LANTMÄTERIET

Geodata
SVERIGE BIT FÖR BIT

2019-03-28

Dnr: LM 2019/001170

RAPPORT GEODATARÅDETS HANDLINGSPLAN 2018

Aktivitet 2 C, Redundans i geodataförsörjningen

Lantmäteriet, 801 82 Gävle
BESÖKSADRESS Lantmäterigatan 2 C, TELEFON 0771 - 63 63 63
E-POST lantmateriet@lm.se, INTERNET www.lantmateriet.se

Innehållsförteckning

Sammanfattning

Uppdraget ingår i fokusområdet *Öppenhet och säkerhet* och utgår från den Nationella geodatastrategin och geodatarådets handlingsplan för 2018-2020. Denna rapport är en av flera delrapporter vilka ska tjäna som underlag till att uppfylla den Nationella geodatastrategin.

Syftet med uppdraget har varit att analysera behoven av redundans bland olika geodataanvändare med samhällskritiska uppgifter samt att skapa en situationsbild över befintliga och kommande tekniska lösningar. Efterhand arbetet fortskred diskuterades begreppet redundans och det finns vissa behov av redundans men de stora behoven omfattas av det vi kallar säkert informationsutbyte.

När behovsinventeringen slutsummerades fanns de högsta kraven hos Försvarsmakten och Polisen, där kraven på säkert informationsutbyte är höga för all information. De vill också ha data från källan och helst då online, vilket i sig ställer högre krav. Det finns även myndigheter med ringa behov av säkert informationsutbyte, dock kan andra myndigheters krav föra med sig att den levererande myndigheten måste höja sin säkerhetsnivå

Det finns även andra krav som den offentliga förvaltningen måste förhålla sig till och ett exempel är EU-direktivet NIS som innebär krav på informationssäkerhet och incidentrapportering för leverantörer av samhällsviktiga och vissa digitala tjänster.

De datateman som det ställs högst krav på är de som innehåller personinformation. Fastighetsinformation innehåller ofta direkt eller indirekt personinformation. Även information om skyddsobjekt hör till de mest kritiska

Vår rekommendation är att myndigheter och kommuner bör använda SGSI (Swedish Government Secure Intranet) där säkert informationsutbyte krävs. SGSI är en tjänst för säker kommunikation mellan myndigheter i Sverige och i Europa. SGSI:s infrastruktur är avskild från Internet och påverkas av den anledningen inte av de störningar som kan förekomma på Internet

Kommunsamverkan där flera kommuner är sammankopplade med sina nät i ett kluster kan vara en lösning om en av dessa kommuner fungerar som en nod för att via SGSI utbyta geodata. Men för att uppnå effektivitet och synergieffekter borde Sveriges myndigheter och kommuner ha en gemensam teknisk lösning för säkert informationsutbyte.

Grundläggande i arbetet med informationssäkerhet är att varje organisation gör en informationssäkerhetsklassificering samt att varje organisation bör arbeta med informationssäkerhet på ett strukturerat sätt som bygger på den svenska och internationella standardserien SS-ISO/IEC 27000.

1 Inledning och bakgrund

1.1 Uppdraget

Uppdraget utgår från den Nationella geodatastrategin och geodatarådets handlingsplan för 2018-2020. Uppdraget ingår i fokusområdet Öppenhet och säkerhet där den övergripande målsättningen är; *Infrastrukturen för geodata behöver såväl öppna data, redundant åtkomst till data samt god informationssäkerhet. Arbetet på detta område inkluderar att närmare kartlägga förutsättningarna för öppna resp. avgiftsfria data, utveckla samverkan kring informationssäkerhet samt att överväga teknik och åtgärder för redundant dataåtkomst*

Inom detta uppdrag ska Lantmäteriet, tillsammans med andra myndigheter, analysera behoven av redundans bland olika geodataanvändare med samhällskritiska uppgifter och skapa en situationsbild över befintliga (t.ex. SGSI-nätet) och kommande tekniska lösningar.

