Myndigheten för
samhällsskydd
och beredskap

Informationssäkerheten i Sveriges kommuner

Analys och rekommendationer utifrån MSB:s kommunenkät 2015

Informationssäkerheten i Sveriges kommuner

Analys och rekommendationer utifrån MSB:s kommunenkät 2015

Informationssäkerheten i Sveriges kommuner
Analys och rekommendationer utifrån MSB:s kommunenkät 2015

Myndigheten för samhällsskydd och beredskap (MSB)

Verksamheten för cybersäkerhet och skydd av samhällsviktig verksamhet

Redaktör: Christina Goede

Produktion: Advant Produktionsbyrå
Tryck: DanagårdLiTHO

Publikationsnummer: MSB1045 - december 2016
ISBN: 978-91-7383-697-5

Innehåll

Inledning

Inledning

Kommunerna har ett av det svenska samhällets mest komplexa uppdrag. Det omfattar allt från den dagliga omsorgen av äldre till att säkerställa att känslig infrastruktur fungerar. En stor del av den samhällsviktiga verksamheten räknas till kommunernas ansvar. I samtliga delar av uppdraget spelar säker informationshantering en central roll.

MSB har tidigare beskrivit informationssäkerheten i kommunerna bl.a. i rapporten *En bild av kommunernas informationssäkerhetsarbete*[1] som gavs ut 2015. Denna rapport syftar till att ytterligare fördjupa och belysa den problematik som kommunerna står inför när det gäller arbetet med informationssäkerhet. I syfte att stärka informationssäkerheten presenterar rapporten även åtgärdsförslag och rekommendationer för fortsatt arbete.

Rapporten är delvis upplagd efter den struktur som finns i ledningssystem för informationssäkerhet, LIS[2] och omfattar en genomgång av kommunernas informationssäkerhetspolicy, styrdokument och mandat, arbete med riskhantering, stöd och resurser, kompetens och budget. Vidare analyseras även rapportering, incident- och kontinuitetshantering och samverkan.

Rapporten tar även kort upp kommunernas upphandling, arbete med att säkra industriella informations- och styrsystem (SCADA) samt införandet av det s.k. Domain Name Security Extension, DNSSEC.[3]

1. En bild av kommunernas informationssäkerhetsarbete 2015, MSB943.
2. SIS Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav (ISO/IEC 27001:2006, IDT).
3. DNS är ett system för adressering av datorer på IP-nätverk. DNSSEC är en utvidgning av DNS-systemet som syftar till att öka säkerheten i DNS och förhindra missbruk där man lurar DNS-systemet med falsk information.

Tidigare arbete

På uppdrag av regeringen genomförde MSB, i samverkan med Sveriges kommuner och landsting (SKL) en undersökning av informationssäkerheten i kommunerna. I december 2015 lämnade MSB in rapporten *En bild av kommunernas informationssäkerhetsarbete 2015* till regeringen.

Över 230 kommuner svarade på enkätfrågor om systematiskt informationssäkerhetsarbete. Resultatet av undersökningen ger en god bild av de brister som finns i kommunernas informationssäkerhetsarbete. I undersökningen framkom många intressanta resultat, bl.a.:

- Över 70 % av kommunerna arbetar inte systematiskt med informationssäkerhet.
- Över 55 % av kommunerna har ingen process för rapportering och hantering av säkerhetsbrister eller incidenter med koppling till informationshanteringen.
- Nära 60 % av kommunerna anger att det inte finns kontinuitetsplaner framtagna för att hantera bortfall av information i kritiska verksamhetsproceser inom kommunen.
- Över 40 % av kommunerna anger att de inte har någon utpekad funktion för informationssäkerhet. Av de som har en funktion svarar 70 kommuner att den utpekade funktionen för informationssäkerhet arbetar mindre än 10 % av sin arbetstid med informationssäkerhet.
- En fjärdedel av kommunerna har inte en beslutad informationssäkerhetspolicy.
- 40 % av kommunerna gör ingen riskanalys avseende informationssäkerhet.
- Nära 60 % av kommunerna uppger att de inte använder en metod för informationsklassning

MSB har sett behov av fördjupad analys utifrån enkätsvaren som kommunerna lämnade 2015, för att ytterligare belysa problematiken och kunna ge rekommendationer. Denna analys sker i denna föreliggande rapport.

SKL:s undersökning e-förvaltning och e-tjänster

SKL genomförde 2011 en undersökning kallad ”E-förvaltning och e-tjänster i Sveriges kommuner 2011”. I SKL:s undersökning hade mindre än en tredjedel av de svarande 190 kommunerna utsett ansvariga för ledning och samordning av informationssäkerhetsarbetet. En lika stor andel av kommunerna hade tagit fram en informationssäkerhetspolicy för att styra arbetet med informationssäkerhet. Detta kan jämföras med den undersökningen som MSB genomförde 2015, då 60 % av kommunerna angav att de hade en utpekad funktion för informationssäkerhet i kommunen och hela 72 % angav att de har en informationssäkerhetspolicy eller motsvarande som är beslutad av kommunens ledning.

Vidare uppgav över hälften av kommunerna att de, år 2011, använde BITS (basnivå för informationssäkerhet) när de tillfrågades om metodik och cirka 20 % av kommunerna uppgav att de arbetade aktivt med informationsklassificering. År 2015 uppgav 18 kommuner (8 %) att de fortfarande använder BITS, medan 45 kommuner angav att de har ledningsstöd för informationssäkerhet, LIS.[4] Hela tre fjärdedelar av kommunerna valde att inte svara på frågan.

4. ISO 27000-serien Ledningssystem för informationssäkerhet.

Informationssäkerhets-policy, styrdokument och mandat

Informationssäkerhetspolicy, styrdokument och mandat

Enkäten visar att en klar majoritet av kommunerna inte arbetar systematiskt med informationssäkerhet. Endast en tredjedel av kommunerna uppger att de tillämpar ett systematiskt arbetssätt i sitt arbete med informationssäkerhet. Även om det finns informationssäkerhetspolicys, så genomförs kontroll och tillsyn av säkerheten i informationssystemen i liten omfattning.

Funktionen som arbetar med informationssäkerheten har i de flesta fall (72 %), en av kommunens ledning, fastställd informationssäkerhetspolicy som stöd i sitt arbete med informationssäkerhetsfrågor. Av de kommuner som svarat att de inte har en sådan policy finns det flera som uppger att de är på gång att ta fram en eller få den beslutad.[5] Av de kommuner som har en policy uppger 40 % att de arbetar med att revidera policyn.

Även om en majoritet av kommunerna har en informationssäkerhetspolicy skiljer sig denna ofta åt t.ex. rörande vad den omfattar och hur gammal den är. En annan skillnad är hur man inom kommunen ser på kommunala bolag, där en knapp majoritet av de kommuner som besvarat enkäten har inkluderat kommunala bolag i policyns omfattning. Det finns också en liten minoritet som har en policy som endast omfattar delar av kommunens verksamhet.

När kommunerna tillfrågas om det finns andra styrdokument som påverkar arbetet med informationssäkerhet så nämns ofta kommunens it-policy, it-säkerhetspolicy, säkerhetspolicy och e-postpolicy. Vidare relateras ofta till instruktioner för olika målgrupper, e-postregleringar, kontinuitetsplaner, internkontrollplan, it-säkerhetsfrågor och frågor kring lagring och skadlig kod etc.

Utifrån den flora av styrdokument som anges, så är det tydligt att kommunerna ser olika på vad ett styrdokument är och även på hur ett styrdokument påverkar informationssäkerhetsområdet. Slutsatsen är att det är svårt att se en likformad och enhetlig struktur hos kommunerna när det gäller styrdokument som påverkar informationssäkerheten.

5. Flera av dessa kommuner hänvisar även till äldre versioner av styrdokument inom området, t.ex. systemsäkerhetsplaner och andra dokument ur FA22/BITS-familjen.

