Personuppgiftsincidenter som beror på antagonistiska angrepp 2019

Datainspektionens rapport 2020:3

Datainspektionen

Personuppgifter som beror på antagonistiska angrepp 2019
DATAINSPEKTIONENS RAPPORT 2020:3

Denna rapport finns att ladda ner på www.datainspektionen.se

Innehåll

Inledning 4

Sammanfattning 5

Rekommendationer 7

- Bättre tekniska och organisatoriska åtgärder kan förebygga fler phishingattacker 7
- Säkrare hantering av personuppgifter i e-post 8
- Offentlig sektor bör säkerställa sin förmåga att upptäcka och anmäla it-angrepp som berör personuppgifter 8
- Grundläggande it-säkerhetsåtgärder stärker skyddet av personuppgifter 9

Vad är en personuppgiftsincident och när ska den anmälas till Datainspektionen? 10

Antagonistiska angrepp – en översiktlig beskrivning 11

Personuppgiftsincidenter

- som beror på antagonistiska angrepp 2019 12
- Anmälda antagonistiska incidenter 12
- Vanliga anmälda antagonistiska incidenter 13
- Fördelning – privat och offentlig sektor 14
- Fördelning på bransch eller verksamhetsområde 16
- Antal berörda som påverkats av incidenten 18
- Förekomst av känsliga och integritetskänsliga personuppgifter 19
- Berörda grupper av registrerade 20
- Incidentens allvarlighetsgrad 21
- Tid innan incidenten upptäcktes 22
- Hur incidenten upptäcktes 23
- Krypterad information 24
- Information till berörda 24
- Incidenter som berör personer i andra länder 25
- Datainspektionens arbete med personuppgiftsincidenter 26

Inledning

Genom EU:s dataskyddsförordning[1] (GDPR) infördes den 25 maj 2018 en skyldighet för privata och offentliga verksamheter som behandlar personuppgifter[2] 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 som anmälaren angett beror på någon form av antagonistiskt angrepp. Begreppet antagonistiskt angrepp kan ha olika definitioner beroende på sammanhang. Den här rapporten fokuserar på it-angrepp med avsikt att orsaka skada, alternativt skapa fördelar för egen vinning på ett otillåtet sätt. It-angreppen kan bestå av olika former av dataintrång, men genomförs oftast på andra sätt.

Rapportens innehåll ska läsas med utgångspunkt från att de anmälande verksamheterna själva gjort bedömningen att it-angreppet utgör en personuppgiftsincident där det inte är osannolikt att risk finns för berördas rättigheter och friheter.

Innehållet i rapporten bygger på internt sammanställd statistik över anmälda personuppgiftsincidenter under 2019 som beror på it-angrepp. Statistiken bygger uteslutande på de uppgifter som lämnats i incidentanmälningarna. Rapportens mer övergripande resonemang, bedömningar och rekommendationer har tagits fram av Datainspektionen. Samverkan har skett med informationssäkerhetsspecialister vid Myndigheten för samhällsskydd och beredskap, MSB, och Säkerhetspolisen, Säpo.

Rapporten är en del av Datainspektionens rapportserie där vi beskriver och analyserar inflödet till myndigheten.[3] Syftet med rapporten är att beskriva generella mönster och iakttagelser från inflödet till Datainspektionen samt 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 Följer av artikel 4.1 i dataskyddsförordningen

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

Sammanfattning

- Av de totalt knappt 4 800 anmälningar om personuppgiftsincidenter som anmäldes till Datainspektionen 2019, utgjordes cirka 600 stycken, 13 procent, av incidenter som uppges bero på antagonistiska angrepp. Andelen var ungefär lika stor 2018, 14 procent. Ett antagonistiskt angrepp kan bero på till exempel fysisk stöld eller it-angrepp. Den här rapporten fokuserar på de drygt 400 stycken, cirka 9 procent, av personuppgiftsincidenterna som beror på it-angrepp.
- En betydande andel, nästan nio av tio, av de anmälda personuppgiftsincidenterna som beror på it-angrepp kommer från privat sektor, och endast cirka en av tio från offentlig sektor. Det är svårt att dra några generella slutsatser varför andelen anmälningar är betydligt större från privat sektor jämfört med offentlig sektor, men tänkbara förklaringar kan vara att privat sektor är mer utsatt för och har större fokus på it-angrepp.
- Det är vanligt att de anmälda antagonistiska incidenterna har genomförts genom breda nätattacker utan specifik mottagare. En vanlig metod för att komma åt information är phishing – som innebär att mottagarna via ett mejl klickar på en länk och leds till en falsk webbplats, där de uppmanas att ange uppgifter. Det är också vanligt att de anmälda incidenterna har resulterat i att e-postkonton använts för att skicka phishingmejl.
- De anmälda personuppgiftsincidenterna som beror på it-angrepp kommer från ett brett spektra av branscher, vilket ligger i linje med att det är vanligt med breda nätattacker utan specifik mottagare. En något större andel kommer dock från detaljhandeln.
- Majoriteten av de anmälda it-angreppen har upptäckts inom ett dygn av anställda, berörda personer eller personuppgiftsbiträden[4]. Den förhållandevis snabba upptäckten kan bland annat bero på att en stor andel av incidenterna utgörs av phishingangrepp eller installerade utpressningsprogram, som är relativt enkla att upptäcka. Knappt en tredjedel av incidenterna har upptäckts genom organisatoriska och tekniska åtgärder.

4 https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/personuppgiftsansvariga-och-personuppgiftsbitraden/

- De anmälande verksamheterna bedömer överlag själva att incidenternas allvarlighetsgrad varit begränsad. Detta kan bero på att varken känsliga, integritetskänsliga personuppgifter eller särskilt sårbara grupper av personer i någon större omfattning berörts. I de fall integritetskänsliga personuppgifter[5] berörts är det oftast personnummer, kort- eller kontonummer som förekommer.
- Även om de antagonistiska incidenterna utgör en liten andel av det totala antalet personuppgiftsincidenter, har de berört ett relativt stort antal personer.
- Datainspektionen gör bedömningen att det sannolikt finns ett mörkertal när det gäller antalet faktiskt inträffade personuppgiftsincidenter som beror på it-angrepp och som inte upptäcks, eller upptäcks men inte anmäls till Datainspektionen. För att upptäcka mer avancerade it-angrepp krävs i regel mognad inom såväl it- som informationssäkerhet. Många verksamheter kan dessutom ha relativt låg kunskap om riskerna och hoten för att utsättas för it-angrepp, varför vidtagna skyddsåtgärder kan vara bristfälliga. Kunskapen om skyldigheten att anmäla incidenter kan också vara bristfällig. Den förhållandevis låga andelen inrapporterade incidenter från offentlig sektor kan tyda på ett större mörkertal inom offentlig sektor jämfört med privat sektor.

5 https://www.datainspektionen.se/vagledningar/en-introduktion-till-dataskyddsforordningen/vad-ar-en-personuppgift/

Rekommendationer

Utifrån anmälda personuppgiftsincidenter som uppges bero på it-angrepp kan några generella rekommendationer ges.

