Anmälda personuppgiftsincidenter 2019

Datainspektionens rapport 2020:2

Datainspektionen

Anmälda personuppgiftsincidenter 2019
Denna rapport finns att ladda ner på www.datainspektionen.se

Innehåll

Inledning

Genom dataskyddsförordningen[1] (GDPR) infördes den 25 maj 2018 en skyldighet för privata och offentliga verksamheter som behandlar personuppgifter att rapportera vissa personuppgiftsincidenter till Datainspektionen. Den 1 augusti 2018 infördes i brottsdatalagen motsvarande anmälningsskyldighet för brottsbekämpande myndigheter.

Denna rapport beskriver anmälda personuppgiftsincidenter under 2019. Rapporten innehåller två delar. Den första delen beskriver hur anmälda incidenter fördelar sig mellan olika samhällssektorer, vad det är för typ av incidenter och vad den organisation som anmält uppger är skälet till att incidenten inträffat. Här beskrivs också förändringar mellan 2018 och 2019. Rapportens andra del redovisar statistik över anmälda personuppgiftsincidenter nedbrutet på olika samhällssektorer.

Rapporten är en del av Datainspektionens rapportserie där vi beskriver och analyserar inflödet till myndigheten.[2] Syftet med att beskriva generella mönster och iakttagelser från inflödet till Datainspektionen är att ge ett underlag som privata och offentliga verksamheter kan använda i sitt fortsatta dataskyddsarbete och bidra till en generell kunskapshöjning om integritet och dataskydd.

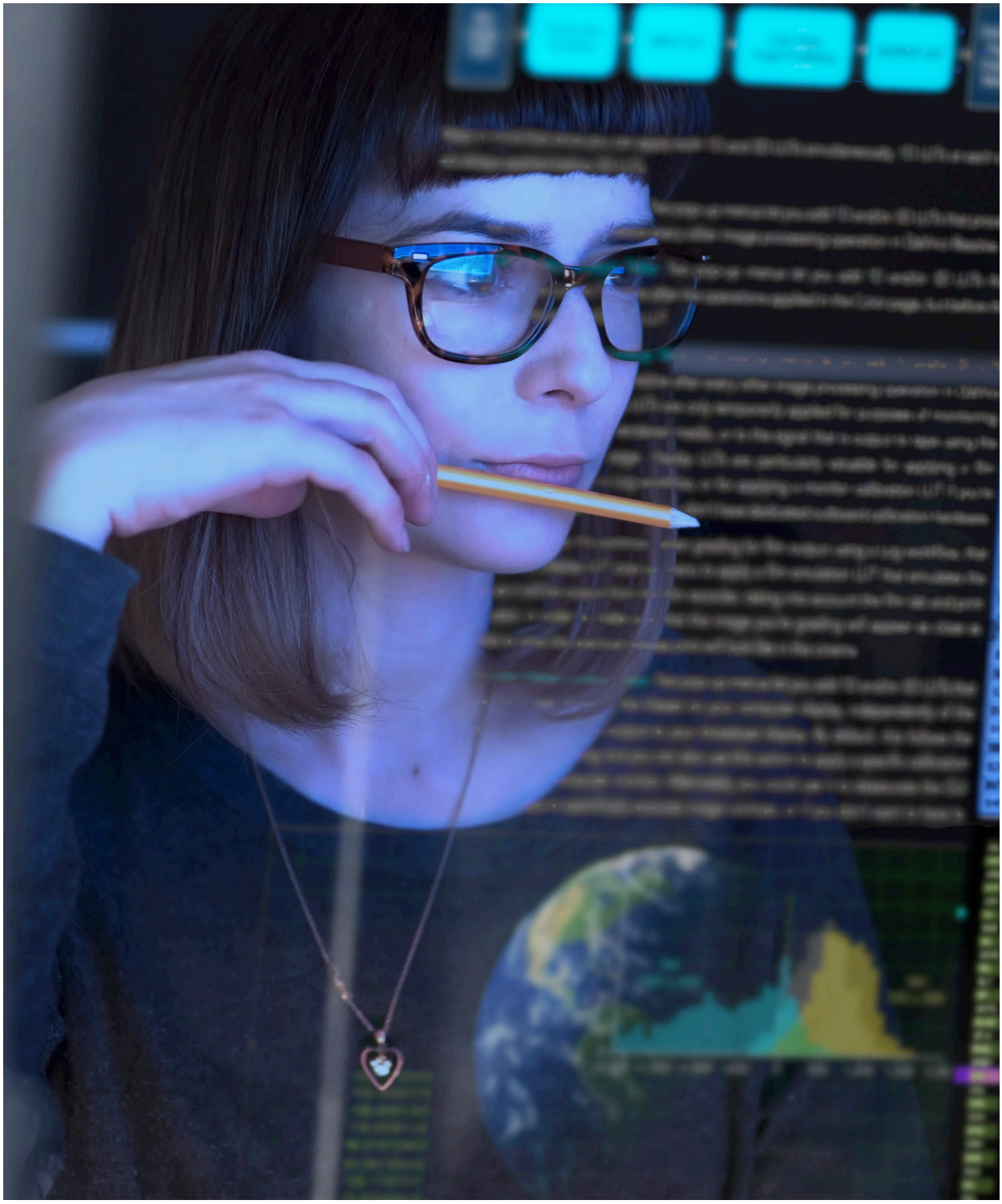
1 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

2 Tidigare rapporter i rapportserien behandlar anmälda personuppgiftsincidenter 2018 (2019:1), anmälda personuppgiftsincidenter januari-september 2019 (2019:3) och klagomål mot personsöktjänster med frivilligt utgivningsbevis (2020:1).

Sammanfattning

- Antalet anmälda personuppgiftsincidenter per månad har ökat 2019 jämfört med 2018. Under 2019 fick Datainspektionen totalt in knappt 4 800 anmälningar om personuppgiftsincidenter, vilket motsvarar cirka 400 anmälda incidenter per månad. 2018 anmäldes cirka 320 incidenter per månad. Ökningen per månad motsvarar 23 procent mellan åren.
- Offentlig sektor står för den största ökningen av anmälda incidenter, i synnerhet statliga myndigheter och hälso- och sjukvården. Båda dessa sektorer anmälde under 2019 dubbelt så många incidenter i snitt per månad jämfört med 2018.
- Inom privat och ideell sektor är antalet anmälda incidenter per månad under 2019 relativt oförändrat jämfört med 2018. Undantaget är finansiell sektor, där antalet anmälda incidenter minskat. Detta beror primärt på att det under 2018 skedde en överrapportering från vissa aktörer inom finans- och försäkringsbranschen, det vill säga att icke-anmälningspliktiga incidenter anmäldes.
- Datainspektionens bedömning är att ökningen av antalet anmälda incidenter i stor utsträckning beror på att rutinerna för att rapportera incidenter internt och anmäla dem till Datainspektionen blivit mer etablerade, i synnerhet inom offentlig sektor.
- Den vanligaste incidenten 2019 är, liksom föregående år, felskickade e-postmeddelanden eller brev, som utgör drygt en tredjedel av incidenterna.
- Den vanligaste orsaken till de anmälda incidenterna är fortsatt den mänskliga faktorn, som uppges ha orsakat hälften av de anmälda incidenterna 2019.
- Det finns relativt stora skillnader mellan olika samhällssektorer avseende vilken typ av incidenter som anmäls och vad som uppges ha orsakat dem. En förklaring till skillnaderna är mängden utskick av personuppgifter som görs i den aktuella verksamheten. I verksamheter som skickar stora mängder brev eller e-post är den vanligaste incidenten genomgående felskickade brev. I verksamheter där personuppgifter främst hanteras i interna it-system eller system som medborgare loggar in i är den vanligaste incidenten istället obehörig åtkomst.

