FSPOS

Finansiella Sektorns Privat-Offentliga Samverkan

Kriskommunikation i finanssektorn – en vägledning vid större störningar

Kunskapsöversikt: Cyberangrepp

FSPOS AG INFO

Innehållsförteckning

1. Sammanfattning

FSPOS Arbetsgrupp Information (AG Information) har under 2016 tagit fram denna rapport för att aktörerna i finanssektorn ska vara väl förberedda inför de kommunikationsinsatser som krävs om en eller flera medlemmar drabbas av ett större cyberangrepp som kan riskera att hota det finansiella systemet.

Det finns två skäl till behovet av denna rapport: Dels bygger finanssektorn och dess infrastruktur på komplexa IT-system som vid ett större cyberangrepp kan påverka den finansiella stabiliteten. Dels visar erfarenheterna från den senaste finanskrisen 2008 hur viktigt det är att sektorn har klara riktlinjer för sin kommunikation.

När bankernas och myndigheternas kommunikation utvärderades 2010 fick sektorn godkänt för sin kommunikation under det akuta skedet, men kritik för sin förmåga att kommunicera risker – i korta drag – för sent, för lite och för otydligt. Enskilda aktörer kan dessutom ha förvärrat krisen genom kommunikativa misstag[1].

AG Information[2] anser är att följande principer ska prägla kommunikationen vid ett cyberangrepp eller annan större störning som kan riskera att hota det finansiella systemet och stabiliteten i Sverige:

- De berörda aktörerna bör vara öppna, snabba och tydliga i sin egen kriskommunikation vid till exempel cyberangrepp och se till att den är väl förankrad i den egna löpande verksamheten.
- De berörda aktörerna bör undvika situationer med bristande öppenhet och avsaknad av kommunikation eftersom sådana riskerar att spä på rykten och öka osäkerheten och få till följd att en kris skapas.
- De berörda aktörerna bör samverka för att upprätthålla kommunikation som främjar den finansiella stabiliteten.

Denna vägledning är en fördjupning till den rekommendation som togs fram 2010 om kriskommunikation. FSPOS har även publicerat en vägledning om krishantering. Den här rapporten rör dock specifikt kommunikationsarbetet vid ett angrepp.

---

[1] *http://www.fspos.se/siteassets/fspos/rapporter/2010/storbankernas-och-myndigheternas-kommunikation.pdf*

[2] *Förutom Handelsbanken, för fullständig lista över medlemmarna – se FSPOS hemsida fspos.se.*

2. Inledning till vägledningen

På senare år har det blivit allt vanligare att cyberangrepp ligger bakom samhällsstörningar. Ett aktuellt exempel är intrånget 2016 som drabbade centralbanken i Bangladesh där drygt 80 miljoner dollar försvann. Ett annat exempel är från Sydkorea 2013 då tre stora banker utsattes för ett cyberangrepp som slog ut cirka 30 000 datorer och servrar.

Det finansiella systemet är ekonomins blodomlopp och det är lätt att tänka sig att det relativt snabbt uppstår en fullskalig kris om det inte är möjligt att betala, ta emot pengar eller få lön. Denna kan dessutom förvärras om banker och myndigheter upplevs som slutna, eftersom brist på information skapar utrymme för rykten och spekulationer. Här finns dessutom risken att en operativ kris utvecklar sig till en finansiell sådan med allt vad det innebär av interna utmaningar. Därför ställs höga krav på öppenhet hos alla berörda aktörer inom den finansiella sektorn.

För att uppfylla kraven bör varje aktör, privat såväl som offentlig, ta sitt ansvar att aktivt kommunicera kring sin egen verksamhet. Vid allvarliga cyberangrepp mot finansiell infrastruktur bör det finnas en ordnad struktur för att hantera de eventuella målkonflikter som kan uppstå mellan aktörerna. Denna vägledning är tänkt att underlätta en sådan struktur. Erfarenheterna från den senaste finanskrisen och från nyligen genomförda övningar - där cyberangrepp varit ett av alla inslag – är en viktig utgångspunkt. Vägledningen består av tre delar:

1. Ett avsnitt om **de kommunikativa utmaningar** som bör hanteras vid cyberangrepp eller andra större störningar. Detta bygger på en gemensam diskussion mellan banker, myndigheter och branschorganisationer. Vi går här igenom de specifika fällor för öppen och aktiv kommunikation som sektorns aktörer bör undvika.

2. En **vägledning för sektorns kriskommunikation** vid cyberangrepp eller andra allvarliga störningar som kan riskera att hota den finansiella infrastrukturen eller stabiliteten (mallar finns i appendix).

3. En **kunskapsöversikt om cyberangrepp i finanssektorn**, aktörer, tillvägagångssätt och konsekvenser för sektorns gemensamma kommunikation. Avsnittet inkluderar två fallstudier av relevanta händelser i Storbritannien och USA.

3. Kommunikativa utmaningar

Ett större cyberangrepp eller någon annan liknande störning kan förväntas innebära komplexa målkonflikter för de berörda aktörerna. Det kan handla om olika intressen på kort och på lång sikt, både för aktörernas egen del och för sektorn som helhet. Dessa utmaningar kräver att vi har ett gemensamt förhållningssätt samt överenskomna rutiner och metoder för kommunikationen (se nästa kapitel, *Vägledning för kriskommunikation vid cyberangrepp*).

3.1 Slutsatser för samordnad kommunikation

Kriskommunikationen kan vara avgörande vid hanteringen av alla sorters samhällsstörningar. Vid till exempel en skogsbrand eller översvämning bidrar kommunikationen till att resurserna kan utnyttjas mer effektivt och till att allmänheten kan bidra till att minska riskerna och konsekvenserna. Det finansiella systemet bygger dock i högre grad på tillit. Själva systemets stabilitet bygger på förtroende, vilket innebär att misslyckad kommunikation kan utgöra själva orsaken till samhällsstörningen. Samtidigt kan lyckad kommunikation vara avgörande för lösningen.

- Effektivt samordnad kommunikation vid cyberangrepp eller annan större störning mot finansiell infrastruktur förutsätter två saker: Dels att varje aktör, privat såväl som offentlig, tar ett ansvar att aktivt kommunicera kring sin egen verksamhet. Dels att det finns en gemensam syn mellan berörda aktörer - tillsynsmyndigheter, finansinstitut och leverantörer - att vara transparent med vad man vet, och framför allt med vad man ännu inte vet.

- Varje aktör behöver dels egna interna rutiner för samverkan mellan IT, kommunikation och beslutsfattare, dels ha god kännedom om den finansiella sektorns gemensamma rutiner för kriskommunikation. Målet bör vara att främja arbetssätt som möter utmaningarna och säkrar en väl fungerande kriskommunikation vid en större störning. Samverkan om behov av gemensam lägesbild kan initieras av berörd aktör men leds av relevant myndighet (Finansinspektionen eller Riksbanken beroende på vad det är för störning).

- Gemensamma arbetssätt behöver en ordnad struktur som tillåter temporär utvidgning eller begränsning av gruppen, eftersom det är svårt att förutse exakt vilka parter som behöver samverka vid oväntade förlopp. Cyberangrepp kan leda till mycket komplexa situationer med behov av kommunikation över organisations-, sektors- eller nationsgränser. För att skapa trygghet för involverade aktörer bör samordningen ledas av relevant myndighet.

