Dokumentklass:	Öppen
Datum:	2015-06-12
Version:	1.0

Fördjupad analys:

Swedish Government Secure Intranet (SGSI) för robust kommunikation

Representanter från kommuner

SOES ska verka för att enskilda individer, företag och det allmänna ska ha tillgång till och förtroende för att:

- samhällets betalningar* fungerar och
- systemen för att betala varor och tjänster fungerar

Syftet är att förebygga allvarliga störningar för att minska konsekvenser av händelser som kan få allvarliga samhällspåverkande effekter.

Detta sker genom att ur ett samhällsperspektiv analysera risk och sårbarhet för kritiska resurser samt beroenden, dokumentera dessa, ta fram förslag för åtgärder, och tillställa ansvariga aktörer.

* *Med samhällets betalningar menas hela kedjan från generering av underlag för utbetalning till att mottagaren kan använda medlen. I målet ingår delar som de olika aktörerna inte har ett direkt ansvar för, men där avbrott påverkar mottagaren menligt. Exempel på detta är aktörer inom finansiella sektorn, för dessa gäller att SOES analyserar och informerar om risker.*

Sammanfattning

I takt med att teknikberoendet ökar i samhället, ökar beroenden till säker kommunikation även mellan myndigheter. System som stödjer information och kommunikation blir därmed alltmer kritiska resurser, vilket även gäller SOES-myndigheter. Under 2014 utvecklade Arbetsgrupp Riskanalyser inom Samverkansområdet ekonomisk säkerhet (SOES) rapporten ”Riskanalys för myndigheterna inom SOES”. Under 2015 genomför SOES en fördjupning av ett antal utvalda risker, varav denna rapport utgår från risken ”internetstörningar”. Ett förslag från 2014 var att beskriva Swedish Government Secure Intranet (SGSI) för SOES-myndigheterna samt undersöka hur SGSI kan öka robustheten i myndigheternas kommunikation och därigenom reducera risken för internetstörningar.

SGSI är ett avgiftsfinansierat nätverk för säker kommunikation mellan myndigheter i Sverige och i Europa. Denna rapport innehåller en övergripande beskrivning av vad SGSI är hur det kan bidra till mer robust kommunikation för SOES-myndigheterna, men inkluderar även några utmaningar från myndigheternas perspektiv. Dessutom beskrivs i denna rapport några internationella motsvarigheter till SGSI.

Styrkorna i SGSI ligger möjligheten till säker kommunikation, i termer av tillgänglighet, tillförlitlighet och konfidentialitet, vilket ges bl.a. genom separering från internet, dubblerad teknisk utrustning och krav på certifikat. Ytterligare säkerhet och robusthet ges även av särskilda krav som ställs på myndigheter som ansluts. En möjlig utmaning kring systemet, utifrån SOES perspektiv, är huruvida kommunikation med ramavtalsbanker vore möjligt via SGSI i framtiden, då anslutning till SGSI förutsätter en särskild prövning och då SGSI huvudsakligen är till för myndigheter. Baserat på denna studie har även ett antal åtgärder föreslagits:

- SOES föreslås genomföra en studie av hur anslutna SOES myndigheter använder SGSI och vilka styrkor och utmaningar som kunnat konstateras vid användningen. Denna studie föreslås även identifiera eventuella kommunikationsbehov hos SOES-myndigheterna som inte tillgodoses av SGSI.

- SOES föreslås genomföra en fördjupad analys kring nyttan av och möjligheterna till anslutning av ramavtalsbank till SGSI.

Vidare bör SOES bevaka resultatet från betänkandet av NISU 2014 (SOU 2015:23), som pekar på vikten av säker infrastruktur för kommunikationstjänster för statliga myndigheter. Betänkandet bereds i regeringskansliet och kommer att remitteras. Hur regeringen väljer att genomföra betänkandets förslag kommer att påverka utvecklingen av SGSI. Därmed kommer detta att påverka hur SOES bör agera avseende SGSI och säkerställandet av säkra kommunikationstjänster.

Innehåll

1 Inledning

Under 2014 utvecklade Arbetsgrupp Riskanalyser inom Samverkansområdet ekonomisk säkerhet (SOES) rapporten ”Riskanalys för myndigheterna inom SOES”. Syftet med detta arbete var att identifiera relevanta risker (med utgångspunkt i SOES syfte och mål), samt beskriva konsekvenser för utvalda risker. Syftet var även att utveckla förslag till fortsatt arbete.

En av de risker som identifierades under 2014 var ”internetstörningar”. Vid bedömningen konstaterades att internetstörningar riskerar väldigt stora delar av SOES-myndigheternas verksamhet, med felaktiga, försenade eller uteblivna utbetalningar som möjlig följd. Med det internetberoende som utvecklats hos myndigheter skulle därmed konsekvensen av avbrott i många avseenden vara omfattande. Mot bakgrund av tidigare års riskanalyser, utgör denna rapport en fördjupning av risken för internetstörningar.

