Myndigheten
för civilt försvar

Redovisning

Cybersäkerhetskollen 2025

Redovisning av uppföljning av nivån på det systematiska cybersäkerhetsarbetet i offentlig förvaltning och samhällsviktig verksamhet

Cybersäkerhetskollen 2025 – Redovisning av uppföljning av nivån på det systematiska cybersäkerhetsarbetet i offentlig förvaltning och samhällsviktig verksamhet

Myndigheten för civilt försvar
651 81 Karlstad

Foto: Myndigheten för civilt försvar, Mikael Svensson (omslag), Melker Dahlstrand (sida 10, 22, 122), Johan Eklund (sida 36) och Thomas Henrikson (sida 42).
Tryck: Ljungbergs tryckeri AB
Produktion: Advant

Publikationsnummer: MCF0101 – februari 2026
ISBN-nummer: 978-91-7927-726-0

Förord

Myndigheten för civilt försvar leder och skapar handlingskraft i den samlade civila hanteringen av krig och kriser nationellt för det civila och militära försvaret. Vi utvecklar och stärker förmågan i hela samhället så att vi tillsammans kan agera om det värsta skulle hända.

Sverige har en hög grad av digitalisering där många sektorer och verksamheter, liksom enskilda människor, nyttjar alla dess fördelar. Stora demokratiska, samhälleliga och ekonomiska värden realiseras genom informationstillgångar och nätverk. Samtidigt befinner vi oss i ett allvarligt säkerhetspolitiskt läge där hybrida angrepp riktas mot mål i Sverige och övriga länder i Europa.

Under 2025 inträffade bland annat de omfattande cyberincidenterna hos Miljödata och SportAdmin. I angreppet mot Miljödata stals personuppgifter från 164 kommuner och fyra regioner. Även privata verksamheter samt universitet och högskolor drabbades.

Resultatet i Cybersäkerhetskollen 2025 visar återigen på allvarliga brister i nivån på det systematiska cybersäkerhetsarbetet hos offentlig förvaltning. I förhållande till 2024 års mätning har inga märkbara resultatförbättringar skett. Tyvärr är det också fortfarande alldeles för få NIS-leverantörer som deltar. Myndigheten för civilt försvar kan därför inte ta fram en samlad bedömning över det systematiska cybersäkerhetsarbetet hos samhällsviktiga verksamheter.

Den 15 januari 2026 trädde cybersäkerhetslagen i kraft. Lagen ställer skärpta krav på riskhantering, vidtagande av säkerhetsåtgärder och incidentrapportering. Givet resultatet i Cybersäkerhetskollen och det allvarliga säkerhetspolitiska läget välkomnar jag skärpta krav på samhällsviktiga verksamhetsutövare. Det är nu hög tid att stärka det systematiska cybersäkerhetsarbetet i Sverige.

Jag ser fram emot att tillsammans med Nationellt cybersäkerhetcenter (NCSC) fortsätta verka för att stärka förmågan i det civila försvaret på cyberområdet, även efter det att myndighetens cyberverksamhet har gått över till NCSC den 1 juli 2026.

Stockholm, 2026-03-02

Åke Holmgren
Avdelningschef, Myndigheten för civilt försvar

Innehåll

Sammanfattning

Myndigheten för civilt försvar[1] följer upp och redovisar nivån på det systematiska cybersäkerhetsarbetet hos samhällsviktiga verksamheter på uppdrag av regeringen. Uppföljningen sker genom Cybersäkerhetskollen. Mätningen 2025 genomfördes mellan den 23 april och den 12 september 2025.

2025 års Cybersäkerhetskollen omfattar för första gången fyra mätningar: Infosäkkollen, It-säkkollen, Ot-säkkollen och Leveranskedjekollen. Den fördjupade Cybersäkerhetskollen innebär ett uppföljningsverktyg och ett stöd som överensstämmer i högre utsträckning med definitionen av cybersäkerhet[2] i EU:s cybersäkerhetsförordning[3] och i cybersäkerhetslagen.[4]

Resultatet i mätningen av Cybersäkerhetskollen 2025 visar på allvarliga brister. Motståndskraften i Sverige behöver förbättras. Även om det finns exempel på organisationer som har ett resultat som motsvarar att de bedriver ett systematiskt cybersäkerhetsarbete i en enskild mätning, har de flesta ett svagare resultat i en annan, varför ytterst få samhällsviktiga verksamheter i Sverige kan sägas arbeta systematiskt med helheten av sitt cybersäkerhetsarbete. Allra störst brister ses i det systematiska ot-säkerhetsarbetet, tillika den cyberdomän som nyttjas för våra mest grundläggande samhällsfunktioner såsom exempelvis vattenrening och elförsörjning. Det säkerhetspolitiska läget kräver en högre nivå och snabbare förbättringstakt än vad resultaten påvisar.

Omkring 300 organisationer deltog i Infosäkkollen respektive It-säkkollen, vilket innebär det största deltagandet hittills. Ot-säkkollen hade ett deltagande om drygt 60 organisationer och Leveranskedjekollen om drygt 220 organisationer. 47 organisationer genomförde samtliga fyra mätningar, och nästan 200 genomförde alla mätningar förutom Ot-säkkollen.

Av de 47 organisationer som deltog i samtliga mätningar framkommer att endast tre organisationer har nått nivå 1 i Cybersäkerhetskollen 2025. Ingen organisation har nått nivå 2 eller högre. Det är resultatet i Ot-säkkollen som primärt drar ned organisationernas övergripande nivå i den samlade Cybersäkerhetskollen.

Not 1. Tidigare Myndigheten för samhällsskydd och beredskap (MSB).

Not 2. Artikel 2(1) i Cybersäkerhetsförordningen (EU) 2019/881 definierar cybersäkerhet som ”all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot”.

Not 3. Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten, https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32019R0881 (hämtad 01/2026).

Not 4. 1 kap. 2 § 5 p. i cybersäkerhetslagen (2025:1506).

När Ot-säkkollen exkluderas, och de 188 organisationer som svarade på Infosäkkollen, It-säkkollen och Leveranskedjekollen beaktas, framgår att två organisationer har nått nivå 3 eller högre i de tre mätningarna, vilket indikerar att de arbetar systematiskt i bredden av sitt cybersäkerhetsarbete. Samtidigt är det 147 organisationer (78 procent) som inte når upp till den första nivån och därmed saknar grunderna i sitt systematiska säkerhetsarbete inom en eller flera mätningar.

Det faktum att tre av fyra mätningar i Cybersäkerhetskollen är helt eller delvis nya bör beaktas gällande resultatet i den samlade Cybersäkerhetskollen. Samtidigt är det tydligt att fler organisationer behöver säkerställa att de bedriver ett systematiskt cybersäkerhetsarbete inom alla de cyberdomäner (informationssäkerhet, it-säkerhet, ot-säkerhet och säkerhet i digitala leveranskedjor) som de bedriver verksamhet inom. Det är först när arbetet bedrivs systematiskt inom samtliga cyberdomäner som arbetet är systematiskt i sin helhet.

I Infosäkkollen når nästan sex av tio organisationer inte nivå 1 som övergripande nivå, vilket indikerar att de saknar grunderna i sitt systematiska informationssäkerhetsarbete. Endast sex procent når upp till nivå 3 eller högre. Nivå 3 indikerar efterlevnad av föreskriftskrav om informationssäkerhet för myndigheter, vilka har funnits i olika former sedan 2009. Enbart nio procent av myndigheterna har uppnått nivå 3 eller högre.

Myndigheten kan vidare konstatera att ingen verklig förbättring i uppnådd övergripande nivå har skett mellan Infosäkkollen 2024 och 2025. I förhållande till de förbättringar som noterats mellan tidigare mättillfällen kan det konstateras att utvecklingstakten mellan mätningen 2024 och 2025 är noterbart lägre. Resultatet indikerar därmed en stagnerande utvecklingstakt. Kommunerna är den aktörsgrupp som, i fråga om antalet vidtagna åtgärder, har förbättrat sig mest i förhållande till både Infosäkkollen 2021 och Infosäkkollen 2024. Trots det presterar kommunerna fortfarande noterbart sämre än myndigheter och regioner inom Infosäkkollen 2025.

Gällande It-säkkollen saknar drygt hälften av organisationerna grunderna i sitt systematiska it-säkerhetsarbete. Vidare är det endast fem procent som når upp till övergripande nivå 3 eller högre, där nivå 3 indikerar att organisationer lever upp till myndighetens föreskriftskrav om it-säkerhet för myndigheter. Inom It-säkkollen når sex procent av myndigheterna nivå 1 eller högre.

När det kommer till Ot-säkkollen saknar så många som nio av tio grunderna i sitt systematiska ot-säkerhetsarbete. Ingen organisation har uppnått nivå 3 eller högre i modellen. Det framgår vidare att den stora majoriteten av deltagarna enbart har vidtagit ett fåtal av de åtgärder som undersöks. Resultatet i Ot-säkkollen är noterbart svagare än i övriga tre mätningar i Cybersäkerhetskollen. Samtidigt var deltagandet så lågt att myndigheten inte kan dra alltför långtgående slutsatser.

Vad gäller Leveranskedjekollen saknar sju av tio grunderna i sitt säkerhetsarbete i digitala leveranskedjor. Endast sex procent av organisationerna har klarat nivå 3 eller bättre. Nivå 3 indikerar att man har ett kvalificerat innehåll i sitt säkerhetsarbete.

I Infosäkkollen, It-säkkollen och Leveranskedjekollen är myndigheterna den aktörsgrupp som, med ett fåtal undantag, presterar starkast. Sammantaget tyder resultaten på att myndigheterna är den starkaste aktörsgruppen inom offentlig förvaltning i fråga om systematiskt cybersäkerhetsarbete. Medan kommuner genomgående är den svagast presterande aktörsgruppen i Infosäkkollen, presterar de noterbart bättre i både It-säkkollen och Leveranskedjekollen i förhållande till övriga aktörsgrupper. I både It-säkkollen och Leveranskedjekollen är det en högre andel kommuner än regioner som når övergripande nivå 1 eller högre, även om skillnaden mellan kommuner och regioner är mindre betydande.

Vissa brister, som drar ned deltagande organisationers resultat, återkommer i flera mätningar. Det gäller framförallt åtgärder avseende uppföljning och utvärdering, där resultatet är genomgående lågt. Den övergripande bild som framkommer är att uppföljning och utvärdering prioriteras ned konsekvent inom cybersäkerhetsarbetet. Ledningens engagemang samt incident- och kontinuitetshantering är andra områden där det finns gemensamma brister mellan mätningarna.

Av enkätutvärderingen av Cybersäkerhetskollen 2025 framkom bland annat svar om organisationernas förutsättningar att bedriva ett systematiskt cybersäkerhetsarbete. 65 procent av organisationerna uppger att de inte har den personal som krävs för att förbättra cybersäkerhetsarbetet.[5] Det är ett allvarligt resultat. Ledningen ansvarar för att säkerställa att det finns tillräckliga resurser för att bedriva ett systematiskt cybersäkerhetsarbete.

Samtidigt som resultatet visar på allvarliga brister är det en stor andel organisationer som har goda möjligheter att förbättra sig till nästa mätning. Det går nämligen att konstatera att många organisationer har genomfört en förhållandevis stor andel åtgärder, men brister exempelvis i fråga om vilken utsträckning de nyttjar sitt beslutade arbetssätt eller saknar någon aspekt av mer kvalificerat innehåll. Med enbart några få riktade åtgärder kan många organisationer nå bättre resultat i Cybersäkerhetskollen.

Not 5. En positiv iakttagelse i enkätutvärderingen av Cybersäkerhetskollen 2025 är att 61 procent uppgett att deras högsta ledning har det engagemang som krävs för att förbättra cybersäkerhetsarbetet. Det motsvarar en förbättring om åtta procentenheter i förhållande till 2024 års utvärdering. Resultatet kan indikera en förbättring gällande ledningens engagemang i cybersäkerhetsarbetet som ännu inte genererat utslag i resultatet av Cybersäkerhetskollen.

Det allvarliga säkerhetsläget och ikraftträdandet av cybersäkerhetslagen med tillhörande föreskrifter kräver att verksamhetsutövare förbättrar sitt systematiska cybersäkerhetsarbete samt inriktar, prioriterar och följer upp fler säkerhetsåtgärder. Dels för sin egen verksamhets skull, dels för att stärka samhällets motståndskraft.

Regeringen har, genom de regeringsuppdrag som ligger till grund för Cybersäkerhetskollen, ålagt Myndigheten för civilt försvar att bedöma nivån på cybersäkerhetsarbetet för det civila försvaret. Liksom i mätningarna 2023 och 2024, är det även 2025 alltför få NIS-leverantörer som deltagit i Cybersäkerhetskollen för att deras resultat ska kunna inkluderas. Därför kan denna redovisning endast redogöra för nivån på cybersäkerhetsarbetet i offentlig förvaltning. Ett stärkt deltagande från privat sektor krävs för att det ska vara möjligt att ta fram en samlad bedömning av nivån på det systematiska cybersäkerhetsarbetet inom ramen för det civila försvaret framöver.

Kapitel 1

Om redovisningen

1. Om redovisningen

Myndigheten för civilt försvar[6] har utifrån tre uppdrag från regeringen samt utifrån särskild styrning i höstbudgetpropositionen 2024 tagit fram en struktur för uppföljning av nivån på det systematiska cybersäkerhetsarbetet hos enskilda organisationer. Cybersäkerhetskollen är samlingsnamnet för myndighetens fyra cybersäkerhetsmätningar:

- Infosäkkollen,
- It-säkkollen,
- Ot-säkkollen och
- Leveranskedjekollen.

Ot-säkkollen och Leveranskedjekollen är helt nya mätningar, medan It-säkkollen har gjorts om för att efterlikna strukturen i Infosäkkollen. De tre nya mätningarna har således genomförts för första gången 2025 och har därför utvärderats. Nedan redogörs summariskt för de uppdrag som myndigheten har fått av regeringen med avseende på Cybersäkerhetskollen med start 2019.

1.1 Uppdrag från regeringen

I september 2019 beslutade regeringen att ge dåvarande Myndigheten för samhällsskydd och beredskap (MSB) i uppdrag att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen.[7] I uppdraget ingick även att myndigheten regelbundet ska lämna en samlad bedömning av nivån på det systematiska informationssäkerhetsarbetet utifrån framtagen uppföljningsstruktur.

I mars 2023 beslutade regeringen att ge MSB i uppdrag att utvidga sin struktur för uppföljning av det systematiska informationssäkerhetsarbetet inom offentlig sektor, den så kallade ”Infosäkkollen”, för att från och med år 2023 även kunna användas av näringslivet och då främst de aktörer som omfattades av lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Dessutom ska myndigheten, från och med år 2025, erbjuda relevanta aktörer som deltar i Infosäkkollen en struktur för uppföljning av det systematiska

Not 6. Sedan 1 januari 2026 är Myndigheten för samhällsskydd och beredskap (MSB) numera Myndigheten för civilt försvar. Redovisningen kommer nämna ”Myndigheten för civilt försvar” eller ”myndigheten”, med undantag för redogörelse över uppdrag som myndigheten fått från regeringen före 2025 då myndigheten hette MSB.

Not 7. Ju2019/03058/SSK, Ju2019/02421/SSK.

it-säkerhetsarbetet. Regeringsuppdraget ska redovisas till Regeringskansliet (Försvarsdepartementet) senast den 1 mars vartannat år.[8]

I februari 2025 beslutade regeringen att ge MSB i uppdrag att ta fram en uppföljningsmodell av ett systematiskt säkerhetsarbete avseende digitala leveranskedjor som kompletterar den struktur för uppföljning av det systematiska informationssäkerhetsarbetet som regeringen uppdrog MSB år 2019.[9]

Ytterligare styrning från regeringen avseende Cybersäkerhetskollen framgår av regeringens nationella strategi för cybersäkerhet.[10]

1.2 Centrala ord och uttryck

Här följer en lista över centrala uttryck och deras definitioner i redovisningen.

Allriskperspektiv handlar om sträva efter att bedöma alla typer av risker för något som ska skyddas och att analysera alla möjliga orsaker till att en risk realiseras.

Aktörsgrupp används för att kunna dela in medverkande organisationer i olika grupper, såsom kommuner, regioner, myndigheter och bolag.

Arbetsområden är de centrala säkerhetsområden som respektive mätning följer upp nivån på det systematiska säkerhetsarbetet inom. Dessa är mellan fem till tio beroende på mätning.

Benchmarks är en form av resultat som används för att analysera, bedöma och jämföra resultat för en viss grupp. Benchmark utgår ifrån majoritetssvaret alternativt det största minoritetssvaret i den grupp som studeras. Om 51 procent av organisationerna i gruppen uppgett ”ja” i ett svar, återges det som ”ja” för alla organisationer i den benchmarken. Resultatet tar även hänsyn till andelen säkra eller osäkra bedömningar per nivå. Benchmark genererar resultat för grupperna typförvaltning, typmyndighet, typregion och typkommun (för mer information om dessa, se förklaring längre ner).

Cybersäkerhet avser all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot i enlighet med definitionen i EU:s cybersäkerhetsförordning[11]. Cybersäkerhetskollen innefattar mot denna bakgrund säkerhetsarbete inom följande domäner: informationssäkerhet, it-säkerhet, ot-säkerhet och digitala leveranskedjor.

Not 8. Fö2023/00697.

Not 9. Fö2025/00390.

Not 10. Regeringen, *En ny era av cybersäkerhet - Nationell strategi för cybersäkerhet 2025–2029*. https://www.regeringen.se/informationsmaterial/2025/03/nationell-strategi-for-cybersakerhet-2025-2029/ (hämtad 2026/01).

Not 11. Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (hämtad 01/2026).

Digital leveranskedja utgörs av de tjänster och infrastrukturer som levererar eller möjliggör leverans av digitala produkter vilka används för att upprätta, upprätthålla, utveckla eller återställa en verksamhets informationshantering och informationssystem.

Föreskriftskrav avser kraven på ett systematiskt cybersäkerhetsarbete i enlighet med myndighetens föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6) och myndighetens föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7).

Infosäkkollen följer upp nivån på det systematiska informationssäkerhetsarbetet och genomförs för fjärde gången (2021, 2023, 2024[12] och 2025). Frågorna i mätningen är desamma sedan den första mätningen år 2021.

It-säkkollen följer upp nivån på det systematiska it-säkerhetsarbetet och genomförs för tredje gången (2023, 2024 och 2025). Frågorna och strukturen har setts över fullständigt till 2025 så att mätningen följer samma struktur som Infosäkkollen. It-säkollen 2025 genomfördes som pilot och har utvärderats efter genomförd mätning.

Leveranskedjekollen är en ny mätning i Cybersäkerhetskollen 2025 som följer upp nivån på det systematiska säkerhetsarbetet avseende digitala leveranskedjor. Mätningen följer samma struktur som Infosäkkollen. Mätningen 2025 genomfördes som pilot och har utvärderats efter genomförd mätning.

Levererande organisation är en organisation som levererar produkter eller tjänster i digitala leveranskedjor till andra organisationer. Uttrycket används i Leveranskedjekollen.

Mottagande organisation är en organisation som mottar digitala produkter eller tjänster i en digital leveranskedja. Uttrycket används i Leveranskedjekollen.

Nivå per arbetsområde eller **arbetsområdesnivå** är ett mått som beskriver hur långt organisationen har kommit i det systematiska cybersäkerhetsarbetet utifrån organisationens resultat inom ett visst arbetsområde inom Infosäkkollen, It-säkkollen, Ot-säkkollen och Leveranskedjekollen. De fyra nivåerna är:

- Nivå 1: Grunderna i cybersäkerhetsarbetet.
- Nivå 2: Cybersäkerhetsarbetet bedrivs med viss systematik.
- Nivå 3: Kvalificerat innehåll i cybersäkerhetsarbetet.
- Nivå 4: Ständiga förbättringar.

För mer information om hur beräkning av nivån per arbetsområde genomförs, se kapitel 2.

Not 12. Cybersäkerhetskollen genomförs normalt varje udda år, men genomfördes på instruktion av regeringen även 2024.

Nivå i Cybersäkerhetskollen är ett resultat som baseras på den övergripande nivå som har uppnåtts vid genomförandet av samtliga mätningar inom Cybersäkerhetskollen. Nivå 1 i Cybersäkerhetskollen innebär att organisationen har nått nivå 1 eller högre inom samtliga fyra mätningar. Resultatet beaktar således det systematiska cybersäkerhetsarbetet inom domänerna informationssäkerhet, it-säkerhet, ot-säkerhet och säkerhet i digitala leveranskedjor, och förutsätter att organisationen arbetar systematiskt inom samtliga fyra domäner. Givet att inte alla verksamheter bedriver Ot-verksamhet, tas även ett samlat resultat fram baserat på resultatet hos organisationer som deltagit i alla mätningar förutom Ot-säkkollen.

NIS-leverantörer är leverantörer enligt 3 kap. (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, NIS-lagen. NIS-lagen har, efter genomförandet av Cybersäkerhetskollen 2025, ersatts av cybersäkerhetslagen.

Ot-säkkollen är en ny mätning i Cybersäkerhetskollen 2025 som följer upp nivån på det systematiska cybersäkerhetsarbetet avseende styr- och kontrollsystem. ”Ot” är en förkortning av ”operativ teknik”. Mätningen 2025 genomfördes som pilot och har utvärderats efter genomförd mätning.

Resultattal beskriver det samlade resultatet för en enskild organisation baserat på organisationens övergripande nivå, nivå per arbetsområde, totalt genomförda åtgärder samt genomförda åtgärder inom enskilda arbetsområden. Organisationens övergripande nivå väger tyngst i beräkningen av resultattalet. Ett genomsnittligt resultattal kan användas för att beskriva det samlade resultatet för en aktörsgrupp. Resultattal mellan och inom aktörsgrupper kan användas för att synliggöra resultatspridning samt jämföra resultat.

Säker/osäker bedömning avser den bedömning som organisationen behöver göra för varje svarsalternativ (åtgärd) som den har uppgett att den har genomfört (det vill säga kryssat i med ”X”). En säker bedömning innebär att en organisation har tydliga och dokumenterade belägg för att åtgärden/arbetssättet genomförs. Avsaknaden av säkra bedömningar är således liktydigt med att det saknas dokumentation på hur säkerhetsarbetet ska bedrivas, vilket i sin tur medför att systematik saknas.

Typkommun, typregion, typmyndighet och **typförvaltning**, så kallade **typaktörer**, är ett sammanvägt mått för respektive aktörskategori baserat på alla deltagande organisationers inrapporterade uppgifter (typkommunen baseras exempelvis på inrapporterade uppgifter från kommuner). De resultat som presenteras utifrån dessa begrepp är baserade på benchmarkfiltreringar för aktuell aktörsgrupp.

Verksamhetsutövare kallas de som omfattas av cybersäkerhetslagen[13] (NIS2). Många fler organisationer omfattas av cybersäkerhetslagen än av den tidigare NIS-regleringen.

Åtgärd/-er är de handlingar som organisationen vidtar i sitt cybersäkerhetsarbete och som överensstämmer med de svarsalternativ som ges i respektive fråga. Om organisationen vidtar en eller flera åtgärder i enlighet med en frågas svarsalternativ sätter den ett ”X” för respektive svarsalternativ som stämmer med organisationens arbetssätt. För varje ”X” genereras poäng i modellen. På varje fråga kan max fem ”X” uppnås. En åtgärd kan generera poäng inom fler än ett arbetsområde. Totalt antal mätbara åtgärder är 200 för Infosäkkollen, 265 för It-säkkollen, 260 för Ot-säkkollen och 75 för Leveranskedjekollen.

Övergripande nivå är det resultat som beskriver organisationens samlade resultat i en viss mätning på en skala noll till fyra. Den övergripande nivån baseras på uppnådd nivå inom enskilda arbetsområden och avgörs av nivån på det arbetsområde med lägst nivå. Skälet till det är att organisationen behöver bedriva ett systematiskt arbete inom samtliga arbetsområden för att det ska anses vara systematiskt. De fyra nivåerna är:

- Nivå 1: Grunderna i cybersäkerhetsarbetet.
- Nivå 2: Cybersäkerhetsarbetet bedrivs med viss systematik.
- Nivå 3: Kvalificerat innehåll i cybersäkerhetsarbetet.
- Nivå 4: Ständiga förbättringar.

1.3 Om Cybersäkerhetskollen

Cybersäkerhetskollen har två huvudsakliga syften, nämligen att:

1. Bidra till genomförande av en organisations eget förbättringsarbete. Resultatet i Cybersäkerhetskollen visar hur cybersäkerhetsarbetet i en organisation ligger till vid tidpunkten för mätningen och utifrån denna kunskap kan organisationen prioritera och inrikta sitt förbättringsarbete.
2. Möjliggöra framtagandet av en nationell lägesbild. Det samlade resultatet utgör nivån på det systematiska cybersäkerhetsarbetet inom det civila försvaret och ska redovisas till regeringen (denna redovisning).

Cybersäkerhetskollen år 2025 är samlingsnamnet för Myndigheten för civilt försvars fyra cybersäkerhetsmätningar: Infosäkkollen, It-säkkollen, Ot-säkkollen och Leveranskedjekollen. Cybersäkerhetskollens modell bygger på att organisationer bedriver ett systematiskt cybersäkerhetsarbete som omfattar samtliga arbetsområden.

Not 13. Cybersäkerhetslag (2025:1506), https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/cybersakerhetslag-20251506_sfs-2025-1506/ (hämtad 2026/01).

Frågorna i Cybersäkerhetskollen beaktar en bred uppsättning aspekter som ingår i ett systematiskt informations-, it-, ot-säkerhetsarbete samt säkerhetsarbete för digitala leveranskedjor. Modellen täcker dock inte allt som kan ingå.

- Infosäkkollen följer upp säkerhetsarbetet inom tio arbetsområden och består av 40 frågor.
- It-säkkollen följer upp säkerhetsarbetet inom tio arbetsområden och består av 53 frågor.
- Ot-säkkollen upp säkerhetsarbetet inom sju arbetsområden och består av 52 frågor.
- Leveranskedjekollen följer upp säkerhetsarbetet inom fem arbetsområden och består av 15 frågor.

Uppföljningsmodellen i Cybersäkerhetskollen delar in det systematiska cybersäkerhetsarbetet i fyra nivåer som är tänkta att motsvara ett stegvis utvecklingsarbete.

- **Nivå 1:** Organisationen har grunderna i cybersäkerhetsarbetet på plats, åtminstone i begränsad utsträckning.
- **Nivå 2:** Organisationen bedriver cybersäkerhetsarbetet med en viss systematik och är bättre på grunderna än på nivå 1.
- **Nivå 3:** Organisationen har ett kvalificerat innehåll i sitt cybersäkerhetsarbete och är bättre på både grunderna och systematiken än på nivå 2.
- **Nivå 4:** Organisationen arbetar avancerat med ständiga förbättringar samt är bättre på såväl grunderna som systematiken och innehållet än på nivå 3.

Gemensamt för alla nivåer är att de bygger vidare på och fördjupar innehållet från föregående nivå. Till exempel har en organisation på nivå 2 inte bara utvecklat en viss systematik i sitt arbete, det vill säga i vilken utsträckning ett arbetssätt eller en åtgärd tillämpas i organisationen, utan också kommit längre med cybersäkerhetens grunder än en organisation på nivå 1.

Många frågor i Cybersäkerhetskollen följer upp om en säkerhetsåtgärd (arbetssätt eller teknisk åtgärd) har funnits på plats under hela den senaste tvåårsperioden och inte bara någon gång under denna period, eftersom nivån på organisationens cybersäkerhetsarbete är resultatet av arbete och val som har gjorts över tid. Eftersom såväl vidareutvecklingsarbete som uppföljning tar tid att genomföra blir det inte lämpligt att mäta för ofta.

Likt andra modeller kan Cybersäkerhetskollen enbart göra anspråk på att beskriva en uppskattning av hur verkligheten ser ut hos en enskild organisation. Enskilda organisationer kan ha större behov av andra åtgärder än de åtgärder modellen visar att de behöver genomföra för att nå en högre nivå.

Det är vidare viktigt att poängtera att Cybersäkerhetskollen inte utgör en modell eller verktyg som följer upp regelefterlevnad. Därför används uttryck såsom att nivå 3 i modellen motsvarar den nivå som myndigheten har definierat som ”en indikation över huruvida en organisation uppfyller myndighetens föreskriftskrav om statliga myndigheters informationssäkerhet”.

Vid lanseringen av Cybersäkerhetskollen 2025 i april 2025 fanns inte cybersäkerhetslagen på plats i Sverige. Mot denna bakgrund är Cybersäkerhetskollen inte fullt ut anpassad till cybersäkerhetslagen. Samtidigt bedöms att de som klarar av myndighetens föreskriftskrav står rustade för att klara de krav som följer av cybersäkerhetslagen och kommande EU-reglering.

För mer information om modellen, se Fördjupningsinformation om Cybersäkerhetskollen.[14]

1.3.1 Infosäkkollen

Infosäkkollen är inriktad på det systematiska informationssäkerhetsarbetet. Ett systematiskt informationssäkerhetsarbete handlar om att organisationen arbetar medvetet och metodiskt med att analysera, planera, genomföra samt följa upp och förbättra sin informationssäkerhet, samt att de olika delarna av arbetet kopplas ihop till en helhet.

Frågorna i Infosäkkollen har tagits fram med beaktande av myndighetens föreskrifter om krav på informationssäkerhet för statliga myndigheter (MSBFS 2020:6), vilka bygger på standardserien ISO/IEC 27000 om ledningssystem för informationssäkerhet. Nivå 3 i modellen indikerar att en organisation efterlever föreskriftskraven.

1.3.2 It-säkkollen

It-säkkollen är inriktad på det systematiska it-säkerhetsarbetet. År 2025 genomfördes mätningen för första gången i full skala med en metod och struktur som efterliknar Infosäkkollen. It-säkkollen genomfördes som en självskattningsundersökning 2023 och 2024. It-säkkollen 2025 består av 53 frågor och följer upp det systematiska säkerhetsarbetet inom tio centrala arbetsområden. Frågorna i It-säkkollen har tagits fram med beaktande av myndighetens föreskrifter om säkerhetsåtgärder för statliga myndigheter (MSBFS 2020:7). Nivå 3 i modellen indikerar att en organisation efterlever föreskriftskraven.

Endast informationssystem, exempelvis nätverk och it-tjänster, som driftas av den egna organisationen ska beaktas vid besvarandet av It-säkkollen. Arbetssätt kopplade till utkontraktering av it-tjänster följs upp i Leveranskedjekollen.

1.3.3 Ot-säkkollen

Ot-säkkollen är inriktad på det systematiska ot-säkerhetsarbetet. Mätningen genomfördes för första gången i Cybersäkerhetskollen 2025, där den genomfördes som en pilot.

Not 14. Myndigheten för civilt försvar, Fördjupningsinformation om Cybersäkerhetskollen https://www.mcf.se/contentassets/81b192d048734b71a0a3bf21dd7665ae/fordjupningsinformation-csk-2025.pdf (hämtad 01/2026).

Ot-säkkollen är primärt avsedd för organisationer vars verksamhet är beroende av industriella informations- och styrsystem, i denna redovisning kallade ot-system. Dessa system förekommer ofta inom samhällsviktiga sektorer såsom energiförsörjning, dricksvattenförsörjning och transporter, men även andra typer av verksamheter kan omfattas.

Utöver industriella informations- och styrsystem kan ot-system utgöras av switchar, reläer, fjärrterminalsenheter, arbetsstationer eller ytterligare annan hårdvara och mjukvara. Dessa övervakar och kontrollerar fysiska enheter, processer och händelser inom samhällsviktiga sektorer. Verksamheter som ansvarar för ot-system förvaltar ofta äldre sådana. Det innebär att det ofta inte ställts moderna och höga säkerhetskrav för dessa vid deras driftsättning.

Givet ot-systemens relation till fysiska och ofta kritiska samhällsviktiga verksamheter samt industriella processer kan ett avbrott eller en annan säkerhetsrelaterad händelse i ot-tillgången få stora konsekvenser på tillgänglighet och pålitlighet. Givet de potentiellt stora samhällskonsekvenser som olika cybersäkerhetshändelser kan ge upphov till på ot, kan ot-system vara särskilt intressanta för cyberhotaktörer. Mot denna bakgrund är det viktigt att organisationer som är beroende av ot-system bedriver ett systematiskt cybersäkerhetsarbete för dessa.

Kommunala och regionala bolag ansvarar ofta för verksamhet som nyttjar ot-system. Många privata bolag är även verksamma inom de samhällsviktiga sektorer som ofta nyttjar ot-lösningar. Statliga myndigheters verksamhet kan också nyttja och vara beroende av ot-system, men de bedöms inte vara fullt lika många som exempelvis kommunala bolag.

Frågorna i Ot-säkkollen har utformats med beaktande av säkerhetsstandardserien IEC 62443, vilken adresserar cybersäkerhet för industriella automationssystem.

1.3.4 Leveranskedjekollen

Leveranskedjekollen är inriktad på systematiskt säkerhetsarbete avseende digitala leveranskedjor. Mätningen genomfördes för första gången 2025. Uppföljningsmodellen stödjer organisationer att säkra sina leverantörskedjor på en strategisk nivå. Mätningen syftar till att utgöra ett stöd för organisationer givet att säkerhet i digitala leveranskedjor regleras i cybersäkerhetslagen och att avbrott i digitala leveranskedjor kan få stora konsekvenser för den enskilda verksamheten, men även på samhället.

Leveranskedjekollen 2025 är en mindre mätning och består av 15 frågor, varav de 12 första riktar sig till så kallade mottagande organisationer och de 3 sista riktar sig till så kallade levererande organisationer. Frågorna följer upp säkerhetsarbetet inom fyra till fem arbetsområden beroende på om man är en mottagande eller levererande organisation. Leveranskedjekollen genomfördes som en pilot i Cybersäkerhetskollen 2025.

Frågorna utgår från myndighetens analyser som visar att allt fler cyberincidenter påverkar digitala leveranskedjor och att just dessa incidenter riskerar att få betydande samhällskonsekvenser. Detta eftersom en stor mängd organisationer

kan påverkas samtidigt eller efter varandra. Inkomna incidentrapporter till myndigheten visar att leveranskedjeincidenter, det vill säga cyberincidenter som inträffat hos en levererande organisation, inträffar allt oftare.[15] Genom att arbeta systematiskt med säkerhet i digitala leveranskedjor kan cyberincidenter förhindras och konsekvenser för såväl enskilda organisationer som samhälle minimeras. I myndighetens rapport *Hoten mot de digitala leveranskedjorna*[16] identifieras femtio rekommendationer för att stärka de digitala leveranskedjorna i Sverige.

1.3.5 Vad är ett systematiskt cybersäkerhetsarbete?

Arbetet med cybersäkerhet är ett gemensamt ansvar för hela organisationen. Att införa samt förvalta säkerhetsåtgärder är en förutsättning för att organisationen ska kunna använda sin information och leverera sina samhällsviktiga tjänster på avsett sätt. Att bedriva ett systematiskt arbete med cybersäkerhet betyder att det finns en tydlig och strukturerad styrning i enlighet med ledningens uppsatta mål och externa krav (såsom reglering och avtal med externa parter).

Det övergripande syftet med ett systematiskt cybersäkerhetsarbete är att skydda information, it-system, industriella kontroll- och styrsystem, där informationen behandlas, samt att säkerställa att detta är möjligt genom att säkra digitala leveranskedjor hos samhällsviktiga verksamheter på rätt nivå genom ständiga förbättringar och anpassningar till en föränderlig värld. De grundläggande stegen vid allt systematiskt cybersäkerhetsarbete är att:

- Identifiera organisationens information, it-system, ot-system liksom beroenden av digitala leveranskedjor.
- Värdera informationstillgångar, it-system, ot-system samt digitala leveranskedjor utifrån konfidentialitet, riktighet, tillgänglighet och autenticitet.
- Bedöma de risker som kan förekomma mot informationstillgångar, it-system, ot-system och digitala leveranskedjor.
- Införa ändamålsenliga och proportionerliga säkerhetsåtgärder för att säkerställa en nivå på säkerheten i tillgångarna och systemen som är lämplig i förhållande till risken.

Not 15. Myndigheten för civilt försvar, *EU förändrar cybersäkerhetsområdet – Årsrapport it-incidentrapportering 2023,* s. 30. https://www.mcf.se/sv/publikationer/eu-forandrar-cybersakerhetsomradet--arsrapport-it-incidentrapportering-2023/ (hämtad 01/2026).

Not 16. Myndigheten för civilt försvar, *Hoten mot de digitala leveranskedjorna – 50 rekommendation för att stärka samhällsäkerheten*. https://www.mcf.se/sv/publikationer/hoten-mot-de-digitala-leveranskedjorna--50-rekommendationer-for-att-starka-samhallssakerheten/ (hämtad 01/2026).

Uppföljning och utvärdering av arbetets olika delar sker återkommande och är ett centralt underlag i styrningen för att bland annat kunna hantera förändringar i omvärlden.

Systematik innebär även att enhetliga arbetssätt tillämpas i organisationen, till exempel avseende styrning och uppföljning och riskhantering, när organisationen har upprättat ändamålsenliga sådana. Enhetliga arbetssätt bidrar även till kostnadseffektivitet för organisationen på så sätt att organisationen inte behöver ”uppfinna hjulet på nytt”. Till exempel kan en organisations fastställda ramverk för riskhantering inom en domän tillämpas i en annan domän med anpassningar efter behov.

Kapitel 2

Rekommendationer

2. Rekommendationer

Rekommendationerna i kapitel 2 grundar sig på de samlade resultaten och slutsatserna från analysen av Cybersäkerhetskollen 2025 och de allvarliga brister som har noterats i mätningarna.

Givet det ansträngda säkerhetspolitiska läget och att det saknas tecken på närstående förbättring, är det av största vikt att de samhällsviktiga verksamhetsutövare som omfattas av cybersäkerhetslagen stärker sin nivå på det systematiska cybersäkerhetsarbetet och därmed även nivån på Sveriges digitala motståndskraft.

Myndigheten vill mot denna bakgrund betona vikten av att organisationer arbetar målmedvetet, kontinuerligt och långsiktigt med sitt cybersäkerhetsarbete samt att organisationens ledning inriktar, styr, tilldelar resurser och följer upp säkerhetsarbetet med samma engagemang och beslutsamhet som i organisationens övriga centrala verksamhetsfrågor.

2.1 Rekommendationer till regeringen

Myndigheten kan efter genomförandet av Cybersäkerhetskollen 2025 återigen konstatera att utav de 600–700 organisationer, främst privata företag, som omfattades av tidigare NIS-lagstiftning, deltog endast 20 bolag. Trots myndighetens utökade informationsinsatser följer det låga deltagandet hos NIS-leverantörer samma mönster som vid tidigare genomföranden. Myndigheten för civilt försvar kan därmed inte fullgöra regeringens uppdrag om att ta fram en samlad bedömning av nivån på det systematiska cybersäkerhetsarbetet i Sverige och kan därför inte bedöma Sveriges motståndskraft i sin helhet.

Givet ikraftträdandet av cybersäkerhetslagen, och utökningen från 7 till 18 sektorer, bedöms antalet verksamhetsutövare som omfattas av lagen öka till 2000 organisationer eller fler. Ett ökat deltagande är avgörande för att en adekvat analys över nivån på det systematiska cybersäkerhetsarbetet ska kunna göras. Att endast 1 av 18 sektorer deltar är otillräckligt. Det gör det mycket svårt att ta fram sektorsspecifika råd och riktat stöd utifrån verksamhetsutövarnas behov.