Att komma överens och skapa tillit är en nyckel till förmågan att värna den finansiella stabiliteten vid cyberangrepp. Det är avgörande att det finns en gemensam uppfattning om vilka förväntningar som finns på varje aktör och förankrade överenskommelser om hur information ska delas. Överenskommelserna måste också vara förankrade innan krisen är ett faktum – under krisens gång är det för sent.

3.2 Fällor att vara förberedd på och att undvika

Osäkerhet om vad som kan kommuniceras

Vid cyberangrepp råder det inledningsvis ofta stor osäkerhet om vad som har hänt och hur verksamheten påverkas. Denna osäkerhet kan ha flera orsaker, exempelvis att det är en extern tjänsteleverantör som drabbats eller att flera aktörer har problem.

Det finns därför en risk att aktörer dröjer med att kommunicera externt i väntan på bekräftad information om vad som har hänt och hur stora problem som har uppstått. Ett sådant handlingssätt kan skapa ett informationsvakuum som kan fyllas av andra aktörer och leda till rykten som är svåra att stävja i ett senare skede. Om de som genomför cyberangreppen har en förberedd kommunikationsstrategi som en del av en påverkanskampanj, eller för att uppnå ideologiska mål, ökar risken att de når framgång.

Slutenhet på grund av interna processer och konkurrens

Oförmåga att kommunicera kan ha flera orsaker. Oavsett skäl är konsekvensen att organisationen eller sektorn uppfattas som sluten av kunder, medier och allmänhet. Ett skäl till oförmågan kan vara att cyberangrepp uppfattas som ett i huvudsak tekniskt problem. Det kan leda till att svårigheter inte rapporteras uppåt till styrelsen/ledningen tillräckligt snabbt. Den som misslyckats med att stävja problemet kan även i värsta fall dröja med att varsla andra delar av organisationen för att kortsiktigt undvika klander.

En annan orsak till slutenhet kan vara ett snävt synsätt på branschens förtroende. Det kan finnas kortsiktiga incitament för att hålla sig ”långt bort” när en konkurrent är utsatt och förlorar pengar, eller att försöka undvika att ”gå ut först” om man själv är drabbad, vilket medför en tendens att hålla sig utanför samverkan och informationsdelning. Organisationen riskerar därmed att gå miste om viktig information från andra aktörer och utrymmet för rykten, spekulation och osäkerhet ökar.

Ytterligare ett skäl till slutenhet kan vara att man saknar en helhetssyn på den finansiella sektorns beroenden och inte förstår sin egen samhällsviktiga roll. Sådana uppfattningar kan göra att man avstår från att kommunicera samt att samverka och dela information med andra aktörer. Detta kan i sin tur leda till att en händelse får spridningseffekter och negativa konsekvenser för den finansiella sektorn som helhet.

Överskattning av krisen

När krisen är oundviklig kan en aktör överdriva hur avancerad attacken är för att ge sken av att det var omöjligt att försvara sig mot den. Strategin kan upplevas som ett skydd mot kritik för att ha investerat för lite i informations- och cybersäkerhet. Ett sådant förhållningssätt skadar informationsutbytet och möjligheterna att upprätta en samlad lägesbild för branschen som helhet.

Underskattning av krisen

När krisen är oundviklig kan en aktör även *underskatta* hur avancerad attacken är och ta ut segern i förskott. Myndigheter, medier, kunder och interna beslutsfattare ställer hårda krav på att aktörens funktionalitet snabbt ska återställas och att exempelvis banktjänster ska vara tillbaka i stabil drift. Frestelsen att kommunicera kontroll över situationen i en komplicerad teknikmiljö riskerar att underminera den samlade lägesbilden och kan få andra parter att agera utifrån en felaktig analys. Förtroendet på längre sikt riskerar att skadas, dels för den enskilde aktören, dels för sektorn som helhet. På motsvarande sätt som under rubriken ”Osäkerhet” ovan, kan detta vara särskilt allvarligt om cyberattacken är en del av en större påverkanskampanj, där angriparen också har en egen kommunikationsstrategi.

Brist på helhetsperspektiv

En central utmaning vid cyberangrepp är risken att en enskild aktörs kortsiktiga intressen kan hota den finansiella stabiliteten, vilket även drabbar den enskilde aktören på längre sikt. När stuprörstänkade råder mellan funktioner och aktörer riskerar beslutsfattare, tekniker och kommunikatörer att göra sämre samlade analyser och bedömningar, vilket kan leda till negativa konsekvenser för samhället i stort.

4. Vägledning för kriskommunikation

4.1 Syftet med vägledningen

Denna vägledning tar sin utgångspunkt i de principer som togs fram 2010[3]; öppenhet, tydlighet, snabbhet, tillgänglighet och samverkan. Mer specifikt pekar vi här på *hur* sektorn ska kunna kommunicera aktivt, transparent och tydligt i en situation med stora osäkerheter och betydande kommunikativa utmaningar. Den kris vi har i tankarna är någon form av större cyberangrepp som kan riskera att hota den finansiella infrastrukturen, men vägledningen fungerar även vid andra större sektorsstörningar.

Med god, samordnad kriskommunikation kan aktörerna i den finansiella sektorn snabbt möta allmänhetens, kundernas och mediernas frågor. Det ökar möjligheterna att motverka motstridiga budskap och ryktesspridning samt minska gapet mellan krisen och *bilden* av krisen. Viktigast av allt: Aktiv och korrekt information minskar *konsekvenserna* av störningen och bidrar därigenom till att bibehålla och stärka förtroendet för sektorn och stabiliteten i det finansiella systemet.

Det strukturerade arbetssättet gör också sektorns aktörer bättre förberedda vid samhällsstörningar eller kriser som kräver samordning med aktörer i andra sektorer eller vid samverkan med andra aktörer i den finansiella infrastrukturen.

---

[3] *http://www.fspos.se/siteassets/fspos/rapporter/2011/rekommendationer_for_kommunikation.pdf*

Målet är att vägledningen ska nyttjas vid störningar och kriser som kräver strategisk och samordnad kriskommunikation.

4.2 Grundläggande utgångspunkter

Vid samverkan om kriskommunikation för att motverka angrepp eller större störningar i den finansiella sektorn bör följande gälla:

- De berörda aktörerna bör vara öppna, snabba och tydliga i sin egen kriskommunikation och se till att den är väl förankrad i den egna löpande verksamheten.
- Berörda aktörer har ansvar att signalera till myndighet som då kan initiera samverkan. Det finns en gemensam syn hos alla aktörer att vara transparenta med vad man vet, och framför allt med vad man ännu inte vet.
- Vi är överens om att det är fullt möjligt att i samverkan dela och inhämta kommunikativa lägesbilder för att få en bättre förståelse för händelsen och samtidigt respektera aktörernas respektive roller i det finansiella systemet.
- Vi utvärderar aktivt effekterna av kommunikationen.

4.3 Förhållningssätt vid aktiv kommunikation

- Att kommunicera samordnat innebär *inte* att säga samma sak utan att dela sin lägesbild till ansvariga myndigheter och att kommunicera transparent kring de risker man ser för sin egen verksamhet. En lägesbild bör kunna delas även om det självklart inte går att ge sekretessbelagd information till en större krets.
- Alla aktörer i den finansiella sektorn bör agera och kommunicera på ett sätt som bidrar till att stärka robustheten i, och upprätthålla förtroendet för, det finansiella systemet i Sverige som helhet. För att uppnå detta bör samtliga aktörer i sin kommunikation sträva efter att vara så öppna, tydliga, snabba och proaktiva som möjligt i sin externa kommunikation.
- Varje aktör förväntas ansvara för kommunikationen kring sin egen verksamhet och inom sitt ansvarsområde.
- Stor vikt läggs vid proaktivitet och samverkan mellan berörda myndigheter och mellan myndigheterna och de privata aktörerna samt branschorganisationer för att värna förtroendet för det finansiella systemet.