- Även om rutinerna för att anmäla och upptäcka incidenter tycks ha förbättrats under 2019 jämfört med 2018 är Datainspektionens bedömning att det i Sverige fortfarande finns ett stort mörkertal i form av anmälningspliktiga incidenter som inte anmäls. Bedömningen baseras bland annat på utvecklingen i andra EU-länder där anmälningsskyldigheten för personuppgiftsincidenter funnits längre.



Vad är en personuppgiftsincident och varför ska den anmälas till Datainspektionen?

En personuppgiftsincident är en säkerhetsincident som rör personuppgifter. Incidenten kan till exempel handla om att personuppgifter har blivit förstörda eller ändrade, gått förlorade eller kommit i orätta händer. Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. I båda fallen är det personuppgiftsincidenter.

En personuppgiftsincident kan innebära risker för den vars personuppgifter det handlar om. Riskerna kan handla om till exempel identitetsstöld, bedrägeri, finansiell förlust, diskriminering eller skadlig ryktesspridning. Om det *inte är osannolikt* att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter ska den anmälas till Datainspektionen inom 72 timmar från att den upptäckts.

Om det finns en *hög risk* att privatpersoners fri- och rättigheter kan påverkas till följd av en personuppgiftsincident är den ansvariga verksamheten skyldig att – förutom att anmäla det inträffade till Datainspektionen – också informera de registrerade om att incidenten inträffat. Det ger den enskilde möjlighet att vidta egna åtgärder, till exempel att byta lösenord. Även när en incident inte anmäls ska den alltid dokumenteras internt.

Del 1.
Personuppgiftsincidenter 2019

Anmälda personuppgiftsincidenter

Datainspektionen fick under perioden 1 januari – 31 december 2019 in totalt 4 757 anmälningar om personuppgiftsincidenter, varav 55 incidenter avser brottsdatalagen. Antalet anmälningar minskade kraftigt under semesterperioden, för att sedan återgå till högre nivåer under hösten.

Antal anmälda personuppgiftincidenter per vecka 2019

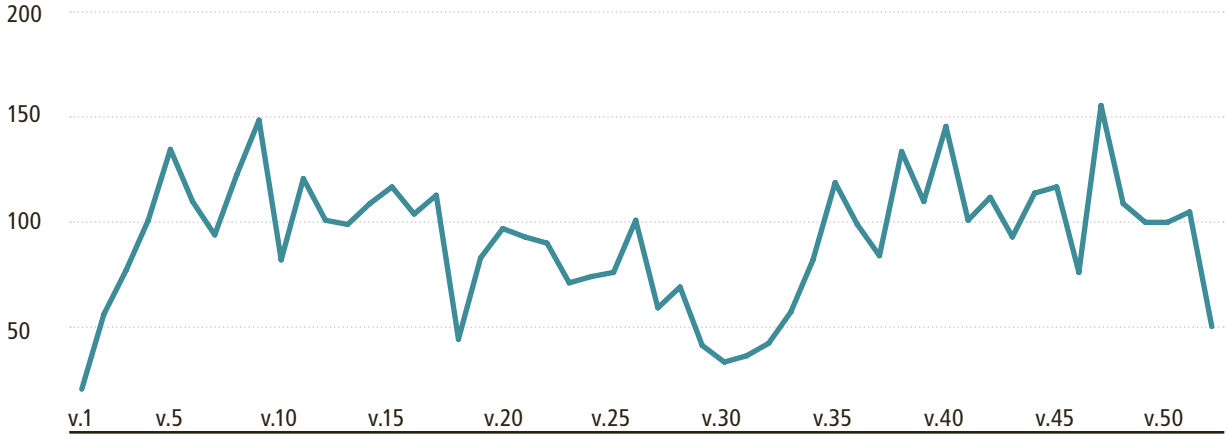


Bild 1. Antal anmälda personuppgiftsincidenter per vecka 2019.

Den absoluta merparten av de incidenter som anmälts under 2019 bedöms utgöra reella personuppgiftsincidenter. Samtidigt gör Datainspektionen bedömningen att det i Sverige fortfarande finns ett stort mörkertal i form av anmälningspliktiga incidenter som inte anmäls. Anmälningsplikten är fortfarande förhållandevis ny, och rutinerna för att upptäcka och anmäla incidenter inte fullt ut etablerade, vilket kan påverka såväl antal som vilka incidenter som anmäls till Datainspektionen.

Erfarenheter från andra EU-länder, där anmälningsskyldigheten för personuppgiftsincidenter i vissa fall funnits längre, tyder också på att antalet anmälningar kan öka över tid. I Nederländerna, där anmälningsskyldigheten infördes år 2016, ökade antalet anmälda incidenter kraftigt varje år under den första treårsperioden. Under 2019 uppgick det totala antalet incidentanmälningar i Nederländerna till cirka 25 000.

Vid en internationell jämförelse av anmälda incidenter per 100 000 invånare placerar sig Sverige på åttonde plats, med 57 anmälda incidenter per 100 000 invånare. Flest anmälningar har Nederländerna med 147

incidenter per 100 000 invånare, följt av Irland med 133 och därefter Danmark med 115 incidenter.[3] Att Nederländerna och Danmark har ett stort antal anmälda incidenter per invånare beror sannolikt bland annat på att länderna sedan tidigare haft skyldighet att rapportera incidenter. Även Irland har sedan 2011 haft frivillig incidentanmälan.

Eftersom incidenter ska anmälas till det land där ett företag har sitt huvudkontor, ökar också antalet anmälningar i länder där många internationella företag finns, vilket är fallet till exempel på Irland. Andra faktorer som kan påverka antalet incidentanmälningar är den nationella dataskyddsmyndighetens arbete, både i form av vägledningar, tillsyn och administrativa sanktionsavgifter. Även olika länders tradition och erfarenhet av inrapportering till statliga myndigheter kan spela in.

Fördelning på olika samhällssektorer

Av de incidenter som anmäldes 2019 kom totalt 61 procent från offentlig sektor eller verksamheter med offentligt uppdrag (hälso- och sjukvård, kommun, skola eller socialtjänst). Motsvarande siffra för 2018 var 46 procent.

