Digitalisaatio ja pankkipalvelut, Pasi Korhonen

PM

31.5.2024
SP/FIVA-EI RAJOITETTU
Julkinen

Teemakyselyn yhteenveto: IT- ja tietoturvariskien hallinta vahinko- ja henkivakuutusyhtiöissä

1 Bakgrunden till den tematiska bedömningen samt slutsatser

Tillsynen av den alltmer digitaliserade finansiella sektorn är ett av fokusområdena i Finansinspektionens strategi. Finansinspektionen har haft en lägesbild om betydande finansiella aktörers beredskapsläge utifrån den kontinuerliga tillsynen samt tidigare inspektioner och tematiska bedömningar. En enhetlig övergripande bild av den finansiella sektorns läge har dock saknats.

Finansinspektionen genomförde en tematisk bedömning om beredskapsläget hos betydande finansiella aktörer i Finland i april–maj 2024, dvs. hur betydande finansiella aktörer har säkerställt sin motståndskraft mot störningar både under normala förhållanden och för undantagsförhållanden.

Den tematiska bedömningen baserar sig på en tematisk enkät som genomförts för betydande finansiella aktörer. I enkäten utreddes organiseringen av beredskap samt beredskapsläget för störningar i företagens verksamhet. Enkäten bestod av 40 frågor som har utarbetats utifrån Finansinspektionens Föreskrifter och anvisningar 8/2014 "Hantering av operativa risker i företag under tillsyn inom finanssektorn". Enkäten skickades till 22 företag, varav samtliga svarade på enkäten.

Slutsatserna från den tematiska bedömningen baserar sig på företagens svar och de har inte verifierats av Finansinspektionen. Flera av de företag som svarat på enkäten har under de senaste åren genomgått Finansinspektionens inspektion av hanteringen av IT- och dataskyddsrisker som innehållit också kontinuitets- och beredskapsplanering. Observationerna från inspektionerna är i linje med de svar som man fått i den tematiska enkäten.

Betydande företag under tillsyn inom finansiella sektorn har organiserat sin verksamhet i enlighet med kraven på kontinuitets- och beredskapsplanering så att verksamhetens motståndskraft mot störningar både under normala förhållanden och för undantagsförhållanden har säkerställts. Inga betydande skillnader i beredskapen observerades mellan tillsynssektorerna. Företagen under tillsyn har i sin egen verksamhet observerat enskilda brister som korrigeras enligt riskhanteringsprocessen.

Utifrån de enkätsvar som företagen gett observerades följande:
- En del aktörer hade brister i den regelbundna testningen av kontinuitetsplanerna.
- En del aktörer hade inte aktuella återställningsplaner eller så hade återställningsplanerna inte testats regelbundet.

- Beredskapsnivån och de målsatta återställningstiderna i samband med den kan vara, och är, på olika nivåer i uppdaterade transaktionsbaserade betalsystem, till exempel i samband med kortbetalningar, jämfört med utbetalningen av lagstadgade pensioner (ArPL, trafikförsäkring, lagstadgad olycksfallsförsäkring) eller i samband med risklivförsäkring och försäkringsplacering.
- I samband med tillsynen är det skäl att göra en mer exakt bedömning av risken vid geografisk diversifiering av ICT-infrastrukturen, till exempel i anslutning till kritiska datacentralfunktioner, samt vid förvaltning av säkerhetskopior.

Enkätresultaten bidrar till att rikta kontinuerlig tillsyn både allmänt och företagsspecifikt. Resultaten används i planeringen av inspektioner som gäller hanteringen av IT- och informationssäkerhetsrisker.

I regel ska man i den kontinuerliga tillsynen och i eventuella separata inspektioner fästa särskild uppmärksamhet vid en regelbunden uppdatering, testning och övning av kontinuitets- och återställningsplaner samt vid den fysiska IT-infrastrukturens beredskapsförmåga när det gäller geografisk diversifiering.

I svaren framkom inga sådana brister i verksamheten hos enskilda företag under tillsyn som skulle kräva att Finansinspektionen uppmanar företaget att vidta omedelbara åtgärder för att korrigera bristen. Korrigeringen av bristerna är redan i gång eller så har bristerna inte varit allvarliga. Korrigeringen av brister kommer dock att följas upp i samband med den kontinuerliga tillsynen och inspektionerna.

Förordningen (DORA[1]), som gäller finansiella sektorns digitala motståndskraft, förenhetligar kraven i EU-området och medför samtidigt nya krav. DORA kommer att tillämpas från och med den 17 januari 2025. Kraven och anvisningarna som gäller den nationella beredskapen förblir oförändrade. Utifrån den tematiska bedömningen har de betydande finansiella företagen under tillsyn förmåga att iaktta de krav som DORA ställer för motståndskraften mot störningar.

