**Från:** Ryd Erik
**Skickat:** den 22 juli 2019 16:25
**Till:** 'Hagelstedt Viktoria'; Käll Tim
**Kopia:** Ericson Linda
**Ämne:** Kommentarer på slutrapport Uppdrag om säkert och effektivt informationsutbyte

Hej,

Jag har nu gått igenom *Slutrapport – Uppdrag om säkert och effektivt informationsutbyte v20190620*. Tyvärr verkar flera kommentarer och frågor som vi tidigare lämnat till projektet lämnats obearbetade eller obesvarade. Nedan listar jag de synpunkter som fortfarande är relevanta.

## Kapitlet *Förslag till åtgärder*

Förslagen i kapitlet redogör inte tillräckligt för en ändamålsenlig hantering av säkerhets- och informationssäkerhetsfrågor. Om denna rapport, så som den nu är skriven, resulterar i en serie åtgärder och nya uppdrag krävs att säkerhetsaspekterna blir genomarbetade ytterligare. Se ytterligare kommentarer under ”Säkerhet och informationssäkerhet” nedan. En utmaning vid utveckling av effektivt och säkert informationsutbyte är inte endast att balansera ”standardisering, likriktning, styrning mot flexibilitet, innovation och frivillighet” (sidan 43-44). Parameterns säkerhet behöver också vägas in – något som ofta kan vara svårt men nog så viktigt.

På sidan 18 anges byggblocket Tillitsregelverk som ett prioriterat byggblock, men det finns inte med som en första åtgärd i kapitlet *Förslag till åtgärder*. Ska det inte omhändertas i ett första skede efter att slutrapporten lämnas in? Nuvarande skrivningar verkar reflektera en ambivalent hållning till hur prioriteringen av byggblocket ser ut.

I nuläget saknas ett byggblock motsvarande ”Säker informationsöverföring”. Byggblocket borde på en minimumnivå ta upp hur bibehållen konfidentialitet och riktighet vid informationsöverföring ska säkras. Vilka krypteringslösningar kan vara aktuella? Även tillgänglighet i form av driftsäkerhet borde tas upp i detta sammanhang.

#### Byggblocket Auktorisation

På vilket sätt är detta en egen kategori/byggblock om ni i byggblock Tillitsregelverk pratar om en federationslösning?

Överväg att byta ut ”auktorisation” mot ”behörighetskontroll”.

#### Byggblocket Tillitsregelverk

Enligt förklaringen av byggblocket på sidan 98 står det att ”MSB ses som den naturliga aktören att hantera Tillitsregelverket som sätter ramarna för övrig koordinering”. Vi har, baserat på det som hittills kommunicerats om detta byggblock, inte kunnat ta ställning till regelverket och vår eventuella roll i framtagandet av det.

Det vore bra med en tydligare redogörelse för hur tilliten ska skapas. Hur ska man arbeta med transparens, tillsyn, revision, kontroll, rättelse, uppdatering osv? Hur ska efterlevnad av tillitsramverket kontrolleras på central och lokal nivå? Kommer det finnas en eller flera myndigheter med ett tillsynsansvar eller ska kontroll ske genom en ackrediteringsprocess? Det krävs sannolikt någon form av uppföljning för att säkerställa efterlevnad.

#### Byggblock Tillgänglighet

Byggblocket är mycket kortfattat beskrivet och verkar kräva ytterligare genomarbetning. Tillgänglighet i form av driftsäkerhet och robusthet kan bli viktigt för delar av samhällets funktionalitet beroende på omfattningen av lösningen för elektroniskt informationsutbyte. Enligt uppdraget ska myndigheterna bl.a. beakta de krav som ställs för att värna Sveriges säkerhet och behovet av ett systematiskt informationssäkerhetsarbete. Hur har dessa krav beaktats när byggblocket tillgänglighet tagits fram?

**Byggblock Spårbarhet**
Inom professionen kallas det som beskrivs här för "säkerhetsloggning".

## Kapitlet *Konsekvenser*

Kapitlet har helt utelämnat eventuella konsekvenser (positiva och negativa) för systematisk informationssäkerhet, samhällssäkerhet och beredskap. Det saknas helt en konsekvensanalys gällande informationssäkerhetsområdet. Informationssäkerheten är ett mycket viktigt område att bedöma i och med att så stora informationsmängder föreslås bli nåbara för en större mängd aktörer. Vad (riskerar) konsekvenserna bli för statens systematiska informationssäkerhetsarbete och Sveriges säkerhet? Vad är riskerna med att säkerhet nedprioriteras och/eller inte ges tillräckligt utrymme i det fortsatta arbetet med de föreslagna åtgärderna i slutrapporten? Hur (o)säkert kan Sveriges framtida informationsutbyte inom centrala delar av offentlig sektor bli till följd av brister i de föreslagna byggblocken?

Det går att hålla övergripande resonemang om eventuella konsekvenser av en ny central arkitektur för informationsutbyte, även i ett tidigt stadium. Om ett fjärrangrepp lyckas tack vare att skyddet mot intrång, manipulation och stöld brister, eller om driften störs till följd av undermålig robusthet och kontinuitetsplanering, riskerar kanske följande att hända:
(1) Allmänheten, näringsliv och andra aktörer tappar tilltro till statens förmåga att digitalisera samhället på ett säkert och ändamålsenligt sätt.
(2) Framtida investeringar och utvecklingsarbete för digitaliseringen av offentlig sektor kan bli svårare att få acceptans och förtroende för.
(3) Detta tillsammans med att incidenter inträffar, möjliggjorda av undermåligt säkerhetsarbete, skulle kunna skada samhällets eller den enskildes säkerhet.