4.4 Förutsättningar för god kriskommunikation

Följande gör det lättare att åstadkomma samordnad kommunikation:

- Kännedom om varandras ansvar, roller och informationsbehov innan det oönskade händer.

- Samsyn kring vad som ur ett samhällsperspektiv är skyddsvärt inom sektorn.
- En samlad kommunikativ lägesbild som en del i den övergripande lägesuppfattningen och som underlag för beslut kring kommunikativa åtgärder.
- Förståelse för vilken information som krävs och hur den delas på lämpligt sätt.
- Kommunikatörsnätverk i vardagen på både strategisk och operativ nivå.
- Regelbunden träning och övning som inkluderar kriskommunikation.
- Årligen uppdaterade och aktuella krisplaner och kontaktlistor.

4.5 Arbetsformer för att samordna kommunikation

Ett överenskommet och övat arbetssätt gör att aktörerna tillsammans snabbt kan identifiera läget, vem som bör säga vad och hur sektorn tillsammans kan bygga tillit med en proaktiv kommunikationsstrategi. Det handlar om att skapa en låg tröskel för samverkan och ge struktur till arbetet med den samlade kommunikativa lägesbilden, se appendix A.

Alla aktörer i den finansiella sektorn har möjlighet att initiera samverkan. Om så bara en aktör identifierar ett samverkansbehov så är det tillräckligt för att samverkan ska vara befogad. En enskild bank behöver inte själv vara värd för en samverkanskonferens men har ansvar för att begära att endera Finansinspektionen eller Riksbanken kallar till en sådan.

5. Kunskapsöversikt: Cyberangrepp i den finansiella sektorn

5.1 Erfarenheter och slutsatser kring kommunikation

Den övning som FSPOS ordnade 2015 tydliggjorde en rad utmaningar som följer i spåren av en cyberattack och vikten av väl fungerande kriskommunikation och samverkan[4].

Flera aktörer ansåg att den samverkan som då fanns gjorde det lättare att hantera händelserna på ett bra sätt. Samtliga aktörer var öppna med sin information och visade att det finns en tydlig vilja att hjälpas åt inom sektorn.

De förbättringsområden som sågs handlade bland annat om hur samverkansmötena organiserades, genomfördes och följdes upp. Det var oklart hur samverkansmötena skulle gå till i praktiken, vilket ledde till mindre effektiva möten som inte mäktade med att inom avsatt tid enas i samlade lägesuppfattningar och koordinerade budskap. Det förekom liten aktiv koordinering och avstämning av budskap, trots att aktörerna noterar i utvärderingsunderlaget att koordineringen av budskap borde göra det lättare att upprätthålla förtroendet hos allmänheten vid en större händelse.

En sammanfattande slutsats var att samverkan fungerar bäst och ger mest effekt då det finns en aktör som har ett utpekat ansvar för att sammankalla till möten, ta fram agenda, moderera samt dokumentera och sprida minnesanteckningar efteråt.

Även Riksbankens enkätundersökningar visar att många aktörer strävar efter ökad samverkan för att hantera cyberangrepp. Majoriteten av respondenterna efterlyser utökad samverkan och mer informationsutbyte inom området.[5]

Detta är också bakgrunden till att medlemmarna i AG Information enades om att ta fram en internationell kunskapsöversikt. Sammanfattningsvis kan konstateras att även vid internationella cyberangrepp har just samverkan lyfts som en central faktor för att kommunikationen ska bli effektiv[6]. Många finansiella aktörer uttryckte dock att de inte kände sig helt trygga med att erkänna sårbarhet, skador och åverkan i en miljö där tillsynsmyndigheten var närvarande och där konkurrenter möjligen kunde dra fördel av informationen.

Även om arbetet med att stärka samverkan inom den finansiella sektorn går framåt innebär risken att resursstarka antagonister riktar angrepp mot flera delar av samhället stora utmaningar. Mer komplexa angrepp medför att flera samhällskritiska sektorer behöver samverka.

---

[4] http://www.fspos.se/siteassets/fspos/rapporter/2016/fspos-sektorsovning-2015---ovningsrapport.pdf
5 http://www.riksbank.se/Documents/Rapporter/FSR/2016/FSR_1/rap_fsr1_160601_sve.pdf
6 För fördjupning hänvisas till två fallstudier som i slutet av detta avsnitt.

5.2 *Beskrivning av cyberangrepp i finanssektorn*[7]

Det finansiella systemet är ekonomins blodomlopp och en central del av infrastrukturen. Det är dessutom beroende av komplexa IT-system vilket gör det sårbart för cyberangrepp[8]. En störning i det finansiella systemet, orsakad av ett cyberangrepp, kan medföra att bankerna inte kan genomföra betalningar till varandra och därmed till exempel inte kan betala ut löner till hushållen i tid. Privatpersoner kan få svårt att betala sina räkningar, den finansiella stabiliteten sammantaget påverkas och det kan i värsta fall leda till stora samhällsekonomiska kostnader (företagskonkurser och arbetslöshet).

Cyberangrepp mot det finansiella systemet kan även kombineras med attacker mot andra sektorer i samhället. Ett exempel på en bredare samhällsstörning är cyberattacken ”*Dark Seoul*” i Sydkorea 2013. Tre stora sydkoreanska banker utsattes för ett sabotage som slog ut cirka 30 000 datorer och servrar. Detta ledde till att kunderna inte kunde använda sina internetbanktjänster samt att bankomater och vissa bankkontor fick stänga. Samtidigt saboterades två stora tv-stationers system, vilket orsakade sändningsstörningar. Attacken skulle kunna tolkas som ett försök till påverkanskampanj[9]. Genom att den både störde banktjänster och gjorde det svårt för allmänheten att inhämta information förstärktes oron.

Attacker kan riktas mot både datorer och mobiltelefoner, oavsett operativsystem. Överbelastningsattacker[10], implementering av skadlig kod[11] eller rena intrång förekommer. De flesta hoten är så kallade bulkattacker, vilket innebär att skadlig kod distribueras i stor skala eller att en angripare söker brett efter sårbarheter att utnyttja för vidare attacker. Man kan till exempel vilja nyttja det angripna systemet för att skicka ut spam. Om en miljon e-postmeddelanden med skadlig kod skickas kan de ställa till med betydande skada, även om endast en promille av mejlen lyckas distribuera koden.

Utöver dessa generella attacker, som inte särskiljer målen, finns riktade attacker som innebär att en angripare utformar attacken specifikt gentemot ett mål. Riktade attacker föregås vanligtvis av en fas där angriparen inhämtar underlag (till exempel namn på

---

[7] *Vi vill rikta ett särskilt tack till Fredrik Hult, cybersäkerhetsspecialist, som har bidragit till avsnitt 5.2-5.3 samt fallstudierna.*

[8] *http://www.riksbank.se/Documents/Rapporter/FSR/2016/FSR_1/rap_fsr1_160601_sve.pdf*

[9] *För definition av påverkanskampanjer se: Sid 41 https://www.msb.se/Upload/Nyheter_press/Rapport%20civilt%20försvar_2014_3277_slut.pdf*

[10] *En överbelastningsattack (Denial of Service (DoS) eller Distributed Denial of Service (DDoS)) syftar i grunden till att förhindra normal åtkomst, men även i vissa fall till att mörklägga en annan pågående attack. En typ av attack är att överösa målet med så mycket trafik som möjligt och lägga beslag på all tillgänglig bandbredd.*

[11] *Skadlig kod inkluderar bland annat virus (exekverbar kod som sprids mellan olika system), trojaner (kod som agerar dörröppnare för ytterligare attacker), ransomware (kod som krypterar filer och tvingar offret att betala pengar för åtkomst), spyware (kod som hämtar information som t.ex. lösenord eller kreditkortsinformation) och mask (kod som replikerar sig själv genom att utnyttja sårbarheter i mjukvara).*

nyckelpersoner), kartlägger interna processer, typ av system och versioner av mjukvara som gör att attacken når största möjliga effekt.

