MYNDIGHETEN FÖR DIGITALISERING OCH BEFOLKNINGSDATA

Utredning av nuläget för den digitala säkerheten inom offentlig förvaltning

Rapporter

17.5.2021

Tel. **0295 536 000** (växel) | Kontaktuppgifter, se **www.dvv.fi/sv**

17.5.2021

Innehållsförteckning

17.5.2021

1 Sammanfattning

Finansministeriet och Myndigheten för digitalisering och befolkningsdata ansvarar för utvecklingsprojekt som gäller digital säkerhet. Finansministeriets verkställighetsplan för den digitala säkerheten inom den offentliga förvaltningen 2020–2023 (Haukka-projektet) verkställer statsrådets principbeslut av den 8 april 2020. Haukka-projektets uppgifter vid Myndigheten för digitalisering och befolkningsdata genomförs i JUDO-projektet. I projekten Haukka och JUDO görs omfattande utredningar, som flera organisationer inom den offentliga förvaltningen och den privata sektorn har deltagit i tillsammans med sina experter.

Denna rapport gäller kartläggningen av nuläget för de system för klassificering av digital säkerhet och kritiskhet som görs som en del av genomförandeplanen samt nuläget för den offentliga förvaltningens säkerhetsarkitektur och överensstämmelse med kraven. Kartläggningen av nuläget genomfördes med hjälp av två enkäter som totalt 186 offentliga organisationer deltog i och som omfattade kommuner, statliga ämbetsverk, sjukvårdsdistrikt, universitet och yrkeshögskolor. Resultaten från analysen av enkäten har sammanställts i denna rapport. Resultaten från den första enkäten som riktades till kommunerna och sjukvårdsdistrikten har sammanställts i en separat rapport som behandlar kommunernas gemensamma tjänster som främjar digital säkerhet och behov i samband med dem.

En central iakttagelse i denna rapport var att de statliga ämbetsverken, sjukvårdsdistrikten och universiteten allmänt taget har kommit något längre i verkställandet av den digitala säkerheten än kommunerna och yrkeshögskolorna, även om det finns undantag. För sjukvårdsdistriktens del beror förmågan inom den digitala säkerheten i hög grad på karaktären på sjukvårdsdistriktens verksamhet, medan de statliga ämbetsverken och universiteten i fråga om den digitala säkerheten har bildat nätverk i större utsträckning än kommunerna och yrkeshögskolorna samt övar på undantagstillstånd som rör den digitala säkerheten i större utsträckning än andra.

I analysen av enkäten identifierades föregångare med tydliga framgångar inom ett eller flera delområden. Samma egenskaper förenade föregångare inom den digitala säkerheten. De viktigaste av dessa egenskaper är förmågan att upptäcka undantagstillstånd i den digitala säkerheten och fungera effektivt när sådana inträffar, regelbundna övningar och utbildningar i digital säkerhet, klassificering av objekt som är kritiska för verksamheten samt metoder för bedömning av den digitala säkerheten och dess aktualitet.

Resultaten från enkäten består av självbedömning av respondenterna, vilket ska beaktas när svaren analyseras och tolkas. Resultaten varierar beroende på deltagarens kompetens, erfarenhet och uppfattningar. Det är meningen att resultaten från enkäten ska preciseras genom temaintervjuer, och resultaten från dem kommer att användas för att fastställa nuläget och den nationella målbilden för den digitala säkerheten.

2 Nuläget för den nationella förmågan beträffande den digitala säkerheten

Syftet med enkäten var att kartlägga nuläget för den nationella förmågan beträffande informationssäkerheten inom den offentliga förvaltningen, för det första för att utreda hur organisationerna inom den offentliga förvaltningen har identifierat de digitala

tjänster, serviceprocesser, informationssystem, den infrastruktur, information och de informationsflöden som är kritiska för organisationens verksamhet och som kan vara förknippade med särskilda krav på den nationella förvaltningen och tryggandet av den. Å andra sidan försökte man med hjälp av enkäten också utreda hurdana klassificeringssystem för kritiskhet den offentliga förvaltningen har till sitt förfogande för att identifiera och bedöma ovan nämnda kritiska objekt.

Enkäten kommer att kompletteras med riktade temaintervjuer för att få bättre information om hur den offentliga förvaltningen identifierar digitala objekt som är kritiska för både sin verksamhet och samhället och hur nuläget ser ut i fråga om överensstämmelse med kraven när det gäller den offentliga förvaltningens informationssäkerhet.

Denna rapport analyserar resultaten från enkäten som skickades till kommunerna, statsförvaltningens organisationer, sjukvårdsdistrikten samt universiteten och yrkeshögskolorna. Sammanlagt svarade 186 personer på enkäten. I enkäten utreddes centrala faktorer i anslutning till digital säkerhet och hur de förverkligas.

Utifrån enkätresultaten identifierades föregångare, det vill säga offentliga organisationer, som hade tydliga framgångar inom ett eller flera delområden.

Respondenterna har delats in i fem grupper enligt organisationstyp – kommuner, enheter inom statsförvaltningen, sjukvårdsdistrikt, universitet och yrkeshögskolor. Sjukvårdsdistrikten, universiteten och yrkeshögskolorna granskas som en grupp. I analysen av kommunernas och statsförvaltningens enheters svar har man även beaktat organisationens personalantal.

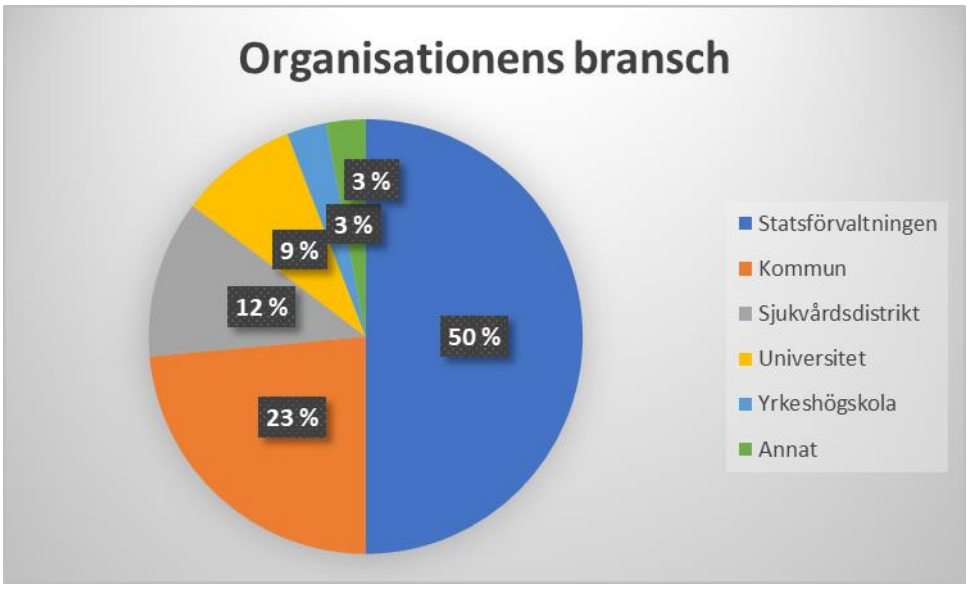
2.1 Föregångare inom digital säkerhet

I det här avsnittet har vi samlat de viktigaste framgångsfaktorerna för att skapa en bra digital säkerhetsnivå. Utifrån dessa faktorer har man identifierat föregångare inom digital säkerhet i enkätmaterialet.

I enkätsvaren identifierades en grupp bestående av 34 organisationer som utifrån svaren kan betraktas som föregångare inom digital säkerhet. Den största gruppen föregångare utgörs av medelstora organisationer inom statsförvaltningen (17 st.).

Figur 1. Föregångarnas fördelning enligt organisationsstorlek

Figur 2. Föregångarnas fördelning enligt organisationernas verksamhetsområde

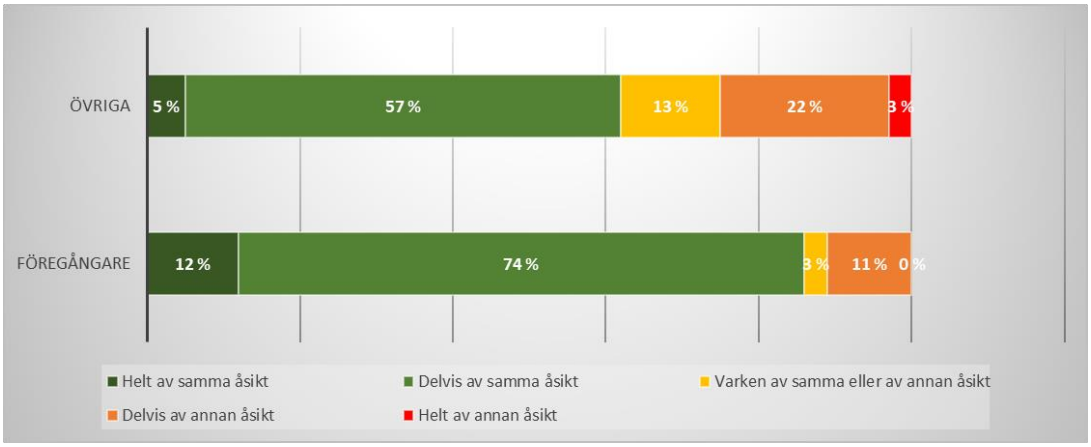


I korthet har föregångarna följande egenskaper:

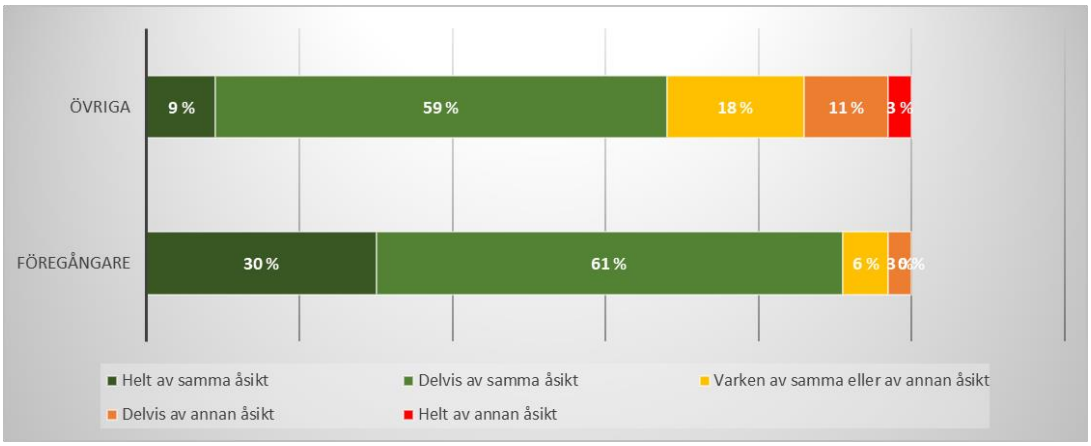
- övningar och utbildningar i digital säkerhet ordnas regelbundet
- objekt som är kritiska för verksamheten har identifierats och klassificerats
- det finns metoder för bedömning av informationssäkerheten och dess aktualitet

När dessa grundläggande saker är i ordning har organisationerna bättre tilltro till att de har förmåga att upptäcka olika avvikelser i informationssäkerheten (Figur 3, i enkäten var 86 % helt av samma åsikt eller delvis av samma åsikt) och att agera effektivt i dessa undantagstillstånd (Figur 4, 91 % var helt av samma åsikt eller delvis av samma åsikt). Bland de övriga respondenterna är resultaten cirka 20 procentenheter lägre.

Figur 3. Förmåga att upptäcka avvikelser i databehandlingen



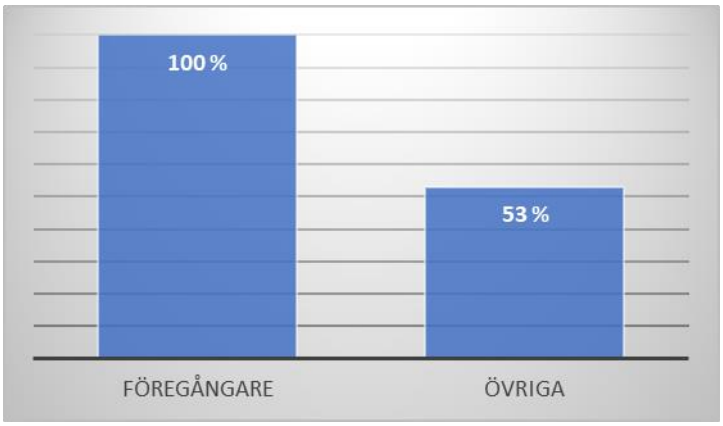
Figur 4. Förmåga att agera effektivt vid avvikelser och snabbt återgå till normal verksamhet



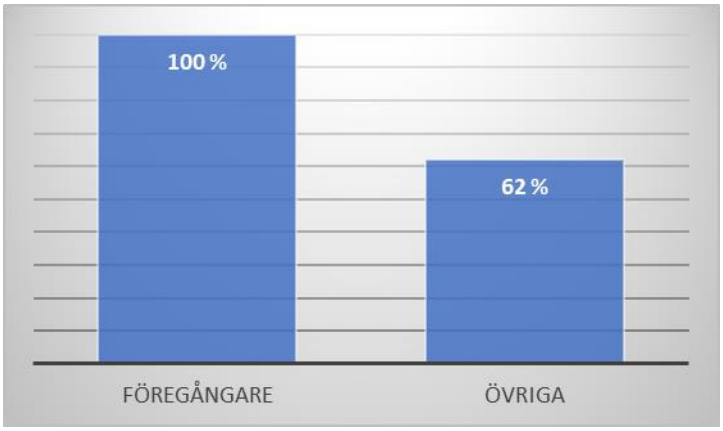
2.1.1 Övningar och utbildningar

Av föregångarna övar alla (Figur 5) på att agera vid informationssäkerhetsincidenter minst en gång om året. Alla ordnar också regelbundet utbildning och introduktion i digital säkerhet (0).

