NORDISKT SAMARBETE OM INFORMATIONSSÄKERHET I KOMMUNER, LANDSTING OCH REGIONER

PROMEMORIA OM INFORMATIONSSÄKERHET OCH DIGITALISERING

SVENSKA KOMMUNER 2015

2008–2015

Promemorian är utarbetad för:

Sveriges Kommuner och Landsting

Augusti 2015

INLEDNING

Digitalisering i form av självbetjäningslösningar för medborgare och verksamheter, nya möjligheter till virtuell kommunikation med omvärlden, mobila och flexibla arbetsplatser och användningen av sociala medier i yrkesmässiga och privata sammanhang betyder att databehandlingen flyttas från stora system och manuella processer till nya digitala plattformar.

Riskbilden för den kommunala informationsanvändningen framstår på flera områden som mer omfattande och komplex än förut:

- Datas pålitlighet och trovärdighet kontrolleras oftare genom system än av människor.
- Data- och systemtillgänglighet är i fokus när åtkomsten till information sker genom system.
- Data kan vara belägna på många olika IT-plattformar i kommunen som oftast endast delvis är under kommunens kontroll.

Informationssäkerhet är ett område som får stor uppmärksamhet bland allmänheten:

- En kommande EU-förordning skärper kraven på behandling av känsliga personuppgifter och fastställer bland annat krav på ansvarsskyldighet.
- En rad händelser har visat hur sårbara IT-system är för kriminella handlingar samt interna fel och internt missbruk.

God praxis för informationssäkerhet beskrivs i standarden ISO 27001 som tar utgångspunkt i en närmare förbindelse mellan förvaltningsorganisationen och den nödvändiga nivån av informationssäkerhet, men utan att föreskriva konkreta minimiinsatser. SKL rekommenderar att kommunerna använder ISO-standarden i syfte att få en gemensam hög säkerhetsstandard inom den offentliga sektorn. Detta innebär en rad förväntningar på organisationens kompetens och förmåga att arbeta med informationssäkerhet gällande

- den övre ledningens ansvar för mål och uppföljning av organisationens informationssäkerhet
- förvaltningsorganisationens ansvar för att organisera en säker IT-användning.

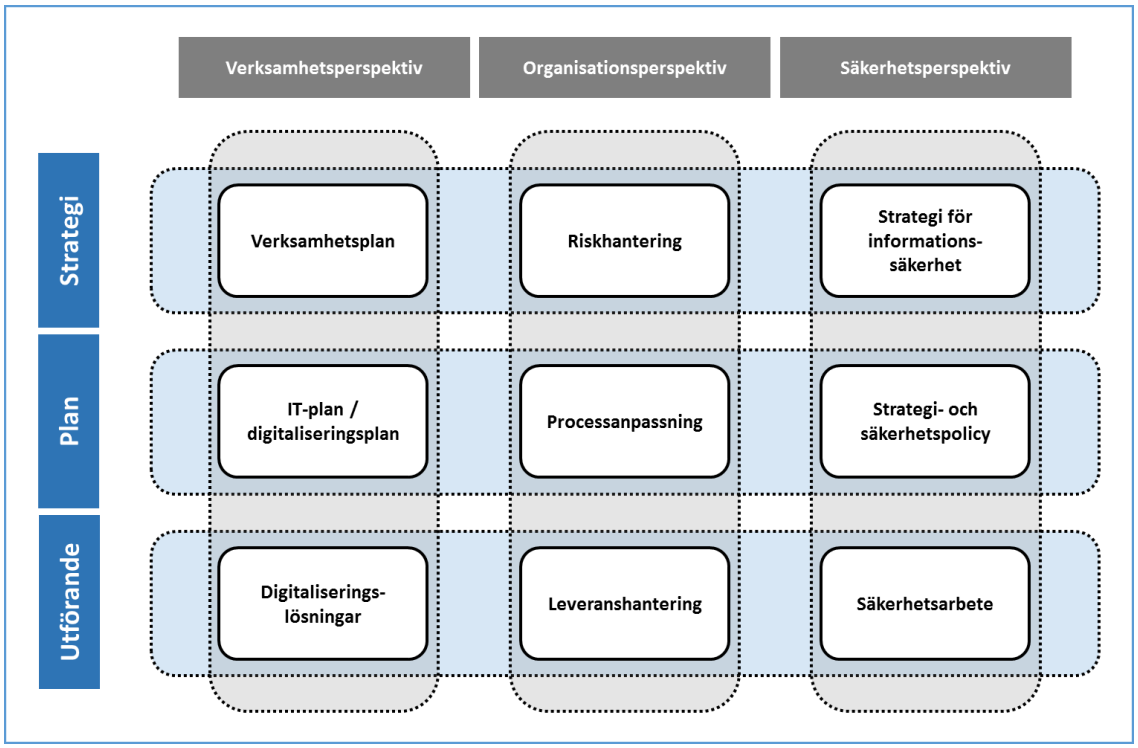
Promemorian visar hur långt svenska kommuner har kommit inom dessa områden och hur ramverket för informationssäkert har organiserats.