Myndigheten för civilt försvar rekommenderar mot bakgrund av det bristande deltagandet i Cybersäkerhetskollen samt det fortsatt låga resultat som genomgående kan noteras bland de som deltar att regeringen överväger att:

- införa ett särskilt mål i den nationella cybersäkerhetsstrategin om att alla verksamhetsutövare i Sverige senast 2030 ska ha uppnått nivå 3 i Cybersäkerhetskollen.
- säkerställa att redan avsatta, samt potentiellt nya medel enligt ett ansökningsförfarande fördelas till utvecklingsarbeten hos offentliga verksamhetsutövare i syfte att åtgärda brister som har framkommit i Cybersäkerhetskollen.
- om en tillströmning av särskilt privata verksamhetsutövare inte noterats efter nästa genomförande, införa krav på verksamhetsutövare enligt cybersäkerhetslagen att delta i Cybersäkerhetskollen.

En satsning kommer att genomföras för att hantera hinder som privat sektor ser för att öka deras deltagande i Cybersäkerhetskollen.

2.2 Rekommendationer till offentlig förvaltning

I detta avsnitt presenterar Myndigheten för civilt försvar de mest centrala rekommendationer som organisationer i offentlig förvaltning behöver följa baserade på identifierade brister i mätningarna. Svaga resultat har uppnåtts i flera av mätningarna när det gäller ledningens engagemang, uppföljning och utvärdering av säkerhetsåtgärder samt incident- och kontinuitetshantering.

Det är viktigt att beakta att organisationer ligger olika till i cybersäkerhetsarbetet och vilka åtgärder som behöver vidtas varierar. En enskild organisation kan därför behöva genomföra andra åtgärder än de som specificeras nedan.

2.2.1 Prioritera arbetet med ett systematiskt cybersäkerhetsarbete på ledningsnivå

Ledningens engagemang är ett område där det uppvisas stora brister i mätningarna. Samtidigt utgör ledningens styrning grunden för ett målmedvetet, systematiskt, kontinuerligt samt riskbaserat cybersäkerhetsarbete. Det innebär att ledningen måste sätta upp mål och inrikta cybersäkerhetsarbetet, hålla sig kontinuerligt informerad om risker samt fatta beslut om vidtagande av säkerhetsåtgärder (organisatoriska, driftsrelaterade eller tekniska).

Därtill är det ledningens ansvar att tilldela tillräckligt med resurser för cybersäkerhetsarbetet (ekonomiska och personella), liksom att tydliggöra mandat och säkerställa kompetens inom cybersäkerhetsområdet. I enkätutvärderingen av Cybersäkerhetskollen 2025 (se avsnitt 4.7) uppger exempelvis 65 procent av organisationerna att de inte har den personal som krävs för att förbättra

cybersäkerhetsarbetet.[17] Detta är ett allvarligt resultat som även har framkommit i tidigare genomförda enkätutvärderingar. Myndigheten för civilt försvar vill mot denna bakgrund framhäva vikten av att ledningen säkerställer att organisationen har tillsatt tillräckligt med personella resurser för att kunna bedriva ett systematiskt cybersäkerhetsarbete som motsvarar nivå 3 i Cybersäkerhetskollen.

För att stärka cybersäkerhetsarbetet är det av högsta vikt att säkerhetsarbetet hanteras och integreras i organisationens befintliga styrning så att frågorna inte hanteras separat. Säkerhetsansvariga, med berörd personal, behöver säkerställa att ledningen får den information som krävs så att medverkande på ledningsnivå har förutsättningar att fatta beslut om mål, inriktning och mandat, liksom tilldelning av adekvata resurser, såväl ekonomiska som personella.

Att cybersäkerhet är en ledningsfråga tydliggörs i cybersäkerhetslagen. Om ledningen inte tar ansvar för cybersäkerhetsarbetet kan det få kostsamma påföljder. Cybersäkerhetslagen och tillhörande föreskrifter om säkerhetsåtgärder innebär att kraven har ökat, särskilt för de verksamhetsutövare som inte tidigare har omfattats av lagen.

2.2.2 Följ upp säkerhetsåtgärder och förbättra arbetssätt

Resultat relaterat till uppföljning och utvärdering är mycket lågt i samtliga fyra mätningar. Uppföljning och utvärdering av vidtagna säkerhetsåtgärder är grundläggande för att organisation och ledning kontinuerligt ska kunna bedöma behov av förändrade eller nya åtgärder i det fall vidtagna åtgärder inte är tillräckliga eller ändamålsenliga.

Som ansvarig för vidtagna säkerhetsåtgärder för informations-, it-, ot- tillgångar eller för digitala leveranskedjor medföljer även ett ansvar att utvärdera om åtgärden är ändamålsenlig. Avsaknad av, eller oregelbunden, uppföljning och utvärdering av säkerhetsarbetet innebär att organisationer inte arbetar systematiskt. Det kan få flera negativa konsekvenser såsom att organisationen inte har ett tillräckligt skydd eller onödiga kostnader i händelse av användning av en föråldrad, icke-ändamålsenlig tjänst från tredjepart.

Hur en säkerhetsåtgärd bör följas upp liksom frekvensen för uppföljningen varierar beroende på skyddsvärdet av tillgången, risken för incidenter och vilken säkerhetsåtgärd det handlar om. Uppföljning och utvärdering behöver genomföras med en viss bestämd regelbundenhet i stället för att ske sporadiskt alternativt i samband med inträffade cyberincidenter.

Not 17. En positiv iakttagelse i enkätutvärderingen av Cybersäkerhetskollen 2025 är att 61 procent uppgett att deras högsta ledning har det engagemang som krävs för att förbättra cybersäkerhetsarbetet. Det motsvarar en förbättring om åtta procentenheter i förhållande till 2024 års utvärdering. Resultatet kan indikera en förbättring gällande ledningens engagemang i cybersäkerhetsarbetet som ännu inte genererat utslag i resultatet av Cybersäkerhetskollen.

För mer stöd avseende uppföljning och förbättring av det systematiska cybersäkerhetsarbetet, se myndighetens metodstöd.[18]

2.2.3 Stärk arbetet med incident- och kontinuitetshantering samt öva

Incident- och kontinuitetshantering, inklusive övning av detsamma, är ytterligare ett område där Cybersäkerhetskollen 2025 visar på stora brister. Samtidigt är incident- och kontinuitetshantering en förutsättning för att organisationer snabbare ska kunna återhämta sig från och mildra konsekvenserna av en inträffad cyberincident eller annan inträffad säkerhetsrelaterad händelse.

Syftet med incident- och kontinuitetshantering är att minimera påverkan på it-miljö, verksamhet eller samhället i stort i händelse av en inträffad cyberincident. Det är därför angeläget att organisationer planerar för hur verksamheten ska kunna bedrivas under både kortare och längre avbrott eller andra händelser som får negativ påverkan på verksamheten.

Att öva sin incident- och kontinuitetshantering är viktigt för att kontrollera att planerna är genomförbara och fungerar. Det gäller både de planer som ledningen ska följa, de som användarna av informationssystemen ska följa, samt de planer som it- och ot-driften ska arbeta utifrån för att få igång informationssystemen igen.

2.3 Rekommendationer från Infosäkkollen

Detta avsnitt ger rekommendationer baserade på resultat i Infosäkkollen 2025. De specifika åtgärder som respektive aktörsgrupp rekommenderas vidta utgår från de åtgärder som typkommunen, typregionen och typmyndigheten hade behövt införa för att nå nivå 3 inom det aktuella arbetsområdet. Om det saknas specifika rekommendationer för en aktörsgrupp beror det på att typaktören har nått nivå 3 eller högre inom det relaterade arbetsområdet.

Resultatet i Infosäkkollen visar att nästan sex av tio organisationer saknar grunderna i sitt systematiska informationssäkerhetsarbete. Endast sex procent når upp till nivå 3 eller högre. Nivå 3 indikerar efterlevnad av föreskriftskrav om informationssäkerhet för myndigheter, vilka har funnits i olika former sedan 2009.

Även om alla organisationer har olika förutsättningar och behov visar analysen ett mönster gällande förbättringsområden som är gemensamma, och som med relativt begränsade insatser kan ge stor effekt. Nedan listas de specifika frågorna, samt vad de syftar till att förbättra.

Not 18. Myndigheten för civilt försvar, Metodstöd för informationssäkerhetsarbete. https://www.mcf.se/sv/amnesomraden/informationssakerhet-och-cybersakerhet/arbeta-systematiskt-med-informationssakerhet-och-cybersakerhet/metodstod-for-informationssakerhetsarbete/ (hämtad 01/2026).

2.3.1 Incident- och kontinuitetshantering:

- Typkommunen, typregionen och typmyndigheten rekommenderas att:
  - Fråga 27 (nivå 2): öva kontinuitetshantering enligt sitt arbetssätt för kontinuitetshantering i ökad utsträckning.
- Typkommunen och typregionen rekommenderas att:
  - Fråga 36 (nivå 3): ombesörja att inträffade avvikelser och incidenter används som underlag för analys av informationssäkerhetsrisker.
  - Fråga 38 (nivå 3): ombesörja att vid behov säkerställa att kontinuitetshanteringsförmåga finns och samt säkerställa att tillgång till alternativ ledningsplats finns vid behov.
- Typkommunen rekommenderas att:
  - Fråga 30 (nivå 3): ombesörja att medarbetarna vet vad de ska göra om en informationssäkerhetsincident inträffar.

2.3.2 Upprättande och utveckling av säkerhetskultur:

- Typkommunen och typregionen rekommenderas att:
  - Fråga 18 (nivå 2): undersöka om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet.
- Typkommunen rekommenderas att:
  - Fråga 30 (nivå 3): ombesörja att undersöka medarbetarnas kunskaper inom fler grundläggande områden.

2.3.3 Analys och hantering av informationssäkerhetsrisker:

- Typkommunen och typmyndigheten rekommenderas att:
  - Fråga 35 (nivå 3): ombesörja att arbetssättet för analys och hantering av informationssäkerhetsrisker omfattar fler centrala typer av sannolikhetsbedömningar.
  - Fråga 36 (nivå 3): ombesörja att arbetssättet för analys och hantering av informationssäkerhetsrisker omfattar riskhantering med fler centrala delar.
- Typkommunen rekommenderas att:
  - Fråga 21 (nivå 2): analysera sina informationssäkerhetsrisker enligt sitt arbetssätt för analys och hantering av informationssäkerhetsrisker i ökad utsträckning.
  - Fråga 23 (nivå 2): fatta beslut om att införa, eller att inte införa, säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker i ökad utsträckning.
  - Fråga 33 (nivå 3): ombesörja att arbetssättet för analys och hantering av informationssäkerhetsrisker omfattar fler centrala delar.

- Typregionen rekommenderas att:
  - Fråga 22 (nivå 2): undersöka och använda resultat från sin omvärldsbevakning vid informationsklassningar och analyser av informationssäkerhetsrisker i ökad utsträckning.

2.3.4 Informationsklassning:

- Typregionen rekommenderas att:
  - Fråga 22 (nivå 2): undersöka och använda resultat från sin omvärldsbevakning vid informationsklassningar och analyser av informationssäkerhetsrisker i ökad utsträckning.

2.3.5 Ledningens styrning och kontroll:

- Typkommunen rekommenderas att:
  - Fråga 14 (nivå 1): följa upp resultatet av sitt systematiska informationssäkerhetsarbete.
  - Fråga 23 (nivå 2): fatta beslut om att införa, eller att inte införa, säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker i ökad utsträckning.
  - Fråga 24 (nivå 2): besluta om att tilldela resurser för att införa beslutade säkerhetsåtgärder i ökad utsträckning.

2.3.6 Uppföljning och utvärdering:

- Typkommunen och typregionen rekommenderas att:
  - Fråga 18 (nivå 2): undersöka om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet i ökad utsträckning.
  - Fråga 26 (nivå 2): utvärdera om införda säkerhetsåtgärder är ändamålsenliga och tillräckliga i ökad utsträckning.
- Typkommunen rekommenderas att:
  - Fråga 7, 8, 9, 10, 11 och 13 (nivå 1): följa upp och utvärdera arbetssätt för informationsklassning, analys och hantering av informationssäkerhetsrisker, hantering av informationssäkerhetsincidenter och -avvikelser, kontinuitetshantering, omvärldsbevakning avseende informationssäkerhet samt, arbetssätt för att säkerställa informationssäkerhet vid upphandling.
  - Fråga 14 (nivå 1): följa upp resultatet av sitt systematiska informationssäkerhetsarbete.
  - Fråga 30 (nivå 3): ombesörja att undersöka medarbetarnas kunskaper inom fler grundläggande områden.

2.3.7 Medarbetarnas kunskaper och utbildningsverksamhet:

- Typkommunen och typregionen rekommenderas att:
  - Fråga 18 (nivå 2): undersöka om medarbetarna använder sina kunskaper i sitt arbete efter genomförd utbildning i informationssäkerhet i ökad utsträckning.
- Typkommunen rekommenderas att:
  - Fråga 30 (nivå 3): ombesörja att undersöka medarbetarnas kunskaper inom fler grundläggande områden.

2.3.8 Inventeringar, undersökningar och omvärldsbevakning:

- Typkommunen och typmyndigheten rekommenderas att:
  - Fråga 11 (nivå 1): införa ett arbetssätt för omvärldsbevakning avseende informationssäkerhet.
- Typregionen rekommenderas att:
  - Fråga 22 (nivå 2): undersöka och använda resultat från sin omvärldsbevakning vid informationsklassningar och analyser av informationssäkerhetsrisker i ökad utsträckning.

2.3.9 Säkerhetsåtgärder och förbättringsarbete:

- Typkommunen och typregionen rekommenderas att:
  - Fråga 26 (nivå 2): utvärdera om införda säkerhetsåtgärder är ändamålsenliga och tillräckliga i ökad utsträckning.
- Typkommunen rekommenderas att:
  - Fråga 23 (nivå 2): fatta beslut om att införa, eller att inte införa, säkerhetsåtgärder utifrån genomförd analys av informationssäkerhetsrisker i ökad utsträckning.
  - Fråga 24 (nivå 2): besluta om att tilldela resurser för att införa beslutade säkerhetsåtgärder i ökad utsträckning.

2.4 Rekommendationer från It-säkkollen

Detta avsnitt ger rekommendationer baserade på resultaten från It-säkkollen 2025. De specifika åtgärder som respektive aktörsgrupp rekommenderas vidta utgår från de åtgärder som typkommunen, typregionen och typmyndigheten hade behövt implementera för att nå nivå 3 inom det aktuella arbetsområdet. Om det saknas specifika rekommendationer för en aktörsgrupp beror det på att typaktören har nått nivå 3 eller högre inom det relaterade arbetsområdet.

Resultatet i It-säkkollen visar att drygt hälften av organisationerna grunderna i sitt systematiska it-säkerhetsarbete. Vidare är det endast fem procent som når upp till övergripande nivå 3 eller högre, där nivå 3 indikerar att organisationer lever upp till myndighetens föreskriftskrav om it-säkerhet för myndigheter.

Även om alla organisationer har olika förutsättningar och behov visar analysen ett tydligt mönster gällande förbättringsområden som är gemensamma, och som med relativt begränsade insatser kan ge stor effekt. Nedan listas de specifika frågor, samt vad de syftar till att förbättra.

2.4.1 Styrning, uppföljning och kontroll:

- Typkommunen, typregionen och typmyndigheten rekommenderas att:
  - Fråga 4, 9, 10 och 11 (nivå 1): följa upp och utvärdera mer frekvent.
  - Fråga 19 (nivå 1): tillse att organisationens ledning informerar sig om status på organisationens it-säkerhetsarbete.
- Typkommunen rekommenderas att:
  - Fråga 3 (nivå 1): följa upp och utvärdera mer frekvent.
  - Fråga 22, 23 och 34 (nivå 3): ombesörja att fler centrala delar är på plats.
- Typregionen rekommenderas att:
  - Fråga 3, 5, 7, 8, 13, 16 och 18 (nivå 1): följa upp och utvärdera mer frekvent.
  - Fråga 35 (nivå 2): införa de säkerhetsåtgärder inom it-säkerhetsarbetet som beslutats.
  - Fråga 41, 46 och 48 (nivå 3): ombesörja att fler centrala delar är på plats.

2.4.2 Dokumentation av it-miljön:

- Typkommunen och typregionen rekommenderas att:
  - Fråga 45 (nivå 3): ombesörja att arbetssättet för säkerhetsloggning omfattar fler centrala uppgifter.

2.4.3 Tekniskt skydd:

- Typkommunen och typregionen rekommenderas att:
  - Fråga 38 (nivå 3): ombesörja att arbetssättet för kryptering omfattar fler centrala områden.
  - Fråga 45 (nivå 3): ombesörja att arbetssättet för säkerhetsloggning omfattar dokumentation av fler centrala uppgifter.
- Typkommunen rekommenderas att:
  - Fråga 25 (nivå 2): använda sitt arbetssätt för kryptering i ökad utsträckning.
- Typregionen rekommenderas att:
  - Fråga 44 (nivå 3): ombesörja att arbetssättet för säkerhetsloggning innebär att säkerhetsloggar utformas utifrån fler centrala principer.

2.4.4 Säkerhetstester och granskning:

- Typregionen rekommenderas att:
  - Fråga 41 (nivå 3): ombesörja att arbetssättet för säkerhetstester och granskning omfattar fler centrala delar.
- Typmyndigheten rekommenderas att:
  - Fråga 28 (nivå 2): analysera sitt behov av säkerhetstester och granskning samt utföra säkerhetstester och granskning enligt sitt arbetssätt i ökad utsträckning.

2.4.5 Incident- och kontinuitetshantering:

- Typkommunen och typregionen rekommenderas att:
  - Fråga 1 (nivå 1): integrera it-säkerhetsarbetet med organisationens övriga kontinuitetshanteringsarbete.
- Typregionen rekommenderas att:
  - Fråga 49 (nivå 3): ombesörja att arbetssättet för återställning av informationssystem omfattar fler centrala områden.

2.5 Rekommendationer från Ot-säkkollen

Detta avsnitt ger rekommendationer baserade på resultaten från Ot-säkkollen 2025. Syftet är att tydliggöra prioriterade åtgärder för att höja den övergripande nivån hos typförvaltningen.[19]

Resultatet i Ot-säkkollen visar att nio av tio organisationer saknar grunderna i sitt systematiska ot-säkerhetsarbete. Ingen organisation har uppnått nivå 3 eller högre i modellen. I första hand bör därför förvaltningarna fokusera på att införa grundläggande arbetssätt inom Ot-säkkollens samtliga sju arbetsområden.

Även om alla organisationer har olika förutsättningar och behov visar analysen ett tydligt mönster gällande förbättringsområden som är gemensamma, och som med relativt begränsade insatser kan ge stor effekt. Nedan listas de specifika frågorna, samt vad de syftar till att förbättra.

2.5.1 Organisation och ledningssystem:

- Fråga 1 (nivå 1): Införa ett arbetssätt för upphandling och säkra leveranskedjor avseende ot.
- Fråga 20 (Nivå 2): Säkerställa att upphandlingar följer arbetssättet för säkra leveranskedjor.
- Fråga 33 (Nivå 3): Utöka ledningssystemet med tydliga regler för personal och leverantörer. Inkludera personkontroller och säkerhetsprövning, roll och ansvarstilldelning, rollanpassad utbildning i cybersäkerhet, kunskapskontroller samt regler för godkänd användning av it-utrustning i ot-miljön.
- Fråga 34 (Nivå 3): Fördjupa de tekniska och administrativa reglerna i ledningssystemet. Täck hot och riskanalys, tilldelning ändring och borttagning av behörigheter, krav på ot-säkerhet vid inköp och upphandling, uppföljning av leverantörer samt säkerhetskrav i systemutveckling, testintegration och driftsättning.

Not 19. Då endast 62 aktörer som deltog i Ot-säkkollen 2025, varav den stora majoriteten var kommuner, riktar sig inte rekommendationer till enskilda aktörsgrupper inom offentlig förvaltning.

2.5.2 Konfigurationshantering:

- Fråga 4 (Nivå 1): Införa ett arbetssätt för att dokumentera och vidmakthålla en inventarielista över alla system och komponenter.
- Fråga 6 (Nivå 1): Införa ett arbetssätt för ändringshantering av konfigurationer i ot-system.

2.5.3 Komponentsäkerhet:

- Fråga 9 (Nivå 1): Införa ett arbetssätt för härdning av komponenter innan de tas i drift.
- Fråga 30 (Nivå 2): Hantera patchar i ot-miljön enligt arbetssättet för patchhantering.

2.5.4 Åtkomstkontroll och skydd av information:

- Fråga 12 (Nivå 1): Införa ett arbetssätt för att identifiera, klassificera och skydda information i ot-miljön.

2.5.5 Incident- och kontinuitetshantering:

- Fråga 15 (Nivå 1): Införa ett arbetssätt för detektering och loggning av säkerhetsavvikelser, händelser och incidenter.
- Fråga 32 (Nivå 2): Hantera incidenter i enlighet med arbetssättet för incidenthantering.
- Fråga 47 (Nivå 3): Utöka arbetssättet för säkerhetsläge i ot-miljön. Definiera stöd för ö-drift, regler för när ö-drift startas och avslutas, samt tekniska funktioner som håller drift igång och säkerställer normala utdata även vid störningar eller brist på indata.
- Fråga 49 (Nivå 3): Fördjupa detektering och loggning av tekniska händelser. Omfatta operativsystemhändelser som omstarter och krascher, onormalt applikationsbeteende, odokumenterade eller obehöriga komponenter och programvara, nya eller ohanterade sårbarheter samt verksamhetsspecifika avvikelser.

2.5.6 Uppföljning och utvärdering:

- Fråga 18 (Nivå 1): Säkerställa att ledningen informeras om status på ot-säkerhetsarbetet.

2.5.7 Nätverk och säkra kommunikationer:

- Fråga 40 (Nivå 3): Fördjupa arbetssättet för trådlös kommunikation. Dokumentera tillåtna protokoll, ställ krav på segmentering mellan trådlösa nät och övriga ot-segment, definiera konfigurationskrav för trådlösa nät och säkerställ dokumentation av aktuell segmentering och konfiguration.

2.6 Rekommendationer från Leveranskedjekollen

Detta avsnitt ger rekommendationer baserade på resultaten från Leveranskedjekollen 2025. De specifika åtgärder som respektive aktörsgrupp rekommenderas vidta utgår från de åtgärder som typkommunen, typregionen och typmyndigheten hade behövt implementera för att nå nivå 3 inom det aktuella arbetsområdet. Om det saknas specifika rekommendationer för en aktörsgrupp beror det på att typaktören har nått nivå 3 eller högre inom det relaterade arbetsområdet.

Resultatet från Leveranskedjekollen visar att sju av tio organisationer saknar grunderna i sitt säkerhetsarbete avseende digitala leveranskedjor. Endast sex procent av organisationerna har klarat nivå 3 eller bättre.

Även om alla organisationer har olika förutsättningar och behov visar analysen ett tydligt mönster gällande förbättringsområden som är gemensamma, och som med relativt begränsade insatser kan ge stor effekt. Nedan listas de specifika frågorna, samt vad de syftar till att förbättra.

2.6.1 Riskhantering:

- Typkommunen och typregionen rekommenderas att:
  - Fråga 1 (nivå 1): införa ett arbetssätt för att hantera risker i sina digitala leveranskedjor.
  - Fråga 5 (nivå 2): använda sitt arbetssätt för att hantera risker i sina digitala leveranskedjor i ökad utsträckning.
- Typmyndigheten rekommenderas att:
  - Fråga 1 (nivå 1): införa ett arbetssätt för att hantera risker i sina digitala leveranskedjor.

2.6.2 Kravställning:

- Typkommunen rekommenderas att:
  - Fråga 6 (nivå 2): använda sitt arbetssätt för kravställning av säkerhet i sina digitala leveranskedjor i ökad utsträckning.

2.6.3 Uppföljning:

- Typkommunen och typregionen rekommenderas att:
  - Fråga 3 (nivå 1): införa ett arbetssätt för att följa upp säkerheten i sina digitala leveranskedjor.
  - Fråga 7 (nivå 2): använda sitt arbetssätt för att följa upp säkerheten i sina digitala leveranskedjor i ökad utsträckning.
  - Fråga 11 (nivå 3): ombesörja att arbetssättet för att följa upp säkerheten i sina digitala leveranskedjor omfattar fler centrala delar.

- Typmyndigheten rekommenderas att:
  - Fråga 7 (nivå 2): använda arbetssättet för att följa upp säkerheten i sina digitala leveranskedjor i ökad utsträckning.
  - Fråga 11 (nivå 3): ombesörja att arbetssättet för att följa upp säkerheten i sina digitala leveranskedjor omfattar fler centrala delar.

2.6.4 Incidenthantering:

- Typkommunen och typregionen rekommenderas att:
  - Fråga 12 (nivå 3): ombesörja att arbetssättet för att hantera incidenter i sina digitala leveranskedjor omfattar fler centrala delar.

2.6.5 Säkra leveranser:

- De kommuner och regioner som levererar produkter eller tjänster i digitala leveranskedjor till andra rekommenderas att:
  - Fråga 14 (nivå 2): använda sitt arbetssätt för att säkerställa säkra leveranser i sina digitala leveranskedjor i ökad utsträckning.
  - Fråga 15 (nivå 3): ombesörja att arbetssättet för att säkerställa säkra leveranser i digitala leveranskedjor omfattar fler centrala delar.
- De myndigheter som levererar produkter eller tjänster i digitala leveranskedjor till andra rekommenderas att:
  - Fråga 14 (nivå 2): använda sitt arbetssätt för att säkerställa säkra leveranser i sina digitala leveranskedjor i ökad utsträckning.

Kapitel 3

Hur resultatet har tagits fram

3. Hur resultatet har tagits fram

Kapitel 3 redogör för analysunderlaget, vilka metoder som används för att sammanställa, jämföra, analysera och presentera resultaten. Det redogör även för NIS-leverantörernas medverkan och varför de har exkluderats från resultatredovisningen.

3.1 Om analysunderlaget

Resultatredovisningen baseras på svar som Myndigheten för civilt försvar har tagit emot under perioden den 23 april till den 12 september 2025. Insamlingen av svar föregicks bland annat av informationsutskick till offentliga förvaltningar och tillsynsmyndigheter enligt NIS-lagen.

Cybersäkerhetskollen riktar sig i första hand till samhällsviktiga verksamheter, det vill säga organisationer inom offentlig förvaltning samt organisationer som omfattas av NIS-reglering. Alla typer av organisationer rekommenderas att använda verktyget och rapportera in sina resultat. Deltagande i Cybersäkerhetskollen är frivilligt.

Samtliga kommuner (290 stycken), regioner (21 stycken) och 238 myndigheter ingår i rampopulationen för Cybersäkerhetskollen 2025. Sammantaget uppgår rampopulationen år 2025 till 549 organisationer i offentlig förvaltning.[20]

När det gäller Infosäkkollen finns data även från tidigare genomförda mätningar (nämligen från 2021, 2023 och 2024) som Myndigheten för civilt försvar genomför jämförande analyser mot. Detta gäller inte för It-säkkollen, Ot-säkkollen och Leveranskedjekollen. För It-säkkollen kan dock deltagarantalet analyseras i förhållande till tidigare års mätningar.

Populationen i hela Cybersäkerhetskollen (de som deltagit i samtliga fyra mätningar) respektive populationen i de enskilda mätningarna varierar. Populationen för respektive mätning framgår av resultatredovisningen för varje mätning.

Not 20. Domstolsverket har rapporterat in ett gemensamt svar för alla domstolars räkning. Myndigheter under riksdagen (5 stycken), statliga affärsverk (3 stycken), AP-fonder (6 stycken), svenska utlandsmyndigheter (108 stycken) ingår inte i populationen.

3.2 NIS-leverantörernas frånvaro

De organisationer som omfattades av NIS-lagen och var leverantörer av samhällsviktiga tjänster, NIS-leverantörer, uppgick till minst 600 organisationer. Genom ikraftträdandet av cybersäkerhetslagen bedöms mellan 3000–5000 verksamhetsutövare omfattas av den nya lagen, varav majoriteten av de samhällsviktiga verksamheterna inom cyberdomänen bedömas utgöras av organisationer inom privat sektor.

I samband med publiceringen av Cybersäkerhetskollen 2025 genomförde Myndigheten för civilt försvar utökade informationsinsatser i förhållande till tidigare år. Utöver riktade informationsutskick till organisationer inom offentlig förvaltning, genomfördes även informationsutskick till tillsynsmyndigheterna enligt NIS-lagen, med en uppmuntran om att skicka informationen om att delta i Cybersäkerhetskollen vidare till anmälda NIS-leverantörer inom respektive sektor. Myndigheten informerade även om lanseringen av 2025 års mätning i sina olika forum (såsom FIDI-nätverk) samt till medlemmar inom Cybercampus och Cybernoden, och genom närvaro på digitala plattformar.

Antalet NIS-leverantörer som rapporterat in sina svar i Cybersäkerhetskollen 2025 är, i enlighet med Cybersäkerhetskollen 2023 och 2024, mycket lågt. Totalt har 20 bolag rapporterat resultat för Cybersäkerhetskollen[21]. Av dessa har 13 stycken uppgett att de är registrerade som NIS-leverantörer.

Givet den låga medverkan från NIS-leverantörer kan Myndigheten för civilt försvar inte genomföra en statistiskt kvalificerad kvantitativ analys över nivån på det systematiska cybersäkerhetsarbetet bland NIS-leverantörerna. Därför har deras inkomna svar exkluderats från samtliga mätningars resultatredovisningar.

Regeringen har uppdragit Myndigheten för civilt försvar att redovisa nivån på det systematiska cybersäkerhetsarbetet inom ramen för det civila försvaret. Myndigheten kan inte redogöra för hela det civila försvarets cybersäkerhetsnivå utifrån att antalet NIS-leverantörer är för få för att redogöras för. Därmed redogörs även 2025 endast för resultatet som inkommit för offentlig förvaltning.

Myndigheten för civilt försvar konstaterar mot denna bakgrund att fler NIS-leverantörer skulle behöva delta i Cybersäkerhetskollen för att myndigheten ska kunna ta fram en nationell bedömning av nivån på det systematiska cybersäkerhetsarbetet inom ramen för det civila försvaret. Under förutsättning att cybersäkerhetslagen inte resulterar i ett ökat deltagande bland privata verksamhetsutövare, rekommenderar myndigheten regeringen att vidta åtgärder för att säkerställa att deltagarunderlaget i framtida mätningar är mer representativt (se avsnitt 2.1).

Not 21. I Infosäkkollen och It-säkkollen har 20 respektive 10 bolag rapporterat in resultat. Tolv bolag har rapporterat in sina svar i både Ot- och Leveranskedjekollen.

3.3 Sammanställning och analys

För att kunna sammanställa, jämföra, analysera och redovisa resultat över uppnådd nivå på det systematiska cybersäkerhetsarbetet används flera specifika metoder som kompletterar varandra. Vid en kvantitativ analys behöver hänsyn tas till antalet vidtagna åtgärder, men även till inbördes relationer mellan olika delar av resultatet. Vidare behövs en metod som är mer nyanserad än enbart nivåindelningen för att kunna jämföra resultat mellan aktörsgrupper. Dessutom ska det inte gå att identifiera enskilda organisationers resultat i sammanställningar och återkoppling.

3.3.1 Beräkning av nivån på det systematiska cybersäkerhetsarbetet

Nivån på det systematiska cybersäkerhetsarbetet i Cybersäkerhetskollen beräknas genom antalet vidtagna åtgärder och andelen säkra bedömningar. För att uppnå respektive nivå krävs ett visst antal genomförda åtgärder som i sin tur ger poäng. Poängen beräknas utifrån jakande svar på frågorna (antal ifyllda ”X”) per fråga och nivå. Varje fråga kan som mest generera fem poäng. Ett arbetsområde kan beakta poäng från ett, eller flera svar, på en eller flera frågor.

För att nå en viss nivå behövs en viss lägsta poäng uppnås. Den lägsta poängen som behöver uppnås beror på nivån. För att nå nivå 1 behövs minst 1 poäng per fråga i nivåavsnitt 1. För att nå nivå 2 behövs minst 2 poäng per fråga i nivåavsnitt 1 och 2 och så vidare. För varje nivå krävs alltså bättre resultat på frågorna i de föregående avsnitten.

”Rörliga poäng” kan vidare bidra till att nå högre i modellens nivåer. Dessa kan samlas på olika sätt. Ett är att samla mer än den lägsta poängen på någon eller några frågor. Ett annat är att svara på någon eller några frågor på högre nivåer.

Slutligen krävs minst 50 procent säkra bedömningar för att en organisation ska uppnå nivå 1. För nivå 2 krävs 60 procent säkra bedömningar, för nivå 3 krävs 70 procent och för nivå 4 krävs 80 procent. En säker bedömning kryssas i när en organisation har tydliga och dokumenterade belägg för de svarsalternativ som de har kryssat i. Avsaknaden av säkra bedömningar är således liktydigt med att det saknas dokumentation på hur säkerhetsarbetet ska bedrivas, vilket i sin tur medför att systematik saknas.

Poängkrav för att uppnå en viss nivå

Kraven för att nå en viss nivå kan sammanfattas i följande ekvation:

Poängkrav för nivå X = (X + 0,5) * antalet frågor som måste besvaras på nivån

X är numret för nivån och är även liktydigt med den lägsta poäng som behövs per fråga för att nå nivån. Antalet rörliga poäng, alltså poäng som kan hämtas från vilken fråga som helst, beräknas som 0,5 * antalet frågor som måste besvaras på nivån.

Nedan följer ett exempel på uträkning av poängkrav för nivå 1 och 2 för It-säkkollen:

- It-säkkollen innehåller 19 frågor på nivå 1. För att uppnå nivå 1 krävs således att organisationen har minst en poäng på varje fråga på nivå 1. Poängkrav för nivå 1 är således 1,5 * 19 frågor = 28,5 (29 poäng).
- För att nå nivå 2 krävs att organisationen har minst två poäng på samtliga frågor på nivå 1 och 2 (det vill säga till och med fråga 35). Poängkrav för nivå 2 är således 2,5 * 35 frågor = 87,5 (88 poäng).

3.3.2 Benchmarks beskriver resultat på gruppnivå för typaktörer

Benchmarks används för att generera resultat för en viss aktörsgrupp baserat på svar från samtliga deltagare i gruppen. I första hand baseras benchmarks på majoritetssvaret för den studerade gruppen. I andra hand redogör det för det största minoritetssvaret. Benchmarks tas fram för exempelvis ”typkommun”, ”typregion”, ”typmyndighet” och ”typförvaltning”.

Benchmark genererar dels ett övergripande resultat för en viss mätning, kallad ”övergripande nivå”, dels en uppnådd nivå inom enskilda arbetsområden, kallad ”nivå per arbetsområde” eller ”arbetsområdesnivå”. Den övergripande nivån baseras i sin tur på nivån inom enskilda arbetsområden. Givet att Cybersäkerhetskollen syftar till att mäta systematik i organisationens cybersäkerhetsarbetes premierar modellen helhet framför spets. Av samma anledning krävs att organisationer uppnår en viss nivå, exempelvis nivå 1, inom samtliga arbetsområden i en mätning för att uppnå 1 som övergripande nivå.

3.3.3 Resultattal är ett precist resultat

Medan benchmarks utgår ifrån ett majoritetssvar alternativt det största minoritetssvaret inom en grupp, är resultattalet ett mått som beskriver det samlade resultatet (baserat på övergripande nivå, nivå per arbetsområde, totalt genomförda åtgärder, samt genomförda åtgärder inom enskilda arbetsområden) för en enskild organisation. Dessutom kan ett så kallat genomsnittligt resultattal användas för att beskriva det samlade resultatet för en aktörsgrupp. Resultattalet representerar en organisations samlade resultat inom en mätning och är ett decimaltal mellan 0 och 4. Genom att jämföra resultattal mellan och inom aktörsgrupper (exempelvis de 10 procent starkaste och de 10 procent svagaste) kan resultattal användas för att synliggöra resultatspridning. På så sätt kompletterar resultattalet benchmark.

3.3.4 Antal genomförda åtgärder

”Antal genomförda åtgärder” kompletterar, nyanserar och fördjupar förståelsen för benchmarkresultaten om ”övergripande nivå” och ”nivå per arbetsområde”. Antalet genomförda åtgärder kan redovisas för en mätning i stort alternativt för ett visst arbetsområde. Genom att analysera antalet genomförda åtgärder är det exempelvis möjligt att notera skillnader mellan aktörsgrupper, hur organisationer presterar mellan olika arbetsområden samt utveckling över tid.

Kapitel 4

Resultat

4. Resultat

Kapitel 4 redovisar resultatet på nivån på det systematiska cybersäkerhetsarbetet för de organisationer som deltagit i Cybersäkerhetskollen 2025. Avsnitt 4.1 beskriver det samlade resultatet i Cybersäkerhetskollen 2025, det vill säga uppnådd övergripande nivå på hela Cybersäkerhetskollen för de organisationer som har deltagit i samtliga fyra mätningar: Infosäkkollen, It-säkkollen, Ot-säkkollen och Leveranskedjekollen.

Kapitlet redovisar sedan uppnådda resultat i respektive enskild mätning: Infosäkkollen, It-säkkollen, Ot-säkkollen och Leveranskedjekollen. Därefter redogör avsnitt 4.6 för jämförelse av resultat mellan mätningar. Avsnitt 4.7 beskriver slutligen resultatet i enkätutvärderingen av Cybersäkerhetskollen 2025.

4.1 Resultat i Cybersäkerhetskollen 2025

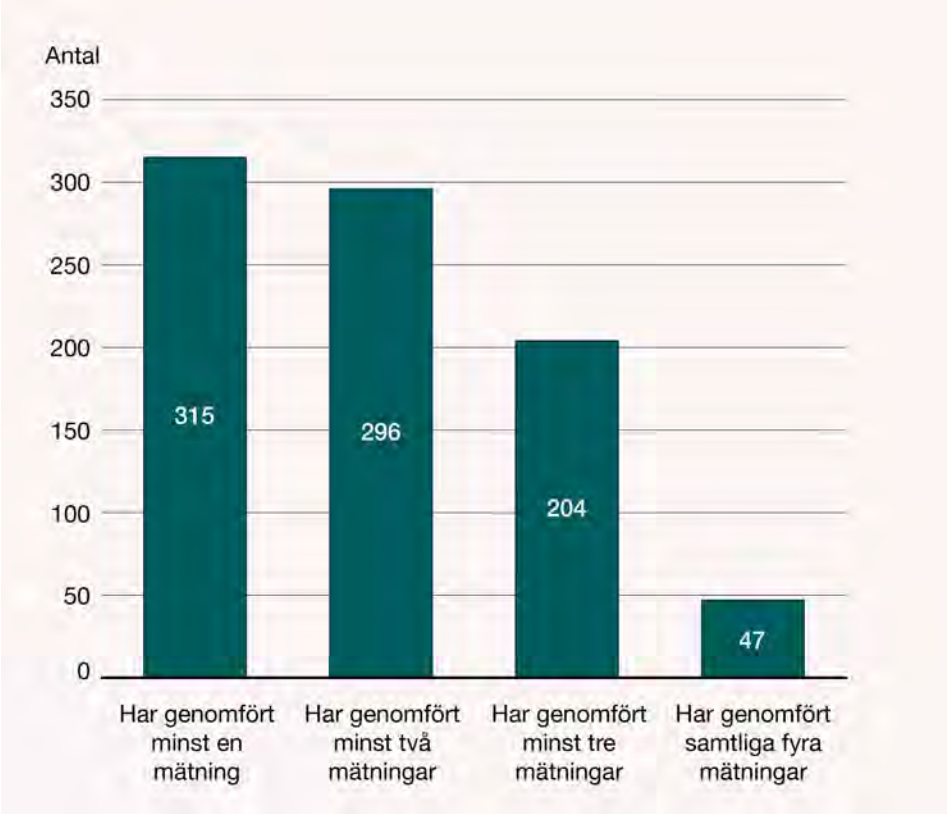
Avsnittet redovisar det samlade resultatet för hela Cybersäkerhetskollen 2025. Då det var relativt få svar som rapporterats in i Ot-säkkollen, delvis mot bakgrund av att alla organisationer inte har ot-system, redovisas även det samlade resultatet för de övriga tre mätningarna.