5.3 Aktörer bakom cyberangrepp

Cyberangrepp kan handla om att utveckla tekniken för att göra den traditionella brottsligheten mer effektiv eller om ”rena” cyberangrepp där målet och brottet är digitalt. Här återfinns till exempel stöld av immateriella rättigheter, insiderhandel, kortbedrägeri, identitetsstöld, bankbetalningsbedrägeri och utpressning.

Cyberangreppen växer snabbt internationellt och Storbritannien uppskattar att de stod för 53 procent av alla brott som begicks i landet år 2015, varav 36 procentenheter är bedrägerirelaterade cyberangrepp.[12]

Cyberangreppen med fokus på betalningsinfrastruktur, utpressningsvirus och sabotage har blivit mer aggressiva. Avancerade cyberangrepp mot **Bangladesh centralbank** ledde till att över 80 miljoner dollar stals. Liknande attacker riktades även mot andra banker men med mindre framgång.[13]

Ett annat exempel på internationella attacker mot banker är de som utförts av den så kallade **Carbanak/Anunak-gruppen** som bedöms ha stulit över en miljard dollar från över hundra banker. Gruppen spanade en längre tid, ibland månader, inne på bankernas nätverk. De studerade bankernas interna betalningsrutiner och identifierade vilka personer, funktioner och system som hade kontroll över betalningsprocessen. Attacken riktade sig mot bankernas betalningsinfrastruktur och personal, inte mot själva kundstocken. Detta har visat sig vara en framgångsrik metod då mycket av bankernas säkerhetsfokus har varit att säkra internetbankstransaktioner.[14]

Leverantörer av mjukvara till betalningsindustrin är andra mål för cyberangrepp. Ett konkret exempel är att **Micros**, en av de tre största globala leverantörerna av betalningsterminaler för kredit- och betalkort, blev attackerat. Cyberbrottslingarna fick därmed tillgång till betalningssystemen hos hundratals företag.[15]

De större kriminella nätverken har flyttat fokus från attacker mot kundernas internetbankkonton till att i stället utpressa dem genom sabotage av kundernas egna datorer, så kallad ”*ransomware*”. Här görs offrets dokument och data obrukbara och otillgängliga tills en lösensumma har betalats ut, oftast i form av bitcoin för att försvåra spårning. Metoden anses medföra relativt låga risker för brottslingen.

---

[12] *http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file*
[13] *http://www.bloomberg.com/news/articles/2016-03-18/hackers-stalked-bangladesh-bank-for-two-weeks-before-big-heist*
[14] *http://www.group-ib.com/files/Anunak_APT_against_financial_institutions.pdf*
[15] *http://www.ft.com/cms/s/0/657447a4-5d95-11e6-a72a-bd4bf1198c63.html#axzz4KkFrFDwn*

Internetbankattacker är mer komplicerade och kräver att cyberbrottslingarna hanterar transaktioner, vilket medför större risker för upptäckt.

Kriminella marknadsplatser[16] där till exempel skadlig kod säljs medför att även ideologiskt drivna aktörer kan ta del av tekniken och nyttja den för sina syften. Politiska cyberangrepp är en del av hotbilden där individer och grupper av ideologiska skäl drivs att sabotera, avslöja företagshemligheter eller bedriva någon sorts digitalt medborgargarde.

Även stater kan genomföra cyberangrepp för att påverka opinioner[17]. Det är ett alltmer etablerat synsätt att cyberangrepp mot civila mål och samhällsviktiga funktioner är en integrerad del av modern krigsföring. Cyberangrepp kan användas för att destabilisera länders politiska system, spionera eller skada deras ekonomi. Genom att ge sig på den finansiella sektorn kan en stat orsaka en annan stat stor skada när en del av infrastrukturen påverkas.

Vissa stater satsar stora nationella resurser på att utveckla avancerad teknik, både för att skydda sig mot och för att genomföra cyberangrepp. Om tekniken hamnar i orätta händer kan det få stora konsekvenser för finanssektorn.

Fallstudie 1: Cyberangrepp mot amerikanska banker (Operation Ababil 2012)

I september 2012 slogs flera amerikanska bankers internet- och mobilbanktjänster ut på grund av en överbelastningsattack som har kommit att kallas för ”Operation Ababil”[18]. Attacken pågick i flera veckor och bankerna hade till en början svårt att försvara sig trots att en aktivistgrupp förvarnade och hotade dem via sajten Pastebin[19]. Gruppen lät meddela att de avsåg att attackera USA som ett svar på en kontroversiell video som lagts upp på Youtube. Deras uttalade mål var New York-börsen och ett antal banker med verksamhet i USA.

Financial Services Information Sharing and Analysis Center (FS-ISAC), ett frivilligt samarbetsorgan för samverkan mellan offentlig och privat sektor, ansvarade för att samordna och dela information om krisens förlopp. Man använde sig av ett så kallat

---

[16] *Exempel på marknadsplatser är de nu nedstängda Silk Road (http://krebsonsecurity.com/2013/10/feds-take-down-online-fraud-bazaar-silk-road-arrest-alleged-mastermind/) och Evolution (https://krebsonsecurity.com/2015/03/dark-webs-evolution-market-vanishes/)*

[17] *Exempel på detta är cyberattacken mot Estland 2007 (https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia) och de förmodade ryska intrången i Demokraternas e-postsystem vid USAs presidentval 2016 (http://www.nytimes.com/2016/10/12/us/politics/obama-russia-hack-election.html?_r=0)*

[18] *https://security.radware.com/ddos-knowledge-center/ddospedia/operation-ababil/*

[19] *http://pastebin.com/mCHia4W5*

trafikljusprotokoll för informationsdelning. Protokollet gör det möjligt för medlemmar att välja olika nivåer för hur information sprids av mottagaren.[20]

Samverkan mellan bankerna inom FS-ISAC var först fragmenterad och skedde främst i mindre grupper som redan kände varandra. Dessa grupper försökte bygga en gemensam lägesbild och dela information med förhoppningen att kunna stå emot framtida attacker. Men i många fall spreds initialt felaktig information. Det största problemet var att informationen inte nådde *rätt* personer inom respektive organisationer *tillräckligt snabbt*. Attackerna började på nytt tre månader senare, i december 2012. Då fungerade informationsdelningen och samverkan mellan bankerna, internetoperatörer, myndigheter och andra företag bättre. Det innebar att denna våg av attacker i princip inte påverkade bankernas onlinetjänster.

Lärdomar av Operation Ababil

En viktig lärdom var att små personliga/frivilliga nätverk utan bredare förankring i den interna organisationen inte fungerar så väl, särskilt inte i en krissituation.