Figur 5. Övning på informationssäkerhetsincidenter minst en gång om året

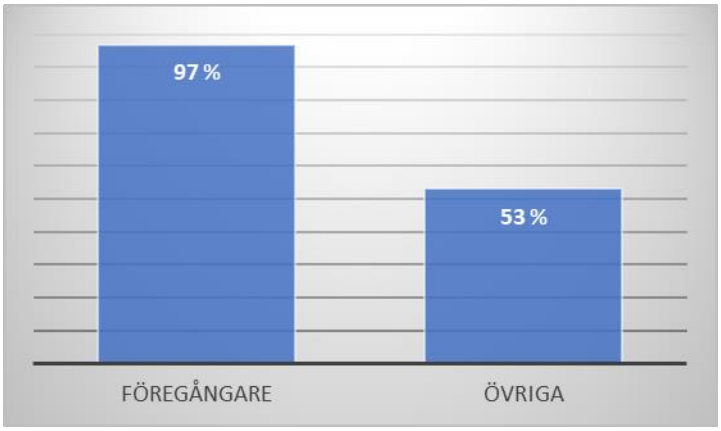


Figur 6. Regelbunden utbildning och introduktion i digital säkerhet



Nästan alla föregångare (0, 97%) uppgav också att de kan beakta frågor som gäller den digitala säkerheten väl i upphandlingar.

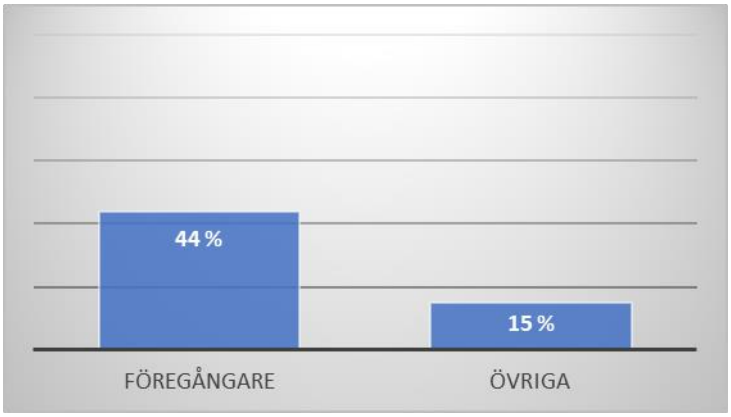
Figur 7. Beaktande av digital säkerhet i upphandlingar



2.1.2 Personal

En betydligt större andel av föregångarna (Figur 8, 44%) upplever också att deras organisation har tillräckligt med personal för att ta hand om den digitala säkerheten. Medeltalet bland de övriga respondenterna var endast 15 %.

Figur 8. Tillräckligt med personal inom digital säkerhet



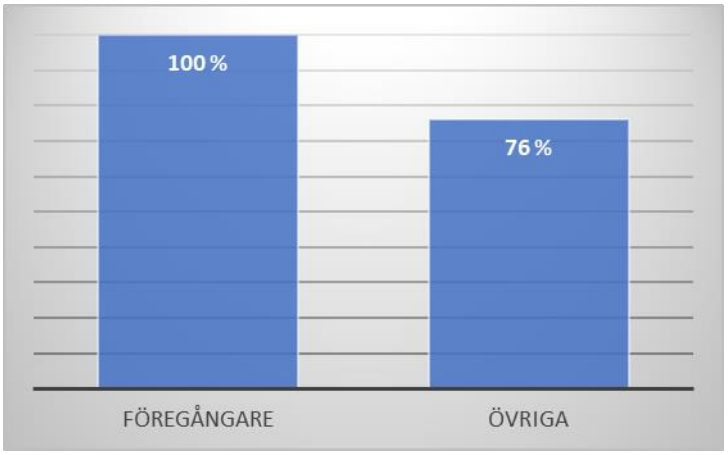
I vilket fall som helst var det en gemensam utmaning för alla respondenter att ha tillräckligt med personal inom digital säkerhet. Det rekommenderas att man fäster uppmärksamhet vid det antingen genom att stärka det egna kunnandet eller nätverket av samarbetspartner.

2.1.3 Kritiska objekt

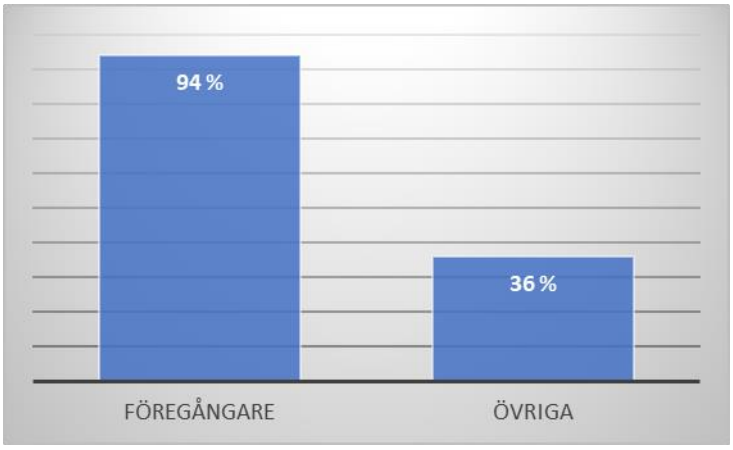
Föregångarna känner väl till och klassificerar objekt som är kritiska med tanke på organisationens digitala säkerhet. Av föregångarna hade alla (Figur 9, 100 %) identifierat kritiska objekt för sin verksamhet och nästan alla (Figur 10, 94 %) hade också ett sätt att klassificera dessa kritiska objekt. Bland de övriga respondenterna var identifieringen av kritiska objekt på en något lägre nivå (76 %). I fråga om klassificeringsmetoderna för kritiska objekt var de övriga respondenterna på en betydligt lägre nivå (36 %). Detta indikerar att organisationerna visserligen i regel identifierar objekt som är

kritiska för sin verksamhet, men de gör det inte systematiskt med hjälp av en viss metod eller referensram. Detta kan leda till att organisationerna inte har en helhetsbild av alla sina kritiska objekt.

Figur 9. Identifiering av objekt som är kritiska för verksamheten

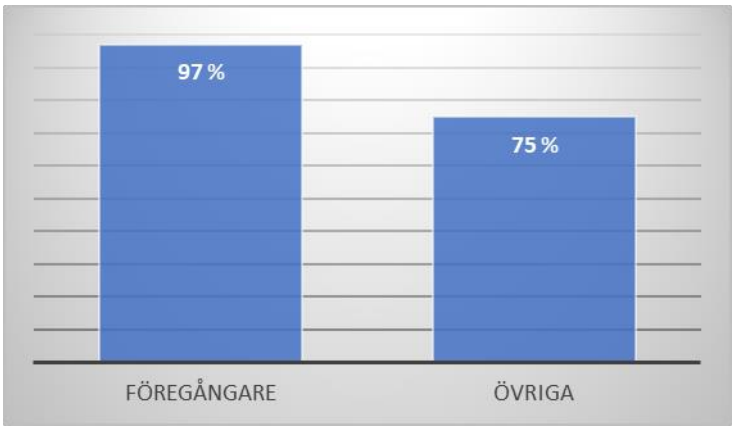


Figur 10. Klassificeringsmetod för kritiska objekt



Nästan alla föregångare (0, 97 %) har också tillgång till ett register över informationssystem eller något annat motsvarande sätt att upprätthålla aktuell information om informationssystemen, medan tre av fyra av de övriga respondenterna använder ett informationssystem. De bäst identifierade kritiska objekten för alla grupper av respondenter var informationssystemen och processerna, medan uppgifter och informationsflöden var sämst identifierade (se Kritiska objekt).

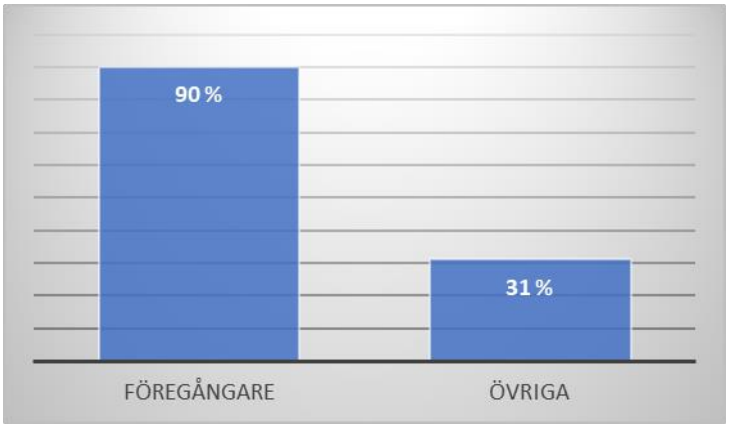
Figur 11. Register över informationssystem eller motsvarande sätt att upprätthålla aktuell information om informationssystemen



2.1.4 Metoder

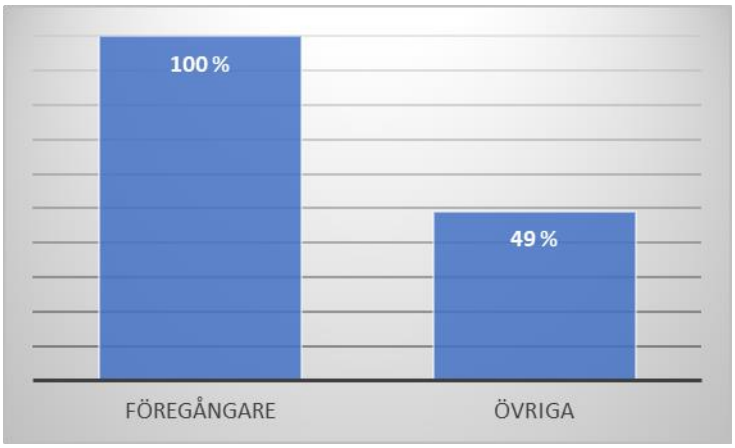
I fråga om metoderna skiljde sig föregångarna från andra organisationer i bedömningen av informationssäkerheten och dess aktualitet. Nästan alla (Figur 12, 90 %) föregångare hade en metod för att bedöma om informationssäkerheten är aktuell i de digitala tjänster och teknologier som används, medan resultatet bland de övriga respondenterna var endast 31 %.

Figur 12. Metod för bedömning av säkerheten hos de digitala tjänster som används



Alla (0) föregångare hade också en metod för bedömning av informationssäkerheten i digitala tjänster och teknologier, medan medeltalet för de övriga respondenterna var 49 %.

Figur 13. Metod för bedömning av informationssäkerheten för digitala tjänster och teknologier som ska upphandlas

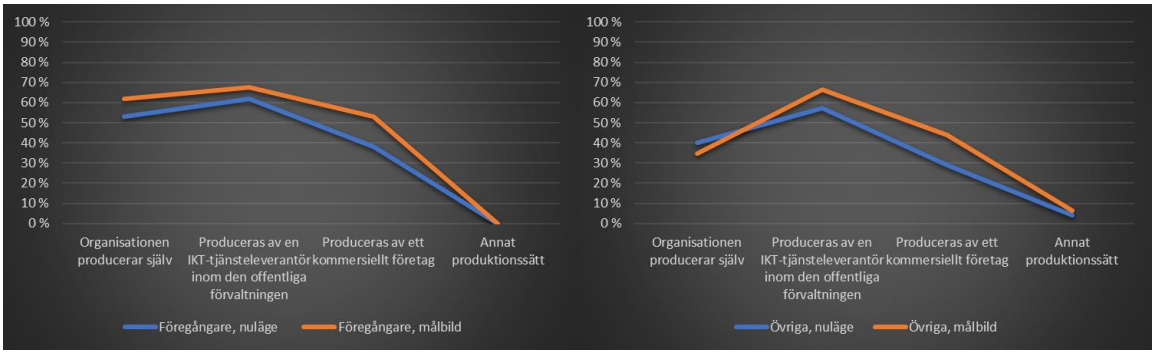


2.1.5 Tillhandahållande av tjänster

I frågor som gällde ordnandet av IKT-tjänster producerade föregångarorganisationerna konsekvent fler tjänster själva än genomsnittet. De förlitade sig dock inte enbart på den egna tjänsteproduktionen, utan samarbetspartner producerar också en del av tjänsterna. Att komplettera den egna kompetensen med ett starkt nätverk av samarbetspartner inom tjänsteproduktionen för digital säkerhet verkar vara en stark trend även när det gäller målbilden för att organisera tjänsteproduktionen.

Cirka hälften av föregångarna producerar själva observations-, reaktions- och analystjänster (säkerhetsoperationscenter) för händelser i datakommunikationsnätet i nuläget (Figur 14). Målbilden är att det till och med ska bli en aning populärare att producera en tjänst själv. När man övergår från nuläget till målbilden ökar dock viljan att också producera dessa tjänster med hjälp av ett kommersiellt företag eller en IKT-tjänsteleverantör inom den offentliga förvaltningen utöver den egna tjänsteproduktionen.

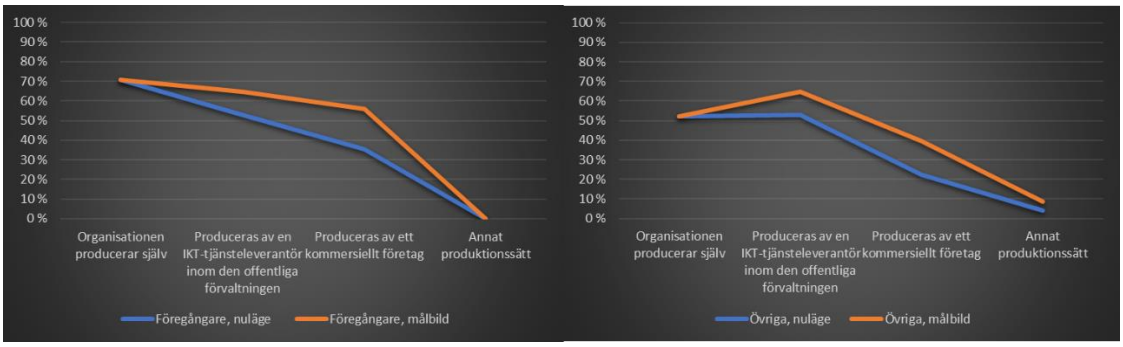
Figur 14. Produktion av observations-, reaktions- och analystjänster för händelser i datakommunikationsnätet i nuläget och enligt målbilden



Observationen av organisationens interna informationssäkerhetshot genom teknisk övervakning som produceras själv ligger på samma nivå både i nuläget och enligt

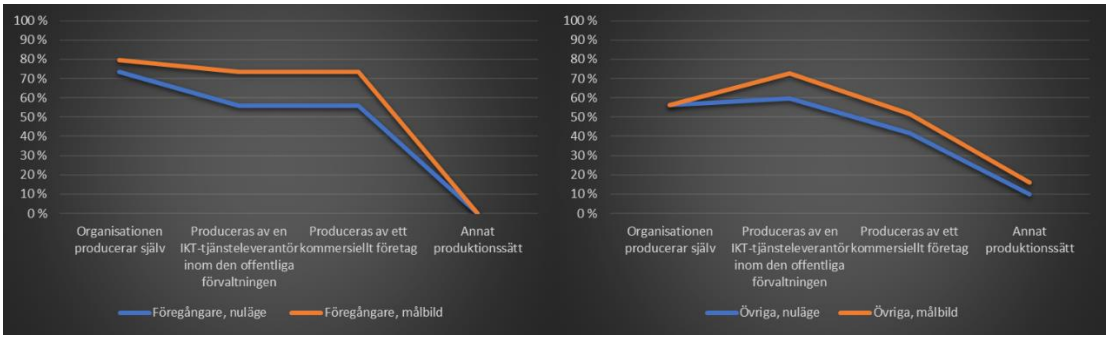
målbilden. Däremot ökar utvidgningen av tjänsteproduktionen med hjälp av tjänster från kommersiella företag eller den offentliga förvaltningens IKT-serviceproducenter betydligt jämfört med nuläget när man övergår till målbilden (**Virhe. Viitteen lähdettä ei löytynyt.**).