4.1.1 Deltagande i Cybersäkerhetskollen

Totalt har 335 organisationer medverkat i en eller flera av mätningarna i Cybersäkerhetskollen. Av dessa är 315 organisationer inom offentlig förvaltning (174 kommuner, 13 regioner och 128 myndigheter) och 20 organisationer är privata aktörer. Som konstaterats är svarsunderlaget för privata aktörer alltför litet (se avsnitt 3.2) för att Myndigheten för civilt försvar ska kunna bedriva en statistiskt kvalificerad kvantitativ analys över nivån på det systematiska cybersäkerhetsarbetet hos denna grupp. Resultatet hos privata aktörer har därför exkluderats från resultatredovisningen.

Diagram 1 illustrerar antalet organisationer inom offentlig förvaltning som har deltagit i en eller flera mätningar.

Cybersäkerhetskollen diagram 1. Förvaltningar som deltagit i en eller flera mätningar i Cybersäkerhetskollen 2025



Av diagram 1 framkommer att förhållandevis få organisationer, 47 stycken, har deltagit i samtliga fyra mätningar. Ot-säkkollen är den mätning med minst antal deltagare i (se avsnitt 4.4.1), vilket även får påverkan på deltagandet i hela Cybersäkerhetskollen 2025. Strax över 200 organisationer har deltagit i minst tre mätningar och knappt 300 organisationer har deltagit i minst två mätningar.

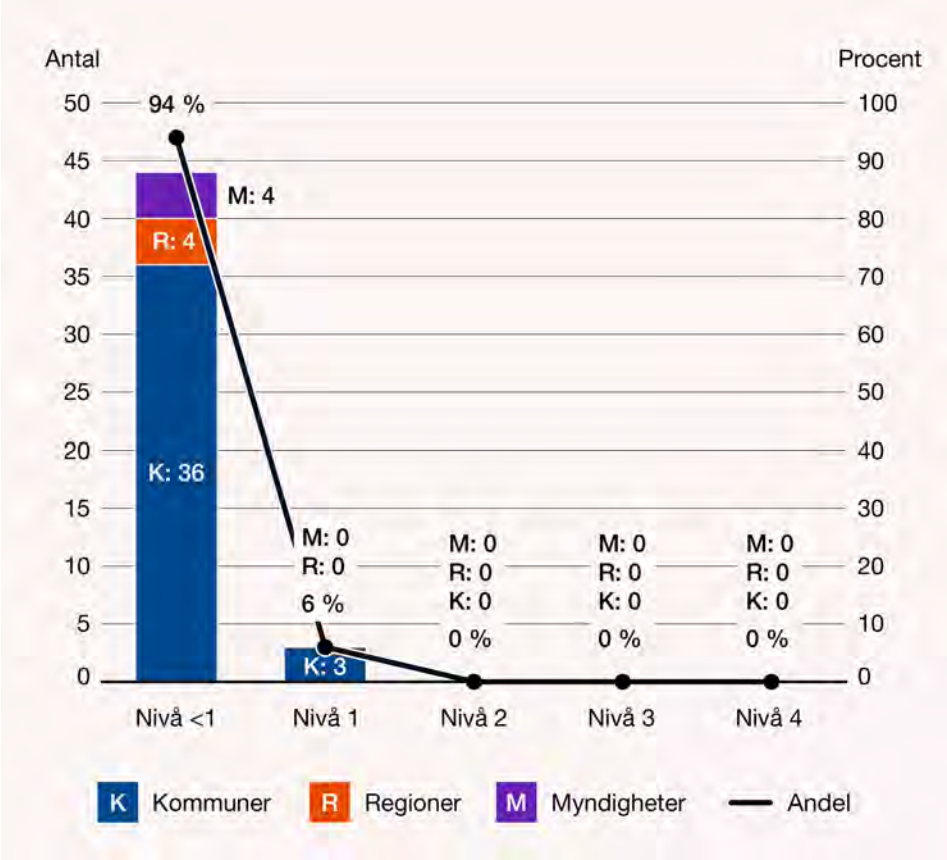
I enkätundersökningen av Cybersäkerhetskollen 2025 (se avsnitt 4.7) undersöktes varför berörda organisationer inte valt att nyttja samtliga mätningar. Det vanligaste skälet var att mätningen eller mätningarna med avseende på organisationens verksamhet inte bedömdes vara relevanta (oftast för att organisationen inte har några ot-system). Andra förekommande förklaringar var att organisationen saknar de resurser eller den kunskap som krävs.

Organisationer har haft mindre tid att planera för sitt deltagande i de tre mätningar som är helt eller delvis nya i Cybersäkerhetskollen. Detta är sannolikt även anledningen till att Infosäkkollen, som genomfördes för fjärde gången, är den mätning med det största deltagandet. Mot denna bakgrund bedömer Myndigheten för civilt försvar det sannolikt att deltagandet i övriga tre mätningar kommer att öka till nästa genomförande.

4.1.2 Fördelning av övergripande nivå i hela Cybersäkerhetskollen

Diagram 2 visar fördelningen av uppnådd övergripande nivå hos de 47 organisationer som svarade på hela Cybersäkerhetskollen, det vill säga som deltog i Infosäkkollen, It-säkkollen, Leveranskedjekollen och Ot-säkkollen. Att en organisation, exempelvis, har nått Cybersäkerhetskollens nivå 1 innebär att organisationen har nått nivå 1 eller högre inom samtliga fyra mätningar.

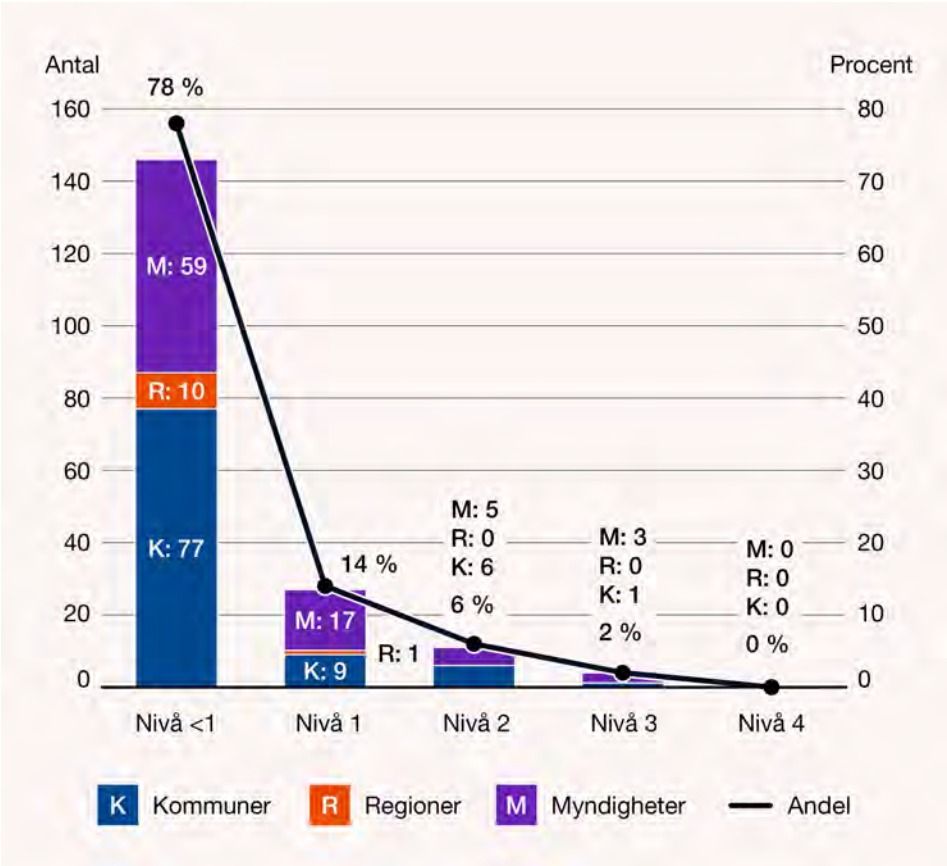
Cybersäkerhetskollen diagram 2. Fördelning av övergripande nivå i hel Cybersäkerhetskollen hos de 47 förvaltningar som har deltagit i samtliga mätningar



Sex procent, motsvarande tre organisationer, har uppnått Cybersäkerhetskollens övergripande nivå 1. Ingen organisation har nått övergripande nivå 2 eller högre. Därmed har mer än nio av tio organisationer inte nått upp till Cybersäkerhetskollens nivå 1. Det som primärt drar ned den övergripande nivån i Cybersäkerhetskollen är uppnått resultat i Ot-säkkollen, där endast sex organisationer nådde övergripande nivå 1 eller högre (se avsnitt 4.4).

Diagram 3 illustrerar fördelningen av uppnådd övergripande nivå när Ot-säkkollen exkluderas, det vill säga när det samlade resultatet för de förvaltningar (188 stycken) som deltagit i Infosäkkollen, It-säkkollen och Leveranskedjekollen beaktas.

Cybersäkerhetskollen diagram 3. Fördelning av övergripande nivå i Cybersäkerhetskollen, exklusive Ot-säkkollen, hos de 188 förvaltningar som deltog i Infosäkkollen, It-säkkollen och Leveranskedjekollen



När de som inte deltagit i Ot-säkkollen exkluderas, har 22 procent av organisationerna uppnått Cybersäkerhetskollens nivå 1 eller högre. En femtedel av organisationerna kan således sägas ha nått den nivå som indikerar att man har grunderna i det systematiska cybersäkerhetsarbetet på plats i samtliga tre cyberdomäner. Det innebär samtidigt att 78 procent av organisationerna saknar grunderna i sitt systematiska säkerhetsarbete inom en eller flera mätningar. Enbart två procent av organisationerna har nått nivå 3 eller högre i samtliga av de tre mätningarna. Nivå 3 är den nivå som indikerar att en organisation arbetar systematiskt inom hela cybersäkerhetsarbetet.

Organisationer bör säkerställa att de bedriver ett systematiskt cybersäkerhetsarbete inom alla de cyberdomäner som de bedriver verksamhet inom. Det är först när arbetet bedrivs systematiskt inom samtliga cyberdomäner som arbetet är systematiskt i sin helhet.

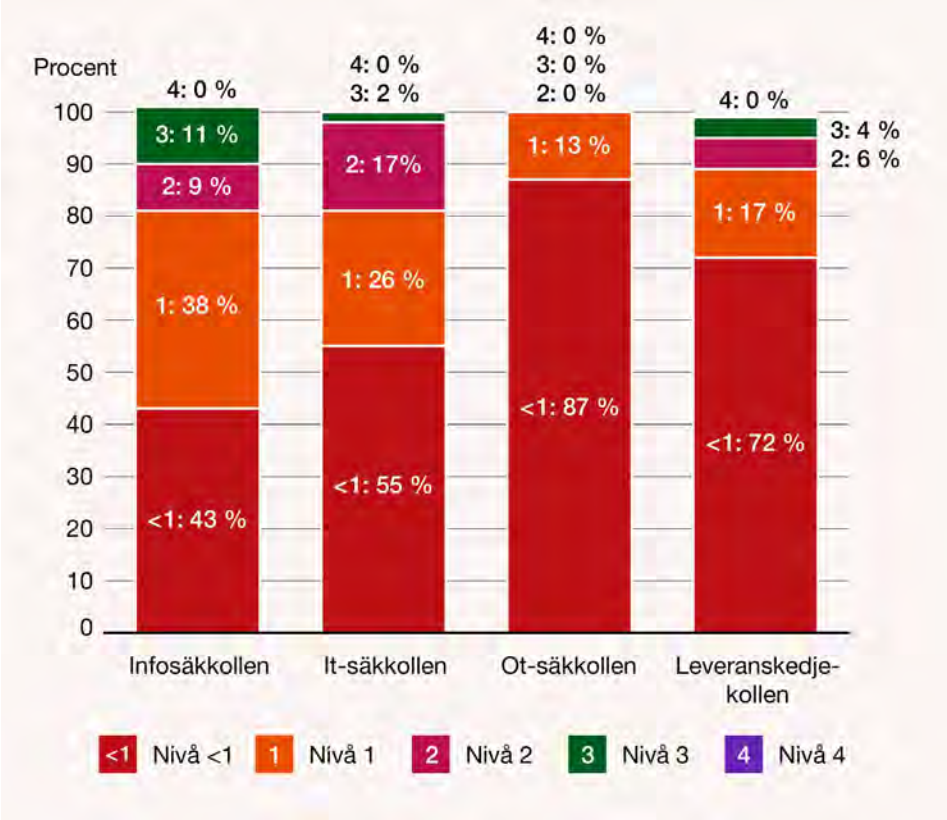
4.1.3 Fördelning av övergripande nivå inom enskilda mätningar

Diagram 4 visar fördelningen av uppnådd övergripande nivå mellan respektive mätning i syfte att jämföra resultatet inom de enskilda mätningarna för de organisationer som har deltagit i samtliga fyra mätningar.[22]

Vid en jämförelse av resultat i enskilda mätningar hos deltagarna, kan konstateras att flest organisationer har nått övergripande nivå 1 eller högre inom Infosäkkollen (57 procent), följt av It-säkkollen (45 procent). När det gäller Ot-säkkollen och Leveranskedjekollen har 13 procent respektive 28 procent uppnått övergripande nivå 1 eller högre. Infosäkkollen är även den mätning där flest organisationer har nått modellens högre nivåer.

Man bör emellertid vara försiktig med att dra slutsatsen att organisationer generellt presterar bättre i informationssäkerhetsarbetet än i de övriga cyberdomäner som följs upp i Cybersäkerhetskollen. Detta eftersom Infosäkkollen har genomförts fyra gånger, medan övriga mätningar genomförs för första gången. Det medför att deltagande organisationer i Infosäkkollen också har haft möjlighet att åtgärda brister som tidigare genomföranden av Cybersäkerhetskollen påvisat. Vidare bör det beaktas att gruppen som deltagit i samtliga fyra mätningar är förhållandevis liten.

Cybersäkerhetskollen diagram 4. Fördelning av övergripande nivå i Infosäkkollen, It-säkkollen, Ot-säkkollen och Leveranskedjekollen hos de 47 förvaltningar som har deltagit i samtliga fyra mätningar



Not 22. Detta till skillnad från de enskilda resultatredovisningarna av de fyra mätningarna inom Cybersäkerhetskollen, där svarsunderlaget varierar mellan mätningarna.

Givet att svarsunderlaget i Cybersäkerhetskollen diagram 4 är förhållandevis litet redovisas diagram 5 som istället illustrerar fördelning av uppnådd övergripande nivå inom Infosäkkollen, It-säkkollen och Leveranskedjekollen hos de 188 organisationer som har deltagit i dessa mätningar.

Cybersäkerhetskollen diagram 5. Fördelning av övergripande nivå hos de 188 deltagande förvaltningarna i Infosäkkollen, It-säkkollen och Leveranskedjekollen

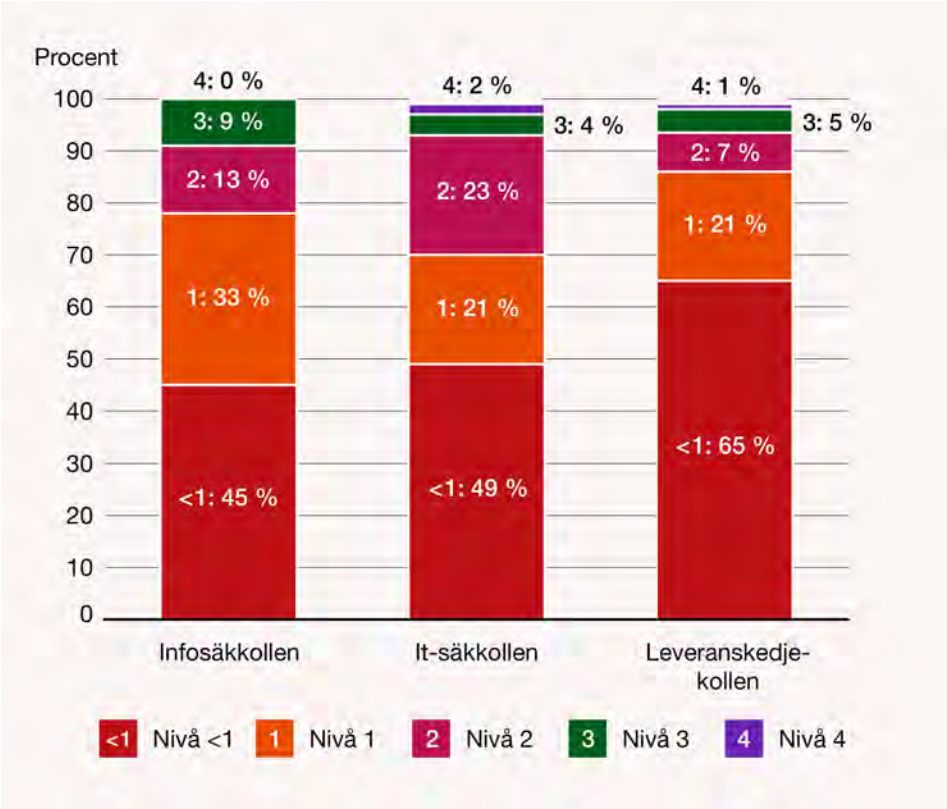


Diagram 5 visar att fler organisationer uppnår nivå 1 eller högre inom samtliga tre mätningar när man beaktar gruppen som har deltagit i Infosäkkollen, It-säkkollen och Leveranskedjekollen. Detta gäller framförallt för It-säkkollen och Leveranskedjekollen. Även om resultatet är jämnare mellan mätningarna återkommer fortfarande det övergripande mönstret. Flest organisationer har uppnått nivå 1 eller högre inom Infosäkkollen (55 procent), följt av It-säkkollen (51 procent). Andelen som har uppnått nivå 1 eller högre är minst i Leveranskedjekollen (35 procent). Återigen bör det faktum att Infosäkkollen genomförts vid fyra tillfällen beaktas, medan övriga mätningar är helt eller delvis nya. Detta innebär att resultatet för de mätningar som utgör nya inslag sannolikt kommer att förbättras i större utsträckning till nästa genomförande av Cybersäkerhetskollen.

En jämförelse av uppnådd övergripande nivå för de organisationer som deltagit i samtliga fyra mätningar respektive Infosäkkollen, It-säkkollen och Leveranskedjekollen kontra motsvarande resultat i enskilda mätningar (se avsnitt 4.2–4,5), visar att gruppen som har deltagit i tre eller fler mätningar generellt har en högre övergripande nivå i mätningarna. Myndigheten för civilt försvar bedömer det sannolikt att det finns ett samband mellan deltagande i fler mätningar och ett väletablerat systematiskt cybersäkerhetsarbete i organisationen. Det är därför även rimligt att de organisationer som har deltagit i fler mätningar, generellt, har ett bättre resultat i Cybersäkerhetskollen än de organisationer som har deltagit i färre.

4.2 Resultat i Infosäkkollen 2025

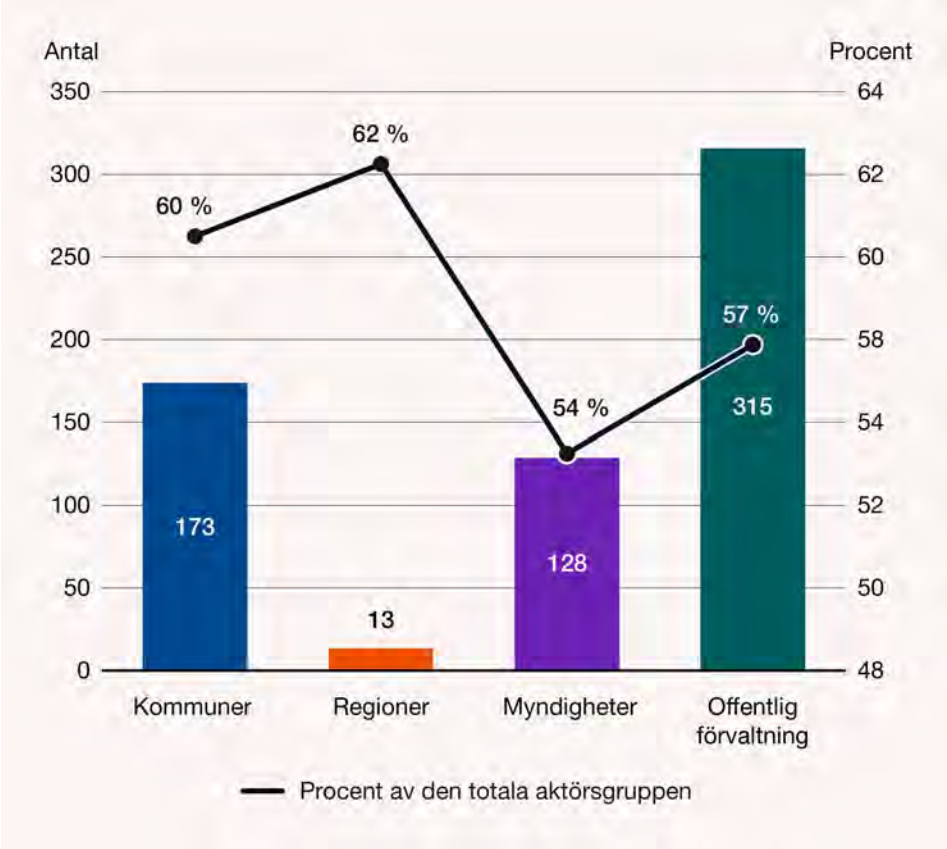
Det här avsnittet redogör för resultatet i Infosäkkollen 2025[23]. Infosäkkollen följer upp nivån på det systematiska informationssäkerhetsarbetet. Resultatredovisningen syftar till att ge en samlad bild över hur informationssäkerhetsarbetet bedrivs, identifiera styrkor och utvecklingsområden samt ge underlag för fortsatt förbättringsarbete.

Eftersom Infosäkkollen har genomförts tidigare redovisas även, till skillnad från övriga tre mätningar i Cybersäkerhetskollen, hur resultatet har förändrats över tid.

4.2.1 Deltagande i Infosäkkollen

Totalt har 315 organisationer inom offentlig förvaltning deltagit i Infosäkkollen 2025, vilket motsvarar 57 procent av Sveriges förvaltningar.[24] Deltagandet utgörs av 173 kommuner, 13 regioner och 128 myndigheter.

Infosäkkollen diagram 1. Deltagande i Infosäkkollen 2025



Not 23. Infosäkkollen har även genomförts 2021, 2023 och 2024.
Not 24. Med Sveriges förvaltningar menas den rampopulation som specificeras i avsnitt 3.1.

I förhållande till sin aktörsgrupp har regionerna deltagit i störst utsträckning (62 procent), följt av kommuner (60 procent) och slutligen myndigheter (54 procent), vilket illustreras i diagram 1. Sett till faktiskt antal är dock kommuner den största aktörsgruppen.[25] Fördelningen mellan aktörsgrupperna liknar i stort sammansättningen av deltagarna i mätningarna 2021, 2023 och 2024.[26]

Infosäkkollen 2025 har det hittills största deltagandet i jämförelse med tidigare års genomföranden. Jämfört med mätningen 2021, som tidigare var den mätning med flest deltagare, har deltagandet ökat inom samtliga tre aktörsgrupper inom offentlig förvaltning. I resultatredovisningen av Cybersäkerhetskollen 2024 konstaterades att deltagandet sjunkit med fyra procentenheter sedan 2023, och med sex procentenheter sedan 2021. Deltagandet i Infosäkkollen 2025 visar därmed på en motsatt trend.

Majoriteten av deltagarna i Infosäkkollen 2025 har även deltagit i tidigare mätningar. Drygt hundra av 2025 års deltagare har rapporterat in sina resultat vid samtliga fyra genomföranden av Infosäkkollen.

4.2.2 Typförvaltningens resultat

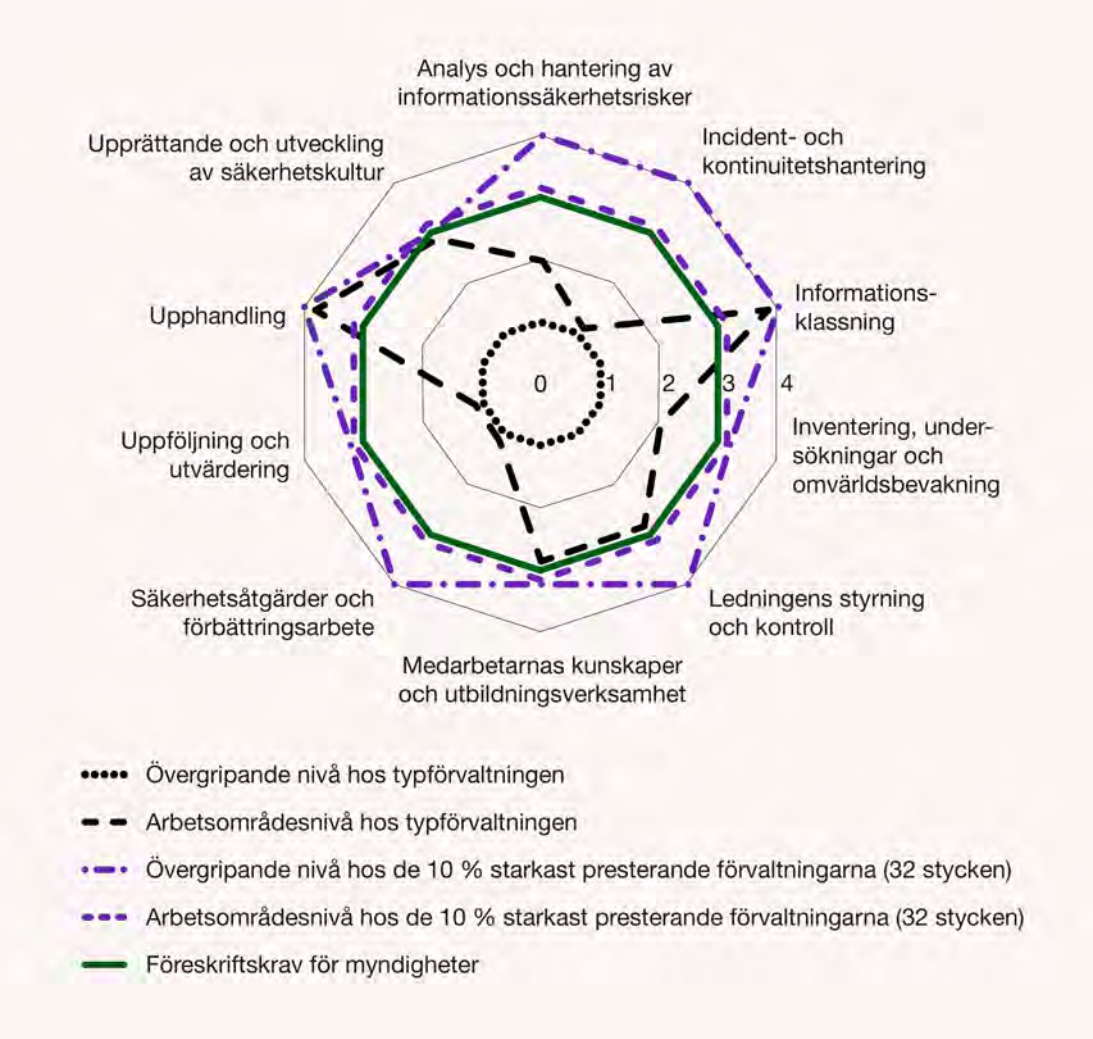
Diagram 2 visar typförvaltningens (se avsnitt 1.2) övergripande nivå inom Infosäkkollen samt nivån inom de tio enskilda arbetsområden som undersöks. Diagrammet presenterar också motsvarande data för de tio procent starkast presterande förvaltningarna. Eftersom nivå tre indikerar efterlevnad av myndighetens föreskrifter om informationssäkerhet för statliga myndigheter[27] har nivån grönmarkerats i diagrammet.

Not 25. Vilken aktörsgrupp som har flest deltagare påverkar typförvaltningens resultat och resultatet för offentlig förvaltning i stort.

Not 26. År 2021 bestod aktörsgruppen offentlig förvaltning av 56 procent kommuner, 3 procent regioner och 41 procent myndigheter. År 2023 utgjordes aktörsgruppen av 53 procent kommuner, 6 procent regioner och 41 procent myndigheter. Motsvarande siffra i mätningen 2024 var 51 procent kommuner, 4 procent regioner och 45 procent myndigheter.

Not 27. Myndighetens föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

Infosäkkollen diagram 2. Resultat i Infosäkkollen för typförvaltningen och typförvaltningen bland de tio procent starkast presterande förvaltningarna



Typförvaltningen har uppnått övergripande nivå 1, vilket indikerar att typförvaltningen har grunderna i ett systematiskt informationssäkerhetsarbete på plats. Nivå 1 var även den övergripande nivå som typförvaltningen uppnådde i Infosäkkollen 2024.[28]

Det kan vidare konstateras att typförvaltningen har uppnått nivå 2 eller högre inom sju av Infosäkkollens tio arbetsområden. För att typförvaltningen ska nå övergripande nivå 2 i Infosäkkollen krävs förbättringar inom *Incident- och kontinuitetshantering, Säkerhetsåtgärder och förbättringsarbete* samt *Uppföljning och utvärdering*.

Det är även värt att notera att typförvaltningen har uppnått nivå 4 inom två arbetsområden, nämligen *Upphandling* och *Informationsklassning*. Resultatet innebär att typförvaltningen inom dessa två arbetsområden har grunderna på

Not 28. I Infosäkkollen 2021 och 2023 nådde inte typförvaltningen nivå 1.

plats, tillämpar relaterade arbetssätt i sin verksamhet, har ett kvalificerat innehåll i sina arbetssätt och följer upp arbetet på ett adekvat sätt.

Vidare kan det konstateras att typförvaltningen har uppnått nivå 3 inom *Ledningens styrning och kontroll*. Detta arbetsområde är samtidigt det arbetsområde där störst andel inte har uppnått nivå 1 eller högre. Diskrepansen förklaras av den kraftiga resultatspridningen inom arbetsområdet (se avsnitt 4.2.5 och avsnitt 4.2.7).

Typförvaltningen bland de tio procent starkast presterande förvaltningarna har uppnått ett resultat som motsvarar nivå 3, vilket indikerar efterlevnad av myndighetens föreskrifter på informationssäkerhetsområdet[29].

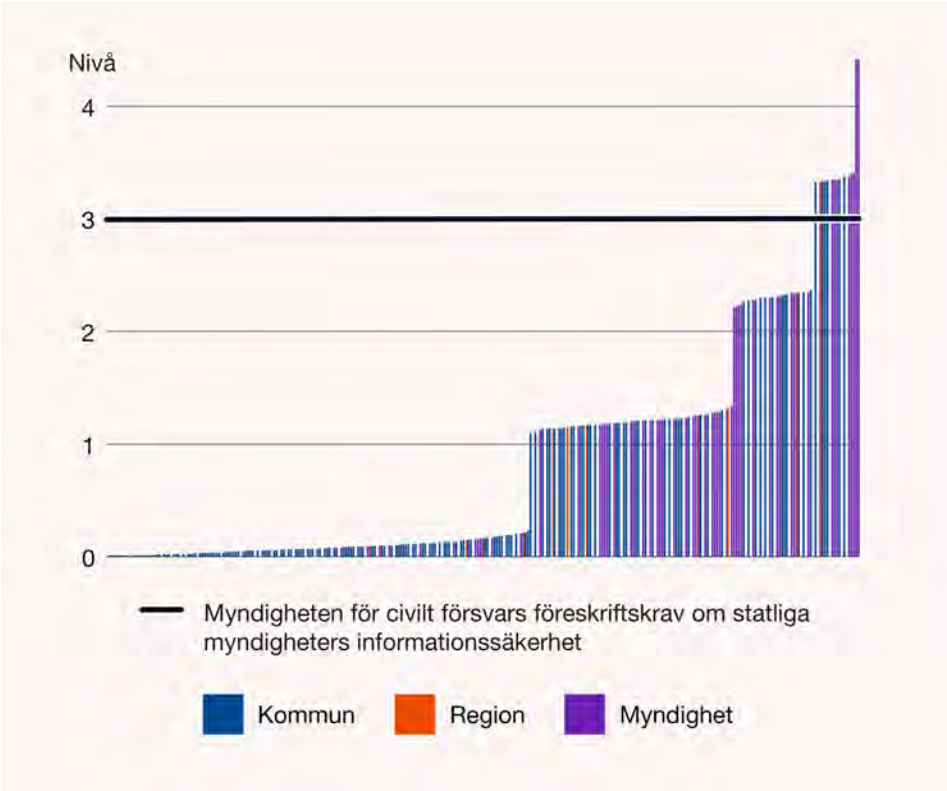
Inom sex av tio arbetsområden har typförvaltningen bland de starkast presterande förvaltningarna uppnått nivå 4. För att de starkast presterande förvaltningarna ska nå nivå 4 som övergripande nivå, vilket är den högsta nivå som kan uppnås inom modellen, hade insatser krävts inom arbetsområdena *Inventering, undersökningar och omvärldsbevakning, Medarbetarnas kunskaper och utbildningsverksamhet, Uppföljning och utvärdering,* samt *Upprättande och utveckling av säkerhetskultur.*

Not 29. Föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

4.2.3 Spridning av resultattal

Diagram 3 syftar inte till att redovisa exakta data, utan till att ge en överblick över resultattalet (se avsnitt 1.2) hos samtliga deltagande förvaltningar och därmed illustrera spridningen i resultaten.

Infosäkkollen diagram 3. Resultattal hos de 314 förvaltningar som deltog i Infosäkkollen 2025



Den svarta linjen i diagrammet motsvarar den nivå som Myndigheten för civilt försvar har definierat som en indikation över huruvida en organisation uppfyller myndighetens föreskriftskrav om statliga myndigheters informationssäkerhet.

Utifrån diagram 3 kan konstateras att resultatspridningen är kraftig både inom och mellan enskilda aktörsgrupper samt i offentlig förvaltning i stort. Det genomsnittliga resultattalet inom offentlig förvaltning är 0,83. Sett utifrån det genomsnittliga resultattalet är kommuner, precis som i tidigare mätningar, den aktörsgrupp som har det lägsta resultatet (0,56). Myndigheterna är den aktörsgrupp som presterar starkast i fråga om genomsnittligt resultattal (1,17). Regionernas genomsnittliga resultattal (0,96) placerar aktörsgruppen mellan kommunerna och myndigheterna. Att myndigheterna presterar starkast i Infosäkkollen, medan kommunerna är svagast, framgår även vid andra aktörsgruppsjämförelser inom ramen för Infosäkkollen.

Vid en jämförelse av det genomsnittliga resultattalet mellan mätningar framkommer att deltagande förvaltningar har förbättrat sig för varje genomförande av Infosäkkollen. En jämförelse av den procentuella förändringen mellan mätningarna indikerar dock att förbättringstakten har saktat in. Mellan mätningen 2023 och 2024 ökade det genomsnittliga resultattalet inom offentlig förvaltning med 33 procent, medan

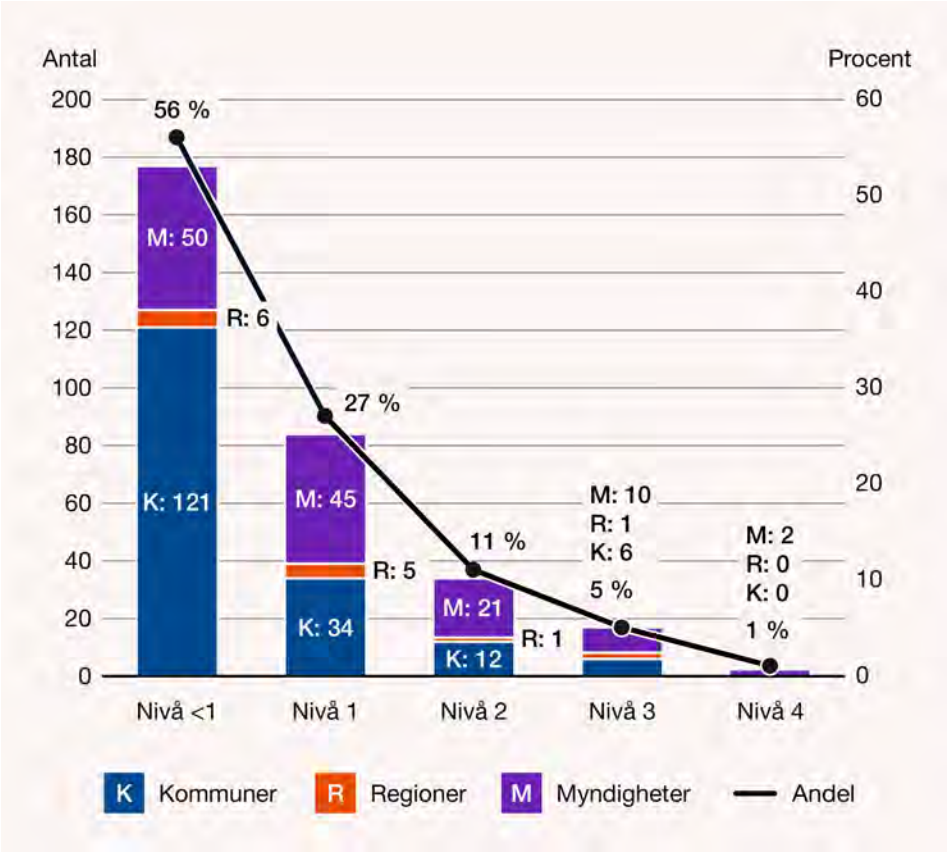
det ökade med 8 procent mellan 2024 och 2025. Även om organisationerna hade dubbelt så lång tid på sig att vidareutveckla sitt informationsarbete mellan Infosäkkollen 2021 och 2023, är det i sammanhanget noterbart att förändringen mellan dessa mätningar motsvarade nästan 130 procent. Mellan 2023 och 2025 var förändringen i stället cirka 45 procent.

Avsaknaden av en större utveckling ska ses i ljuset av att majoriteten av organisationerna saknar grunderna i sitt systematiska informationssäkerhetsarbete. Resultatredovisningen återkommer till den stagnerade förbättringstakten i Infosäkkollen i flera av avsnitten nedan.

4.2.4 Fördelning av övergripande nivå

Diagram 4 visar fördelningen av övergripande nivå bland deltagande förvaltningar, det vill säga andelen som inte uppnått nivå 1 alternativt har nått upp till någon av modellens fyra nivåer. Nivå 1 motsvarar att en organisation har grunderna i ett systematiskt informationssäkerhetsarbete på plats.

Infosäkkollen diagram 4. Fördelning av övergripande nivå hos deltagande förvaltningar



Cirka 44 procent av deltagarna har ett resultat som motsvarar nivå 1 eller högre i Infosäkkollen. Detta innebär att majoriteten av deltagande organisationer, cirka 56 procent, inte når nivå 1. Krav som ställs för nivå 1 i Infosäkkollen är exempelvis att organisationen har etablerade arbetssätt för centrala delar av informationssäkerhetsarbetet, såsom informationsklassning och kontinuitetshantering.