Det fanns en tillit inom de grupper som hade vana av att samverka men flera aktörer inom övriga finanssektorn hade inte tidigare samverkat och övat. De saknade därför erfarenhet av att samarbeta. Denna brist hade kunnat åtgärdas med samverkansövningar som innefattar fler och som simulerar olika typer av cyberangrepp.

Samarbetsorgan för informationsdelning behöver både starka band *mellan* medlemmarna och en djup förankring *internt* i respektive organisation – detta för att säkerställa att man kan dela både strategisk och operativ information som gör att man kan bygga en gemensam lägesbild och handlingsplan.

Fallstudie 2: Brittiska cyberövningsprogram för den finansiella sektorn

År 2010 anordnade brittiska finansinspektionen FSA, tillsammans med banken Credit Suisse, en övning för att se vad som skulle hända om landets finanssektor blev utsatt för en bred och koordinerad cyberattack (Waking Shark). Övningen var tänkt att testa om branschen hade en gemensam syn på hur den ska hantera en bred cyberattack och på hur kommunikationen skulle nå fram. Cirka 100 deltagare från 33 finansinstitut övade tillsammans med myndigheterna.

Ett resultat av övningen var insikten att det inte fanns någon branschgemensam syn på vem som ska leda vid en bredare kris eller vilken myndighet som ska koordinera arbetet att bekämpa cyberattacken. Medlemmarna i branschens samarbetsforum hade dessutom ingen kontakt med interna nyckelpersoner inom cybersäkerhet vilket försvårade koordineringen av insatser och försämrade informationsdelningen.

[20] *https://www.us-cert.gov/tlp*

De samarbetsforum som fanns var inte lämpliga för att skapa en gemensam lägesbild. Medlemmarna i samarbetsforumen befann sig på hög strategisk ledningsnivå snarare än på operationell. Ett parallellt forum för operativt utbyte av underrättelse- och incidentinformation efterlystes för att man snabbare skulle kunna identifiera orsaken till skadorna och kunna bekämpa attacker. Många finansföretag kände sig heller inte trygga med att erkänna sårbarhet, skada och åverkan i en miljö där tillsynsmyndigheten var närvarande och där konkurrenter möjligen kunde dra fördel av informationen.

Storbritannien har flera så kallade "Information Exchanges" inom den kritiska nationella infrastrukturen som ska främja informationsutbyte mellan privata och offentliga aktörer. Det forum som verkar inom finanssektorn, Financial Services Information Exchange (FSIE), omvandlades till en operativ grupp för utbyte av information i kris. Denna omvandling testades sedan i nästa stora kontinuitetsövning MarketWide 2011. Här simulerades en stor cyberattack i kombination med en större gasexplosion i centrala bankdistriktet under OS i London.

Även denna övning visade att många finansinstitut fortfarande, sex månader efter Waking Shark, hade problem att integrera affärskontinuitet, planering och cyberattackrespons. FSIE-forumet visade sig visserligen ge deltagarna bättre insikter om omfattningen av cyberattacken, men deltagarna var fortfarande på ledningsnivå. Det operationella samarbetet behövde ha ett eget forum. Övningen visade också vikten av att finansföretagen har en mogen intern organisation där personal som bekämpar cyberangrepp har rätt mandat för att kunna agera snabbt när så krävs.

Två år senare hölls nästa övning *Waking Shark II*[21]. Under tiden mellan övningarna byggde brittiska myndigheter en operationell samarbetsplattform, CiSP[22]. Ett av målen med Waking Shark II var att operationellt testa CiSP i en simulerad kontinuitetsövning och att stimulera finanssektorn att använda plattformen i större utsträckning. CiSP använder ett trafikljusprotokoll för att medlemmarna ska kunna kontrollera hur information delas vidare av andra medlemmar. Det går också att anonymisera information, sammanställa trender och hjälpa till att sprida en gemensam lägesbild bland medlemmarna i CiSP.

Slutsatserna från Waking Shark II var att CiSP är en användbar plattform för delning av operationell information och när man vill kunna bygga en delad lägesbild före, under och efter en bredare kris. Medlemsantalet har ökat markant sedan övningen.

Lärdomar från det brittiska cyberövningsprogrammet

[21] *http://www.bankofengland.co.uk/financialstability/fsc/Documents/wakingshark2report.pdf*
[22] *https://www.ncsc.gov.uk/cisp*

Storbritannien har, liksom USA, arbetat för att finanssektorn ska samverka mer än tidigare både operationellt och strategiskt. Det finns nu formella överenskommelser om hur samarbete ska ske och vilka regler som gäller.

Storbritannien visar också att finanssektorn inte behöver utsättas för en stor riktig attack för att kunna samverka. Bra övningar räcker långt, men cyberangreppen mot USA snabbade på intresset för samarbete. Eftersom samma hot inte blivit verklighet i Storbritannien har det tagit längre tid att få till stånd ett djupare samarbete.

I båda fallen har myndigheterna spelat en nyckelroll för att underlätta privat-offentlig samverkan. I Storbritannien stod tillsynsmyndigheten för det huvudsakliga initiativet.

5.4 Svenska finansiella myndigheterns arbete för cybersäkerhet

Myndigheter som Riksbanken, Finansinspektionen och Riksgälden värnar den finansiella stabiliteten och även här ligger fokus alltmer på cyberangrepp. Frågor kopplade till finansiell stabilitet analyseras löpande, risker kommuniceras och likaså rekommendationer om vilka åtgärder som bör genomföras för att hantera dem. Dessutom övar sektorn på att både förebygga och hantera kriser. Även tillsammans med Finansdepartementet i det finansiella stabilitetsrådet anordnas övningar för att öva kriskommunikationen kring olika hot mot den finansiella stabiliteten.

Det finns även samverkansforum där man utbyter känslig information om och praktiska erfarenheter av aktuella cyberangrepp. Ett exempel är FIDIFinans, ett forum för informationsdelning med inriktning på finanssektorn, under ledning av Myndigheten för samhällsskydd och beredskap[23]. För en fullständig lista över aktörer som bör samverka, se appendix C.

[23] *MSB och samhällets informationssäkerhet, Faktablad januari 2014. MSB.*

Appendix A: 4-fältare för kommunikativ lägesbild

A.1 Stödfrågor för att ta fram en intern lägesbild

1. FAKTA	2. PROGNOS
Vad har hänt? Vilka åtgärder har vi vidtagit? *Vilka konsekvenser för interna/externa målgrupper har bekräftats?* *Vilka frågor får vi internt?* *Vilka frågor får vi från externa målgrupper?* *Hur ser den mediala bilden ut (vilka rapporterar och med vilka vinklar?)* *Vilka resurser har vi till förfogande?* *Vilka kommunikativa åtgärder har vidtagits?*	Vad tror vi om utvecklingen? Vilka centrala antaganden har gjorts? *Vilka konsekvenser kan händelsen få för interna/externa målgrupper?* *Vilket informationsbehov (vilka frågor?) kan händelsen föranleda internt/externt?* *Hur kan den mediala bilden komma att utvecklas?* *Vilka behov finns av ytterligare information från intern eller extern aktör?*
3. INRIKTNING OCH ÅTGÄRDER	**4. KOMMUNIKATION**
Vilken är vår strategiska inriktning? Vilka åtgärder planerar vi att genomföra? *Vilken är vår kommunikativa inriktning?* • *Proaktiv eller reaktiv kommunikation?* • *Omfattning?* • *Vilka är särskilt viktiga målgrupper?* • *Vilka värderingar ska styra/kännetecknа vår kommunikation?* *Vilka kommunikativa åtgärder planerar vi att genomföra?*	Hur ska vi kommunicera? • Interna budskap • Externa budskap • Kanaler för informationsdelning