Figur 15. Observation av organisationens interna informationssäkerhetshot genom teknisk övervakning



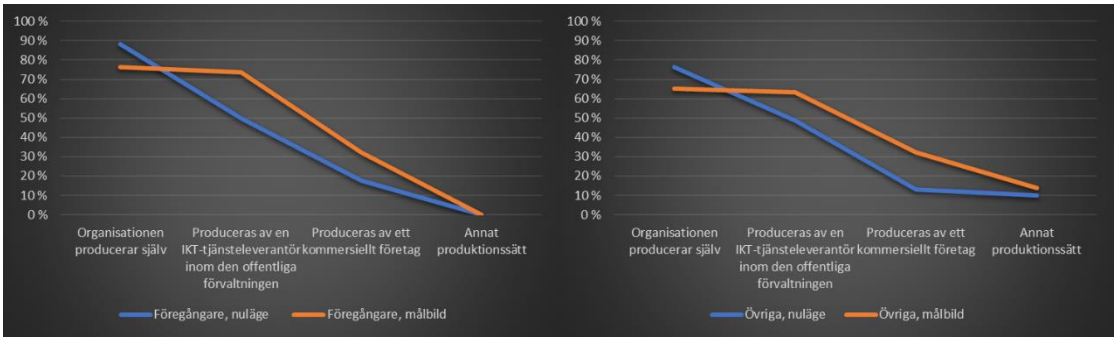
En liknande trend observeras också i expertstödstjänsterna för allvarliga kränkningar av informationssäkerheten. Föregångarna producerar dessa tjänster själva i hög grad både i nuläget och enligt målbilden, men man kommer även att förlita sig mycket på samarbetspartner (både kommersiella och offentliga) i framtiden (Figur 16). När man övergår från nuläget till målbilden ökar användningen av tjänster från såväl den offentliga förvaltningens IKT-serviceproducenter som från kommersiella aktörer.

Figur 16. Expertstöd vid allvarliga kränkningar av informationssäkerheten

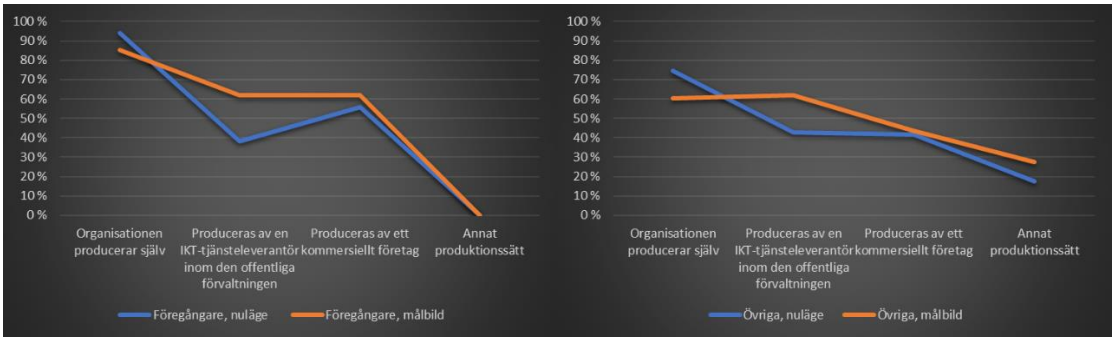


Utöver de ovan beskrivna tjänsterna förlitar sig organisationerna också starkt på sin egen kompetens när man meddelar om informationssäkerhetshot som håller på att spridas (0) samt i fråga om expertstöd för genomförande av informationshanteringslagen och digital säkerhet (Figur 18).

Figur 17. Meddelanden om informationssäkerhetshot som håller på att spridas



Figur 18. Expertstöd för genomförande av informationshanteringslagen och digital säkerhet



Andelen tjänster som man producerar själv är betydligt större bland föregångarna än bland övriga respondenter. Detta innebär dock inte att alla borde producera tjänsterna själva. Det är viktigare att beakta det omfattande nätverk av samarbetspartner som framgår av föregångarnas svar. Med hjälp av nätverket kan organisationen själv leda IKT-tjänsteproduktionen för den digitala säkerheten och komplettera sin egen kompetens med hjälp av lämpliga tjänster från antingen den offentliga förvaltningen eller kommersiella företag.

2.2 De viktigaste utvecklingsobjekten

I det här avsnittet har de viktigaste utvecklingsobjekten som identifierats på basis av enkäten sammanställts. Utifrån resultaten identifierades utvecklingsområden som de som inte är föregångare kan utgå ifrån för att förbättra sin digitala säkerhetsnivå.

De organisationer vars digitala säkerhet behöver utvecklas mer än genomsnittet är enligt enkäten kommuner med färre än 500 anställda eller små enheter inom statsförvaltningen. Även yrkeshögskolorna har mer att utveckla i fråga om den digitala säkerheten än vad universiteten har.

De viktigaste utvecklingsobjekten är de delområden som beskrivs i föregående stycke och som utgjorde framgångsfaktorer bland föregångarna. I de organisationer som hade mest att utveckla ordnas övningar och utbildningar i digital säkerhet oregelbundet eller inte alls. Det finns också brister i identifieringen av kritiska objekt och de kritiska objekt som har identifierats har knappt blivit klassificerade. En brist som

observerats i enkäten är metoden för bedömning av informationssäkerhetens aktualitet, både i de digitala tjänster och teknologier som används och de som ska skaffas.

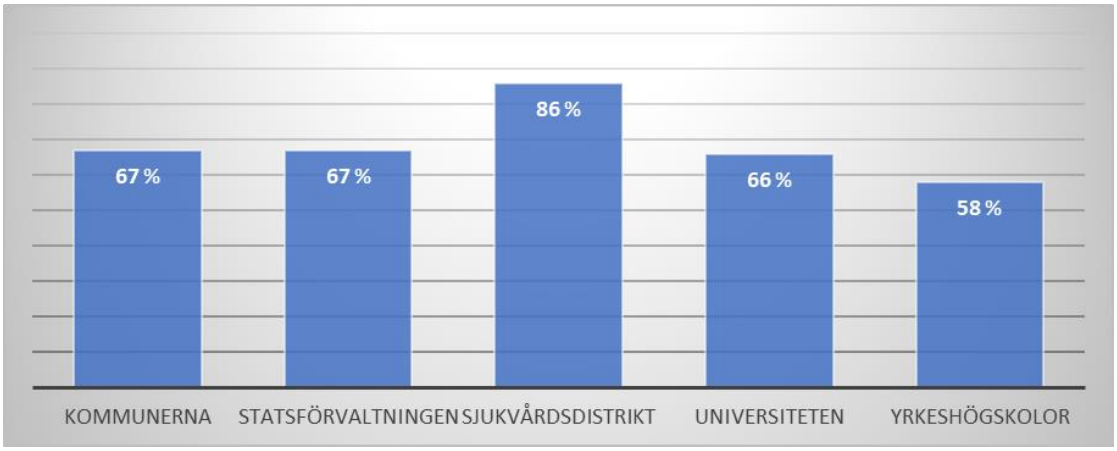
Organisationer som har mer att utveckla inom digital säkerhet producerar färre IKT-tjänster själva än vad föregångarna gör. Detta tyder på att styrningen av tjänsteproduktionen och den digitala säkerheten blir bristfälliga när IKT-tjänsteproduktionen läggs ut på entreprenad och att organisationen inte kan få en realistisk lägesbild av den egna digitala säkerhetsnivån. Man måste komma ihåg att organisationen alltid ansvarar för sin egen digitala säkerhet, även om tjänsteproduktionen har lagts ut på entreprenad till en samarbetspartner.

3 Hantering av digital säkerhet

3.1 Observations- och reaktionsförmåga

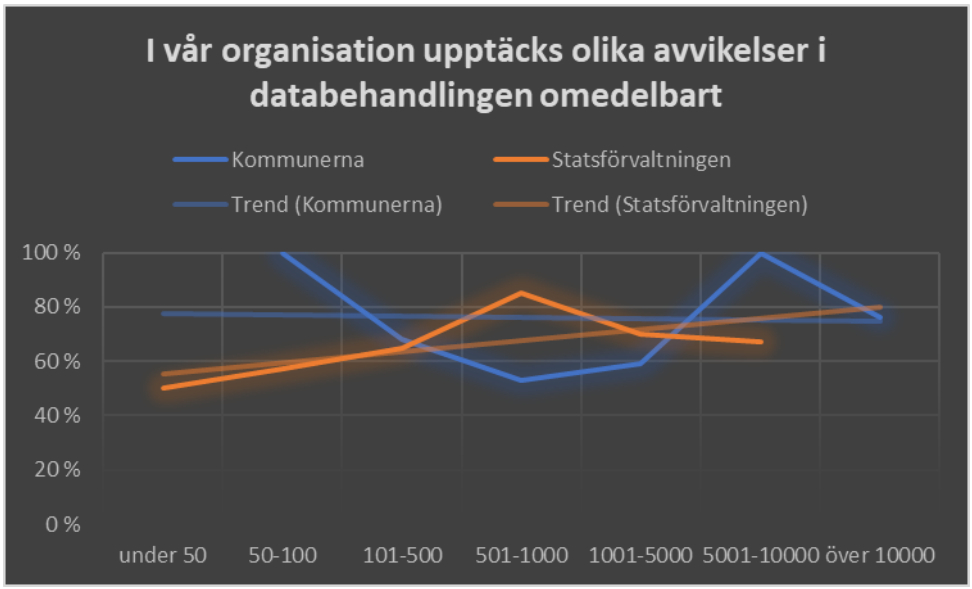
Allmänt taget har organisationer inom den offentliga förvaltningen stort förtroende för förmågan att observera olika typer av avvikelser i databehandlingen. Sjukvårdsdistrikten och social- och hälsovårdsorganisationerna avviker bland organisationerna inom den offentliga förvaltningen.

Figur 19. I vår organisation upptäcks olika avvikelser i databehandlingen omedelbart



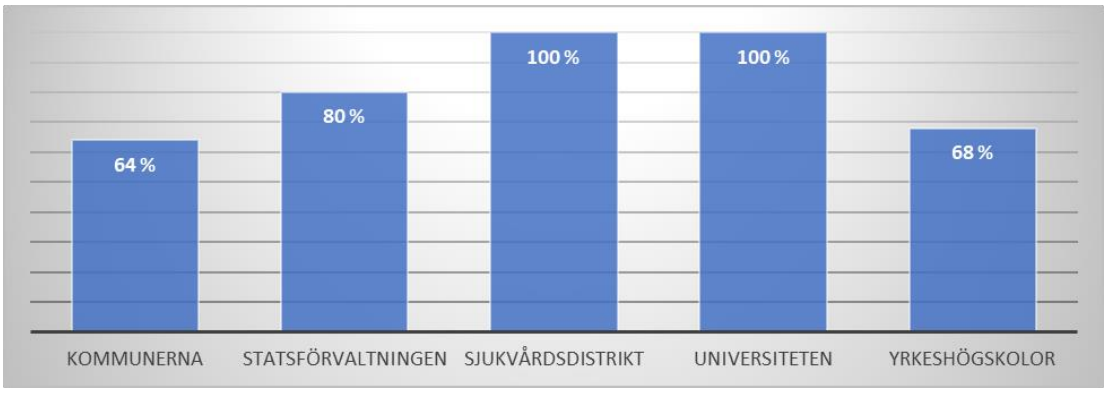
Kommunerna och statsförvaltningen verkar ha samma observationsförmåga (Figur 19), men när man granskar svaren enligt organisationens storlek märks skillnader mellan kommunerna och statsförvaltningens enheter (Figur 20). Små kommuner har betydligt större förtroende för sin observationsförmåga än enheter inom statsförvaltningen av samma storlek. När storleken ökar minskar kommunernas förtroende och statsförvaltningens ökar tills kommunfältets förtroende i fråga om stora organisationer blir större än bland statsförvaltningens organisationer. Orsakerna till detta kan vara bättre medvetenhet om informationssäkerheten vid små enheter inom statsförvaltningen och stora organisationers möjligheter att investera i förmågan att observera avvikelser. Små kommuner kan lita på sina IKT-servicepartners observationsförmåga och de har inte nödvändigtvis möjlighet att bedöma om det finns täckning för förtroendet.