## Säkerhet och informationssäkerhet (kommentarer på rapportens alla delar)

Det krävs en fördjupad och systematisk genomarbetning av (informations)säkerhetsaspekterna i rapportens behovsanalys, omvärldsanalys, förslag tillgemensamma lösningar, åtgärder och konsekvenser av dessa. Säkerhetsaspekter, så som krav som ställs för att värna Sveriges säkerhet och behovet av ett systematiskt informationssäkerhetsarbete, är inte tillräckligt redogjorda för i rapporten – trots att uppdraget handlar om säkert och effektivt elektroniskt informationsutbyte.

Rapporten skulle bli både tydligare och i mindre grad missa viktiga aspekter i de olika kapitlen om den följde ett mer konsekvent användande av terminologin från informationssäkerhetsområdet. Som det är nu utelämnas någon eller några av aspekterna tillgänglighet, konfidentialitet eller riktighet i flera stycken där de är relevanta att lyfta och hantera. Dessutom nämner rapporten inte en enda gång att informationssäkerhetsarbetet ska vara riskbaserat. Detta är ett krav som åligger alla svarande myndigheter i detta uppdrag enligt 5§ MSBFS 2016:1.

Sidan 6: Behovsanalysen har deltas upp i kategorierna ”Informationshantering” och Tillit och säkerhet”. Detta blir en märklig uppdelning. Så som informationshantering beskrivs (riktighet) borde det hamna under tillit och säkerhet. Informationshantering bör snarare handla om behovet att kunna lita på att varje aktör har förmåga att hantera informationen på sådant sätt att informationsutbyte möjliggörs.

Sidan 10, ur rapporten: ”[…] klassning av information utifrån bland annat regler om dataskydd (sekretess, integritet och säkerhet).”
Avser ni endast dataskydd i meningen skydd av personuppgifter? Vad innebär sekretess, integritet och säkerhet – och hur förhåller de sig till varandra? Vore det inte bättre att på en övergripande utgå ifrån de krav som statliga myndigheter har på sig att arbeta systematiskt med informationssäkerhet enligt MSBFS 2016:1? I så fall är det bättre att skriva ut att information ska klassas efter de krav som finns om tillgänglighet, riktighet och konfidentialitet.

Sidan 12, ur rapporten: ”Lösningarna ska vara förenliga med gällande rätt, t.ex. regleringen om behandling av personuppgifter, offentlighetsprincipen samt att beakta säkerhetsaspekterna.”
Omformulera sista delen till "... offentlighetsprincipen samt att beakta informationssäkerhetsaspekterna."

Sidan 34: Avsnittet *4.2.2.3 Rättsliga utgångpunkter för utlämnande av information* behöver breddas. Regelverken som pekas ut här rör inte bara *utlämnandet* av information utan också hur informationen ska *hanteras*. De olika förordningarna ställer krav som påverkar hur organisationer ska hantera

Sidan 26-33, avsnittet Gällande rätt: Enligt uppdraget ska krav som ställs för att värna Sveriges säkerhet beaktas – men i nuläget nämns bara denna lagstiftning i förbifarten. Har behov, förslag på lösningar och konsekvenser av dessa analyserats utefter det krav som ställs i lagstiftningen?

Sidan 53: Vad avses med ”stabsmyndighet”? Statskontoret och ESV? Eller menar ni bevakningsansvariga myndigheter med en s.k. TiB-funktion enligt förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap?

Sidan 59: Det kan vara bra att nämna att SGSI endast erbjuds till myndigheter.

Sidan 89, ur rapporten: ”Det är viktigt att information klassas för att klargöra vilket skyddsvärde den har […]”
Överväg att byta ut *skyddsvärde* mot *skyddsbehov*.

Sidan 90, ur rapporten: ”Säkerhetsgruppen har identifierat en rad olika viktiga komponenter/byggblock som är avgörande för ett säkert och effektivt informationsutbyte men det ska påtalas att det inte är en komplett analys utan detta arbete behöver bedrivas vidare i det fortsatta arbetet.”
Vilka är de hittills identifierade viktiga komponenterna/byggblocken? Hur ska de involverade myndigheterna säkerställa att säkerhetsarbetet bedrivs i tillräcklig utsträckning parallellt med eller inom kommande projekt?

Bilaga 1, avsnitt 1.4.5: Avsnittet fokuserar i nuläget alltför ensidigt på antagonistiska hot, ni bör ha ett bredare allriskperspektiv. Vikten och betydelsen av tillgänglighet och driftsäkerhet ges nästintill inget utrymme i slutrapportens nuvarande version. Det är rimligt att anta att de lösningar som nu kommer på plats på sikta kan vara av central betydelse för delar av Sveriges offentliga sektors funktion dag till dag, och dess förmåga till informationsutbyte med övriga delar av samhället. Hur säkerställer de involverade myndigheterna att några nya lösningar inte kommer på plats där tillräcklig robusthet och säkerhet saknas?

Hör av er vid ytterligare frågor eller funderingar kring detta. Ha en fortsatt trevlig sommar!

Med vänlig hälsning

Erik Ryd
Analytiker

Myndigheten för samhällsskydd och beredskap
Avdelning för cybersäkerhet och säker kommunikation
Enheten för strategi och samordning
651 81 Karlstad
Tel växel 010-240 240
Tel direkt 010-240 4386
E-post erik.ryd@msb.se

www.msb.se