1.1 Bakgrund

En snabb teknikutveckling ställer höga krav på tillgänglighet, tillförlitlighet och konfidentialitet i kommunikationen.[1] Samtidigt blir SOES-myndigheterna alltmer beroende av kommunikation, där alltmer känslig information delas i kommunikationsnäten. Därutöver blir IT-attacker allt vanligare, vilket även drabbar SOES-myndigheter.

I samband med 2014 års arbete inom SOES Arbetsgrupp Riskanalyser föreslogs att Swedish Government Secure Intranet (SGSI) skulle kunna utgöra ett robusthetshöjande alternativ vid internetstörningar. Då kunskapen om SGSI föreföll vara låg hos representanter för myndigheter inom SOES, beslutade SOES Arbetsgrupp Analys att under 2015 genomföra en fördjupad analys med fokus på SGSI.

1.2 Mål och syfte

Syftet med fördjupningen är att öka kännedomen om SGSI hos SOES-myndigheterna och utreda i vilken utsträckning SGSI är ett robusthetshöjande alternativ vid internetstörningar för myndigheterna inom SOES. Fördjupningen vänder sig således till representanter hos myndigheterna som har ett kritiskt beroende till internet och säker kommunikation, samt de aktörer som förvaltar SGSI.

Målet med denna fördjupning är därför att kortfattat beskriva vad SGSI är och att redogöra för möjligheter och begränsningar samt för- och nackdelar med SGSI som potentiellt robusthetshöjande alternativ.

1.3 Ingångsvärden och avgränsningar

I samband med utvecklingen av rapporten ”Riskanalys för myndigheterna inom SOES” konstaterades att internetberoendet hos SOES-myndigheterna är stort och svårligen

---

[1] SIS (2011), *Terminologi för Informationssäkerhet Utgåva 3*, Med *tillgänglighet* menas att informationstillgångar skall kunna utnyttjas i förväntad utsträckning och inom önskad tid, med *tillförlitlighet* (eller riktighet) menas att information inte förändras, vare sig obehörigen, av misstag eller på grund av funktionsstörning, med *konfidentialitet* menas att informations inte får göras tillgänglig eller avslöjas för obehöriga.

beskrivs i detalj. Samtidigt konstaterades att internetstörningar riskerar stora delar av SOES-myndigheternas verksamhet.

En aspekt som noterats i SOES rapport är även att internetberoendet påverkar SOES-myndigheterna indirekt genom ramavtalsbankerna. I befintliga ramavtal finns ett antal krav specificerade rörande tillgänglighet och krishantering. Det har dock framhållits att reservrutiner skulle kunna kommuniceras tydligare för en händelse att en eller flera ramavtalsbanker står stilla. Denna rapport utreder inte vidare hur kommunikation mellan SOES-myndigheter och ramavtalsbanker skulle tillgodoses av anslutning till SGSI. Däremot föreslås att frågan bör utredas vidare i ett senare skede.

Denna rapport utreder inte internetberoendet hos SOES-myndigheterna ytterligare. Rapporten fokuserar heller inte i första hand på befintligt användande av SGSI hos SOES-myndigheterna. Rapporten fördjupar snarare tidigare analys av risken för internetstörningar genom att redogöra för SGSI som ett förebyggande och riskreducerande alternativ.

1.4 Övergripande Metod

Denna rapport har främst utgått från en intervjustudie med representanter från Myndigheten för samhällsskydd och beredskap (MSB), som är systemägare till SGSI. Intervjustudien har därutöver kompletterats med informationsinhämtning från öppna källor. Rapporten innehåller även en kortfattad redogörelse för två internationella motsvarigheter till SGSI (Bilaga 1 – Internationella motsvarigheter). För dessa beskrivningar har information inhämtats genom dialog över e-post med företrädare för de aktuella systemen samt från öppna källor.

Vid intervjuerna har en uppsättning frågor varit vägledande för att skapa ökad förståelse för SGSI. Förteckning över intervjufrågorna, samt över de personer som intervjuats, återfinns i Bilaga 2 - Intervjupersoner och vägledande frågor.

2 Vad är SGSI?

SGSI är ett avgiftsfinansierat kommunikationsnätverk som ger säker kommunikation mellan myndigheter i Sverige och i Europa. SGSI har en egen infrastruktur som är skild från internet och påverkas således inte av internetstörningar, som till exempel genom överbelastningsattacker.

I dagsläget är totalt 27 aktörer anslutna till SGSI. Bland anslutna myndigheter kan nämnas Försäkringskassan, Skatteverket, Riksbanken och Finansinspektionen. Pensionsmyndigheten har hittills varit partiellt anslutet, via Försäkringskassans anslutning.