Figur 20. Förtroende för förmågan att observera avvikelser (kommunerna och statsförvaltningen)



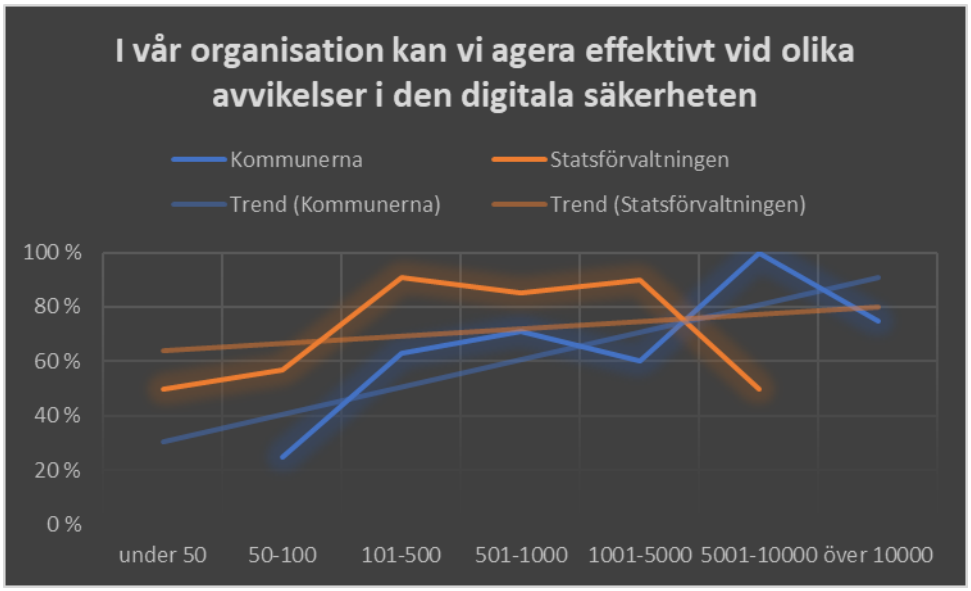
När man granskar reaktionsförmågan vid undantagstillstånd märker man att skillnaderna ökar mellan organisationstyperna. Sjukvårdsdistriktens och universitetens reaktionsförmåga är enligt alla respondenters bedömning som den ska, statsförvaltningen är på en högre nivå än kommunernas och yrkeshögskolornas reaktionsförmåga (Figur 21). Sjukvårdsdistriktens förtroende förklaras sannolikt av karaktären på sjukvårdsdistriktens verksamhet och de krav som ställs på verksamheten.

Figur 21. I vår organisation kan vi agera effektivt vid olika avvikelser i den digitala säkerheten och snabbt återgå till normal verksamhet



När man granskar skillnaderna mellan kommunerna och statsförvaltningen stiger förtroendetrenden i båda grupperna i takt med att organisationsstorleken ökar, men utgångsnivån i små kommuner är betydligt lägre än i enheter av motsvarande storlek inom statsförvaltningen (Figur 22).

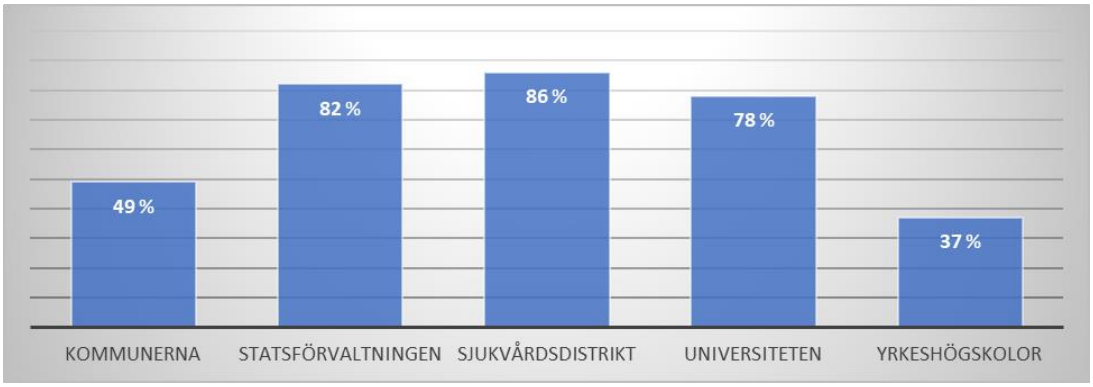
Figur 22. Förtroende för reaktionsförmågan (kommunerna och statsförvaltningen)



3.2 Övning och utbildning

Agerande i informationssäkerhetssituationer övas betydligt mer vid statsförvaltningens enheter, i sjukvårdsdistrikten och på universiteten än i kommunerna och yrkeshögskolorna (Figur 23). Skillnaden är framträdande och torde bero på att statsförvaltningen, sjukvårdsdistrikten och universiteten mer aktivt deltar i informationssäkerhetsövningar och samarbetsnätverk för informationssäkerhet.

Figur 23. Vi övar minst en gång om året på att agera i informationssäkerhetssituationer

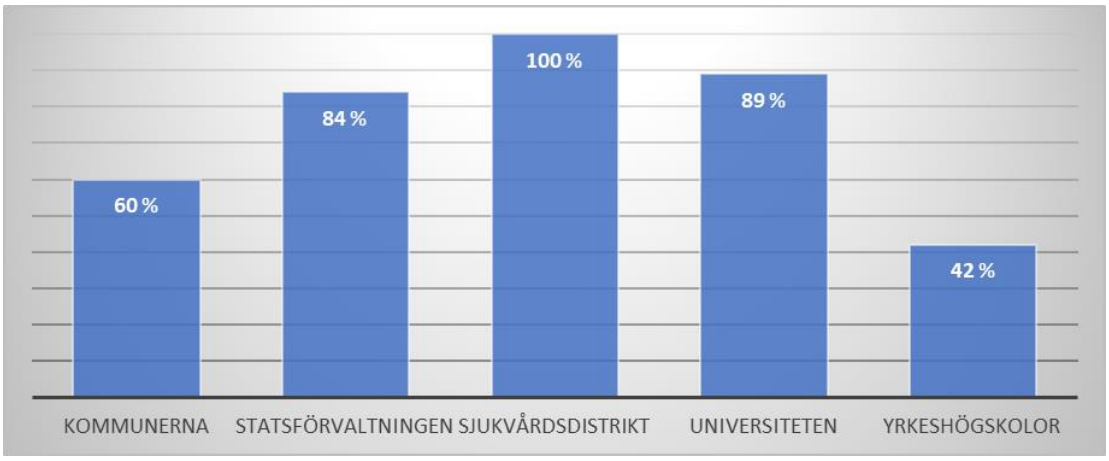


När man jämför kommunerna och statsförvaltningen märker man en trend enligt vilken övandet ökar i takt med att organisationsstorleken växer (Figur 24). Det är anmärkningsvärt att den kommunala sektorns övande oberoende av organisationsstorlek är på en klart lägre nivå än inom statsförvaltningen. Särskilt oroväckande är situationen i kommunorganisationer med färre än 100 personer, där man enligt svaren inte alls övar på att agera i informationssäkerhetssituationer.

Figur 24. Övning i informationssäkerhetssituationer (kommunerna och statsförvaltningen)

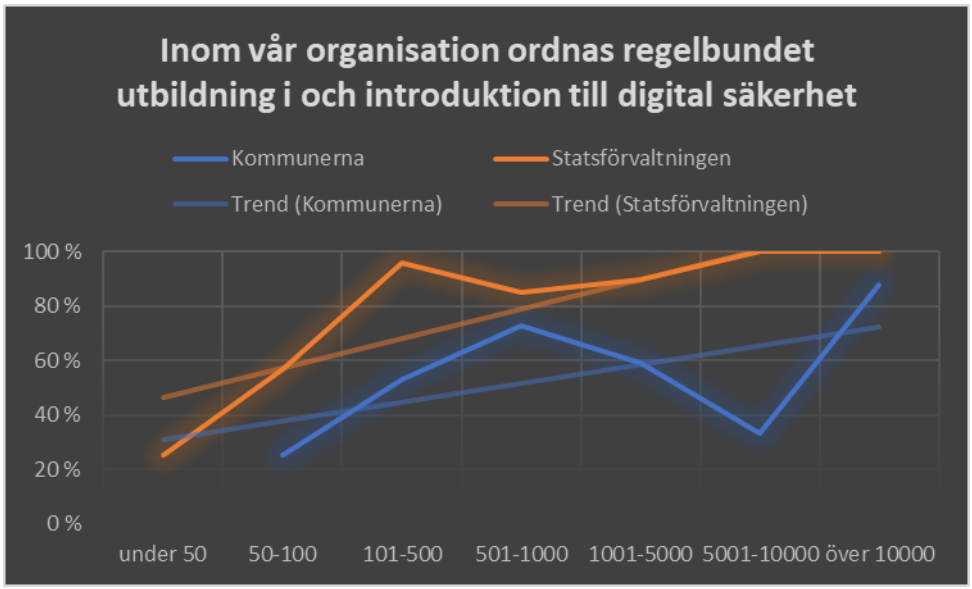
Regelbunden utbildning och introduktion i digital säkerhet ordnas väl i sjukvårdsdistrikten, på universiteten och i statsförvaltningens organisationer (Figur 25). Bland sjukvårdsdistriktens respondenter uppgav alla att de ordnar regelbunden utbildning i digital säkerhet, vilket andra organisationer kan ta modell av. Kommunerna och yrkeshögskolorna låg också i detta fall på en något lägre nivå än de övriga respondentgrupperna.

Figur 25. Vår organisation ordnar regelbundet utbildning i och introduktion till digital säkerhet



När man jämför kommunerna och statsförvaltningen märker man samma trend som när det gäller observationsförmågan – ju större organisation, desto mer utbildning i digital säkerhet ordnas (Figur 26). Den enda skillnaden i kurvan är egentligen att kommunerna är på en lägre nivå över hela linjen. Detta är ett tydligt utvecklingsobjekt i kommunerna, liksom i yrkeshögskolorna. Det framgick av svaren att de organisationer som övar på att agera vid informationssäkerhetsincidenter också ordnar mer informationssäkerhetsutbildning än andra organisationer.

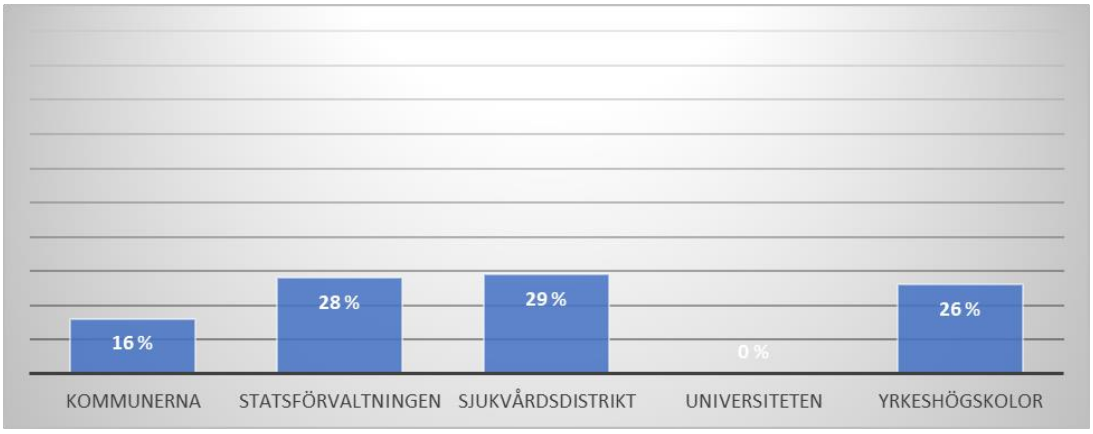
Figur 26. Utbildning i digital säkerhet (kommunerna och statsförvaltningen)



3.3 Resurser för digital säkerhet

Generellt sett anser alla respondenter att det inte finns tillräckligt med personal för den digitala säkerheten (Figur 27). Det något större antalet jakande svar bland små organisationer kan förklaras med att de i brist på egna informationssäkerhetspersoner förlitar sig mer på sina IT-servicepartner än stora organisationer, såsom det kommunala företaget för IKT-tjänsteproduktion eller, i fråga om statsförvaltningen, till exempel Valtoris tjänster.

Figur 27. Vår organisation har tillräckligt med personal för att ta hand om den digitala säkerheten



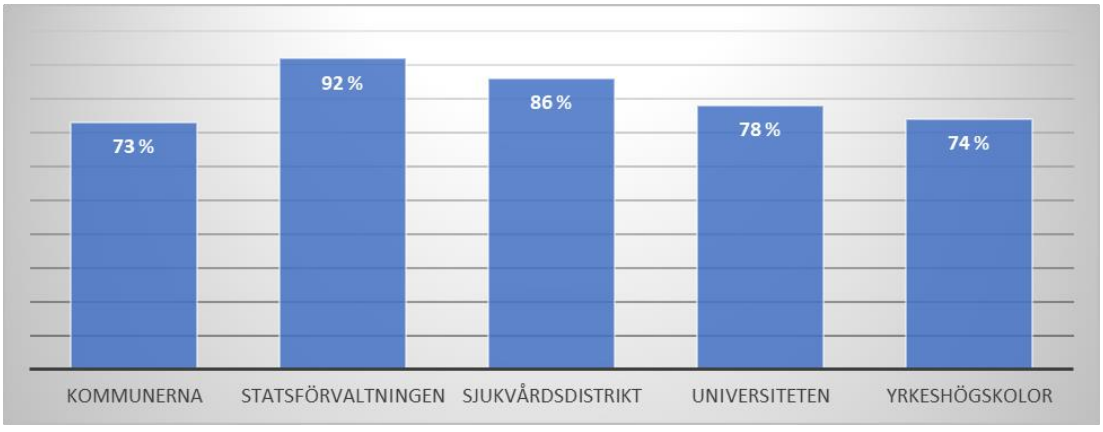
När kommunerna och statsförvaltningen jämförs är det intressant att notera att trenden inom statsförvaltningen sjunker när organisationsstorleken ökar, men stiger något i kommunerna (Figur 28).