A.2 Stödfrågor för att snabbt kunna dela lägesbild

1. FAKTA VI VILL DELGE SEKTORN	2. PROGNOS VI VILL DELGE SEKTORN
Vad har hänt? Vilka åtgärder har vi vidtagit? ***Fakta*** *vi vill delge sektorn ur ett kommunikationsperspektiv:* • *Bekräftade konsekvenser för målgrupper* • *Aktuellt informationsbehov* • *Aktuell mediebild* • *Vidtagna kommunikative åtgärder*	Vad tror vi om utvecklingen? Vilka centrala antaganden har gjorts? ***Prognos*** *vi vill delge sektorn ur ett kommunikationsperspektiv:* • *Vår prognos avseende för målgrupper* • *Vår prognos avseende informationsbehov* • *Vår prognos avseende utvecklingen av den mediala bilden* • *Vårt informationsbehov från andra aktörer*
3. BEHOV AVSEENDE KOORDINERING AV ÅTGÄRDER	**4. BEHOV AVSEENDE KOORDINERING AV BUDSKAP**
Vilka åtgärder behöver vi samordna med andra aktörer? • På kort och lång sikt • Förslag på ansvarig • Förslag på tidsplan *Kommunikativa åtgärder vi har behov av att samordna med andra aktörer*	Vilka budskap behöver vi samordna med andra aktörer? • Interna budskap • Externa budskap • Kanaler för informationsdelning

A.3 Ytterligare exempel på stödfrågor

- Vad vill vi uppnå med vår kommunikation?
- Hur kan vår kommunikation påverka händelseutvecklingen?
- Vilka rekommendationer kan vi inkludera i våra budskap?
- Vilka är våra prioriterade målgrupper och hur når vi dem?
- Hur ser våra målgruppers informationsbehov ut på kort och lång sikt?
- Vilka åtgärder behöver vi vidta för att möta dessa informationsbehov?
- Hur påverkas informationsbehovet av vidtagna och planerade åtgärder för att hantera händelsen?
- Vem ansvarar för att svara på vilka frågor? Samordningsbehov?
- Vilka aktörer behöver vi samordna våra kommunikativa åtgärder med?

Appendix B: Arbetssätt och struktur - samverkansmöten

B.1 Tips för att ta fram en samlad kommunikativ lägesbild

Nedan följer de steg som bör hanteras och vidtas:

- **Kontakt**: Effektiv samverkan förutsätter att berörda aktörer enkelt kan nå varandra. FSPOS har en uppdaterad kriskontaktlista, se vidare appendix C.

- **Sammankallande/Inbjudande**: En inbjudan skickas till de aktörer som bör delta. Av inbjudan ska framgå tidpunkt, form för samverkanskonferensen (telefon/webb/video/fysiskt), instruktioner för deltagande (till exempel hur uppringning sker, möteskoder, användande av mutefunktion), syfte och agenda. Sammankallande eller inbjudande aktör utser ordförande och sekreterare för mötet och ser till att dokumentation upprättas.

- **Initiera/signalera behov av samverkan:** Utsedd myndighet kallar till samverkan men behovet kan vara signalerat av annan aktör. Vid behov kan Myndigheten för samhällsskydd och beredskap (MSB) vara sammankallande och värd, särskilt vid händelser då flera samhällssektorer är berörda.

- **Mötesformer och syften**[24]: Möten kan ha olika syften och olika former. Det viktigaste är att först fokusera på vad mötet ska uppnå – önskat resultat. Först därefter planeras, sammankallas och genomförs mötet.

  Samverkanskonferenser kan ha olika syften, till exempel att dela information, upprätta en samlad lägesbild, prioritera åtgärder eller samordna kommunikation. Ett säkert misstag är att göra för många saker vid varje möte. Komplettera därför större samverkanskonferenser med mindre arbetsmöten med uppgifter som kan utföras av färre deltagare.

- **Leda samverkan.** Riksbanken och Finansinspektionen är de som oftast har denna roll i FSPOS-sammanhang utifrån sina respektive ansvarsområden, rutin och tekniska förutsättningar. Den som leder samverkan driver processen så att alla berörda aktörer kan fokusera på det som är viktigast för stunden och känna sig trygga med att ingen får otillbörliga fördelar av att ha rollen att leda.

- **Mötesledare/ordförande**[25]: Mötesledaren ansvarar för att förbereda och leda mötet. Ett möte med många deltagare i ett pressat läge kräver tydlig och lugn ledning samt noggranna förberedelser. Även svåra och kontroversiella frågor

---

[24] *Se MSB Samverkanskonferenser - Råd och rekommendationer för dig som leder eller deltar i samverkanskonferenser, avsnitt 2, sid 15-18 för exempel på möten med olika syften.*

[25] *Se MSB Samverkanskonferenser - Råd och rekommendationer avsnitt 4, sid 20-21 för praktiska råd till mötesledaren.*

behöver lyftas. Det är inte nödvändigt med enig syn, men vid ett stressat läge är det en fördel om motstridiga budskap undviks så långt möjligt.

- **Deltagare i samverkan/ mötesdeltagare:** Vilka personer/funktioner som kallas beror dels på situationen och dels på syftet med mötet (se resonemang ovan). Om det är ett arbetsmöte kanske det är lämpligt att det är kommunikatörer, strateger eller pressansvariga med viss expertis som träffas. Om det är ett beslutsmöte kräver det kanske chefsnärvaro eller att representanterna har rätt mandat. Kommunikationschefer kan behöva stämma av innan sektorn som helhet håller en större samverkanskonferens. Oavsett vilket, ställer det krav på den som deltar att vara väl förberedd[26].

- **Dokumentation**: I ett pressat läge kan det vara svårt att minnas vad man kommit överens om. Deltagare vid samma möte kan få väldigt olika bild av vad som sades. Dokumentera därför mötesresultatet och överenskommelser på enklaste sätt och dela mellan aktörerna så att det blir tydligt vilka åtgärder som ska vidtas och av vem.

- **Teknik:** Beroende på vem som står värd för mötet så kan olika tekniker användas (telefon, webb, video eller fysiskt möte). Avgörande är inte vilken teknik som används utan att den är lätt att använda och är tillgänglig för alla som ska delta.

- **Informationsdelning**[27]: Alla aktörer bör förbereda sig på att efterfråga information från andra (var tydlig med vilken information som behövs och vad den ska användas till), skapa informationsunderlag (ta reda på vem som ska ha informationen och om den behöver säkerhetsklassas), göra information tillgänglig för andra (i den mån den inte är sekretessbelagd).

B.2 Ytterligare stöd

Krisinformation.se: På webben och i sociala medier förmedlas information från finansiella sektorns aktörer till allmänhet och medier. När sektorns aktörer har publicerat bekräftad information kan portalen Krisinformation.se bidra till att sprida den till allmänhet och medier. Krisinformation.se drivs av MSB. All information som finns på sajten är bekräftad information från myndigheter och övriga ansvariga.

FSPOS kansli: FSPOS kansli uppdaterar löpande den kontaktlista som den finansiella sektorns aktörer ska utgå från när snabb samverkan behövs.