SGSI skapades 2004 och utvecklades ursprungligen för att tillgodose behovet av skyddad kommunikation mellan svenska myndigheter och EU-myndigheter.[2] Inledningsvis nyttjades SGSI nationellt mer av Polisen och mindre av de myndigheter som är anslutna idag. Statskontoret var systemägare för SGSI i samband med uppstarten, men systemägandet gick 2005 över till den nya myndigheten Verva. 2007

[2] Regeringen (2015), *Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten*, s. 155.

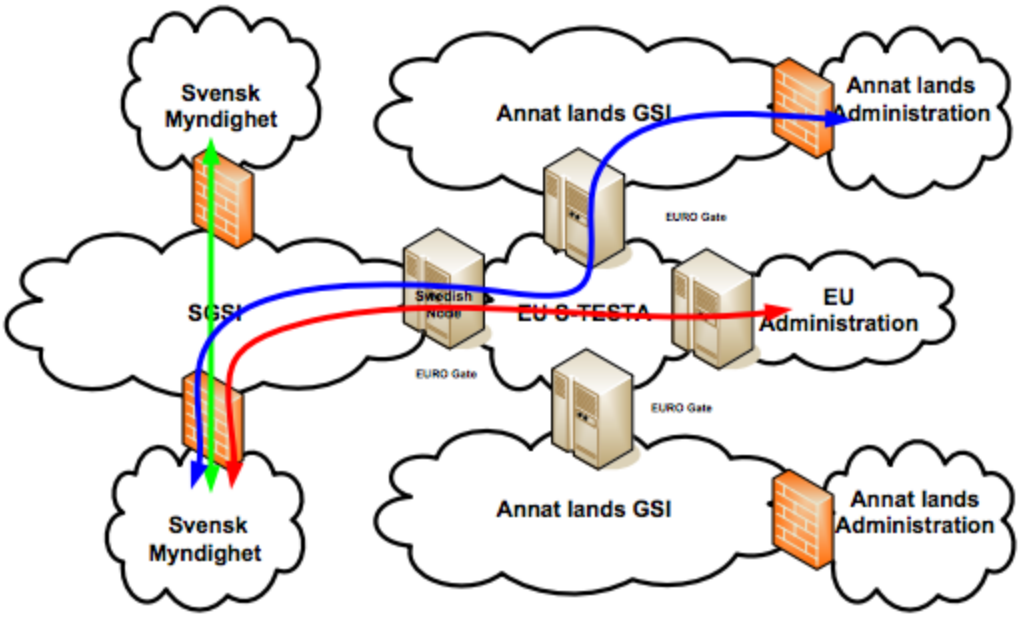
blev Krisberedskapsmyndigheten systemägare och i och med skapandet av Myndigheten för samhällsskydd och beredskap (MSB) 2009 har systemägaransvaret för SGSI överförts dit.

2.1 Kommunikation med SGSI

Myndigheter använder SGSI som ett säkert nätverk för utbyte av känslig information och minskar därmed risker kopplat till att skicka känslig information över internet. SGSI bör därmed ses som en säker ”bärare” för kommunikation mellan myndigheter.

Kommunikation med SGSI kan exempelvis ske genom att en myndighet ges säker åtkomst till en annan myndighets databas. SGSI möjliggör även krypterad e-post och videokonferens. Krypterad e-post kan ske dels genom relay-server, dels genom så kallad krypterad VPN[3]-tunnel, enligt punkt-till-punkt mellan myndigheter. Vid skyddad videokonferens upprättas en krypterad VPN-tunnel genom en videokonferensknutpunkt (”videobrygga”), som möjliggör upp till 50 deltagare. Myndigheterna bestämmer själva vad som ska kommuniceras över SGSI och med vem. Avsändare och mottagare kommer överens om vad som ska skickas och MSB administrerar öppningen för kommunikation.

Anslutna myndigheter kan även kommunicera säkert via SGSI med EU-administrationen eller med en annan ansluten medlemsstat genom secure Trans European Services for Telematics between Administrations (sTESTA). Genom sTESTA är SGSI bland annat anslutet till Common Emergency Communication and Information System (CECIS), som är en databas för samverkan kopplat till EU-länders civilförsvarsresurser. Figur 1 illustrerar användningen av SGSI bland enskilda svenska myndigheter och i andra länder inom EU.



Figur 1:Användningen av SGSI bland svenska myndigheter och andra EU-länder (Källa: MSB)

[3] Virtual Private Network är en teknik som används för att skapa säkra förbindelser mellan två punkter i nätverk.

2.2 Drift av SGSI

MSB är systemägare för SGSI och står för samordning, förvaltning, utveckling, samt för ackreditering av deltagare. Försvarsmaktens logistik (FMLOG) står för övervakning. TeliaSonera SNS (Speciell nätsäkerhet) levererar drift av förbindelser i MPLS-nät samt helpdesk som är tillgänglig dygnet runt. Försvarets radioanstalt (FRA) ansvarar för certifikat och genomförande av utbildningar.