Figur 28. Personal inom digital säkerhet (kommunerna och statsförvaltningen)

3.4 Kritiska objekt

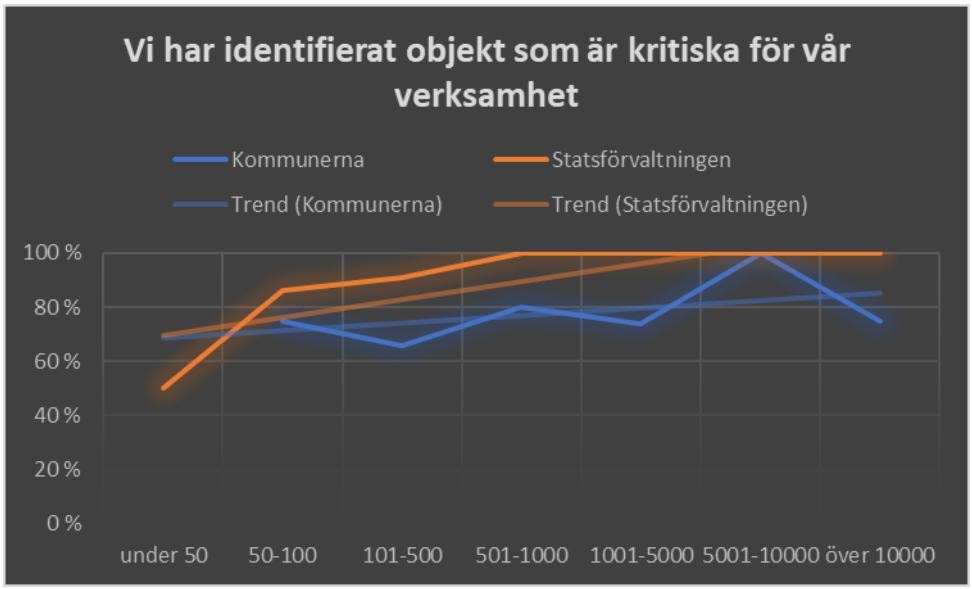
Enligt svaren har de objekt som är kritiska för verksamheten identifierats väl (Figur 29). De mest kritiska objekten, som i detta sammanhang avser kritiska informationssystem, digitala tjänster och processer, datalager, uppgifter och informationsflöden samt infrastruktur, har identifierats inom statsförvaltningen och sjukvårdsdistrikten. Enkätmaterialet visade att de organisationer som hade identifierat sina kritiska objekt överlag litade mer på sin observations- och reaktionsförmåga än andra.

Figur 29. Vi har identifierat objekt som är kritiska för vår verksamhet



I kommunernas och statsförvaltningens svar kan man se att organisationer med fler än 500 personer inom statsförvaltningen alla har identifierat sina kritiska objekt (Figur 30).

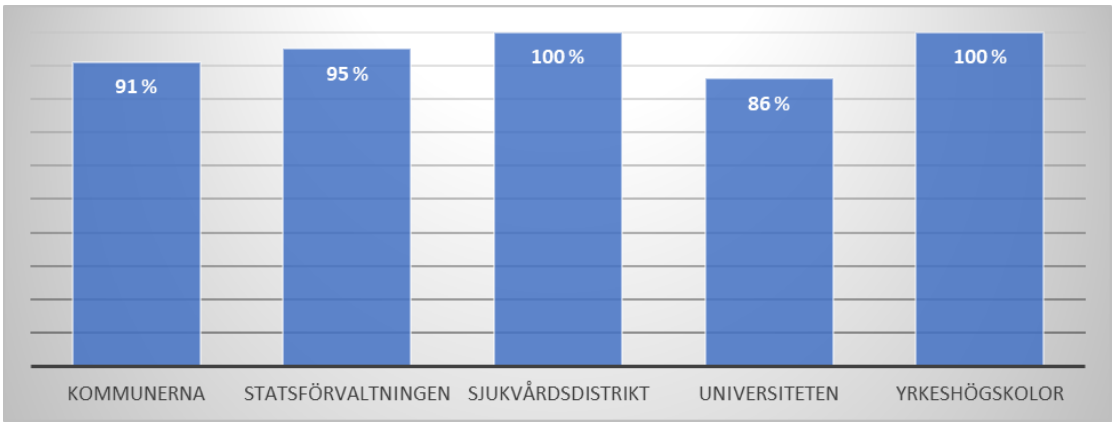
Figur 30. Identifiering av kritiska objekt (kommunerna och statsförvaltningen)



3.4.1 Kritiska informationssystem

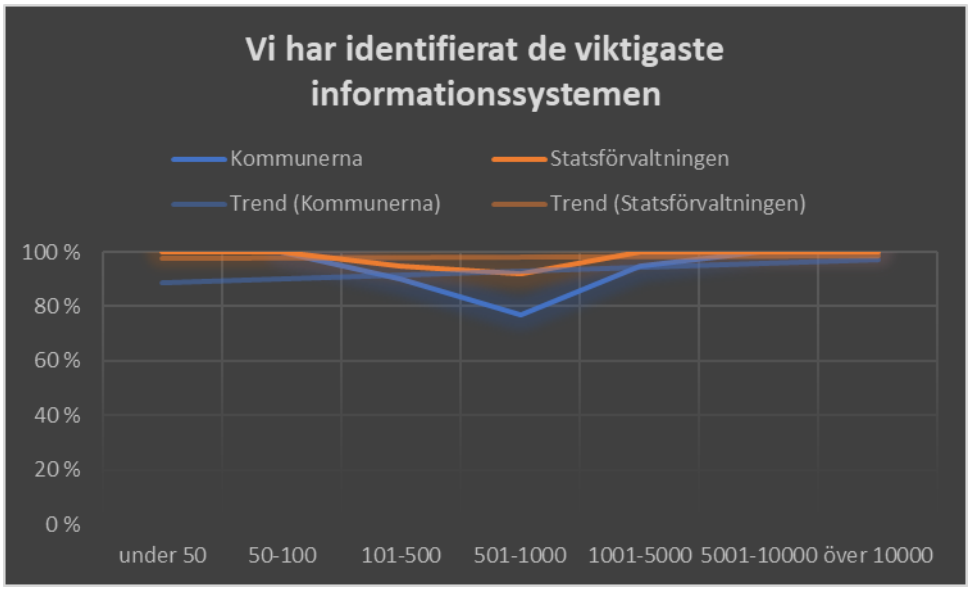
De informationssystem som är kritiska med tanke på verksamheten har identifierats till nästan hundra procent bland de respondenter som svarade att de identifierat sina kritiska objekt (Figur 31). Detta torde bero på att informationssystemen främst är användare och dagliga användningsfall. Därför är det lätt att identifiera informationssystem som är viktiga för verksamheten – om systemet inte fungerar förhindras verksamheten. Eftersom de informationssystem som är kritiska med tanke på den egna verksamheten är väl identifierade, rekommenderas organisationerna att också fundera över hur kritiska de är med tanke på om kritiska (eller andra) informationssystem har betydelse på nationell nivå.

Figur 31. Vi har identifierat kritiska informationssystem



Det finns egentligen ingen annan skillnad mellan kommunerna och statsförvaltningen än i storleksklassen 501–1000 där nedgången hos båda grupperna en aning större inom kommunsektorn (0).

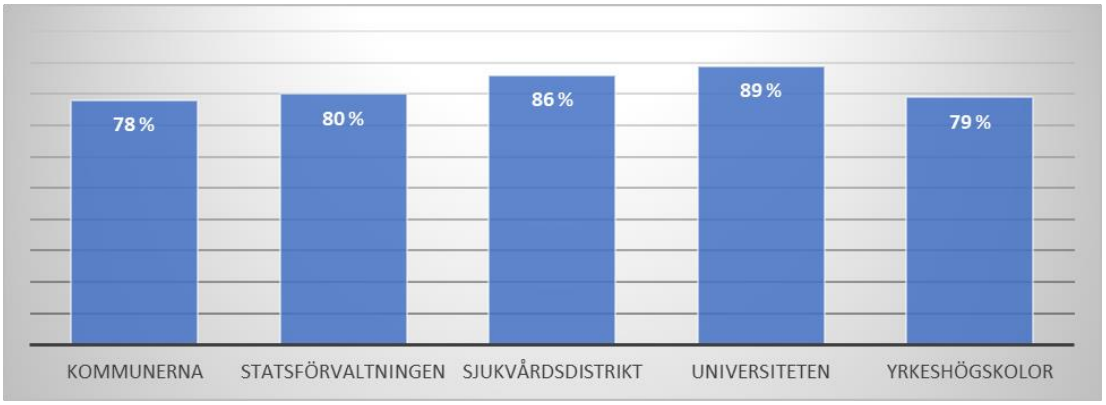
Figur 32. De viktigaste informationssystemen (kommunerna och statsförvaltningen)



3.4.2 Register över informationssystem

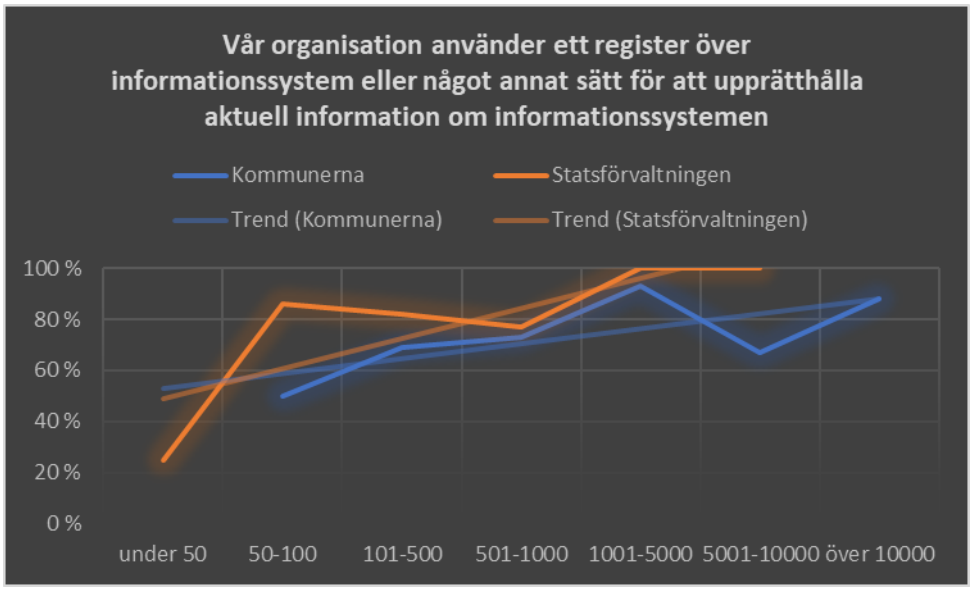
Eftersom kritiska informationssystem har identifierats väl är det ingen överraskning att även största delen av respondenterna har tillgång till ett register över informationssystemen eller något annat sätt att upprätthålla aktuell information om dem (Figur 33).

Figur 33. Vår organisation använder ett register över informationssystem eller något annat sätt för att upprätthålla aktuell information om informationssystemen



När man granskar skillnaderna mellan kommunerna och statsförvaltningen ökar trenden beroende på organisationsstorlek (Figur 34). Inom statsförvaltningen stiger trendkurvan kraftigt, vilket beror på att de minsta enheterna inom statsförvaltningen använder register över informationssystemen mer sällan än de större enheterna. Även de minsta kommunorganisationerna har brister i användningen av register över informationssystemen.

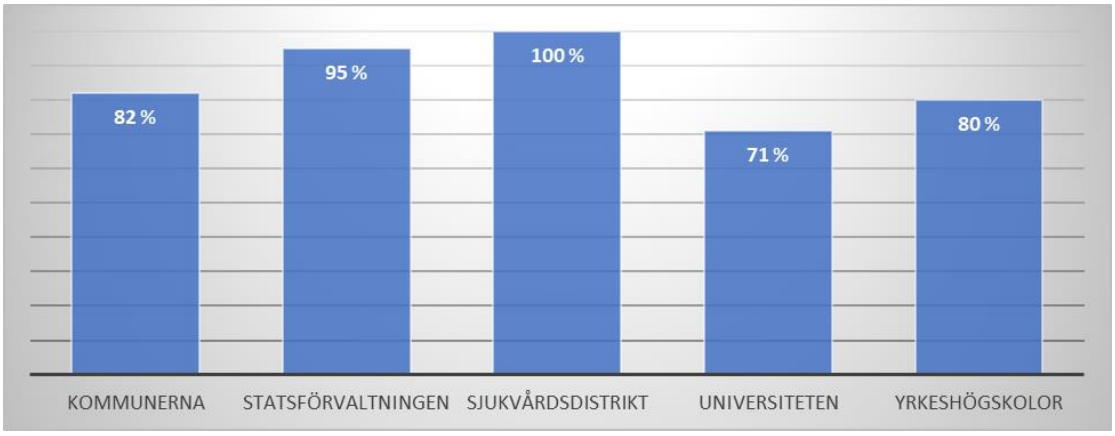
Figur 34. Register över informationssystem (kommunerna och statsförvaltningen)



3.4.3 Kritiska funktioner, tjänster och processer

De organisationer som svarat har också lyckats bra med att identifiera de funktioner, tjänster och processer som är kritiska för verksamheten (Figur 35). Orsaken torde vara densamma som för kritiska informationssystem, det vill säga att det är relativt enkelt att identifiera de funktioner, tjänster och processer som är kritiska för det dagliga arbetet och verksamheten. De kritiska funktionerna, tjänsterna och processerna har identifierats bäst i sjukvårdsdistrikten och statsförvaltningen, men de andra respondentgrupperna var inte mycket sämre.

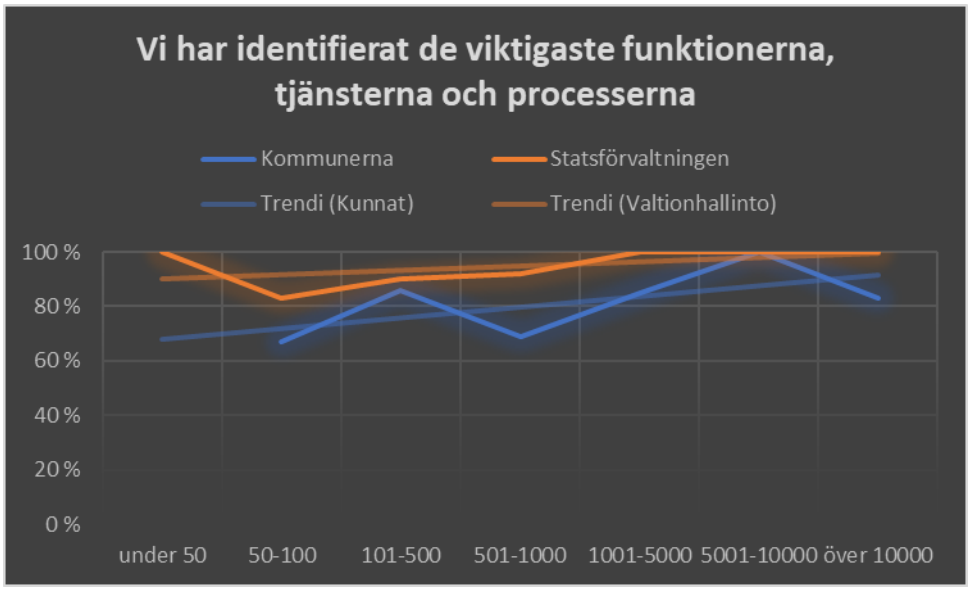
Figur 35. Vi har identifierat de viktigaste funktionerna, tjänsterna och processerna



När man jämför kommunerna och statsförvaltningen ser vi en mycket likartad stigande trend (Figur 36). I sin helhet ligger statsförvaltningens organisationer på en något bättre nivå än kommunerna. Av statsförvaltningens organisationer har

organisationer med fler än 1000 personer alla identifierat sina viktigaste funktioner, tjänster och processer.