Arbetet omfattar följande:

- Definiera vilka behov av redundans som finns samt vilka geodata som innefattas i de behoven. Workshop med det temat genomförs med arbetsgruppen samt därefter kontakt med fler myndigheter och kommuner för fortsatt behovsinventering
- Analysera användarbehoven relaterat till befintliga lösningar och kommande kända lösningar. Beskriv eventuellt gap mellan behov och utkast på befintliga tekniska lösningar
- Workshop med arbetsgruppen kring behovsbilden samt relevanta tekniska lösningar och kända framtida lösningar genomförs
- Förankring av den framtagna situationsbilden kopplat till användarbehoven
- Resultatet av uppdraget sammanställs i en rapport
- Granskning av rapporten genomförs av de inblandade och därefter införs eventuella justeringar
- Slutrapportering den 2 april 2019

2 Intressenter

2.1 Deltagare i referensgruppen

Följande myndigheter medverkar i referensgruppen: Lantmäteriet, Länsstyrelsen i V:a Götaland, Myndigheten för samhällskydd och beredskap, Polismyndigheten och Sveriges geologiska undersökning. Lantmäteriet har varit uppdragsledare.

2.2 Myndigheter och kommuner

Deltagare i samband med behovsinventeringen samt som granskare av rapporten

2.2.1 MYNDIGHETER

Lantmäteriet

Länsstyrelserna i V:a Götaland, Gävleborg, Jönköping och Skåne

Myndigheten för samhällskydd och beredskap

Polismyndigheten

Riksantikvarieämbetet

Skatteverket

Sveriges geologiska undersökning

Trafikverket

2.2.2 KOMMUNER

Sveriges kommuner och landsting

Bollnäs kommun

Gävle kommun

Göteborgs stad

Ljusdals kommun

3 Tillvägagångssätt

3.1 Arbete i referensgruppen

Två workshopar har genomförts med referensgruppen. Den inledande hade fokus på att förtydliga uppdraget och att lägga grund inför behovsinventeringen. Den andra hade fokus på resultatet av behovsinventeringen och slutsatser som kan dras samt rekommendationer för fortsatt arbete. Vid båda tillfällena diskuterades och informerades också om de tekniska lösningar som finns att tillgå för säkert informationsutbyte.

3.2 Behovsinventering

Behovsinventeringen genomfördes i form av enskilda möten med myndigheter och kommuner där deras behov av säkert informationsutbyte av geodata diskuterades. Dessa myndigheter och kommuner valdes dels för att få en mix på verksamheter som bidrar och dels även i storlek på verksamheter. Efterhand gjordes avstämningar av de synpunkter som kom in och även om det fanns behov av att intervjua fler. Inför respektive möte skickades information om uppdraget ut till mötesdeltagarna.

4 Förutsättningar, krav och antaganden

4.1 Bakgrund

Behovet av att skydda information från obehörig åtkomst samt upprätthålla tillgänglighet och robusthet i IT-nätverk har ökat i omfattning. Alltmer datatrafik kräver förbättrade nätverk och fler och fler IT-attacker gör att fler blir varse om de hot som föreligger. Via Internet kan attacker genomföras över hela världen, både mot privata medborgare och myndigheter.

Försvarets radioanstalt (FRA) skriver i sin årsrapport för 2018 att de genom signalspaning ser att IT-angrepp mot svenska myndigheter och företag pågår här och nu. Därför måste verksamheter som hanterar information som är intressant för främmande länders underrättelsetjänster utgå från att man blir utsatt. Även leverantörer till sådan verksamhet kan vara intressanta för en angripare, som en lättare väg till målet. FRA har även kunnat konstatera att statliga aktörer angriper kritisk infrastruktur i Sverige. Syftet kan exempelvis vara att allvarligt störa viktiga samhällsfunktioner vid en eventuell kris- eller krigssituation[1]. I ett reportage från januari 2019 relaterades till två år gamla siffror där FRA redovisade att de upptäckte 10 000 aktiviteter per månad från statliga utländska angripare – mot mål Sverige. I dag är siffran högre, säger FRA[2].

Enligt en rapport från IT-säkerhetsföretaget NTT-security 2017 är svenska myndigheter det vanligaste målet för en IT-attack. Och trots att MSB också rekommenderar myndigheter att även polisanmäla intrångsförsök är det få som gör det. Under 2018 var det ungefär 10 procent av de svåra attackerna som anmäldes, medan det under 2017 var runt 20 procent. Det spekuleras i att myndigheter drar sig för att anmäla utifrån en föreställning om att man då visar sin dåliga IT-säkerhet [3].