Figur 2: Drift av SGSI

2.3 Förutsättningar för anslutning

Vid önskemål om anslutning görs en ansökan till MSB. Därefter genomförs ett ackrediteringsmöte där underlag och krav diskuteras. Uppfyllnad av kraven utvärderas genom ackreditering, som bygger på internationell standard inom informationssäkerhet (ISO 27000). Bland annat ställs administrativa krav på policy/regelverk och rutiner, samt på övervakning, revision och uppföljning. Därutöver ställs mer tekniska krav på fysisk säkerhet och IT-säkerhet. Kraven syftar sammantaget till att upprätthålla en hög grundnivå på säkerheten hos aktörer som är anslutna. Kraven bidrar även till att skapa förtroende och tillit till användningen av SGSI. Tabell 1 visar ett antal exempel på kraven kopplade till ackrediteringen.

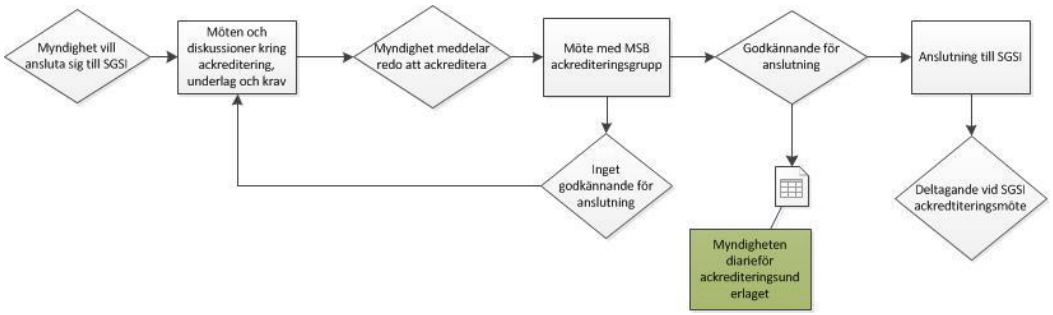
Tabell 1: Exempelkrav ackreditering SGSI

Exempelkrav 1	Informationssäkerhetspolicyn är omsatt i styrdokument i form av regelverk/riktlinjer eller andra styrdokument som gäller för hela organisationen.
Exempelkrav 2	Det finnas en struktur för informationsägarskap inom myndigheten som tillämpas för alla informationstillgångar.
Exempelkrav 3	Nätverk är uppdelade i olika säkerhetszoner med ”trafikkontroll och styrning” mellan zonerna. T.ex. internet, DMZ, internt nät, SGSI-nät.

Vid ackrediteringsmötet deltar SGSI:s referensgrupp, som består av representanter från fyra anslutna myndigheter. Myndigheter i referensgruppen sitter under en två-årsperiod, och varje år ersätts två av myndigheterna i syfte att få kontinuitet i gruppen.

Efter godkännande genomförs installation och anslutning sätts upp. Den utrustning som krävs lånas ut av MSB till anslutna aktörer. Ledtiden från ansökan till anslutning, inklusive ackreditering, är cirka 3 månader. Detta förutsätter som sagt att den aktör som

önskar ansluta sig till SGSI uppfyller de IT-säkerhetskrav som ställs vid ackrediteringen. För redan anslutna aktörer sker även en årlig re-ackreditering, i form av ett möte där ansluta organisationer redovisar sin säkerhet. Dessutom genomförs årligen cirka fem platsbesök hos enskilda anslutna aktörer, där utrustning och säkerhet inspekteras och MSB ger råd. Processen för anslutning illustreras i Figur 3.



Figur 3: Ackrediterings- och godkännandeprocessen (Källa: MSB)

2.4 Kostnader

SGSI är en betaltjänst, där anslutna aktörer betalar dels en fast kostnad vid uppstart för utrustning, installation och uppsättning av brandväggar. Denna kostnad varierar i dagsläget mellan 60 000 kronor och 85 000 kronor. Därutöver betalas en månatlig kostnad för abonnemang och service, som varierar mellan ca 15 000 kronor och 24 000 kronor beroende på servicenivå.

SGSI är en avgiftsfinansierad verksamhet inom MSB, vilket innebär att kostnader ska balanseras mot intäkter. Avgifterna finansierar driften som beskrivits ovan och MSB gör inga ytterligare pålägg utöver den avgift exempelvis Telia tar ut mot MSB. Med fler aktörer som ansluts, ges stordriftsfördelar i drift och förvaltning. Skulle antalet anslutna myndigheter öka, kan därmed avgifterna minska.