Undersökningens frågetema är utformat så att det avspeglar organisationens samlade fokus på informationssäkerhet – från den övre ledningen till det konkreta arbetet. Dessutom har frågetemat fokus på kommunernas användning av IT och de riskanalyser som utförs. Undersökningen har kvar frågor som knyter tillbaka till 2012 och tidigare, men strävar även efter att hitta trender i IT-användning och initiativ till säkrare alternativ.

Tidigast 2017 planeras en rad bestämmelser om skydd av personuppgifter att träda i kraft i enlighet med EU:s personuppgiftsförordning. Undersökningen innehåller en genomgång av tre av de fyra huvudområdena i förordningen. För dem som vill ha full täckning av det fjärde området finns det möjlighet att svara på extrafrågor.

Slutligen innehåller undersökningen en rad frågor om upplevda händelser och följderna av dessa.

Förhållandet mellan användning av system och information i verksamhetssyfte och kommunernas bedömning av informationssäkerhet visas i modellen nedan.



Denna promemoria har utformats med svenska kommuner i åtanke. I januari–februari 2015 erbjöds kommuner och landsting att svara på frågorna: Två av tre kommuner svarade på undersökningen vilket motsvarar nästan 70 %. 16 av 21 landsting deltog.

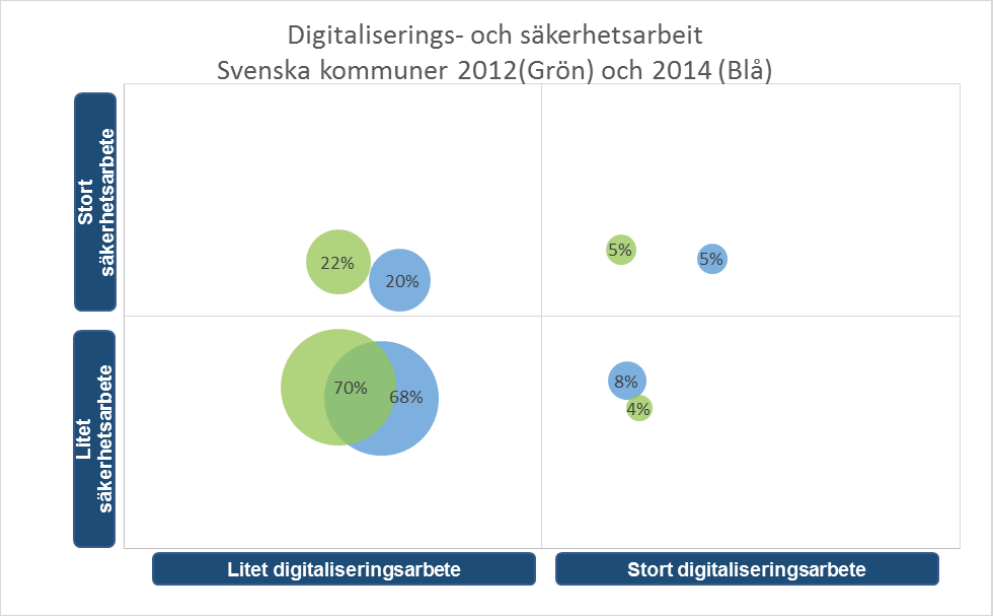
I Danmark finns en motsvarande rapport, framtagen av PRIMO Danmark (http://www.primodanmark.dk/) och KIT@ (Foreningen af Kommunale it-chefer), http://www.komdir.dk/Nyheder/News_1.aspx.