Mer och mer vanligt blir de s.k. DDoS-attackerna, då nätverk och system blir överbelastade. Ofta kan utpressningshot vara förknippade med sådana attacker men det kan ofta handla om att ställa till med skada. Till exempel har sådana attacker har medfört tågförseningar[4]. Inför valet i september 2018 utsattes t.ex. Socialdemokraternas hemsida för flera överbelastningsattacker[5]. Exemplen är många och vittnar om att säkerheten måste tas på största allvar för att skydda känslig information, personlig integritet m.m.

4.2 Redundans eller säkert informationsutbyte

Uppdragets titel innehåller ordet redundans och när det gäller geodataförsörjningen innebär det dubbel eller flerdubbel uppsättning av viktiga komponenter för att system och nätverk ska fungera även om något går sönder. Det finns vissa behov av redundans men de stora behoven omfattas av det

[1] https://www.fra.se/
[2] https://www.svt.se/nyheter/fra-cyberangreppen-mot-sverige-okar
[3] https://www.svt.se/nyheter/inrikes/myndigheter-daliga-pa-att-polisanmala-it-attacker
[4] https://computersweden.idg.se/2.2683/1.690504/ddos-bakom-tagforseningar
[5] https://www.svt.se/nyheter/inrikes/ny-overbelastningsattack-mot-socialdemokraternas-hemsida

vi kallar säkert informationsutbyte. Då vi diskuterat behoven av säkert informationsutbyte har vi utgått från de säkerhetsaspekter som beskrivs i följande kapitel och enbart i något fall har vi kommit in på redundans i form av dubbla lösningar.

4.3 Säkerhetsaspekter

En tillhandahållandelösning ska ur säkerhetssynpunkt ses utifrån säkerhetsaspekterna insynsskydd (konfidentialitet), riktighet och tillgänglighet. Där insynsskydd ska säkerställa att informationen inte tillgängliggörs eller avslöjas för obehöriga, riktighet att informationen garanteras fullständighet eller exakthet samt tillgänglighet där informationen ska vara åtkomlig och användbar i förväntad utsträckning och inom önskad tid. Dessa säkerhetsaspekter finns formulerade i MSB:s Modell för klassificering av information.[6]

Det är varje myndighets ansvar att deras informationshanteringssystem uppfyller grundläggande och vid behov även särskilda säkerhetskrav. Dessa krav har konkretiserats i MSB:s föreskrifter där det bl.a. står att myndigheter ska klassa sina data utifrån ovanstående säkerhetsaspekter, genomföra risk- och sårbarhetsanalyser samt utifrån det införa ändamålsenliga och proportionella säkerhetsåtgärder.[7]

4.3.1 ENKLA EXEMPEL PÅ ANVÄNDNINGSFALL

Med utgångspunkt i säkerhetsaspekterna insynsskydd (konfidentialitet), riktighet och tillgänglighet redovisas nedan några enkla användningsfall för att exemplifiera detta ur perspektivet säkert informationsutbyte.

Exempel på utbyte av ortofoton

Lantmäteriet har ett utbyte med en kommun som levererar in ortofoton de producerat själva. I en del ortofoton ingår information relaterad till Försvarsmakten (s.k. skyddsobjekt) vilket innebär att alla ortofoton ska granskas av Lantmäteriets avdelning för Kart- och bildsekretess enligt lagen om skydd för geografisk information. Efter granskning ska samtliga ortofoton skickas tillbaka till kommunen.

Med avseende på säkerhetsaspekterna:

- **Insynsskydd**. Vid utbytet av ortofoton får informationen inte vara åtkomlig för obehöriga till dess att de blivit granskade och skyddsobjekten i respektive ortofoto åtgärdade
- **Riktighet**. Vid utbytet ska det också säkerställas att informationen inte förvanskas på vägen
- **Tillgänglighet**. Har en lägre prioritet, det är inte kritiskt om leveransen kommer en dag senare. Däremot kan det, vid stora datamängder, behövas ökad bandbredd för att möjliggöra leverans

[6] https://www.msb.se/RibData/Filer/pdf/25602.pdf

[7] MSBFS 2018:8

De beskrivna kraven ovan kan inte säkerställas vid informationsutbyte via Internet utan för att uppfylla kraven är en lösning att leverans görs via SGSI-nätet (Swedish Government Secure Intranet).[8]. Idag sker leverans via krypterad FTP och vid större datamängder via extern (bärbar) hårddisk.