Rekommendationerna handlar i stor utsträckning om it- och informationssäkerhetsarbete, den typen av tekniska och organisatoriska säkerhetsåtgärder som regleras i artikel 32 i dataskyddsförordningen.

Ett väl fungerande informationssäkerhetsarbete utgör en viktig komponent i ett effektivt dataskydd. Informationssäkerhetsarbetet syftar till att skydda verksamheternas information så att den alltid finns när den behövs, att den är riktig och inte manipulerad och att endast behöriga personer får ta del av den. Informationssäkerhets- och dataskyddsarbetet har många beröringspunkter och likheter, till exempel det systematiska, riskbaserade och långsiktiga arbetssättet.

I samband med personuppgiftsincidenter finns krav på verksamheten att kunna visa hur incidenten har hanterats, genom att dokumentera omständigheterna kring incidenten, dess effekter och de korrigerande åtgärder som har vidtagits.[6]

1. Bättre tekniska och organisatoriska åtgärder kan förebygga fler phishingattacker

Enligt dataskyddsförordningen är den personuppgiftsansvariga verksamheten skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.[7]

Ett av de vanligaste it-angreppen som anmäldes till Datainspektionen 2019 var phishingattacker. Av anmälningarna framgår att många mottagare faktiskt klickar på länkar i phishingmejl, vilket understryker behovet av organisatoriska skyddsåtgärder som utbildning, information och löpande påminnelser om hur vanliga it-angrepp går till. Medarbetarna kan också påminnas om att vara vaksamma kring länkar och bilagor i mejl. Genom att utbilda medarbetarna i angriparnas metoder och tillvägagångssätt samt de risker angreppen kan resultera i kan fler phishingattacker förebyggas.

Att cirka en av tio anmälda antagonistiska incidenter har upptäckts genom tekniska åtgärder kan innebära att verksamheterna har väl fungerande rutiner för att upptäcka och stoppa till exempel spam- och phishingmejl. Att majoriteten av incidenterna har upptäckts på annat

6 Följer av artikel 33.5 i dataskyddsförordningen

7 Följer av artikel 32.1 i dataskyddsförordningen

sätt än genom tekniska skyddsåtgärder, indikerar dock att det kan finnas utrymme för förbättringar. Genom åtgärder som till exempel spamfilter och uppdaterade it-miljöer kan fler phishingattacker upptäckas och stoppas.

2. Säkrare hantering av personuppgifter i e-post

En vanlig antagonistisk incident som anmäls till Datainspektionen är angrepp riktade mot olika e-postkonton i syfte att ta över dem för att skicka phishingmejl. I och med att angriparna får åtkomst till lösenord kan de logga in på mottagarnas konton och ta del av innehåll i e-posten. För att förhindra att personuppgifter, och särskilt känsliga personuppgifter, kommer i orätta händer samband med intrång i e-postkonton, behövs riktlinjer och rutiner för säker e-posthantering. Det kan till exempel handla om att inte hantera fler uppgifter än som behövs via e-post och att inte spara uppgifterna längre än nödvändigt.[8] Även här är information och utbildning av betydelse för att alla medarbetare ska ha goda hanteringsrutiner men också kunna bidra till att upptäcka misstänkta meddelanden.

3. Offentlig sektor bör säkerställa sin förmåga att upptäcka och anmäla it-angrepp som berör personuppgifter

Mot bakgrund av att det sannolikt finns ett mörkertal när det gäller faktiska it-angrepp som berör personuppgifter är det viktigt att alla verksamheter arbetar för att förbättra det systematiska arbetet med att förebygga, upptäcka och hantera it-angrepp, i syfte att minska risker och negativa konsekvenser.

Det faktum att förhållandevis få antagonistiska incidenter anmälts till Datainspektionen, samt MSBs erfarenheter av att statliga myndigheter anmäler för få it-incidenter, innebär att det finns anledning att anta att antalet antagonistiska incidenter som rapporteras, framför allt från offentlig sektor, till Datainspektionen också är för få. Offentlig sektor bör därför säkerställa sin förmåga att upptäcka och anmäla it-angrepp som rör personuppgifter. Tydliga interna instruktioner och rutiner för när ett it-angrepp som berör personuppgifter ska anmälas till Datainspektionen är angeläget. Att identifiera, hantera och anmäla antagonistiska incidenter till Datainspektionen ingår i en effektiv incidenthantering. Genom att dokumentera incidenterna internt kan kunskap återkopplas till verksamheterna. Därmed skapas förutsättningar för ökat lärande i organi-

8 Följer av artikel 5 i dataskyddsförordningen

sationerna i syfte att stärka upptäcktsförmågan och därmed integritetsskyddet.

4. Grundläggande it-säkerhetsåtgärder stärker skyddet av personuppgifter

En viktig grund i arbetet med att stärka skyddet av personuppgifter vid it-angrepp, är att implementera relevanta tekniska säkerhetsåtgärder. I väntan på nya föreskrifter om en grundnivå för statliga myndigheters it-säkerhet, har MSB i sin årsrapport för statliga myndigheters it-incidentrapportering 2019, pekat på ett antal grundläggande it-säkerhetsåtgärder. Avsikten med åtgärderna är att primärt bemöta antagonistiska hot. Åtgärderna kan även bidra till att höja den generella nivån när det gäller informations- och cybersäkerhet.[9]

Exempel på tekniska åtgärder som kan öka skyddet av personuppgifter vid it-angrepp är säkerhetsuppdateringar, uppgradering av mjuk- och hårdvara samt operativsystem, införande av flerfaktorsautentisering, samt användning av antivirusprogram. Flera av MSBs rekommenderade åtgärder bidrar även till att uppfylla kraven på säkerhet i samband med behandling av personuppgifter i artikel 32 i dataskyddsförordningen. Artikeln anger även kryptering som exempel på säkerhetsåtgärd.

9 MSB: Årsrapport it-incidentrapportering 2019, sid 40

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

En personuppgiftsincident är en säkerhetsincident som rör personuppgifter. Incidenten kan till exempel handla om att personuppgifter har blivit förstörda, 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 berördas rättigheter och friheter ska den anmälas till Datainspektionen inom 72 timmar från att den upptäckts.[10]

Om personuppgiftsincidenten sannolikt leder till en hög risk för berördas rättigheter och friheter, är den ansvariga verksamheten skyldig att – förutom att anmäla det inträffade till Datainspektionen – också informera de berörda om att personuppgiftsincidenten inträffat. Det ger de berörda personerna möjlighet att vidta egna åtgärder, till exempel att byta lösenord eller spärra kredit- och kontokort. Även när en incident inte anmäls ska den alltid dokumenteras internt.[11]

10 Följer av artikel 33.1 i dataskyddsförordningen
11 Följer av artikel 33.5 i dataskyddsförordningen

Antagonistiska angrepp – en översiktlig beskrivning

Svenska företag, myndigheter och andra organisationer utsätts kontinuerligt för mer eller mindre allvarliga it-angrepp som riskerar att skada såväl de angripna verksamheterna som samhället i stort. Angreppen påverkar alla samhällssektorer och skadorna kan variera från förlust av små belopp till förlust av affärskritisk information.

