2016-09-01

S L U T S K R I V E L S E

Till verkställande direktören
i skade- och livförsäkringsföretag

FI Dnr 16-2639
(Anges alltid vid svar)

Finansinspektionen
Box 7821
SE-103 97 Stockholm
[Brunnsgatan 3]
Tel +46 8 408 980 00
Fax +46 8 24 13 35
finansinspektionen@fi.se
www.fi.se

Enkätundersökning om beredskapsplan och uppdragsavtal i försäkringsföretag

Sammanfattning av undersökningen och slutsatserna

Finansinspektionen (FI) har genomfört en enkätundersökning under våren 2016 för att få en bild av försäkringsföretagens beredskap inför allvarliga avbrott, störningar eller kriser som gäller it-tjänster. Undersökningen grundas på bestämmelser i försäkringsrörelselagen (2010:2043)[1] och i EU-förordningen 2015/35[2].

De försäkringsföretag som deltagit i undersökningen får genom denna slutskrivelse en gemensam återkoppling av de viktigaste iakttagelserna. Syftet med slutskrivelsen är att sprida information om viktiga iakttagelser och att skapa medvetenhet kring vikten av heltäckande beredskapsplaner. Försäkringsföretagen ombeds även använda slutskrivelsen för att identifiera egna brister i förhållande till FI:s generella observationer.

Försäkringsföretagens beredskapsplaner omfattar i hög grad viktiga områden för verksamhetens återställning och kontinuitet i händelse av en incident. Test och uppdatering av planerna är inte lika omfattande. Centrala underleverantörer bör därför involveras mer i beredskapsplaneringen och testen av planerna.

Försäkringsföretagens svar visar att 37 procent av incidenterna som inträffar i it-verksamheten medför att viktiga arbetsuppgifter måste senareläggas och att 4 procent av incidenterna innebär att kritiska arbetsuppgifter måste senareläggas. Incidenter som rör kommunikation och infrastruktur tycks vara de svåraste att åtgärda baserat på att de ofta återkom. Dessa incidenter har också störst påverkan på verksamhetens viktiga och kritiska arbetsuppgifter.

[1] 10 kap. 3, 19-22 §§ försäkringsrörelselagen (FRL)
[2] Kommissionens delegerade förordning (EU) 2015/35 av den 10 oktober 2014 om komplettering av Europaparlamentets och rådets direktiv 2009/138/EG om upptagande och utövande av försäkringsverksamhet (Solvens II), artikel 258.3.

Vad gäller uppdragsavtal finns det god spridning bland leverantörerna men FI kommer att utreda om det finns underliggande koncentrationsrisker genom samarbete bland leverantörerna. Användningen av så kallade molntjänster är utbredd.

Observera att FI inom ramen för denna undersökning inte har tagit ställning till enskilda bolags beredskapsplaner i materiellt avseende och att det kan komma att granskas inom den löpande tillsynen.

Undersökningens syfte

Tjänster och affärsverksamheter inom den finansiella sektorn blir alltmer beroende av it och får allt större it-innehåll, t.ex. genom appar[3] och självbetjäning över internet. Samtidigt har fenomenet *Internet of Things* (att allt fler enheter blir internetbaserade) inneburit en drastisk ökning av antalet attacker mot olika delar av den internetbaserade infrastrukturen. Detta eftersom antalet ingångar till och integration med det globala nätverket har ökat.

För att kunna föra en relevant dialog med svenska försäkringsföretag om cyberrisker och operativa risker i it-verksamheten genomförde FI en heltäckande enkätundersökning med fokus på beredskapsplaner, inträffade incidenter och tredjepartsleverantörer.

Undersökningens utformning och övergripande resultat

Enkätundersökningen hade tre delar. I den första delen begärde FI information om försäkringsföretagens beredskapsplan. Med några få undantag har samtliga försäkringsföretag beredskapsplaner. Tester och uppdatering av beredskapsplanerna sker dock i varierande grad. För många försäkringsföretag skulle det även finnas flera fördelar i att involvera tjänsteleverantörerna mer när det gäller att ta fram och testa beredskapsplanerna.