2.5 Framtida utveckling

SGSI har en kunddriven tjänsteutveckling, bland annat med ett utvecklingsråd som består av anslutna myndigheter. Under 2013 genomfördes en behovsinventering av tjänster i SGSI som myndigheter efterfrågar och för flera av de identifierade behoven har det under 2014 genomförts pilotprojekt. Bland annat har det genomförts projekt för skyddad internetåtkomst, vilket skulle kunna möjliggöra säkrare kommunikation även över det öppna internet. Detta skulle exempelvis kunna inkludera ett stärkt grundskydd genom DDoS[4]-skydd, mailtvätt och sensorer för att upptäcka attacker.

Projekt har även genomförts med fokus på mobila lösningar, med syfte att över SGSI få åtkomst till myndighetsintern information via mobila enheter, samt möjlighet till skyddat tal mellan de anslutna myndigheterna.[5]

[4] Distributed Denial of Service är en form av överbelastningsattack.

[5] MSB (2014), *Nationell handlingsplan för samhällets informationssäkerhet, Statusrapport genomförande*, (s.30-31).

Under 2013 beslutades om en särskild utredning för att föreslå strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och IT-system.[6] Utredningen överlämnade i mars 2015 ett betänkande (SOU 2015:23), där bland annat föreslås att samtliga myndigheter som anges i bilagan till förordningen (2006:942) om krisberedskap och höjd beredskap ansluts till SGSI. Utredaren föreslår att SGSI bör utvecklas för att utgöra en av delarna i en säker kommunikationsinfrastruktur för statliga myndigheter. Därutöver föreslås att SGSI vidareutvecklas, bland annat gällande upptäckt av intrång och angrepp.[7]

3 SGSI som ett robust alternativ för SOES-myndigheterna?

I dagsläget är huvudsakligen myndigheter anslutna till SGSI. SOES-myndigheternas behov att kommunicera med andra aktörer, såsom ramavtalsbanker, ligger därmed för närvarande utanför SGSI. Det är således oklart huruvida en ramavtalsbank skulle godkännas vid förfrågan om anslutning. För att besvara denna fråga bör man genomföra en fördjupad utredning. Eventuellt kan den koppling som krävs mellan myndigheter och ramavtalsbank specificeras och särskiljas på ett sätt som inte strider mot informationssäkerhetskrav som ställs på anslutna deltagare.

Med säkerhet i kommunikationen, skulle robustheten i myndigheters betalningar kunna stärkas. Därigenom skulle risken för internetstörningar förebyggas och risken minskas avseende försenade, uteblivna eller felaktiga utbetalningar från SOES-myndigheterna.

Vidare bör, enligt MSB, SGSI ses som ett robusthetshöjande alternativ för säkrare kommunikation. Det bör emellertid inte ses som en reservrutin, utan som ett primärt alternativ. Anledningen till detta är tvåfaldigt:

- SGSI tillhandahåller säker och skyddad kommunikation, vilket internet inte gör.
- Krishanteringen kan effektiviseras om samma system används i vardagen som i kris.

3.1 Styrkor och utmaningar med SGSI

Styrkorna i SGSI motsvaras av möjlighet till säker kommunikation, i termer av tillgänglighet, tillförlitlighet och konfidentialitet.

En hög tillförlitlighet och konfidentialitet ges av möjlighet till kryptering och användning av certifikat. Eftersom att SGSI är skiljt från internet kan anslutna myndigheter kommunicera via SGSI vid överbelastning på internet. Även webbplatser i SGSI skulle vara tillgängliga.[8] En styrka med SGSI är således dess mycket höga tillgänglighet (99.98%). Detta tack vare god redundans genom att den tekniska utrustningen i SGSI är dubblerad; skulle ett system drabbas av störningar går det fort

---

[6] Regeringen (2013), *Dir. 2013:110, Strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och IT-system.*

[7] Regeringen (2015), *Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten*, s.246.

[8] Verva (2006) *Arkitektur och ramverk för interoperabilitet – förstudie 2006.*

att övergå till ett annat. Vid högre servicenivåer finns även möjlighet till geografiskt diversifierad anslutning.

Enligt MSBs beskrivning finns ingen s.k. single-point-of-failure i själva SGSI. Ännu en fördel med SGSI är att en aktör som har flera enskilda punktförbindelser kan ersätta dessa med en gemensam förbindelse in i SGSI-nätverket, och därigenom reducera kostnader kopplade till drift och förvaltning av flera enskilda punktförbindelser. Detta förutsätter dock att berörda aktörer är anslutna till SGSI.

Vid tidigare års analyser inom SOES av risken för internetstörningar, har framhållits att nätägare ofta har dubblerade nät, men att det trots detta kan finnas knutpunkter där sårbarheten är särskilt stor. Möjligheten till geografiskt separerade anslutningar via SGSI innebär därmed en hög robusthet mot risken för störningar i kommunikationen.