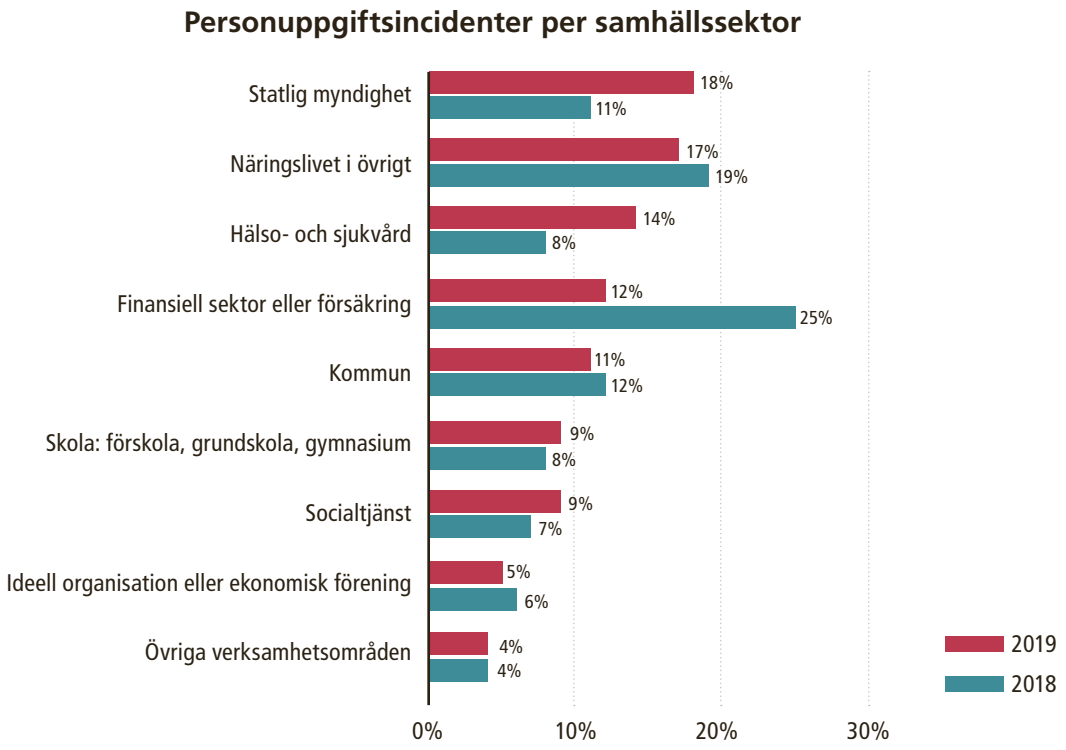


Bild 2. Andel personuppgiftsincidenter per samhällssektor 2018 och 2019.

3 Rapport från den Nederländska dataskyddsmyndigheten januari 2020. DLA Piper GDPR Data Breach Survey: January 2020

Eftersom anmälningsskyldigheten infördes den 25 maj 2018 finns inga jämförbara helårssiffror över antal anmälda incidenter mellan 2018 och 2019. En jämförelse kan istället göras i antalet anmälda incidenter per månad.

	2018	2019	Differens/antal
Statliga myndigheter	36	67	31
Hälso- och sjukvård	26	55	29
Socialtjänst	23	33	10
Skola	26	36	10
Kommuner	39	45	6
Näringslivet i övrigt	61	67	6
Övriga verksamheter	13	16	3
Ideella organisationer	19	21	2
Finansiell sektor/försäkring	81	48	-33

Tabell 1. Antal anmälda personuppgiftsincidenter i genomsnitt per månad per samhällssektor, 2018 och 2019. Sektorerna redovisas efter störst genomsnittlig ökning i antal anmälda incidenter per månad.

Ökningen av antalet anmälningar från offentlig sektor bedöms bero på ett flertal faktorer. Många verksamheter i offentlig sektor behandlar stora mängder personuppgifter och ofta känsliga personuppgifter, vilket kan bidra till att fler incidenter betraktas som anmälningspliktiga vid riskbedömningen. Den främsta förklaringen är sannolikt att rutinerna blivit mer etablerade för att rapportera incidenter internt och anmäla dem till Datainspektionen. Även att det under 2019 skett flera incidenter i offentlig sektor som fått stor massmedial uppmärksamhet kan ha bidragit till en ökad medvetenhet och anmälningsbenägenhet.

Att en organisation eller en bransch anmäler många personuppgiftsincidenter behöver inte nödvändigtvis vara en indikation på bristande säkerhet. Ofta kan det tvärtom tyda på att verksamheten har strukturer och rutiner som ger en god förmåga att upptäcka och rapportera personuppgiftsincidenter.

Inom finans- och försäkringsbranschen har antalet anmälningar per månad minskat kraftigt 2019 jämfört med 2018. Minskningen bedöms i första hand bero på den överrapportering som skedde från en finansiell aktör direkt efter att anmälningsskyldigheten infördes. Inom näringslivet i övrigt och den ideella sektorn har antalet anmälningar per månad ökat marginellt.

Typ av incident

Den största delen av de anmälda incidenterna utgörs av **felaktiga brevutskick**, det vill säga brev eller e-post som innehåller personuppgifter och oavsiktligt hamnat hos fel mottagare. Andelen felaktiga brevutskick utgjorde under 2019 drygt en tredjedel av samtliga anmälda incidenter.

Obehörig åtkomst är den näst största kategorin av anmälda personuppgiftsincidenter och utgjorde under 2019 knappt en fjärdedel av anmälningarna. Obehörig åtkomst handlar om att någon olovligen berett sig tillgång till personuppgifter, till exempel genom att behörigheter till ett it-system har tilldelats felaktigt eller för generellt. Även så kallade phishingattacker[4] är vanligt förekommande i kategorin obehörig åtkomst. Ett annat återkommande exempel är att det upptäcks att personuppgifter har funnits tillgängliga på en gemensam lagringsyta utan behörighetsstyrning.

Obehörigt röjande står för knappt en fjärdedel, 23 procent, av anmälningarna 2019. Obehörigt röjande innebär att den personuppgiftsansvarige eller någon under den personuppgiftsansvariges ledning hanterat personuppgifter på ett sätt så att de kommit till obehörigas kännedom. Det kan till exempel handla om att personuppgifter avsiktligt eller oavsiktligt röjts för någon som saknar behörighet att ta del av dem eller att brister i ett tekniskt system gör att stora mängder personuppgifter kommit till fel mottagares kännedom.

Stöld och förlust utgör en relativt liten andel av anmälningarna, endast 11 procent. De anmälda incidenterna kan till exempel vara att tjänstedatorer glömts i kollektivtrafiken, att organisationen haft inbrott eller varit utsatta för ett antagonistiskt angrepp genom till exempel malware[5] eller hacking.[6] Även om dessa incidenter är förhållandevis få till antalet är det typiskt sett större grupper av registrerade som berörs.

De förändringar som finns i statistiken mellan 2018 och 2019 när det gäller vilken typ av incidenter som anmäls och vad de uppges bero på bedöms i huvudsak bero på att överrapporteringen från finansiell sektor minskat under 2019. Överrapporteringen bestod av ett stort antal felskickade brev som berodde på mänsklig faktor.

4 Phishing eller nätfiske är en metod för IT-brottslighet där internetanvändare luras att lämna ut känslig information som sedan kan användas till bedrägerier.

5 Malware eller Sabotageprogram är skadlig programvara som installeras på en dator eller nätverk utan användarens samtycke för att till exempel samla in information.