Hotaktörerna kan utgöras av allt från enskilda individer till organiserad brottslighet eller statsunderstödda aktörer. Syftet med ett it-angrepp är ofta att komma åt information som på olika sätt kan användas för ekonomisk vinning. Det kan till exempel handla om att få tillgång till lösenord eller kontokortsuppgifter som sedan kan säljas vidare eller användas för egna syften. Det kan också handla om att komma över viktig företagsinformation, som utvecklings- och affärsplaner. I vissa fall kan angreppen utgöra en del av främmande makts aktivitet mot Sverige, i syfte att till exempel bedriva spionage eller politisk påverkan. Att identifiera vem som ytterst ligger bakom ett angrepp är ofta svårt, både av tekniska skäl men också för att det förhållandevis enkelt går att köpa tjänsten av någon annan som rent faktiskt utför it-angreppet.

I vissa fall är angreppen riktade mot enskilda verksamheter eller individer, men en stor andel av attackerna genomförs i form av breda nätattacker utan en specifik mottagare. Det förekommer även att angreppen utgör ”språngbräda” i större processer där syftet är att få tillgång till verksamheternas infrastruktur för att kunna använda den vid senare attacker med andra syften. I och med att angriparna kontinuerligt upptäcker nya sårbarheter i program- och hårdvara, är det en utmaning för företag, myndigheter och andra organisationer att löpande anpassa sitt tekniska och organisatoriska skydd efter de nya angreppsmetoderna.

Personuppgiftsincidenter som beror på antagonistiska angrepp 2019

Anmälda antagonistiska incidenter

Under 2019 tog Datainspektionen emot totalt 4 757 anmälningar om personuppgiftsincidenter varav 616 stycken, 13 procent, avsåg incidenter som anmälaren uppgivit beror på ett antagonistiskt angrepp.

Eftersom anmälningsskyldigheten infördes den 25 maj 2018 finns inga jämförbara helårssiffror avseende antalet anmälda antagonistiska incidenter mellan 2018 och 2019. Det kan dock konstateras att andelen antagonistiska incidenter 2018 uppgick till ungefär samma andel, 14 procent.

Av de anmälda incidenterna som beror på antagonistiska grepp utgörs majoriteten, drygt två tredjedelar, 413 incidenter, av obehörig åtkomst, vilket innebär att någon olovligen berett sig tillgång till personuppgifter, vanligen genom olika it-angrepp. Drygt en fjärdedel av de antagonistiska incidenterna utgörs av förlust eller stöld, till exempel genom att en organisation haft inbrott.

Den här rapporten fokuserar på de 413 stycken, 8,7 procent, av personuppgiftsincidenterna som beror på obehörig åtkomst i form av it-angrepp. Statistiken bygger på ett slumpmässigt urval motsvarande 200 av dessa incidenter.

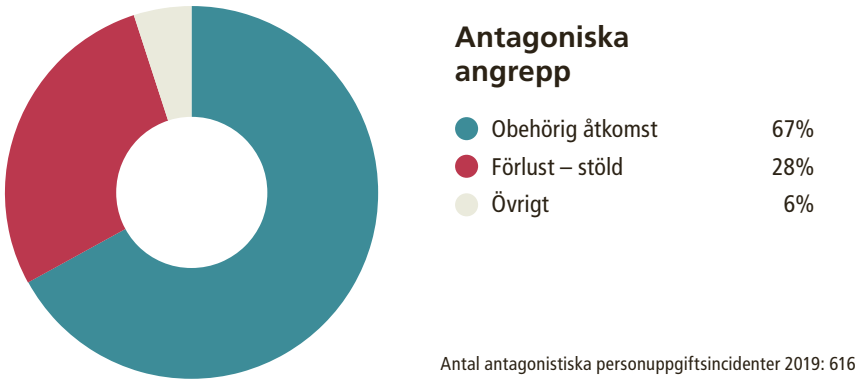

Bild 1. Fördelning av anmälda antagonistiska incidenter.

Såväl MSB som Säpo har tidigare konstaterat att kunskap och förmåga avseende informations- och cybersäkerhetsarbete generellt sett är

begränsad och behöver öka.[12] Datainspektionens erfarenhet av säkerhetsarbete utifrån dataskyddsregleringen bekräftar den bilden och att det sannolikt gäller både privat och offentlig sektor. Många verksamheter har en relativt låg kunskap om risker och hot för att utsättas för it-angrepp, vilket innebär att verksamheternas beredskap och vidtagna åtgärder för att skydda verksamheten kan vara bristfälliga. Utvecklingen inom området går dessutom snabbt och angriparna kan vara skickliga, vilket leder till att angrepp inte upptäcks och därmed inte anmäls. Det finns också en risk att verksamheter som utsatts för angrepp väljer att inte anmäla incidenten för att undvika att blotta sårbarheter i verksamheten eller för att undvika negativ publicitet som kan skada förtroendet. Det finns därför sannolikt ett stort mörkertal när det gäller antalet faktiskt inträffade antagonistiska incidenter.

Vanliga anmälda antagonistiska incidenter

En stor andel av de it-angrepp som anmälts till Datainspektionen under 2019 har genomförts genom bredare nätattacker utan specifik mottagare, där en av de vanligaste incidenterna är att it-angreppet resulterat i olika e-postkonton skickat phishingmejl.

Ett vanligt tillvägagångssätt vid breda attacker är att angriparna identifierat en sårbarhet som de vill utnyttja. Angreppen initieras ofta genom att mottagarna får ett mejl, där de uppmanas klicka på en länk eller bilaga som leder till att skadlig kod, så kallad malware, installeras på användarnas dator. Meddelandet i mejlet utformas i regel för att efterlikna ett utskick från en bank, kreditkortsbolag, en systemleverantör eller någon annan känd och betrodd aktör. Tillvägagångssättet kallas nätfiske, eller phishing, och kan genomföras på olika sätt. I vissa fall installeras den skadliga koden när mottagaren klickar på länken eller bilagan, vilket innebär att angriparen kan ta sig in i systemet för att nå sina mål. Ett annat sätt att använda phishing är att via e-postmeddelandet leda mottagaren till en falsk webbsida. På den falska webbsidan finns ett inloggningsformulär där användaren uppmanas logga in genom att ange lösenord, sina mejlkontouppgifter, lösenord, kreditkortsnummer eller andra känsliga uppgifter. Detta möjliggör åtkomst till uppgifterna för den som satt upp den falska webbsidan, som ofta är mycket lik originalet.[13] Phishingattackerna kan också vara riktade angrepp mot specifika enskilda eller grupper av individer, så kallad spear phishing.

