LANTMÄTERIET

Geodata
SVERIGE BIT FÖR BIT

2019-04-25

Dnr: LM 2019/001170

RAPPORT GEODATARÅDETS HANDLINGSPLAN 2018

Aktivitet – Informationssäkerhet och Totalförsvar

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

Innehållsförteckning

Sammanfattning

Inom informationssäkerhetsområdet sker ständiga förändringar i hotbilder, mänskligt synsätt och medvetenhet samt tekniska utmaningar. Det betyder att information kan ha olika värde vid olika tidpunkter beroende bland annat på förändringar i omvärlden vilket för med sig att en bedömning om tekniska och administrativa lösningar för att skydda information måste analyseras och bedömas kontirnuerligt.

Risk och sårbarhetsanalyser måste göras om vid förändringar av lösning eller förändringar i omvärlden som kan påverka lösningen menligt.

För syftet att kunna dela information som inte är helt öppen finns ett antal behov som idag inte finns tillgängliga lösningar för. Det största behovet är en sammanhållen lösning för att säkert kunna identifiera konsumenter som vill ta del av informationen.

En lösning för att stödja den digitala samhällsbyggnadsprocessen som har till syfte att dela information till medborgare, myndigheter och företag kan inte skyddas på ett sätt som möjliggör hantering av säkerhetsskyddsklassificerade uppgifter inom lösningen.

1 Inledning och bakgrund

Uppdraget utgår från den Nationella geodatastrategin och geodatarådets handlingsplan för 2018-2020. Uppdraget ingår i fokusområdet Öppenhet och säkerhet.

För att ta hand om säkerhetsaspekterna i Lantmäteriets uppdrag har ett delprojekt handlat om vilka säkerehetsaspekter som måste tas om hand och hur man ska kunna samarbeta kring detta.

1.1 Informationssäkerhet

All information har inte samma behov av skydd och därför är informationsklassificering en grundläggande aktivitet i säkerhetsarbetet. Syftet med informationsklassificeringen är att genom konsekvensanalys identifiera skyddsbehovet för informationstillgångar.

Myndigheten för samhällsskydd och beredskap (MSB) tillhandahåller metodstöd för informationssäkerhet. I det metodstödet ingår även en model för informationssäkerhetsklassificering. Modelen är välkänd inom Myndighetssverige. Vissa myndigheter använder den som den är och vissa myndigheter har gjort anpassningar till sin verksamhet.

1.2 Säkerhetsskydd

Inom säkerhetsskydd är bedömningen att erfarenheterna och kunskapsnivån rent allmänt i den civila sektorn inte är lika hög. Detta innebär att man inte har förståelse för vilka långtgående åtgärder som krävs om information klassas som säkerhetsskyddade uppgifter.

2 Intressenter

2.1 Delatagare

Inledningsviss skulle arbetsgruppen bestå av delagare från olika myndigheter och ledas av representanter från Lantmäteriet. Detta visade sig dock var svårt då viss osäkerthet kring informationsmängder som skulle ingå fanns. Efter den Proof of Concept som genomförts i andra delar av projektet, förändrades inrikningen och arbetsmetoden.

Då förändrades arbetsgruppen till att bestå av Lantmäteriet enbart.

3 Tillvägagångssätt

Projektet valde att använda Proof of Concept (PoC) metod för att komma fram till resultaten.

PoC begränsades till tillhandahållande av detaljplaninformation

3.1 Informationssäkerhet

Lantmäteriet har lång erfarenhet av att jobba med informationssklassningar. Vi valde detaljplaniformation för att göra en Prof of Concept, i det ingick:

- Klassificering av detaljplaninformation enlgt MSB:s modell för informationsklassificering.
- En risk- och sårbarhetsanalys användes för att identifiera vilka risker som finns när en datavärd tillgänliggör av olika myndigheters information information.

3.1.1 MSB:S MODELL

Klassificering av information görs utifrån flera kriterier. De kriterier som tas upp i ISO/IEC 27000-serien är värde, legala krav, känslighet och betydelse för organisationens verksamhet. Även andra kriterier kan dock vara relevanta för den egna organisationen.

I modellen klassificeras information utifrån de konsekvenser som oönskad påverkan på informationens kvalitet bedöms leda till. Konsekvenserna värderas i termer av oönskad påverkan på verksamheten eller annan part till följd av:

- Konfidentialitet
- Riktighet

- Tillgänglighet.

Om exempelvis organisationen lider allvarlig skada av att viktig information för verksamheten blir tillgänglig för obehöriga, ska informationen placeras i en klass med hög konsekvensnivå avseende konfidentialitet.