Exempel på utbyte där personinformation ingår

Skatteverket ansvarar för folkbokföringen och personuppgifter omfattas av GDPR och kan även vara sekretessbelagda. Därför finns oftast stora behov av säker hantering av informationsmängder där personinformation ingår. Många tjänster där personinformation ingår är också onlinetjänster med höga krav på tillgänglighet.

Med avseende på säkerhetsaspekterna:

- **Insynsskydd** och **riktighet**. Höga krav utifrån dessa aspekter då det kan handla om sekretessbelagda uppgifter
- **Tillgänglighet**. Om personuppgifter utbyts via onlinetjänster ökar kraven på tillgänglighet

För att uppnå säker hantering av personuppgifter utifrån säkerhetsaspekterna insynsskydd, riktighet och tillgänglighet räcker inte Internet utan en säkrare lösning behövs, t.ex. SGSI-nätet

Exempel DDoS-attack

DDoS-attack (Distributed Denial of Service) är ett angrepp i syfte att hindra normal användning av det attackerade systemet/systemen. Den vanligaste angreppstypen är överbelastningsattack som bygger på att en stor mängd anrop, med en relativt liten mängd data, samtidigt och kontinuerligt från flera datorer skickas till ett datorsystem eller nätverk. Överbelastningsangrepp har drabbat flera olika sektorer såsom myndigheter, banker, massmedia och spel- och vadslagningsföretag, ofta med inslag av utpressning.

Med avseende på säkerhetsaspekterna:

- **Insynsskydd**. DDoS-attack syftar inte till att komma åt data utan att överbelasta systemet. Så ur den aspekten är risken liten
- **Riktighet**. Vid attacken skickas mycket som kan betraktas som ”skräptrafik”, men i övrigt påverkar det inte riktigheten
- **Tillgänglighet**. Just den här säkerhetsaspekten är den man vill komma åt vid en DDoS-attack. Det handlar om överbelastning av nätverket vilket ibland kan leda till att det kollapsar

SGSI-nätet har hög grad av säkerhet när det gäller tillgänglighet och är i det här fallet en säker lösning för att undvika hackerattacker

[8] https://www.msb.se/sv/Produkter--tjanster/SGSI---Swedish-Government-Secure-Intranet-/

5 Behovsinventering

5.1 Bakgrund

Behovsinventeringen har genomförts i formen av möten med representanter för myndigheter och kommuner, dels fysiska möten och dels via Skype. Det som varit uppe till diskussion på dessa möten har till största delen haft fokus på säkert informationsutbyte, men även till en del kring redundans. Inriktningen vid dessa möten har varit utifrån användandet av geodata, även om flera av aktörerna hanterar annan samhällskritisk information. En risk som diskuterades i ett tidigt skede var att en allt för detaljerad sammanställning skulle kunna avslöja sårbara verksamheter, informationssystem etc. i samhället. Därav kommer denna rapport inte att innehålla en redovisning på detaljnivå.

5.2 Säkert informationsutbyte

5.2.1 GENERELLT

Det finns ett stort spann mellan behoven av säkert informationsutbyte hos myndigheterna. Högsta kraven har Försvarsmakten och Polisen där kraven på säkert informationsutbyte är höga för all information. De vill också ha data från källan och helst då online, vilket i sig ställer högre krav. Å andra sidan finns det myndigheter med ringa behov av säkert informationsutbyte och där utbytet av geodata till stor del handlar om nedladdning och därefter lagring lokalt på myndigheten. Däremot har det visat sig att även om en enskild myndighet inte har egna behov av säkert informationsutbyte kan andra myndigheter ha de kraven på den myndigheten då de ska utbyta information.

Det finns även författningar som ställer krav och NIS-direktivet[9] omfattar verksamheter som levererar samhällsviktiga tjänster och digitala tjänster och genomfördes under 2018 i Sverige. Direktivet innebär krav på informationssäkerhet och incidentrapportering för leverantörer av samhällsviktiga och vissa digitala tjänster. Dessutom har ett antal myndigheter tillsynsansvar kopplat till den nya regleringen. MSB har en bred roll kopplat till regleringen som bland annat innefattar föreskriftsrätt, samordning och mottagare av incidentrapporter.[10]

Av de datateman som det ställs högst krav på är de som innehåller personinformation genomgående det mest kritiska. Fastighetsinformation rent generellt är också något som har högre krav och då oftast genom att de innehåller personinformation, direkt eller indirekt. Högre krav har också information om skyddsobjekt, ledningsinformation (främst dricksvatten) samt vissa sammansatta eller aggregerade informationsmängder.