När kommunerna tillfrågas om de resurser som tillsätts för att arbeta med informationssäkerhet har tillräckligt mandat, så svarar bara hälften av kommunerna. Av de som svarar så anser två tredjedelar att mandatet är gott och en tredjedel att mandatet är bristfälligt.

Bedömning och rekommendationer

De flesta kommunerna har en av kommunledningen fastställd informationssäkerhetspolicy, men generellt sett arbetas det inte systematiskt med uppföljning av informationssäkerheten.

Vissa kommuner är tydliga i enkätunderlaget med att det finns stora brister, att det saknas rutiner och utpekat ansvar. Flertalet pekar på att det är en fråga för it-funktionen eller så anses ansvaret för frågorna ligga ute på de olika förvaltningarna. Det kan i det sistnämnda fallet vara så att det i vissa kommuner finns riktlinjer, rutiner, styrande dokument etc. för informationshanteringen ute hos respektive förvaltning utan att det finns en central styrning. Det bedrivs då ett informationssäkerhetsarbete i olika delar inom kommunen utan att det samordnas på ett strukturerat sätt. En viktig del i förutsättningarna för att kunna stödja det systematiska informationssäkerhetsarbetet är att ha en väl etablerad systemförvaltningsorganisation (dvs. en systemförvaltningsmodell med roller, ansvar mm.).

Att det finns en bredd i hur kommunerna arbetar med policydokument och reglering behöver inte vara ett problem. Vad som dock är oroväckande är resultatet att 59 % av kommunerna (141 st) uppger att de inte kontrollerar efterlevnaden av regelverk avseende informationssäkerhet. Detta är problematiskt. Kommunerna kan därmed inte ha kunskap om regelverkens effektivitet och behov av justeringar.

När uppföljning inte sker på en fastställd informationssäkerhetspolicy så är det troligt att det över tid uppstår ett allt större gap mellan de krav som finns i policyn och de faktiska omständigheterna ute i verksamheten. Detta kan exempelvis visa sig genom att åtgärder som vidtas saknar ändamålsenlighet då de inte baseras på kraven eller inte grundar sig på de problem som finns, eller genom att åtgärder inte vidtas trots att de behövs och policyn medför att de borde prioriteras.

Bristen på kontroll av efterlevnad innebär att det kan ifrågasättas om en fastställd informationssäkerhetspolicy medför någon reell höjning av säkerheten. Detta innebär troligtvis att kommunerna har större verksamhetsrisker avseende informationssäkerheten än kom-

munerna är medvetna om. Det innebär också att många kommuner därmed står utan underlag utifrån vilka de kan göra prioriteringar rörande åtgärdsinsatser.

Vad ligger då bakom att uppföljning inte sker? Resurs- och eller kompetensbrist kan vara en förklaring. En annan förklaring skulle kunna vara om det saknas konkreta handlingsplaner för det dagliga arbetet. Handlingsplaner behövs för att implementera policyn i verkligheten.

Rekommendationer:

- Om det inte finns, ta fram en informationssäkerhetspolicy för kommunen!
- Se över eventuella vidtagna åtgärders ändamålsenlighet genom att jämföra dem med kraven i informationssäkerhetspolicyn och omständigheterna ute i verksamheten. Behöver nya åtgärder vidtas? Behöver policyn justeras?
- Ta fram konkreta handlingsplaner, utifrån informationssäkerhetspolicyn, med inplanerade avstämningspunkter där arbetet utvärderas.
- Arbeta systematiskt med uppföljning och kontroll av informationssäkerheten. Genomför regelbunden och frekvent uppföljning på informationssäkerhetspolicyns efterlevnad för att kontrollera om handlingsplanen ger önskad effekt. Har nya omständigheter tillkommit i verksamheten? Behöver fler åtgärder vidtas?
- Se till att även inkludera kommunala bolag i kommunens informationssäkerhetsarbete. Fäst särskild vikt vid de bolag som driver eller direkt understödjer samhällsviktig verksamhet (kritisk infrastruktur).
- Upprätta en gemensam struktur för kommunens styrdokument för informationssäkerhet. Det stärker möjligheten till jämförbarhet.
- Inför en systemförvaltningsorganisation om en sådan inte finns. Säkerställ att roller och ansvar tydliggörs.
- På sikt bör kommunerna se över möjligheten att ta fram gemensamma rekommendationer vad avser en grundläggande struktur för styrdokument på informationssäkerhetsområdet.

Riskhantering

Riskhantering

Riskhantering är en process, vilken innebär att identifiera de risker som finns i verksamheten, analysera dessa och utvärdera och besluta om hur riskerna skall hanteras på bästa sätt. Att ha kunskap om, samt vidta åtgärder för att omhänderta informationssäkerhetsrisker är grundläggande för att kunna förebygga eller minska oönskade effekter som t.ex. läckage av personuppgifter.

Nära 60 % av kommunerna (141 st) uppger att de arbetar systematiskt med riskanalyser avseende informationssäkerhet. Det förhållandevis höga antalet står i kontrast till att enbart lite över 2 % (36 st) av kommunerna uppger att de utför riskanalyser med jämna intervaller. Vidare uppger endast 2 % av kommuner (36 st) att de har en fastställd metod för riskanalys för informationssäkerhet. Flertalet av dessa kommuner är de som även utför riskanalys regelbundet.

När kommunerna tillfrågas om de har någon särskild metod som de använder för sin analys väljer över hälften av kommunerna att inte svara på frågan. Av de som besvarat frågan, svarar 40 % (58 st) att de inte har någon särskild metod.

Kommunerna uppger att riskanalys avseende informationssäkerhet främst sker inom it-verksamhet, social vård och omsorg, skolan och kommunledningen. Intressant är att 48 kommuner anger att de utför riskanalyser för informationssäkerhet hos kommunala industriella informations- och styrsystem.

Enbart en tredjedel av kommunerna anger att det inom kommunen finns ett sätt att omsätta riskanalysens resultat i konkreta åtgärder. Antingen sker det inga riskanalyser alls inom området eller så sker det reaktivt efter att något inträffat.

På frågan hur kommunerna gör för att identifiera risker inom informationssäkerhetsområdet så beskriver kommunerna allt från att det sker i samband med rapporteringen av risk- och sårbarhetsanalysen eller inom ramen för internkontrollplanen till att ”det hanteras när de dyker upp” eller att frågan inte hanteras över huvud taget. Mycket få kommuner uppger att de genomför regelbunden riskanalys för informationssäkerhet. Många kommuner lyfter dock fram att de avser att initiera ett arbete med metod för riskanalys under innevarande år. Det finns också exempel på kommuner där risker är en stående punkt på ledningsgruppens agenda.

Ansvaret för att genomföra riskanalyser ligger ofta på de separata verksamheterna eller hos systemägare/informationsägare och någon samlad bild av informationssäkerhetsrisker finns sällan för hela kommunens verksamhet.

När det gäller informationsklassning, uppgav 42 % (102 st) av kommunerna att det finns en metod för hur klassning utförs i kommunen.

Bedömning och rekommendationer

Enkätundersökningen visar att få kommuner arbetar systematiskt med riskanalyser avseende informationssäkerhet. Antingen genomförs få oregelbundna riskanalyser i allmänhet eller så genomförs sådana analyser först efter att något har inträffat. Om riskhanteringsarbetet inte sker eller sker osystematiskt innebär det i princip att det inte finns någon process för att hantera informationssäkerhetsincidenter. Utöver det så genererar en riskhanteringsprocess som sker på ad-hoc-basis sällan mycket av värde, särskilt då det är mycket svårt att genomföra utvärderingar kopplade till processen och att systematiskt utveckla relevanta säkerhetsåtgärder.

Kommunerna tillhandahåller många olika tjänster som nyttjar eller innehåller känslig information om exempelvis kommunens medborgare. Kommunerna har därför ett stort ansvar för att säkerställa en säker informationshantering. När det gäller kommunernas förmåga att identifiera och analysera risker inom informationssäkerhetsområdet bedömer MSB att det framkommit stora brister. Detta i kombination med att bara en tredjedel av kommunerna anger att det inom kommunen finns ett sätt att omsätta riskanalysens resultat i konkreta åtgärder ger sammantaget en oroväckande bild. Det innebär att huvuddelen av kommunerna sannolikt saknar praktiska förutsättningar för att bedriva en systematisk riskhantering för informationssäkerhet.