En relativt vanligt förekommande incident är även att skadlig kod i form av ransomware, eller utpressningsprogram, installeras vid angreppen. När ett ransomware infekterar en dator eller ett nätverk låses

12 Säkerhetspolisens årsbok 2019, sid 22 och 37, samt MSB: Årsrapport it-incidentrapportering 2018, sid 39
13 MSB: Årsrapport it-incidentrapportering 2018, sid 20

möjligheten att komma åt viktiga filer, och angriparna kräver sedan en lösensumma för att låsa upp dem.

Ytterligare en form av skadlig kod som förekommer bland anmälningarna är spyware, det vill säga spionprogram. När programmen körs på datorn kan information om till exempel lösenord, e-postadresser eller andra uppgifter vidarebefordras till angriparen.

Ett annat angrepp som förekommer bland de anmälda antagonistiska incidenterna är överbelastningsattacker, som går ut på att belasta exempelvis en webbplats med så mycket trafik som möjligt. I regel leder attackerna till att webbplatsen, systemet eller nätverksresurserna blir otillgängliga.

En anställd inom utbildningsverksamhet fick ett mejl med en länk. Den anställde klickade på länken, vilket resulterade i att en obehörig person i annat land loggat in på den anställdes konto. Den anställde hade behörighet till system med känsliga personuppgifter om elever. I anmälan framgick att den anmälande verksamheten bedömde att risk fanns för att uppgifterna var röjda.

PERSONUPPGIFTSINCIDENT ANMÄLD TILL DATAINSPEKTIONEN

Ett företag utsattes för ransomware, där system låsts och krypterats och 5 000 kunders personnummer, namn och kontaktuppgifter gjordes otillgängliga. Företaget uppmanades betala en lösensumma för att angriparna skulle låsa upp systemen. Företaget övervägde att betala lösensumman, för att förhindra ekonomiska förluster för företaget.

PERSONUPPGIFTSINCIDENT ANMÄLD TILL DATAINSPEKTIONEN

Fördelning – privat och offentlig sektor

Av samtliga personuppgiftsincidenter som anmäldes till Datainspektionen under 2019 kom majoriteten, cirka sex av tio, från offentlig sektor eller verksamheter med offentligt uppdrag. Datainspektionen har tidigare bedömt att rutinerna för att rapportera incidenter internt och anmäla dem till Datainspektionen blivit mer etablerade, i synnerhet inom offentlig sektor.[14]

När det gäller anmälda personuppgiftsincidenter som beror på it-angrepp ser fördelningen av anmälningar dock annorlunda ut. En

14 Anmälda personuppgiftsincidenter 2019, Datainspektionens rapport 2020:2, sid 10

påfallande stor andel, nästan nio av tio, av de anmälda antagonistiska incidenterna 2019 kom från privat sektor, och endast cirka en av tio incidenter kom från offentlig sektor.

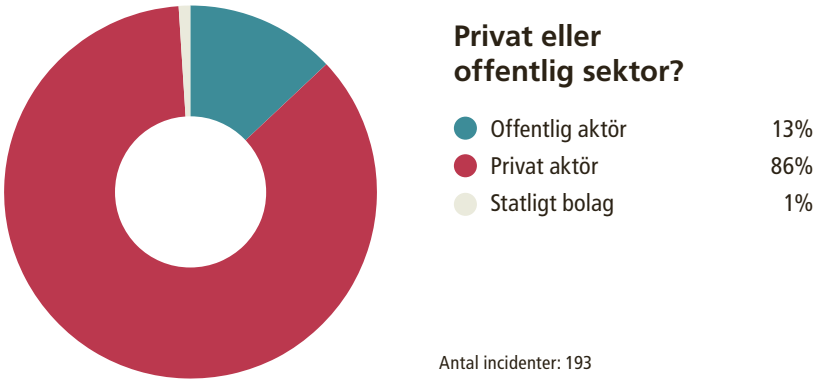

Bild 2. Andel anmälda incidenter från privat- respektive offentlig sektor.

Utifrån den information som finns i incidentanmälningarna går det inte att dra säkra slutsatser kring varför andelen anmälningar är betydligt större från privat sektor jämfört med offentlig sektor.

En möjlig förklaring kan vara att privat sektor är mer utsatt för antagonistiska angrepp. Sektorn hanterar i stor omfattning kunduppgifter som är kommersiellt intressanta för angripare, till exempel kontokortsuppgifter, e-postadresser och personnummer. Genom angreppen kan angriparna komma över uppgifter som de kan använda för egen vinning alternativt sälja vidare.

Det kan också vara så att privat sektor har ett större fokus på it-angrepp, eftersom angripna system som inte fungerar kan få stora ekonomiska konsekvenser för försäljningen och därmed lönsamheten. De tydligare ekonomiska konsekvenserna kan bidra till att de antagonistiska incidenter som upptäcks också i större utsträckning anmäls.

När det gäller offentlig sektor har Datainspektionen tidigare gjort bedömningen att rutinerna för att upptäcka och anmäla personuppgiftsincidenter generellt förbättrats och blivit mer etablerade under 2019.[15] Möjligen finns en risk att antagonistiska it-angrepp upptäcks inom it-organisationen men inte rapporteras vidare internt till dataskyddsombudet på samma sätt som andra typer av personuppgiftsincidenter. Detta skulle kunna bidra till att antagonistiska it-angrepp mot offentlig sektor anmäls till Datainspektionen i lägre utsträckning än andra typer av personuppgiftsincidenter.

15 Datainspektionen rapport 2019:2

Myndigheten för samhällsskydd och beredskap, MSB, har sedan april 2016 mottagit rapporter om allvarliga it-incidenter från statliga myndigheter. MSB konstaterar i sin årsrapport om it-incidentrapportering 2019[16], att det är för få incidenter som rapporteras, och för få myndigheter som rapporterar. Totalförsvarets forskningsinstitut, FOI, har haft i uppdrag från regeringen att belysa orsakerna till myndigheternas begränsade rapportering av it-incidenter till MSB[17]. Utifrån FOIs analys lyfter MSB i sin årsrapport ett antal tänkbara anledningar till att myndigheterna inte rapporterar allvarliga it-incidenter; till exempel att rutiner för att identifiera, bedöma, hantera, dokumentera och rapportera it-incidenter saknas eller är bristfälliga, hög arbetsbelastning på myndigheterna, svårigheter i att bedöma it-incidenters allvarlighetsgrad samt att myndigheten inte upplever någon nytta med rapporteringen till MSB. Det finns också oklarheter gällande rapporteringsskyldighet samt ansvarsfördelning när värdmyndigheter för it-drift används.[18] De aspekter som FOI identifierat som tänkbara orsaker till varför statliga myndigheter inte i tillräcklig omfattning rapporterar it-incidenter till MSB, kan även vara möjliga förklaringar till offentlig sektors begränsade anmälningar av antagonistiska incidenter till Datainspektionen.

Fördelning på bransch eller verksamhetsområde

De personuppgiftsincidenter som beror på it-angrepp och som anmälts till Datainspektionen kommer från ett brett spektra av branscher och verksamheter, vilket ligger i linje med att en stor andel av angreppen utgörs av breda nätattacker utan specifik mottagare.