Potentiella utmaningar för SGSI är begränsningar av överföringskapaciteten, som är beroende av kryptoutrustningen. Idag är den högsta kapacitet som erbjuds 2 Gbit/s. Vidare anges i betänkandet av Informationssäkerhetsutredningen NISU 2014 att ”Under utbyggnaden av SGSI bör det vidtas åtgärder för att utveckla system för att upptäcka intrång och angrepp”[9], vilket skulle kunna indikera en begränsning kopplat till skyddet mot skadlig kod.

MSB konstaterar vid intervju att en ytterligare utmaning är att kännedomen kring SGSI hos anslutna myndigheter generellt sett är låg, bland annat om att den egna myndigheten är ansluten eller vad SGSI är och vilka möjligheter som finns vid anslutning och hos de erbjudna tjänsterna.

[9] Regeringen (2015), *Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten*, s.18.

4 Avslutande kommentarer

I takt med att teknikberoendet ökar i samhället, ökar beroenden till säker kommunikation även mellan myndigheter. System som stödjer information och kommunikation blir därmed alltmer kritiska resurser, vilket även gäller SOES-myndigheter. Detta understryks inte minst i SOES egna analyser av risker och beroenden.

Denna rapport har utrett SGSI som en möjlig reservrutin vid internetstörningar för myndigheterna inom SOES. SGSI bör ses som ett robusthetshöjande alternativ för säkrare kommunikation. SGSI bör, enligt MSB, emellertid inte ses som en reservrutin, utan som ett primärt alternativ. Säker kommunikation mellan SOES-myndigheter kan exempelvis tillgås gällande åtkomst till databaser, samt avseende säker e-post och videokonferens.

Styrkorna i SGSI ligger i goda möjligheter till säker kommunikation, i termer av tillgänglighet, tillförlitlighet och konfidentialitet. Anslutna myndigheter bestämmer själva vad som ska kommuniceras över SGSI och med vem. Myndigheters egna bedömningar av vilken kommunikation och information som är kritisk och känslig, t.ex. utifrån risk- och sårbarhetsanalyser, kan därmed vara en utgångpunkt för beslut om SGSI-anslutning. Därutöver bör ovan nämnda förslag beaktas om att samtliga myndigheter som anges i bilagan till förordningen (2006:942) om krisberedskap och höjd beredskap bör anslutas till SGSI.

Från beskrivning av de internationella motsvarigheterna till SGSI, kan noteras att länder som Spanien och Finland har system som i flera avseenden är snarlika SGSI. Skillnader finns emellertid, bland annat att anslutning av myndigheter är reglerat i lag i dessa länder och att antalet användare är större.

En möjlig utmaning kring systemet, utifrån SOES perspektiv, är huruvida kommunikation med andra aktörer, såsom ramavtalsbanker, vore möjligt via SGSI i framtiden, då anslutning till SGSI förutsätter en särskild prövning och då SGSI huvudsakligen är till för myndigheter. En ytterligare utmaning är att kännedomen om SGSI och möjligheterna att genom SGSI skydda och säkra aktörernas kommunikation och informationshantering hittills varit relativt låg inom SOES-myndigheter. Denna rapport väntas bidra till att höja kunskapsnivån hos myndigheterna.

5 Nästa steg

5.1 Förslag till fortsatt arbete inom SOES

SOES föreslås genomföra en fördjupad studie av hur anslutna SOES myndigheter använder SGSI och vilka styrkor och utmaningar som kunnat konstateras vid användningen. Denna studie föreslås även identifiera eventuella kommunikationsbehov hos SOES-myndigheterna som inte tillgodoses av SGSI.

SOES föreslås även genomföra en fördjupad analys kring nyttan av och möjligheterna till anslutning av ramavtalsbank till SGSI. MSB, som är systemägare till SGSI, föreslås ha en aktiv roll i utredning av förutsättningarna för anslutning av, givet de kriterier för anslutning som gäller i dagsläget.

Vidare bör SOES bevaka resultatet från betänkandet av NISU 2014. Hur regeringen väljer att genomföra betänkandets förslag kommer att påverka utvecklingen av SGSI. Därmed kommer detta att påverka hur SOES bör agera avseende SGSI och säkerställandet av säkra kommunikationstjänster.

Bilagor

Bilaga 1 – Internationella motsvarigheter

Spanien[10]

Det finns ett antal internationella motsvarigheter till SGSI. Ett exempel på en sådan är spanska Red SARA (Sistemas de Aplicacions y Redes para las Administraciones). Likt SGSI är Red SARA ett kommunikationsnätverk som ger säker kommunikation mellan myndigheter i Spanien och i Europa via sTESTA. Initiativet till Red SARA togs i syfte att effektivisera och reducera kostnaderna för delning av data, information och infrastruktur mellan samhällsviktiga aktörer.

Användandet av och anslutning till Red SARA är reglerat i ett flertal spanska lagar.[11] I linje med dessa lagar är samtliga spanska statliga myndigheter, inklusive större aktörer såsom den spanska centralbanken, anslutna till Red SARA. Gällande finansiella myndigheter är samtliga anslutna till Red SARA. Däremot tillåts inte andra finansiella institutioner, som till exempel storbanker, att ansluta till Red SARA. Detta motiveras av att nätverket endast är till för statliga aktörer.