Det är en utmaning att integrera riskhantering i en organisations ordinarie processer, särskilt vad avser informationssäkerhet. Här är det särskilt viktigt att identifiera de mest kritiska processerna, inklusive deras stödprocesser. Att med jämna mellanrum göra en risk och sårarhetsanalys enligt krisberedskapsförordningen och MSB:s föreskrifter borde vara miniminivån, men ska en organisation arbeta seriöst med risker, så måste arbetet ske löpande särskilt vad avser kritiska processer. Som en del i uppföljning av arbetet kan t.ex. den egna internrevisionen och dess kontrollplan användas för att se över efterlevnad.

Det är positivt att över 40 % av kommuner har en metod för informationsklassning. Här skulle mer information behövas kring om denna metod används och i så fall hur. Av de kommuner som svarat att de inte har en metod för informationsklassning, så nämns ofta brist på stöd i arbetet med informationssäkerhet samt kompetensbrist som en viktig faktor, men även brist på personella resurser.

Rekommendationer:

- Identifiera vilken information som hanteras i verksamheten. Klassa sedan informationen efter hur allvarliga konsekvenserna skulle bli av bristande informationssäkerhet. Fokusera på den mest kritiska informationen/känsliga informationen som är i behov av höga skyddskrav.[6]
- Etablera och implementera en process för riskhantering och se till att den är spridd inom kommunen.
- Identifiera informationssäkerhetsrisker och bedöm dessa.
- Se sedan till att omsätta riskanalysens resultat i beslut samt konkreta åtgärder. Dessa beslut samt åtgärder bör vara dokumenterade. Detta är särskilt viktigt för de kritiska processerna i kommunen!
- Kommunledningen bör säkra upp så att den blir kontinuerligt informerad om informationssäkerhetsriskerna och hanteringen av dessa, särskilt vad avser samhällsviktig verksamhet i kommunen.
- Genomför riskanalyser vid varje förändring i kommunens kritiska system.

6. Stöd för verksamhetsanalys och identifierande av informationstillgångar finns att finna i Metodstöd för LIS: https://www.informationssakerhet.se/siteassets/metodstod-for-lis/2.-analysera/verksamhetsanalys.pdf

Stöd – resurser, kompetens och budget

Stöd – resurser, kompetens och budget

Resurser

För att uppnå god informationssäkerhet krävs att någon arbetar aktivt med området och som helst har ett utpekat ansvar och mandat. Nära 60 % av de kommuner som svarat uppger att de har en utpekad funktion för informationssäkerhet. Organisatoriskt är funktionen placerad på olika ställen inom kommunens organisation, men vanligast förekommande är antingen inom it-organisationen (it/service), inom räddningstjänsten eller på ledningskontor/kommunledningskontoret.

Det kan tyckas anmärkningsvärt att ett flertal kommuner har placerat informationssäkerhetsansvaret hos räddningstjänst. De frågor som räddningstjänst hanterar traditionellt är koncentrerat till fysiskt skydd, brand, olyckor och kriser. Motiveringen till detta kan variera, men en hypotes är att man valt att lägga informationssäkerhetsarbetet på en av kommunens obligatoriska funktioner.

Funktionen för informationssäkerhet är även i många fall placerad hos it-funktionen (it/service), vilket inte är anmärkningsvärt då de här frågorna traditionellt varit en fråga som handlat om teknik, it- och systemsäkerhet. Samtidigt visar resultatet att en förändring skett och att informationssäkerhetsansvaret hos nästan en tredjedel av landets kommuner är placerad på ledningskontoret på kommunen.

Det är tydligt av svaren i enkäten att ett mycket stort antal varierande titlar används för informationssäkerhetsfunktionen. Detta gör det svårt att bedöma om det enbart är olika namn på samma funktion eller om det finns skillnader i vad funktionen har för ansvarsområde. Variationen i hur funktionen betecknas skulle kunna motivera att man inom området centralt tydliggör vad denna funktion ska kallas och vad ansvaret generellt bör innehålla.

De kommuner som svarat att det inte finns en informationssäkerhetsfunktion inom kommunen (41 %, 102 kommuner) har i enkäten fått en följdfråga kring hur de då hanterar informationssäkerhetsfrågor. Den bild som ges är mycket diversifierad. Informationssäkerhetsfrågan har i de här kommunerna ingen tydlig struktur och har oklara ansvarsförhållanden. Här visar det sig att många av de som svarat på enkäten inte riktigt vet hur det förhåller sig i kommunen utan det görs en hel del antaganden.

Resursens arbetsinsats i tid

Resultatet från den här undersökningen visar, likt tidigare undersökningar, att informationssäkerhetsfunktionen inom kommunen endast förlägger en liten del av sin arbetstid med informationssäkerhetsfrågor. Av de kommuner som svarat att det finns en utpekad funktion uppger nästan hälften av kommunerna att deras utpekade funktion arbetar mindre än 10 % av sin tid med informationssäkerhetsfrågor. Hela 96 kommuner uppger att den utpekade funktionen arbetar 10 % eller mindre av sin arbetstid med kommunens informationssäkerhet. Bara 34 kommuner anger att resursen/resurserna har möjlighet att ägna 50 % eller mer av sin arbetstid till informationssäkerhetsfrågor.

I svaret till enkäten som ingick i MSB:s rapport *En bild av kommunernas informationssäkerhetsarbete 2015*, skrev en kommun följande kommentar:

”Det finns en vilja och ambition att jobba mer ambitiöst med informationssäkerhetsarbetet i kommunen och ledning tycker också detta är av vikt. Dock är det väldigt tufft att avsätta tid för de som ska driva arbetet då dessa personer som regel redan har minst varsitt heltidsjobb med andra sysslor. Troligtvis är detta ett generellt problem i mindre kommuner och även informationsägare/systemägare m.fl. som behöver involveras är svåra att alls boka in tid med för analyser.”

Sett utifrån arbetstid som kan läggas på informationssäkerhetsinsatser så bedömer över 70 % av de svarande kommunerna att funktionens möjlighet att bedriva informationssäkerhetsarbetet är bristfällig, vilket kan ses som att en viktig faktor för ett framgångsrikt arbete – möjligheten att lägga tid på informationssäkerhetsarbetet – inte är på plats.

Kompetens

En informationssäkerhetsutbildning i någon form till medarbetarna har många vinster. Med rätt insatser kan utbildning höja kunskapsnivån vad gäller informationssäkerhet hos de anställda och öka medvetenheten.[7] Kommunens ledning skickar, genom att satsa på informationssäkerhetsutbildningar, tydliga signaler till organisationen om att de ser informationssäkerhetsfrågorna som betydelsefulla och att de förväntar sig att medarbetarna har ett säkert beteende. Utifrån detta är siffran över kommuner som erbjuder medarbetarna informationssäkerhetsutbildning låg.

7. Här rekommenderas att en mätning av kunskapsnivån sker före insats samt efter insats. Detta för att kunna fastställa att en kunskapsökning skett.

Kompetensutvecklingen sker, enligt kommunerna själva, inte på ett strukturerat sätt och i mycket begränsad form. I många fall sker det dessutom mycket liten kompetensutveckling för informationssäkerhetsfunktionen inom kommunen. Kommunerna ser en förbättringspotential vad gäller den utsedda funktionens kompetensnivå, nära 49 kommuner bedömer att dennes kompetens är bristfällig. Svaren visar att det främst beror på avsaknaden av resurser och stöd från ledningen. Kommunen har krav på sig att anordna utbildningar inom flera områden. Informationssäkerhetsutbildningen står då i konkurrens med andra kurser och prioriteras inte.