Kommunerna har idag små möjligheter till säkert informationsutbyte när det gäller geodata, detta för att de bl.a. inte haft samma tillgång till samma tekniska lösningar som myndigheter har samt att det är förenat med stora

[9] https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32016L1148&from=EN
[10] MSBFS 2018:7

kostnader. Behoven finns men de har andra stora behov inom kommunerna att lösa och deras resurser är begränsade. Dessutom har de oftast få resurser med kompetens inom tjänsteutvecklingsområdet och är då beroende av systemleverantörer och andra konsulter. Det är visserligen tekniskt möjligt att ansluta 290 kommuner med unika kopplingar till SGSI, men en effektivare lösning vore att sammanslutningar av flera kommuner hade en gemensam koppling till deras infrastruktur.

5.2.2 NÅGRA VIKTIGA PUNKTER

• Utifrån säkerhetsaspekterna Insynsskydd (konfidentialitet), Riktighet och Tillgänglighet dominerar den senare, tillgängligheten, i samtalen vi haft.

- Insynsskydd kommer mest på tal när direkt eller indirekt personinformation eller utbyte av information som är relaterad till Försvarsmakten
- Riktighet gäller de flesta datateman och handlar inte bara om aktuella och riktiga data utan även att olika tillämpningar blir uppdaterade så att det inte blir missmatch och att dialog förs utifrån olika utgångspunkter eller att blåljuspersonal åker fel väg etc. Att ha tjänster online som läser från källan är ett sätt att minimera dessa problem, men ställer då ökade krav på tillgänglighet…
- Tillgänglighet handlar enligt definition i MSB:s modell för informationsklassning om att informationstillgångar skall kunna utnyttjas i förväntad utsträckning och inom önskad tid. Det är och kommer fortsatt att vara en utmaning då samhället mer och mer går mot onlinetjänster

• Utöver själva utbytet är det viktigt att säkerställa att alla parter som medverkar vid t.ex. en krissituation använder samma versioner av information. Då blir det viktigt att veta vem som är ansvarig att ta fram och tillhandahålla informationen. Det är också viktigt att veta vilka verktyg som ska användas och vilka versioner av verktygen som gäller

• För att effektivisera tillgängliggörandet av geodata bör det finnas en gemensam teknisk lösning där tillhandahållandet sedan kan göras via tjänster ut till landets myndigheter och kommuner. Som det är idag tar flera myndigheter hem geodata och gör sina egna kartor. I stället borde de kartorna finnas på ett ställe för nedladdning eller visning

• Krav på säkert informationsutbyte är olika mellan myndigheter och därför är dialogen mellan beställare och leverantör central eftersom det är viktigt att de ligger på samma säkerhetsnivå

• Informationsklassning är viktig och ska göras med utgångspunkt i vilka konsekvenser det medför om informationen skulle hanteras felaktigt, för-

svinna, komma i orätta händer m.m. Vid framtagande av nya data, sammanställningar av data eller liknande bör alltid informationsklassning genomföras [11]

• För kommuner är stöttning i användandet viktigt för att de ska kunna nyttja tjänster och stöttning ska finnas även i förvaltningsfas, inte bara under utveckling och lansering. Kommunerna är mångt och mycket beroende av systemleverantörer, vilket är dyrbart, och det blir hela tiden en prioritering av kommunens pengar och just geodata har inte högsta prio

• För kommunernas del har det fram till 2019 inte funnits någon möjlighet att koppla upp sig mot en teknisk lösning för säkert informationsuybyte och det har försvårat säkert utbyte av geodata. Om flera kommuner går ihop i ett nätverkskluster skulle de kunna ha en gemensam koppling för utbyte av geodata, vilket borde bli effektivt och kostnadsbesparande. Ett exempel på detta finns hos Länsstyrelserna. Där är Länsstyrelsen i Västra Götaland en nod och de tar hem allt geodata för vidare spridning/användning av landets övriga Länsstyrelser via sitt eget Lst-net