Vid jämförelse mellan branscherna utmärker sig detaljhandeln. Störst andel, en femtedel, kommer från den branschen. En tänkbar förklaring till den större andelen från detaljhandeln kan vara att den uppenbara förekomsten av finansiell information som till exempel kortuppgifter drar till sig angripare. Den växande e-handeln kan också skapa sårbarheter, i och med att e-handelsplattformar kan utgöra en väg in i den interna it-miljön. En förklaring kan också vara att detaljhandeln har rutiner på plats för att upptäcka och rapportera incidenter.

16 MSB: Årsrapport it-incidentrapportering 2019

17 FOI: IT-incidenter på statliga myndigheter. Orsaker till utebliven rapportering, Rapportnummer: FOI-R--4815--SE

18 MSB: Årsrapport it-incidentrapportering 2019, sid 35-36

Kassan i en webbshop som ingår i en internationell detaljhandelskedja angreps i syfte att komma åt kortuppgifter, som i krypterad form skickades till obehörig part. Mellan 10-100 kunder berördes av angreppet. Den anmälande verksamheten bedömde angreppet som mycket allvarligt.

PERSONUPPGIFTSINCIDENT ANMÄLD TILL DATAINSPEKTIONEN

En detaljhandelskedja drabbades av angrepp mot sin e-handelsplattform. En konstgjord kassa installerades, där kortbetalningar endast kunde genomföras. Kunderna angav sina kortnummer som sedan skickades till en obehörig part. Därefter vidarebefordrades kunden till den korrekta kassan. Angreppet upptäcktes av en anställd.

PERSONUPPGIFTSINCIDENT ANMÄLD TILL DATAINSPEKTIONEN

Fördelning bransch/verksamhetsområde

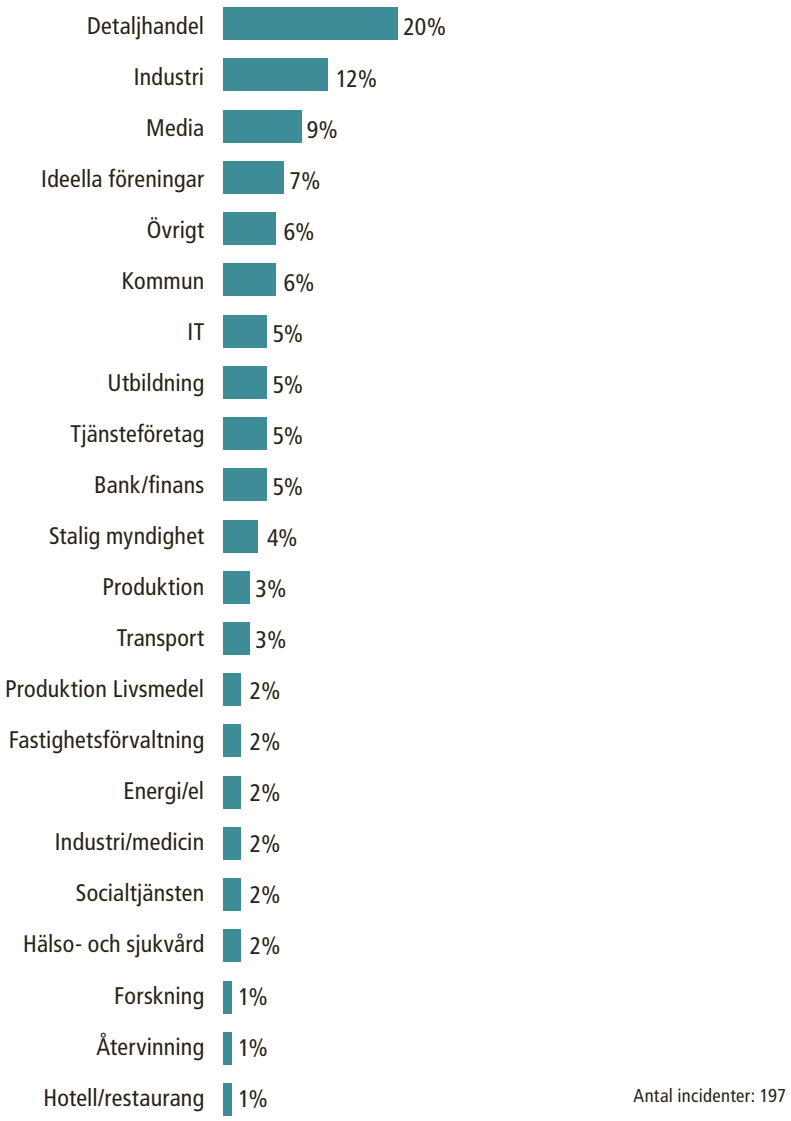

Bild 3. Anmälda incidenter fördelade på bransch/verksamhetsområde.

Antal berörda som påverkats av incidenten

Även om antalet personuppgiftsincidenter som beror på it-angrepp utgör en förhållandevis liten andel av samtliga personuppgiftsincidenter, har incidenterna haft påverkan på ett stort antal personer. Omfattningen av antalet berörda framgår bland annat av att två incidenter uppges ha berört mellan en halv till en miljon personer, och ytterligare två incidenter uppges ha berört fler än en miljon personer. En knapp tredjedel av angreppen bedöms ha rört mindre än 100 personer.

En relativt stor andel, cirka en tredjedel, av de anmälande verksamheterna uppger att antalet registrerade som påverkas av incidenten är okänt. Det finns flera tänkbara anledningar till att verksamheterna inte känner till hur många personer som berörs av incidenten. Även om den personuppgiftsansvariga verksamheten har ansvar för de personuppgifter de behandlar, kan det vara svårt och kräver mognad i it- och informationssäkerhetsarbetet att kunna spåra vilka som till exempel klickat på en länk vid en phishingattack. Ytterligare en bidragande orsak kan vara att många incidenter anmälts relativt omgående efter att de upptäckts, och att verksamheterna inte hunnit analysera hur många personer som berörts.

Ett antal medarbetare i en ideell organisation mottog mejl från falsk intern avsändare där de uppmanades att uppge sin mejladress och byta lösenord till e-postkontot. Efter någon dag upptäcktes att phishingmejlen från den falska interna avsändaren även skickades till externa mottagare. Den ideella organisationen kunde inte uppge hur många externa mottagare som erhållit phishingmejlen. Allvarlighetsgraden uppskattades som begränsad, men den anmälda verksamheten uppgav att risk fanns för skadat anseende.