Flera kommuner nämner i kommentarerna att de önskar externt hjälp och metodstöd för att arbeta vidare med informationssäkerhetsarbetet. Några hänvisar till att de saknar det form av stöd som fanns i FA22[8] eller Basnivå för informationssäkerhet, BITS[9].

Budget

Det är få av de svarande kommunerna som uppger att den utpekade funktionen för informationssäkerhet har en egen budget för att bedriva arbetet. Om medel avsätts till informationssäkerhetsarbetet så kommer dessa sannolikt från en budgetpost som även ska gå till andra ändamål.

Hela 109 kommuner bedömer att den utsedda funktionen inte har möjlighet att bedriva kommunens informationssäkerhetsarbete sett utifrån given budget. Det innebär att nära tre fjärdedelar av kommunerna inte ser att det finns finansiella förutsättningar att bedriva ett systematiskt informationssäkerhetsarbete.

8. FA22 var benämningen på de föreskrifter och allmänna råd om grundsäkerhet i samhällsviktiga datasystem, som togs fram av Överstyrelsen för civil beredskap, ÖCB. Där föreskrev ÖCB grundsäkerheten för samhällsviktiga datasystem hos beredskapsmyndigheter och angav den lägsta säkerhetsnivå som måste vara uppfylld för att beredskapsmyndigheten skulle kunna utföra sina uppgifter på ett tillfredsställande sätt under höjd beredskap.
9. Basnivå för informationssäkerhet var tidigare MSB:s (eg. KBM:s) rekommendationer för att skapa och upprätthålla en basnivå för informationssäkerhet. Fr.o.m. 2011 uppdaterar MSB inte längre BITS utan hänvisar till informationsäkerhet.se.

Bedömning och rekommendationer

En kommun är en stor och komplex organisation. Utifrån antalet medarbetare är många kommuner större än de flesta företag och myndigheter. Stöd i form av resurser, kompetens och budget är viktiga komponenter för att skapa informationssäkerhet. Det är positivt att så många kommuner har en utpekad funktion för informationssäkerheten i kommunen.

Vad som är mindre positivt är att den utpekade funktionen förlägger så lite tid på att arbeta med det som är tänkt att vara dess huvuduppgift. Sett mot tid som kommunerna uppger att resursen kan lägga på informationssäkerhet, så innebär detta med största sannolikhet att arbetet med informationssäkerhet blir underordnat andra arbetsuppgifter. Sett mot hur informations- och teknikberoende samhället är idag och på hur mycket känslig information som kommunerna hanterar, så borde denna siffra vara högre. Och till detta tillkommer att 40 % av kommunerna inte har någon utsedd funktion för informationssäkerhet över huvud taget.

Det är viktigt att skapa en förståelse för vad som avses med kvalitet i kommunens informationshantering. Ett sätt att uppnå förståelse är att utbilda personalen. Det skapar förståelse för att säker informationshantering krävs i de flesta processer. Många gånger ges resurser för krishantering. Det är också viktigt att det är säkerställt att funktionen med informationssäkerhetsansvar har mandat att sammankalla till riskanalyser och systemförvaltarträffar och att dessa möten kan prioriteras i arbetet.

Vad många inte tänker på är att information ofta står i centrum vid krishantering. Utvärderingar av kriser har visat att information varit en av de viktigaste faktorerna för hanteringen av krisen. För de som försöker lösa en kris kan tillgången till korrekt information i rätt tid vara helt avgörande. Att kommunerna inte utbildar i någon större grad i informationssäkerhet tyder på avsaknad av resurser och/eller stöd från ledningen.

Att så många kommuner bedömer att den utsedda funktionen inte har möjlighet att bedriva kommunens informationssäkerhetsarbete sett utifrån given budget är en svårbedömd uppgift eftersom få kommuner uppger att de har en egen budget för informationssäkerhetsarbetet.

Rekommendationer:

- Se till att det finns en utpekad funktion för informationssäkerhet inom kommunen och som har informationssäkerhet som sitt huvudsakliga arbetsområde och med ett från kommunledningen tydligt mandat och ansvar.
- Se över vilka resurser som behövs för att införa, upprätthålla, underhålla och förbättra den beslutade informationssäkerheten i kommunen, samt tillhandahåll resurser.
- Höj medvetenheten kring informationssäkerhet i hela kommunen. Se till att de anställda i kommunen är medvetna om informationssäkerhetspolicyn och det säkerhetsansvar de har i sitt dagliga arbete.
- Se till att informationssäkerhetsfunktionen kompetensutvecklas.
- Kompetens behöver även i sig ses som en informationstillgång inom organisationen. När informationstillgångar inventeras och klassificeras inom verksamheten är det av stor vikt att medarbetares kompetens och erfarenheter, inte minst hos de som aktivt jobbar med informationssäkerhet, tas med i processen.

Rapportering

Rapportering

Ett viktigt steg i processen för systematisk informationssäkerhet är att rapportera informationssäkerhetsrisker och incidenter till beslutsfattare och att de sedan, utifrån ett utförligt underlag, tar beslut på vilken åtgärdshantering som bedöms som lämplig. För att få kännedom om vilka incidenter som inträffar, och därmed kunna sammanställa dessa i en rapport, så måste det finnas en metod och en rapporteringsväg att anmäla in incidenter och risker genom.

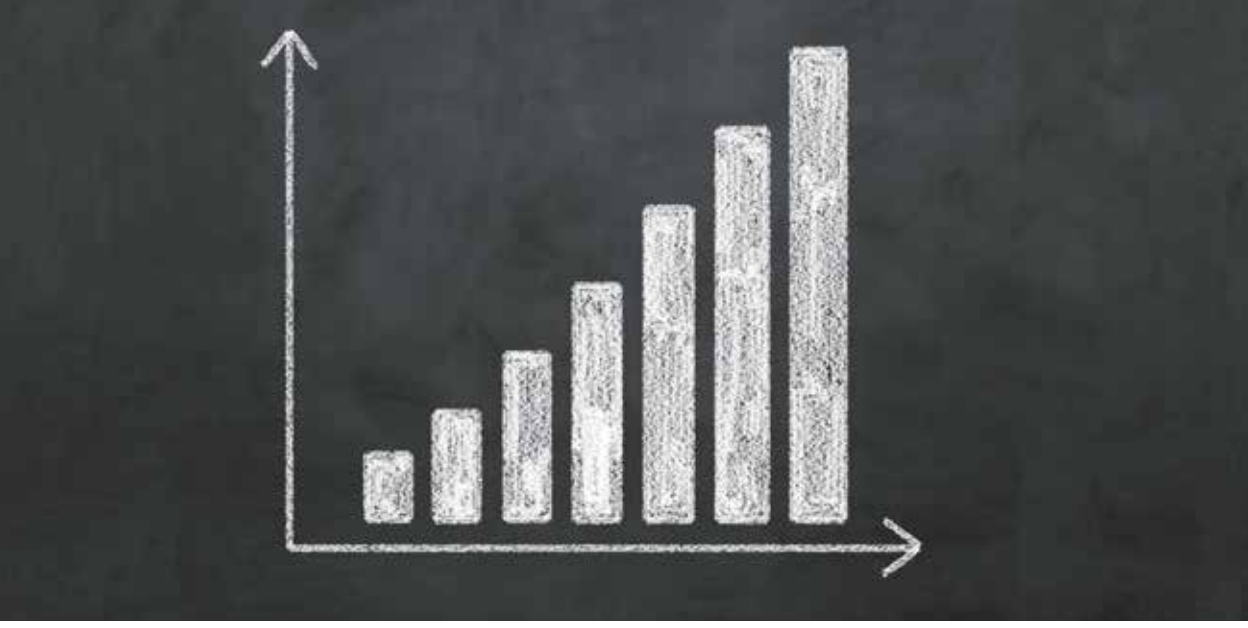
En viktig form av rapportering är it-incidentrapportering, som, om den görs systematiskt, kan ge ett mycket bra underlag för att vidta åtgärder. Att brister eller risker i informationshanteringen rapporteras till rätt part, när de upptäcks, är ofta en grundförutsättning för att lämpliga åtgärder ska kunna vidtas i syfte att avvärja eller minska riskerna.