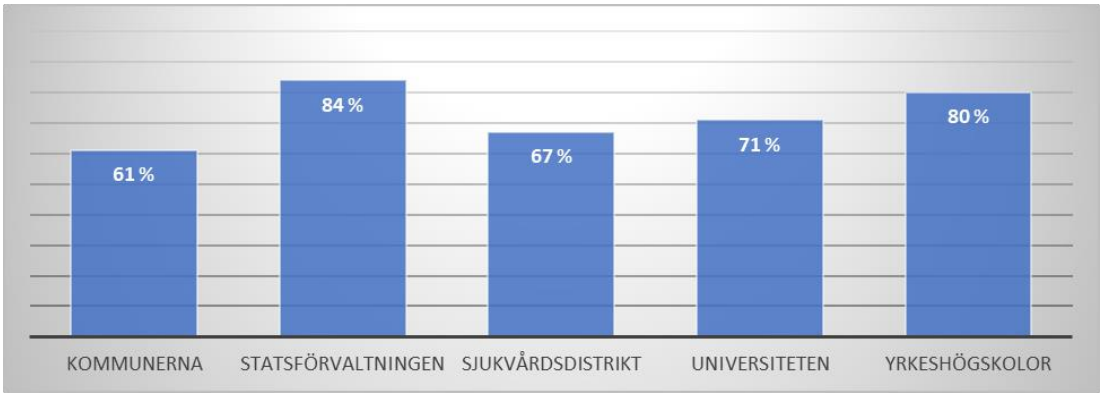
Figur 36. De viktigaste funktionerna, tjänsterna och processerna (kommunerna och statsförvaltningen)



3.4.4 Kritiska datalager

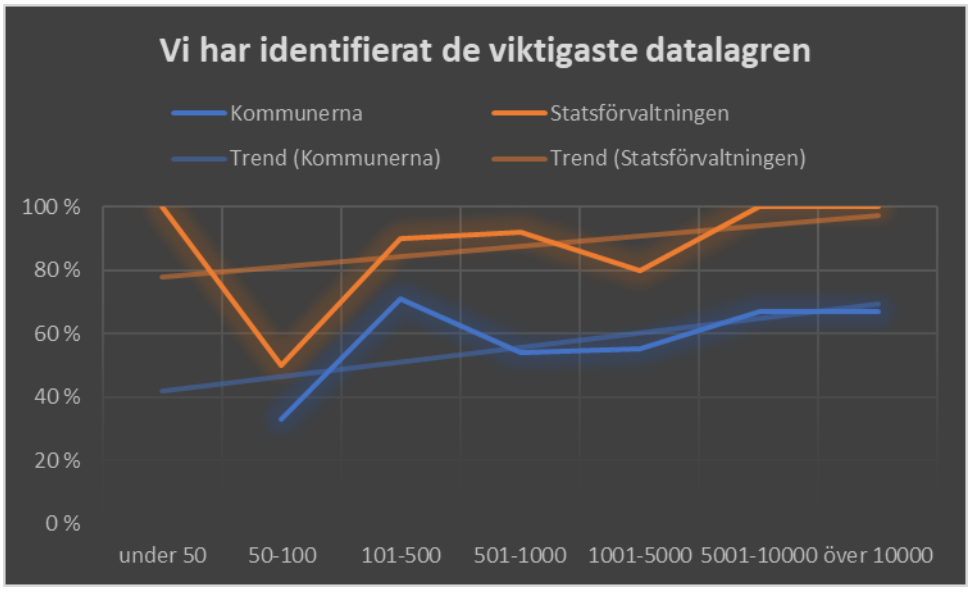
De datalager som är kritiska för verksamheten, det vill säga de vanligaste databaserna, hade också identifierats på en relativt god nivå, bäst inom statsförvaltningen och vid yrkeshögskolorna (0). Nivån är dock en aning lägre än för föregående objekt. Detta torde bero på att identifieringen av datalager som är kritiska för verksamheten är något mer krävande än identifieringen av informationssystem, funktioner, tjänster eller processer.

Figur 37. Vi har identifierat de viktigaste datalagren



I jämförelsen mellan kommunerna och statsförvaltningen är kurvorna återigen mycket likartade (Figur 38). När organisationsstorleken ökar är också datalagren i allmänhet bättre identifierade. Statsförvaltningen ligger före kommunsektorn i identifieringen av de viktigaste datalagren.

Figur 38. De viktigaste datalagren (kommunerna och statsförvaltningen)



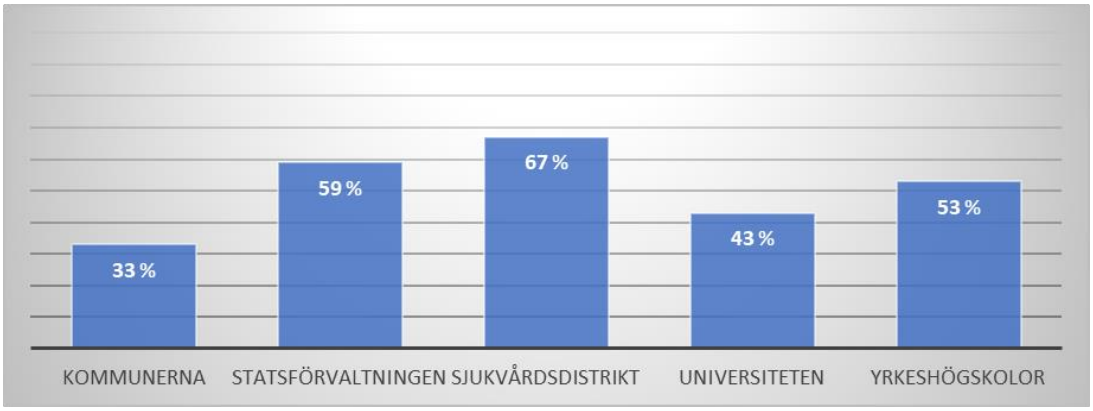
3.4.5 Kritiska uppgifter och informationsflöden

Identifieringen av uppgifter och informationsflöden (integrationer) som är kritiska för verksamheten är ett tydligt utvecklingsobjekt i alla organisationer (Figur 39). Identifieringen av uppgifter som är kritiska för verksamheten är bunden till identifieringen av kritiska datalager, men går ett steg djupare. Man kan till exempel närma sig identifieringen av uppgifter via kritiska processer och uppgifter som behandlas i dem.

Kritiska informationsflöden är överföring av uppgifter antingen inom organisationen till exempel från ett informationssystem till ett annat eller från en organisation utåt, till exempel till en partner. I fråga om informationshantering och personuppgifter är det

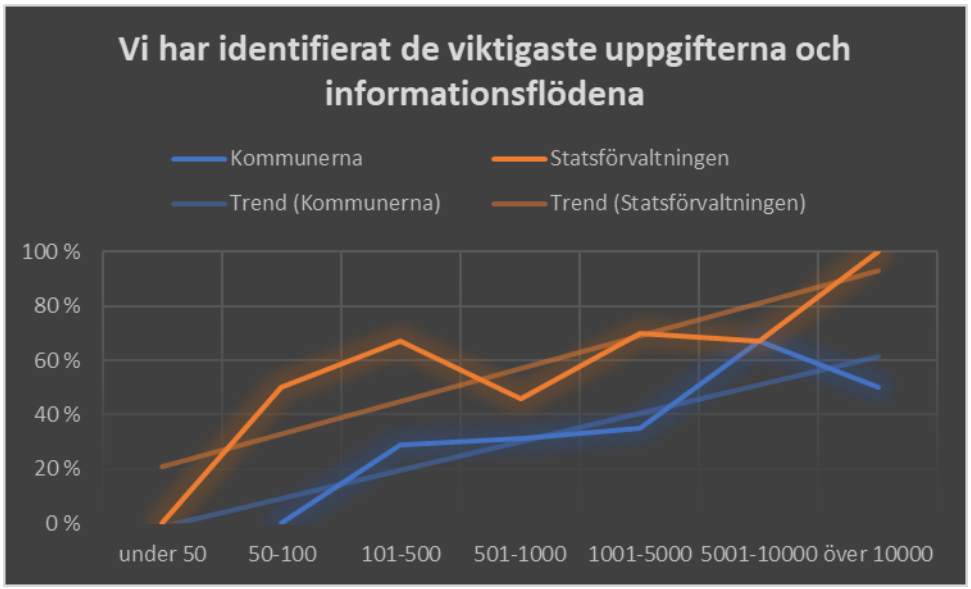
viktigt att också identifiera informationsflödena och de uppgifter som överförs i dem ur dataskyddssynvinkel.

Figur 39. Vi har identifierat de viktigaste uppgifterna och informationsflödena



När man jämför kommunerna och statsförvaltningen kan man i båda upptäcka en klart växande trend i takt med att organisationsstorleken ökar (0). De stora organisationerna har identifierat sina kritiska uppgifter och informationsflöden bättre än de små. Statsförvaltningen ligger återigen en aning före kommunsektorn. Det rekommenderas att uppgifter och informationsflöden identifieras via de kritiska informationssystemen samt de kritiska funktionerna och processerna, eftersom de har identifierats bättre.

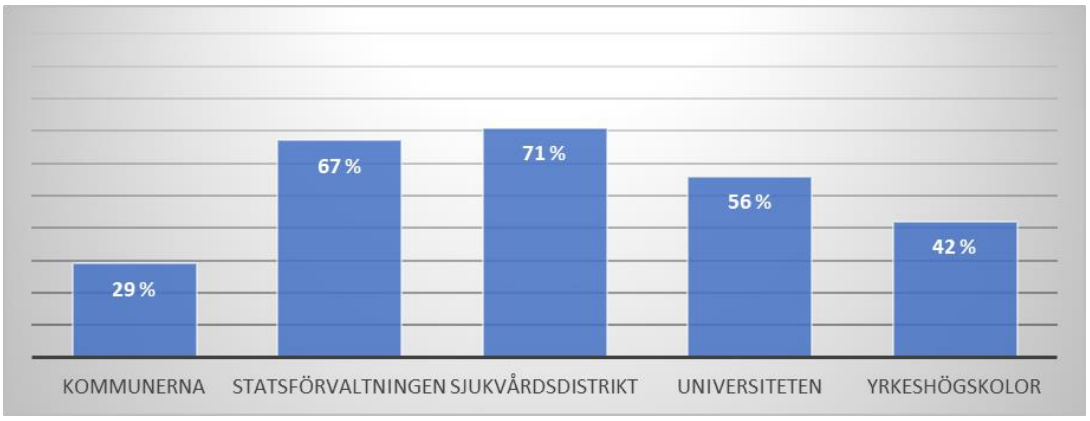
Figur 40. De viktigaste uppgifterna och informationsflödena (kommunerna och statsförvaltningen)



3.4.6 Klassificering av kritiska objekt

Klassificeringsförfarandet i organisationer som hade identifierat sina kritiska objekt användes bäst i sjukvårdsdistrikten och inom statsförvaltningen (Figur 41). På basis av svaren identifieras kritiska objekt i kommunerna, men de klassificeras fritt utan ett etablerat förfarande. Universiteten ligger på en något högre än yrkeshögskolorna i fråga om klassificeringsförfarandet.

Figur 41. Organisationen har ett sätt att klassificera kritiska objekt



När man granskar kommunerna och statsförvaltningen noggrannare avslöjas en bekant trend. Ju större organisation, desto mer sannolikt är det att det finns ett förfarande för klassificering av kritiska objekt (Figur 42). Inom statsförvaltningen kan bakgrunden vara Statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen, som styr statsförvaltningens organisationer till ett formellt förfarande även i klassificeringen av kritiska objekt. Inom kommunsektorn är kurvan

oroväckande låg ända till de största kommunorganisationerna, vilket visar att kommunsektorn inte har något etablerat klassificeringsförfarande för kritiskhet.