6 Hacking innebär att någon bryter sig in i it-system utan användarens samtycke eller vetskap.

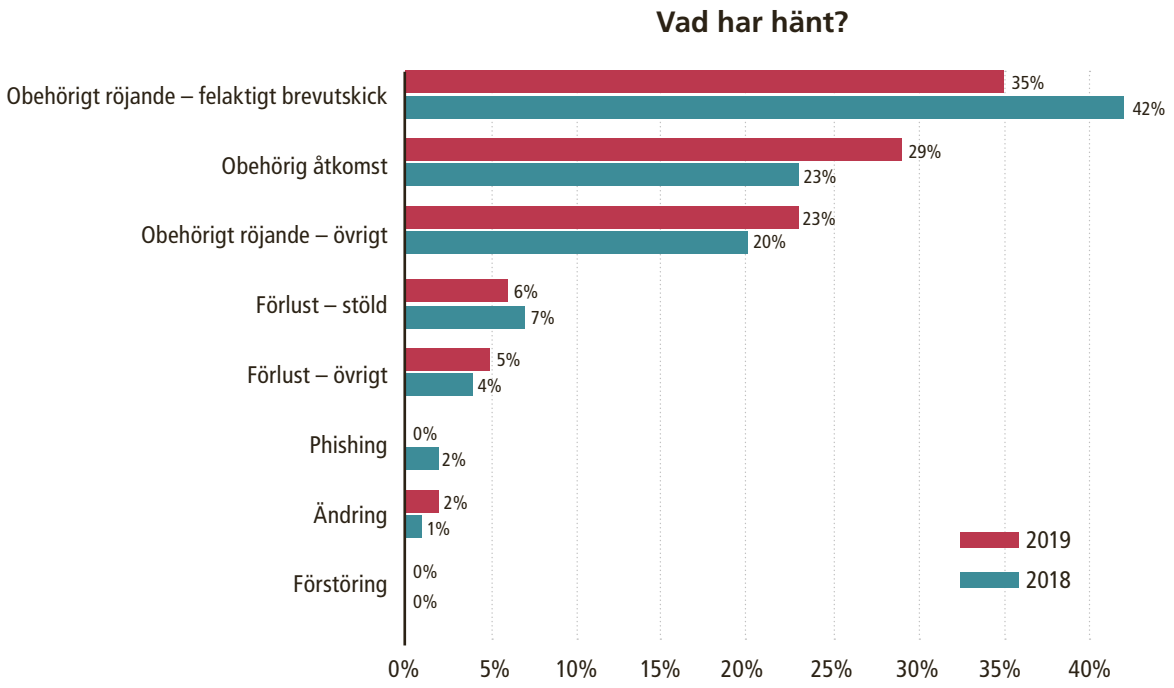


Bild 3. Andel av incidenterna fördelat på typ av incident 2018 och 2019.

Varför inträffade incidenten?

Den **mänskliga faktorn** utgör den vanligaste orsaken till anmälda personuppgiftsincidenter. I drygt hälften av de incidentanmälningar som inkom under 2019 angavs den mänskliga faktorn som förklaring. Incidenter som beror på den mänskliga faktorn består i huvudsak av individer som begått ett misstag vid hantering av personuppgifter i sina verksamheter. Det kan också handla om att individer, medvetet eller omedvetet, inte följer interna rutiner för hantering av personuppgifter. Omkring hälften av de incidenter som beror på den mänskliga faktorn handlar om felskickade brev och e-postmeddelanden.

Tekniska fel uppgavs vara orsaken till 16 procent av alla incidenter 2019, medan **antagonistiska angrepp** och **brister i organisatoriska rutiner och processer** stod för 13 respektive 12 procent.

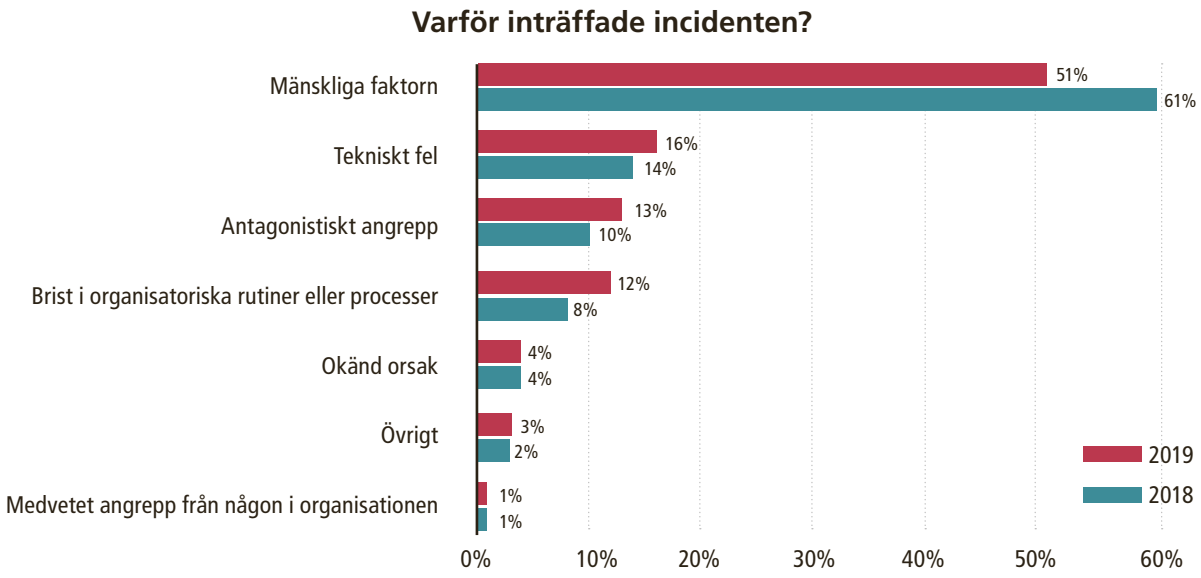


Bild 4. Andel av incidenterna fördelat på orsak 2018 och 2019.

Del 2.
Skillnader mellan olika samhällssektorer

Det finns relativt stora skillnader mellan olika samhällssektorer när det gäller vilka incidenter som anmäls och orsakerna till dem. Skillnaderna speglar i stor utsträckning vilken typ av verksamhet som bedrivs inom respektive sektor. I verksamheter som i stor omfattning hanterar och distribuerar personuppgifter i e-post eller brev, är den vanligaste incidenten felskickade brev. Inom samhällssektorer där personuppgifter främst hanteras i interna eller externa system, är den vanligaste incidenten i stället obehörig åtkomst.

Samhällssektorer där felaktiga brevutskick utgör den vanligaste incidenten är statliga myndigheter, finansiell sektor och försäkring, socialtjänsten, ideella organisationer samt hälso- och sjukvården.

Inom näringslivet i övrigt, kommuner och skolor är istället den vanligast förekommande incidenten som anmäls obehörig åtkomst. Verksamheterna behandlar mycket personuppgifter men hanteringen sker i stor utsträckning i interna system eller digitala lösningar mot medborgare och kunder. Inom skolan handlar det många gånger om olika digitala verktyg och plattformar för kommunikation med föräldrar där skolresultat och annan information dokumenteras.

Anmälda incidenter per samhällssektor

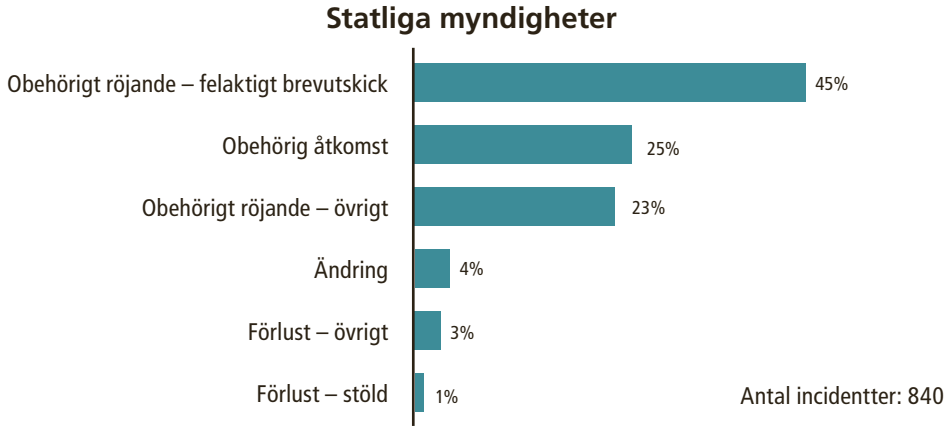


Bild 5. Fördelning av incidenter inom statliga myndigheter 2019.