Kommuner och landsting har tillgång till självskattningsverktyget NordSec som användes för undersökningen och de organisationer som inte deltog kan även under 2016 svara på frågorna, se sin egen status och jämföra sig med övriga svenska och nordiska organisationer.

INFORMATIONSSÄKERHET OCH DIGITALISERING

Det samlade arbetet

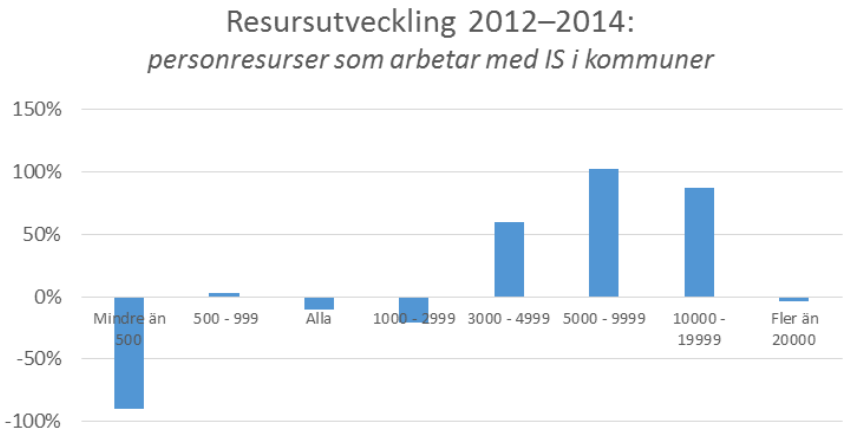
NordSecs undersökning ger möjlighet att sätta den yrkesmässiga användningen av IT för tjänster riktade till medborgare eller företag i förhållande till säkerhetsinitiativen.



De senaste åren har kommunerna fokuserat på att införa digitala plattformar och medborgarorienterade tjänster, och diagrammet visar en tydlig förflyttning mot en större grad digitalisering sedan 2012. Under samma period kan man se att uppmärksamheten på informationssäkerhet har sjunkit för den största andelen kommuner. Tre av fyra kommuner utför fortfarande ett begränsat arbete inom detta område.

Resursinsatser

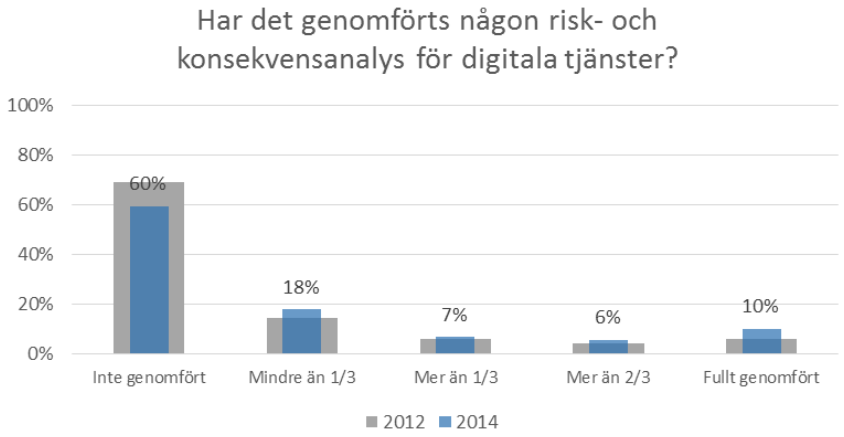
Deltagarna tillfrågades om hur många personresurser som arbetar med informationssäkerhet. Resultatet visar att kommuner med färre än 3 000 medarbetare har svårt att hålla fast vid samma nivå som 2012. Där emot har de större kommunerna kunnat öka resursinsatserna.