I den andra delen begärde FI information om den senaste it-incidenten som försäkringsföretagen hade drabbats av. Här var FI i första hand ute efter en övergripande förståelse för vilken typ av incidenter försäkringsbranschen drabbas av, vilka konsekvenser olika typer av incidenter får och hur lång tid de tar att åtgärda. Sammanfattningsvis är problem med kommunikationstjänster utbrett. Sådana problem omfattade hela 40 procent av incidenterna och ledde ofta till att viktiga eller kritiska arbetsuppgifter måste senareläggas. Däremot var förekomsten av cyberattacker få och när skadlig kod upptäcks kan det i normalfallet åtgärdas inom tio timmar.

I den tredje delen begärde FI information om vilka underleverantörer som försäkringsföretagen använder för olika typer av tjänster. Många försäkringsföretag redogjorde även för om de skulle fortsätta att anlita eller

[3] Små program i mobiler och surfplattor.

säga upp sina nuvarande leverantörer. Vilka leverantörer som används förändras alltså hela tiden. Syftet med frågan var dock i första hand att identifiera centrala leverantörer och utbredningen av molntjänster. FI redovisar därför inte enkätresultatet vad gäller enskilda underleverantörer i denna slutskrivelse.

Skadecaptivebolagen har, med några få undantag, skickat in ofullständiga svar med hänvisning till att verksamheten sköts av tredje part. Dessa företag är därför inte medräknade i fördelningarna som anges, såvida det inte särskilt uppges.

Undersökningen omfattade även försäkringsgrupper. Dessa saknade i de flesta fall egna beredskapsplaner, egen infrastruktur och särskilda leverantörer av it-tjänster. Svaren från grupperna är i stället inräknade i solobolagens svar.[4]

Försäkringsföretag i undersökningen

Enkätundersökningen skickades till följande antal försäkringsföretag och försäkringsgrupper, uppdelade efter typ:

2	försäkringsgrupper
41	skadecaptives
28	livförsäkringsbolag
38	skadeförsäkringsbolag
8	unit-linkedbolag
40	större lokala försäkringbolag.

Observationer och FI:s rekommendationer

Beredskapsplaner
I stort sett alla försäkringsföretag har beredskapsplaner. Av försäkringsföretagen har dock 18 procent svarat att de inte har testat planerna det senaste året[5] och 47 procent har inte involverat tjänsteleverantörerna vid test av beredskapsplanerna. I 37procent av försäkringsföretagen har tjänsteleverantörerna heller inte varit delaktiga i framtagandet av beredskapsplanerna.

Beredskapsplanernas omfattning och tester kan komma att granskas i den löpande tillsynen. Försäkringsföretagen ska säkerställa att planerna täcker alla relevanta områden och att tjänsteleverantörerna, i förekommande fall, involveras samt i övrigt uppfyller aktuella bestämmelser.

[4] Bara två försäkringsgrupper är med i sammanställningen eftersom de har särskilda beredskapsplaner, infrastruktur och underleverantörer på gruppnivå.
[5] Om ett försäkringsföretag svarade ”nej” men samtidigt angav att test var inplanerat i närtid registrerades svaret som ”ja”.