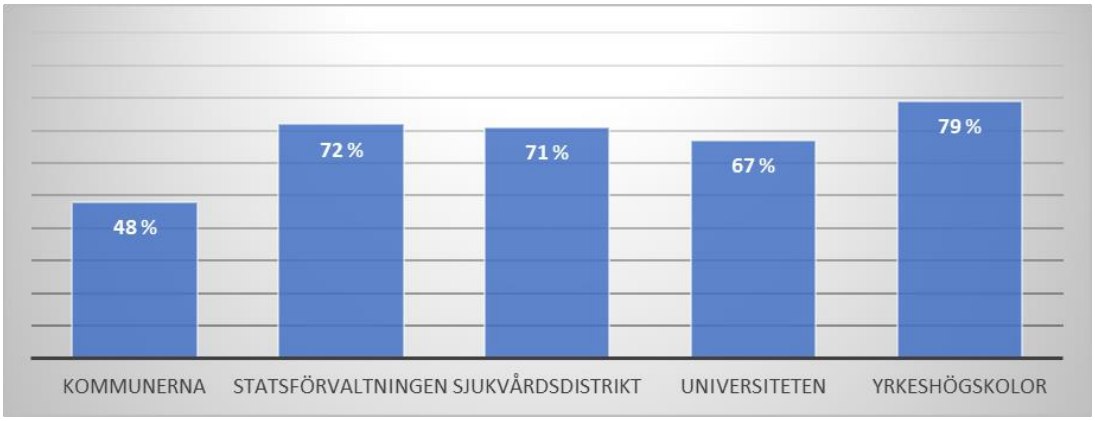
Figur 42. Klassificeringsförfarande för kritiska objekt (kommuner och statsförvaltningen)

3.5 Upphandling och utveckling av e-tjänster

3.5.1 Digital säkerhet vid upphandlingar

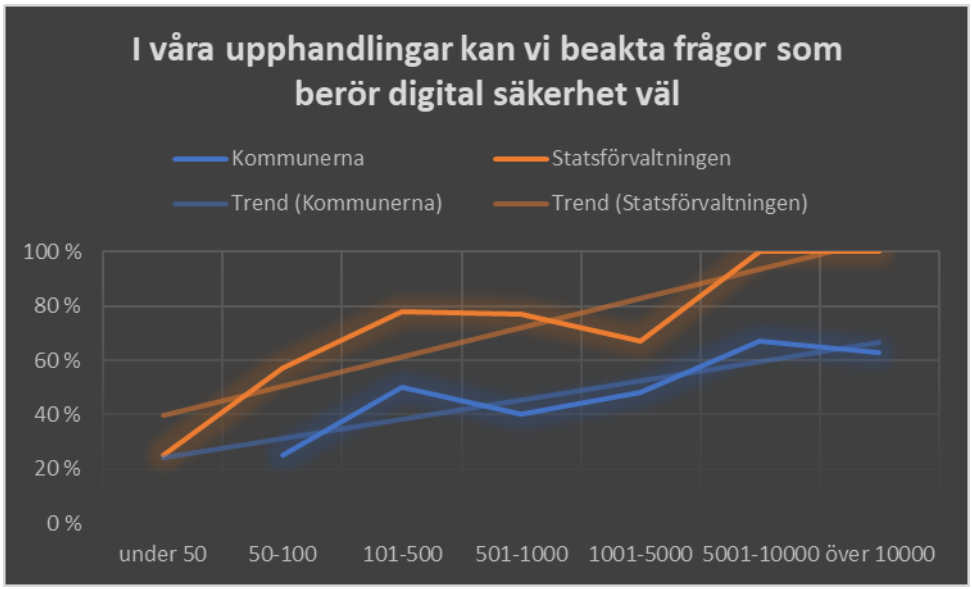
Utifrån svaren beaktas digital säkerhet väl vid upphandlingar (Figur 43). Ett undantag är kommunsektorn, där endast cirka hälften av respondenterna svarade ja. På basis av svaren har yrkeshögskolorna bäst beaktat digital säkerhet vid upphandlingar, men statsförvaltningen och sjukvårdsdistrikten är på nästan lika god nivå.

Figur 43. I våra upphandlingar kan vi beakta frågor som berör digital säkerhet väl



När vi granskar kommunerna och statsförvaltningen enligt organisationsstorlek ser vi samma trend som för utbildningen om digital säkerhet (0). Ju större organisation, desto bättre beaktas den digitala säkerheten i upphandlingarna. Likaså ligger statsförvaltningens kurva hela tiden på en högre nivå än kommunkurvan. Utveckling krävs i synnerhet när det gäller små kommuners och statsförvaltningsenheters förmåga att beakta digital säkerhet vid upphandlingar. Eftersom trendkurvorna för utbildning och upphandling är nästan identiska kan man fundera på om regelbunden utbildning i digital säkerhet också ger vägledning för att bättre beakta digital säkerhet vid upphandlingar.

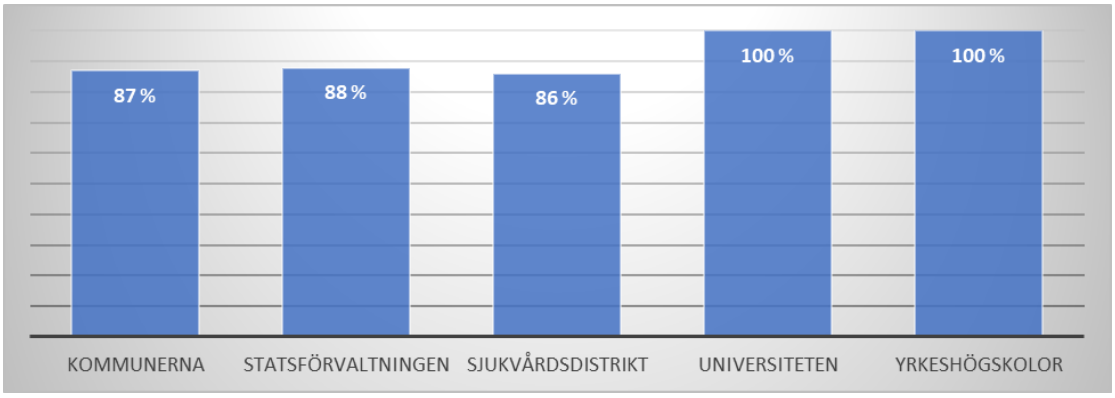
Figur 44. Digital säkerhet vid upphandlingar (kommunerna och statsförvaltningen)



3.5.2 Beaktande av datanätens säkerhet i tjänsteutvecklingen

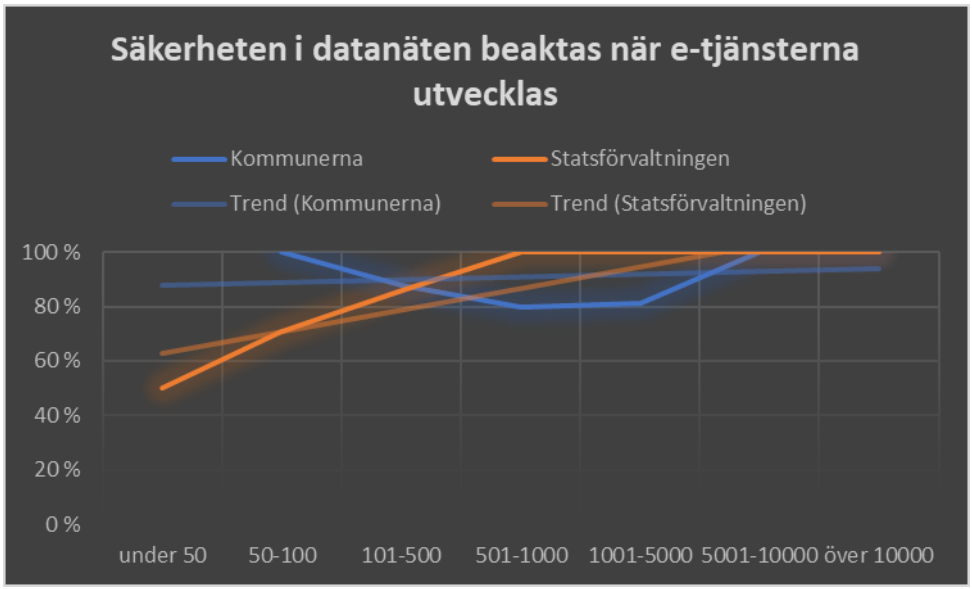
I utvecklingen av e-tjänster har organisationerna utifrån svaren fäst stor uppmärksamhet vid säkerheten i datanäten (Figur 45). Andelen jakande svar var över 85 procent för alla organisationstyper.

Figur 45. Säkerheten i datanäten beaktas när e-tjänsterna utvecklas



I en noggrannare jämförelse mellan kommunerna och statsförvaltningen förekommer knappt några skillnader (0). Endast de minsta organisationerna inom statsförvaltningen ligger enligt svaren på en något lägre nivå.

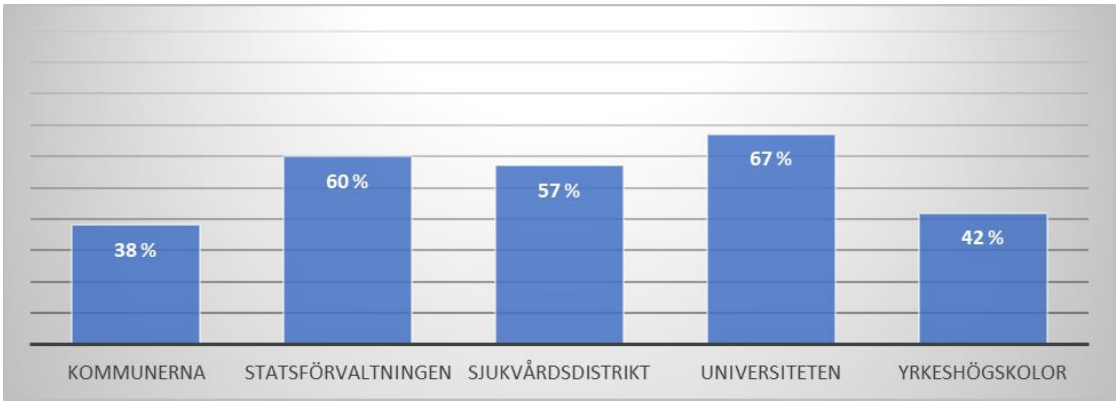
Figur 46. Datanätens säkerhet i utvecklingen av e-tjänster (kommunerna och statsförvaltningen)



3.5.3 Ansvar och skyldigheter för den digitala säkerheten

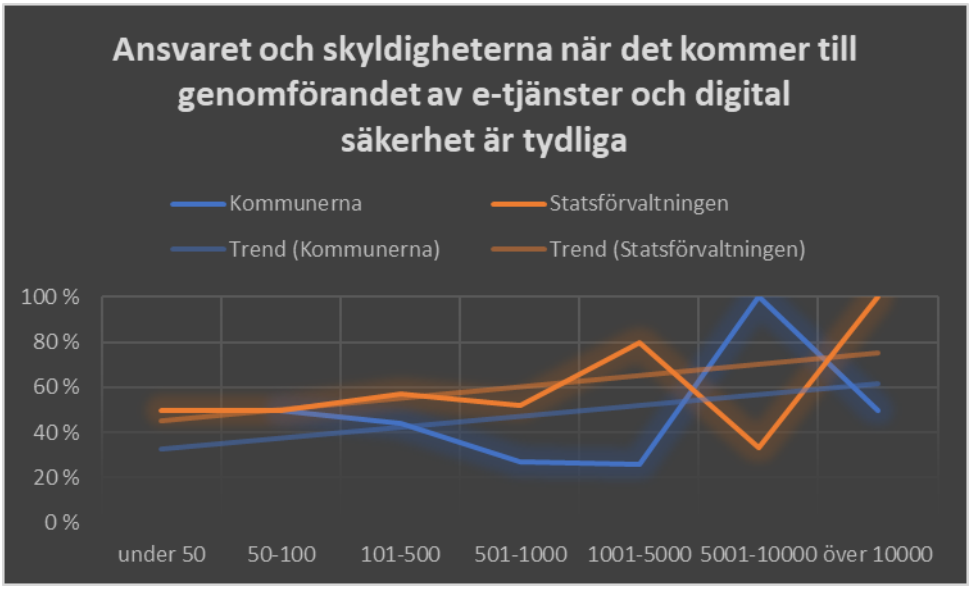
Ansvaret och skyldigheterna i fråga om den digitala säkerheten är inte lika tydliga vid tillhandahållandet av e-tjänster som vid beaktandet av datanätens säkerhet (Figur 47). Universiteten och statsförvaltningen har bäst koll på ansvaret och skyldigheterna, men alla organisationstyper behöver ännu utvecklas.

Figur 47. Ansvaret och skyldigheterna när det kommer till genomförandet av e-tjänster och digital säkerhet är tydliga



När man jämför kommunfältet och statsförvaltningen är trenden likartad när organisationsstorleken ökar och stiger något (0). Själva svaren visar att det är problematiskt inom kommunsektorn i storleksklassen 501–5000, där endast cirka en fjärdedel av respondenterna uppgav att ansvaret och skyldigheterna är tydliga. Inom statsförvaltningen syns motsvarande minskning i storleksklassen 5001–10000, där en tredjedel av respondenterna svarade att ansvaret och skyldigheterna var tydliga.

Figur 48. Ansvar och skyldigheter för den digitala säkerheten i utvecklingen av e-tjänsterna (kommunerna och statsförvaltningen)



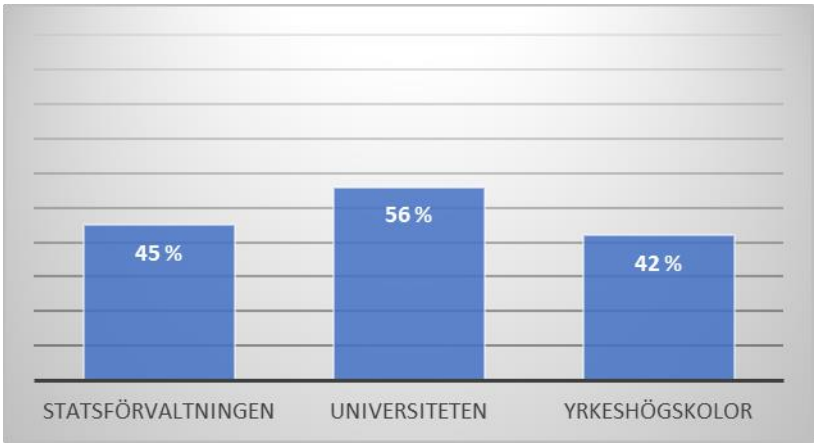
3.6 Bedömning av informationssäkerheten

Utöver de föregående frågorna frågade man statsförvaltningens enheter, universiteten och yrkeshögskolorna hur de bedömer informationssäkerheten i fråga om de digitala tjänster som används och skaffas. Dessa frågor ingick inte i kommunenkäten.