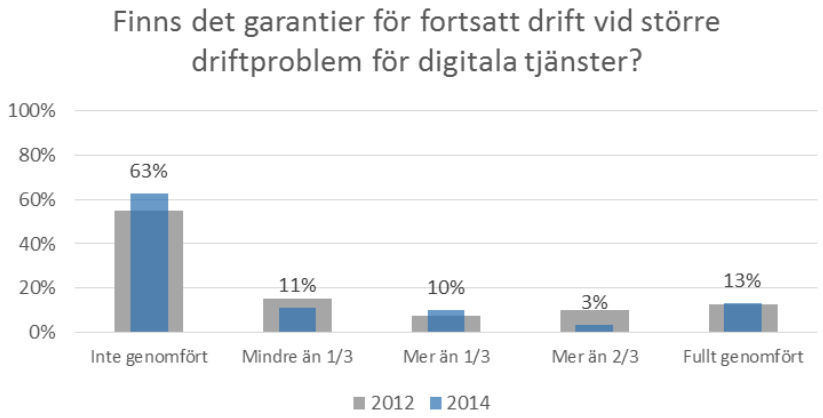
Digitalisering

I samband med omläggningen av medborgartjänster från personalstyrda processer till digitaliserade och automatiserade tjänster som finns tillgängliga via internet ändras riskbilden på flera områden. Hot mot tjänsternas tillgänglighet och informationens konfidentialitet samt konsekvenserna av överträdelse skiftar alla karaktär vid fel, missbruk m.m.

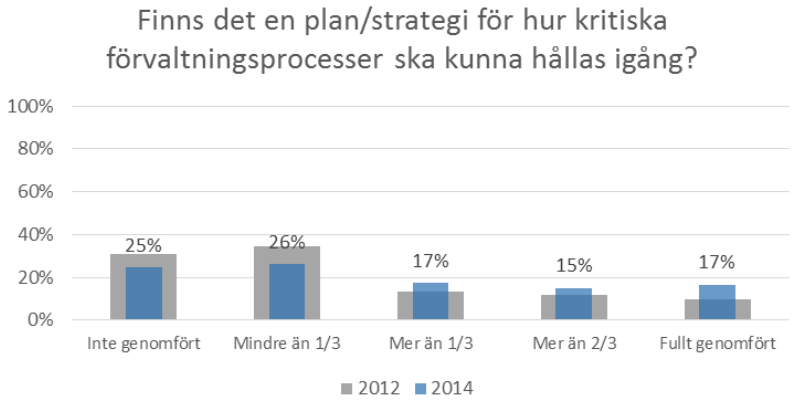
Antalet kommuner som utför risk- och konsekvensanalyser för digitala tjänster har ökat 2014 i jämförelse med 2012. 60 % av kommunerna har inte påbörjat detta.



I och med omläggningen till digitala tjänster ligger kraven inte uteslutande på medarbetares och systems tillgänglighet utan även på medborgares och verksamheters tillgång till digitala tjänster.
Siffrorna för riskhantering visar att en liten del av kommunerna har fokuserat på tillgången till tjänster. Två av tre kommuner har inga garantier för att digitala tjänster ska vara tillgängliga om det inträffar större driftproblem.



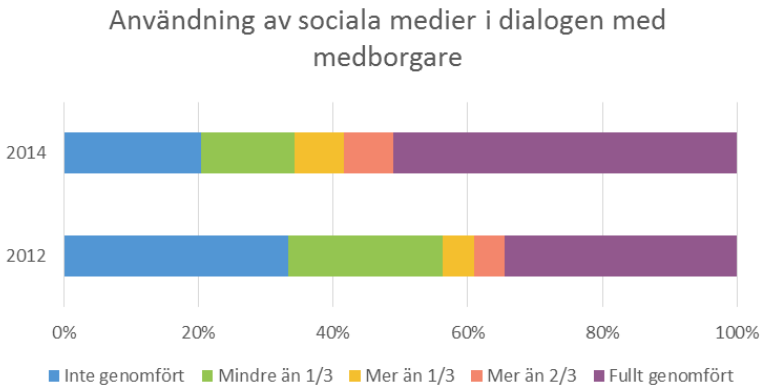
Kommunerna är i ökande omfattning uppmärksamma på att kritiska processer måste kunna hållas igång om det uppstår problem med tillgång till IT eller andra kritiska resurser. Var tredje kommun har en Business Continuity Plan, dvs. en plan för hur tjänster ska kunna utföras om kritiska resurser inte finns tillgängliga.