Säkerhetsaspekt Konsekvensnivå	Konfidentialitet	Riktighet	Tillgänglighet
Allvarlig	Information där förlust av konfidentialitet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Betydande	Information där förlust av konfidentialitet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Måttlig	Information där förlust av konfidentialitet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Ingen eller försumbar	Information där det inte föreligger krav på riktighet, eller där förlust av riktighet inte medför någon eller endast **försumbar** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där det inte föreligger krav på konfidentialitet, eller där förlust av konfidentialitet inte medför någon eller endast **försumbar** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där det inte föreligger krav på tillgänglighet, eller där förlust av tillgänglighet inte medför någon eller endast **försumbar** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild.

3.1.2 INFORMATIONSKLASSNING

Informationsklassningen gjordes alltså på den detaljplaneinformation som ingick i Proof Of Concept enligt MSB:s modell.

För dessa informationsmängder framkom höga krav på riktighet, i övrigt inga högre krav.

Inom andra så kallade teman (informationsmängder) förväntas dock kraven på informationssäkerhet vara högre, varför denna informationsmängd inte kan anses dimensionerande.

3.1.3 RISK OCH SÅRBARHETSANALYS

Efter informationsklassning gjordes en påbörjades en risk och sårbarhetsanalys (RSA) för informationen för att få fram dimensionerande säkerhetskrav på en tänkt lösning baserat på informationsklassning. Denna blev dock väldigt osäker då tänkt lösning inte var särskilt tydlig.

3.2 Säkerhetsskydd

Här har vi varit lite i osynk med verkligheten eftersom en ny Säkerhetsskyddslag träder i kraft den 2019-04-01. Under tiden projektet har löpt har

ny information och nya föreskrifter kommit, den senaste var Säkerhetspolisens föreskrifter som kom 2019-03-06.

Vi har analyserat förutsättningarna för att hantera säkerhetsskyddade uppgifter i en lösning som bygger på datavärdssskap utifrån den kommande lagstiftningen och föreskrifter kopplade till densamma.

4 Förutsättningar, krav och antaganden

4.1 Informationsmängder

Eftersom det under projektets gång inte varit tydligt exakt vilka informationsmängder som är avseedda att att ingå utan det har utretts parallelt, så har vi riktat in oss på en modell hur vi ska hantera informationsmängder som är tänkta att ingå.

Det innebär att vi har använt oss av detaljplane informationen som ingått i den PoC som gjorts.

4.2 Informationssäkerhet

När man arbetar med informationssäkerhet är centrala frågeställningar vem eller vilka som har rätt att ta del av information, förändra information och när information ska vara tillgänglig. Här har först och främst de två första belysts, då tillgänglighetsapekten till stor del hanterats i ”Redundans i geodataförsörjningen”.

4.2.1 ÅTKOMST

För att informationska som inte är helt öppen ska kunna hämtas från flera olika teman och oberoende av vem som är datavärd för informationen behöver en gemensam källa för användaridentitet användas. Denna centrala källa är något som saknas idag.

4.2.2 AUKTORISATION

Om informationen inte ska vara tillgänglig för alla som har en användare i systemet, måste en mekanism finnas för att avgöra om en användare är behörig att ta del av informationen i en tjänst.

4.2.3 FÖRTROENDE FÖR INFORMATION

En viktig frågeställning är hur en konsument av information, kan lita på information som levereras från en datavärd, dvs inte direkt ifrån den som är informationsägare och ansvarig för informationen.

Om man endast hanterar informationsmängder som ska konsumeras av människor kan viss del av denna bedömning av förtroende lämnas över till den mänskliga konsumenten. I fallet med datavärdsskap är målsättningen större, dvs det ska innefatta även maskin-maskin kommunikation och maskiner måste ha fasta definerade faktorer för att kunna bedöma förtroende för information för att kunna göra bedömningar.

I samband med denna förtroendefråga för informationen, måste även svar på frågor om kvalitet och aktualitet kunna maskinellt avgöras.

4.3 Säkerhetsskydd

Inom området säkerhetsskydd är möjligheten till aggregering av information en faktor som måste tas i beaktande och som kan påverka den samlade informationens känslighet. Det innebär att varje enskild producents information inte faller inom ramen för säkerhetsskydd, men om man kan kombinera informationen med liknande information från flera producenter så att en överblicksbild kan fås, kan informationen blsäkerhetsskyddsklassificerad.

Denna bedömning om och när aggregerad information blir blir säkerhetsskyddsklassificerade är svår för både producenter och datavärdar att göra.

5 Omvärldsanalys

5.1 Informationssäkerhet

5.1.1 IDENTIFIERING

I Sverige idag finns ett antal mer eller mindre sektorsspecifika lösningar och sammanslutningar för identitetshantering. Ingen av dem har som målsättning att bli en heltäckande identitetslösning för hela Sveriges behov.

Försäkringskassan till handahåller en identitetslösning, MyndighetsCA[1], för att leverera betrodd identifiering. Denna lösning är tillgänglig för myndigheter och det är tjänstelegitimationer som levereras.