---

[26] *Se MSB Samverkanskonferenser - Råd och rekommendationer avsnitt 3, sid 19 för praktiska råd till mötesdeltagaren.*

[27] *Gemensamma grunder för samverkan och ledning – Sammanfattning, sid 15.*

Finanskartan.se: Finanskartan visar hur den finansiella sektorns aktörer är sammanlänkade och visar deras roller och mandat i normalt läge och i krisläge. Tipsa gärna journalister om denna faktasida.

B.3 Samverkans-/arbetsmöte för kommunikatörer inom FSPOS

- Arbetsmöte för kommunikatörer inom FSPOS genomförs som förberedelse för sektorns övergripande samverkanskonferenser i syfte att förbereda den samlade kommunikativa lägesbilden som sedan blir en del av den övergripande lägesbilden. Arbetsmöte för kommunikatörer kan producera en samlad kommunikativ lägesbild som kan komplettera en övergripande lägesbild

- Roller för deltagande individer kan variera. Det centrala är att representanterna för de olika aktörerna har med sig rätt underlag samt mandat till mötet så att en samlad kommunikativ lägesbild kan upprättas, överenskommelser kan göras och beslut fattas.

- Samverkans- och arbetsmöten kan, och bör ibland, genomföras på olika nivåer (chefer och beslutsfattare, strateger, kommunikatörer, webbredaktörer eller pressansvariga) beroende på mål och syfte med mötet. Försök renodla mötet och undvik att försöka göra för många saker samtidigt.

- Mötet genomförs via telefon om inget annat beslutas. Arbetsmöten kan vid behov självklart också genomföras som fysiska möten eller med stöd av annan teknik.

- Sammankallande aktör och värden för mötet, vilken kan variera beroende på händelse, ser till att resultaten dokumenteras och delges deltagande aktörer.

- För konkreta tips och råd för mötesledare och mötesdeltagare se MSB:s publikation ”Samverkanskonferenser – råd och rekommendationer till dig som leder eller deltar i samverkanskonferenser”[28].

B.4 Dagordning

Mål och syfte uppdateras utifrån aktuell händelse.

Mål – Mötet kommer att resultera i en samlad kommunikativ lägesbild och en överenskommen övergripande kommunikativ inriktning samt beslutade och avstämda åtgärder (gemensamma såväl som aktörsspecifika).

Syfte – Mötets syfte är att utifrån aktuell händelse skapa en samlad kommunikativ lägesbild som ska ingå i den övergripande samlade lägesbilden för den finansiella sektorn samt kommunikativ inriktning och åtgärder som bidrar till en effektiv hantering.

---

[28] *https://www.msb.se/RibData/Filer/pdf/27251.pdf*

1. Mötet öppnas och närvaro kontrolleras
2. Beskriv att dokumentationsansvarig är utsedd och redo att dokumentera samt hur dokumentationen kommer distribueras.
3. Presentera mål och syfte med mötet (alltså tydliggör önskat resultat)
4. Aktörsgemensam kommunikativ lägesbild.
    a. Respektive deltagande aktör delger för sektorn som helhet relevanta delar av sin interna lägesbild som bidrag till den samlade kommunikativa lägesbilden. (Mall i appendix A)
    b. Mötesledaren sammanfattar den samlade kommunikativa lägesbilden.
    c. Lägesanalys och diskussion vid behov.
5. Mötesledaren föreslår övergripande inriktning för det aktörsgemensamma kommunikationsarbetet utifrån lägesbilden och överenskommelse görs.
6. Beroende på händelsens karaktär och utveckling diskuteras alla eller några av följande punkter:
    a. Behov av gemensamma budskap
    b. Behov av gemensamma kommunikationsinsatser
    c. Behov av gemensamt avstämda frågor och svar
    d. Arbetsfördelning och tidplan
    e. Information om aktörsspecifika kommande kommunikationsinsatser
    f. Finns det oklarheter i informationsansvar? Vilka åtgärders behövs?
    g. Behov av att ytterligare analyser målgrupper och kanaler specifika för händelsen
    h. Finns det tydliga kontaktvägar mellan berörda kommunikationsfunktioner?
    i. Ytterligare samverkansbehov så som till exempel resurser och förstärkningar.
7. Sammanfattning av beslut/åtgärder/ansvarig samt när återkoppling kring genomförda åtgärder sker och hur, samt tid för nästa möte.

Appendix C – FSPOS medlemmar och roller vid kris

Detta är en kortfattad översikt över aktörer som kan behöva samordna sin kommunikation vid en samhällsstörning i den finansiella sektorn.

OBS: För kontaktuppgifter hänvisas till FSPOS kriskontaktlista.

C.1 Riksbanken

Riksbanken ska bidra till finansiell stabilitet genom att se till att betalningar kan ske säkert och effektivt. Riksbanken förser Sverige med sedlar och mynt, arbetar för att förebygga finansiella kriser, ha beredskap och verktyg för krishantering på plats samt att se till att det finns ett centralt betalningssystem (RIX) som andra aktörer kan använda för att göra betalningar. I ett finansiellt krisläge kan Riksbanken även stötta med likviditetsstöd till enskilda institut eller generella likviditetsstärkande åtgärder. Riksbanken bidrar även med övergripande bedömningar av den finansiella stabiliteten.

C.2 Finansinspektionen

Finansinspektionen är en statlig myndighet med uppdrag att arbeta för att det finansiella systemet ska fungera väl med stabila företag och ett gott konsumentskydd. Myndigheten lyder under Finansdepartementet.

Finansinspektionen ansvarar för tillsynen av finansiella företag och i Sverige och har rätt att ingripa mot verksamheter som inte följer lagstiftningen. Tillsynen kan bland annat bestå av att säkerställa att aktörer inte tar på sig större risker än de klarar av. Stresstester är ett sätt att bedöma verksamheternas förmåga att klara av påfrestningar, till exempel vid finansiella kriser.

Utöver tillsynsansvaret har Finansinspektionen i uppdrag att analysera och motverka potentiella samhällsekonomiska risker som inte är kopplade till finansiella företag och vid behov föreslå åtgärder.

Finansinspektionen ska underrätta regeringen om den bedömer att instabilitet i finanssektorn hotar det svenska finansiella systemets funktionalitet. Finansinspektionen kan tidigt få indikationer på brister hos de finansiella företagen, och underrättar regeringen om den bedömer att eventuell instabilitet hotar det svenska finansiella systemets funktionalitet.

C.3 Riksgälden

Riksgälden är statens finansförvaltning och har en central roll i statens åtgärder för att värna finansiell stabilitet. I rollen ingår att ge stöd till banker och andra kreditinstitut vid hot om en allvarlig störning i det finansiella systemet. Riksgälden har ansvar för förberedelserna och hanteringen av kriser i banker, andra kreditinstitut och värdepappersbolag. Riksgälden är en resolutionsmyndighet vilket innebär att de kan ge förebyggande stöd till verksamheter genom garantier, och vid behov ta kontroll över problemdrabbade institut för att rekonstruera eller avveckla dem under kontrollerade former.

Riksgälden ansvarar också för insättningsgarantin, ett konsumentskydd för sparande på konto. Skyddet dämpar oron vid en finansiell kris och minskar risken för uttagsanstormningar. Medlen för att finansiera stödåtgärderna kommer från Stabilitetsfonden som Riksgälden har ansvar för. Banker och andra kreditinstitut betalar en årlig avgift till Stabilitetsfonden.

C.4 MSB

MSB är en statlig myndighet med ansvar för att stödja och samordna arbetet med skydd mot olyckor, krisberedskap och civilt försvar. Vid en samhällsstörning ska MSB kunna bistå med stödresurser och se till att ansvariga aktörer samordnar sina åtgärder och sin kommunikation med medier och allmänhet. MSB har en stödjande och samordnande roll i arbetet med samhällets informations- och cybersäkerhet, och ansvarar för Sveriges nationella IT-incidenthanteringsfunktion CERT-SE.