En fungerade Business Continuity Plan förutsätter lokala handlingsplaner för enskilda förvaltningsområden: en fjärdedel av kommunerna har sådana på plats. Av de kommuner som har en beredskap arbetar var tredje med en regelbunden utbildning och kontroll av beredskapen.

Digital dialog

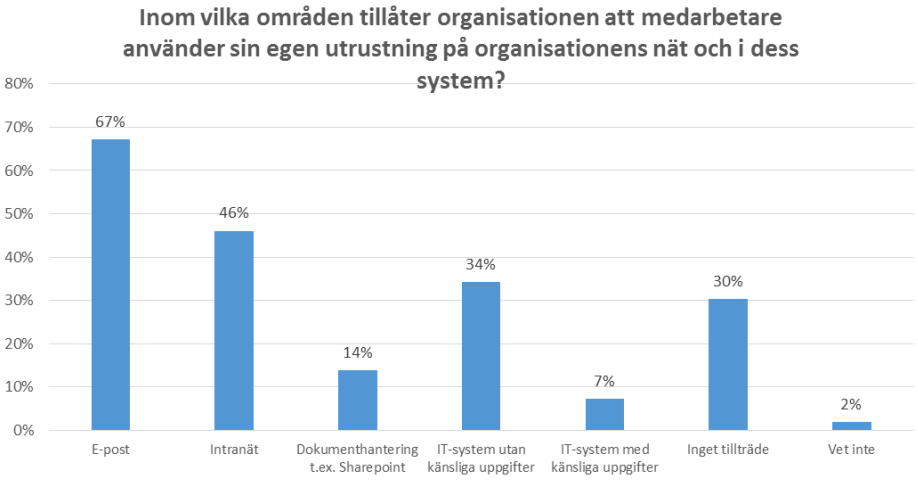
2012 utnyttjade en del av kommunerna informationsteknik till en digital dialog med medborgarna. Digital dialog omfattar bland annat användning av de sociala nätverkens chattfunktioner, information via Facebook och likande. Denna trend har fortsatt under 2014 där varannan kommun arbetar med detta.



Var femte kommun arbetar i en viss omfattning med användning av ljud/videoprogram, som till exempel Skype, som en plattform för dialog med medborgare och verksamheter. Antalet är oförändrat från 2012.

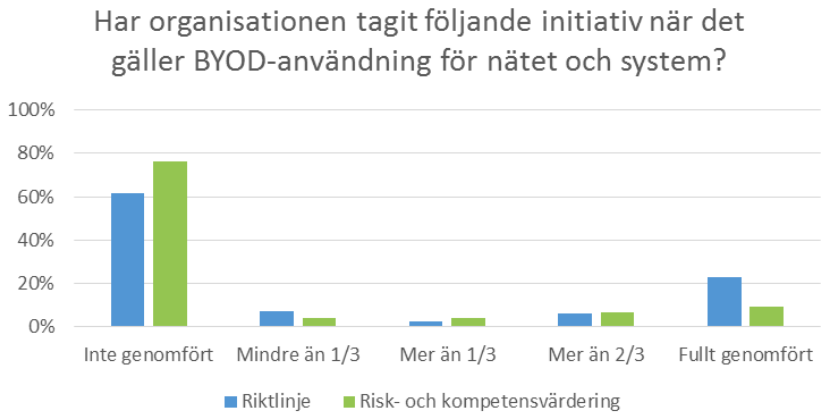
Ny teknik

Under de senaste åren har det skett en betydlig spridning av den utrustning som används tillsammans med informationssystemen (mobila arbetsplatser, telefoner osv.). Denna trend förstärks av att medarbetare i allt större omfattning efterfrågar möjligheten att använda sin egen utrustning på organisationernas nät – både privat och för uppgifter. I undersökningen för 2012 svarade 7 kommuner att de i en viss omfattning tillät medarbetare att använda egen utrustning. 2014 tillåter 2/3 det.



Det är främst för tillgång till e-postsystemet och på Intranätet som de anställda har möjlighet att använda sin egen utrustning. 7 % av kommunerna har get tillgång till applikationer med känsliga uppgifter.