SITHS[2] är en annan identifieringstjänst som riktar sig till myndigheter och organisationer, främst inom offentlig förvaltning. Den levereras av Inera och har framförallt en stark marknadsställning inom sjukvårdssektorn.

BankID[3] är den största levernatören av digital identifiering i Sverige idag. Den drivs av ett privat företag, Finansiell ID-Teknik, som samägs av de flesta stora bankerna som verkar på den svenska marknaden. Den riktar sig främst till privatpersoner och alla fysiska personer med ett svenske personnummer kan erhålla en digital idehandling.

5.1.2 AUKTORISERING

Det finns i Sverige idag ett fåtal så kallade federativa lösningar för auktorisering där man kan kontroller vilka rättigheter in viss identifierad användare har i systemet.

Den största federationen är Sambi, vilken är öppen för alla organisationer inom hälso-, sjukvård eller omsorgsområdet.

[1] Försäkringskassans MyndighetsCA https://www.forsakringskassan.se/myndigheter/e-tjanster/myndighets-ca
[2] Ineras identifieringstjänst https://www.inera.se/tjanster/identifieringstjanst-siths/
[3] Finansiell ID teknik https://www.bankid.com/

I övrigt är de flesta fedrationer så kallade två parts federationer, där två parter har kopplat samman för att lita på varandras iidentifikationer och auktorisationer.

5.2 Säkerhetsskydd

5.2.1 NY SÄKERHETSSKYDDSLAG

Sverige har redan sedan tidigare haft en säkerhetsskyddslag, men den kommer att införas i en ny version 2019-04-01. Till denna lag kommer nya föreskrifter och riktlinjer från de båda tillsynsmyndigheterna, Säkerhetspolisen och Militära Underrättels- och Säkerhetstjänsten.

Förändringarna är stora för vad som förväntas av både mydigheter, organisationer och privata företag. Alla aspekter av denna nya lag och medföljande föreskrifter och riktlinjer har inte analyserats då föreskrifterna inte publiserats förrän i slutet av februari 2019.

6 Lösningsförslag

6.1 Informationssäkerhet

Säkerhet handlar i stor utsträckning om förtroende i olika form. Hur mycket man litar på kunskaper, processer och teknik. För att informationsägare ska kunna ha förtroende för att en datavärd hanterar deras information i enlighet med deras krav och önskemål, krävs att man har dokumenterat vilka skyddsåtgärder man vidtagit för att säkerställa att informationen är densamma som skickades till datavärden och att den inte kan förändras eller spridas till obehöriga.

6.1.1 INFORMATIONSKLASSNING

Eftersom man juridiskt kommit fram till en lösning där informationsägarskapet ska ligga kvar hos producenten och inte hos den som tillhandahåller informationen måste informationsklassning göras av producenten. Detta bör sedan ligga till grund för de krav på teknisk och administrativt skydd som datavärden ska erbjuda. Om datavärden ser stora skillnader i hur olika konsumenter klassar liknande information, bör samordningsmöten initieras av datavärden.

Som datavärd måste man dock beakta informationsklassificeringen och ha en diskussion med producenten för att bedöma informationen ur ett säkerhetsskyddsperspektiv.

För att uppnå en gemensam syn på informationklassning och informations värde bör MSB få i uppdrag att utbilda deltagande myndigheter inom

6.1.2 RISK OCH SÅRBARHETSANALYS

För att en RSA skall vara framgångsrik och ge svar på frågor som syftar till att få fram en balanserad säkerhetslösning för informationshanteringen, både teknisk, administrativ och processmässig krävs att den tänkta lösningen är väldefinierad.

En RSAbör göras på tänkt lösning när en sådan är framtagen och väl specificerad. Den bör då kopplas till de informationsklasser informationen som ska hanteras i lösningen ställer krav på och en ny RSA bör inte behöva göras om inte nya informationsmängder med högre krav än tidigare information tas in i lösningen.

6.1.3 IDENTIFIERING AV PRODUCENT

För att kunna tillgängliggöra information via en datavärd måste information kunna laddas upp till datavärden. För att inte vem som helst ska kunna ladda upp information måste naturligtvis producenten identifiera sig innan uppladdning kan ske.

Antalet uppladdande källor är relativt begränsade och de är alltid väl kända. Detta innebär att en mer konventionell metod för identitetshantering kortsiktigt kan användas. För detta mönster bör datavärden stå för identiteten som sedan används av producenten vid uppladdning.

Långsiktigt bör dock även denna lösning luta sig mot en nationell lösning för identifiering.