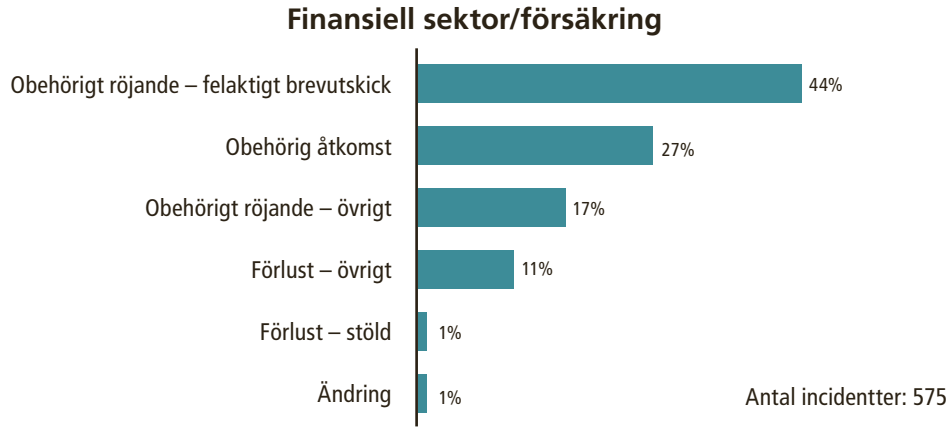


Bild 6. Fördelning av incidenter inom finansiell sektor och försäkring 2019.

Bild 7. Fördelning av incidenter inom socialtjänsten 2019.

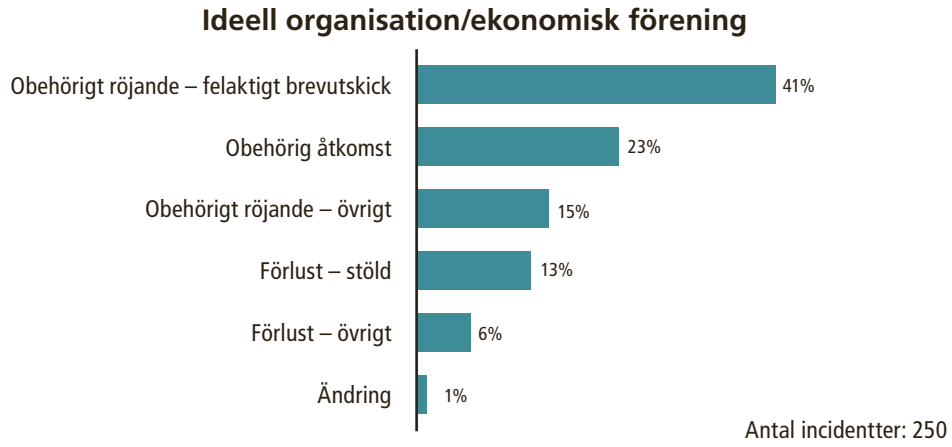


Bild 8. Fördelning av incidenter inom ideella organisationer och ekonomiska föreningar 2019. I sektorn ingår bland annat idrottsföreningar, trossamfund och fackförbund.

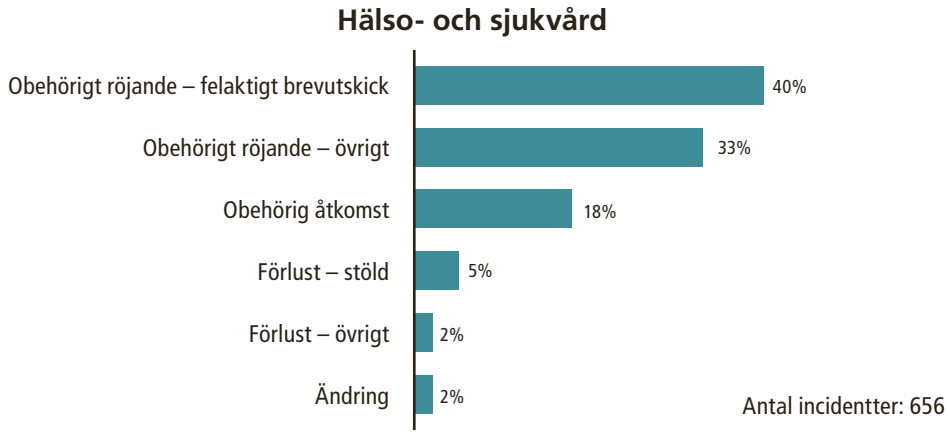


Bild 9. Fördelning av incidenter inom hälso- och sjulvård 2019.

Bild 10. Fördelning av incidenter inom näringslivet i övrigt 2019.

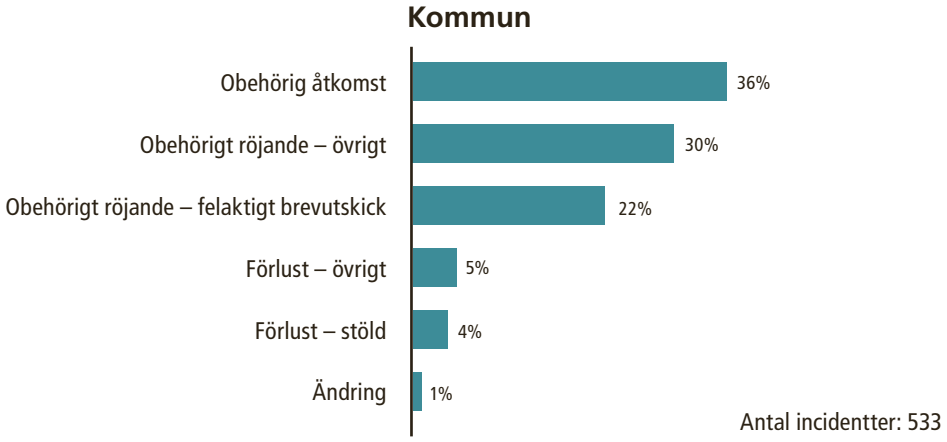


Bild 11. Fördelning av incidenter inom kommuner 2019.