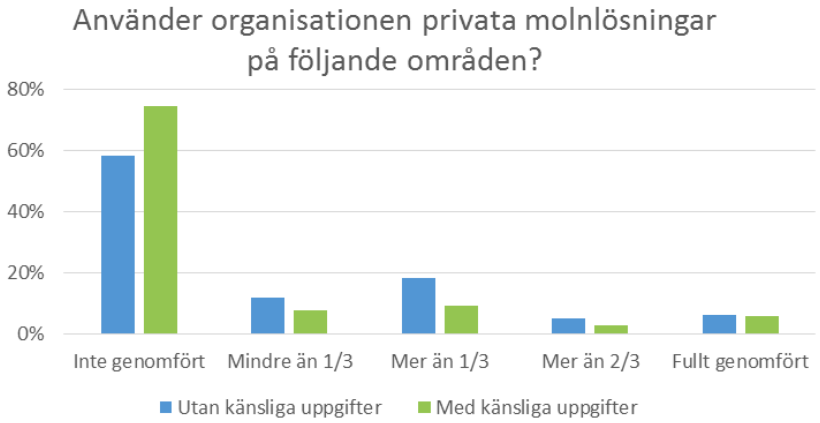
I bland de kommuner som tillåter att medarbetare använder egen utrustning till kommunens nät och system har fem riktlinjer för detta och tio har gjort en riskanalys.



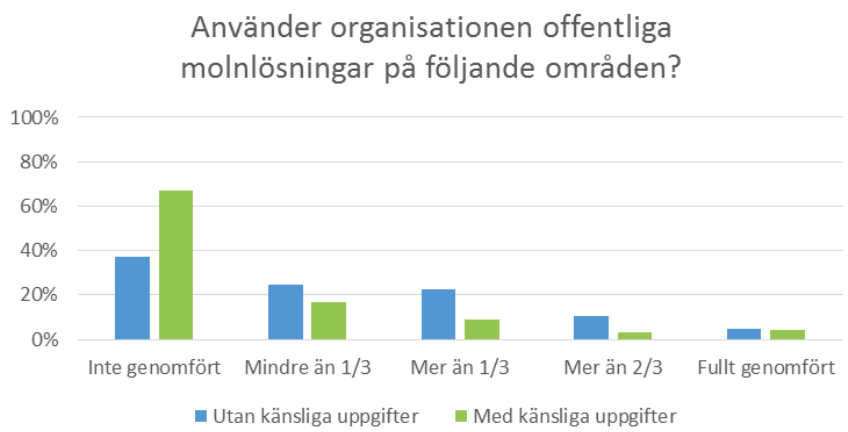
Ingen av de kommuner som tillåter att medarbetare har tillgång till känsliga uppgifter från egen utrustning har riktlinjer för användningen eller har utfört en riskanalys på området.

Användning av molntjänster

Tillgången till molnbaserade tjänster är uppdelade i dedikerade tjänster (Private Cloud) och offentligt tillgängliga tjänster. Som framgår av diagrammet är det enskilda kommuner som använder dedikerade molntjänster oavsett om det är inom områden med känsliga uppgifter eller ej.



När det gäller användningen av offentliga molnlösningar framgår att kommunerna till viss del använder dem för områden med icke-känsliga uppgifter.

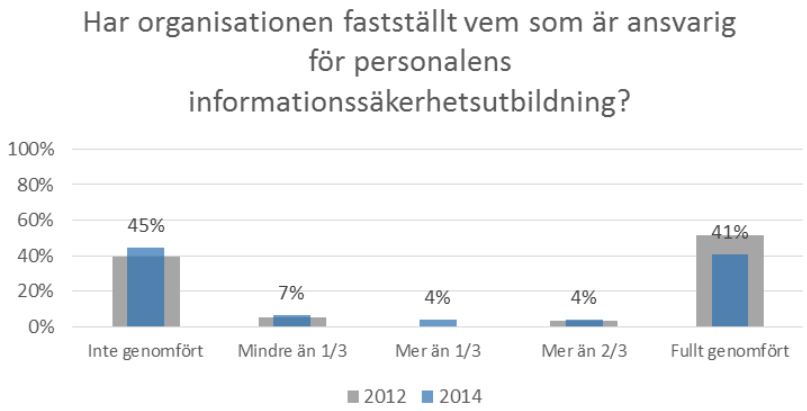


Det finns ett antal rekommendationer för säkerhetshantering i samband med användningen av molnlösningar. Det är avgörande att organisationer tar ställning till de risker som är kopplade till de molnbaserade tjänsterna och man kan se att långt flera kommuner arbetar med detta.