PERSONUPPGIFTSINCIDENT ANMÄLD TILL DATAINSPEKTIONEN

Antal registrerade som påverkas av incidenten

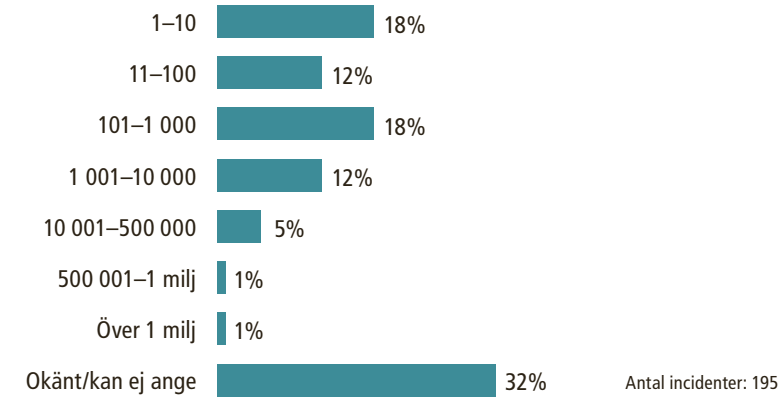

Bild 4. Antal registrerade som berörs av incidenten.

Förekomst av känsliga och integritetskänsliga personuppgifter

Vissa personuppgifter är till sin natur särskilt känsliga och ska därför ha ett starkare skydd. Känsliga personuppgifter beskrivs i artikel 9 i dataskyddsförordningen och omfattar uppgifter om till exempel etniskt ursprung, politiska åsikter, hälsa, sexuell läggning samt genetiska och biometriska uppgifter i syfte att identifiera en person. Det finns även andra typer av personuppgifter som anses särskilt skyddsvärda, så kallade integritetskänsliga personuppgifter. Hit hör exempelvis uppgifter om lagöverträdelser, personnummer och i regel även uppgifter om enskildas sociala och ekonomiska förhållanden.

I mer än hälften av de antagonistiska incidenterna berörs enligt anmälarna varken känsliga eller integritetskänsliga personuppgifter, vilket troligen kan relateras till vilken typ av angrepp verksamheterna varit utsatta för. Eftersom vanliga antagonistiska incidenter till exempel är phishingattacker riktade mot e-postkonton, med syftet att ta över kontona för att skicka phishingmejl, är det oftast inte känsliga uppgifter som berörs.

I cirka en tredjedel av incidenterna har känsliga, och främst integritetskänsliga, personuppgifter berörts. Integritetskänsliga personuppgifter förekommer ofta vid angrepp riktade mot företag där kunduppgifter är centrala för verksamheten. Detaljhandeln står för störst andel av de anmälda antagonistiska incidenterna där integritetskänsliga personuppgifter berörs, men även bank och finans, utbildning och tjänstesektorn har anmält incidenter där integritetskänsliga personuppgifter förekommer. De integritetskänsliga personuppgifterna utgörs i stor omfattning av personnummer samt kort-och kontouppgifter.

Vid cirka en av tio incidenter kan verksamheterna inte ange om känsliga personuppgifter berörts.

En extern angripare tog sig in i ett av bolagens mejlkonton och skickade ut phishingmejl. Det angripna mejlkontot innehöll känsliga personuppgifter om anställda. Fler anställda mottog sedan phishingmejl där de ombads att uppge sina inloggningsuppgifter. Angriparna loggade sedan in på de anställdas mejlkonton. Angreppet var en del av att större angrepp.

PERSONUPPGIFTSINCIDENT ANMÄLD TILL DATAINSPEKTIONEN

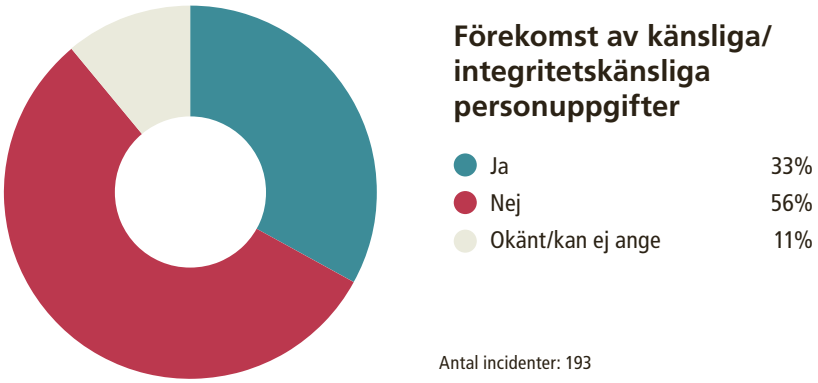

Bild 5. Förekomst av känsliga och integritetskänsliga personuppgifter.

Berörda grupper av registrerade

När verksamheterna anmäler personuppgiftsincidenter anger de bland annat vilka grupper av registrerade personer som berörts vid angreppet. Datainspektionen använder sedan verksamheternas uppgifter som underlag för att bedöma incidentens allvarlighetsgrad. Vissa grupper av personer anses som särskilt sårbara, till exempel patienter, barn, skolelever och personer som lever med skyddad identitet.

I majoriteten, drygt åtta av tio, av de anmälda incidenterna berörs inte särskilt sårbara grupper av registrerade. En anledning till att särskilt sårbara grupper i någon större omfattning inte berörts kan vara att majoriteten av de anmälda antagonistiska incidenterna kommer från privat sektor, där särskilt sårbara grupper av registrerade förekommer i mindre omfattning. En liten andel, fem procent, berör dock särskilt sårbara grupper av registrerade.

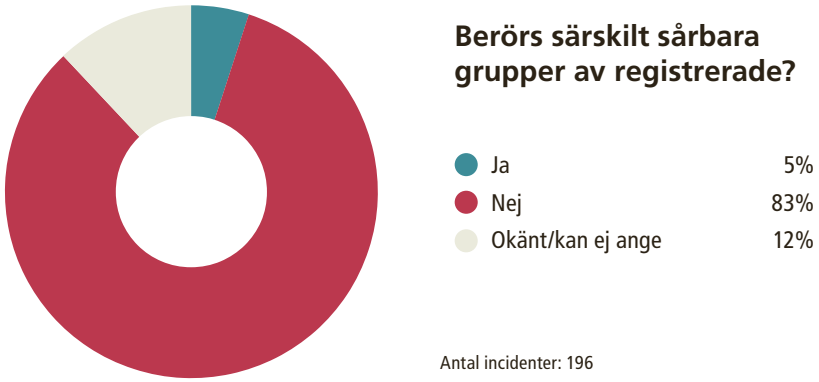

Bild 6. Andel av incidenterna där särskilt sårbara grupper av registrerade berörs.

Incidentens allvarlighetsgrad

När en anmälan om en personuppgiftsincident registrerats gör Datainspektionen en första bedömning av incidenten. Myndigheten granskar bland annat hur allvarlig incidenten är, till exempel hur många registrerade som berörts, om incidenten rör känsliga eller integritetskänsliga personuppgifter eller särskilt sårbara grupper av registrerade och om incidenten beror på ett antagonistiskt angrepp.

I anmälan gör även den anmälande verksamheten en egen bedömning av incidentens allvarlighetsgrad. I majoriteten av fallen, knappt två tredjedelar av de antagonistiska incidenterna, har verksamheterna bedömt att allvarlighetsgraden varit begränsad (allvarlighetsgrad två på en fyrgradig skala). Detta kan bland annat bero på att en stor andel av de uppgifter som berörts varken är känsliga eller integritetskänsliga, samt att särskilt sårbara grupper av registrerade inte berörts.