3.6.1 Informationssäkerheten hos de digitala tjänster som används

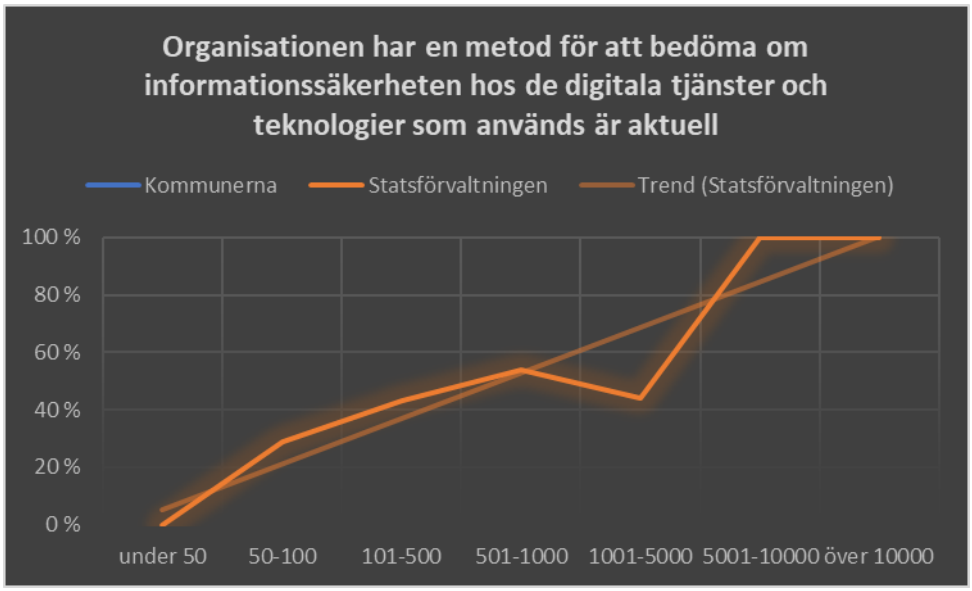
Ungefär hälften av respondenterna använde en metod för att bedöma om informationssäkerheten hos de digitala tjänster och teknologier som används är aktuell (Figur 49). Med tanke på hanteringen av informationssystemens och de digitala tjänsternas livscykel blir bedömningsmetoderna för digital säkerhet ett utvecklingsobjekt som kan förbättra organisationernas kapacitet.

Figur 49. Organisationen har en metod för att bedöma om informationssäkerheten hos de digitala tjänster och teknologier som används är aktuell



När man granskar statsförvaltningens enheter närmare märker man att utvärderingsförmågan ökar kraftigt i takt med att organisationsstorleken ökar (Figur 50). Detta tyder på att utvecklingsbehovet är störst i de minsta organisationerna.

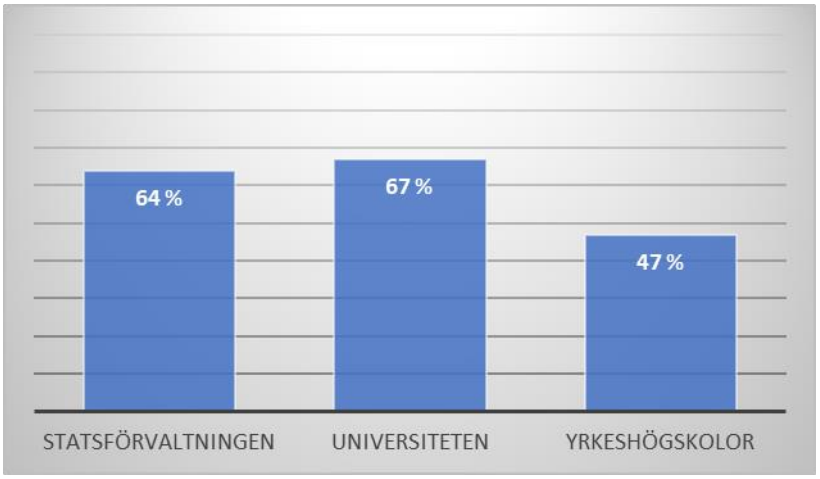
Figur 50. Förmåga att bedöma informationssäkerheten hos de digitala tjänster och teknologier som används (statsförvaltningen)



3.6.2 Bedömning av informationssäkerheten hos digitala tjänster som upphandlas

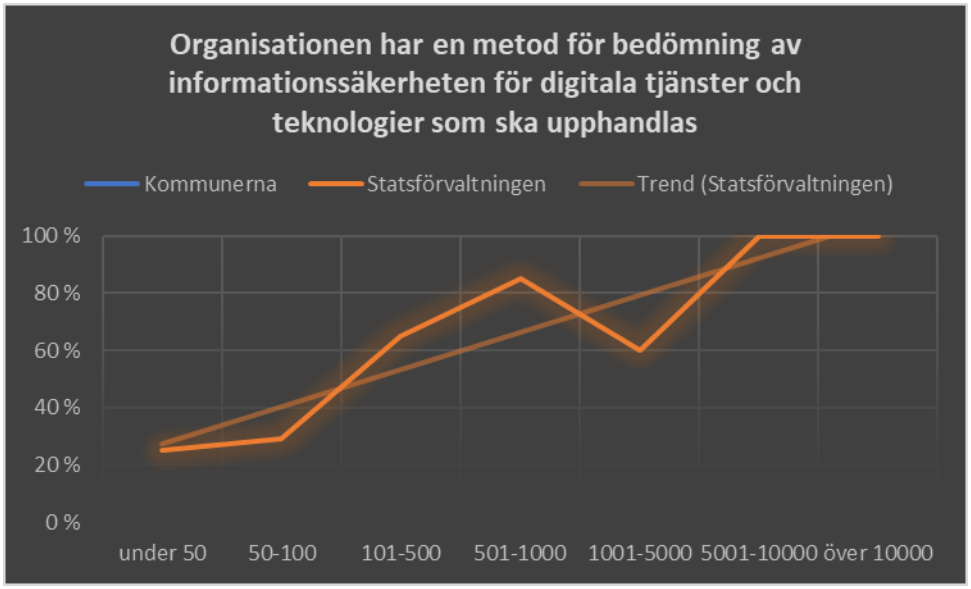
Vid bedömningen av informationssäkerheten för de digitala tjänster och teknologier som ska upphandlas ligger man på en aningen bättre nivå, i synnerhet vid universiteten och enheterna inom statsförvaltningen (0).

Figur 51. Organisationen har en metod för bedömning av informationssäkerheten hos de digitala tjänster och teknologier som ska upphandlas



Inom statsförvaltningen verkar trenden vara densamma som vid bedömningen av informationssäkerheten i fråga om de tjänster och de teknologier som används, det vill säga förmågan ökar i takt med att organisationsstorleken ökar (Figur 52). Således finns det mest att utveckla i små organisationer inom statsförvaltningen med färre än 100 anställda.

Figur 52. Förmåga att bedöma informationssäkerheten hos digitala tjänster och teknologier som ska upphandlas (statsförvaltningen)



4 Identifierade behov

Resultaten från enkäten visar att helheten av digital säkerhet inom den offentliga förvaltningen kan utvecklas genom att man i organisationerna fäster särskild uppmärksamhet vid en konsekvent och metodisk klassificering av kritiska objekt, användning av etablerade metoder för bedömning av digital säkerhet samt regelbunden utbildning av personalen och regelbunden övning på undantagssituationer.

Detta avsnitt innehåller en sammanfattning av de öppna svaren i anslutning till behoven av digital säkerhet. Behoven kunde delas in i fyra kategorier: övning och utbildning, resurser, tjänster för digital säkerhet och andra åtgärder som förbättrar den digitala säkerheten.

4.1 Övning och utbildning

I svaren önskades mer riksomfattande stöd och tjänster för utveckling av informationssäkerheten och dataskyddet, såsom:

- Nationella riktlinjer och konkreta anvisningar, modeller och checklistor för att förbättra informationssäkerheten
- Utbildning om informationssäkerhet och dataskydd för den offentliga sektorn
- Webbinarier och avgiftsfria utbildningar om informationssäkerhet
- Tekniska rekommendationer för datanät, arkitektur och system
- Utbildning om och hjälp vid störningar
- Regelbundna nationella övningar

- Anvisningar för ibruktagande av molntjänster
- Övning i samarbetsnätverken

Allmänt taget är alla former av riksomfattande stöd och verksamhetsmodeller välkomna. Man tyckte att den digitala säkerhetsveckan Digiturvaviikko och TAISTO-övningarna var bra och önskade flera sådana.

Man önskade också kontinuerlig utbildning och information för användarna om betydelsen av vad man själv gör. Detta behov är ett bra exempel på att organisationen i första hand själv ansvarar för ordnandet av informationssäkerhetsåtgärder. Det finns utbildning att tillgå, men organisationen måste själv förbinda sig till att ständigt och regelbundet öka personalens medvetenhet om informationssäkerhet som en del av sin verksamhet.

4.2 Resurser för digital säkerhet

Som det framgick av enkäten hade alla organisationer som svarade knappa resurser för digital säkerhet. Detta återspeglades också i de fritt formulerade svaren:

- Det är lätt att få utbildning, men för att föra saker framåt behövs mer resurser och pengar så att man kan förankra det man lärt sig under utbildningarna.
- Informationssäkerhet och dataskydd kräver ny kompetens och yrkesskicklighet och kan inte utföras vid sidan av den egna befattningen, så detta ska synas i både informationssäkerhets- och dataskyddsresurserna samt i positionen och lönen för dem som utför dessa arbeten.
- Små kommuners resurser och kompetens är otillräckliga för att upprätthålla och utveckla den digitala säkerheten. För detta efterlyses nationella stödåtgärder.
- Tillräckliga resurser för att trygga den digitala säkerheten. Behovet kommer att framhävas i framtiden när elektroniska tjänster tas i bruk i allt större omfattning.
- Höj personalens kompetens och engagera ledningen i informationssäkerheten.
- Man önskade att den offentliga sektorn delar med sig av god praxis och sin kompetens, eftersom ämbetsverkens resurser är små.
- Antalet personer som ansvarar för den digitala säkerheten är mycket litet inom organisationen och det verkar som om man inte orkar lyssna på samma typer hela tiden. Därför skulle det vara välkommet med en påverkare som skulle komma utifrån.
- Vid en liten IKT-enhet finns ingen person som är särskilt insatt i informationssäkerhet. Således sköts ärenden som gäller digital säkerhet vid sidan av andra arbeten i den mån man hinner. Detta är inte en idealisk lösning och bidrar inte till att öka kompetensen.
- Det måste finnas en expert i den egna organisationen som behärskar helheten. Nu verkar alla inom sina egna verksamhetsområden utan att beakta helheten, till

exempel gör man upphandlingar endast för sin egen del och ser inte om helheten fungerar.

4.3 Tjänster som stöder digital säkerhet

Tjänster som stöder digital säkerhet är det tredje delområdet där behoven identifierades. Behoven i anslutning till tjänsterna varierade från sparring till omfattande och gemensamma tekniska tjänster för digital säkerhet inom den offentliga förvaltningen. Man önskade också att kostnaderna för de gemensamma och centraliserade tjänsterna skulle vara så låga som möjligt. De identifierade servicebehoven var följande:

- Gemensamt centraliserat säkerhetsoperationscenter för den offentliga förvaltningen
- Så smidigt och kostnadseffektivt införande som möjligt av lösningar som Havaro i organisationerna
- Tjänst för kartläggning av informationssäkerhetssvagheter
- Centraliserat uppföljningssystem för informationssäkerhetshändelser
- Alla tjänster som produceras centraliserat för förvaltningen bör utvärderas eller auditeras för att de organisationer som är skyldiga att använda dem ska ha en klar uppfattning om tjänsternas status.
- Sparringshjälp i problemsituationer och andra situationer.
- Kommunerna behöver en centraliserad organisation som tekniskt och operativt hjälper IT-avdelningarna och informationsförvaltningen.
- Analys och lägesbild av nivån på kommunernas informationssäkerhet för att rätt nationella tjänster och åtgärder ska kunna riktas till kommunen.
- Cybersäkerhetscentrets resultat, till exempel informationssäkerhets- och dataskyddskrav för upphandlingar inom social- och hälsovården, som är tillräckligt konkreta frågor som kan omsättas i praktiken och som kan förbättra informationssäkerhetsnivån.
- Små ämbetsverk är tvungna att starkt förlita sig på de tjänster som Valtori erbjuder, så vi önskar att Valtori har lösningar som tydligt auditerats för en viss nivå av informationssäkerhet samt alternativa lösningar för olika krypteringsbehov. Dessutom önskar man att Valtori utvecklar rapporteringen till kunden om informationssäkerhetsfall som observerats med hjälp av teknisk övervakning.
- Statsrådets informationssäkerhetsenhets expertis och handledning upplevs som nödvändig, eftersom den egna kompetensen inte upplevs som tillräcklig. Dessutom har Myndigheten för digitalisering och befolkningsdatas tjänster för digital säkerhet, läromaterial och Vahti-arbete upplevts som mycket nyttiga.
- Centraliserad SIEM-lösning eller någon annan lösning som är kostnadseffektiv för organisationen, skanningstjänst för sårbarheter, IDS-tjänst eller något annat kostnadseffektivt sätt att övervaka nättrafiken.

- Gemensamma miljöer för teknisk monitorering och testning kunde utvecklas.
- Myndigheterna borde erbjuda miljöerna på högre nivå.

4.4 Övriga åtgärder som förbättrar den digitala säkerheten

Utöver ovan nämnda delområden identifierades i svaren även andra åtgärder som förbättrar den digitala säkerheten, såsom:

- Införande av riskanalys.
- Bedömningen av molntjänster måste förenklas.
- Starkare roll för Valtori i den tekniska informationssäkerheten.
- Utveckling av det digitala säkerhetsnätverkets verksamhet och utökat djupare samarbete mellan centrala aktörer, VIRT för allmän.
- Utveckling av samarbete på nationell nivå, kommunikation i hotfulla situationer och nätverk för informationsutbyte.
- Gemensamma procedurer för den offentliga förvaltningen.
- En attitydförändring behövs.
- Ökad användning av tvåfaktorsautentisering.
- Utökad hantering av mobila enheter.
- Det ska vara tydligt inom hela organisationen vem som äger processen och tjänsterna och har tillhörande informationssäkerhetsansvar.
- Effektivare spridning av lägesinformation mellan offentliga organisationer.
- Lagstiftningen om och auditeringskraven för digital säkerhet inom social- och hälsovårdssektorn borde förnyas och det borde ställas tydliga krav på service-producenterna när det gäller vilka krav på digital säkerhet de ska uppfylla för att kunna producera tjänster för social- och hälsovårdsaktörer.
- Tydligare ansvar och skyldigheter för olika aktörer.

Hanteringen av nationellt säkerhetsklassificerad information ska uppfylla samma krav som behandlingen av EU-säkerhetsklassificerad information så att det krävs myndigheternas godkännande för de tjänster som används.

25.3.2021