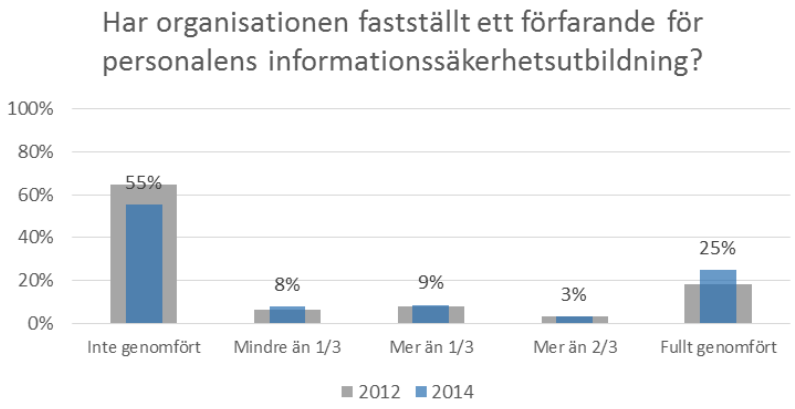
Kompetenskrav för organisationen

I och med användningen av digitala tjänster och digitala plattformar – e-post, digital dialog, m.m. – möts medarbetare av andra och annorlunda utmaningar än förr.

Det framgår att 4 av 10 kommuner har slagit fast ett formellt ansvar inom organisationen för att medarbetare ska ha tillräcklig och relevant kompetens för säker användning – och att knappt hälften inte har arbetat med detta.



Var fjärde kommun har upprättat ett ramverk för genomförandet av personalutbildning – en ökning jämfört med 2012 då det var femte kommun hade upprättat ett. Mer än hälften av kommunerna – färre än 2012 – arbetar inte med detta område.

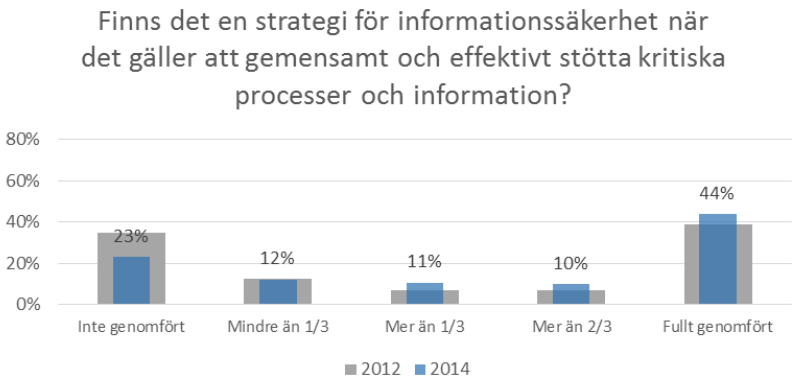


4 % av kommunerna har avsatt medel till initiativ som kan göra medarbetarna uppmärksammare på säker IT-användning – 90 % av kommunerna har inte tagit några initiativ på detta område.

Undersökningen 2012 visade att 5 % av de deltagande kommunerna genomförde mätningar gällande om medarbetarna hade tillräcklig kompetens för säker användning av system och information. Dessa siffror är oförändrade 2014 och 9 av 10 kommuner har inte arbetat med detta.

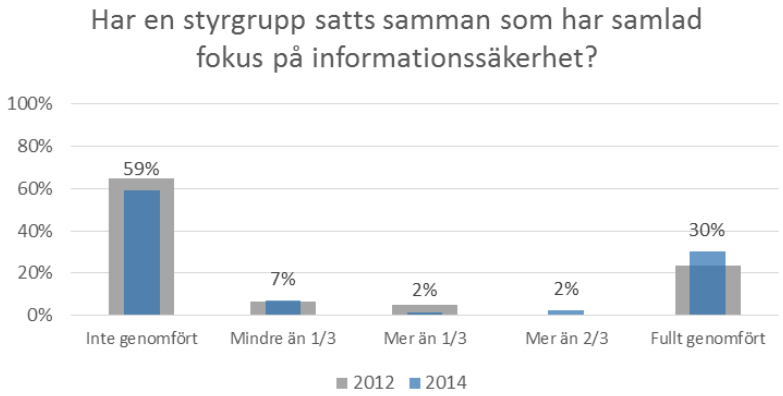
Informationssäkerhet inom organisationen

Införandet av digitala tjänster och användningen av digitala plattformar genomförs i nära samarbete med kommunernas förvaltningsområden. Förändringsprocesserna och den framtida hanteringen är alltså i hög grad kopplade till förvaltningsområdenas uppgifter och ansvar.