Vid cirka en femtedel av incidenterna bedöms allvarlighetsgraden som betydande (allvarlighetsgrad tre av fyra) och i åtta anmälningar, fyra procent, anges allvarlighetsgraden som mycket allvarlig (allvarlighetsgrad fyra av fyra). De incidenter som bedömts som mycket allvarliga har samtliga, utom en, inträffat inom offentlig sektor. De har enbart berört personer i Sverige. Vid en av tio anmälningar bedöms allvarlighetsgraden vara obetydlig.

Ett it-system larmade om att en extern part via extern dator tagit sig in i en anställds dator och listat samtliga mejladresser, inklusive känsliga adresser som till exempel admin-mejladresser tillhörande hela koncernen. Angriparen fick endast åtkomst till mejladresser, och inte tillhörande koder och därmed inte heller innehållet i mejlkontona. Allvarlighetsgraden bedömdes som begränsad.

PERSONUPPGIFTSINCIDENT ANMÄLD TILL DATAINSPEKTIONEN

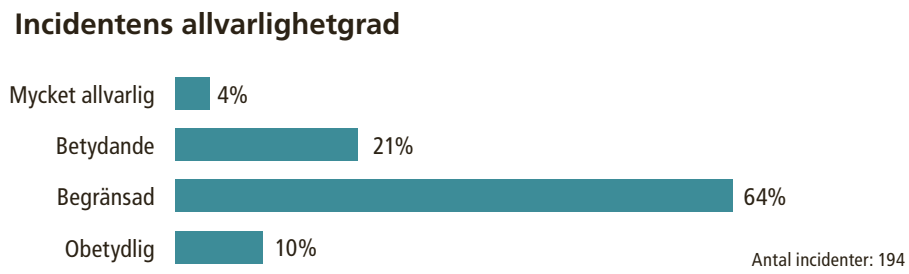

Bild 7. Anmälande verksamheters bedömning av incidentens allvarlighetsgrad.

Tid innan incidenten upptäcktes

Datainspektionens generella bedömning när det gäller personuppgiftsincidenter är att det finns ett förhållandevis stort mörkertal – antingen på grund av att incidenter inte upptäcks eller att de inte anmäls.[19] Detta gäller sannolikt även för antagonistiska it-angrepp. När angripare manipulerar sig in i system för att komma över data, är ett av syftena att ta sig in obemärkt och vara kvar länge för att få möjlighet att ta del av önskad information. Kvalificerade angrepp är därför ofta svåra att upptäcka.

Av de it-angrepp som anmäls har majoriteten, nästan sex av tio, upptäckts relativt snabbt, det vill säga inom ett dygn, efter att händelsen inträffat. Den snabba upptäckten kan bero på att en stor andel består av phishingattacker och ransomware, som är relativt enkla att upptäcka. Avsikten med ransomware är dessutom att angreppet ska upptäckas. Resterande incidenter, cirka fyra av tio, har tagit längre tid att upptäcka. En mindre andel, cirka en av tio, har upptäckts först efter en månad eller senare.

En användare tog sig via brister in i ett system, som innehöll ekonomiska uppgifter om anställda. Incidenten varade under en längre tid och anmäldes först efter ett halvår efter att den inträffat.

PERSONUPPGIFTSINCIDENT ANMÄLD TILL DATAINSPEKTIONEN

19 Anmälda personuppgiftsincidenter 2019, Datainspektionens rapport 2020:2, sid 3

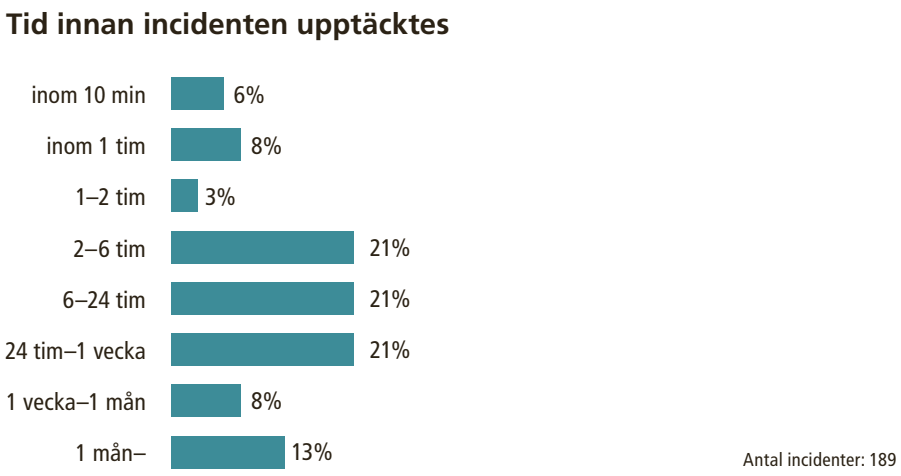

Bild 8. Andel incidenter relaterat till tid innan incidenten upptäcktes.

Hur incidenten upptäcktes

En stor andel av de anmälda antagonistiska incidenterna, nästan sju av tio, har upptäckts av anställda, berörda personer eller personuppgiftsbiträden. En knapp tredjedel har upptäckts genom organisatoriska rutiner och automatiserade processer. Var tionde incident upptäcktes dock av någon utanför organisationen, en registrerad eller annan. Att en knapp tredjedel av de anmälda antagonistiska incidenterna upptäckts genom organisatoriska rutiner och automatiserade processer kan vara resultatet av att verksamheterna har fungerande rutiner och tekniska säkerhetsåtgärder, och därmed till exempel identifierar och stoppar spam- och phishingmejl via spamfilter. Mot bakgrund av att phishingattacker är en av de vanligaste anmälda antagonistiska incidenterna är det dock också möjligt att fler angrepp kan förhindras via bättre tekniska säkerhetsåtgärder och organisatoriska kontroller och åtgärder.

En anställd på ett företag upptäckte att en supportserver blivit hackad och skickade ryska e-postmeddelanden. Vid granskning av meddelandena framkom att servern utnyttjats för en rysk phishingattack. Angriparna tog sig in i systemen via svagheter i en brandvägg.

PERSONUPPGIFTSINCIDENT ANMÄLD TILL DATAINSPEKTIONEN

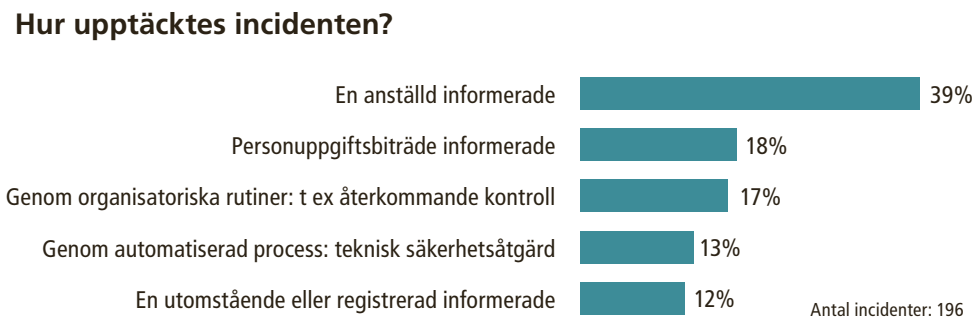

Bild 9. Fördelning avseende på vilket sätt incidenten upptäcktes.