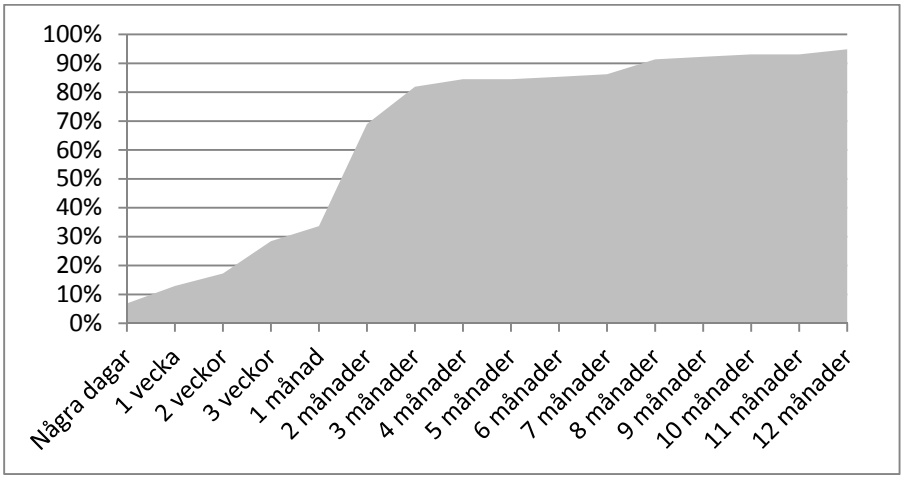
Incidenter

För att kartlägga it-incidenter som försäkringsbranschen i Sverige drabbas av valde FI en enkätmetod som ger en noggrann beskrivning av en specifik incident (den senaste), i stället för att alla typer av incidenter under ett år skulle beskrivas var för sig. Med ett tillräckligt stort urval, i detta fall mellan 110 och 116 försäkringsföretag[6], antar FI att frekvensen och påverkan som framkom i undersökningen är representativ för försäkringsbranschen i Sverige.

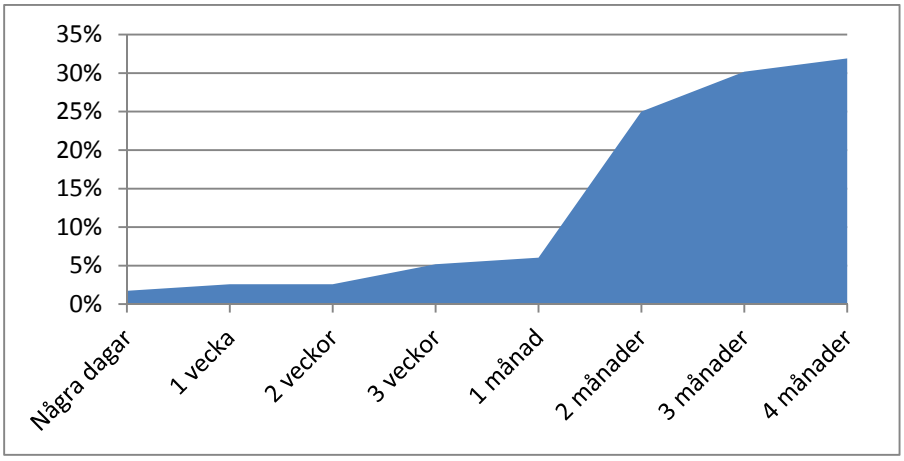
Det är få försäkringsföretag förunnat att, under en tolvmånadersperiod, inte uppleva några störningar i it-miljön. Om perioden maj 2015–april 2016 antas vara indikativ för hur en normal tolvmånadersperiod ser ut har ungefär vart tionde försäkringsföretag haft någon form av störning efter en vecka, ungefär vart tredje försäkringsföretag efter en månad, ungefär fyra av fem försäkringsföretag efter tre månader och nästan alla, 95 procent, efter ett år. Drygt hälften av störningarna har ingen eller liten påverkan på försäkringsverksamheten, medan ungefär en tredjedel av incidenterna gör att viktiga arbetsuppgifter måste senareläggas. Fyra procent av bolagen angav att deras senaste incident påverkade kritiska arbetsuppgifter[7].