• Det finns även behov av säkra förbindelser när t.ex. kommuner ska leverera information till Lantmäteriet. Ett exempel kom från en kommun där ett informationsutbyte sker av ortofoton som de tar fram i egen regi och som sedan ska utbytas med Lantmäteriet. Där ingår information relaterad till Försvarsmakten som gör att säkerheten på utbytet bör höjas. Det är dessutom olika säkerhetsnivå på utbytet med högre nivå från kommunen till Lantmäteriet än åt andra hållet. Ett annat exempel är de 39 Kommunala Lantmäterimyndigheterna som arbetar i samma system som den Statliga Lantmäterimyndigheten och där bl.a informationsutbyte av personinformation hanteras. Dessa båda exempel belyser behov av ökade krav på säkert informationsutbyte

5.3 Redundans

5.3.1 REDUNDANS VID KRISLÄGEN

Behovet av dubbla eller flerdubbla lösningar kan variera beroende på verksamhet och är inte heller avhängigt av att redundansen ska bestå av en annan nätverkslösning om den ordinarie är obrukbar. I vissa krislägen kan det vara så att nätverk, elförsörjning eller annan infrastruktur inte är tillgängligt och ordinarie informationssystem och nätverk således är utslagna. Då kan analoga varianter vara det redundanta alternativet, det kan t.ex. vara tryckta kartor.

För t.ex. Försvarsmakten är tryckta kartor en självklarhet, det går inte att enbart ha digitala lösningar vid ett krisläge och på platser med dålig nätverksförbindelse. Även blåljusverksamheten har behov av redundanta och ibland analoga lösningar. T.ex. i samband med de stora skogsbränderna 2018 var behovet stort av ständigt uppdaterade och tryckta kartor. För

[11] https://www.msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/Modell-for-klassificering-av-information---rekommendationer/

brandmännen ute i fält fungerar det bäst med en tryckt karta i benfickan jämfört med en karta i en app.

Vid krislägen, om t.ex. Internet eller andra nätverk inte är tillgängliga, kan även fysiska leveranser av data ersätta de API:er som då är obrukbara. En myndighet sade att de vid ett sådant krisläge helt enkelt kan ta data på en extern hårddisk eller USB-minne och leverera till den kund/organiastion som har behov av data.

5.3.2 REDUNDANS I FORM AV DUBBLA NÄTVERKSLÖSNINGAR

Även om vi inte fått in så många behov kring dubbla nätverkslösningar så finns givevis de behoven. Ett exempel är Lantmäteriets positioneringstjänst SWEPOS där ökande krav och anpassningar till nya tillämpningar måste hanteras. På senare tid har kraven ökat på grund av s.k. autonoma fordon där tillgänglighetskraven är stora samt att denna realtidstjänst ska vara tillgänglig dygnet runt under 365 dagar om året. För SWEPOS ska redundans införas så att tjänsten levereras via dubbla nätverkslösningar vilka driftas från olika orter. Denna lösning underlättar också i samband med de planerade servicetillfällen som kan innebära kortare avbrott.[12]

För att uppnå redundans i geodataförsörjningen för all geodata på nationell nivå och på en massmarknad krävs stora investeringar i infrastruktur. I den här rapporten ligger fokus på informationsutbyte mellan myndigheter och kommuner och ett informationsutbyte på en massmarknad kräver i sig en vidare utredning.

6 Säkra nätverk

6.1 Generellt

Vi har i vårt arbete fokuserat på SGSI-systemet för informationsutbyte av geodata, bl.a. därför att det rekommenderas av Geodatarådet samt används av flera myndigheter. Det presenteras särskilt nedan.

Kommuner och regioner har tillgång till och utvecklar även säkra nät. De är inte utvecklade för att hantera geodata utan används främst för meddelanden, sjukjournaler etc. Därför går vi inte in på dessa system i detta arbete. Dock har kommuner och regioner nätverkskluster där de gått ihop för informationsutbyte samt av effektiviseringsskäl. Sådana kluster skulle kunna vara intressanta för att nå flera aktörer via en nod i SGSI. Mer om det i kap 7.1.4. Vi går heller inte in på nätverk som används av Försvarsmakten utan beskriver kort ett par andra systemlösningar, RAKEL och WIS.