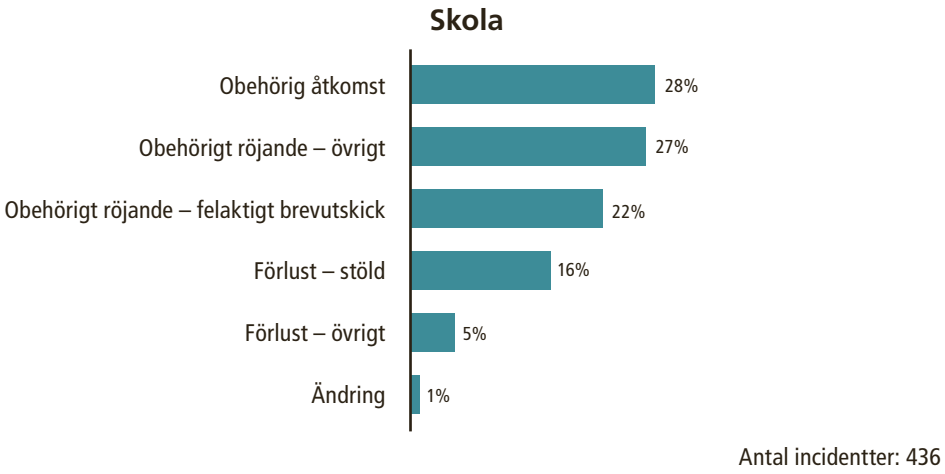


Bild 12. Fördelning av incidenter inom skolan 2019.

Orsaker till anmälda incidenter per samhällssektor

Inom i stort sett samtliga samhällssektorer utgör den mänskliga faktorn den vanligaste orsaken till de anmälda incidenterna. Andelen incidenter som orsakas av mänsklig faktor varierar dock i storlek mellan sektorerna. Hälso- och sjukvården uppger i störst utsträckning att anmälda incidenter orsakats av den mänskliga faktorn, sju av tio incidenter inom uppges bero på detta.

För statliga myndigheter, ideella organisationer och socialtjänsten uppges omkring sex av tio incidenter bero på den mänskliga faktorn. Gemensamt för verksamheterna är att de hanterar och distribuerar stora mängder personuppgifter via e-post och brev, där den mänskliga faktorn är den vanligaste orsaken till felutskick.

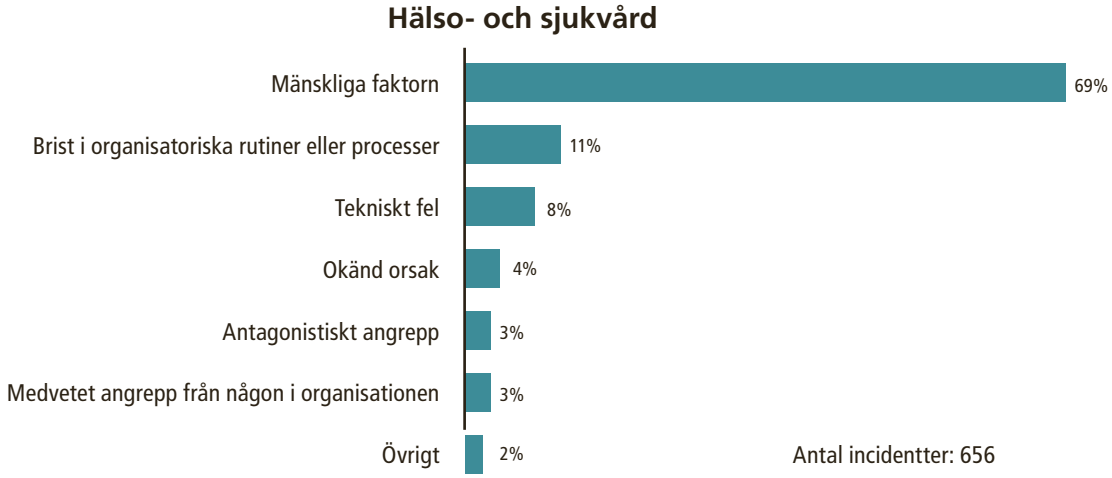


Bild 13. Fördelning av orsaker till incidenterna inom hälso- och sjukvården 2019.

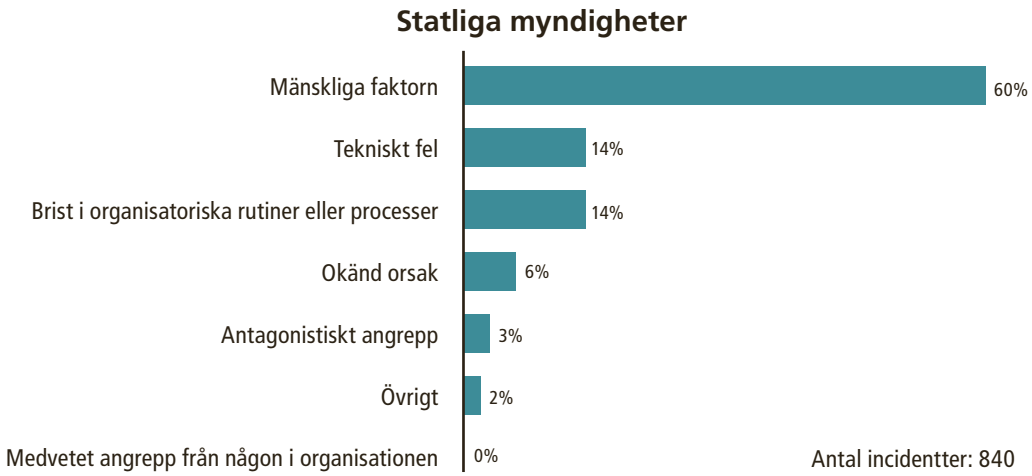


Bild 14. Fördelning av orsaker till incidenterna inom statliga myndigheter 2019.

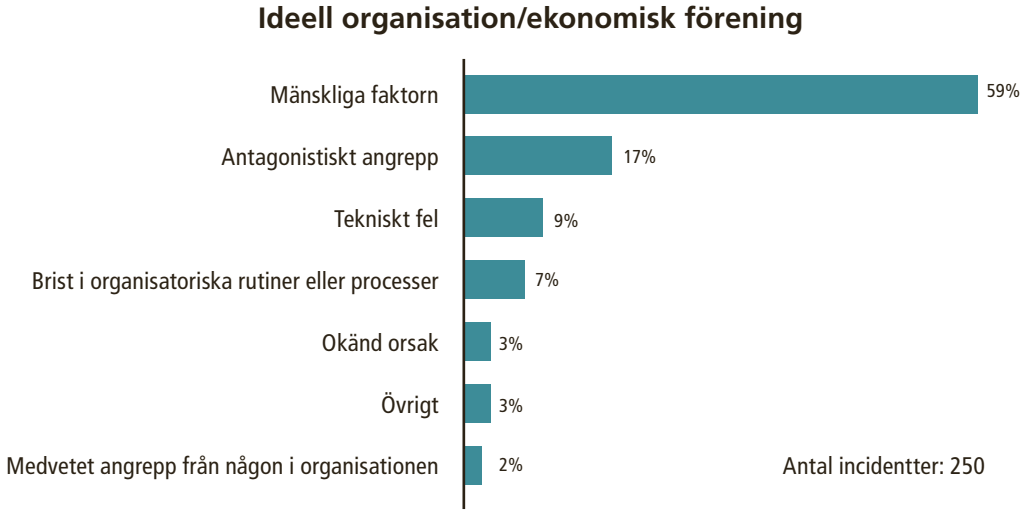


Bild 15. Fördelning av orsaker till incidenterna inom ideella organisationer och ekonomiska föreningar 2019. I sektorn ingår bland annat idrottsföreningar, trossamfund och fackförbund.

Bild 16. Fördelning av orsaker till incidenterna inom Socialtjänsten 2019.

Bild 17. Fördelning av orsaker till incidenterna inom skolan 2019.