Några av försäkringsföretagen som har angett att den senaste incidenten innebar att kritiska arbetsuppgifter fick senareläggas har inte rapporterat incidenten till FI, i enlighet med *Finansinspektionens allmänna råd (FFFS 2013:11) om rapportering av händelser av väsentlig betydelse*[8] eller 4 kap. *Finansinspektionens föreskrifter och allmänna råd (FFFS 2015:13) om tillsynsrapportering för försäkringsrörelse*. Försäkringsföretagen bör därför säkerställa att de riktlinjer, checklistor eller liknande som används för intern rapportering och hantering av incidenter även omfattar incidenter i it-miljön och kriterier för när sådana incidenter ska rapporteras till FI i enlighet med FFFS 2015:13.

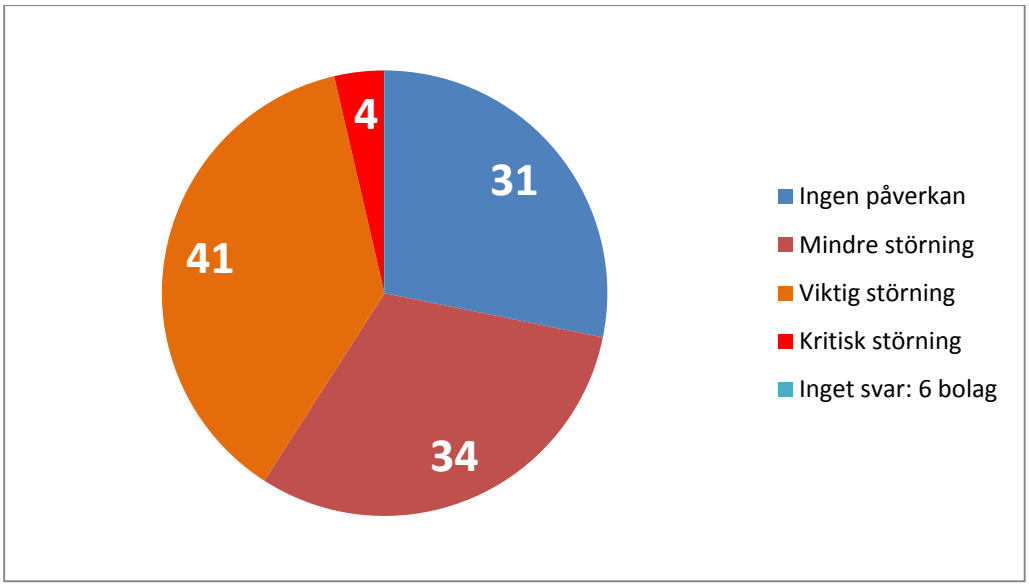
[6] Skadecaptives är inte inkluderade i urvalet och alla försäkringsföretag svarade inte på alla frågor.
[7] Frågan som skulle besvaras var om incidenten inte påverkade verksamheten alls eller om mindre viktiga, *viktiga* eller *kritiska* arbetsuppgifter fick senareläggas.
[8] Den 1 januari 2016 ersattes FFFS 2013:11 av *Finansinspektionens allmänna råd (FFFS 2015:15) om rapportering av händelser av väsentlig betydelse*.



Figur 1: Hur många försäkringsföretag har haft störningar i it-miljön efter viss tid?