När incidenter uppstår eller risker identifieras i verksamhetens informationshantering är det i dagsläget en minoritet av kommunerna (44 %) som har en formaliserad process för att rapportera och hantera incidenter. Majoriteten av dem som har en sådan process säger dock att den är fastställd. Det är generellt sett lämpligt att verksamhetens gällande processer fastställs genom beslut och diarieförs.[10] Det är en tydlig skillnad mellan kommuner som har en utpekad funktion för informationssäkerhet respektive de som inte har en funktion; hälften av de kommuner som har en funktion uppger att de rapporterar informationssäkerhetsfrågor vilket kan jämföras med enbart 18 % för de kommuner som inte har någon utsedd funktion.

I de kommuner som har rapportering på informationssäkerhetsområdet, så går denna oftast via informations- eller säkerhetssamordnaren vilken vanligtvis rapporterar resultatet på kommunledningens möten. Resultatet av enkäten visar dock att det finns en större mängd olika rapporteringsvägar och rapporteringssätt. Därmed saknas möjligheten att skapa en gemensam nationell bild av de risker som uppmärksammats.

På frågan till vilken funktion eller roll som det övergripande läget och status vad gäller informationssäkerhet rapporteras, svarar en stor del av respondenterna kommunstyrelsen eller kommundirektör/stadsdirektör. Av de 31 % som valt alternativet ”Annat” har kommunerna till övervägande del svarat säkerhetschef, men drygt 20 respondenter säger också att det inte sker någon rapportering alls.

10. Svaren i enkäten på frågan om hur länge den aktuella processen funnits ger en bild av att vissa av kommunerna har svårt att svara på när processen beslutades och var kraven förekommer. Vissa har svarat att kraven kan finnas i styrande dokument ute på respektive förvaltning och andra har sagt att de regleras i informationssäkerhetspolicyn.



Bedömning och rekommendationer

Generellt tyder resultatet på att många kommuner är mogna och förstår betydelsen av att rapportera informationssäkerhetsfrågor direkt till ledningen. Resultatet visar att kommunens högsta ledning till stor del får information kopplat till informationssäkerhetsfrågor. Även om svaren tyder på att många kommuner rapporterar övergripande läge och status vad gäller informationssäkerhet och att det till stor del görs till kommunens högsta ledning, så säger samtidigt inte svaren något om vad som rapporteras. Då många av respondenterna är från it-avdelningen och att informationssäkerhetsansvaret i många fall är placerat där, kan det innebära att det främst är it-säkerhetsrelaterade frågor och it-incidenter som rapporteras.

Kommunernas rapporteringsarbete på informationssäkerhetsområdet är relativt utvecklat, men kan utvecklas ytterligare, till exempel vad avser incidentrapportering och rapporteringsvägar. Med en systematisk incidentrapportering kan arbetet med informationssäkerhet utvecklas från att många gånger enbart vara it-relaterat till att även inkludera informationssäkerhet i hela organisationen.

Sett mot de många rapporteringsvägar som finns för att rapportera informationssäkerhetsrisker, så ser sannolikt rapporteringen mycket olika ut. Möjligheten att skapa en nationell bild av informationssäkerhetsriskerna i landets kommuner försvåras därmed. Här är bedömningen att kommunerna skulle ha mycket att vinna på att ta fram gemensamma rekommendationer på rapporteringsstruktur t.ex. utifrån standardiseringsarbete för riskhantering på informationssäkerhetsområdet.[11]

11. Se t.ex. Riskhantering – Principer och riktlinjer (ISO 31000:2009, IDT).

Liksom för andra aktörer kommer det bli en utmaning för kommunerna att integrera de olika riskhanteringsprocesserna inom organisationen. Säkerhetsrisker, arbetsmiljörisker och finansiella risker kommer att bli allt mer hoptvinnade framöver.

För att få en väl fungerande incidentrapportering så är det också viktigt att ha ett processperspektiv på arbete. Rapporterade händelser/risker måste hanteras och erfarenheter från incidenten och de vidtagna åtgärderna måste omhändertas ur ett läroperspektiv, så att det leder till ett systematiskt förbättringsarbete.

Kommunerna bör säkerställa att avtalen mellan kommunen och de leverantörer som hanterar kommunens informationstillgångar, innehåller krav på incidentrapportering. Något som bör beaktas är möjligheten att lägga in detta krav i standardiserade avtalsmallar i de fall sådana används. Det bör vidare säkerställas att det finns en process inom kommunen som systematiskt omhändertar dessa rapporter i syfte att skydda informationstillgångarna. Detta avser både hantering av händelser samt mer långsiktiga åtgärder med förebyggande aspekter på informationssäkerheten.

Rekommendationer:

- Se till att den utpekade informationssäkerhetsfunktionen får möjlighet att regelbundet presentera aktuell status på området för kommunens ledning (inkl. aktuella risker).
- Säkerställ att det inte enbart är it-säkerhetsrelaterade frågor eller it-incidenter som rapporteras till ledningen, utan informationssäkerhetsrelaterade frågor ur ett bredare perspektiv.
- Se till att incidentrapporteringen omhändertas ur ett läroperspektiv och att den leder till ett systematiskt förbättringsarbete.
- Ta fram, informera om och öva en formaliserad process för att rapportera in och omhänderta inkomna informationssäkerhetsincidenter.
- Säkerställ att avtal med externa parter innehåller krav på incidentrapportering.
- Säkerställ att incidentrapporteringsprocessen omfattar kommunens externa leverantörer.

På sikt bör kommunerna se över möjligheten att ta fram gemensamma rekommendationer vad avser en grundläggande struktur på det som rapporteras på informationssäkerhetsområdet.

Incidenthantering och kontinuitetsplanering

Incidenthantering och kontinuitetsplanering

Att kunna hantera incidenter underlättas om organisationen använder en beprövad incidenthanteringsmodell. För att verksamheten ska kunna bedrivas även i störda förhållanden, så bör kontinuitetsplanering upprättas och införas.

Nära 60 % (142 st) av kommunerna uppger att de saknar en plan för hur bortfall av information i kommunens kritiska verksamhetsprocesser ska hanteras. Av de kommuner som har en kontinuitetsplan är det en överväldigande majoritet, 80 % av kommunerna (78 st), som aldrig eller endast enstaka gånger övar planen.

Av de kommuner som har planer uppger flera kommuner att de reviderar sin kontinuitetsplan årligen. Den vanligaste anledningen till att planerna revideras är större verksamhetsförändringar och systemförändringar.

Idag är det många kommuner som har lagt ut hela eller delar av informationshanteringen på entreprenad hos externa leverantörer. En knapp majoritet (57 %) av de kommuner som har en incidentrapporteringsprocess säger att den innefattar kommunens externa leverantörer såsom exempelvis driftleverantörer.

Enligt kommunerna är återföring av kunskap rörande incidenter sällan systematisk, utan sker mer oregelbundet på ad-hoc-basis.

Bedömning och rekommendationer

Att majoriteten av kommuner uppger att de saknar kontinuitetsplanering för bortfall i information för kritiska processer måste bedömas som mycket allvarligt. Kommunerna har ett stort ansvar gentemot enskilda och en incident kan ha stora konsekvenser. Kommunerna kan tjäna mycket på att börja arbeta med kontinuitetsplanering för de mest kritiska informationsresurserna såsom t.ex. infrastruktur (internetaccess, DNS, brandväggar, routing, nätverk), webb och telefoni.

Att de kommuner som har en kontinuitetsplan i stort sett aldrig övar planen visar att riskarbetet ytterligare måste integreras i verksamheten. Övning är avgörande för att veta hur man ska agera i en krissituation. En kontinuitetsplan som inte övas revideras oftast inte, vilket gör att planen till slut oftast blir utdaterad och därmed inte kan fylla sitt syfte.