Bild 18. Fördelning av orsaker till incidenterna inom finansiell sektor och

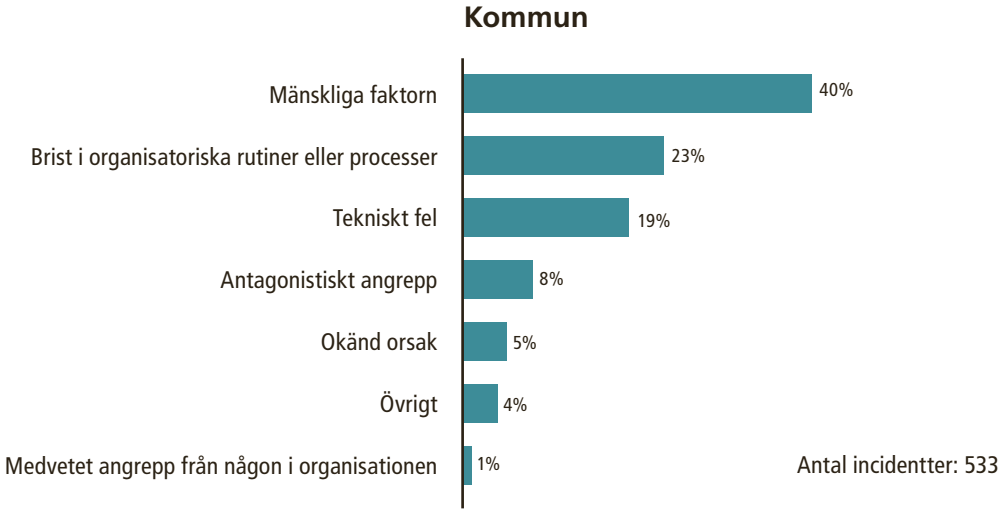
försäkring 2019.

Vid jämförelse mellan verksamhetsområdena är incidenter som uppges bero på den mänskliga faktorn minst vanliga i kommunerna, där fyra av tio incidenter uppges bero på den mänskliga faktorn. I Datainspektionens statistik redovisas socialtjänsten och grundskolan separat, vilket kan förklara varför incidenter som uppges bero på den mänsklig faktorn är mindre vanliga i kommunerna. De kommunala verksamheter som här ingår i statistiken hanterar troligen inte i samma omfattning utskick med personuppgifter.

Värt att notera är att kommunerna är den sektor som i störst utsträckning uppger att de anmälda incidenterna beror på brister i organisatoriska processer och rutiner. I kommunerna uppges 23 procent av samtliga anmälda incidenter bero på brister i organisatoriska processer och rutiner, vilket kan jämföras med 7–14 procent i övriga sektorer. Detta ligger i linje med resultatet i den undersökning som Datainspektionen

genomförde i den Nationella integritetsrapporten 2019. Dataskyddsombud bland kommuner och regioner var överrepresenterade bland dem som uppgav att de endast delvis tagit fram rutiner och riktlinjer för hur verksamheterna ska hantera personuppgifter. [7]

Bild 19. Fördelning av orsaker till incidenterna inom kommunerna 2019.



Näringslivet i övrigt skiljer sig från övriga samhällssektorer genom att den vanligaste orsaken till anmälda incidenter uppges vara ett antagonistiskt angrepp. Närmare hälften, 46 procent, av alla anmälda incidenter uppges bero på ett antagonistiskt angrepp.

Det kan ligga en reell skillnad bakom siffrorna, det vill säga att näringslivet är mer utsatta för antagonistiska angrepp än till exempel myndigheter, skola och socialtjänst. Samtidigt finns även andra tänkbara förklaringar till att så stor andel incidenter i näringslivet uppges bero på antagonistiska angrepp – förklaringar som snarare är relaterade till mognadsgraden när det gäller att identifiera och anmäla incidenter.

De flesta privata företag är inte skyldiga att utse ett dataskyddsombud. I Datainspektionens Nationella integritetsrapport 2019 framgår att endast 42 procent bland företag utan dataskyddsombud tagit fram rutiner för att rapportera personuppgiftsincidenter. Bland verksamheter med dataskyddsombud uppgav nästan dubbelt så stor andel, 79 procent, att de tagit fram rutiner för att rapportera incidenter. Med sämre rutiner för att anmäla incidenter ökar risken för okunskap eller missuppfattningar om vad en personuppgiftsincident är och vilken typ av incidenter som ska anmälas – vilket kan resultera till exempel i att incidenter som beror på ett antagonistiskt angrepp anmäls i större utsträckning än andra typer av incidenter. [8]

7,8 Datainspektionens Nationella Integritetsrapport 2019
https://www.datainspektionen.se/globalassets/dokument/rapporter/nationell-integritetsrapport-2019.pdf

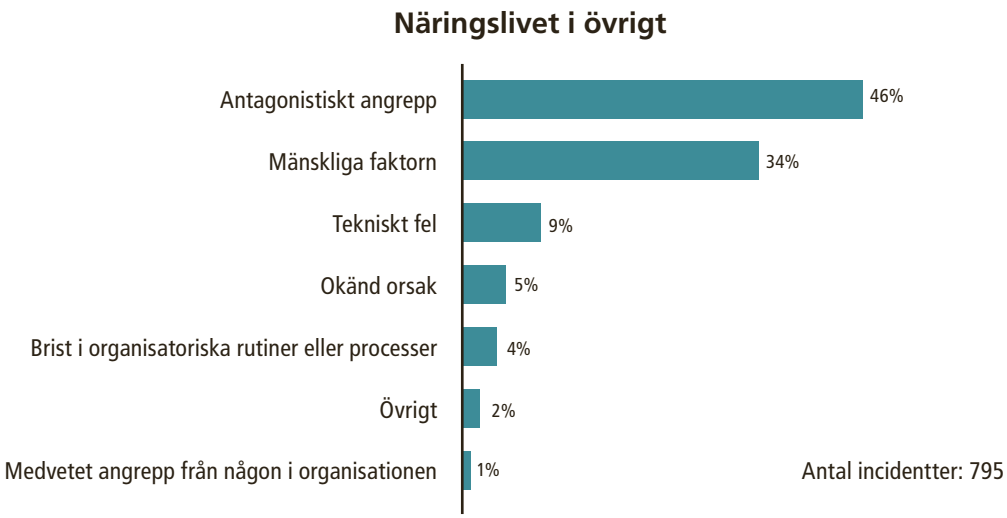


Bild 20. Fördelning av orsaker till incidenterna inom näringslivet i övrigt 2019.

Rekommendationer

Utifrån de personuppgiftsincidenter som hittills anmälts går det att ge generella rekommendationer som kan bidra till att förebygga incidenter och mildra konsekvenserna om en incident ändå inträffar. Flera av dessa rekommendationer har funnits med i Datainspektionens tidigare rapporter om anmälda personuppgiftsincidenter, men är fortfarande relevanta.

Rutiner för att upptäcka och anmäla incidenter kan ytterligare förbättras

Även om antalet anmälda incidenter per månad ökat i de flesta samhällssektorer, finns flera sektorer där ökningen är relativt liten. Alla organisationer som hanterar personuppgifter behöver ha rutiner för att upptäcka, dokumentera, anmäla och hantera personuppgiftsincidenter. I Datainspektionens nationella integritetsrapport uppgav knappt 80 procent av de intervjuade dataskyddsombuden att deras organisation har tagit fram rutiner för att anmäla personuppgiftsincidenter. Bland företag utan dataskyddsombud uppgav bara drygt 40 procent att de hade sådana rutiner. Bland företag utan dataskyddsombud finns därmed stor förbättringspotential.[9]

Löpande intern utbildning

Den stora andelen incidenter som uppges bero på den mänskliga faktorn understryker betydelsen av att styrdokument och tekniska informationssäkerhetsåtgärder kompletteras med löpande utbildning och andra åtgärder för att öka kunskap och medvetenhet hos medarbetarna.