Av diagram 4 framgår vidare att 27 procent av organisationerna har uppnått nivå 1 och 11 procent har uppnått nivå 2. Enbart sex procent av organisationerna har uppnått nivå 3 eller högre. Nivå 3 är den nivå som indikerar efterlevnad av föreskriftskrav på informationssäkerhetsområdet.[30]

När det gäller utvecklingen över tid har det skett en förbättring i fråga om andelen som har uppnått övergripande nivå 1 eller högre sedan den första mätningen av Infosäkkollen, vilken skedde år 2021. Andelen organisationer som har uppnått nivå 1 eller högre har ökat med 25 procentenheter sedan 2021, och med 13 procentenheter sedan mätningen 2023. Jämfört med Infosäkkollen 2024 är dock andelen organisationer som har uppnått nivå 1 eller högre endast marginellt större, enbart två procentenheter. Jämfört med Infosäkkollen 2024 syns ingen noterbar förbättring i fråga om andelen organisationer som har uppnått Infosäkkollens högre nivåer.[31] Även andelen som har uppnått övergripande nivå 3 i Infosäkkollen 2025 är densamma som vid mätningen 2024.

Det noteras att nästan 70 procent av kommunerna inte når övergripande nivå 1 eller högre. Motsvarande siffra hos regionerna är 46 procent, och hos myndigheterna 39 procent. Hos kommunerna rör det sig således om en betydligt större grupp som brister i de mest grundläggande delarna av informationssäkerhetsarbetet, jämfört med de två övriga aktörsgrupperna. I förhållande till 2024 års mätning är det också enbart en procentenhets större andel av kommunerna som har uppnått ett resultat som motsvarar nivå 1 eller högre.[32]

I Infosäkkollen 2025 har 54 procent av regionerna uppnått nivå 1 eller högre. I Infosäkkollen 2024 var motsvarande siffra 83 procent. Det rör sig således om en minskning om 30 procentenheter. Den huvudsakliga förklaringen till resultatförsämringen är att merparten av de svagaste regionerna i Infosäkkollen 2025 inte deltog i mätningen år 2024. Eftersom det totala antalet regioner, och följaktligen också regioner som deltagit i mätningen, är så få ger en mindre förändring i deltagarunderlaget ett stort utslag på resultatet.

Det är vidare noterbart att endast nio procent, motsvarande 12 stycken, av de totalt 128 myndigheterna har nått ett resultat som motsvarar nivå 3 eller högre. Resultatet innebär således att över 90 procent av myndigheterna inte har uppnått ett resultat som indikerar efterlevnad av rådande föreskriftskrav.

Not 30. Föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).
Not 31. I Infosäkkollen 2024 uppnådde 9 procent av organisationerna inom offentlig förvaltning nivå 2, 4 procent uppnådde nivå 3 och 1 procent uppnådde nivå 4.
Not 32. I Infosäkkollen 2024 uppnådde 40 av totalt 136 deltagande kommuner nivå 1, eller högre.

Även om myndighetens föreskrifter för statliga myndigheters informationssäkerhetsarbete har uppdaterats i några omgångar sedan de först trädde i kraft 2009, har myndigheterna omfattats av föreskriftskrav på att bedriva ett systematiskt informationssäkerhetsarbete i över 15 år. Marginellt fler myndigheter når nivå 3 eller högre jämfört med 2024 års genomförande av Infosäkkollen.[33]

Vilka åtgärder som typkommunen, typregionen och typmyndigheten hade behövt vidta för att höja sin övergripande nivå redovisas i avsnitt 3.3.

4.2.5 Fördelning av nivå per arbetsområde

Diagram 5 visar vilken nivå organisationerna har uppnått inom Infosäkkollens tio arbetsområden. Diagrammet synliggör också en förhållandevis stor variation gällande hur deltagande organisationer presterar inom varje enskilt arbetsområde.

Mätningarna inom Cybersäkerhetskollen syftar till att mäta systematik i säkerhetsarbetet och premierar därför helhet. Modellen ställer därför krav på att man har nått en viss nivå, exempelvis nivå 1, inom samtliga arbetsområden för att man också ska nå nivå 1 som övergripande nivå.

Not 33. År 2024 nådde 8 av de 120 myndigheter som deltog i Infosäkkollen nivå 3 eller högre.

Infosäkkollen diagram 5. Fördelning av nivå per arbetsområde hos deltagande förvaltningar

Infosäkkollen diagram 5 fortsättning. Fördelning av nivå per arbetsområde hos deltagande förvaltningar

Precis som i Infosäkkollen 2024 är de tre arbetsområden där den största andelen organisationer når nivå 1 eller högre *Säkerhetsåtgärder och förbättringsarbete*[34] (99 procent), *Informationsklassning* (80 procent) samt *Analys och hantering av informationssäkerhetsrisker* (76 procent). Det bör dock uppmärksammas att det inom två arbetsområden, *Inventering, undersökningar och omvärldsbevakning* samt *Upphandling*, rör sig om en nästan lika stor andel som uppnått nivå 1 eller högre (75 procent) som *Analys och hantering av informationssäkerhetsrisker.*

Arbetsområdena *Upphandling* och *Informationsklassning* är de arbetsområden där den högsta andelen (45 respektive 39 procent) har nått nivå 3 eller högre. Inom arbetsområdet *Upphandling* nådde över 75 procent av regionerna ett resultat som motsvarar nivå 3 eller högre.

Av diagram 5 kan också konstateras att de arbetsområden där den minsta andelen har nått nivå 1 eller högre är *Ledningens styrning och kontroll* (53 procent), *Uppföljning och utvärdering* (59 procent), samt *Incident- och kontinuitetshantering* (65 procent).

I fråga om utvecklingen över tid bör det uppmärksammas att det är samma tre arbetsområden där den minsta andelen organisationer har uppnått nivå 1 eller högre som i Infosäkkollen 2024. Det är vidare noterbart att andelen som har uppnått nivå 1 eller högre inte har ökat alls alternativt ökat i marginell utsträckning sedan 2024 års mätning. Gällande *Ledningens styrning och kontroll* är andelen som har nått nivå 1 eller högre densamma som i mätningen 2024. Inom detta arbetsområde kan det samtidigt konstateras att 20 procent har uppnått nivå 3 eller högre, en siffra som överträffar flera andra arbetsområden. Det visar på en stor resultatspridning inom arbetsområden *Ledningens styrning och kontroll*.

Inom arbetsområdet *Uppföljning och utvärdering* har andelen som har uppnått nivå 1 eller högre enbart ökat med två procentenheter sedan mätningen 2024. Förbättringen är att betrakta som blygsam med hänsyn till den låga grundnivån. *Uppföljning och utvärdering* är också det arbetsområde där den minsta andelen (15 procent) har uppnått nivå 3 eller högre.

I Infosäkkollen 2024 var även *Incident- och kontinuitetshantering* ett av de tre arbetsområden där den minsta andelen organisationer uppnådde nivå 1 eller högre. Andelen som uppnår nivå 1 eller högre i Infosäkkollen är dock fortfarande 65 procent, samma som i 2024 års mätning.

Diagram 5 synliggör inte vilken nivå som de olika aktörsgrupperna har uppnått. Det bör dock uppmärksammas att kommunerna är den aktörsgrupp som har den lägsta andelen som uppnår nivå 1 eller högre inom alla arbetsområden förutom *Analys och hantering av informationssäkerhetsrisker*. Inom detta arbetsområde har i stället regionerna har det svagaste resultatet. Kommunernas resultat inom arbetsområdena *Ledningens styrning och kontroll* samt *Uppföljning och*

Not 34. Den mycket höga andelen som uppnått nivå 1 inom arbetsområdet för Säkerhetsåtgärder och förbättringsarbete bör också tolkas i ljuset av att det enbart krävs genomförande av två åtgärder för att nå nivå 1 för arbetsområdet.

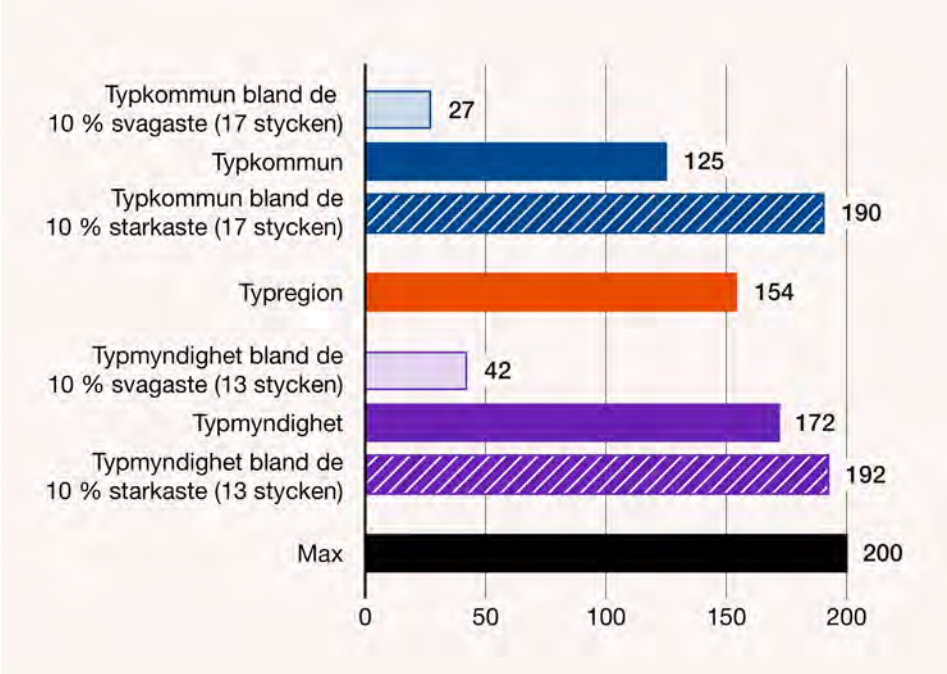
utvärdering avviker särskilt eftersom en majoritet av kommunerna inte uppnår nivå 1. Kommunernas resultat för *Ledningens styrning och kontroll* är särskilt anmärkningsvärt då endast 39 procent av kommunerna når nivå 1 eller högre.

4.2.6 Antal genomförda åtgärder hos typaktörerna

Infosäkkollen undersöker totalt 200 stycken åtgärder. Diagram 6 och 7 redogör för det totala antalet åtgärder som aktörsgrupperna har genomfört respektive antalet åtgärder som aktörsgrupperna infört inom varje enskilt arbetsområde. Det bör samtidigt understrykas att diagrammen inte synliggör huruvida de åtgärder som vidtagits avser mer grundläggande åtgärder eller åtgärder som undersöks inom modellens högre nivåer.

Diagram 6 visar antalet vidtagna åtgärder hos typkommunen, typregionen och typmyndigheten samt antalet genomförda åtgärder hos typmyndigheten och typkommunen hos de tio procent starkaste respektive tio procent svagaste kommunerna och myndigheterna.

Infosäkkollen diagram 6. Totalt antal genomförda åtgärder hos typkommunen, typregionen och typmyndigheten, samt de 10 procent svagast presterande respektive starkast presterande kommunerna och myndigheterna[35]



Av diagram 6 framgår att typmyndigheten är den aktörsgrupp som genomfört flest åtgärder (172 stycken), följt av typregionen (154 stycken). Typkommunen är den aktörsgrupp som genomfört minst antal åtgärder (125 stycken). Mellan den starkaste aktörsgruppen, det vill säga myndigheterna, respektive den svagaste, det vill säga kommunerna, skiljer det sig därmed 47 åtgärder.

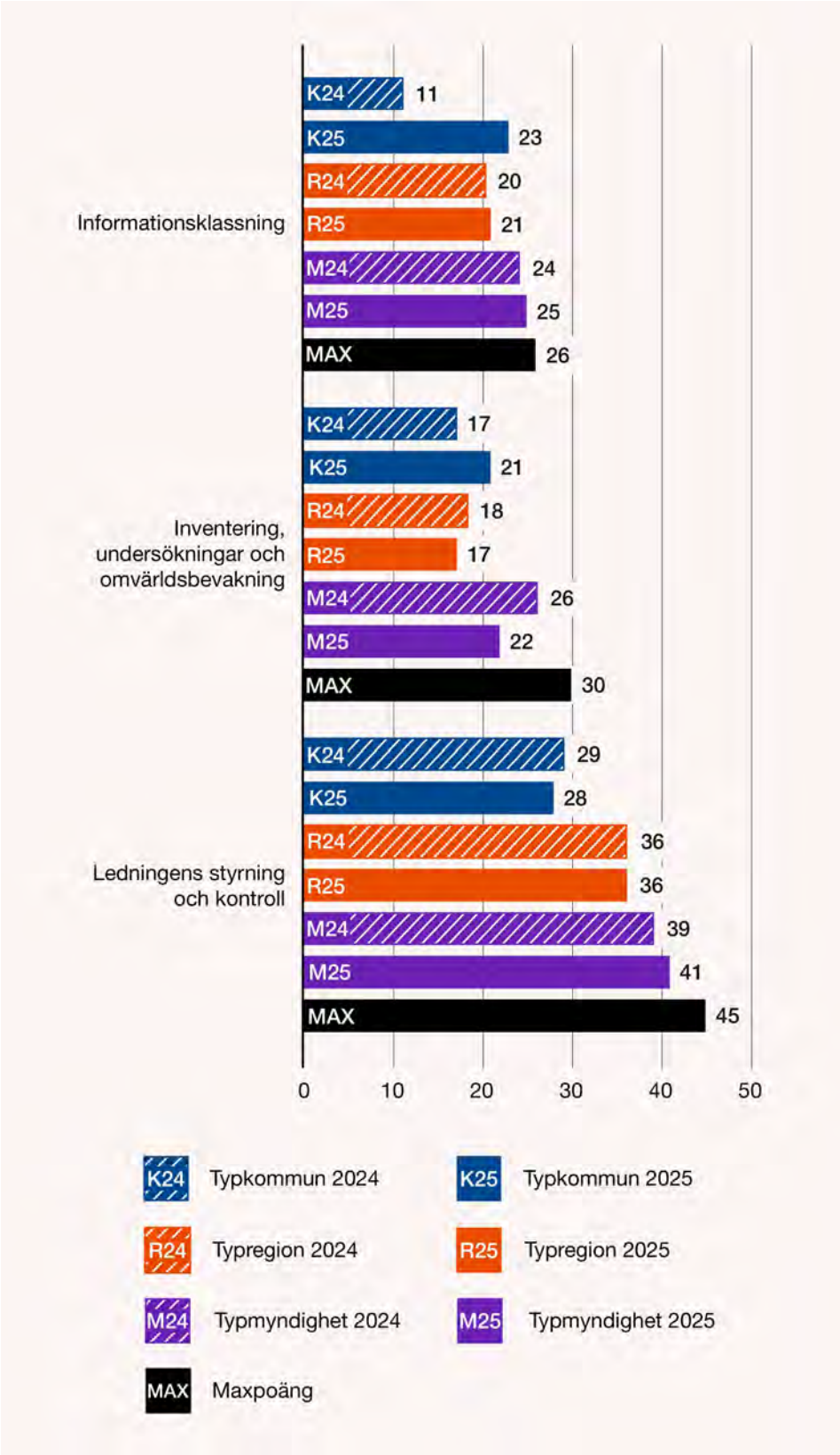
Not 35. Regionerna är en för liten aktörsgrupp för att det ska vara fruktsamt att ta fram resultatet för de tio procent starkaste regionerna.

Diagrammet synliggör också att typmyndigheten hos de tio procent svagaste myndigheterna presterar starkare än motsvarande aktörsgrupp hos kommunerna. Skillnaden mellan dessa två aktörsgrupper motsvarar totalt 15 åtgärder.

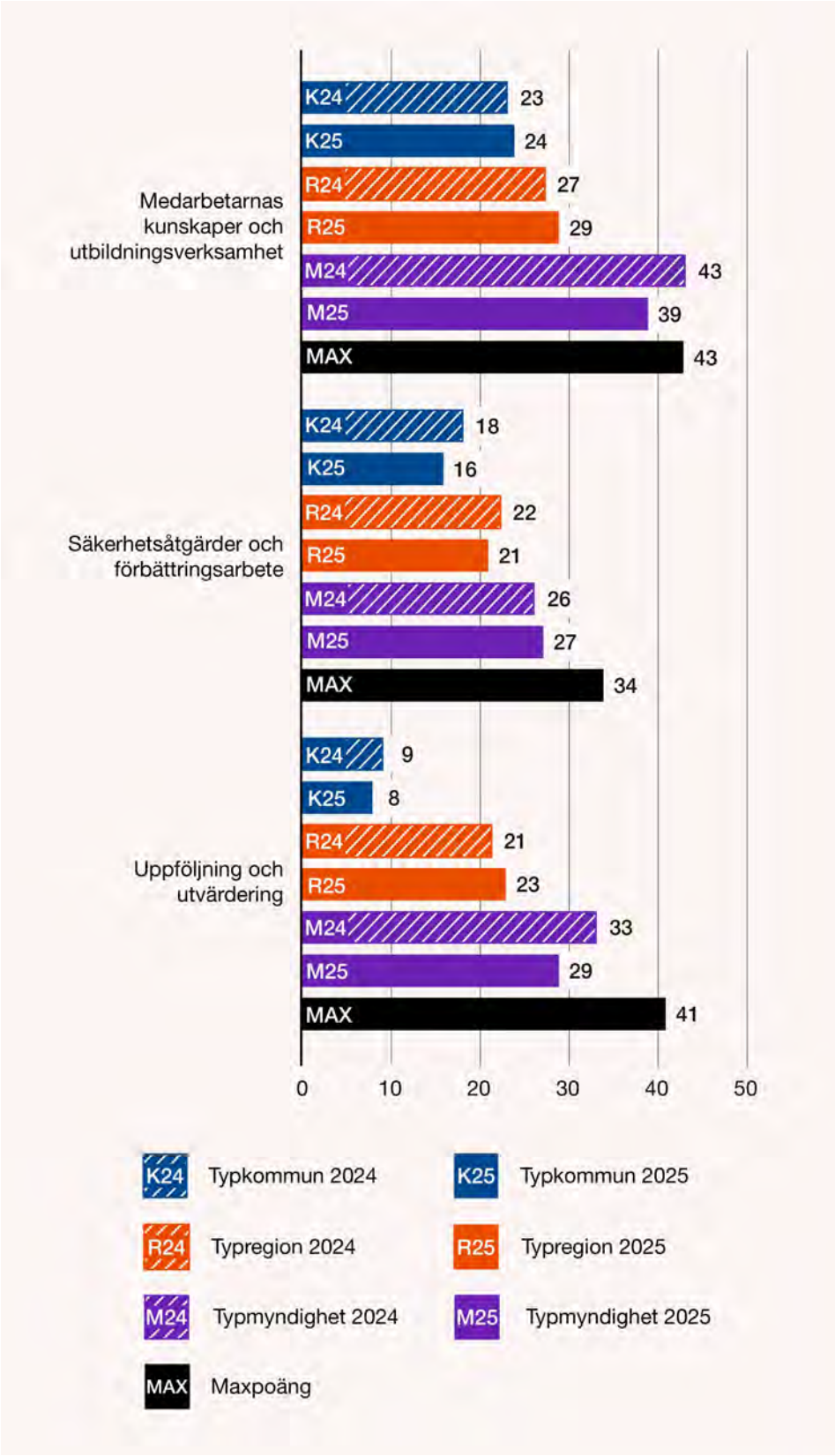
Mellan typkommunen hos de starkaste kommunerna respektive typmyndigheten hos de starkaste myndigheterna skiljer det sig dock enbart två åtgärder. Inom båda dessa grupper saknas enbart ett fåtal av de åtgärder som undersöks inom Infosäkkollen.

Infosäkkollen diagram 7. Antal genomförda åtgärder per arbetsområde hos typkommunen, typregionen och typmyndigheten år 2024 respektive 2025

Infosäkkollen diagram 7 fortsättning. Antal genomförda åtgärder per arbetsområde hos typkommunen, typregionen och typmyndigheten år 2024 respektive 2025



Infosäkkollen diagram 7 fortsättning. Antal genomförda åtgärder per arbetsområde hos typkommunen, typregionen och typmyndigheten år 2024 respektive 2025



Infosäkkollen diagram 7 fortsättning. Antal genomförda åtgärder per arbetsområde hos typkommunen, typregionen och typmyndigheten år 2024 respektive 2025

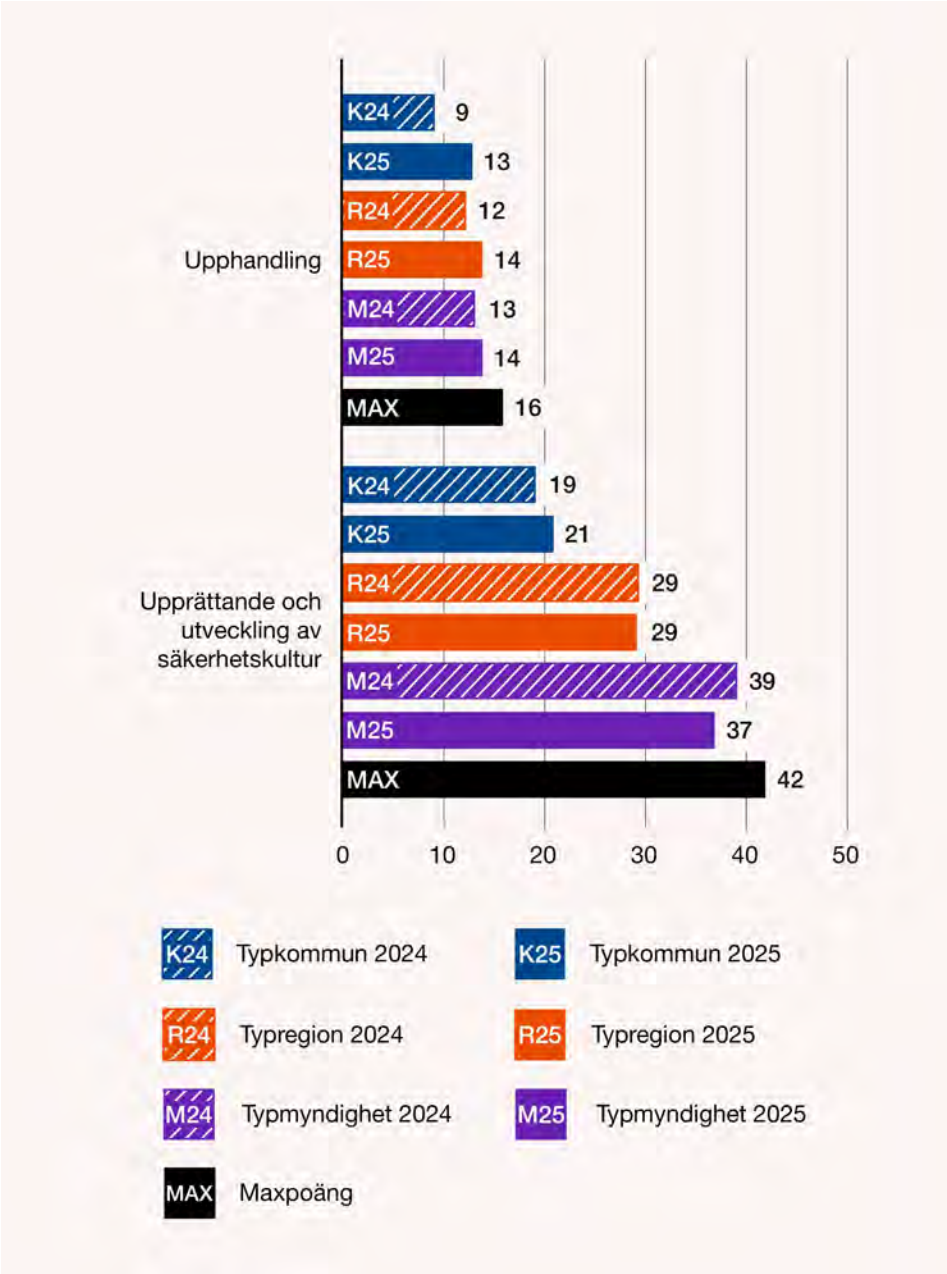


Diagram 7 ger en mer detaljerad bild över antalet vidtagna åtgärder genom att visa hur många åtgärder som aktörsgrupperna har genomfört inom varje arbetsområde. I syfte att tydliggöra utvecklingen inom informationssäkerhetsarbetet synliggör även diagrammet motsvarande resultat i Infosäkkollen 2024.

I Infosäkkollen 2025 har samtliga aktörsgrupper vidtagit förhållandevis många åtgärder (i genomsnitt över 85 procent) inom arbetsområdena *Informationsklassning* och *Upphandling*. Inom arbetsområdet *Informationsklassning* är det noterbart att typmyndigheten har vidtagit över 95 procent av de åtgärder som modellen mäter.

Alla tre aktörsgrupper har vidtagit den minsta andelen åtgärder (i genomsnitt 49 procent) inom arbetsområdet *Uppföljning och utvärdering*. Som konstaterats i avsnitt 4.2.5 är det också ett av de arbetsområden där den minsta andelen av organisationerna har uppnått nivå 1 eller högre. I fråga om arbetsområdet *Uppföljning och utvärdering* är det vidare anmärkningsvärt att typkommunen enbart har genomfört 20 procent av de åtgärder som undersöks. Detta är ett resultat som avviker från både de övriga två aktörsgrupperna liksom typkommunens resultat inom andra arbetsområden.

Det bör också noteras att samtliga tre aktörsgrupper, i jämförelse med övriga arbetsområden, har genomfört förhållandevis många åtgärder inom arbetsområdet *Ledningens styrning och kontroll*, vilket samtidigt är det arbetsområde där den minsta andelen organisationer har uppnått nivå 1 eller högre. Antalet åtgärder som vidtagits inom detta arbetsområde indikerar att aktörsgrupperna har goda förutsättningar att höja sin nivå inom detta arbetsområde, förutsatt att åtgärder inom modellens lägre nivåer vidtas.

Av diagram 7 kan vidare konstateras att typkommunen, med undantag för *Inventering, undersökningar och omvärldsbevakning* samt *Informationsklassning* (där typregionen i stället har genomfört minst antal åtgärder), är den aktörsgrupp som har vidtagit minst antal åtgärder inom arbetsområdena. Inom tre arbetsområden, *Säkerhetsåtgärder och förbättringsarbete*, *Analys och hantering av informationssäkerhetsrisker* samt *Uppföljning och utvärdering*, har typkommunen vidtagit mindre än hälften av undersökta åtgärder. Typmyndigheten har, med undantag för arbetsområdet *Incident- och kontinuitetshantering* (där typregionen i stället har det starkaste resultatet), genomfört lika många eller fler åtgärder än typregionen.

I fråga om utvecklingen sedan Infosäkkollen 2024 är det noterbart att förbättringen inom enskilda arbetsområden, med några undantag, är marginell. I vissa fall har typaktörerna till och med ett lägre resultat än föregående år. Det saknas även positiva signaler för det arbetsområde där samtliga tre aktörsgrupper har genomfört det minsta antalet antal åtgärder, det vill säga arbetsområdet *Uppföljning och utvärdering*. Inom detta arbetsområde har endast regionerna förbättrat sitt resultat. Kommunerna och myndigheterna har i stället ett sämre resultat jämfört med Infosäkkollen 2024.

Typkommunen uppvisar en markant förbättring i fråga om antalet genomförda åtgärder inom arbetsområdena *Analys och hantering av informationssäkerhetsrisker* samt *Informationsklassning*. Inom dessa två arbetsområden har man genomfört över dubbelt så många åtgärder genomförda jämfört med Infosäkkollen 2024. I övriga arbetsområden uppvisar typkommunen antingen en svag förbättring eller till och med en försämring.

Typregionens resultat motsvarar i stora drag resultatet i 2024 års mätning. I de arbetsområden där resultatet har förbättrats rör det sig enbart om enstaka åtgärder. I fyra arbetsområden har typregionen samma, alternativt ett marginellt svagare resultat.

Typmyndigheten uppvisar den svagaste resultatutvecklingen i förhållande till Infosäkkollen 2024. I arbetsområdena *Inventering, undersökningar och omvärldsbevakning*, *Medarbetarnas kunskaper och utbildningsverksamhet*, *Uppföljning och utvärdering* samt *Upprättande och utveckling av säkerhetskultur* har typmyndigheten genomfört fyra respektive två färre åtgärder jämfört med 2024. I övriga sex arbetsområden har typmyndigheten enbart förbättrat sitt resultat med en åtgärd.

Diagram 7 tydliggör slutligen att omfattningen av arbetet varierar mellan arbetsområdena, särskilt hos kommunerna. Variationen indikerar att organisationer inom offentlig förvaltning har valt att fokusera på vissa områden och, medvetet eller omedvetet, nedprioriterat andra.

4.2.7 Resultatspridning

Diagram 8 jämför det genomsnittliga resultattalet (se avsnitt 1.2) mellan normalfördelningsgruppen samt de svagaste respektive starkast presterande förvaltningarna i syfte att tydliggöra resultatspridningen bland deltagarna. Normalfördelningen ses i detta sammanhang som de 80 procent som varken hör till de svagaste eller bäst presterande förvaltningarna.

Infosäkkollen diagram 8. Resultatspridning hos deltagande förvaltningar

Infosäkkollen diagram 8 fortsättning. Resultatspridning hos deltagande förvaltningar

Utifrån diagram 8 kan det konstateras att resultatspridningen, både i Infosäkkollen som helhet, och inom enskilda arbetsområden, är mycket stor. Medan de tio procent svagaste förvaltningarna, med ett undantag[36], har ett genomsnittligt resultattal på noll, har de tio procent starkaste förvaltningarna ett resultattal på över tre i samtliga arbetsområden. Inom fler än hälften av arbetsområdena ligger de tio procent starkaste förvaltningarnas genomsnittliga resultattal närmare fyra. Den grupp som här benämns som normalfördelningen ligger generellt närmare de tio procent svagaste än de tio procent starkaste.

Not 36. Inom området *Säkerhetsåtgärder och förbättringsarbete* har de svagaste tio procenten av förvaltningarna ett högre resultattal än för övriga arbetsområden. Den huvudsakliga förklaringen till detta är dock att modellen enbart ställer krav på två åtgärder för att uppnå nivå 1.

Den största skillnaden mellan de bästa presterande förvaltningarna och den grupp som benämns som normalfördelningen finns inom arbetsområdet *Incident- och kontinuitetshantering*, följt av *Ledningens styrning och kontroll*.

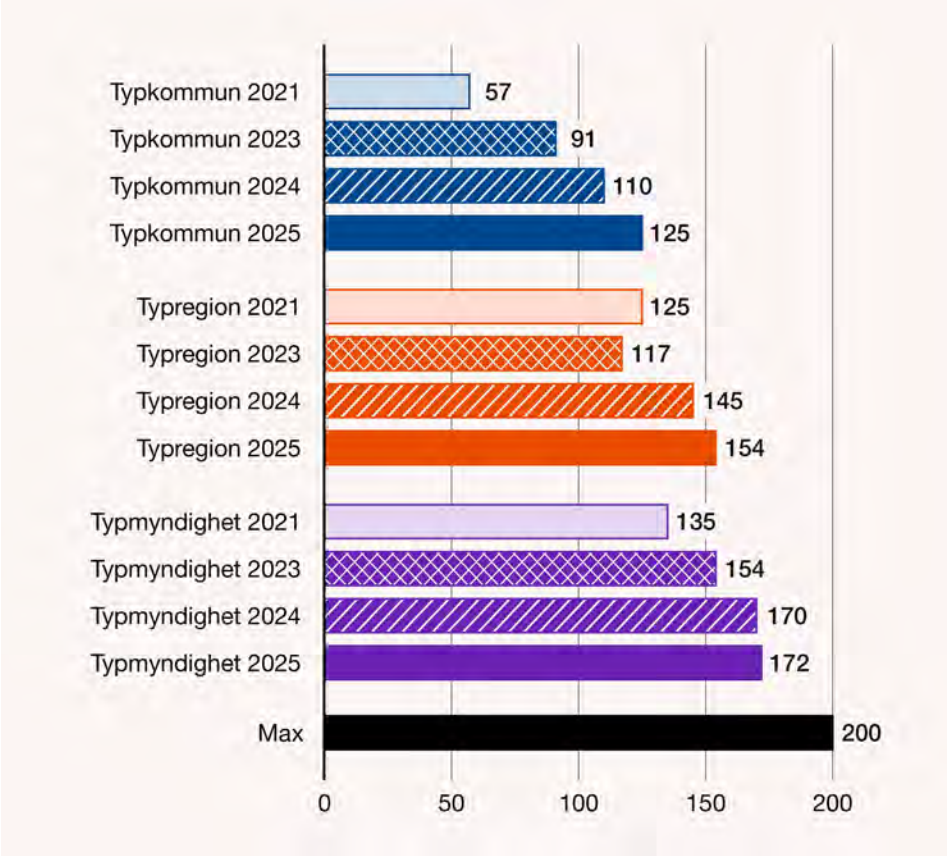
Även om det inte framgår av diagram 8 bör det uppmärksammas att resultatspridningen även är kraftig inom varje aktörsgrupp. I fråga om resultatet i Infosäkkollen i stort har myndigheterna den största resultatspridningen. Regionerna är den mest homogena aktörsgruppen.

4.2.8 Djupdykning i resultatet

Som konstateras i avsnitt 4.2.3. har det genomsnittliga resultattalet förbättrats för varje genomförande av Infosäkkollen. En jämförelse av den procentuella förändringen mellan mätningarna indikerar samtidigt att förbättringstakten har saktat in 2025.

Diagram 9 tydliggör de tre aktörsgruppernas resultatförbättringar mellan mätningarna från och med 2021 till 2025 genom att visa antalet åtgärder som typkommunen, typregionen och typmyndigheten har vidtagit vid samtliga fyra genomföranden av Infosäkkollen.

Infosäkkollen diagram 9. Totalt antal genomförda åtgärder hos typkommunen, typregionen och typmyndigheten år 2021, 2023, 2024 respektive 2025



Typkommunen är den aktörsgrupp som har förbättrat sig i störst utsträckning sedan det första genomförandet av Infosäkkollen, det vill säga 2021. Kommunerna är även den aktörsgrupp som förbättrat sitt resultat i störst utsträckning i fråga om antalet genomförda åtgärder jämfört med 2024 års mätning. Förbättringen mellan Infosäkkollen 2024 och 2025 motsvarar 15 fler åtgärder. Typkommunens resultatförbättring förklaras till stor del av deras i grunden svaga resultat och att det därmed finns fler åtgärder att vidta inom modellens grundläggande nivåer, jämfört med de två andra aktörsgrupperna.

Typregionen, som haft en mer ojämn utveckling[37], har förbättrat sitt resultat med nio åtgärder jämfört med mätningen 2024. Typmyndigheten uppvisar den svagaste utvecklingen i förhållande till Infosäkkollen 2024, med endast två fler åtgärder genomförda. Denna utveckling är betydligt lägre än förbättringen mellan 2023 och 2024.

Samtidigt som typkommunen uppvisar den starkaste utvecklingen är det noterbart att typkommunen fortfarande ligger långt efter de två övriga aktörsgrupperna. Typkommunens resultat 2025 motsvarar typregionens resultat från 2021. Vidare hade det krävts tio fler genomförda åtgärder för att typkommunens resultat skulle vara likvärdigt med typmyndighetens resultat år 2021.

Även om samtliga tre aktörsgrupper har förbättrat sitt resultat när det gäller antalet genomförda åtgärder mellan Infosäkkollen 2024 och 2025, har utvecklingen saktat in i förhållande till den förbättring som uppvisades mellan Infosäkkollen 2023 och 2024. Detta stärker sammantaget bilden av en stagnerande utvecklingstakt i fråga om det systematiska informationssäkerhetsarbetet.

Not 37. Att regionernas uppvisade ett svagare resultat 2023 jämfört med 2021 grundar sig i att en större population regioner deltog i Infosäkkollen 2023, jämfört med övriga mätningar. Flera av de svagare regionerna som deltog i Infosäkkollen i Infosäkkollen 2023 deltog heller inte i Infosäkkollen 2024 eller 2025.

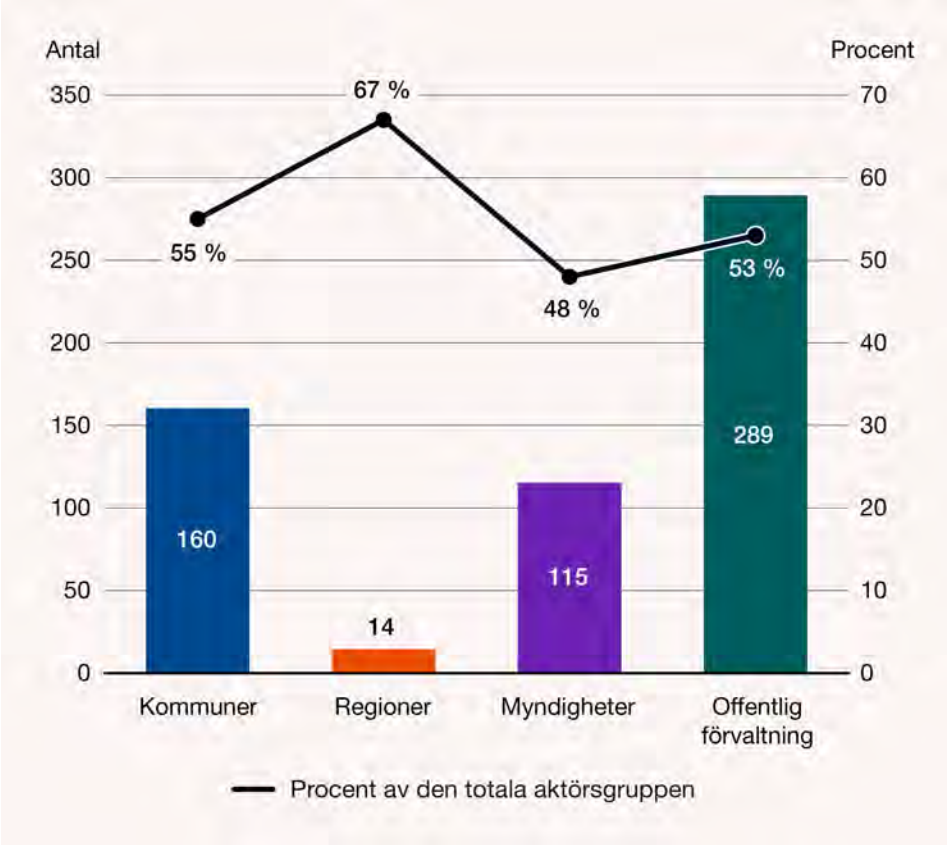
4.3 Resultat i It-säkkollen 2025

Det här avsnittet redogör för resultatet i It-säkkollen 2025. It-säkkollen följer upp nivån på det systematiska it-säkerhetsarbetet och genomförs för tredje gången. It-säkkollen 2025 genomförs dock för första gången enligt en struktur som liknar Infosäkkollens.[38] Syftet med It-säkkollen, liksom övriga mätningar, är att ge en samlad bild av hur arbetet med it-säkerhet bedrivs, identifiera styrkor och utvecklingsområden samt ge underlag för fortsatt förbättringsarbete.

4.3.1 Deltagande i It-säkkollen

Totalt har 289 organisationer i offentlig förvaltning deltagit i It-säkkollen 2025, vilket innebär att drygt hälften av Sveriges förvaltningar[39] har rapporterat sina resultat. Deltagande förvaltningar utgörs av 160 kommuner, 14 regioner och 115 myndigheter har deltagit.