2 Kontinuitetsplanering

Med kontinuitetsplanering avses säkerställande av förmågan att upprätthålla verksamheten och begränsa förluster i händelse av olika slag av störningar i verksamheten. Hit hör till exempel skador eller avsiktliga handlingar som drabbar personalen, lokalerna, IT-systemen eller datakommunikationerna samt vattenskador, eldsvådor och avbrott i exempelvis el-, värme- eller vattenförsörjningen. Inom ramen för kontinuitetsplaneringen

[1] Digital Operational Resiliency Act, länk https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32022R2554&qid=1682057478749

upprättas kontinuitetsplaner för viktiga verksamheter för att upprätthålla verksamheten i händelse av eventuella störningar.

I regel uppfyller företagen under tillsyn de krav som ställs på kontinuitetsplaneringen. Det finns uppdaterade och tillräckliga kontinuitetsplaner för företagets centrala verksamheter. Företagen under tillsyn har ett tydligt handlingsmönster för upprättande, underhåll och testning av kontinuitetsplaner och för uppföljning av kontinuitetsplaneringen. För IT-systemen upprättas återställningsplaner med beskrivningar av hur olika datasystem kan fås funktionsdugliga efter allvarliga störningar eller katastrofer. Kontinuitetsplanerna uppdateras regelbundet. Kontinuitetsplanerna testas och övningar ordnas regelbundet.

Brister har dock identifierats i den regelbundna testningen av kontinuitetsplanerna och i den regelbundna uppdateringen och testningen av återställningsplanerna.

3 Beredskap för undantagsförhållanden

Beredskapsplaneringen, dvs. beredskapen för undantagsförhållanden bygger på kontinuitetssystemen för normala förhållanden. Med undantagsförhållanden avses situationer enligt 3 § i beredskapslagen.

En störning under undantagsförhållanden varar i typiska fall längre än situationer för vilka det finns beredskap i kontinuitetsplanen för normala förhållanden. Hot under undantagsförhållanden är vidare i regel allvarligare än de hot för vilka kontinuitetsplaner upprättas.

Beredskap för undantagsförhållanden kan också tillämpas på andra allvarliga störningar och kriser än undantagsförhållanden enligt beredskapslagen. Allvarliga störningar och kriser kan uppstå till exempel vid allvarliga hot mot personalens handlingsförmåga eller förstörelse av lokaler eller datormiljö hos företag under tillsyn.

I vissa svar framkommer det att IT-infrastrukturen inte fullständigt diversifierats geografiskt. Regleringen ger för närvarande inte en exakt bestämning på hur infrastrukturen bör diversifieras, men i regel bör respondenterna beakta att längre el- eller dataavbrott i enskilda områden bör uppmärksammas. Risken för el- eller dataavbrott på grund av naturkatastrofer är relativt liten i Finland, men olyckor eller avsiktliga påverkansförsök höjer risknivån till exempel i situationer där IT-infrastrukturen har placerats i en enskild datacentral eller dubblerats till lägen som geografiskt ligger nära varandra. Utan diversifiering kan IT-infrastrukturens funktion bli sårbar till exempel på grund av påverkan eller en olycka i anslutning till den omgivande infrastrukturen, till exempel i en situation där elförsörjningen avbryts till följd av en allvarlig störning eller en cyberattack. Ett scenario där den kritiska datakommunikationen som betjänar den odiversifierade IT-infrastrukturen av någon

orsak inte är tillgänglig eller inte kan fungera med full kapacitet är också möjligt.

4 Beredskapsplanering

Med beredskapsplan avses en förhandsbeskrivning av de åtgärder som de beredskapsskyldiga vidtar för att säkerställa kontinuiteten i verksamheten vid allvarliga störningar under normala förhållanden och för undantagsförhållanden. Beredskapsplanen kan ingå i kontinuitetsplanen, förutsatt att den i tillräcklig mån beaktar behoven av beredskap för undantagsförhållanden. Hos de flesta företag ingår beredskapsplanen i kontinuitetsplanen.

En del av respondenterna har identifierat brister i testningen av beredskapsplanerna till exempel beträffande återställningen från störningar. Företagen har utarbetat beredskapsplaner men hade inte övat eller testat dem på många år till exempel när det gäller brandmurar eller utbetalningen av pensioner.

I de fall där den bristande övningen eller testningen av beredskaps- och återställningsplanernas funktion eller utmaningarna i uppfyllandet av målnivån höjer risknivån för säkerställandet av kontinuiteten i normala förhållanden är det värt att beakta att detta också höjer risknivån för beredskapen för undantagsförhållanden på ett betydande sätt. Det kan antas att återställningsförmågan efter mer allvarliga och komplexa scenarier under undantagsförhållanden är lägre än vid scenarier i normala förhållanden.

Den nationella försörjningsberedskapen bör säkerställas också i fall där respondenterna utöver betalningsrörelsen och finansieringstjänsterna sköter andra lagstadgade skyldigheter, till exempel utbetalningen av pensioner (ArPL-aktörer, skadeförsäkringsaktörer).