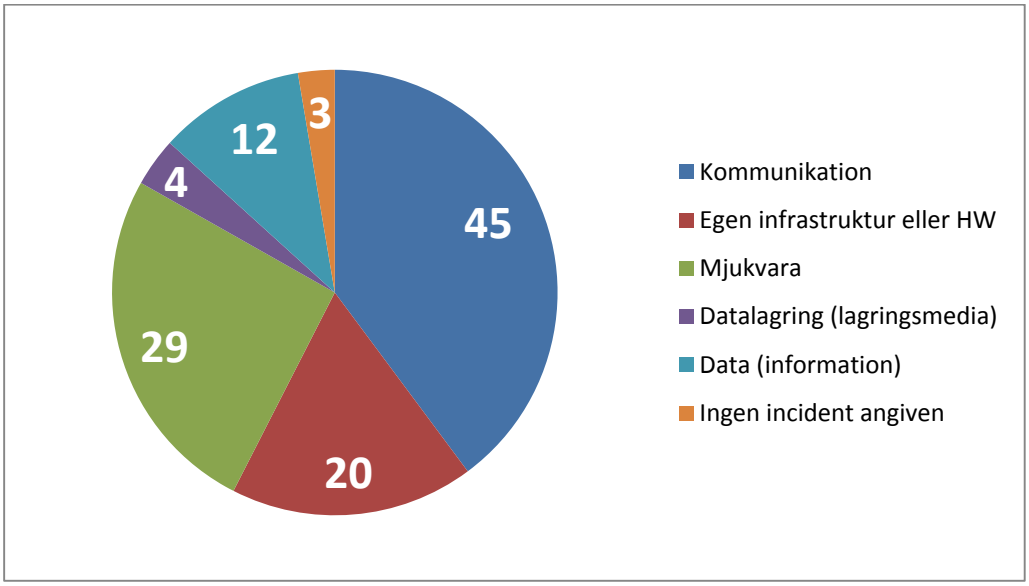
Figur 2: Hur många försäkringsföretag har haft allvarliga störningar i it-miljön efter viss tid?



Figur 3: Hur påverkades försäkringsföretaget av störningen (antal)?

Undersökningen visar att 25 procent av alla incidenter beror på återkommande fel. Detta är incidenter som försäkringsföretaget har drabbats av tidigare men som alltså inte lösts tillfredsställande.

FI frågade också hur lång tid det tog att åtgärda den senaste incidenten i it-miljön. Frågan har dock tolkats olika av försäkringsföretagen, där några har angett löpande timmar från det att incidenten inträffat medan andra har angett arbetstimmar. FI utesluter därför i huvudsak dessa enkätsvar i analysen.



Figur 4: Var uppstår störningar oftast i it-miljön i svenska försäkringsföretag (antal)?

Ungefär var femte incident är kopplad till handhavandefel och ungefär var tionde incident beror på skadlig kod. Andra typer av cyberattacker står för 3 procent av incidenterna. Ungefär var tredje incident kopplad till skadlig kod påverkar viktiga eller kritiska arbetsuppgifter i verksamheten, men problemen från merparten av dessa incidenter (ungefär 9 av 10) tar mindre än tio timmar att åtgärda[9].

Uppdragsavtal

Sjuttio procent av de svenska försäkringsföretagen[10] har lagt ut någon del av it-verksamheten till moder- eller systerbolag. Motsvarande andel för svenska skadecaptives är 54 procent, medan 29 procent av svenska skadecaptives anlitar någon av de två stora aktörerna på marknaden för heltäckande tjänster för skadecaptivebolag. Resterande skadecaptives anlitar andra leverantörer[11].

[9] Med antagandet att åtgärder påbörjas direkt när incidenten har upptäckts.
[10] Exklusive skadecaptives.
[11] Tre skadecaptives har inte svarat på frågan.

Förekomsten av uttalade molntjänster och tjänster som skulle kunna knytas till molntjänster är utbredd.

Med undantag för skadecaptivebolagen har uppdragsavtal inom försäkringsbranschen i Sverige god spridning bland tjänsteleverantörerna. Vid tidpunkten för denna slutskrivelse har FI inte analyserat hur samarbetet mellan tjänsteleverantörerna ser ut. Stickprov indikerar dock att samarbete i någon form, mellan tjänsteleverantörerna, är norm på marknaden.

Sammanställning av vissa av enkätsvaren

Beredskapsplaner

Hur många försäkringsföretag har en beredskapsplan?

Försäkringsgrupper	100 %
Skadecaptives	90 %
Livförsäkringsbolag	100 %
Skadeförsäkringsbolag	100 %
Unit linked-bolag	100 %
Större lokala försäkringbolag	100 %

Vad omfattar beredskapsplanerna?

