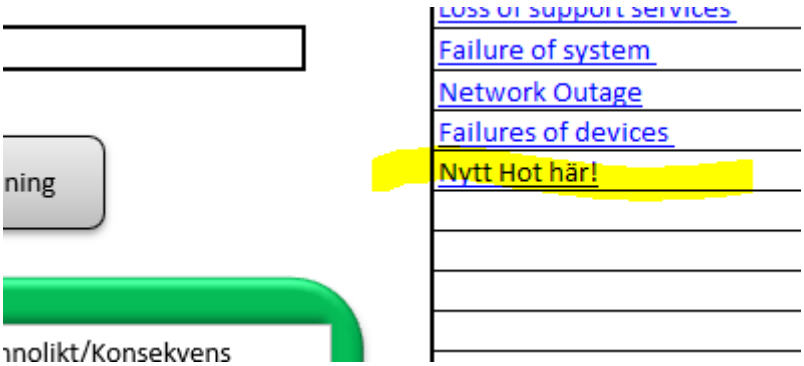
**Figur 4**. Infoga nytt bashot under fliken ”Bashot”


Därefter skapar du en ny flik (Figur 5) med samma namn, ex FK 6 och skriver samma Benämning på hotet som du skrev under fliken ”Bashot”. Du kan med fördel kopiera en befintlig flik. Gå sedan till fliken ”Sammanställning” (Figur 6) och tryck på knappen **Uppdatera sammanställning** och det nya bashotet läggs upp i kolumnen *Sammanställning av hot för objekten.*

**Figur 5**. Ny flik, ex OH 5, Benämning och Fliknamn.




**Figur 6**. Nytt bashot visas i listan

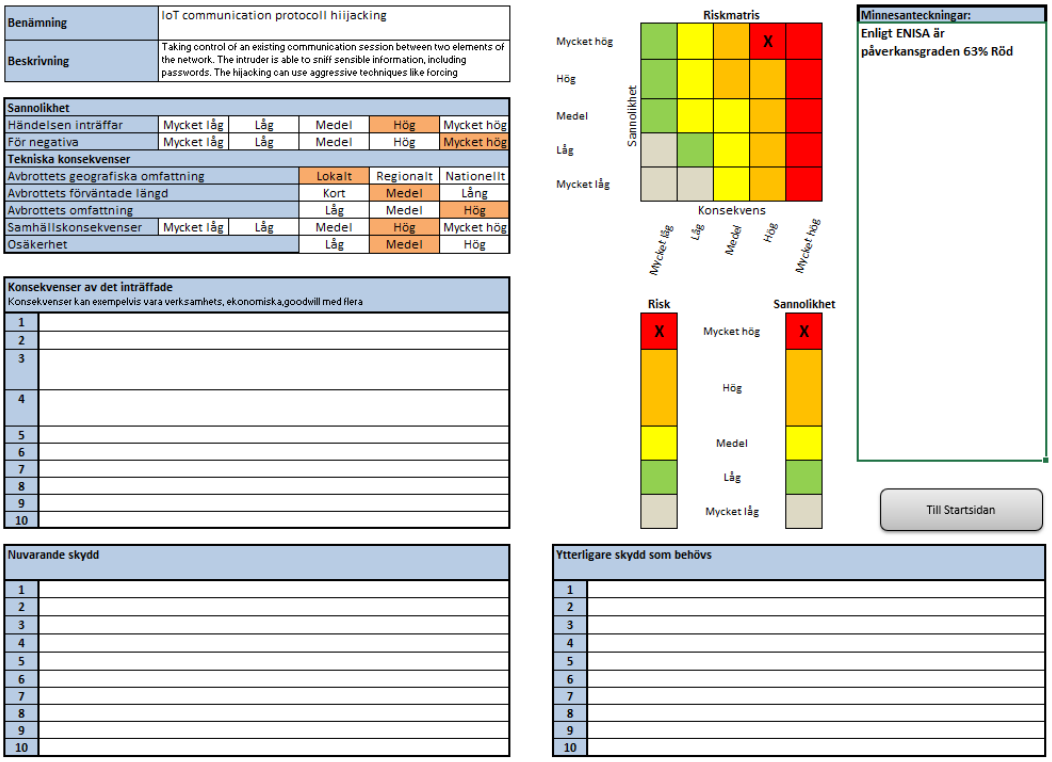


### *Analysera hot*

Benämning och beskrivning av hotet skrivs in (Figur 7).
Tabellen med sannolikhet och konsekvenser fylls i och i Riskmatrisen kommer ett kryss att automatiskt placeras på rätt plats i matrisen och ge en vägledning till hur låg eller hög risken är.

Sammanfattning av hotet får du genom att titta på Risk och Sannolikhetstaplarna under Riskmatrisen.
Ju mer samhällskonsekvens hotet har desto större risk. Allt utom grönt kräver en åtgärd direkt (röd) eller senare (orange eller gul), detsamma gäller vid Sannolikhet röd, orange, gul eller grön.

**Figur 7**. Fliken hot




I tabellen *Konsekvenser av det inträffade* dokumenteras konsekvenserna av att ett hot inträffar.

I tabellerna *Nuvarande skydd* och *Ytterligare skydd* anges nuvarande skydd och om det behövs ytterligare skydd för att hantera risken. Anteckningarna i tabellen *Ytterligare skydd* kommer att utgöra underlaget för åtgärder som sammanställs automatiskt i en lista under fliken **Åtgärdslista**. Även anteckningarna i tabellen *Nuvarande skydd* sammanställs automatiskt under fliken **Nuvarande skydd**.

I fältet för minnesanteckningar kan det noteras viktiga saker kring bedömningarna t.ex. hur man kommit fram till bedömningen för sannolikheten.

När analysen är klar klicka på knappen **Till Startsidan** och klicka där på knappen **Uppdatera sammanställning** varvid kolumnerna *Risk* och *Sannolikhet* uppdateras.

**Riskhantering och kontinuitetsplanering**
Efter analysen använd underlaget för fortsatt riskhantering i enlighet med *kapitel 9.4, Riskhantering och kontinuitetsplanering.*