RAKEL (RAdioKommunikation för Effektiv Ledning) är ett system för radiokommunikation som främst används av säkerhetsorganisationerna och blåljusorganisationerna i Sverige. Användare är även myndigheter, länsstyrelser, kommuner, regioner, energibolag och frivilligorganisationer som t.ex. Sjöräddningen.

[12] https://www.lantmateriet.se/sv/Kartor-och-geografisk-information/GPS-och-geodetisk-matning/Swepos/

RAKEL är utvecklat för att säkra hög täckningsgrad och robusthet och underlättar samverkan mellan aktörerna, såväl i det dagliga arbetet som vid större krissituatioer. RAKEL är inte direkt utvecklat för att leverera geodata men i nästa generation av systemet, som håller på att utvecklas, kommer större datamängder att kunna överföras, bl.a. bildfiler. [13]

WIS (Webbaserat informationssystem) är ett verktyg för informationsdelning mellan aktörer i det svenska krishanteringssystemet. WIS underlättar för aktörer att dela information före, under och efter samhällsstörningar och syftet är att, utifrån samlade lägesbilder, skapa överblick och helhetssyn i samband med kris.

WIS används av organisationer såväl som privata aktörer och varje aktör äger sin egen information och väljer själv vilka man vill dela den med. Kommunikationen över internet är krypterad men WIS är dock inte utvecklat för att hantera sekretessbelagd information. [14]

6.2 SGSI

6.2.1 BAKGRUND

SGSI (Swedish Government Secure Intranet) är en tjänst för säker kommunikation mellan myndigheter i Sverige och i Europa. SGSI är sammankopplat med det skyddade nätverket TESTA (Trans European Services for Telematics between Administrations) och det skapar möjlighet att utbyta information med andra EU-stater (Schengenområdet). SGSI förvaltas av MSB och finansieras via avgifter som ska balansera de kostnader som finns.[15]

SGSI:s infrastruktur är avskild från Internet och påverkas av den anledningen inte av de störningar som kan förekomma på Internet. Mellan anslutna myndigheter sker trafiken punkt till punkt i så kallade VPN-tunnlar som krypteras med försvarsmaktens krypto. För att en myndighet ska kunna bli ansluten måste de ha en ackreditering, detta för att skapa förtroende för hur de hanterar informationssäkerheten.

Ackrediteringskraven för de som ska ansluta sig handlar om att ha ordning på sitt arbete med IT-säkerhet. Kraven bygger på den internationella standardserien SS-ISO/IEC 27000. Där 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

6.2.2 ANVÄNDNING

SGSI används sedan flera år för informationsutbyte mellan myndigheter och användningen ökar succesivt. Från och med 1 januari 2019 finns också

[13] https://www.msb.se/sv/Produkter--tjanster/Rakel/Om-Rakel/
[14] https://www.msb.se/sv/Produkter--tjanster/WIS/
[15] https://www.msb.se/sv/Produkter--tjanster/SGSI---Swedish-Government-Secure-Intranet-/

möjlighet för kommuner och regioner att ansluta sig. SGSI används av myndigheter som en säker förbindelse för utbyte av känslig information och minskar därmed IT-säkerhetsrisker som hot och sabotage från enskilda personer, organiserad brottslighet eller främmande makt. I takt med ökad användning kommer MSB att utveckla SGSI och bl.a. öka kapaciteten på nätet.

I behovsinventeringen för detta uppdrag har det framkommit att alla myndigheter inte har behov av att utbyta information via ett säkrare nätverk än det öppna Internet. Det ska ses mot medskick från andra myndigheter som menar att SGSI borde vara obligatoriskt för alla myndigheter! I Nationell Geodatastrategi 2016-2020 finns en målformulering om att: *Säkerställa att geodataproducerande myndigheter kan erbjuda redundant och säker åtkomst till geodata via SGSI-nätet.*[16]

I betänkandet av 112-utredningen tas också användandet av SGSI upp. Bland annat påpekas det att när information med hårdare säkerhetskrav ska hanteras kan t.ex. SGSI-nätet väljas för informationsdelning och informationsutbyte mellan hjälporgan och den nationella alarmeringsfunktionen.[17]

7 Lösningsförslag

7.1 Rekommendationer

7.1.1 SGSI

Vår rekommendation är att myndigheter och kommuner bör använda SGSI där säkert informationsutbyte krävs utifrån ett robusthetsperspektiv. När det gäller informationsutbyte som innefattar personinformation, direkt eller indirekt, är vår rekommendation att användning av SGSI bör vara obligatoriskt. Information relaterad till Försvarsmakten (s.k. skyddsobjekt) kräver högre säkerhetsklassificering vilket inte SGSI kan hantera i nuläget.