Kommunikation	96 %
Egen infrastruktur och hårdvara (HW)	96 %
Mjukvara (SW)	97 %
Datalagring	97 %
Information (data)	97 %
Nyckelkompetenser	95 %
Lokaler	93 %

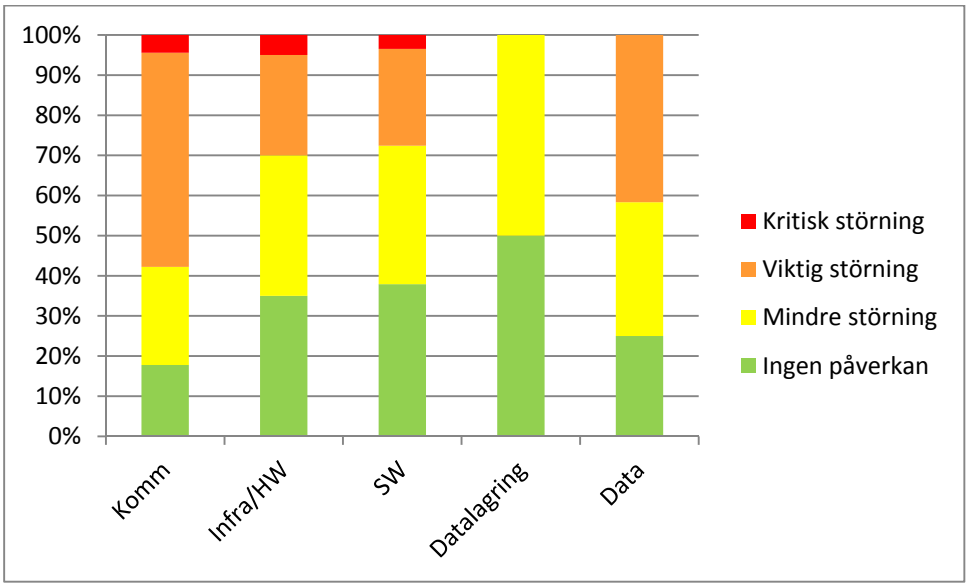
- 93 procent av de försäkringsföretag som har beredskapsplaner testar dem regelbundet.

- 82 procent av de försäkringsföretag som har beredskapsplaner har testat hela eller någon del av planerna det senaste året.

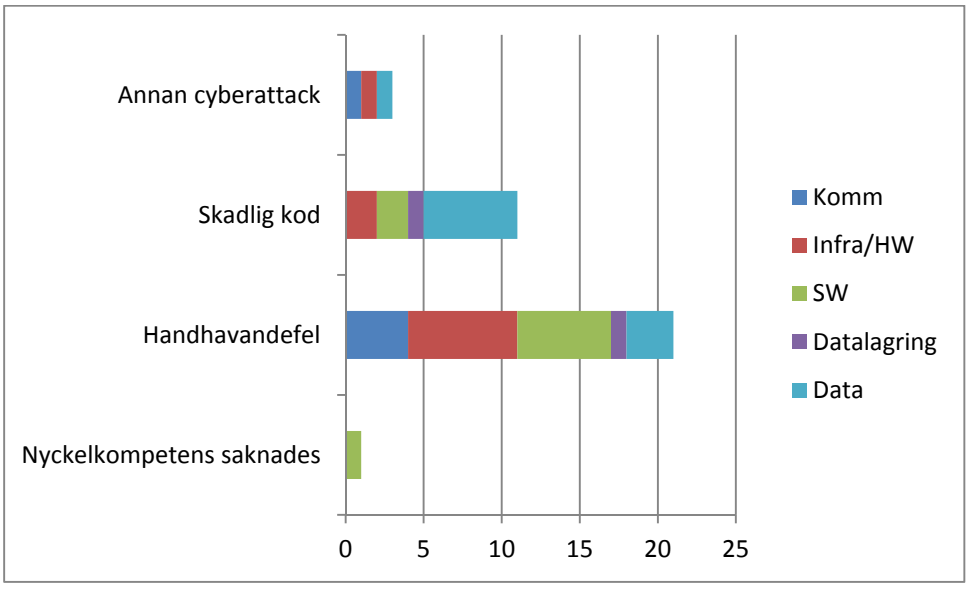
- 63 procent av de försäkringsföretag som har beredskapsplaner har involverat tjänsteleverantörerna när beredskapsplanerna har tagits fram.