Krypterad information

I majoriteten av incidenterna, sju av tio, har de anmälande verksamheterna angett att berörda personuppgifter inte varit krypterade. I 15 procent har de anmälande verksamheterna inte uppgett om berörda personuppgifterna varit krypterade. I ytterligare 15 procent av incidenterna har dock uppgifterna varit krypterade. I dessa anmälningar har inte framgått om krypteringen varit svag eller om angriparna fått tillgång till krypteringsnyckeln, varför det är svårt att bedöma allvarlighetsgraden i de fall angriparna kommit över krypterade personuppgifter.

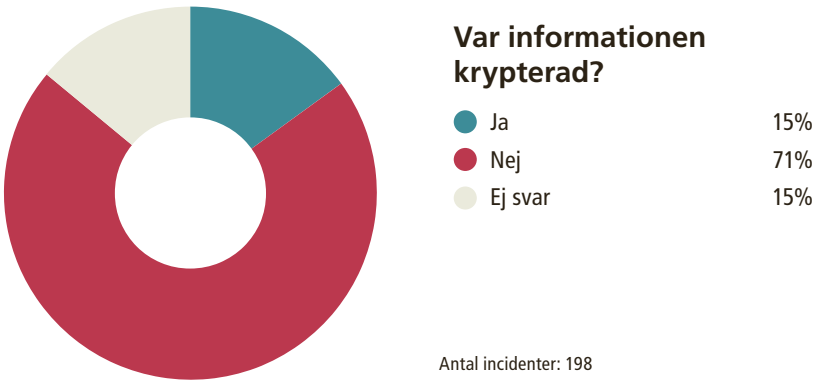

Bild 10. Andel av de antagonistiska incidenterna där personuppgifter varit krypterade.

Information till berörda

När en personuppgiftincident inträffar ska den anmälande verksamheten, det vill säga den personuppgiftsansvarige, bedöma risken för de personer som berörs. Om personuppgiftsincidenten sannolikt leder till en hög risk för berörda personers fri- och rättigheter ska de informeras. En huvudorsak till att berörda personer ska informeras är att de ska kunna

vidta åtgärder för att skydda sig mot effekterna av en personuppgiftsincident.[20]

Vid en fjärdedel av incidenterna har de anmälande verksamheterna bedömt allvarlighetsgraden som betydande eller mycket allvarlig. Andelen som informerat berörda personer är dock större och uppgår till drygt fyra av tio. Att en större andel valt att informera, än andelen som bedömer att allvarlighetsgraden är betydande eller allvarlig, kan indikera att verksamheterna eftersträvar att vara transparenta och vill påvisa att de tar ansvar och agerar seriöst vid it-angrepp.

I drygt en femtedel av incidenterna uppger verksamheterna att de kommer att informera berörda personer. I 17 procent av incidenterna har de anmälande verksamheterna inte tagit ställning om de ska informera, och i ytterligare 17 procent kommer berörda personer inte att få information om incidenten.

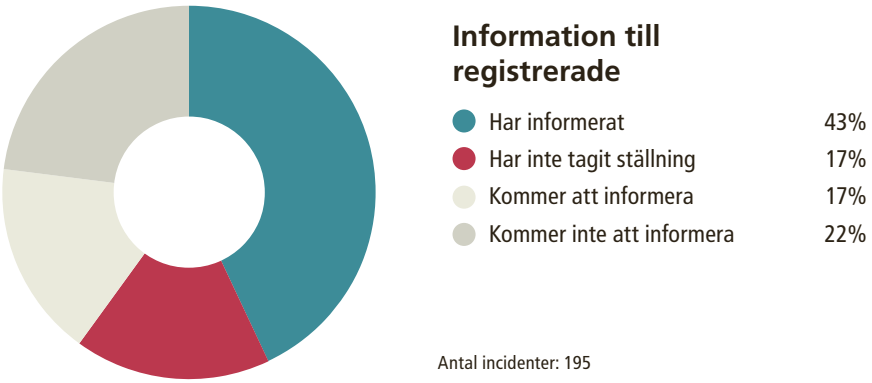

Bild 11. Andel som har informerat berörda personer om incidenten.

Incidenter som berör personer i andra länder

Dataskyddsförordningen gäller i hela EU och har till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter så att det fria flödet av uppgifter inom Europa inte hindras. Att över hälften av de anmälda antagonistiska incidenterna berör personer i andra länder är en följd av att främst det privata näringslivet idag har en stor internationell prägel.

20 Följer av artikel 34.1 i dataskyddsförordningen

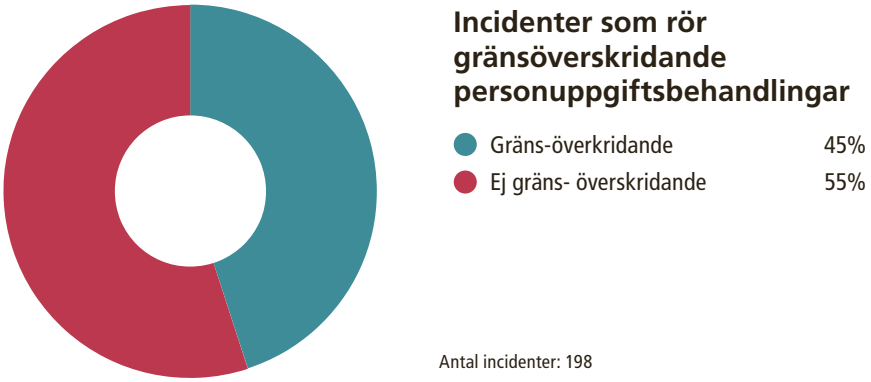

Bild 12. Andel incidenter som rör personer i andra länder.

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. I några fall där incidenten bedöms som särskilt allvarlig, incidenten inte har rapporterats i tid eller tillräckliga åtgärder inte har vidtagits, skickas incidenten över till myndighetens operativa enheter för övervägande om tillsyns ska inledas. Bedömningen görs med utgångspunkt i myndighetens tillsynspolicy och tillsynsplan.

Datainspektionens bedömning är att den stora merparten av de incidentanmälningar som inkommit under 2019 kommer att avslutas utan ytterligare åtgärd. Myndigheten utvecklar arbetet med personuppgiftsincidenter löpande, och under våren 2020 har myndigheten driftsatt en e-tjänst där personuppgiftsincidenter kan anmälas digitalt.

Kontakta Datainspektionen

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

Datainspektionen