It-säkkollen diagram 1. Deltagande i It-säkkollen 2025



Not 38. Utöver 2025, har It-säkkollen genomförts 2023 och 2024. Vid mätningarna 2023 och 2024 var dock It-säkkollen en enklare självskattningsenkät.

Not 39. Med Sveriges förvaltningar menas den rampopulation som specificeras i avsnitt 3.1.

I förhållande till sin aktörsgrupp har regionerna deltagit i störst utsträckning (67 procent), följt av kommunerna (55 procent) och slutligen myndigheter (48 procent) i It-säkkollen 2025. I fråga om faktiskt antal är dock deltagandet störst bland kommunerna.[40]

I jämförelse med It-säkkollen 2024 har deltagandet 2025 ökat med drygt ett trettiotal organisationer[41]. Ökningen förklaras i huvudsak av att fler kommuner har deltagit. Vidare har tre fler regioner och ytterligare en myndighet deltagit år 2025 i förhållande till It-säkkollen 2024.

4.3.2 Typförvaltningens resultat

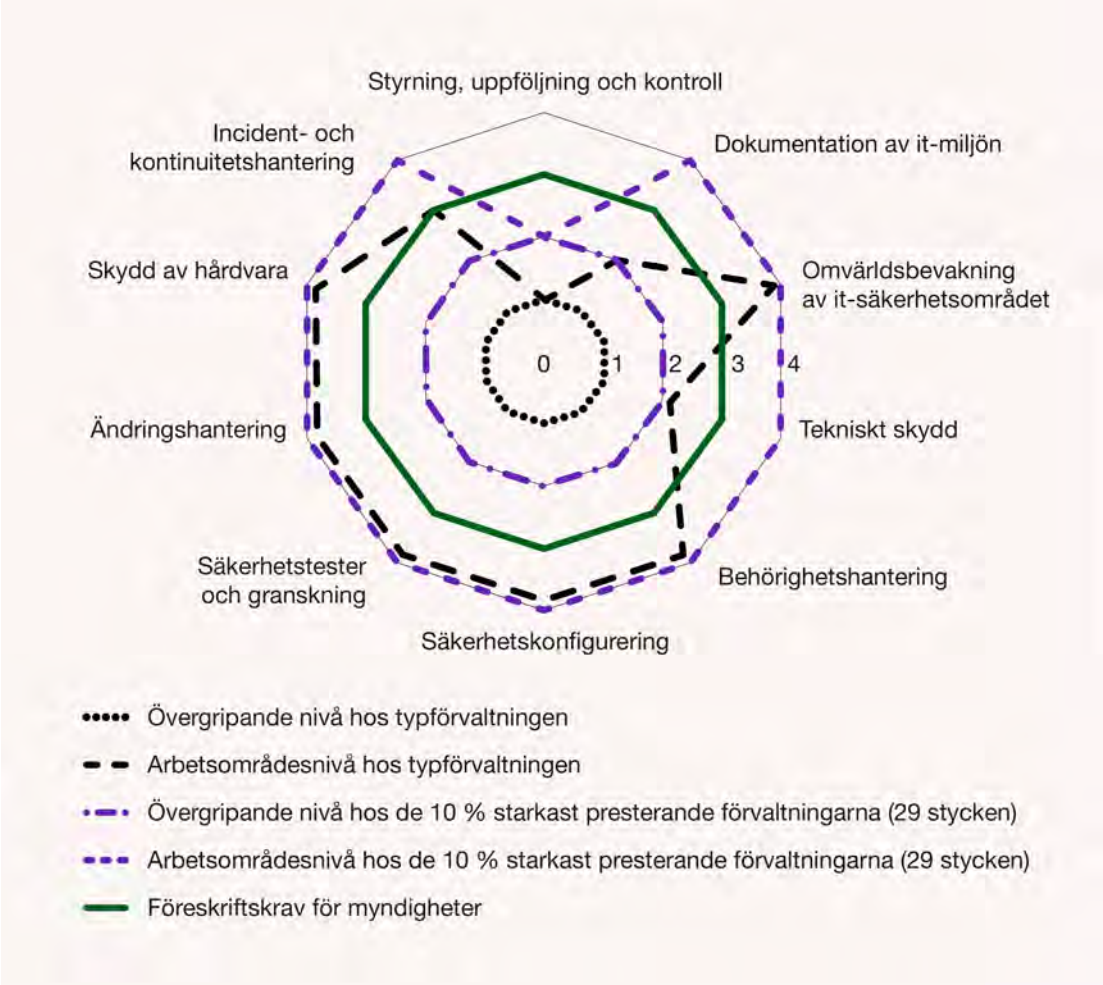
Diagram 2 illustrerar typförvaltningens övergripande nivå samt typförvaltningens uppnådda nivå inom respektive arbetsområde (se avsnitt 1.2) i It-säkkollen. Dessutom illustreras den övergripande nivån samt uppnådd nivå per arbetsområde hos de 10 procent starkast presterande förvaltningarna. Därtill illustreras It-säkkollens nivå 3 i diagrammet med en grön markering, vilken indikerar efterlevnad av myndighetens föreskrifter.[42]

Not 40. Vilken aktörsgrupp som har flest deltagare påverkar typförvaltningens resultat och resultatet för offentlig förvaltning i stort.

Not 41. Totalt deltog 256 organisationer i offentlig förvaltning i It-säkkollen 2024.

Not 42. Myndighetens föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7).

It-säkkollen diagram 2. Resultat i It-säkkollen för typförvaltningen och typförvaltningen bland de tio procent starkast presterande förvaltningarna



Typförvaltningen har uppnått övergripande nivå 1 i It-säkkollen 2025, vilket betyder att grunderna i ett systematiskt it-säkerhetsarbete på plats. Endast ett arbetsområde, nämligen *Styrning, uppföljning och kontroll*, drar ner typförvaltningens övergripande nivå till nivå 1. Det finns således goda förutsättningar att typförvaltningen ska nå övergripande nivå 2 till nästa mätning förutsatt att förvaltningarna prioriterar att förbättra resultatet inom detta område. *Tekniskt skydd* och *Dokumentation av it-miljön* är de näst svagaste arbetsområdena, inom vilka typförvaltningen har uppnått nivå 2. För att nå nivå 3 i It-säkkollen behöver typförvaltningen således även prioritera att vidta åtgärder inom dessa två arbetsområden.

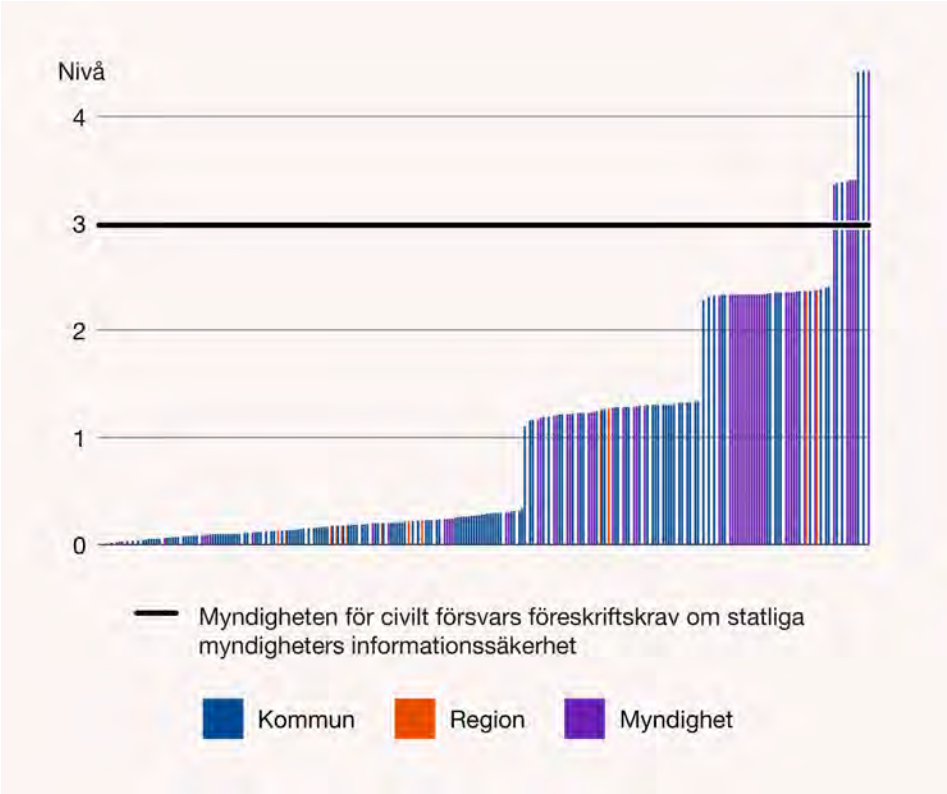
Inom hela sju arbetsområden har typförvaltningen uppnått nivå 3 eller högre. Det innebär att typförvaltningen har grunderna på plats, använder sina arbetssätt i tillräcklig utsträckning och har ett kvalificerat innehåll i sitt it-säkerhetsarbete. Att nå nivå 3 indikerar även föreskriftsefterlevnad. Inom sex av dessa arbetsområden, nämligen *Skydd av hårdvara, Ändringshantering, Säkerhetstester och granskning, Säkerhetskonfigurering, Behörighetshantering,* samt *Omvärldsbevakning av it-säkerhetsområdet*, har typförvaltningen uppnått den högsta möjliga nivån i modellen.

Diagram 2 visar också att typförvaltningen bland de 10 procent starkast presterande förvaltningarna har uppnått övergripande nivå 2. Det framgår vidare att det endast är ett arbetsområde, nämligen *Styrning, uppföljning och kontroll*, som hindrar denna grupp från att nå nivå 3 i It-säkkollen 2025. Även för de starkast presterande förvaltningarna finns det således goda förutsättningar att höja det övergripande resultatet till nästa mätning.

4.3.3 Spridning av resultattal

Diagram 3 syftar inte till att redovisa exakta data, utan till att ge en överblick över resultattalet (se avsnitt 1.2) hos samtliga deltagande förvaltningar och därmed illustrera spridningen i resultaten.

It-säkkollen diagram 3. Resultattal hos de 289 förvaltningar som deltog i It-säkkollen 2025



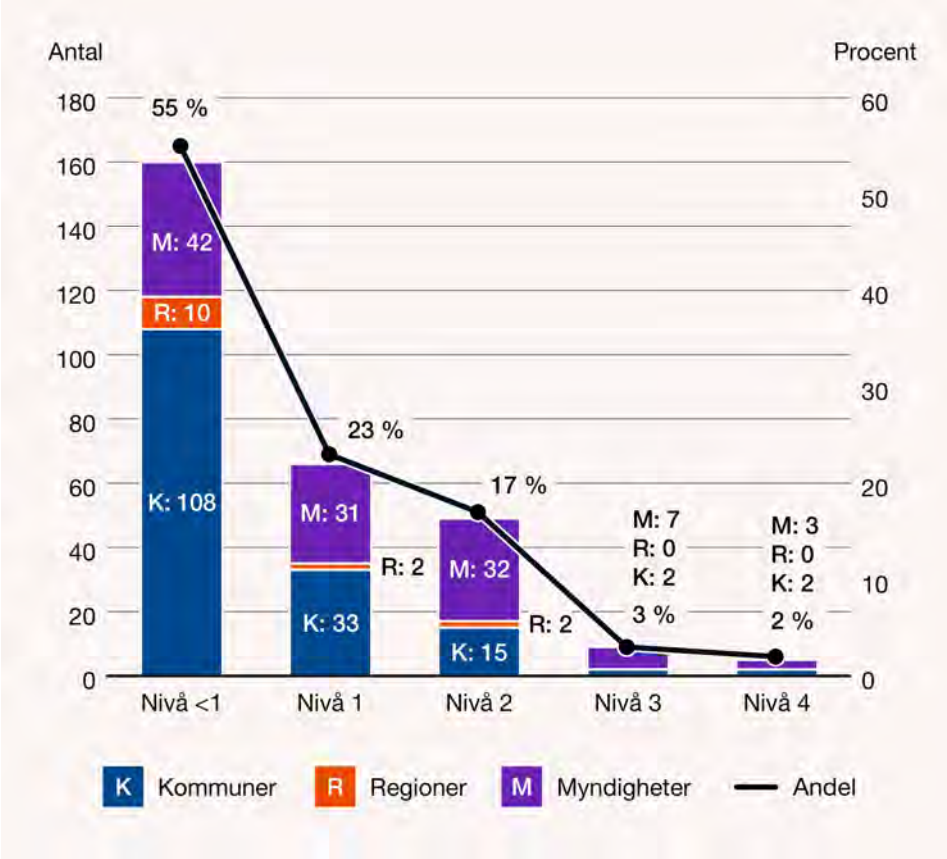
Den svarta linjen i diagrammet motsvarar den nivå som Myndigheten för civilt försvar har definierat som en indikation över huruvida en organisation uppfyller myndighetens föreskriftskrav på it-säkerhetsområdet.

Diagram 3 synliggör en stor resultatspridning bland de deltagande organisationerna. Resultatspridningen är även stor inom aktörsgrupperna. Hos de deltagande förvaltningarna är det genomsnittliga resultattalet 0,95. Baserat på det genomsnittliga resultattalet är myndigheterna den aktörsgrupp som presterar starkast (1,36). Kommunernas respektive regionernas genomsnittliga resultattal är likvärdigt (0,64 respektive 0,68). Som konstateras i avsnitt 4.3.6 presterar dock regionerna något bättre än kommunerna i fråga om antalet genomförda åtgärder.

4.3.4 Fördelning av övergripande nivå

Diagram 4 illustrerar fördelningen gällande övergripande nivå bland deltagande organisationer, det vill säga andelen som inte uppnått nivå 1 alternativt har nått upp till någon av modellens fyra nivåer. Nivå 1 motsvarar att en organisation har grunderna i sitt it-säkerhetsarbete på plats.

It-säkkollen diagram 4. Fördelning av övergripande nivå hos deltagande förvaltningar



Över hälften, 55 procent av deltagarna, uppnår inte övergripande nivå 1 i It-säkkollen och saknar därmed grunderna i ett systematiskt it-säkerhetsarbete. 23 procent av deltagarna når upp till nivå 1 och 17 procent når upp till nivå 2. Endast fem procent når upp till nivå 3 eller bättre.

Vidare konstateras att 95 procent inte når upp till nivå 3 i modellen. Nivå 3 indikerar att en organisation lever upp till föreskriftskraven på it-säkerhetsområdet. Endast sex procent av myndigheterna, motsvarande sju organisationer, uppnår nivå 3 eller bättre. Föreskriftskraven för statliga myndigheter har funnits i över femton år.

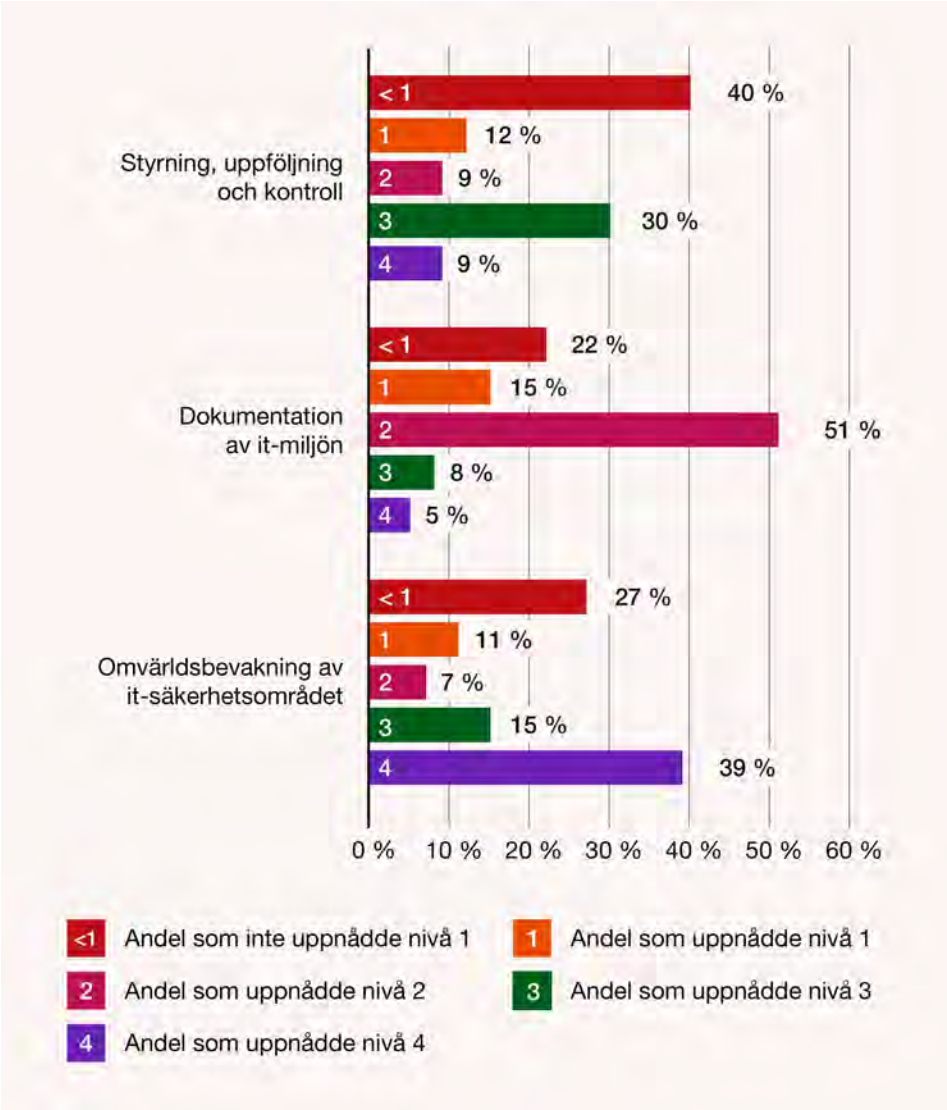
Nästan 40 procent av kommunerna uppnår inte nivå 1 eller högre. Motsvarande siffra hos regionerna är 47 procent, och hos myndigheterna är det 15 procent. Det går således att konstatera att myndigheter är den aktörsgrupp som presterar bäst när det gäller att ha grunderna i ett systematiskt it-säkerhetsarbete på plats.

Vilka åtgärder som typkommunen, typregionen och typmyndigheten hade behövt vidta för att höja sin övergripande nivå redovisas i avsnitt 2.4.

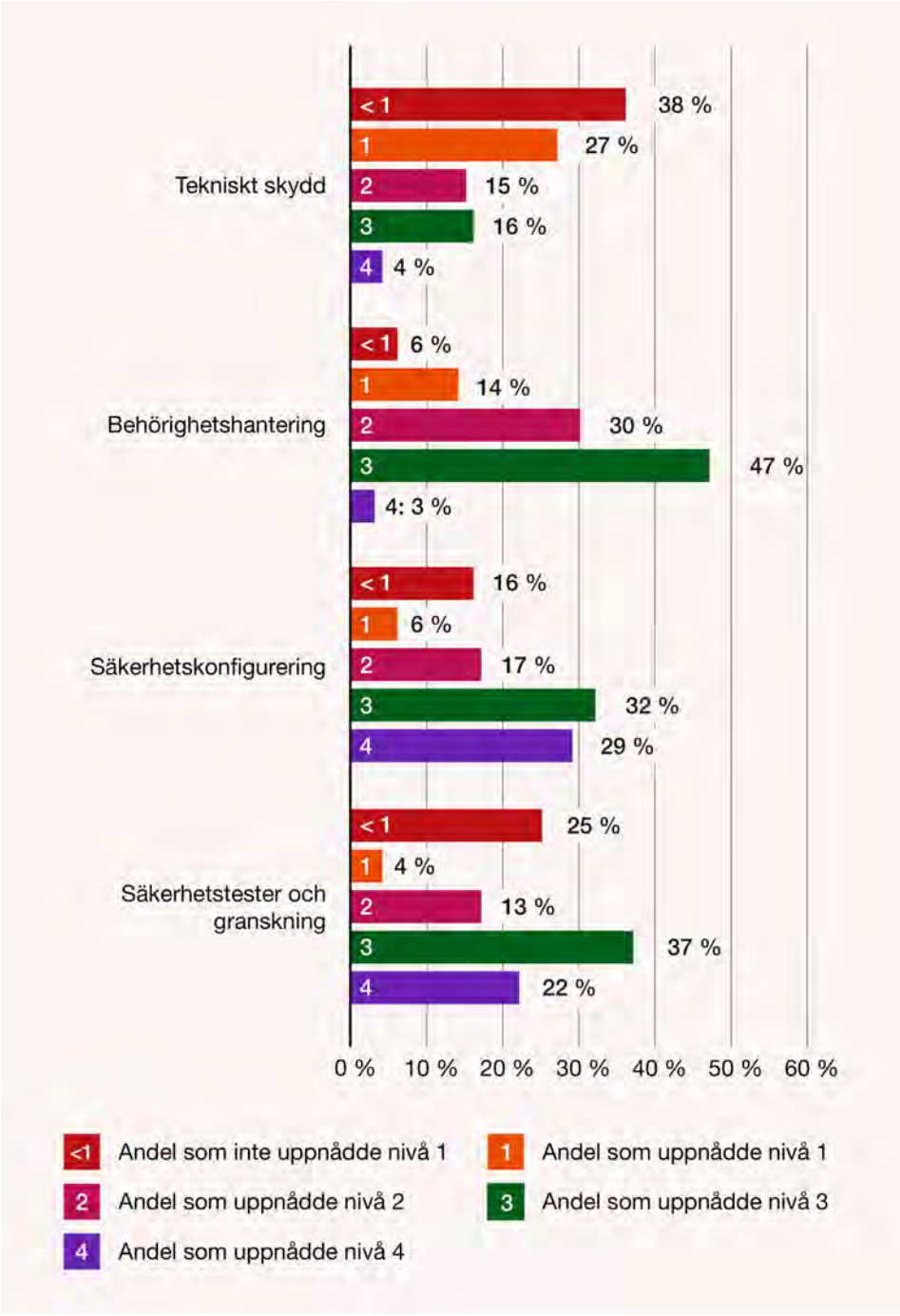
4.3.5 Fördelning av nivå per arbetsområde

Diagram 5 visar fördelningen av uppnådd nivå per arbetsområde inom It-säkkollen. Utifrån diagrammet kan det också konstateras att deltagande organisationers prestation inom de enskilda arbetsområdena varierar. Mätningarna inom Cybersäkerhetskollen syftar till att mäta systematik i säkerhetsarbetet och premierar därför helhet. Modellen ställer därför krav på att man har nått en viss nivå, exempelvis nivå 1, inom samtliga arbetsområden för att man också ska nå nivå 1 som övergripande nivå.

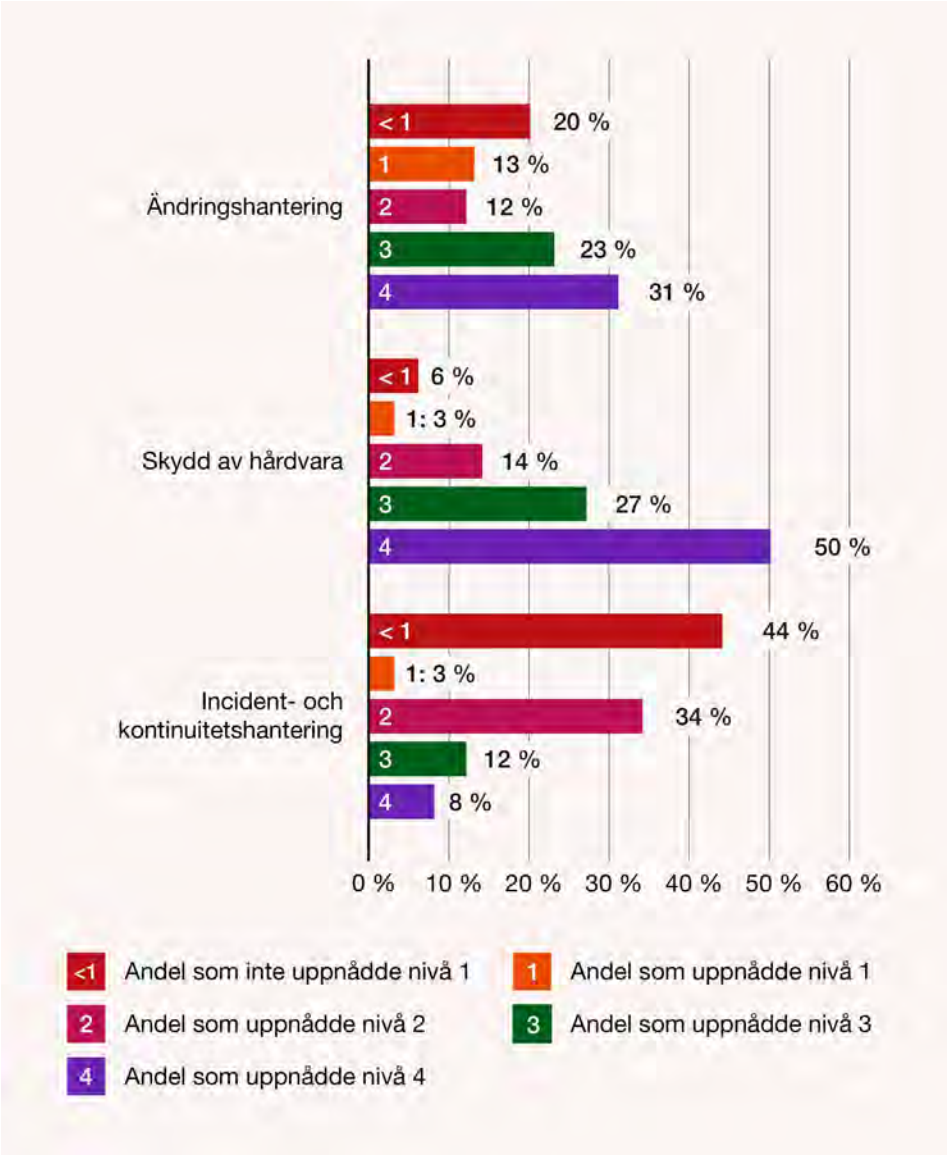
It-säkkollen diagram 5. Fördelning av nivå per arbetsområde hos deltagande förvaltningar



It-säkkollen diagram 5 fortsättning. Fördelning av nivå per arbetsområde hos deltagande förvaltningar



It-säkkollen diagram 5 fortsättning. Fördelning av nivå per arbetsområde hos deltagande förvaltningar



De arbetsområden där den största andelen organisationer når nivå 1 eller högre är *Behörighetshantering* (94 procent), *Skydd av hårdvara* (94 procent) och *Säkerhetskonfigurering* (84 procent). De arbetsområden där den högsta andelen har nått nivå 3 eller högre är *Skydd av hårdvara* (77 procent), *Säkerhetskonfigurering* (61 procent), samt *Säkerhetstester och granskning* (59 procent).

Utifrån diagram 5 kan det även konstateras att de arbetsområden där den minsta andelen organisationer har nått nivå 1 eller högre är *Incident- och kontinuitetshantering* (44 procent), *Styrning, uppföljning och kontroll* (40 procent) samt *Tekniskt skydd* (38 procent). *Incident- och kontinuitetshantering* är således det arbetsområde där den högsta andelen organisationer har grundläggande brister i sitt it-säkerhetsarbete.

Diagram 5 synliggör inte vilken nivå som de enskilda aktörsgrupperna har uppnått. Det bör dock uppmärksammas att fördelningen av nivå per arbetsområde skiljer sig på aktörsgruppsnivå. Med undantag för två arbetsområden, *Behörighetshantering* och *Ändringshantering*, finns den största andelen organisationer som uppnått nivå 1 eller högre hos myndigheterna. Hos kommunerna och regionerna är andelen som har uppnått nivå 1 eller högre inom de tio arbetsområdena relativt snarlik. Inom vissa arbetsområden har fler kommuner nått nivå 1 eller högre jämfört med regionerna, och i andra arbetsområden är förhållandet det motsatta.

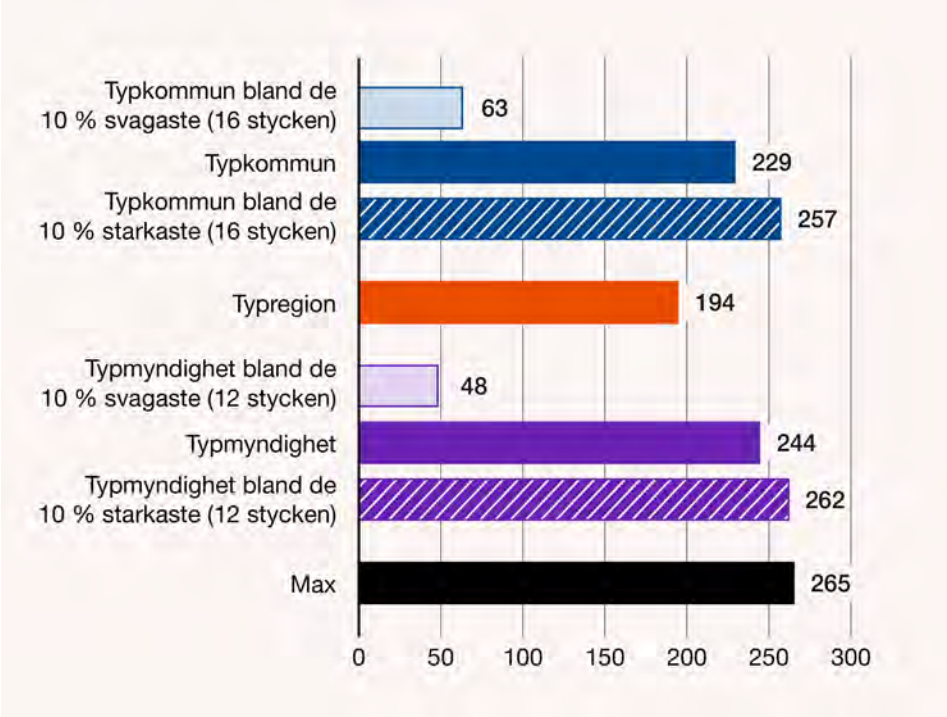
Den största skillnaden mellan hur olika aktörsgrupper har presterat återfinns inom arbetsområdet *Styrning, uppföljning och kontroll*. Inom detta arbetsområde har 75 procent av myndigheterna uppnått nivå 1 eller högre. Motsvarande siffra hos kommunerna och regionerna är 52 procent respektive 36 procent.

4.3.6 Antal genomförda åtgärder hos typaktören

Totalt antal möjliga åtgärder att vidta i It-säkkollen är 265 stycken. Diagram 6–7 redogör för det totala antalet åtgärder som aktörsgrupperna har genomfört samt antalet åtgärder som aktörsgrupperna infört inom varje enskilt arbetsområde. Det bör samtidigt understrykas att diagrammen inte synliggör huruvida de åtgärder som vidtagits avser mer grundläggande åtgärder eller åtgärder som undersöks inom It-säkkollens högre nivåer.

Diagram 6 redogör för antalet vidtagna åtgärder hos typkommunen, typregionen och typmyndigheten samt antalet genomförda åtgärder hos typmyndigheten och typkommunen hos de tio procent starkaste respektive tio procent svagaste typkommunerna och typmyndigheterna.

It-säkkollen diagram 6. Totalt antal genomförda åtgärder hos typkommunen, typregionen och typmyndigheten, samt de 10 procent svagast presterande respektive starkast presterande kommunerna och myndigheterna[43]



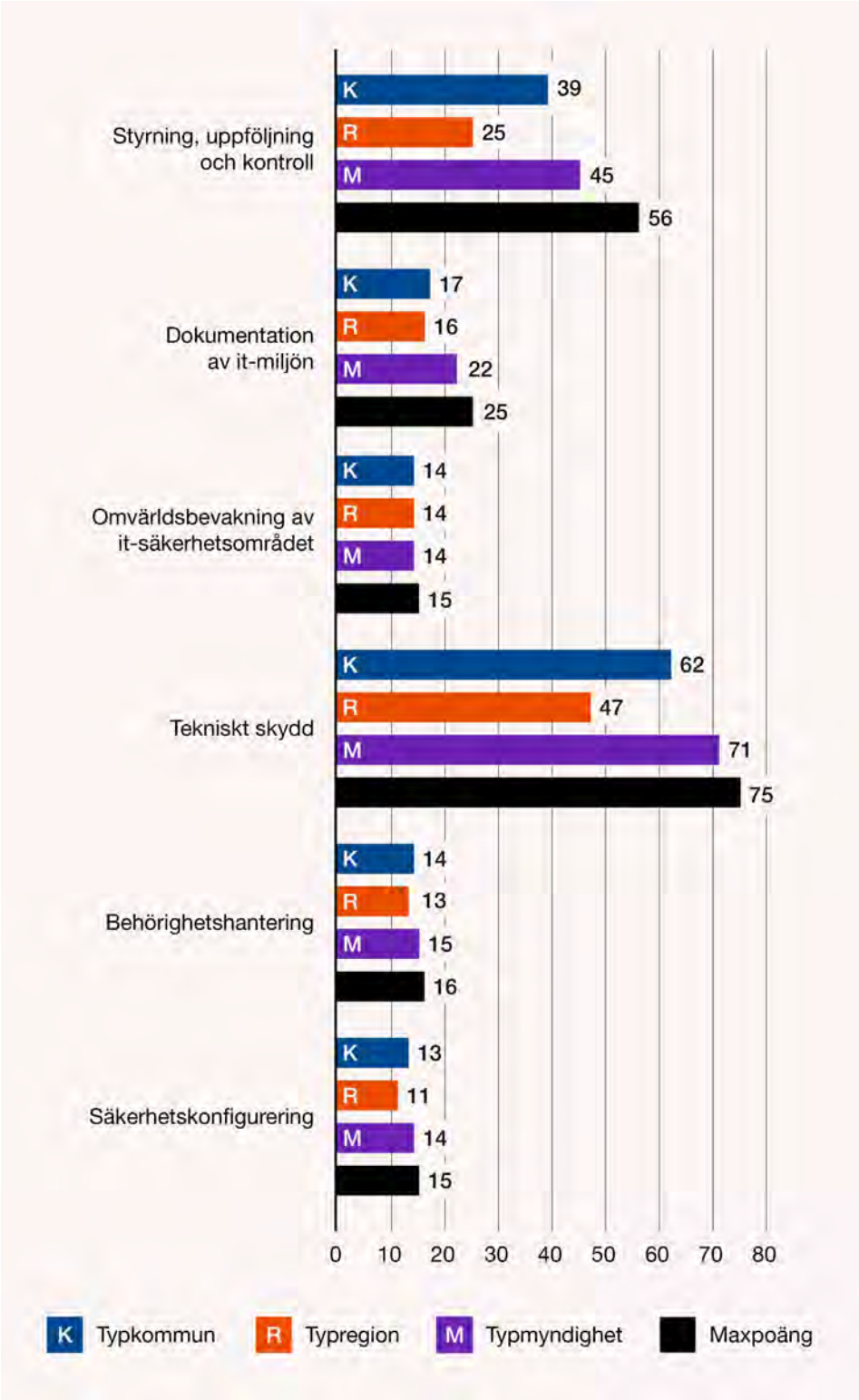
Av diagram 6 framgår att typmyndigheten har vidtagit flest antal åtgärder (244 stycken), följt av typkommunen (229 stycken). Typregionen har genomfört minst antal åtgärder (194 stycken). Det skiljer således ett vidtagande om 50 åtgärder mellan den starkaste presenterande aktörsgruppen, det vill säga typmyndigheten, och den svagaste presterande aktörsgruppen, det vill säga typregionen.

Typmyndigheten hos de tio procent starkast presterande myndigheterna har vidtagit 262 åtgärder och är därmed endast tre åtgärder ifrån att ha vidtagit samtliga åtgärder som mäts inom ramen för It-säkkollen. Typkommunen hos de tio procent starkaste kommunerna har vidtagit 257 åtgärder och behöver således endast införa 8 ytterligare åtgärder för att ha vidtagit samtliga åtgärder.

Även om typmyndigheten har vidtagit fler åtgärder än typkommunen har dock typkommunen bland de tio procent svagaste kommunerna vidtagit fler åtgärder än motsvarande aktörsgrupp hos myndigheterna. Detta visar på en större resultatspridning hos myndigheterna än kommunerna.

Not 43. Regionerna är en för liten aktörsgrupp för att det ska vara fruktsamt att ta fram resultat för de tio procent starkaste regionerna.

It-säkkollen diagram 7. Antal genomförda åtgärder per arbetsområde hos typkommunen, typregionen och typmyndigheten



It-säkkollen diagram 7 fortsättning. Antal genomförda åtgärder per arbetsområde hos typkommunen, typregionen och typmyndigheten

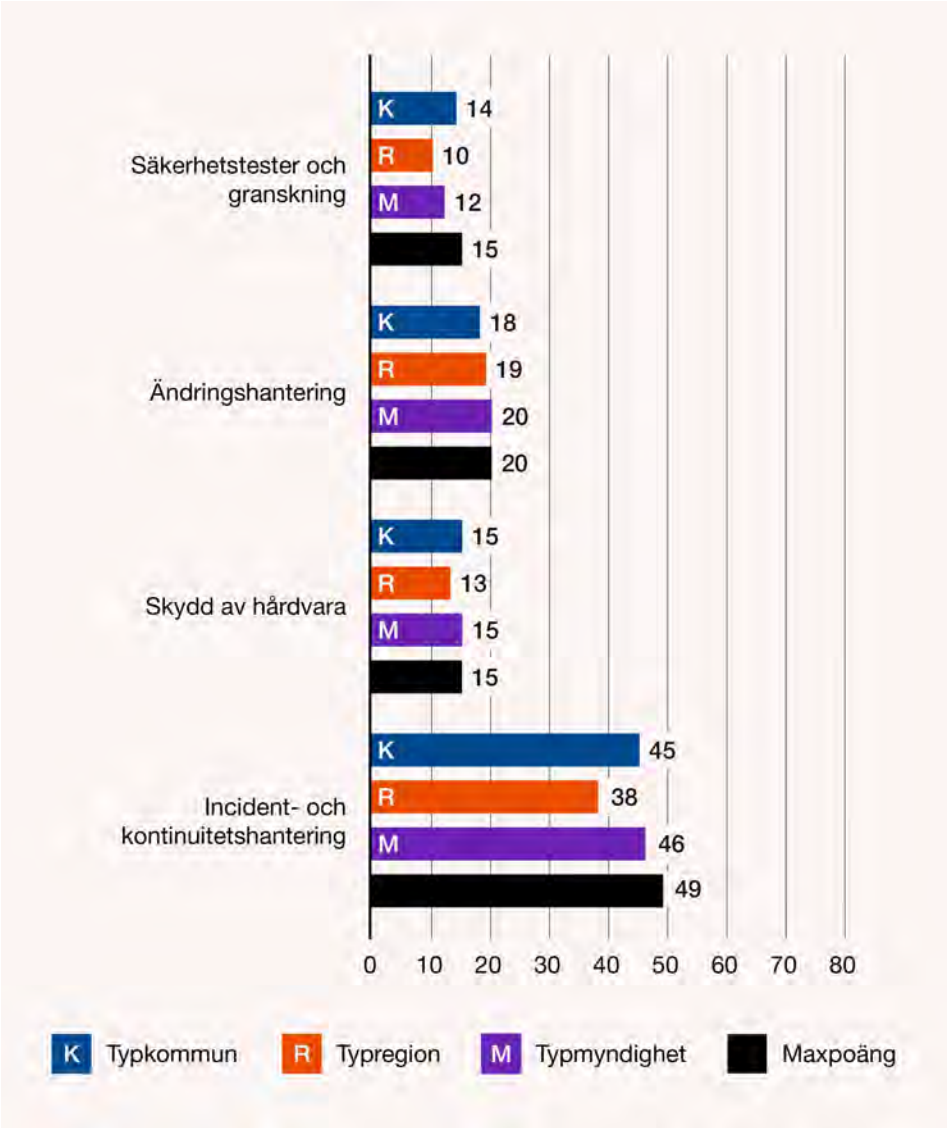


Diagram 7 ger en mer detaljerad bild över antalet vidtagna åtgärder genom att visa hur många åtgärder som aktörsgrupperna har genomfört inom varje arbetsområde. Av diagrammet framgår att typaktörerna har genomfört relativt många åtgärder i förhållande till vad som är möjligt inom flera arbetsområden. Att de trots detta inte når en högre övergripande nivå i It-säkkollen än nivå 1 betyder att de behöver tillämpa sina beslutade arbetssätt i högre utsträckning.