Rekommendationer:

- Se till att ta fram en kontinuitetsplan för hur bortfall av information och andra informationssäkerhetsrisker i kommunens kritiska verksamhetsprocesser ska hanteras.
- Öva kontinuitetsplanen med jämna mellanrum.
- Informera om kontinuitetsplanen och håll den uppdaterad.

Samverkan

Samverkan

För en informationssäkerhetsfunktion inom en kommun är det ofta ett ensamt uppdrag som ska utföras i konkurrens med många andra arbetsuppgifter. Då den eller de personer som har ett informationssäkerhetsansvar inom en kommun ställs inför liknande utmaningar som informationssäkerhetsansvariga inom andra kommuner, finns det stora vinster med att dela med sig av erfarenheter och kunskaper. Det blir på det sättet naturligt att ha ett utbyte med andra kommuner på området för att öka effektiviteten och sin egen kunskap.

En majoritet av kommunerna uppger att de har ett samarbete med andra kommuner vad gäller informationssäkerhet. Hur samarbetet ser ut skiljer sig åt mellan kommunerna men ett stort antal uppger att de deltar i nätverket KIS, Informationssäkerhetsnätverket Sveriges kommuner. Nätverket etablerades 2011 av MSB och SKL i samverkan. Syftet med nätverket är att stödja den funktion som samordnar informationssäkerheten i kommunen i arbetet med att förbättra och effektivisera kommunens informationssäkerhetsarbete.[12]

Det finns olika anledningar till att samarbeten uppkommer mellan kommuner inom området. Det kan vara ekonomiska skäl, exempelvis att flera kommuner gemensamt finansierar en tjänst eller kan söka medel. I dagens informationssamhälle flödar också informationen mellan kommuner, myndigheter och företag på ett helt annat sätt än tidigare och e-förvaltningsfrågorna ökar i betydelse, vilket bl.a. gör att samarbeten på området blir en naturlig följd.

12. Funktioner vars arbetsuppgifter handlar om att samordna och utveckla informationssäkerheten i kommunen har behov av att utbyta erfarenheter, kunskap och information med företrädare för andra kommuner och organisationer. Inom KIS finns ett digitalt forum för detta till vilket alla medlemmar får ett eget personligt konto. Där går det att dela med sig av dokument och goda exempel, ställa öppna frågor, starta onlinemöten, ta del av andras erfarenheter etc.

Resultatet visar att det i vissa fall finns en person som samordnar informationssäkerheten i flera kommuner. Det finns då i en del fall även en gemensam informationssäkerhetspolicy och andra styrande dokument. Oftast är det angränsande kommuner som etablerar ett samarbete. I förekommande fall spelar dock kommunens storlek en avgörande roll, och då kan samarbeten upprättas mellan kommuner som inte gränsar till varandra.

I en del fall är det svårt att avgöra hur samarbetet ser ut, vilket kan bero på att det finns olika uppfattningar om vad informationssäkerhet innefattar. Exempelvis uppger ett antal kommuner kort och gott att det finns en gemensam it-drift, vilket i sig inte säger något om samarbete rörande informationssäkerhet. Däremot visar resultatet att genom att flera kommuner har en gemensam drift skapas incitament för samarbete kring informationssäkerhet.

Länsstyrelsernas roll

Regeringsuppdraget till MSB om informationssäkerheten i kommunerna[13] innehöll även ett särskilt uppdrag att se på länsstyrelsernas roll i arbetet med informationssäkerhet hos Sveriges kommuner. I enkäten uppger 25 % av de svarande kommunerna (62 st) att de har samverkan med länsstyrelserna. Vid närmare undersökning om vad samverkan består av, så handlar det till största del om begränsade projekt såsom införande av DNSSEC, punktinsatser i form av seminarier eller nätverk för kriskommunikatörer och beredskapshandläggare. Ett fåtal mer bestående nätverk inom informationssäkerhetsområdet finns dock, till exempel i nordöstra Skåne, Norrbotten, Kalmar och Jönköping.

Slutsatsen blir att majoriteten av kommunerna inte samverkar med länsstyrelsen inom informationssäkerhetsområdet.

Bedömning och rekommendationer

Bedömningen är att kommunerna skulle kunna stärka sitt samarbete, både mellan kommunerna och med länsstyrelserna. Fokus för samarbetet bör vara att skapa mer permanenta löpande samarbeten som båda parter får nytta av.

Rekommendationer:

- Se till att den/de som har ett informationssäkerhetsansvar har etablerade kontaktvägar till andra relevanta aktörer för att ha möjlighet att diskutera informationssäkerhetsfrågor.
- Se över möjligheterna att samarbeta med länsstyrelsen om informationssäkerhetsfrågor.

13. En bild av kommunernas informationssäkerhetsarbete 2015, MSB943 https://www.msb.se/RibData/Filer/pdf/27967.pdf.

Upphandling

Upphandling

Upphandlingen är en viktig del i säkerhetsarbetet. Det är väsentligt att kraven ur informationssäkerhetssynpunkt är med i hela processen. På så sätt går det att åstadkomma hög säkerhet i de produkter och tjänster som levereras och dessutom minska risken för oväntade kostnader i efterhand.

Undersökningen visar att det hos en majoritet (61 %) av de kommuner som svarat inte finns en process som säkerställer att informationssäkerhetsrelaterade aspekter beaktas vid upphandling. Det stämmer väl med den bild som framkommer i övrigt vad gäller t.ex. kommunernas brist på kontinuitetshantering, övning, utbildning, och styrande dokument på informationssäkerhetsområdet.

En tredjedel av kommunerna svarade att funktionen för informationssäkerhet har mandat att stoppa en pågående upphandling eller leverans med otillräcklig säkerhet.

Endast en av tre kommuner har en särskilt utpekad ansvarig för informationssäkerhet i projekt som kan påverka informationshanteringen, t.ex. upphandling av nya it-system. Bland de kommuner som har detta arbetssätt varierar det vilken funktion som i så fall har ansvaret, informationssäkerhetssamordnare och systemägare förekommer ofta. Det framgår tydligt av svaren att det till stor del helt saknas systematik för att i projekt med påverkan på informationshantering analysera informationssäkerhet. De kommuner som gör sådana analyser gör på olika sätt, vilket tyder på att det saknas kunskap om hur informationssäkerhet förs in i projektmodeller.

Något förvånande är det vanligast att granskning för att verifiera säkerhetskrav vid upphandling görs av it-enheten, it-chef eller it-samordnare. Resultaten visar att funktionen för informationssäkerhet mer sällan används för verifiering av säkerhetskrav. Informationssäkerhetssamordnare eller liknande roll förekommer som granskar i hälften av fallen. Resultatet är svårtolkat då det kan vara ett tecken på att funktionen för informationssäkerhet inte deltar i varje projekt utan att man har ett arbetssätt där policy och riktlinjer utfärdade av informationssäkerhetsfunktionen tillämpas av andra.

En stor andel har även svarat att de inte vet om det sker någon granskning eller att ingen granskning sker alls. Bland de som anger att verifiering av upphandling sker, dvs. att upphandlingen skett efter de krav som ställts, anger nästan alla att granskningen sker gemensamt av flera funktioner. Vid frågan varför flera parter deltar, så är det vanligaste svaret att det saknas rutiner. Som kontrast är det

näst vanligaste svaret att man tvärtom regelmässigt gör en helhetsanalys med hänvisning till flera områden med relevanta lagar, ISO-standard och interna styrdokument. De som avstått från att svara uppger att man inte vet hur frågan ska besvaras.

Den lagstiftning som många lyfter fram särskilt är PuL där flera kommuner nämner PuL som ensamt underlag för analys vid upphandling alternativt i kombination med en riskanalys. (Vid användning av personuppgiftsbiträdesavtal behandlas till viss del även säkerhetsaspekter.) Andra svar lyfter fram vissa delar som t.ex. behörighetskontroll, kontinuitet och drift eller liknande.