6.1.4 IDENTIFIERING AV KONSUMENT

För att kunna hantera information som inte är helt öppen krävs att en lösning för identifiering av användare ska finnas. Denna lösning måste hantera identifiering på ett sådant sätt att gränssnitten som tillgängliggör informationen, beroende av informationens klassificering med tillräckligt stor sannolikhet kan lita på identifieringsinformationen.

Eftersom flera olika myndigheter kommer att agera datavärd eller leverantör av information till samhällsbyggnadsprocessen krävs en identitetsutfärdare som alla dessa kan lita på. Detta är något som inte finns idag, det närmaste som finns i Sverige idag är BankID som dock har den stora begränsningen att av att bara vända sig till fysiska personer med svenskt personnummer. Denna identifieringslösning stödjer alltså inte maskin-maskin vilket gör att inte är lämplig.

Långsiktigt måste lösningen bli att föreslå att någon myndighet bör få ansvar för att ta fram en heltäckande lösning för identifiering av privatpersoner, juridiska personer och system/ting.

För att få en lösning med fungerande datavärdsskap på kort sikt måste en tillfällig lösning på plats. En möjlig lösning är att varje datavärd ger ut identiteter vilket är mindre bra för konsumenter då identiteter från flera datavärdar kan behövas, eller att den myndighet som har samordningsansvar får i uppdrag att utfärda identiteter för användning inom lösningen vilket å andra sidan betyder att alla datavärdar måste lita på samordnarens identietslösning.

Att få en lösning på plats i Sverige för gemensam digital identifiering är en förutsättning för att snabbare kunna utbyta information.

6.1.5 AUKTORISATION

Att få till en gemensam lösning för att ge tillgång till tjänster hos olika myndigheter som inte är öppna bedöms vara ett komplext och tidskrävande arbete. Lösningen för överskådlig framtid bör vara att varje datavärd ger tillgång till sina tjänster, vilket också innebär att ansvaret att följa upp vilka som har tillgång till tjänster ligger hos respektive myndighet som aggerar datavärd.

Här bör man följa vad som händer inom DIGG:s uppdrag ”Säkert informationsutbyte”. Inom det uppdraget är dessa frågor under utredning.

6.1.6 FÖRTROENDE FÖR INFORMATION

Säkerhet handlar om tidigare konstaterats i hög grad av förtroende. I Sverige idag har medborgare stort förtroende för statlig myndigheter och organisationers information. Detta betyder att man inte ifrågasätter om informationen är korrekt. Om man även framgent ska kunna behålla detta förtroende är det viktigt att man kan visa att informationen är korrekt, speciellt eftersom en datavärd inte är tänkt att vara ansvarig för informtionen som levereras.

Mänskliga konsumenter kan bedöma förtroende på ett antal olika grunder medan en maskin endast kan hantera inlärda mönster att agera på. Detta innebär att lösningen måste innehålla någon form av signering eller möjlighet till maskinell validering.

Hur denna signering eller validering ska ske är väldigt beroende av hur informationen ska se ut vid lagring och leverans. Den tekniska lösningen bör dock beakta detta.

6.1.7 ÖVRIGA SKYDD

De övriga skyddsåtgärder som krävs för att skydda informationen när den ligger hos datavärden ankommer på de enskilda datavärdarna. Vilka tekniker och lösningar som används beror på kunskap, historiskt valda lösningar och befintliga processer hos datavärden. Utgångspunkten är att det ofta är säkrare att använda sig av befintliga lösningar för skydd än att införa nya som man inte har lika stor kunskap och erfarenhet av., om lösningarna syftar till att lösa samma uppgift.

Även inom detta område har planerar MSB att under hösten 2019 släppa en fastställd vägledning för grundläggande IT-säkerhetsåtgärder.

6.2 Säkerhetsskydd

3 kap. 5 § i säkerhetsskyddsförordningen (2018:658) är tydlig med att uppgifter som omfattas av säkerhetsskydd under transport utanför kontrollerat nätverk, måste skyddas med hjälp av en kryptografisk lösning som godkänts av Försvarsmakten. Det innebär i praktiken att någon form av signalsskydd måste anavändas för att skydda informationen under transport.

För denna typ av skydd finns endast en metod för mer generellt skydd av information och det är SGSI. SGSI är å andra sidan endast godkänt för transport av uppgifter som klassats i den lägsta säkerhetsskyddsklassen, ”begränsat hemlig”, för övriga uppgifter finns inte någon generellt godkänd metod tillgänglig. SGSI kan inte heller ses som en generell metod för skydd av informationen då det inte är en allmänt tillgänglig lösning.

Eftersom inga generella metoder för överföring av dessa typer av information finns måste lösningen vara att information klassad som säkerhetsskyddade uppgifter inte får finnas i information som överförs till datavärd eller att uppgifter som kan andvändas som delmängder i en aggregering som klassas som säkerhetsskyddade uppgifter inte ska överöras till datavärd.