Ändringshantering, *Omvärldsbevakning av it-säkerhetsområdet*, *Skydd av hårdvara* är arbetsområden där samtliga tre aktörsgrupper har vidtagit flest åtgärder (i genomsnitt över 90 procent av åtgärderna). Av diagrammet framgår även att typmyndigheten och typkommunen har vidtagit över 90 procent av de åtgärder som undersöks inom arbetsområdet *Incident- och kontinuitetshantering*.

Styrning, uppföljning och kontroll samt *Dokumentation av it-miljön* är de arbetsområden som samtliga tre aktörsgrupper har minst andel vidtagna åtgärder inom (i genomsnitt 65 respektive 73 procent). Det är noterbart att typregionen enbart har vidtagit 45 procent av de åtgärder som undersöks inom *Styrning, uppföljning och kontroll*.

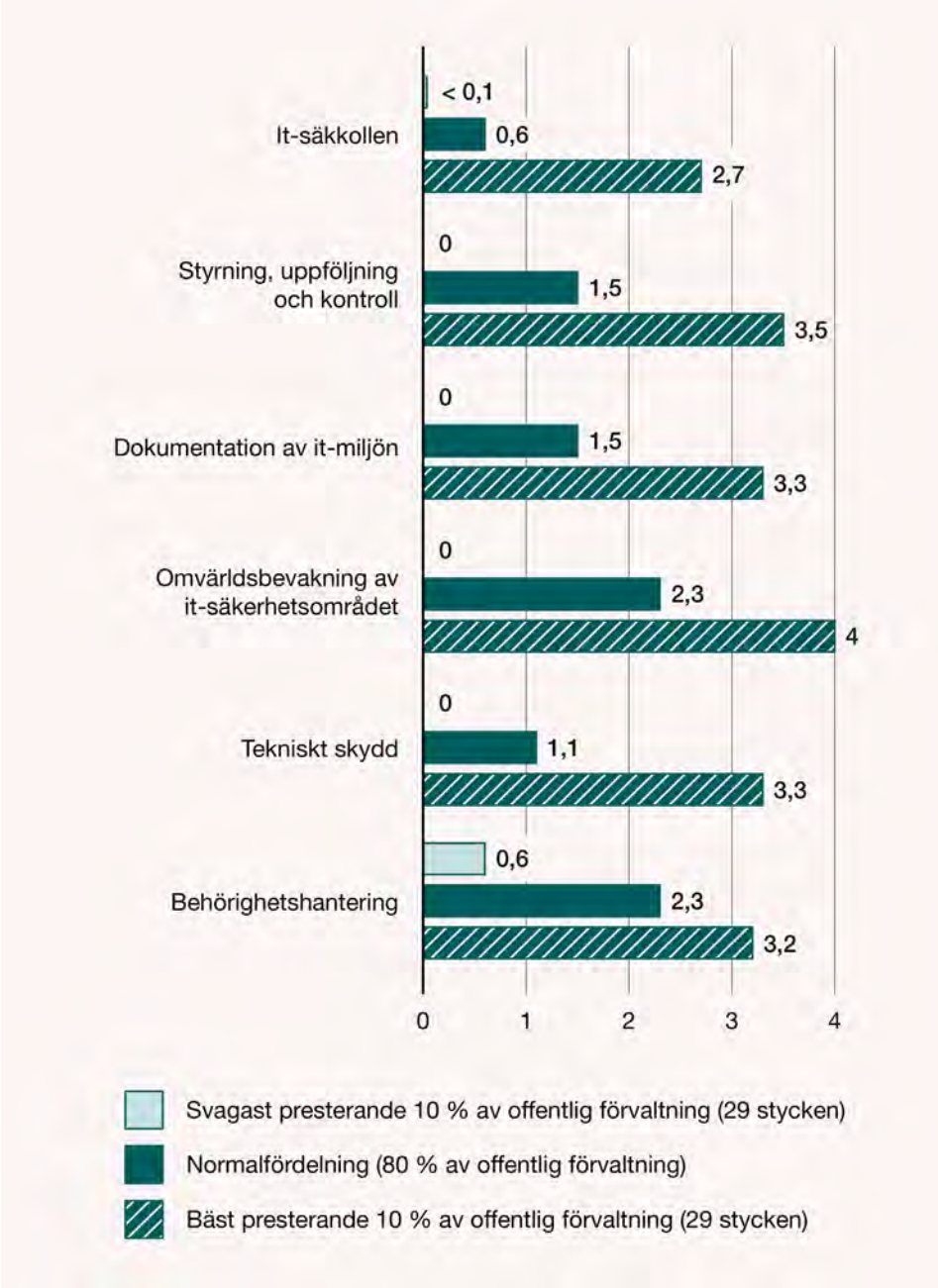
Av diagram 7 går vidare att konstatera att typmyndigheten har vidtagit flest åtgärder av de tre aktörsgrupperna inom alla arbetsområden förutom *Säkerhetstester och granskning*. Med undantag för ett arbetsområde, *Ändringshantering*, har typkommunen vidtagit lika många eller fler åtgärder än typregionen. Typregionen är således den aktörsgrupp som generellt presterar svagast i It-säkkollen.

Utifrån mängden genomförda åtgärder inom de enskilda arbetsområdena liksom It-säkkollen i stort kan det utläsas att de allra flesta organisationer, med bara några nya åtgärder införda till nästa mätning, har goda förutsättningar att höja sin övergripande nivå till nästa mätning. Antingen behöver de införa några grundläggande åtgärder till, alternativt använda sina beslutade arbetssätt i en högre utsträckning för att kunna klättra i modellen.

4.3.7 Resultatspridning

Diagram 8 visar det genomsnittliga resultattalet (se avsnitt 1.2) mellan normalfördelningsgruppen samt de svagaste respektive starkast presterande förvaltningarna i syfte att tydliggöra resultatspridningen. Normalfördelningen ses i detta sammanhang som de 80 procent som varken hör till de svagaste eller bäst presterande förvaltningarna.

It-säkkollen diagram 8. Resultatspridning hos deltagande förvaltningar



It-säkkollen diagram 8 fortsättning. Resultatspridning hos deltagande förvaltningar

Diagram 8 bekräftar den stora resultatspridningen som även tidigare noterats. De tio procent starkaste förvaltningarnas genomsnittliga resultattal är tre eller högre inom samtliga arbetsområden. Denna grupp har ett noterbart starkare resultat än normalfördelningsgruppen, vars genomsnittliga resultattal inom arbetsområdena ligger på 0,6. Gruppen som utgörs av de svagaste tio procenten har ett genomsnittligt resultattal på noll inom fyra arbetsområden samt på It-säkkollen i stort.

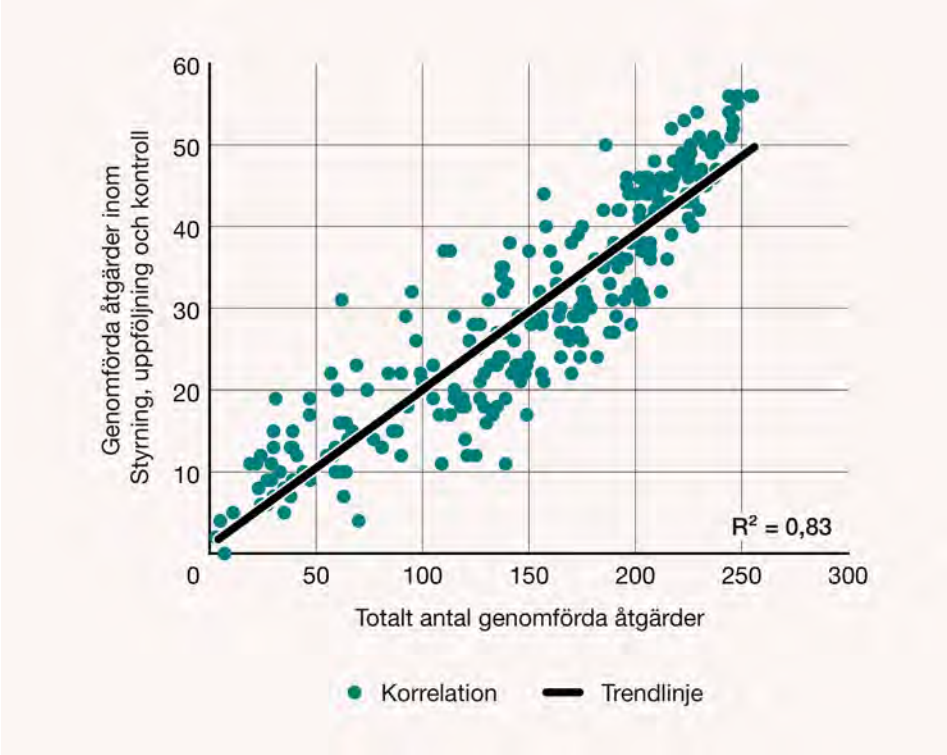
Skillnaden mellan gruppen om de bäst presterande förvaltningarna och gruppen som utgör normalfördelningen är störst inom arbetsområdet *Tekniskt skydd*. Den minsta resultatspridningen finns inom arbetsområdet *Skydd av hårdvara*.

Även om det inte framgår av diagram 8 bör det också uppmärksammas att resultatspridningen även är kraftig inom varje aktörsgrupp. I fråga om resultatet i Infosäkkollen i stort är regionerna den mest homogena aktörsgruppen. Resultatspridningen mellan kommunerna och regionerna är likvärdig.

4.3.8 Djupdykning i It-säkkollen

Avsnitt 4.3.5 konstaterar att arbetsområdena *Styrning, uppföljning och kontroll*, *Tekniskt skydd* samt *Incident- och kontinuitetshantering* är de tre arbetsområden där den minsta andelen organisationer har nått nivå 1 eller högre. Samtidigt är dessa även de tre arbetsområden med den starkaste korrelationen (det vill säga sambandet) mellan genomförda åtgärder inom arbetsområdet och totalt antal genomförda åtgärder i hela It-säkkollen.[44] Diagram 9, 10 och 11 synliggör denna korrelation[45].

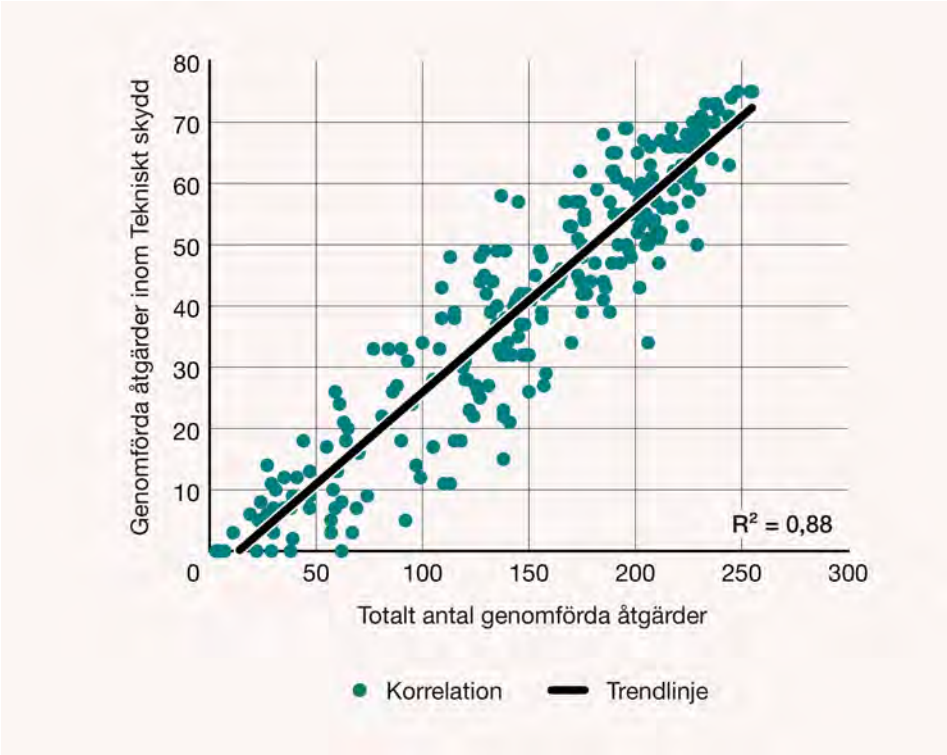
It-säkkollen diagram 9. Korrelation mellan totalt genomförda åtgärder inom *Styrning, uppföljning och kontroll* och totalt antal genomförda åtgärder i It-säkkollen



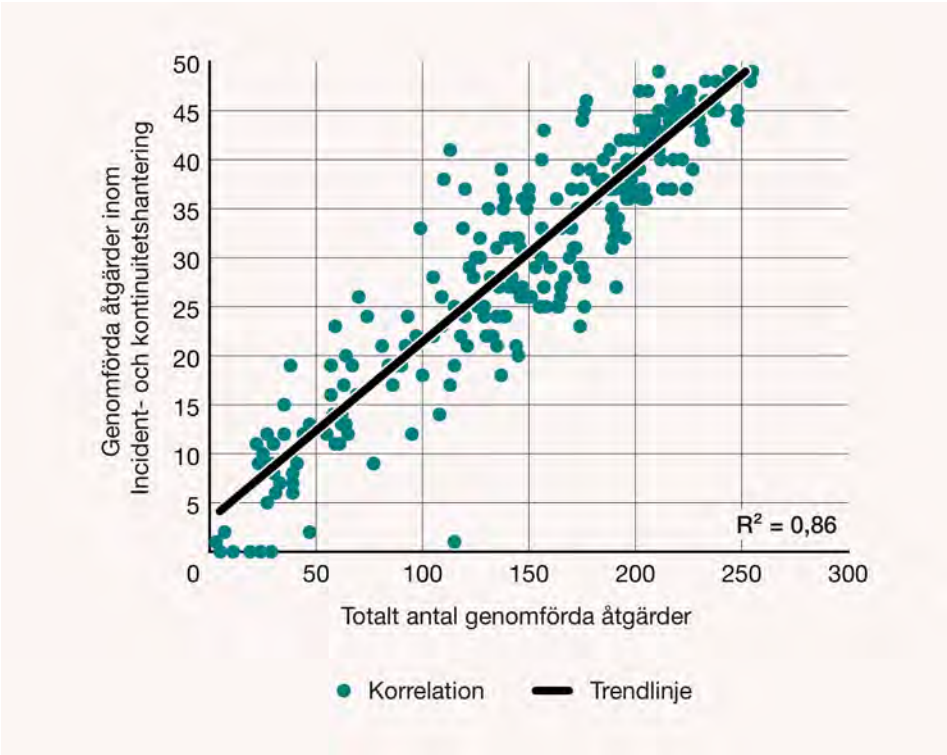
Not 44. Inom övriga sju arbetsområden varierar korrelationen mellan 0,6 och 0,74.

Not 45. Korrelationskoefficienten (R^2) har ett värde mellan 1 och -1. 1 anger maximalt positivt samband och -1 anger maximalt negativt samband.

It-säkkollen diagram 10. Korrelation mellan totalt genomförda åtgärder inom *Tekniskt skydd* och totalt antal genomförda åtgärder i It-säkkollen



It-säkkollen diagram 11. Korrelation mellan totalt genomförda åtgärder inom *Incident- och kontinuitetshantering* och totalt antal genomförda åtgärder i It-säkkollen



Diagrammen ovan påvisar en stark korrelation mellan resultatet inom respektive arbetsområde och resultatet i It-säkkollen i stort. Den starkaste korrelationen mellan genomförda åtgärder inom arbetsområdet i förhållande till totalt genomförda åtgärder i mätningen finns inom *Tekniskt skydd,* följt av *Incident- och kontinuitetshantering.* Den tredje starkaste korrelationen finns för arbetsområdet *Styrning, uppföljning och kontroll.*

Även om korrelation inte nödvändigtvis är samma sak som kausalitet är det rimligt att anta att systematiskt arbete inom incident- och kontinuitetshantering samt tekniskt skydd är värdefullt även för andra arbetsområden inom av it-säkerhetsarbetet. Likaså bör åtgärder inriktade på styrning, uppföljning och kontroll av it-säkerhetsarbetet skapa positiva effekter för it-säkerhetsarbetet i stort.

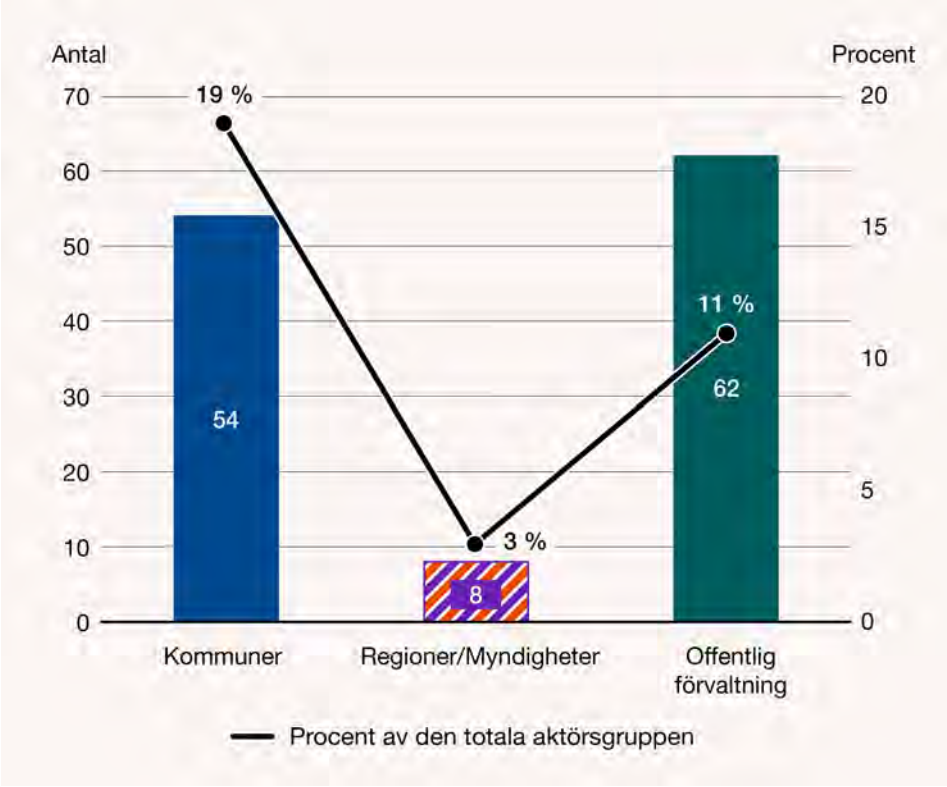
4.4 Resultat i Ot-säkkollen 2025

Det här avsnittet redogör för resultatet i Ot-säkkollen 2025. Ot-säkkollen följer upp nivån på det systematiska ot-säkerhetsarbetet och genomförs för första gången. Syftet med resultatredovisningen är att ge en samlad bild av hur arbetet med ot-säkerhet bedrivs, identifiera styrkor och utvecklingsområden samt ge underlag för fortsatt förbättringsarbete.

4.4.1 Deltagande i Ot-säkkollen

Totalt har 62 organisationer i offentlig förvaltning deltagit i Ot-säkkollen 2025. Deltagandet motsvarar elva procent av Sveriges förvaltningar.[46] Den stora majoriteten av deltagarna utgörs av kommuner (87 procent), vilket medför att antalet regioner och myndigheter som deltagit är allt för få för att Myndigheten för civilt försvar ska kunna dra några statistiskt säkra slutsatser för dessa enskilda aktörsgrupper. Följaktligen presenteras resultat enbart för kommuner och för den samlade gruppen offentlig förvaltning, bestående av representanter från alla tre aktörsgrupper.

Ot-säkkollen diagram 1. Deltagande i Ot-säkkollen 2025



Deltagandet i Ot-säkkollen är lågt i förhållande till deltagandet i övriga mätningar inom ramen för Cybersäkerhetskollen 2025. En förklaring är att ot-lösningar används mer frekvent av bolag än offentliga förvaltningar. Exempel på sådana verksamheter är energi- och transportföretag eller vattenreningsverk.

Not 46. Med Sveriges förvaltningar menas den rampopulation som specificeras i avsnitt 3.1.

En ytterligare förklaring till det låga deltagandet är att Ot-säkkollen genomfördes för första gången 2025 och Myndigheten för civilt försvar har fått återkoppling om att flera organisationer inte var medvetna om att Ot-säkkollen skulle ingå i 2025 års mätning och därför inte hade avsatt tid eller resurser för att kunna besvara frågorna.

Eftersom svarsgruppen för Ot-säkkollen är så pass liten i förhållande till antalet samhällsviktiga verksamheter som bedriver ot-säkerhetsarbete går det inte att dra alltför långtgående slutsatser. Resultaten bör därför främst ses som en indikation på nuläget.

4.4.2 Typförvaltningens resultat

Diagram 2 illustrerar övergripande nivå samt uppnådd nivå per arbetsområde hos typförvaltningen (se avsnitt 1.2) i Ot-säkkollen. Motsvarande visas även för de tio procent starkast presterande förvaltningarna. Kvalificerat innehåll, nivå 3, indikeras i diagrammet med en grön markering. Nivå 3 uppnås av organisationer som har beslutade arbetssätt (nivå 1) som de använder i tillräcklig utsträckning (nivå 2) och som dessutom har ett kvalificerat innehåll i sina arbetssätt (nivå 3).

Ot-säkkollen diagram 2. Resultat i Ot-säkkollen för typförvaltningen och typförvaltningen bland de tio procent starkast presterande förvaltningarna

Typförvaltningen har inte uppnått övergripande nivå 1 i Ot-säkkollen. Detta betyder att typförvaltningen brister i de grundläggande delarna av ot-säkerhetsarbetet. Den låga nivån hos typförvaltningen beror på att deltagande förvaltningar är svaga inom fem av sju arbetsområden, nämligen *Organisation och ledningssystem*, *Uppföljning och utvärdering*, *Incident- och kontinuitetshantering*, *Åtkomstkontroll och skydd av information* samt *Komponentsäkerhet*. Brister i dessa områden påvisar att grundläggande arbetssätt saknas och flera åtgärder behöver införas för att fler ska uppnå nivå 1.

Inom två arbetsområden har typförvaltningen nått nivå 1, nämligen inom *Konfigurationshantering* samt *Nätverk och säkra kommunikationer*. Det innebär att typförvaltningen har grunderna på plats inom dessa områden, åtminstone i begränsad utsträckning.

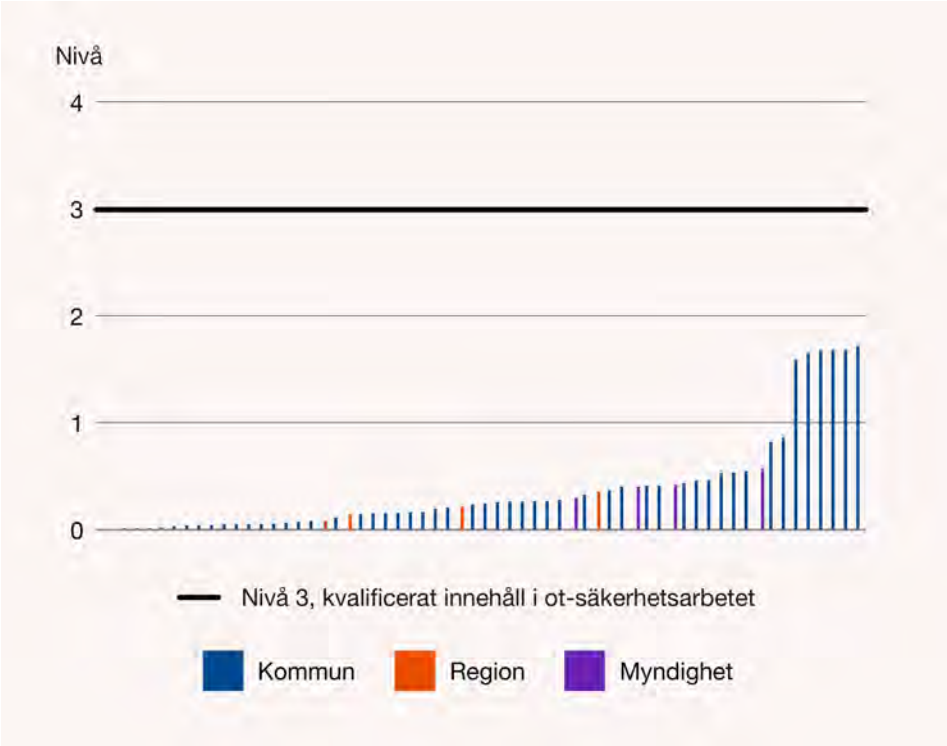
Diagram 2 visar också att typförvaltningen hos de tio procent starkast presterande förvaltningarna utmärker sig genom att nå övergripande nivå 1 i samtliga sju arbetsområden, medan typförvaltningen som konstaterats endast når nivå 1 på två utav sju arbetsområden. Inom fyra arbetsområden har typförvaltningen hos de tio procent starkast presterande organisationerna nått nivå tre eller bättre, vilket visar på att det också finns kvalificerat innehåll i arbetssätten (*Konfigurationshantering, Nätverk och säkra kommunikationer, Uppföljning och utvärdering*) och att man genomför ständiga förbättringar (*Åtkomstkontroll och skydd av information*).

Resultatet indikerar sammantaget att många organisationer med relativt begränsade insatser skulle kunna nå nivå 2. De områden som särskilt behöver stärkas är *Organisation och ledningssystem, Incident- och kontinuitetshantering* samt *Komponentsäkerhet*. Genom att adressera dessa arbetsområden skulle många organisationer kunna ta ett steg uppåt i modellen till nästa mätning.

4.4.3 Spridning av resultattal

Diagram 3 syftar inte till att redovisa exakta data, utan till att ge en överblick över resultattalet (se avsnitt 1.2) hos samtliga deltagande förvaltningar och därmed illustrera spridningen i resultaten.

Ot-säkkollen diagram 3. Resultattal hos de 62 förvaltningar som deltog i Ot-säkkollen 2025



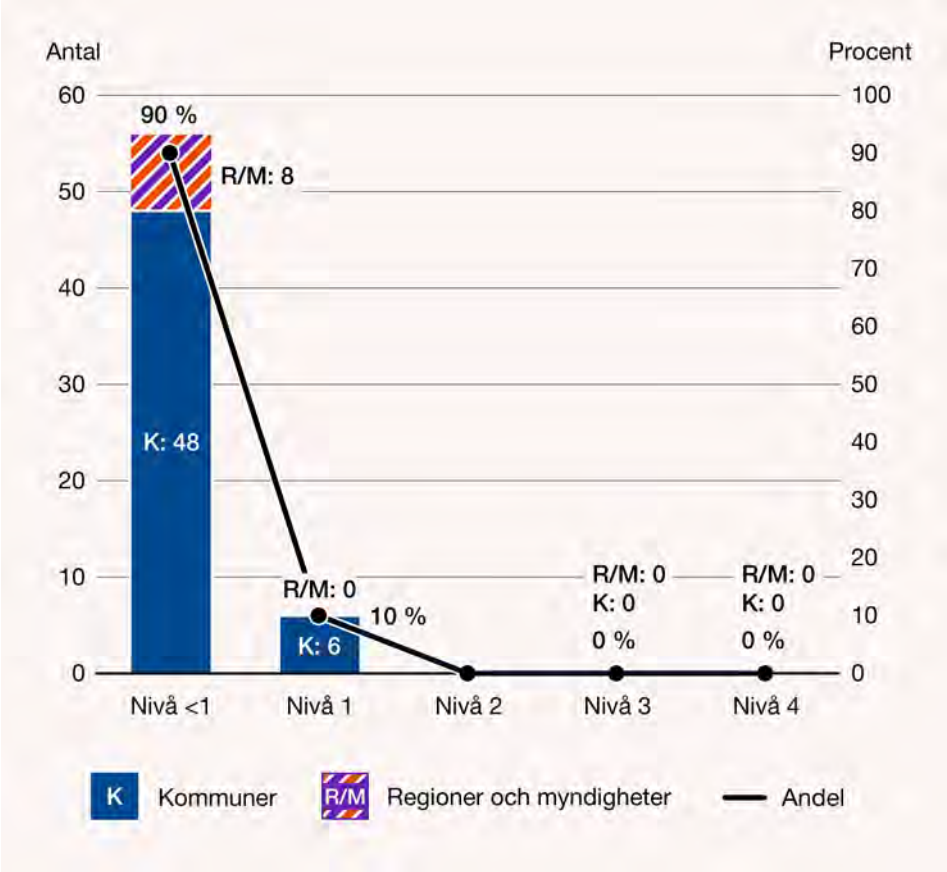
Den svarta linjen i diagrammet motsvarar den nivå som Myndigheten för civilt försvar har definierat som en indikation över huruvida en organisation uppfyller den nivå i modellen som motsvarar kvalificerat innehåll i ot-säkerhetsarbetet.

Av diagram 3 framkommer att resultatspridningen, i jämförelse med övriga mätningar, är förhållandevis låg. Det förklaras av att majoriteten av de deltagande organisationerna har ett resultattal nära noll. Det genomsnittliga resultattalet i Ot-säkkollen är 0,37. Endast 19 procent av deltagarna har ett resultattal över 0,5.

4.4.4 Fördelning av övergripande nivå

Diagram 4 illustrerar fördelningen gällande uppnådd övergripande nivå bland deltagande organisationer, det vill säga andelen som inte uppnått nivå 1 alternativt har nått upp till någon av modellens fyra nivåer. Nivå 1 motsvarar att en organisation har grunderna i ett systematiskt leveranskedjesäkerhetsarbete på plats.

Ot-säkkollen diagram 4. Fördelning av övergripande nivå hos deltagande förvaltningar



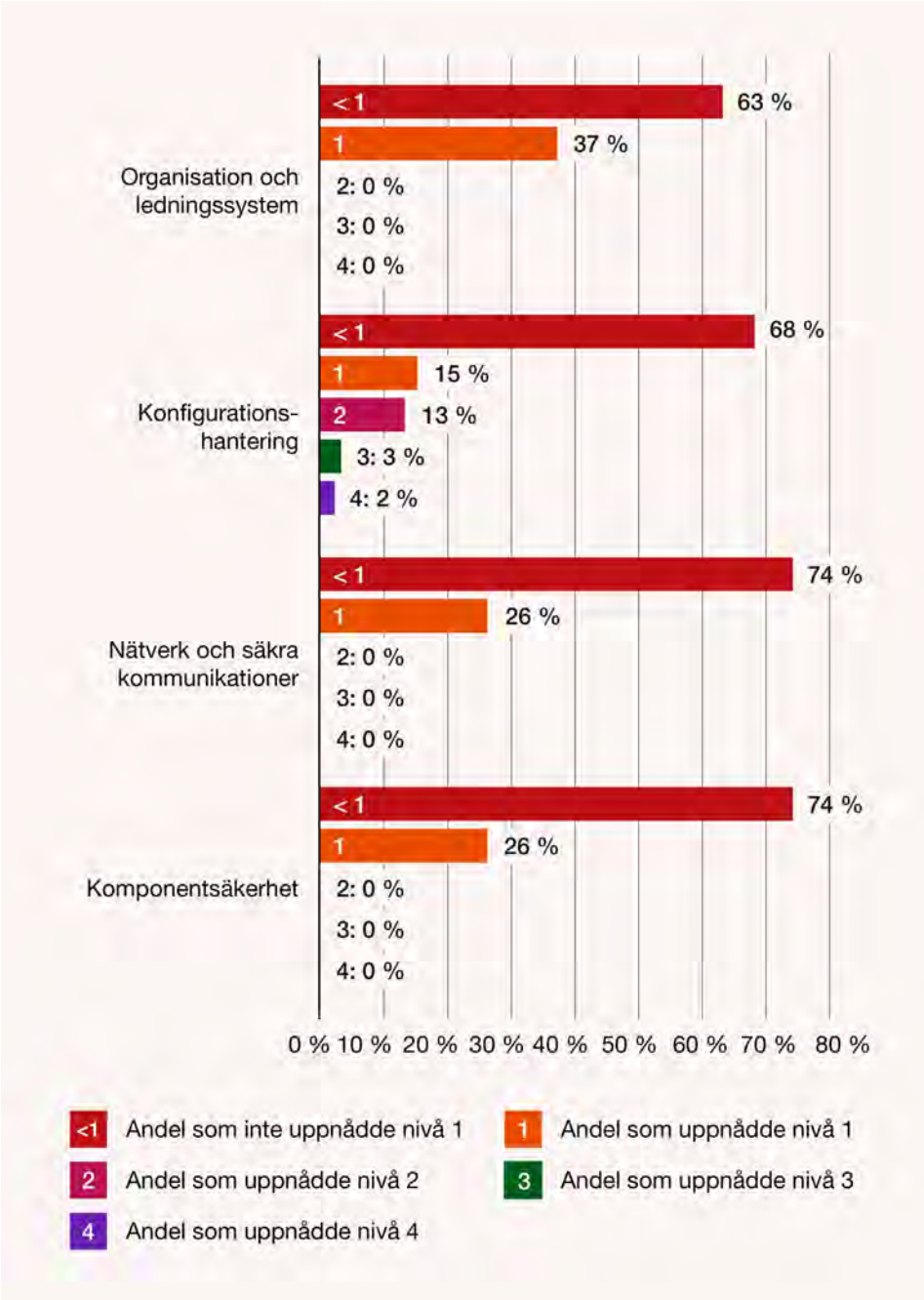
Av diagram 4 framgår att 90 procent av deltagande förvaltningar, motsvarande 56 organisationer, inte når nivå 1. Enbart tio procent av organisationerna når nivå 1, varav samtliga är kommuner. Det kan också konstateras att ingen av de deltagande förvaltningarna når modellens högre nivåer.

Vilka åtgärder som typförvaltningen hade behövt vidta för att höja sin övergripande nivå redovisas i avsnitt 2.5.

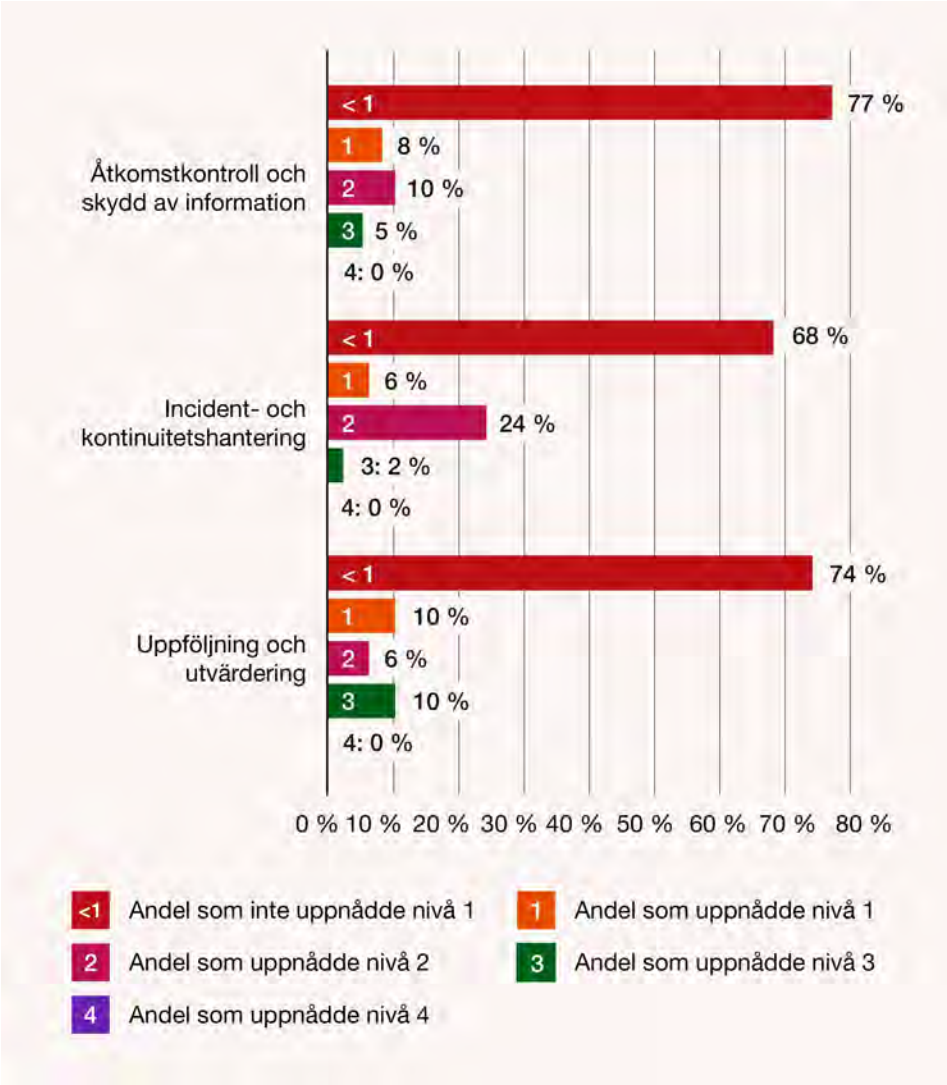
4.4.5 Fördelning av nivå per arbetsområde

Diagram 5 visar vilken nivå deltagande förvaltningar har uppnått inom Ot-säkkollens sju arbetsområden. Diagrammet synliggör även variationen i prestation inom ett visst arbetsområde mellan organisationerna.

Ot-säkkollen diagram 5. Fördelning av nivå per arbetsområde hos deltagande förvaltningar



Ot-säkkollen diagram 5 fortsättning. Fördelning av nivå per arbetsområde hos deltagande förvaltningar



Den största andelen organisationer har nått nivå 1 eller högre inom *Organisation och ledningssystem* (37 procent), *Konfigurationshantering* samt *Incident- och kontinuitetshantering* (båda 32 procent). Även om flest organisationer nådde upp till nivå 1 gällande *Organisation och ledningssystem* var det ingen organisation som nådde nivå 2 på detta arbetsområde.

De arbetsområden där den högsta andelen har nått nivå 3 eller högre är *Uppföljning och utvärdering* (10 procent), *Konfigurationshantering* och *Åtkomstkontroll och skydd av information* (båda 5 procent).

Diagram 5 synliggör också att den minsta andelen organisationer har nått nivå 1 eller högre är *Åtkomstkontroll och skydd av information* (23 procent) samt *Nätverk och säkra kommunikationer, Komponentsäkerhet* och *Uppföljning och utvärdering* (samtliga 26 procent).