De allra flesta kommuner, sju av tio, använder sig av leverantörernas standardavtal. Bland de 30 % som har svarat nej på frågan kan noteras att de flesta har en tydlig uppfattning om varför de inte använder dem och det speglar att det är ett medvetet beslut. Bland de skäl som anges märks särskilt att de anser att dessa avtal är otillräckliga när det gäller informationssäkerhet, att de uppfattas som leverantörsvänliga och att man har som beslutad rutin att kommunen själv formulerar sitt avtal.

Bland de delar man anser saknas i leverantörernas standardavtal återfinns frågor om personuppgiftshantering, tydlighet i ansvarsfördelning mellan parterna och kommunspecifika frågor. Man lyfter även fram mer konkreta brister inom området informationssäkerhet, som t.ex. brister i spårbarhet, lagring av information, tillgång, kontinuitetskrav och tider för återställning av data.

Bedömning och rekommendationer

Att en majoritet av kommunerna inte har en fastställd process för upphandling gör det svårt att få in informationssäkerhet som en del i upphandlingsprocessen. Att inte få in informationssäkerhetsaspekter vid upphandling kan leda till att informationssäkerheten i vissa funktioner eller processer kan fördröjas i flera år då det kan bli mycket kostsamt att omförhandla innan kontraktstiden gått ut. Därför är det av stor vikt att få till en fastställd upphandlingsprocess där informationssäkerhetskrav ingår som en naturlig del av processen.

Att flera kommuner lyfter fram PuL i upphandlingssammanhang, visar att informationshantering i kommunerna till övervägande del omfattar personuppgifter och att denna lagstiftning är väl känd.

Resultatet att endast enbart en handfull (6 st) av kommunerna anger att funktionen för informationssäkerhet har mandat att stoppa en pågående upphandling eller leverans med otillräcklig säkerhet kan tyda på att man inte har anpassat sina processer fullt ut efter den faktiska it-miljön där verksamhetssystem inte längre är isolerade öar utan där starka beroenden finns. Bristande säkerhet för en del kan ge negativ påverkan utanför det område som den aktuella verksamheten kan besluta om och mycket talar för att en centralt placerad funktion med ansvar för informationssäkerhet bör ha denna typ av mandat.

Att 30 % uppger att de inte använder standardavtal är intressant och tyder på en ökad mognad där standardavtalens innehåll ifrågasätts och/eller kompletteras efter behov.

Rekommendationer:

- Se över om det går att få till en fastställd upphandlingsprocess där informationssäkerhet ingår som en del.
- Se till att informationssäkerhetskrav identifieras och inkluderas i upphandlingen.
- Ge funktionen för informationssäkerhet mandat att påverka och i möjligen även att kunna stoppa en pågående upphandling med bristande informationssäkerhet.

Övrigt

Övrigt

Industriella informations- och styrsystem

I enkäten tillfrågades kommunerna om informationssäkerhet i relation till industriella informations- och styrsystem, s.k. SCADA-system[14]. SCADA-system är idag en viktig del för att styra och övervaka olika system i industriell miljö, men har även börjat användas allt mer i andra miljöer som t.ex. för att styra temperatur i fastighetheter, s.k. fastighetsautomation.

Noterbart i enkäten är att det tycks finnas svårigheter att förstå begreppet industriella informations- och styrsystem och den växande andel verksamheter i vilka sådana kan vara inbegripna. Därmed bör svaren tas med viss försiktighet.

Enkäten ger en indikation på att kommunerna inte har en sammanhållen bild av säkerhetsarbetet vad gäller, för kommunen, kritiska SCADA-system. Säkerhetsansvar har kanske delegerats till kommunens bolag vilket gör att kommunen inte har insyn på samma sätt som den verksamhet som sker i kommunens egen regi. Relaterat till detta är beroendeförhållandet när verksamhet sker i lokaler som är hyrda av en extern part, och denna antas vara ansvarig för säker drift av lokalerna, eller som i fallet där en extern part tillhandahåller hela tjänsten t.ex. fjärrvärme.

DNSSEC

MSB:s undersökning avseende informationssäkerhetsarbetet i kommuner visar på att 57 % av alla tillfrågade har infört DNSSEC på sina webbplatser för att kommuninvånare och andra intressenter ska kunna vara trygga med att de nått rätt webbplats.

Behovet av korrekt implementerad DNSSEC kommer med tiden växa och bli allt mer relevant då allt fler kommuner erbjuder e-tjänster. DNSSEC är ett tillägg till DNS-tjänsten som måste underhållas och uppdateras regelbundet för att säkerställa rätt funktionalitet. Enligt undersökningen har 77 % redan följt upp sitt införande av DNSSEC så att det är korrekt implementerat och detta är ett arbete som bör göras regelbundet.

14. SCADA (Supervisory Control And Data Acquisition) är ett system för övervakning och styrning av processer. Dessa system används framförallt inom industrin för processövervakning, men har på senare år även börjat användas inom t.ex. fastighetsautomation.

Om jämförelser mellan kommunerna

Utan en separat validering och verifiering av enkätresultaten är det svårt att avgöra om kommuner som satsar på informationssäkerhet har en högre nivå av informationssäkerhet än andra kommuner. Därför görs det inga djupare analyser av skillnader mellan kommuner i denna rapport.

Går det då ändå att ge en rudimentär bild av eventuella skillnader mellan de kommuner som satsat på informationssäkerhet respektive de som inte gjort så? Nedan presenteras en jämförelse mellan en grupp av kommuner som bedöms ha en god systematik i sitt informationssäkerhetsarbete och en grupp som kan bedömas inte arbeta lika systematiskt med området.

Ur frågebatteriet valdes sju frågor som indikatorer och användes för att filtrera resultatet. De sju parametrarna representerar ett urval av viktiga delar i ledningssystem för informationssäkerhet, LIS. De frågor som användes var följande:

- Finns det en utpekad funktion för informationssäkerhet inom kommunen?
- Kontrolleras efterlevnad rörande informationssäkerhet?
- Tillämpar kommunen ett systematiskt arbetssätt när det gäller informationssäkerhet?
- Har kommunen en metod för informationsklassning?
- Genomför kommunen riskanalys avseende informationssäkerhet?
- Finns kontinuitetsplaner för att hantera bortfall av information i kritiska verksamhetsprocesser inom kommunen?
- Finns det en process för rapportering och hantering av säkerhetsbrister/incidenter kopplade till informationshantering inom kommunen?

Sammanlagt 15 kommuner svarade *JA* på ovanstående frågor och 21 kommuner svarade *NEJ* på samma frågor. Generella drag är att de som svarat *NEJ* är kommuner med färre anställda.

Vid en jämförelse mellan de övriga svaren ur enkäten kan följande iakttas.

- Av de kommuner som svarade JA på frågorna hade alla (100 %) en beslutad informationssäkerhetspolicy. Av de kommuner som svarade NEJ hade mindre än hälften en sådan policy (41 %). Genomsnittet för samtliga kommuner som besvarat enkäten var 73 %.

- De kommuner som svarat *JA* hade i högre grad (93 %) än genomsnittet ett samarbete med andra kommuner. De som svarade *NEJ* har på motsvarande sätt en lägre grad av samverkan (32 %). Genomsnittet för samtliga kommuner som besvarat enkäten var 55 %.
- De kommuner som svarat *JA* på frågorna har en informationssäkerhetsfunktion som i högre grad än genomsnittet anser sig ha mandat (93 %) och kompetens (93 %) för uppdraget. Genomsnittet för de kommuner som besvarat enkäten är vad gäller både mandat, som kompetens 67 %.
- De kommuner som svarade *JA* på frågorna erbjöd i högre grad (86 %) utbildning i informationssäkerhet till de anställda. Enbart en minoritet (36 %) bland de kommuner som svarade *NEJ* erbjöd en sådan utbildning. Genomsnittet för att erbjuda utbildning i informationssäkerhet för samtliga kommuner som besvarat enkäten var 58 %.

Det går också att notera en skillnad i ålder på informationssäkerhetspolicyn; för de kommuner som svarat *JA* var åldern på policyn mellan 1 och 3 år och för de som svarat *NEJ* var den genomsnittliga åldern 4–5 år.