- 53 procent av de försäkringsföretag som har beredskapsplaner och testar dem regelbundet har involverat sina tjänsteleverantörer när testerna har utförts.

Incidenter[12]

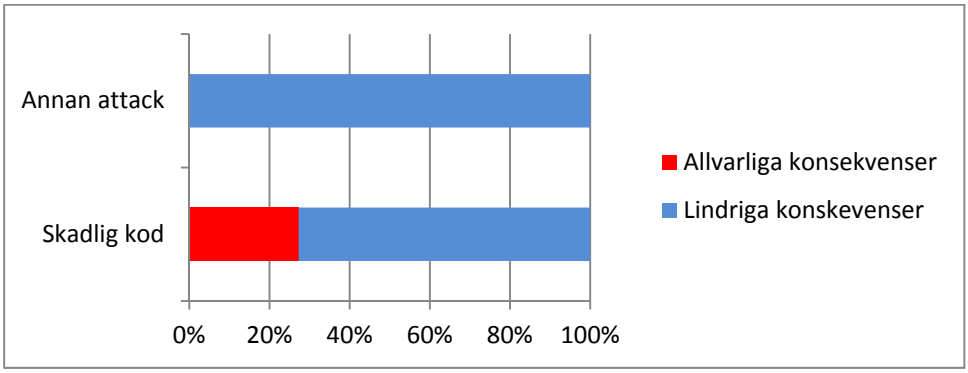


Figur 5: Hur påverkas försäkringsföretagen av olika typer av incidenter?

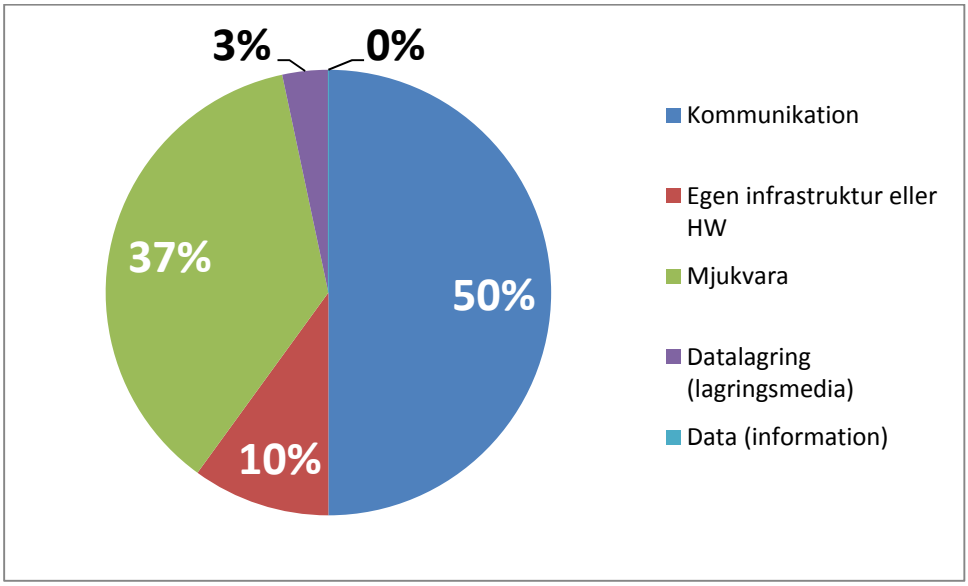


Figur 6: Har incidenterna koppling till någon av de fyra specificerade händelserna?