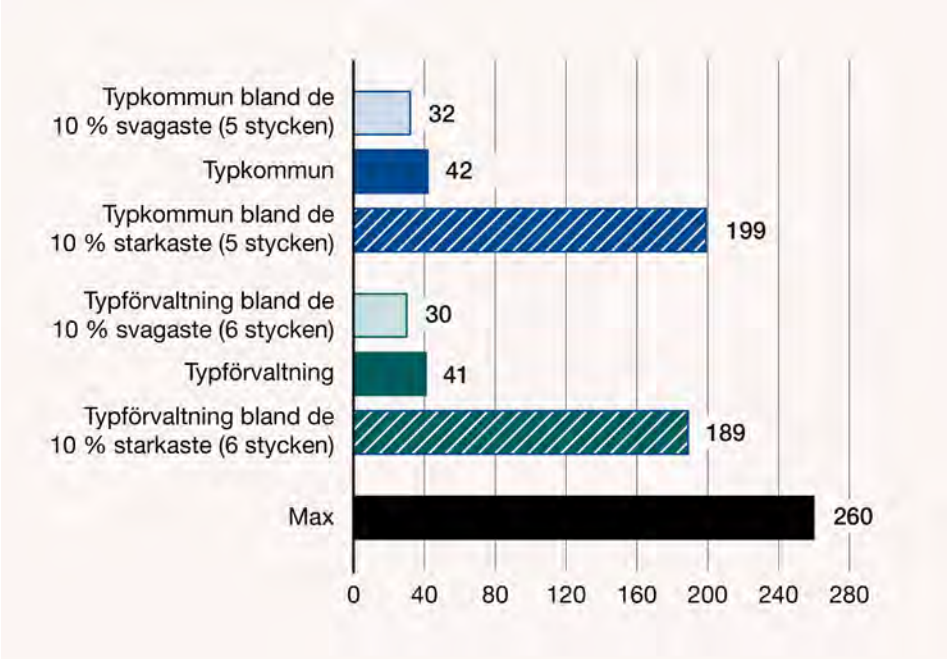
Generellt är resultaten så svaga på samtliga arbetsområden att det är svårt att dra några egentliga slutsatser utifrån en jämförelse dem emellan. Det är heller inte fruktbart att jämföra resultaten mellan aktörsgrupperna.

4.4.6 Antal genomförda åtgärder hos typaktörerna

Inom Ot-säkkollen undersöks totalt 260 stycken åtgärder. Diagram 6–7 redogör för det totala antalet åtgärder som aktörsgrupperna har genomfört samt antalet åtgärder som aktörsgrupperna infört inom varje enskilt arbetsområde. Det bör samtidigt understrykas att diagrammen inte synliggör huruvida de åtgärder som vidtagits avser mer grundläggande åtgärder eller åtgärder som undersöks inom modellens högre nivåer.

Diagram 6 redogör för antalet vidtagna åtgärder hos typkommunen och typförvaltningen samt antalet genomförda åtgärder hos typkommunen och typförvaltningen hos de tio procent starkaste respektive tio procent svagaste kommunerna och förvaltningarna.

Ot-säkkollen diagram 6. Totalt antal genomförda åtgärder hos typkommunen och typförvaltningen, samt de 10 procent svagast presterande respektive starkast presterande kommunerna och förvaltningarna



Både typkommunen och typförvaltningen har genomfört mindre än 20 procent av de åtgärder som undersöks inom Ot-säkkollen. Vidare bör noteras att typkommunen och typförvaltningen enbart har vidtagit cirka tio fler åtgärder än typkommunen respektive typförvaltningen hos de tio procent svagaste inom de två aktörsgrupperna. Att resultatspridningen är så pass liten förklaras av att den stora majoriteten av deltagande organisationerna har genomfört enbart ett fåtal av de åtgärder som undersöks.

Diagram 6 synliggör samtidigt att typkommunen och typförvaltningen hos de tio procent starkast presterande inom aktörsgrupperna har vidtagit cirka tre fjärdedelar av åtgärderna. Jämfört med typkommunen och typförvaltningen är resultatspridningen kraftig. Mellan typförvaltningen och typförvaltningen hos de 10 procent starkaste skiljer det sig totalt 148 åtgärder. Skillnaden mellan typkommunen och typkommunen hos de 10 procent starkaste motsvarar hela 157 åtgärder.

Ot-säkkollen diagram 7. Antal genomförda åtgärder per arbetsområde hos typkommunen och typförvaltningen

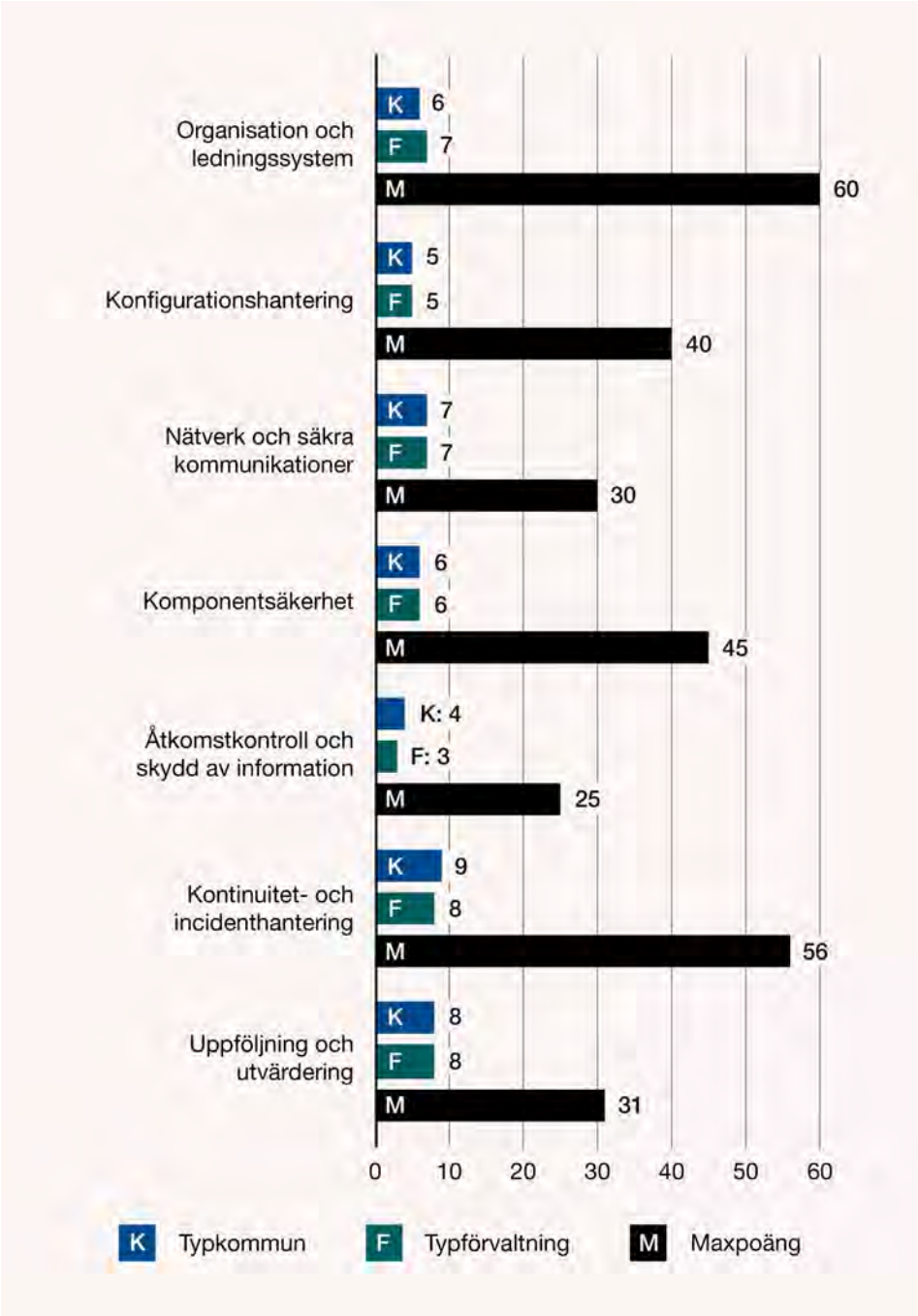


Diagram 7 ger en mer detaljerad bild över antalet vidtagna åtgärder genom att visa hur många åtgärder som aktörsgrupperna har genomfört inom varje arbetsområde.

I enlighet med vad som framgår av diagram 8 kan det utifrån diagram 7 konstateras att både typkommunen och typförvaltningen har genomfört en mycket liten andel av de åtgärder som undersöks inom de respektive arbetsområdena. *Uppföljning och utvärdering* (26 procent) samt *Nätverk och säkra kommunikationer* (23 procent) är de arbetsområden där den högsta andelen åtgärder har genomförts. I övriga arbetsområden har båda aktörsgrupperna genomfört runt 10 till 15 procent av undersökta åtgärder.

Sammantaget tydliggör diagram 7 att såväl typkommunen som typförvaltningen måste vidta fler åtgärder inom samtliga arbetsområden för att höja sin övergripande nivå inom Ot-säkkollen.

4.4.7 Resultatspridning

Diagram 8 jämför det genomsnittliga resultattalet (se avsnitt 1.2) mellan normalfördelningsgruppen samt de svagaste respektive starkast presterande förvaltningarna i syfte att tydliggöra resultatspridningen bland deltagarna. Normalfördelningen ses i detta sammanhang som de 80 procent som varken hör till de svagaste eller bäst presterande förvaltningarna.

Ot-säkkollen diagram 8. Resultatspridning hos deltagande förvaltningar

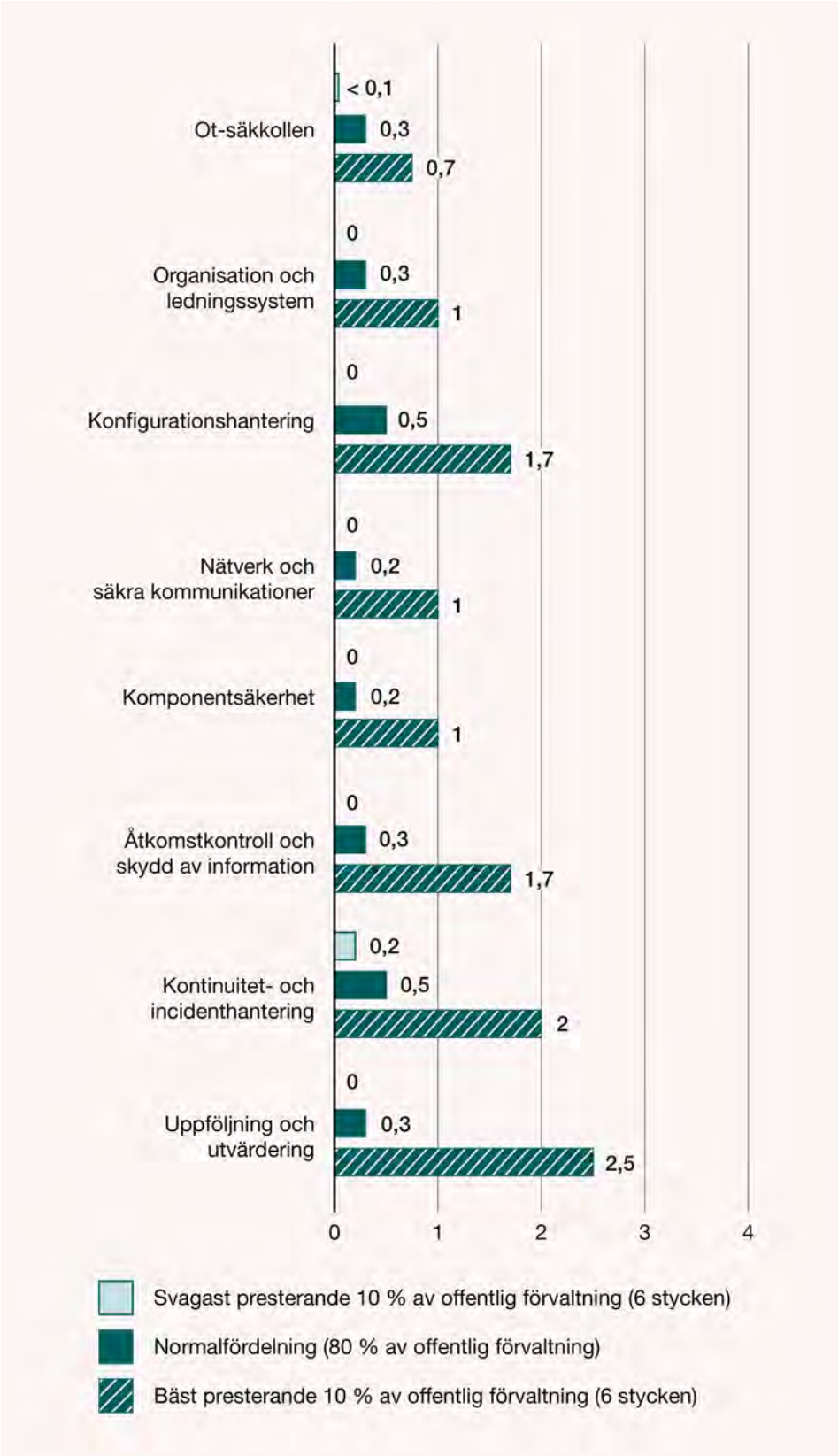


Diagram 8 visar på en mindre resultatspridning både inom Ot-säkkollen och enskilda arbetsområden jämfört med övriga mätningar inom Cybersäkerhetskollen. Det bör noteras att normalfördelningens resultat ligger nära de tio procent svagaste förvaltningarna, vilket förklaras av att den stora majoriteten av organisationerna har ett mycket lågt resultat.

Diagrammet visar dock på en reell skillnad mellan de tio procent starkaste förvaltningarna och den grupp som utgör normalfördelningen. De tio procent starkaste förvaltningarna har ett genomsnittligt resultattal på 1 eller högre, jämfört med normalfördelningen som i genomsnitt ligger på 0,4. Gruppen som utgör normalfördelningen har ett relativt jämnt, men likväl lågt resultat inom arbetsområdena, medan de bäst presterande har en större variation.

Skillnaden mellan de starkast presterande förvaltningarna och den grupp som i detta sammanhang benämns som normalfördelningen är störst inom arbetsområdet *Uppföljning och utvärdering*. Den minsta resultatskillnaden återfinns inom arbetsområdet *Organisation och ledningssystem.*

4.4.8 Djupdykning i Ot-säkkollen

I avsnittet konstateras att nio av tio av de deltagande organisationerna har brister i de mest grundläggande delarna av ot-säkerhetsarbetet. Avsnitt 4.4.6 tydliggör att både typkommunen och typförvaltningen har genomfört mindre än 20 procent av de åtgärder som undersöks inom Ot-säkkollen. De tio procent starkast presterande av förvaltningarna har samtidigt vidtagit över 70 procent av åtgärderna, vilket utgör en anmärkningsvärd skillnad mot typförvaltningen.

Sammantaget talar resultatet för typförvaltningen bland de tio procent starkaste förvaltningarna har goda förutsättningar för att höja den övergripande nivån till nästa mätning. Givet att det rör sig om en så pass stor andel av deltagande förvaltningarna som brister i de mest grundläggande delarna av ot-säkerhetsarbetet spelar de starkast presterande förvaltningarna en i synnerligen viktig roll eftersom de kan möjliggöra lärande för organisationer som brister i de mest grundläggande delarna.

Till skillnad från avsnitt 3.5, som fokuserar på rekommendationer som förvaltningar bör vidta baserat på typkommunens resultat i Ot-säkkollen, belyser detta avsnitt i stället vilka områden som de organisationer som redan är förhållandevis starka i sitt ot-säkerhetsarbete bör adressera för att höja sin övergripande nivå i Ot-säkkollen.

Typförvaltningen bland de tio procent starkaste når övergripande nivå 1 i Ot-säkkollen. En mer detaljerad analys visar dock att den övergripande nivån hade kunnat höjas till nivå 3 genom att enbart ett fåtal ytterligare åtgärder vidtas. Som berörs i avsnitt 4.4.2 är det tre arbetsområden, *Organisation och ledningssystem*, *Komponentsäkerhet* samt *Incident- och kontinuitetshantering*, som drar ned typförvaltningen bland de tio procent starkaste förvaltningarnas övergripande nivå.

För att nå nivå 3 hade typförvaltningen hos de starkast presterande förvaltningarna också behövt vidta fler av åtgärderna på den grundläggande nivån, det vill säga nivå 1. Sådana åtgärder inkluderar exempelvis att dokumentera fler av sina arbetssätt. De arbetssätt där det finns det största behovet av att vidta åtgärder av mer grundläggande karaktär inkluderar arbetssätt för att härda komponenter innan de tas i drift i ot-miljön samt arbetssätt för att upprätta, verifiera och vidmakthålla ritningar/dokumentation över ot-miljöns arkitektur och infrastruktur.

Inom ramen för Ot-säkkollens nivå 2 hade gruppen behövt hantera komponenter och system i ot-miljön i enlighet med sitt arbetssätt för säker livscykelhantering (av komponenter och system i ot-miljön) i en större utsträckning. Organisationens ledningssystem för ot-säkerhet hade även behövt omfatta regler och riktlinjer för fler personalrelaterade delar.

På nivå 3 hade mer kvalificerat innehåll behövt implementeras i arbetssätt för detektering och loggning av säkerhetsavvikelser, händelser och incidenter i ot-miljön. Även för arbetssätt för säkerhetsläge i ot-miljön samt arbetssätt för att hantera trådlösa nätverk, protokoll och kommunikation hade fler åtgärder, som visar på kvalificerat innehåll i ot-säkerhetsarbetet, behövt vidtas.

4.5 Resultat i Leveranskedjekollen 2025

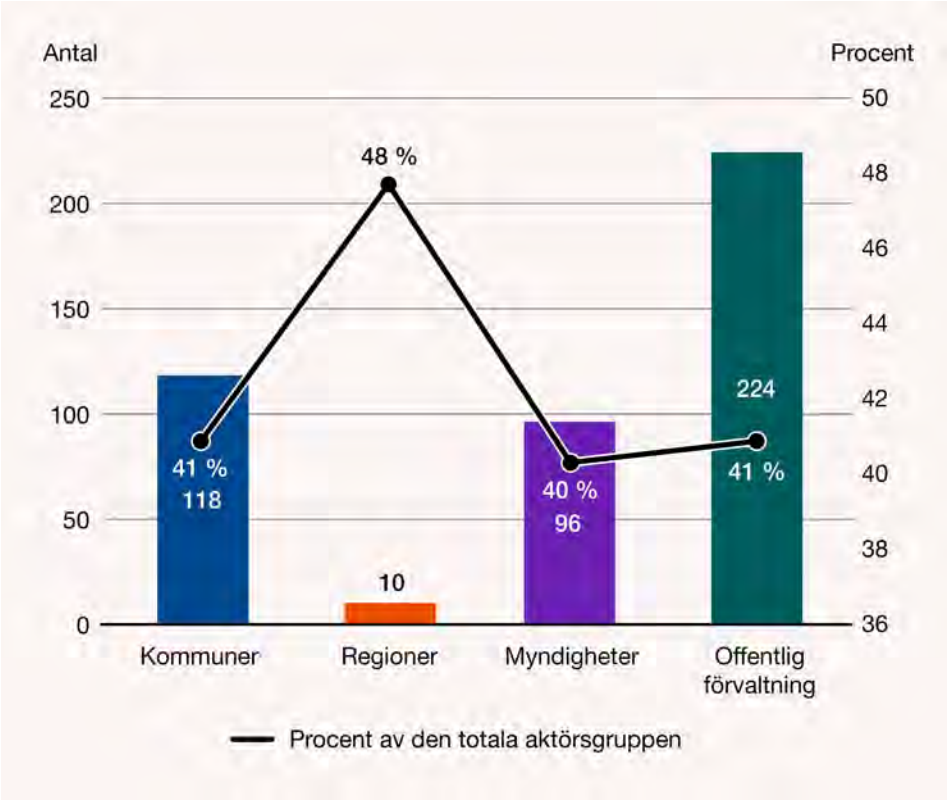
I det här avsnittet redogörs för resultat av Leveranskedjekollen 2025. Leveranskedjekollen följer upp nivån på det systematiska säkerhetsarbetet avseende digitala leveranskedjor och mätningen genomförs för första gången. Syftet är att ge en samlad bild av hur säkerhetsarbetet med digitala leveranskedjor bedrivs, identifiera styrkor och utvecklingsområden, samt ge underlag för fortsatt förbättringsarbete.

Leveranskedjekollen följer upp nivån på det systematiska säkerhetsarbetet för digitala leveranskedjor dels hos så kallade mottagande organisationer, dels hos så kallade levererande organisationer (se avsnitt 1.2). Sett utifrån både antalet arbetsområden och frågor är Leveranskedjekollen den minsta mätningen i Cybersäkerhetskollen om totalt 15 frågor och fem arbetsområden.

4.5.1 Deltagande i Leveranskedjekollen

Totalt har 224 organisationer i offentlig förvaltning deltagit i mätningen. Utav dessa är 118 kommuner, 10 regioner och 96 myndigheter. Deltagarna utgör cirka en tredjedel av offentlig förvaltning.[47] Drygt två tredjedelar av de som genomförde Cybersäkerhetskollen 2025 svarade även på Leveranskedjekollen.

Leveranskedjekollen diagram 1. Deltagande i Leveranskedjekollen 2025



Not 47. Enligt den rampopulation som specificeras i avsnitt 3.1.

I förhållande till sin aktörsgrupp har regionerna deltagit i störst utsträckning i Leveranskedjekollen (48 procent), följt av kommunerna (41 procent) och slutligen myndigheterna (30 procent). Sett till faktiskt antal är dock kommuner, i likhet med deltagandet i övriga mätningar, den största aktörsgruppen.[48]

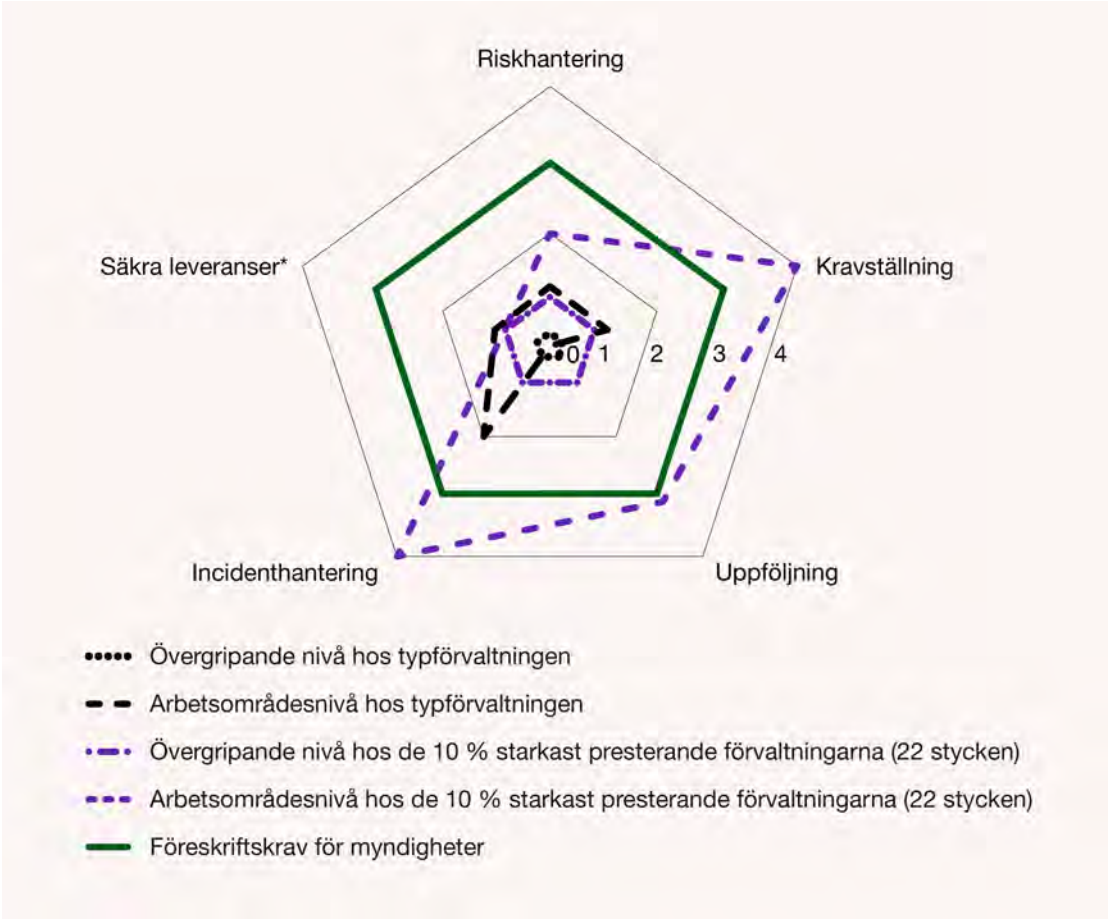
Utav de 224 förvaltningar som deltagit, har 26 organisationer (12 procent) uppgett att de även är en levererande organisation, det vill säga att de utgör startpunkten i en digital leveranskedja genom att tillgängliggöra tjänster eller produkter som andra organisationer nyttjar.

4.5.2 Typförvaltningens resultat

Diagram 2 visar övergripande nivå samt uppnådd nivå per arbetsområde för typförvaltningen i Leveranskedjekollen. Dessutom illustreras den övergripande nivån samt uppnådd nivå per arbetsområde hos de tio procent starkaste förvaltningarna. Leveranskedjekollens nivå 3, vilket grönmarkerats i diagrammet, uppnås av organisationer som har beslutade arbetssätt (nivå 1) som de använder i tillräcklig utsträckning (nivå 2) och som dessutom har kvalificerat innehåll i sina arbetssätt (nivå 3).

Not 48. Vilken aktörsgrupp som har flest deltagare påverkar typförvaltningens resultat och resultatet för offentlig förvaltning i stort.

Leveranskedjekollen diagram 2. Resultat i Leveranskedjekollen för typförvaltningen och typförvaltningen bland de tio procent starkast presterande förvaltningarna



Resultatet i arbetsområdet *Säkra leveranser* baseras enbart på de förvaltningar som uppgett att de är en levererande organisation (se avsnitt 1.2). Nivån hos de 10 procent starkast presterande förvaltningarna är baserad på resultaten hos de tre förvaltningar.

Typförvaltningen har inte nått upp till övergripande nivå 1 i Leveranskedjekollen, vilket indikerar avsaknad av grunderna i ett systematiskt leveranskedjesäkerhetsarbete. *Uppföljning* är det arbetsområde som drar ner typförvaltningens övergripande nivå till nivå 0. Typförvaltningen presterar starkast inom arbetsområdet *Incidenthantering*, där man har uppnått nivå 2. I övriga tre arbetsområden, det vill säga inom *Riskhantering, Kravställning*, och *Säkra leveranser* uppnår typförvaltningen nivå 1. Med riktade insatser inom *Uppföljning* skulle således typförvaltningen kunna höja sin övergripande nivå till nästa mätning.

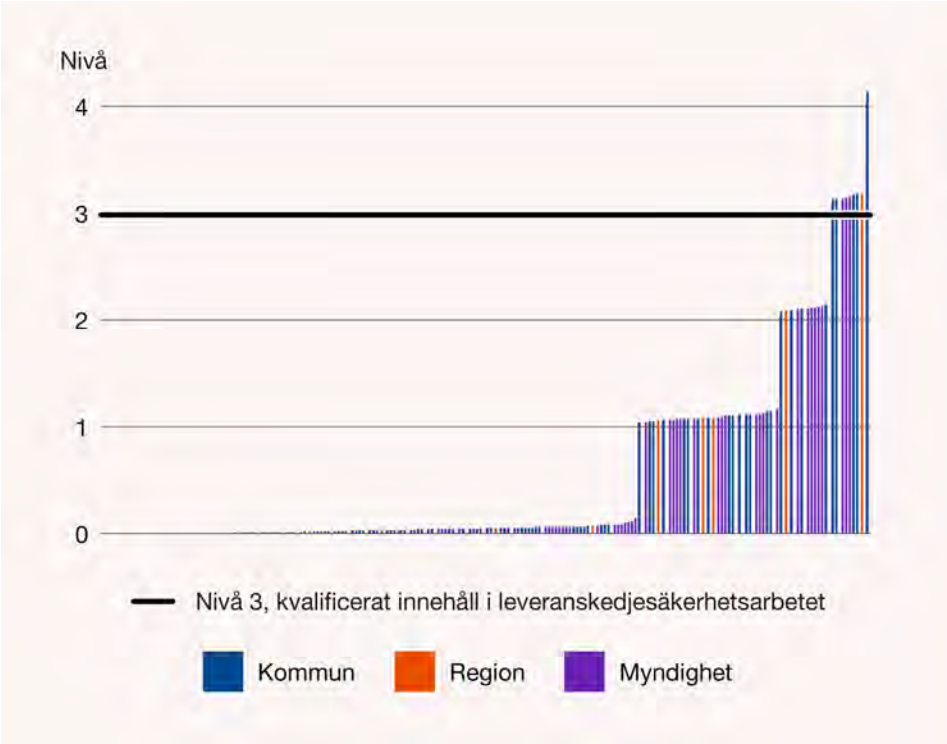
Utifrån diagram 2 kan det även konstateras att typförvaltningen hos de tio procent starkast presterande förvaltningarna uppnår nivå 1. Det som drar ned den övergripande nivån är resultatet inom arbetsområdet *Säkra leveranser*, där typförvaltningen uppnår nivå 1. Inom övriga fyra arbetsområden når typförvaltningen hos de tio procent starkast presterande förvaltningarna nivå 2 eller högre. I likhet med typförvaltningen är resultatet starkast inom *Incidenthantering*, där nivå 4 har uppnåtts.

För att förstå resultatet är det viktigt att beakta att Leveranskedjekollen är den mätning i Cybersäkerhetskollen med minst antal frågor, vilket medför att resultatet ”slår hårdare”. Det innebär samtidigt att de organisationer som väljer att vidareutveckla sitt säkerhetsarbete avseende digitala leveranskedjor kan stiga i nivå genom att vidta förhållandevis få åtgärder.

4.5.3 Spridning av resultattal

Diagram 3 syftar inte till att redovisa exakta data, utan till att ge en överblick över resultattalet (se avsnitt 1.2) hos samtliga deltagande förvaltningar och därmed illustrera spridningen i resultaten.

Leveranskedjekollen diagram 3. Resultattal hos de 224 förvaltningar som deltog i Leveranskedjekollen 2025



Den svarta linjen i diagrammet motsvarar den nivå som Myndigheten för civilt försvar har definierat som en indikation över huruvida en organisation uppfyller den nivå i modellen som motsvarar kvalificerat innehåll i leveranskedjesäkerhetsarbetet.

Diagram 3 synliggör, i likhet med Infosäkkollen och It-säkkollen, en stor spridning av resultatet med avseende på resultattalet hos medverkande förvaltningar samt inom de tre aktörsgrupperna.

Det genomsnittliga resultattalet för samtliga deltagande förvaltningar är 0,56. Baserat på resultattalet presterar myndigheterna starkast (0,7), följt av kommunerna (0,44). Utifrån resultattalet har regionerna det svagaste resultatet (0,27). Det genomsnittliga resultattalet, både i offentlig sektor i stort och inom aktörsgrupperna, är lågt eftersom majoriteten av de deltagande organisationerna har ett resultattal mindre än 0,5.

4.5.4 Fördelning av övergripande nivå

Diagram 4 illustrerar fördelningen vad gäller uppnådd övergripande nivå hos deltagande aktörsgrupper i Leveranskedjekollen 2025, det vill säga andelen som inte nått upp till nivå 1, eller som nått upp till en viss nivå. Nivå 1 motsvarar att en organisation har grunderna i ett systematiskt leveranskedjesäkerhetsarbete på plats.

Leveranskedjekollen diagram 4. Fördelning av övergripande nivå hos deltagande förvaltningar

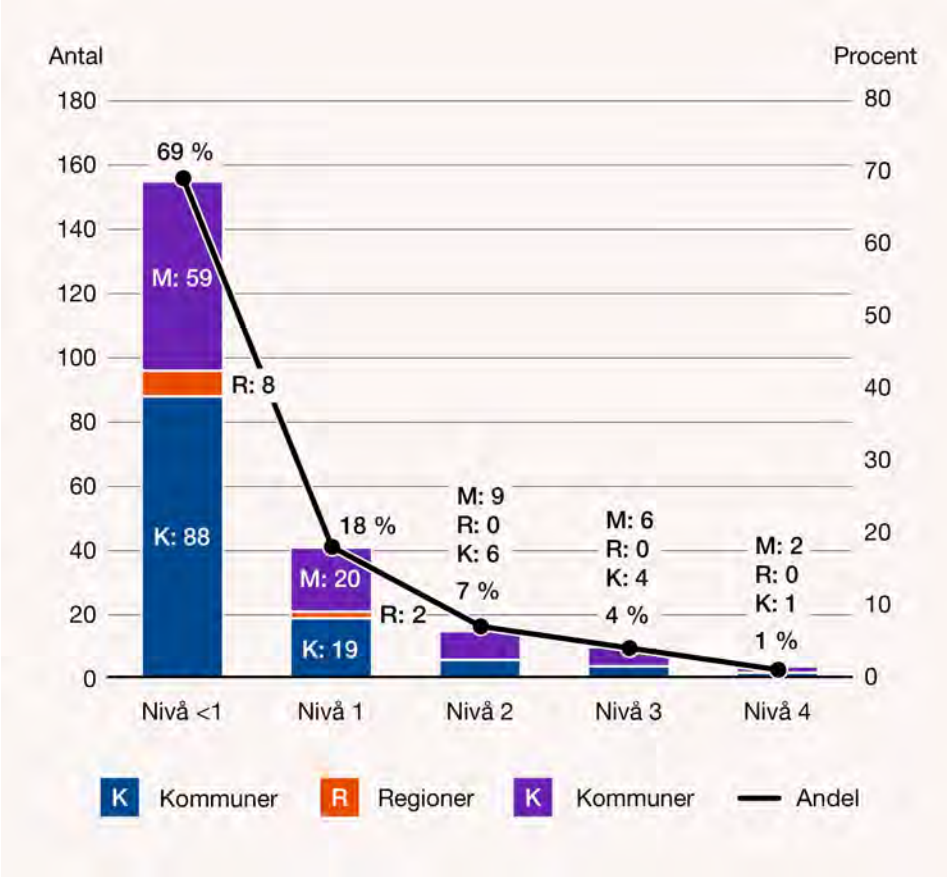


Diagram 4 visar att 69 procent, nästan sju av tio förvaltningar, inte når övergripande nivå 1 eller högre i Leveranskedjekollen. En majoritet av deltagande organisationer saknar därmed grunderna i sitt systematiska leveranskedjesäkerhetsarbete. 18 procent av de deltagande organisationerna har uppnått nivå 1 och 7 procent har uppnått nivå 2. Endast fem procent, motsvarande 13 organisationer, har uppnått nivå 3 eller högre. Nivå 3 indikerar att organisationen har ett kvalificerat innehåll i sina arbetssätt.

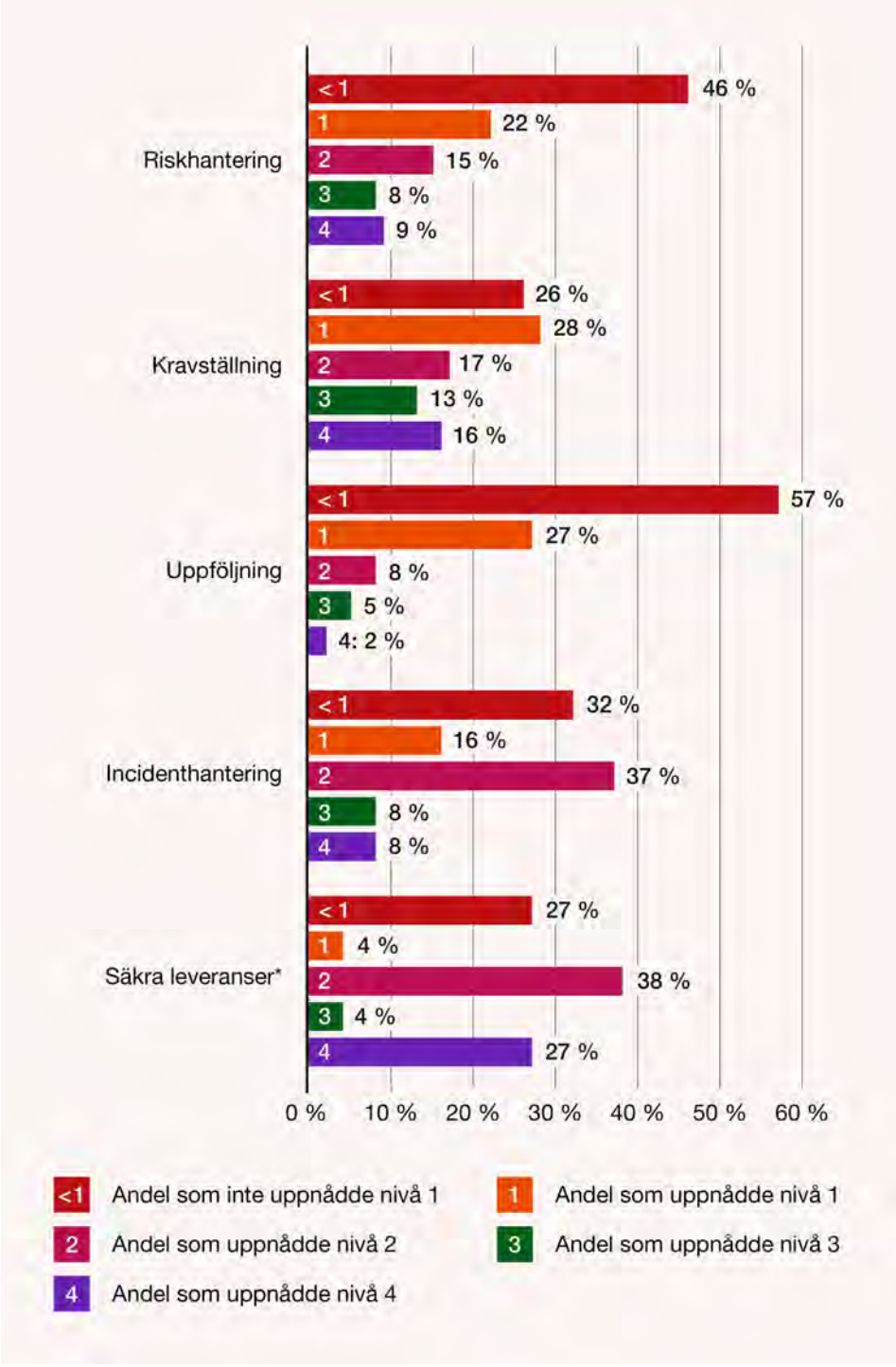
Myndigheter är den aktörsgrupp där den största andelen organisationer, 39 procent, har uppnått nivå 1 eller bättre. Motsvarande siffra hos regionerna och kommunerna är 20 respektive 25 procent. Myndigheter är således den aktörsgrupp som presterar bäst när det gäller att ha grunderna i ett systematiskt leveranskedjesäkerhetsarbete på plats.

Vilka åtgärder som typkommunen, typregionen och typmyndigheten hade behövt vidta för att höja sin övergripande nivå redovisas närmare i avsnitt 2.6.

4.5.5 Fördelning av nivå per arbetsområde

Diagram 5 visar fördelningen av uppnådd nivå per arbetsområde inom Leveranskedjekollen. Utifrån diagrammet kan också konstateras att det finns en förhållandevis stor variation i hur organisationerna presterar inom varje enskilt arbetsområde.

Leveranskedjekollen diagram 5. Fördelning av nivå per arbetsområde hos deltagande förvaltningar



Resultatet i arbetsområdet Säkra leveranser baseras enbart på de förvaltningar som uppgett att de är en levererande organisation (se avsnitt 1.2).

Av de fem arbetsområden som följs upp i Leveranskedjekollen har den största andelen nått nivå 1 eller högre inom arbetsområdena *Säkra Leveranser* (73 procent[49]) och *Kravställning* (74 procent). *Säkra leveranser* och *Kravställning* är även de två arbetsområden där den högsta andelen har nått nivå 3 eller högre (31 respektive 29 procent).