Flera av resultaten är väntade och nära förknippade med resurser – finns det en funktion som arbetar med frågorna är naturligtvis mycket av det som tas upp ovan betydligt enklare att genomföra. Allt tyder på att tillräckliga resurser har stor betydelse för att uppnå god informationssäkerhet. Intressant är dock att några kommuner besvarat samtliga frågor med *JA* men ändå har en resurs som arbetar *mindre än halvtid* med frågorna (40 % av de kommuner som svarat *JA* på frågorna). En möjlig förklaring till det resultatet är att en del av de uppgifter som normalt associeras med informationssäkerhetsfunktionen har förlagts ute i verksamheterna. Uppgifterna som en sådan funktion har kan variera beroende på om syftet med den är att den primärt ska vara en utförare eller en stödjande funktion som hjälper andra att utföra informationssäkerhetsarbete.

Men utöver resurser, så behövs en struktur där resurserna kan verka. Allt tyder på att tillräckliga resurser är ett nödvändigt villkor för att uppnå god informationssäkerhet. Det är däremot inte nödvändigtvis ett tillräckligt villkor. För att en aktör ska uppnå en tillräckligt hög nivå av informationssäkerhet behövs en strukturerad process för att arbeta systematiskt med informationssäkerhet. Frågan är om det inte är hur väl kommunen fått till en strukturerad process för att kunna arbeta systematiskt med informationssäkerhet, som är en framgångsfaktor.

De kommuner som har en företrädare för informationssäkerhetsfrågor har självklart större möjligheter att bedriva ett mer systematiskt arbete med informationssäkerhet, t.ex. genom att skapa en struktur med processer. Skillnaderna märks till exempel i hur rapporteringsvägar fungerar, hur riskanalys och informationsklassning tillämpas och hur informationssäkerhetsaspekter hanteras i samband med projekt och upphandlingar.

Det finns sannolikt större verksamhetsrisker avseende informationssäkerheten än många av kommunerna är medvetna om idag. Återföringen av kunskap kring incidenter synes sällan vara systematisk, utan ske mer oregelbundet. Detta innebär att det är svårt att lära av incidenter och händelser och svårt med ständiga förbättringar.

Att brister eller risker i informationshanteringen rapporeras till rätt part, när de upptäcks, är ofta en grundförutsättning för att lämpliga åtgärder ska kunna vidtas i syfte att avvärja eller minska riskerna. När brister eller risker uppstår i verksamhetens informationshantering är det i dagsläget en minoritet av kommunerna (44 %) som uppgett att de har en formaliserad process för att rapportera och hantera incidenter. Majoriteten av dessa har dessutom fastställt processen formellt. Det är generellt sätt lämpligt att verksamhetens gällande processer fastställs genom beslut samt diarieförs. Svaren i enkäten på frågan om hur länge den aktuella processen funnits ger bilden av att vissa av kommunerna har svårt att svara på när processen beslutades och var kraven förekommer. Vissa har svarat att kraven kan finnas i styrande dokument ute på respektive förvaltning och andra har sagt att de regleras i informationssäkerhetspolicyn.

Idag är det många kommuner som har lagt ut hela eller delar av informationshanteringen på entreprenad hos externa leverantörer. En knapp majoritet (57 %) av de kommuner som har en incidentrapporteringsprocess säger att den innefattar kommunens externa leverantörer såsom exempelvis driftleverantörer. Det vore önskvärt att siffran var högre.

Kommunerna bör säkerställa att avtalen mellan kommunen och de leverantörer som hanterar kommunens informationstillgångar, innehåller krav på informationssäkerhet samt incidentrapportering. Något som bör beaktas är möjligheten att lägga in detta krav i standardiserade avtalsmallar i de fall sådana används. Det bör vidare säkerställas att det finns en process inom kommunen som systematiskt omhändertar dessa rapporter i syfte att skydda informationstillgångarna. Detta avser både hantering av händelser samt mer långsiktiga åtgärder med förebyggande aspekter på informationssäkerheten.

Vilka är då framgångsfaktorerna?

Även om det finns en relativt stor förbättringspotential rörande informationssäkerhetsarbetet i kommunerna, så kan man också identifiera framgångsfaktorer, det som förenar de kommuner som anser sig bedriva ett mer kvalificerat arbete med informationssäkerhet där flera av de centrala komponenterna ingår. Ingen av insikterna nedan är att betrakta som nya och omvälvande, utan ligger väl i linje med de budskap som under lång tid förmedlats kring informationssäkerhet:

- Ett tydligt ansvar är viktigt för ett systematiskt informationssäkerhetsarbete. En aktiv kommunledning som tar initiativ inom området och tydliggör ansvaret, skapar goda förutsättningar för att styrningen av en organisations informationssäkerhet blir mer effektiv.
- Det är mer effektivt att bedriva ett systematiskt informationssäkerhetarbete, där kommunen upprätthåller och utvecklar goda rutiner för hur de hanterar information på ett säkert sätt i linje med identifierade krav.
- De kommuner som har en utpekad funktion, som kan lägga tillräckligt med tid och som arbetar fokuserat med informationssäkerhet, har lättare att bedriva ett mer kvalificerat arbete med informationssäkerhet.
- Organisatorisk placering är av central betydelse. Närheten till kommunledningen är viktig för att kunna föra fram informationssäkerhetsaspekter på kommunens verksamhet.

Slutord

Slutord

Resultatet tyder på att informationssäkerheten i kommunerna ytterligare bör stärkas på flera områden. En klar majoritet av kommunerna arbetar idag inte systematiskt med informationssäkerhet. Kontroll och tillsyn av säkerheten i informationssystemen genomförs i liten omfattning. En majoritet av kommunerna saknar en plan för bortfall av information i kommunens kritiska verksamhetsprocesser. Övning och utbildning är eftersatta områden.

Kommunerna har påbörjat införandet av ett ramverk för informationssäkerhet och utsett ansvar, men har inte implementerat ett arbete med informationsklassning och riskhantering i någon större utsträckning.

Enbart en tredjedel av kommunerna att ett systematiskt arbetssätt i sitt arbete med informationssäkerhet. Att huvuddelen av kommunerna har otillräcklig riskhantering ligger i linje med detta. Detta i kombination med att nära 7 av 10 kommuner lägger 10 % eller mindre av en arbetskraft på att säkra informationen i kommunen borde mana till eftertanke.

Enkätsvaren tyder på att det finns ett gap mellan det som står i kommunens informationssäkerhetspolicy och det som operationaliseras i verksamheten. Det finns därmed sannolikt större verksamhetsrisker hos kommunerna avseende informationssäkerheten än de är medvetna om idag.

När det gäller hur Sveriges kommuner arbetar med informationssäkerhet är det mycket som liknar arbetet hos de statliga myndigheterna. En avgörande skillnad är dock att arbetet med informationssäkerhet vid myndigheterna med stor sannolikhet gynnats av att MSB har föreskriftsrätt inom området. MSB:s föreskrifter innehåller en hänvisning till standarder inom området (SS-ISO/IEC 27001 och 27002) vilket troligen ytterligare fungerat som stöd för myndigheterna i arbetet med att driva informationssäkerhetsfrågor.[15] Sveriges kommuner har inte motsvarande informationssäkerhetsföreskrifter, vilket troligen bidragit till att det finns större brister i kommunerna, exempelvis i fråga om informationsklassning och riskanalyser.

15. Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet; MSBFS 2016:1.

Ytterligare stöd för detta resonemang är att de kommuner, som eftersträvar och säger sig ha uppnått ett systematiskt arbete med informationssäkerhet, i stort sett hanterar information på ett sätt som går i linje med identifierade krav i MSB:s förordning.

Resultaten från denna undersökning visar att de budskap som under lång tid förmedlats kring informationssäkerhet har lika stor aktualitet idag som tidigare. Resultaten och rekommendationerna i denna analys ger förhoppningsvis ytterligare underlag som kan användas för att stärka informationssäkerheten i kommunerna.

Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB1045 - december 2016 ISBN 978-91-7383-697-5