I Datainspektionens nationella integritetsrapport 2019 uppgav knappt 50 procent av dataskyddsombuden att dataskydd och informationssäkerhet ingår i introduktionsutbildningen till nya medarbetare i deras organisation. Endast 36 procent av dataskyddsombuden uppgav att medarbetarna i deras organisation får löpande utbildning i dataskydd och informationssäkerhet.[10]

Grundläggande åtgärder som kontinuerligt kan behöva informeras om internt är till exempel

- att alltid kontrollera att korrekt mottagare är angiven innan ett brev eller e-post skickas ut, att använda funktionen dold kopia (bcc) vid

9, 10 Datainspektionens Nationella Integritetsrapport 2019 https://www.datainspektionen.se/globalassets/dokument/rapporter/nationell-integritetsrapport-2019.pdf

utskick som ska till flera mottagare samt att använda e-post som är skyddad med kryptering vid utskick av känsliga eller integritetskänsliga uppgifter.

- att om personuppgifter lagras på flyttbara media som är särskilt sårbara för stöld eller förlust – till exempel usb-minnen, bärbara datorer och mobiltelefoner – bör informationen krypteras så att ingen obehörig kan ta del av den.
- att det för att förebygga antagonistiska angrepp är angeläget att inte öppna länkar eller bifogade filer från okända avsändare.

God behörighetsstyrning kan förebygga incidenter

Obehörig åtkomst och obehörigt röjande är näst vanligaste anmälda personuppgiftsincidenten. En central del i arbetet med informationssäkerhet och dataskydd handlar om behörighetsstyrning. Alla organisationer som hanterar personuppgifter behöver ha stabila rutiner för att säkerställa att behörigheter tilldelas korrekt, att behörigheterna löpande kontrolleras och följs upp samt att åtkomstkontroller genomförs.

Incidenter kan ge viktiga signaler om utvecklingsbehov

En generell rekommendation är att de flesta organisationer kan vinna på att aktivt använda de personuppgiftsincidenter som upptäcks som ett underlag för att identifiera brister och utvecklingsbehov till det löpande och systematiska arbetet med dataskydd och informationssäkerhet.

Datainspektionens arbete med personuppgiftsincidenter

När en anmälan om en personuppgiftsincident registrerats hos Datainspektionen gör myndigheten omgående en första bedömning av incidenten. I denna första bedömning granskar myndigheten bland annat

- om incidentanmälan är fullständig eller om anmälaren uppgett att de kommer att komplettera anmälan
- hur allvarlig incidenten är, till exempel hur många registrerade som berörs, om incidenten rör känsliga personuppgifter eller särskilt sårbara grupper av registrerade och om incidenten beror på ett antagonistiskt angrepp
- hur incidenten har hanterats, till exempel om incidenten har anmälts i tid och om de registrerade har informerats när så ska ske, samt vilka åtgärder som vidtagits i övrigt.

Om anmälan inte behöver kompletteras, incidenten har hanterats på ett tillfredsställande sätt och risken för enskildas fri- och rättigheter bedöms som låg avslutas ärendet vid Datainspektionen. Anmälaren får då ett brev från myndigheten med besked om att ärendet avslutas.

Datainspektionens bedömning är att den stora merparten av de incidentanmälningar som inkommit under 2019 kommer att avslutas utan ytterligare åtgärd. Hittills har närmare 90 procent av samtliga anmälningar som inkommit sedan den 25 maj 2018 avslutats.

Datainspektionen utvecklar arbetet med personuppgiftsincidenter löpande. Målsättningen är att under första halvåret 2020 driftsätta en e-tjänst där personuppgiftsincidenter kan anmälas digitalt. Närmare information om datum för driftsättning av e-tjänsten kommer att publiceras på Datainspektionens webbplats.

Pågående tillsynsärenden som rör personuppgiftsincidenter

För incidenter som bedöms som särskilt allvarliga gör Datainspektionen en fördjupad bedömning. Myndigheten har möjlighet att inleda tillsyn baserat på hanteringen av själva incidenten och anmälan, men också utifrån mer generella brister som incidenten indikerar. För närvarande pågår ett tiotal tillsynsärenden som inletts direkt baserat på anmälda personuppgiftsincidenter. För merparten bedömer Datainspektionen att beslut kommer att fattas under första halvåret 2020.

- **1177 Vårdguiden.** Tillsynerna inleddes i mars och juni 2019. Datainspektionens granskar incidenten kring 1177 Vårdguiden. Granskningen omfattar sex tillsynsärenden och behandlar bland annat regionernas behandling av personuppgifter som rör sjukvårdsrådgivningen, kopplingen mellan regionerna och sjukvårdsrådgivningen via 1177 Vårdguiden samt ansvarsförhållandet mellan de olika aktörerna.
- **Utbildningsnämnden Stockholm Stad.** Tillsynen inleddes i juni 2019 och granskar hur Stockholms stad hanterar skolpersonalens behörighet att ta del av uppgifter om elever.
- **Statens servicecenter.** Tillsynen inleddes i september 2019 och avser en granskning av myndighetens rutiner för att upptäcka och utreda personuppgiftsincidenter.
- **Region Uppsala.** Tillsynen inleddes i september 2019 och utreder bakgrunden till att regionen har skickat patientuppgifter utan kryptering.
- **Polisen.** Tillsyn inleddes i mars 2020 och utreder orsaker till felaktiga utskick av utdrag ur belastningsregistret, samt vilka åtgärder som vidtagits.

Datainspektionen har också sju pågående tillsynsärenden som fokuserar på de generella rutinerna för incidenthantering, men där tillsynsärendet inte har inletts utifrån en specifik personuppgiftsincident som anmälts. Tillsynerna fokuserar på rättsväsendet, mot bakgrund bland annat av att få incidenter är anmälda utifrån Brottsdatalagen, och syftar till att ta reda på om myndigheten har dokumenterade rutiner för att upptäcka, rapportera och hantera personuppgiftsincidenter.

- **Polisen och Ekobrottsmyndigheten**.
  Tillsynerna inleddes i juni 2019.
- **Skatteverket, Kustbevakningen, Tullverket, Åklagarmyndigheten och Kriminalvården**.
  Tillsynerna inleddes i december 2019.

Slutligen har Datainspektionen en pågående tillsyn som rör en misstänkt incident som inte anmälts till myndigheten, utan istället kommit till myndighetens kännedom på annat sätt:

- **Umeå Universitet.** Tillsynen inleddes i augusti 2019. Universitetet har enligt uppgift skickat känsliga personuppgifter via okrypterad e-post. Datainspektionen granskar nu universitetets hantering av känsliga personuppgifter.

Kontakta Datainspektionen

E-post: datainspektionen@datainspektionen.se Webb: www.datainspektionen.se
Tfn 08-657 61 00. Postadress: Datainspektionen, Box 8114, 104 20 Stockholm

Datainspektionen