Den minsta andelen organisationer har uppnått nivå 1 eller högre inom *Uppföljning* (43 procent) och *Riskhantering* (54 procent). I likhet med vad som konstaterades i avsnitt 4.5.2 presterar således deltagande organisationer i synnerligen svagt inom *Uppföljning* jämfört med övriga arbetsområden.

Diagram 5 visar inte vilken nivå som de enskilda aktörsgrupperna har uppnått. I sammanhanget bör dock uppmärksammas att kommuner är den aktörsgrupp där den minsta andelen organisationer har nått nivå 1 eller högre inom samtliga fem arbetsområden. Kommunernas resultat inom arbetsområdet *Incidenthantering* avviker särskilt från övriga två aktörsgrupper. Inom detta arbetsområde når 47 procent av kommunerna inte nivå 1 eller högre. Motsvarande siffra hos regionerna och myndigheterna är 10 respektive 15 procent.

Andelen kommuner och regioner som har uppnått nivå 1 eller högre inom de fem arbetsområdena är förhållandevis likvärdigt. Med undantag från arbetsområdet *Uppföljning*, där en betydligt större andel myndigheter (60 procent) har nått nivå 1 eller högre jämfört med regionerna (40 procent), är andelen regioner som har nått nivå 1 eller högre större bland regionerna än myndigheterna.

4.5.6 Antal genomförda åtgärder hos typaktörerna

Totalt antal möjliga åtgärder i Leveranskedjekollen är 75 stycken. Diagram 6–7 redogör för det totala antalet åtgärder som aktörsgrupperna har genomfört samt antalet åtgärder som aktörsgrupperna infört inom respektive arbetsområde. Det bör samtidigt understrykas att diagrammen inte synliggör huruvida de åtgärder som vidtagits avser mer grundläggande åtgärder eller åtgärder som undersöks inom Leveranskedjekollens högre nivåer.

Diagram 6 visar för antalet vidtagna aktörer hos typkommunen, typregionen och typmyndigheten samt antalet genomförda åtgärder hos typmyndigheten och typkommunen hos de tio procent starkaste respektive tio procent svagaste myndigheterna och kommunerna.

Not 49. Andelen är baserad på de 26 organisationer som uppgett att de är en levererande organisation.

Leveranskedjekollen diagram 6. Totalt antal genomförda åtgärder hos typkommunen, typregionen och typmyndigheten, samt de 10 procent svagast presterande respektive starkast presterande kommunerna och myndigheterna[50]

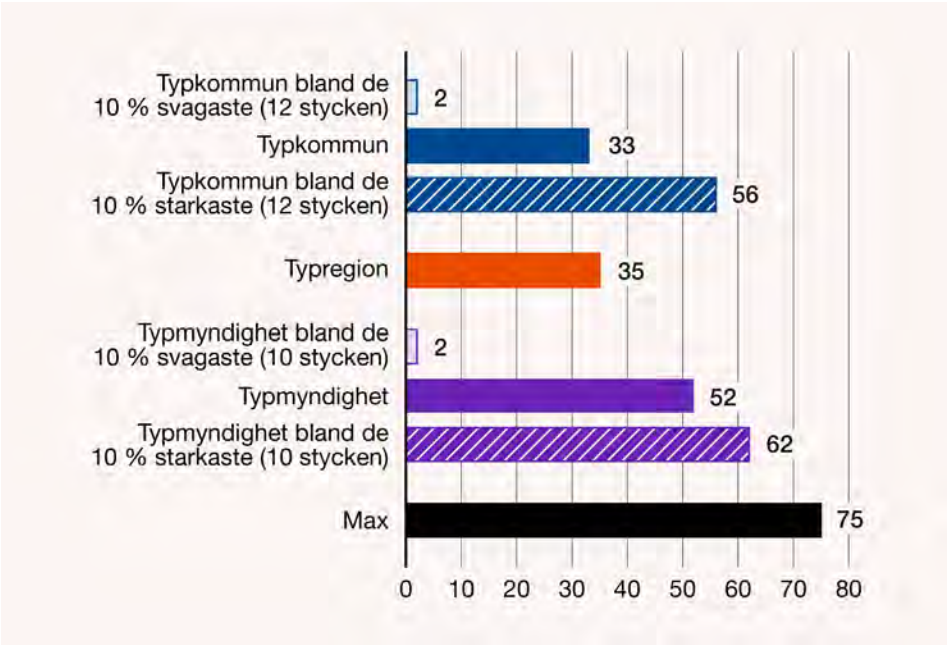


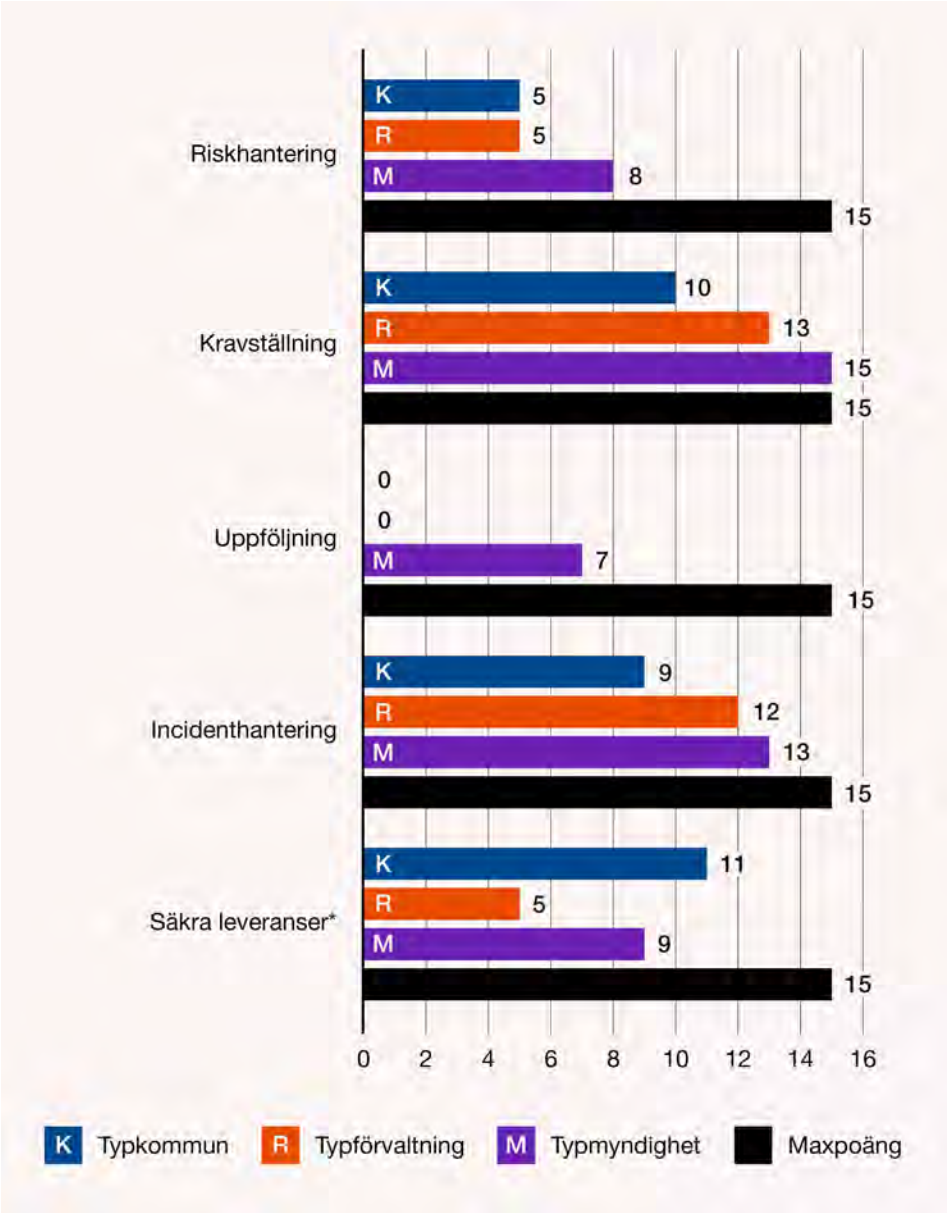
Diagram 6 visar att typmyndigheten är den aktörsgrupp som har vidtagit flest åtgärder (52 stycken). Både typkommunen och typregionen har genomfört noterbart färre åtgärder än typmyndigheten (33 respektive 35 stycken). Typkommunen och typregionen presterar således förhållandevis likvärdigt.

Resultatskillnaden mellan myndigheterna kontra övriga aktörsgrupper illustreras även av att typkommunen bland de tio procent starkast presterande kommunerna endast har infört sex fler åtgärder än typmyndigheten. Det rör sig dock om en mindre resultatskillnad när man jämför resultatet hos typmyndigheten bland de tio procent starkaste med motsvarande grupp hos kommunerna. Detta hör samman med att skillnaden mellan typmyndigheten och typmyndigheten bland de tio procent starkaste är förhållandevis liten.

Diagrammet visar även att både typmyndigheten bland de tio procent svagaste myndigheterna liksom typkommunen bland de tio procent svagaste kommunerna enbart har vidtagit 2 av de totalt 75 åtgärder som undersöks i mätningen.

Not 50. Regionerna är en för liten aktörsgrupp för att det ska vara fruktsamt att ta fram resultatet för de tio procent starkaste regionerna.

Leveranskedjekollen diagram 7. Antal genomförda åtgärder per arbetsområde hos typkommunen, typregionen och typmyndigheten



Resultatet i arbetsområdet Säkra leveranser baseras enbart på de förvaltningar som uppgett att de är en levererande organisation (se avsnitt 1.2).

Diagram 7 redogör för antalet vidtagna åtgärder inom Leveranskedjekollens fem arbetsområden. *Kravställning* och *Incidenthantering* är de två arbetsområden som aktörsgrupperna sammantaget har vidtagit flest åtgärder inom (84 respektive 72 procent i genomsnitt). I fråga om arbetsområdet *Kravställning* är det noterbart att typmyndigheten har genomfört samtliga av de åtgärder som undersöks.

Uppföljning samt *Riskhantering* är de arbetsområden där samtliga tre aktörsgrupper har genomfört det minsta antalet åtgärder. Resultatet inom *Uppföljning* är i synnerhet noterbart då typkommunen och typregionen inte har vidtagit en enda av de åtgärder som undersöks. Typmyndigheten har vidtagit något mindre än hälften av åtgärderna.

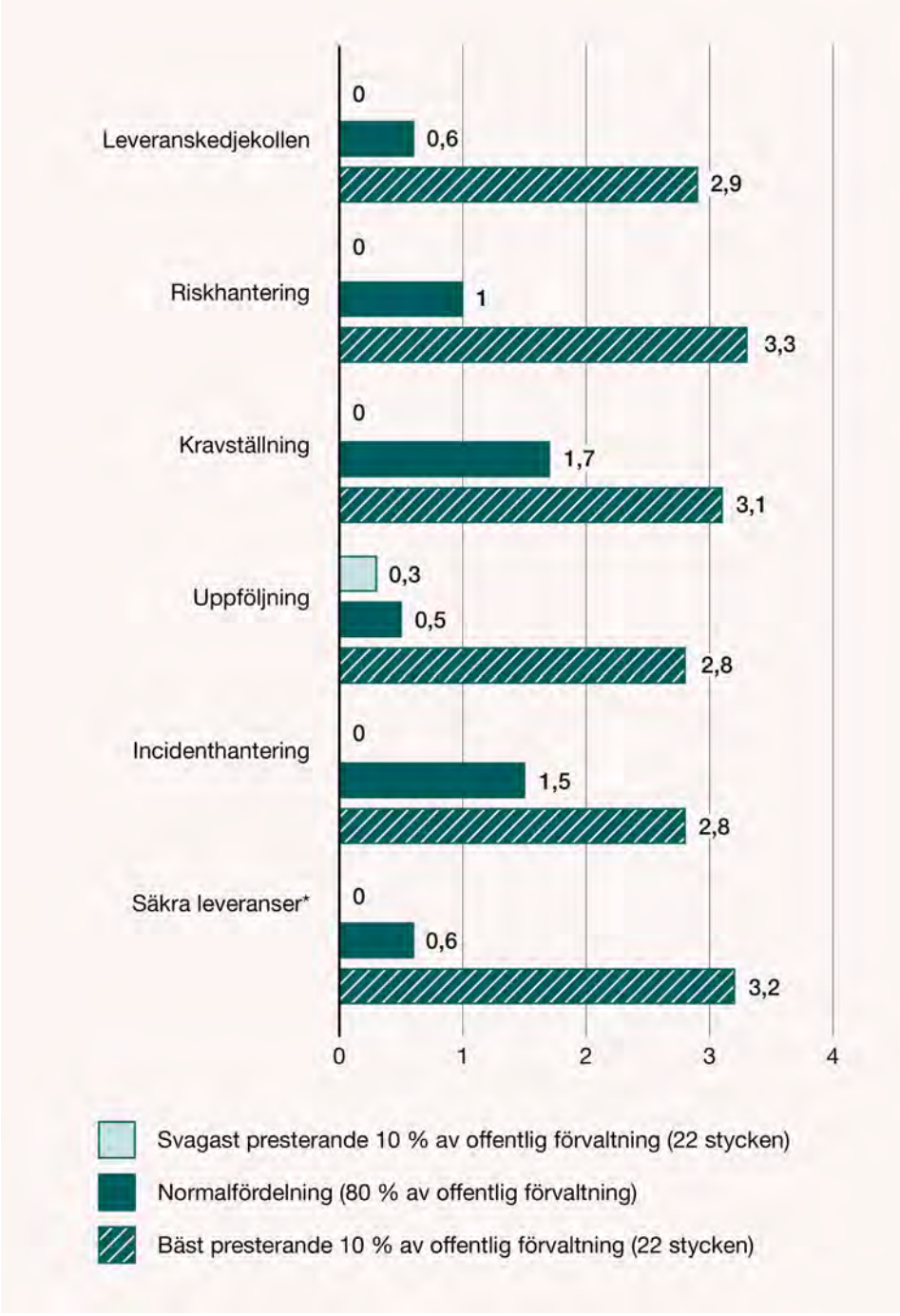
Av diagram 7 kan vidare konstateras att typmyndigheten och typregionen presterar bättre än typkommunen inom samtliga arbetsområden med undantag för ett, *Säkra leveranser*, där typkommunen i stället har det starkaste resultatet.

Även om typförvaltningen inte uppnår nivå 1 eller högre i Leveranskedjekollen, visar antalet genomförda åtgärder på att många organisationer har god potential att förbättra sin övergripande nivå genom att enbart vidta några fler åtgärder. Antingen behöver de införa några grundläggande åtgärder till, alternativt använda sina beslutade arbetssätt i en högre utsträckning för att kunna klättra i modellen.

4.5.7 Resultatspridning

Diagram 8 jämför det genomsnittliga resultattalet (se avsnitt 1.2) mellan normalfördelningsgruppen samt de svagaste respektive starkast presterande förvaltningarna i syfte att tydliggöra resultatspridningen hos deltagarna. Normalfördelningen ses i detta sammanhang som de 80 procent som varken hör till de svagaste eller bäst presterande förvaltningarna.

Leveranskedjekollen diagram 8. Resultatspridning hos deltagande förvaltningar



Resultatet i arbetsområdet Säkra leveranser baseras enbart på de förvaltningar som uppgett att de är en levererande organisation (se avsnitt 1.2).

Diagrammet påvisar en stor resultatspridning inom såväl enskilda arbetsområden som Leveranskedjekollen i stort. De svagaste tio procenten av förvaltningarna har ett genomsnittligt resultattal på noll inom Leveranskedjekollen, samt inom fyra av fem arbetsområden. De tio procent starkaste förvaltningarna genomsnittliga resultattal är cirka 3 inom enskilda arbetsområden och mätningen i stort, medan gruppen som representerar normalfördelningen har ett resultattal som varierar mellan 0,5 och 1,5.

I sammanhanget är det också noterbart att gruppen som utgör normalfördelningen har ett mer ojämnt resultat mellan arbetsområdena, än de tio procent svagaste respektive starkaste förvaltningarna.

Skillnaden mellan de starkast presterande förvaltningarna och den grupp som i detta sammanhang benämns som normalfördelningen är störst inom arbetsområdet *Säkra leveranser.* Den minsta skillnaden finns inom arbetsområdet *Incidenthantering*.

Även om det inte framgår av diagram 8 bör det uppmärksammas att resultatspridningen även är påtaglig inom aktörsgrupperna. Regionerna är dock den klart mest homogena arbetsgruppen. Resultatspridningen är störst hos myndigheterna.

4.5.8 Djupdykning i Leveranskedjekollen

Uppföljning är det arbetsområde i Leveranskedjekollen där minst antal organisationer har uppnått nivå 1 eller högre (se avsnitt 4.5.5). I avsnitt 4.5.6 konstateras också att det är det arbetsområde där samtliga tre aktörsgrupper inom offentlig förvaltning har vidtagit det minsta antalet åtgärder. Typkommunen och typregionen har noterbart inte vidtagit en enda av de åtgärder som undersöks inom arbetsområdet. Givet de tydliga brister avseende *Uppföljning* som framkommit i resultatredovisningen följer följande djupdykning upp resultatet inom arbetsområdet närmare.

En närmare granskning av resultatet visar att över hälften (52 procent) av de deltagande organisationerna har svarat *nej* på frågan om de under de senaste två åren haft ett arbetssätt för att följa upp säkerheten i sina digitala leveranskedjor. Av de organisationer som uppgett att de har haft ett arbetssätt för att följa upp säkerheten i digitala leveranskedjor uppger två tredjedelar att arbetssättet *varit beslutat eller på annat sätt medvetet valt av organisationen*. Närmare 60 procent uppger att arbetssättet *omfattat fördelning av roller och ansvar*. Hälften uppger att arbetssättet *varit beskrivit i stöd och vägledning samt varit kommunicerat till berörda medarbetare*, och något mindre än hälften procent uppger att arbetssättet varit *integrerat i organisationens övergripande arbetssätt för leverantörs- och avtalsuppföljning*.

Resultatet visar också att de organisationer som trots allt har haft ett arbetssätt för att följa upp säkerheten i digitala leveranskedjor enbart nyttjar det i låg utsträckning. Hos de organisationer som har ett sådant arbetssätt har endast en femtedel följt upp *mer än 50 procent av befintliga leverantörsrelationer*. Enbart en av tio uppger att uppföljningen har avsett *mer än 75 procent av de befintliga leverantörsrelationerna*.

Av de organisationer som har uppgett att de har haft ett arbetssätt för att följa upp följa upp säkerheten i digitala leveranskedjor är det också enbart en minoritet som kan sägas ha kvalificerat innehåll i arbetssättet. Endast en tredjedel av organisationerna uppger att arbetssättet omfattat *kontroll av att befintlig kravställning av säkerhet i leveranskedjan uppfylls på ett ändamålsenligt sätt* samt *bedömning av om den befintliga kravställningen fortsatt är tillräcklig och ändamålsenlig utifrån organisationens behov*.

Det är också enbart en tredjedel av organisationerna vars arbetssätt inbegripit *uppföljning av inträffade incidenter och störningar i leveransen med orsaksanalys omfattande aktuella delar av leveranskedjan*. 41 procent uppger att arbetssättet omfattat *bedömning av leverantörens fortsatta lämplighet utifrån exempelvis förändrade förutsättningar kring utländskt ägande och/eller skilda jurisdiktioner i leveranskedjan*. Slutligen uppger endast 16 procent att arbetssättet inkluderat *uppföljning av leverantörens och dess underleverantörers arbete med kontinuitetshantering och övning samt förmåga att leverera i kris och höjd beredskap*.

Den sammantagna bild som framkommer är att det finns mycket grundläggande brister avseende uppföljning av säkerhet i digitala leveranskedjor inom offentlig förvaltning. Det mycket svaga resultatet inom arbetsområdet ska också ses i ljuset av att 41 procent av de cyberincidenter som inrapporterades till myndigheten från statliga myndigheter under år 2023 uppges ha inträffat hos en leverantör.[51] Det understryker ytterligare behovet av att organisationer arbetar systematiskt med leveranskedjesäkerhet.

Not 51. Myndigheten för civilt försvar, *EU förändrar cybersäkerhetsområdet – Årsrapport it-incidentrapportering 2023,* s. 30. https://www.mcf.se/sv/publikationer/eu-forandrar-cybersakerhetsomradet--arsrapport-it-incidentrapportering-2023/ (hämtad 01/2026).

4.6 Jämförelse av resultatet i de enskilda mätningarna

Avsnittet jämför resultatet inom Infosäkkollen, It-säkkollen, Ot-säkkollen och Leveranskedjekollen med avseende på områden som berörs i flera av mätningarna. Därefter jämförs hur de olika aktörsgrupperna inom offentlig förvaltning har presterat inom de enskilda mätningarna. Syftet är att belysa gemensamma mönster liksom skillnader.

4.6.1 Typförvaltningens resultat mellan mätningarna

Som framgår av avsnitt 4.2–4.5 undersöks vissa aspekter av det systematiska cybersäkerhetsarbetet inom flera mätningar. Några sådana aspekter är ledningens engagemang, uppföljning och utvärdering, incident- och kontinuitetshantering, upphandling samt riskanalys och riskhantering, vilka samtliga är centrala för hela cybersäkerhetsarbetet.

I vissa mätningar utgör dessa centrala delar av cybersäkerhetsarbetet egna arbetsområden (exempelvis arbetsområdet *Uppföljning och utvärdering* inom Infosäkkollen), medan det i andra mätningarna utgör delar av ett arbetsområde (exempelvis arbetsområdet *Styrning och kontroll* inom It-säkkollen som både följer upp både ledningens styrning och mer generell uppföljning av it-säkerhetsarbetet). Eftersom frågor liksom arbetsområden ser olika ut i olika mätningar kan resultaten inte alltid jämföras rakt av mot varandra. Det går dock att identifiera vissa övergripande mönster.

En för cybersäkerhetsarbetet mycket central och grundläggande aspekt som följs upp i flera mätningar är ledningens engagemang. Vissa specifika frågor ingår även i flera mätningar. På frågan om *ledningen har följt upp informationssäkerhetsarbetet/it-säkerhetsarbetet under de senaste två åren* kan det noteras att typförvaltningen har genomfört samtliga av de åtgärder som undersöks i både Infosäkkollen och It-säkkollen. Även huruvida *ledningen har informerat sig om status på säkerhetsarbetet under de senaste två åren* undersöks inom ramen för både Infosäkkollen, It-säkkollen och Ot-säkkollen. Här kan det noteras att typförvaltningen inom Infosäkkollen har nått ett bättre resultat (fyra av fem genomförda åtgärder kopplat till frågan), medan typförvaltningen inom It-säkkollen och Ot-säkkollen har ett svagare resultat (en av fem genomförda åtgärder respektive noll av fem genomförda åtgärder kopplat till frågan).

Även uppföljning av det systematiska cybersäkerhetsarbetet är en aspekt som behandlas i samtliga mätningar. Resultateten i de enskilda mätningarna visar att detta område är genomgående svagt. Inom både Infosäkkollen och Leveranskedjekollen är det arbetsområde som fokuserar på uppföljning ett av de svagaste arbetsområdena hos typförvaltningen. I båda mätningarna är det också det arbetsområde där typaktörerna för samtliga tre aktörsgrupper har vidtagit det minsta antalet åtgärder. I Leveranskedjekollen är resultatet för *Uppföljning* synnerligen svagt. Vidare framgår att typförvaltningen i Infosäkkollen och It-säkkollen inte har följt upp cirka 40 respektive 30 procent av de arbetssätt som undersöks. För Ot-säkkollen är siffran ännu högre, omkring 60 procent av arbetssätten har inte följts upp.

Vidare undersöks aspekter kopplade till incident- och kontinuitetshantering inom samtliga fyra mätningar. Inom Infosäkkollen tillhör *Incident- och kontinuitetshantering* ett av de två svagaste arbetsområdena för typförvaltningen, som endast har nått nivå 1 inom området. När det gäller motsvarande arbetsområde inom It-säkkollen har typförvaltningen däremot uppnått nivå 3, och inom Leveranskedjekollen har typförvaltningen uppnått nivå 2. I Ot-säkkollen, där typförvaltningen dock enbart når nivå 1 eller högre inom ett fåtal arbetsområden, har typförvaltningen inte uppnått någon nivå för arbetsområdet. Det ojämna resultatet mellan mätningarna kan indikera att incident- och kontinuitetshantering är något som har kommit olika långt inom de olika cyberdomänerna.

Slutligen undersöks aspekter kopplat till upphandling både i Infosäkkollen och Leveranskedjekollen[52]. I Infosäkkollen behandlas dock upphandling i fråga om just informationssäkerhet, medan det i Leveranskedjekollen behandlas bredare. Inom Infosäkkollen tillhör arbetsområdet *Upphandling* ett av de starkaste arbetsområdena och typförvaltningen uppnår nivå 4. Regionerna uppvisar ett synnerligen starkt resultat inom området. Resultatet inom Infosäkkollens arbetsområde *Upphandling* kan jämföras med det övergripande resultatet i Leveranskedjekollen, som visar att typförvaltningen saknar grunderna i ett systematiskt leveranskedjesäkerhetsarbete.

4.6.2 Aktörsgruppernas resultat mellan mätningarna

Vissa jämförelser kan även göras mellan aktörsgruppernas prestation inom de enskilda mätningar som Cybersäkerhetskollen består av. Då närmare 90 procent av deltagarna i Ot-säkkollen utgjordes av kommuner är det dock inte möjligt att analysera aktörsgruppernas enskilda resultat på samma vis för denna mätning, som de övriga.

I både Infosäkkollen, It-säkkollen och Leveranskedjekollen är myndigheterna den aktörsgrupp som, med ett fåtal undantag, presterar starkast. Inom samtliga av dessa mätningar är myndigheterna den aktörsgrupp där den största andelen (61, 63 respektive 39 procent) har uppnått övergripande nivå 1 eller högre. Inom både Infosäkkollen, It-säkkollen och Leveranskedjekollen är myndigheterna även den aktörsgrupp som genomfört flest antal åtgärder, jämfört med övriga aktörsgrupper. Den bild som framkommer är därför att myndigheterna är den aktör inom offentlig förvaltning som är starkast i fråga om systematiskt cybersäkerhetsarbete.

Not 52. Frågor som undersöker arbetssätt om utkontraktering av it-tjänster hanteras i Leveranskedjekollen. It-säkkollen undersöker endast informationssystem och nätverk och it-tjänster som sköts i egen regi.

Medan kommunerna genomgående är den svagast presterande aktörsgruppen i Infosäkkollen, presterar kommunerna bättre i It-säkkollen och Leveranskedjekollen i förhållande till övriga aktörsgrupper. Inom Infosäkkollen är andelen kommuner (30 procent) som når övergripande nivå 1 eller högre noterbart mindre än övriga två aktörsgrupper (54 respektive 61 procent). Inom både It-säkkollen och Leveranskedjekollen är det i stället en högre andel kommuner än regioner som når övergripande nivå 1 eller högre, även om skillnaden mellan kommuner och regioner är mindre betydande.[53]

Att kommunerna, relativt sett, presterar bättre i It-säkkollen och Leveranskedjekollen tydliggörs också när man beaktar antal genomförda åtgärder. I Infosäkkollen har typkommunen vidtagit betydligt färre åtgärder än övriga två aktörsgrupper. Inom It-säkkollen har typkommunen däremot genomfört noterbart fler åtgärder än typregionen. I Leveranskedjekollen presterar typkommunen och typregionen likvärdigt i fråga om totalt antal genomförda åtgärder. Resultatet är svårtolkat. Detta eftersom det inte går att belägga om det handlar om att kommunerna är i synnerligen svaga i förhållande till andra aktörsgrupper inom informationssäkerhetsarbetet alternativt om det är regionerna som, i jämförelse med övriga aktörsgrupper, är svaga inom it-säkerhets- och leveranskedjesäkerhetsarbete.

4.7 Resultatet från enkätundersökningen

Den 23 september 2025 skickade myndigheten ut en enkät om Cybersäkerhetskollen 2025 till samtliga deltagare. Deltagande i enkäten var frivilligt och enkäten var öppen till den 7 oktober 2025. Enkäten syftade till att öka myndighetens förståelse för deltagares synpunkter på Cybersäkerhetskollen i fråga om sakinnehåll, användning och upplevd nytta. Den syftade även till att utreda organisationernas förutsättningar att arbeta systematiskt med cybersäkerhet, vilket bidrar till en fördjupad förståelse av de resultat som presenteras i avsnitt 4.1–4.5. Svaren var anonyma.

Totalt svarade 165 deltagare på enkäten, varav 159 representerade offentliga förvaltningar.[54] Eftersom antalet deltagande bolag var så pass få har svaren från dessa exkluderats från redogörelsen nedan.[55] Representationen bland respondenterna bestod av cirka 55 procent kommuner (motsvarande 87 stycken), 40 procent myndigheter (motsvarande 63 stycken) och 6 procent (motsvarande nio stycken).

Not 53. I It-säkkollen nådde 33 procent av kommunerna övergripande nivå 1 eller högre, medan motsvarande siffra hos regionerna var 29 procent. Inom Leveranskedjekollen nådde 25 procent av kommunerna och 20 procent av regionerna övergripande nivå 1 eller högre.

Not 54. Det vill säga drygt hälften av de som deltog i Cybersäkerhetskollen 2025. 2024 besvarade totalt 165 enkätutvärderingen av Infosäkkollen och It-säkkollen 2024, varav 83 kommuner, 7 regioner samt 76 statliga myndigheter.

Not 55. Bolag exkluderades av samma anledning även från presentationen av resultaten från enkätundersökningen i Cybersäkerhetskollen 2024.

Majoriteten av respondenterna hade rollen som CISO/informations-säkerhets-samordnare. Andra vanligt förekommande roller var it-chefer, it-strateger. informationssäkerhetsstrateger och säkerhetsskyddschefer.

Nedan redogörs för de svar som berör organisationernas förutsättningar att bedriva ett systematisk cybersäkerhetsarbete. Det görs även en kommentar om hur resultatet förhåller sig till enkätutvärderingen av Cybersäkerhetskollen 2024.

4.7.1 Förutsättningar för att bedriva ett systematiskt cybersäkerhetsarbete

Gällande i vilken utsträckning respondenterna arbetar med cybersäkerhet svarade 40 procent *heltid*, 6 procent angav *cirka 75 procent*, 20 procent angav *cirka 50 procent* och 35 procent angav *cirka 25 procent.* Andelen som uppgav att man arbetar heltid med cybersäkerhet har minskat med tre procentenheter i förhållande till 2024 års enkätuvärdering, samtidigt som andelen som uppger att man arbetar cirka 75 procent har ökat något. Frågan rörde dock endast respondenten (den svarande rollen). Det kan därmed finnas ytterligare kollegor i organisationen som arbetar med frågorna i större utsträckning än vad respondenten gör.

På frågan om samma kollegor är ansvariga för organisationens cybersäkerhetsarbete som för två år sedan uppgav 23 procent *ja, alla medarbetare är kvar*, 33 procent *de flesta medarbetarna är kvar*, 32 procent *nej, vi har haft viss personalomsättning* och 12 procent *nej, vi har haft omfattande personalomsättning*. Siffrorna är svårtolkade då Myndigheten för civilt försvar saknar uppgifter om vad som utgör en normal personalomsättning inom branschen och tidsspannet. Det är dock positivt att andelen som uppgett att man haft viss respektive omfattande personalomsättning har minskat med totalt sex procentenheter i förhållande till 2024 års enkätundersökning.

Myndigheten för civilt försvar undersökte även deltagarnas syn på huruvida organisationen har de resurser och den kompetens som krävs för att förbättra cybersäkerhetsarbetet.

I fråga om organisationen har den personal som krävs för att förbättra cyber-säkerhetsarbetet uppgav 20 procent *stämmer inte*, 45 procent *stämmer knappt,* 31 procent *stämmer väl*, 4 procent *stämmer helt*. Andelen som besvarat påståendet med stämmer väl respektive stämmer helt har minskat med cirka fyra procent-enheter jämfört med resultatet i enkätutvärderingen 2024.

Gällande frågan om organisationen har den kompetens som krävs uppgav 6 procent *stämmer inte*, 35 procent *stämmer knappt*, 51 procent *stämmer väl*, 9 procent *stämmer helt*. Andelen som har uppgett att påståendet stämmer knappt respektive stämmer inte har minskat med tre procentenheter, vilket är att betrakta som en marginell förändring.

På frågan om organisationens högsta ledning har det engagemang som krävs för att förbättra cybersäkerhetsarbetet svarade 8 procent *stämmer inte*, 31 procent *stämmer knappt*, 47 procent *stämmer väl*, 14 procent *stämmer helt*. Att 61 procent av respondenterna uppger att deras högsta ledning har det engagemang som krävs för att förbättra cybersäkerhetsarbetet (*stämmer väl och stämmer helt*) motsvarar en förbättring om åtta procentenheter i förhållande till 2024 års utvärdering.

Sammantaget kan det konstateras att fördelningen av svar liknar fördelningen som framkom i 2024 års enkätutvärdering. Även om förändringen jämfört med enkätutvärderingen 2024 är liten pekar den i positiv riktning. Den enda fråga där utvecklingen är negativ gäller den fråga som berör huruvida organisationen har den personal som krävs för att förbättra cybersäkerhetsarbetet. Att enbart 31 procent respektive 4 procent uppgav *stämmer väl* respektive *stämmer helt* är också att betrakta som ett mycket svagt resultat. Det indikerar ett stort behov av att tillsättande av resurser också leder till tillsättning av den personal som krävs.

Den största förbättringen har skett gällande andelen som uppger att organisationens ledning har det engagemang som krävs för att förbättra cybersäkerhetsarbetet. Detta resultat ska även tolkas i ljuset av att *Ledningens styrning och kontroll* har utgjort det arbetsområde där minst antal organisationer har uppgett nivå 1 eller högre vid de senaste genomförandena av Infosäkkollen. Många av frågorna i Cybersäkerhetskollen ställer krav på att en åtgärd har funnits på plats i minst två år. Resultatet kan indikera en förbättring gällande ledningens engagemang i cybersäkerhetsarbetet som ännu inte genererat utslag i resultatet av Cybersäkerhetskollen.

Kapitel 5

Utvecklingen framåt

5. Utvecklingen framåt

Det saknas tecken på att det allvarliga säkerhetspolitiska läget kommer att förbättras inom en närstående framtid. Cybersäkerhet utgör en grundpelare i Sveriges motståndskraft och därigenom totalförsvarsförmåga. De allvarliga brister i det systematiska cybersäkerhetsarbetet som framkommit i Cybersäkerhetskollen 2025 utgör en sårbarhet som kräver åtgärder från ansvariga samhällsviktiga verksamhetsutövare.

Andelen organisationer som identifieras som samhällsviktiga i cybersäkerhetslagen respektive svarsunderlaget i Cybersäkerhetskollen skiljer sig samtidigt mycket åt. Medan majoriteten av de organisationer som omfattas av cybersäkerhetslagen finns inom det privata näringslivet, var den stora majoriteten av deltagarna i Cybersäkerhetskollen 2025 offentliga förvaltningar. För att kunna redogöra för nivån på det systematiska cybersäkerhetsarbetet i Sverige krävs ett ökat deltagande från privata företag. Utan deltagande från fler verksamhetsutövare i enlighet med cybersäkerhetslagen i framtida mätningar, riskerar de slutsatser och rekommendationer som tas fram på basis av resultatet att bli felaktiga.

Behovet av att stärka cybersäkerhetsarbetet avspeglas även i ny lagstiftning. Cybersäkerhetslagen, som trädde i kraft den 15 januari 2026, ställer mer långtgående krav på samhällsviktiga verksamheters cybersäkerhetsarbete än tidigare. Några exempel på skyldigheter gäller styrning av säkerhetsarbetet liksom riskhantering. Säkerhetsåtgärder ska utgå från ett allriskperspektiv och säkerställa en nivå på säkerheten i nätverks- och informationssystem som är lämplig i förhållande till risken. I propositionen till lagen tydliggörs att ledningen ansvarar för säkerhetsåtgärder och att det inte behöver skrivas ut särskilt i cybersäkerhetslagen.[56] Ingripandeåtgärderna som följer av cybersäkerhetslagen har även skärpts. I det fall verksamhetsutövare inte lever upp till skyldigheterna som följer av lagen eller tillhörande beslutade föreskrifter kan tillsynsmyndigheter komma att exempelvis besluta om sanktionsavgift.

I syfte att åstadkomma en strategisk samt operativ förmågehöjning på cybersäkerhetsområdet på nationell nivå, liksom för att åstadkomma en samlad och samordnad nationell styrning inom cybersäkerhetsarbetet beslutade regeringen den 20 november 2025 att Myndigheten för civilt försvars centrala verksamheter inom cybersäkerhet ska föras över till Nationellt cybersäkerhetscenter, vilket utgör en del av Försvarets radioanstalt (FRA). Verksamhetsövergången ska genomföras

Not 56. Regeringen, proposition 2025/26:28 Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag, s. 98. https://www.regeringen.se/rattsliga-dokument/proposition/2025/10/prop.-20252628 (hämtad 2026/02).

den 1 juli 2026 och innefattar även de regeringsuppdrag som Cybersäkerhetskollen vilar på. Det innebär att Nationellt cybersäkerhetscenter (NCSC) kommer överta ansvaret för Cybersäkerhetskollen från och med sommaren 2026. Regeringens ambition är att NCSC ska utgöra navet i det nationella cybersäkerhetsarbetet.

EU har under de senaste åren lanserat flera initiativ i syfte att stärka cybersäkerheten i unionen, bland annat genom flera regleringar såsom cyberresiliensförordningen (CRA) och NIS2 (som Sverige nu implementerat genom cybersäkerhetslagen). Ett ytterligare exempel är verktygslådan för säkerhet i digitala leveranskedjor[57], vilken publicerades i februari 2026. Verktygslådan, som har tagits fram av EU-kommissionen och medlemsstaterna, syftar till att stärka och harmonisera medlemsstaternas insatser för att identifiera, bedöma och hantera risker kopplade till digitala leveranskedjor.

Nytt för Cybersäkerhetskollen 2025 var lanseringen av fullskalig version av It-säkkollen, samt två helt nya mätningar: Ot-säkkollen och Leversanskedjekollen. Dessa har utvärderats inom ramen för bland annat enkätutvärderingen av Cybersäkerhetskollen 2025. Till nästa genomförande kommer innehållet i Cybersäkerhetskollen ses över baserat på inkomna synpunkter liksom de krav som följer av cybersäkerhetslagen och tillhörande föreskrifter.

Närmare stöd inom it-säkerhet, ot-säkerhet och säkerhet i digitala leveranskedjor kommer tas fram i syfte att säkerställa att det möter verksamhetsutövares behov. Vid utformningen av stödet är resultatet i Cybersäkerhetskollen vägledande.

Nästa mätning av Cybersäkerhetskollen sker under 2027. Givet den ökade aktiviteten och negativa utvecklingen på cybersäkerhetsområdet de senaste åren samt att tecken på ett förbättrat omvärldsläge saknas, är det centralt att det systematiska cybersäkerhetsarbetet hos de samhällsviktiga verksamhetsutövare som Sverige är beroende av prioriteras högre. För att Sverige ska stå redo för kris och krig måste motståndskraften förbättras, och det omgående.

Not 57. EU-kommissionen, EU ICT Supply Chain Security Toolbox. https://digital-strategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security (hämtad 2026/02).

Myndigheten
för civilt försvar