Även ett stort antal samhällsviktiga aktörer på lokal nivå är anslutna till Red SARA. Ett utdrag av en lag som reglerar användandet av Red SARA redovisas nedan:

> *Public Administrations will use preferably the Communication Network of the Spanish Public Administrations to communicate with each other, purpose for which they will connect to it, either their respective networks, or their interoperability nodes, in a way that the interchange of information and services among them is facilitated, as well as the interconnection with the networks of the Institutions of the European Union and of other Member States.*
>
> *SARA network will provide the Communication Network of the Spanish Public Administrations.*[12]

Den lagstadgade regleringen av breda användare innebär att nätverket tillåter säker och riktad kommunikation på flera olika ansvars- och eskaleringsnivåer. Den totala mängden användare av Red SARA uppgår till över 3700.

För större aktörer medger Red SARA säker kommunikation i upp till 10 Gb/s, och för mindre aktörer upp till 100 Mb/s. Likt SGSI kan även krypterade videokonferenser genomföras via Red SARA. För att upprätthålla dessa hastigheter och god tillgänglighet nyttjar Red SARA diversifierad anslutning och dubblerad teknisk utrustning. Vid behov

---

[10] Informationen presenterad nedan har inhämtats från textbaserade intervjuer (Bilaga 2 - Intervjupersoner och vägledande frågor) samt öppna källor

[11] Gobierno de España (2010), *LAW 11/2007, of 22 June, on electronic access to Public Services for members of the public*; Gobierno de España (2010), *Royal Decree 4/2010, of January 8th, which regulates the National Interoperability Framework within the e-government scope*; Gobierno de España (2010), *Royal Decree 3/2010, of January 8th, which regulates the National Security Framework within the e-government scope*.

[12] Gobierno de España (2010), *Royal Decree 4/2010, of January 8th, which regulates the National Interoperability Framework within the e-government scope*.

av teknisk hjälp finns det även en supportfunktion för Red SARA som är tillgänglig dygnet runt, alla dagar på året.

För att en aktör ska få ansluta till Red SARA finns det ett antal krav som regleras i spansk lag.[13] Likt kraven för anslutning till SGSI syftar dessa till att upprätthålla en hög lägstanivå avseende informationssäkerhet bland anslutna aktörer.

Jämfört med SGSI är nätverken i många hänseenden lika. De mest framträdande skillnaderna mellan Red SARA och SGSI är lagkrav kopplat till nätverket och mängden anslutna aktörer. I övrigt ligger Red SARA även ett steg före SGSI inom ramen för system för att upptäcka antagonistiska intrång och angrepp. Red SARA har flera system för att upptäcka intrång och angrepp på nätverket som kontinuerligt bevakas av CERT (Computer Emergency Response Team) vid det spanska nationella centrumet för kryptering. Utvecklingen av ett liknande system för SGSI har föreslagits i betänkandet SOU 2015:23.[14]

Finland[15]

Ytterligare en internationell motsvarighet till SGSI är finska förvaltningens säkerhetsnät, TUVE. TUVE är ett nät för myndigheter som tillgodoser hög tillgänglighet och säkerhet. TUVE har beskrivits som robust och redundant och målsättningen är att nätverket ska finnas tillgängligt i alla lägen. Ett av nätverkets huvudsyften är att förbättra den finska statsledningens förmåga att på ett säkert sätt kommunicera och leda myndighetssamarbeten. TUVE underlättar även kommunikationen mellan enskilda myndigheter i linje med fastställda informationssäkerhetsbestämmelser.

Lagen om verksamhet i den offentliga förvaltningens säkerhetsnät anger vilka användare som ska anslutas till säkerhetsnätet. Det finns cirka 30 000 individuella anslutna användare av TUVE bland myndigheter och kommunala säkerhetsaktörer. Bland annat är den finska sjöräddningen, gränssäkerheten och nödcentralsverksamheten anslutna till TUVE.[16]

Förutom effektivisering av kommunikationsförmågor innebär anslutning till TUVE att enskilda aktörer kan ersätta tidigare individuella datakommunikationsförbindelser och tillhörande förvaringsutrymmen, vilket bland annat innebär reducerade kostnader för till exempel underhåll. I lagen om verksamheten i den offentliga förvaltningens säkerhetsnät står angivet:

> *Säkerhetsnätet kan användas även av andra användare än de som avses i 3 §, om nätet används för skötseln av uppgifter i anslutning till verksamhet som avses i 2 § 1 mom., användaren hör till en sådan användargrupp inom myndighetsnätet som bestäms i enlighet med informationssamhällsbalken och finansministeriet har godkänt användaren som användare av säkerhetsnätet.*[17]

---

[13] Gobierno de España (2011), *Resolution of the Secretary of State for Public Service, 19 July 2011*.