C.5 Banker

Bankerna omvandlar sparande till finansiering, hanterar risker och erbjuder betalningslösningar så att företag och hushåll kan spara, låna och investera. Bankerna skapar genom kreditgivning och andra finansiella tjänster förutsättningar för små och

medelstora företag att starta och växa och för stora företag att lyckas i den internationella konkurrensen.

C.6 Bankföreningen

Svenska Bankföreningen företräder de svenska bankerna i syfte att skapa förutsättningar för konkurrenskraftiga finansiella produkter och tjänster. De har bland annat en kunskapsspridande roll om bankernas roll för tillväxt och välfärd i samhället.

Vid krishantering agerar Bankföreningen som samverkansforum för bankerna, och skapar förutsättningar för samordning mellan svenska banker genom exempelvis samverkanskonferenser.

C.7 Sparbankernas riksförbund

Sparbankernas riksförbund representerar de svenska sparbankerna, och fungerar även som samarbetsorganisation för medlemmarna.

C.8 Svensk försäkring

Försäkringsbolags grundläggande idé är att skapa en ekonomisk trygghet hos individer och företag där det finns risker av olika slag. Försäkringstagare betalar in premier i utbyte mot ersättning om de skulle drabbas av en ekonomisk förlust. Försäkringsbolag förvaltar stora summor pengar och är stora investerare i obligationer som är en betydande finansieringskälla för de svenska bankerna.

Till skillnad från banker kan försäkringsbolagen inte drabbas av uttagsanstormningar, utan det krävs en konkurs där försäkringsbolag inte kan betala utbetalningar till drabbade.

C.9 Svenska Fondhandlareföreningen

Svenska Fondhandlareföreningen representerar gemensamma intressen hos företag som driver värdepappersrörelse i Sverige. Föreningen har för närvarande 29 banker och värdepappersbolag som medlemmar. Fondhandlareföreningen syftar till att skapa förutsättningar för en sund och effektiv svensk värdepappersmarknad.

Fondhandlareföreningen har ett samverkande uppdrag i frågor där medlemmar har ett gemensamt intresse, som exempelvis vid framtagande av standardavtal.

C.10 Bankgirot

Bankgirot ägs av de svenska bankerna och är den centrala aktören vid förmedling av massbetalningar mellan bankerna i Sverige. Systemet är öppet för alla banker som är verksamma i Sverige, och fungerar som adresser som pekar på bankkonton vilket möjliggör byte av bankkonto utan påverkan på användningen.

Bankgirot ansvarar även för att skulder och fordringar mellan banker regleras hos Riksbanken för flöden som t.ex. VISA och MasterCard, allt detta inom ramen för Bankgirots Clearing och Avvecklingstjänst.

C.11 Nasdaq

NASDAQ OMX Stockholm AB (NASDAQ OMX) är den centrala marknadsplatsen för handel med bland annat aktier, premieobligationer, konvertibler, warranter, obligationer och börshandlade fonder i Sverige. Dessutom erbjuds handel i svenska, finska, norska och danska derivat såsom aktieoptioner, indexoptioner, räntederivat, aktie- och indexterminer samt vissa OTC derivat.

NASDAQ OMX Clearing Aktiebolag bedriver verksamhet som rör clearing av derivattransaktioner. För dessa transaktioner fungerar NASDAQ OMX Clearing som central motpart. Det innebär att NASDAQ OMX Clearing går in som säljare till alla köpare, och köpare till alla säljare. Både den köpande och säljande parten får därmed NASDAQ OMX Clearing som motpart.

C.12 Euroclear

Euroclear är både värdepappersförvarare och clearingorganisation och tillhandahåller tjänster mot emittent, mellanhand och investerare, gällande emission och hantering av finansiella instrument, samt clearing och avveckling av affärer.

Betalningar i samband med förfall av värdepapper och corporate actions (exempelvis utdelningar) administreras också av Euroclear. I vissa fall sker betalning i samband med avvecklingen via centralbankskonton i Euroclear och Riksbanken och i andra fall sker betalning via Bankgirot.

C.13 FSPOS

FSPOS är en förkortning för Finansiella Sektorns Privat-Offentliga Samverkan och bildades den 1 september 2005. FSPOS är ett frivilligt samverkansforum med deltagare från det privata näringslivet och de offentliga institutionerna i finanssektorn. FSPOS vision är att samhällsviktiga finansiella tjänster alltid ska fungera. Verksamhetsidén är att FSPOS ska stärka den finansiella infrastrukturen genom att samverka, öva, kartlägga och dela information och på så sätt värna sektorn och samhället. FSPOS har medlemmar såsom; banker, försäkringsbolag, fondkommissionärer, finansiella infrastrukturbolag, Riksgälden, Riksbanken och Finansinspektionen.

MSB stödjer utvecklingen av FSPOS, dels ekonomiskt, dels genom att upprätthålla FSPOS kanslifunktion. Verksamheten styrs av styrelsen som består av representanter från de deltagande medlemsföretagen/aktörerna.

C.14 Finansdepartementet

Vid en kris arbetar Finansdepartementet med att ta fram förslag till åtgärder som regeringen kan vidta om myndigheternas verktyg inte skulle räcka till. Stödlagen ger regeringen rätt att ingripa med olika former av stöd till svenska banker och kreditinstitut för att förhindra allvarliga störningar i det finansiella systemet. Finansdepartementet ger förslag till hur ingreppen i så fall bör se ut. Det sker i samråd med myndigheterna. Finansiella Stabilitetsrådet leds av ett kansli som arbetar under Finansdepartementet.

Appendix D: Referenslitteratur

- MSB (2013) Samverkanskonferenser – Råd och rekommendationer till dig som leder eller deltar i samverkanskonferenser
- MSB (2014) Gemensamma grunder för samverkan och ledning vid samhällsstörningar
- Länsstyrelsen i Västra Götalands län (2015) Kommunikationssamverkan i Västra Götalands län – Inriktning och rutiner
- Krisinformation.se (2016) www.krisinformation.se
- MSB (2016) Att stödja och samordna kommunikation. https://www.msb.se/Upload/Utbildning_och_ovning/Konferenser_seminarier/Dokumentation/Kriskommunikation_20160921/Att%20st%C3%B6dja%20och%20att%20samordna%20kriskommunikation%20med%20andra%20myndigheter%2C%20Inger%20Frendel.pdf
- Johansson, Carina (2013) Hur bedrivs framgångsrik informationssamordning? Mittuniversitetet. https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nyhetsarkiv/Nyhetsarkiv-2013/Hur-bedrivs-framgangsrik-informationssamordning/
- MSB (2015) Kriskommunikation vid kemikalieolyckor och oljespill i USA https://www.msb.se/sv/Start1/Kalender/Seminarium-om-amerikansk-kriskommunikation-vid-kemikalieolyckor-och-oljespill/
- MSB (Kunskapsplattform Ledning) Hur arbetar Jordbruksverket med samverkan och ledning? https://www.msb.se/Upload/Utbildning_och_ovning/Revinge/Pdf/Artikelserie%20Kunskapslpattform%20ledning/Hur%20arbetar%20Jorbruksverket%20med%20samverkan%20och%20ledning,%20interjvu%20med%20Catrin%20Molander,%20enhetschef.pdf