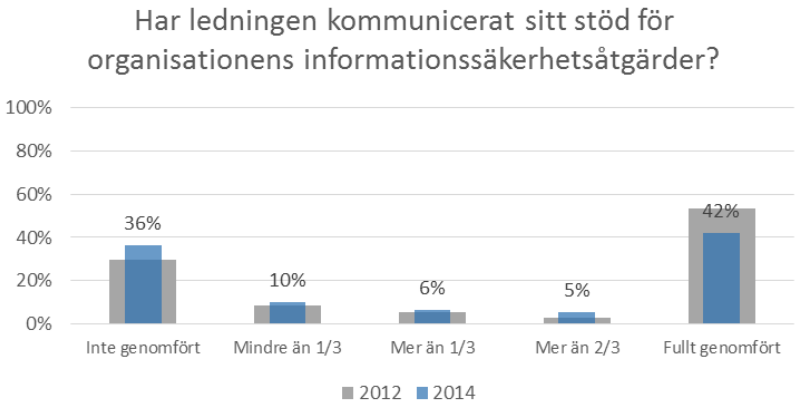
Varannan kommun arbetar med en faktisk strategi för informationssäkerhet.

Förankringen av informationssäkerhetsarbetet inom organisationen omfattar i var fjärde kommun etableringen av styrgrupper som har samlad fokus på området – en ökning i förhållande till 2012.

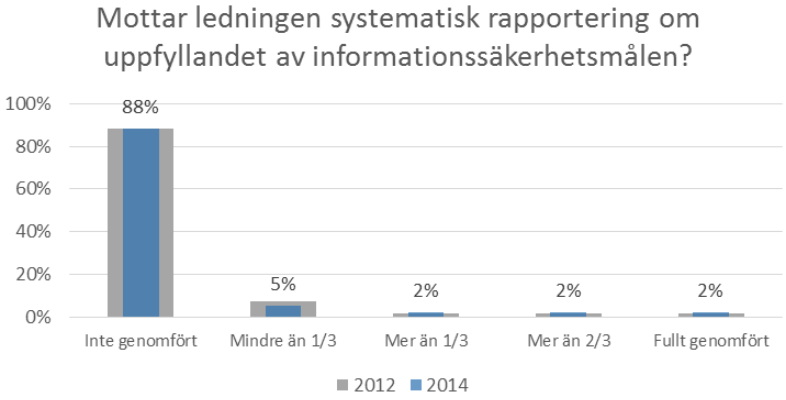


Informationssäkerhet som ledningsområde

Ledningens synliga stöd för organisationens informationssäkerhetsarbete framhävs ofta som en avgörande faktor för god praxis. Detta är fallet i fyra av tio kommuner – en minskande andel i jämförelse med 2012.



Siffrorna ser annorlunda ut för om ledningens stöd för informationssäkerhetsarbete följs upp av regelbunden och systematisk statusrapportering till ledningen. Under 10 % av kommunerna arbetar systematiskt med detta.



Riskhanteringsunderlag är ett av de områden där ledningen kan ha inflytande över säkerhetsarbetet. Detta inflytande kan utövas genom att säkerställa att de metoder som används är välkända och liknar organisationens övriga riskhantering samt att de risker som identifieras övervägs enhetligt.

Mindre än hälften av kommunerna har genomfört en riskanalys för IT-användning som stämmer överens med organisationens övriga riskhantering, och nio av tio kommuner har inte utarbetat kriterier för vad som är acceptabla risker.

För de kommuner som inte har samlad fokus på risker kan riskhanteringen av IT-användning bli avskuren från resten av riskhanteringen i organisationen.