Detta är dock en fråga där stora insatser krävs för att uppnå mål 3d i Nationell Geodatastrategi 2016-2020 och vår rekommendation är att frågan utreds vidare..

Vid informationsutbyte kan det vara att en myndighet har behov av säkra lösningar för utbytet medan den andra myndigheten inte har samma behov. Då måste i alla fall båda myndigheterna uppfylla kraven för ackreditering eftersom de behöver ligga på samma säkerhetsnivå. Det ska samtidigt ses som något positivt då det handlar om att uppfylla kraven för IT-säkerhet.

[16] https://www.geodata.se/globalassets/dokumentarkiv/styrning-och-uppfoljning/geodatastrategin/nationell_geodatastrategi_2016-2020.pdf
[17] SOU 2018:28 En nationell alarmeringstjänst – för snabba, säkra och effektiva hjälpinsatser

7.1.2 INFORMATIONSKLASSNING

Grundläggande i arbetet med informationssäkerhet är att varje organisation gör en informationssäkerhetsklassificering. Klassificeringen av informationen bygger på att den klassificeras utifrån den funktion och betydelse för verksamheten som den har och de konsekvenser det medför om informationen skulle hanteras felaktigt, försvinna, komma i orätta händer etc. bestämmer skyddsnivån för respektive informationsmängd. Detta är ett löpande arbete och ska göras när nya krav kommit på informationen, när nya informationshanteringssytem införs, i samband med framtagande av nya data, sammanställningar av data eller liknande.

7.1.3 INFORMATIONSSÄKERHET

För att ett säkert informationsutbyte ska vara tillförlitligt räcker det inte bara med fokus på tekniska lösningar, det ställer höga krav på både leverantör och mottagare av informationen. Vår rekommendation är att respektive organisation arbetar med informationssäkerhet på ett strukturerat sätt som bygger på den svenska och internationella standardserien SS-ISO/IEC 27000.

En viktig del i ackrediteringen för att få ansluta sig till SGSI är att organisationen öppet redovisar sitt informationssäkerhetsarbete i stort, samt mer i deltalj om säkerheten kring anslutningen till just SGSI.

7.1.4 TEKNISK LÖSNING FÖR KOMMUNER

Kommuner har inte tidigare haft tillgång till SGSI-nätet men kan efter 1 januari 2019 ansöka om tillgång. Ett problem de flesta kommuner har är dock resurser och kompetens att genomföra detta helt och fullt, i den problematiken ligger också att krav för ackreditering ska vara uppfyllda. Kommunsamverkan där flera kommuner är sammankopplade med sina nät i ett kluster kan vara en lösning om en av dessa kommuner fungerar som en nod för att via SGSI utbyta geodata. Det skulle både effektivisera och bli kostnadsbesparande för alla parter.

Länsstyrelserna har i praktiken en liknande lösning för geodata, även om de idag inte har en SGSI-anslutning för det. De tar hem geodata till Länsstyrelsen i Västra Götaland och därifrån sprids sedan data via Lst-net till övriga länsstyrelser i landet.

7.1.5 GEMENSAM LÖSNING

Sveriges myndigheter och kommuner borde ha en gemensam lösning för säkert informationsutbyte av geodata. Grunden bör vara att tillgängliggöra geodata via nedladdnings- och visningstjänster samt e-tjänster. Där så krävs även fysisk leverans repektive analogt material.

7.1.6 TÄNK BREDARE

I arbetet bör inte bara vardagens problem hanteras utan även tänka in om det händer större kriser, krigshot etc. Även om åtkomst via onlinetjänster direkt vid källan ur flera aspekter är att föredra måste konsekvenserna vid en stor och/eller långvarig driftstörning belysas och hanteras.

Teknik går sönder, människor gör fel, risken för långvariga elavbrott är ökande, omvärldsrisker i form av hot från främmande makt ökar.

Oavsett om kommunikationen går via det öppna Internet, via SGSI eller hyrda förbindelser kommer tillgängligheten ibland vara obefintlig.