[14] Regeringen (2015), *Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten*, s.246.

[15] Informationen presenterad nedan har inhämtats från öppna källor

[16] Finansministriet (2015), http://ministryoffinance.fi/vm/sv/05_projekt/05_tuve/index.jsp

[17] Justitieministeriet (2015), *10/2015 Lag om verksamheten i den offentliga förvaltningens säkerhetsnät*.

Att det finska finansministeriet är en av de användarna som regleras i 2 § 1 mom. indikerar potentiella möjligheter för anslutning av övriga finansiella institutioner. Någon sådan information har dock ännu inte kunnat bekräftas.

TUVE är baserat på den finska försvarsmaktens specialskyddade data- och kommunikationsnät och förvaltas av förvaltningens IT-central HALTIK. Det finska finansministeriet ansvarar för strategisk och ekonomisk styrning av säkerhetsnätverket, liksom för styrningen och övervakningen av serviceproduktionen.

Det finns likheter mellan SGSI och TUVE. Bland annat har nätverken liknande syften och båda nätverken har tydliga informationssäkerhetsbestämmelser. Däremot är TUVE ett säkerhetsnätverk vars anslutna användare regleras i lag, vilket inte ännu finns för SGSI. Även antalet användare skiljer sig mellan SGSI och TUVE, där TUVE har över 30 000 individuella användare på både myndighets- och lokalaktörsnivå. Då ingående detaljer kring teknisk specifikation för TUVE saknas har dock inte någon jämförelse med SGSI inom ramen för tekniska- och redundanslösningar kunnat genomföras.

Bilaga 2 - Intervjupersoner och vägledande frågor

MSB:

Följande frågeställningar har legat till grund för de intervjuer som genomförts:

- Vad kan SGSI användas för, t.ex. typer av funktioner/system?
- Vilka begränsningar har SGSI?
- Vilka är de främsta fördelarna med SGSI? Ur SOES perspektiv?
- Vilka är de främsta nackdelarna med SGSI? Ur SOES perspektiv?
- Vilken kapacitet har SGSI?
- I vilken utsträckning kan SGSI ses som ett robusthetshöjande alternativ/reservrutin vid internetstörningar?
- I vilken utsträckning kan SGSI nyttjas vid DDoS-attacker?
- Vilka krav finns på myndigheter för att ansluta sig till SGSI?
- Vad är kostnaden för att ansluta sig till SGSI?
- Hur ser planen ut för utveckling av SGSI under närmaste året/åren?
- Finns relevant dokumentation om SGSI, som SOES kan ta del av?

Intervjuer har genomförts med följande myndighetsrepresentanter:

- Mats Persson (MSB) 31 mars 2015
- Evert Enblom (MSB) 31 mars 2015
- Kristina Bram (MSB) 31 mars 2015

Secretaría de Estado de Administraciones Públicas:

Följande frågeställningar har legat till grund för de intervjuer som genomförts:

- Vad är Red SARA?
- I vilken utsträckning används Red SARA?
- Finns det några lagar som reglerar användandet av Red SARA?
- Vilken kapacitet har Red SARA?
- Finns det några begräsningar för Red SARA?
- Används Red SARA av finansiella institutioner?
- Finns relevant dokumentation om Red SARA, som SOES kan ta del av?

Textbaserade intervjuer har genomförts med följande representant:

- Miguel A. Amutio Gómez (Secretaría de Estado de Administraciones Públicas) 23 april 2015; 5 maj 2015

Bilaga 3 - Litteraturförteckning

Gobierno de España (2010), *LAW 11/2007, of 22 June, on electronic access to Public Services for members of the public*.

Gobierno de España (2010), *Royal Decree 3/2010, of January 8th, which regulates the National Security Framework within the e-government scope*.

Gobierno de España (2010), *Royal Decree 4/2010, of January 8th, which regulates the National Interoperability Framework within the e-government scope*.

Gobierno de España (2011), *Resolution of the Secretary of State for Public Service, 19 July 2011*.

Justitieministeriet (2015), *10/2015 Lag om verksamheten i den offentliga förvaltningens säkerhetsnät*.

MSB (2014) *Nationell handlingsplan för samhällets informationssäkerhet - Statusrapport genomförande*.

MSB (2014) *SGSI – Swedish Government Secure Intranet*.

Regeringen (2013), *Dir. 2013:110, Strategi och mål för hantering och överföring av information i elektroniska kommunikationsnät och IT-system*.

Regeringen (2015), *Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten, SOU 2015:23)*.

SIS (2011), *Terminologi för Informationssäkerhet Utgåva 3*.

SOES (2014) *Riskanalys för myndigheterna inom SOES*.

Verva (2006) *Arkitektur och ramverk för interoperabilitet – förstudie 2006*.