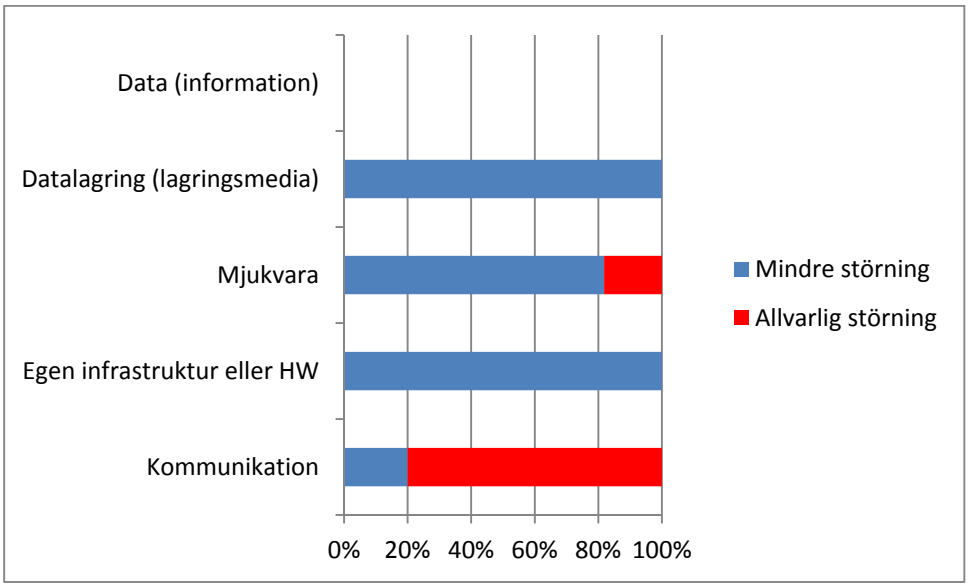
[12] Exklusive skadecaptives.



Figur 7: Hur allvarliga är konsekvenserna av cyberattacker?



Figur 8: Vilken typ av fel återkommer oftast? (Inget bolag uppgav att den senaste incidenten som rörde data var återkommande.)



Figur 9: Hur påverkar återkommande fel verksamheten? (Inget bolag uppgav att den senaste incidenten som rörde data var återkommande.)

FI:s fortsatta arbete

Resultaten från enkäten kan komma att användas när FI utformar tillsynsplanerna för branschen. I förekommande fall kan resultaten också bidra till att prioritera frågor i den löpande tillsynen av enskilda försäkringsföretag.

FI kommer vid ett senare tillfälle att ta ställning till om en enklare variant av enkäten ska genomföras regelbundet, i första hand för att följa upp frekvensen av olika typer av incidenter och hur branschen påverkas.

Övrigt

FI påminner om skyldigheten enligt 10 kap. 21 § FRL att anmäla uppdragsavtal, som gäller sådan operativ verksamhet eller sådana funktioner som är av väsentlig betydelse, till FI innan avtalet börjar gälla. Enligt samma bestämmelse är försäkringsföretag även skyldiga att snarast möjligt anmäla väsentliga förändringar inom den operativa verksamheten eller funktionerna till FI.

I aviseringsbrevet, som skickades ut innan enkäten, bad vi företagen att kontrollera att FI hade uppdaterade kontaktuppgifter till regelansvarig i företaget. Efter uppdatering visade det sig dock att ett antal adressater blev felaktiga. Felet berodde på att de uppdaterade uppgifterna inte hade bekräftats av användaren. När uppgifter i systemet har uppdaterats måste de bekräftas för att ändringen ska registreras. I systemet finns en flik som heter ”Bekräftelse av uppgifter”, där det finns en knapp där gjorda ändringar ska bekräftas.

FINANSINSPEKTIONEN

Ellinor Samuelsson
Avdelningschef
Risktillsyn försäkring

Per Haaland
Senior finansinspektör