FSPOS

Finansiella Sektorns Privat-
Offentliga Samverkan

Informationsdelning av cyberrisker inom finansiell verksamhet

Version: 2017-12-07
FSPOS FG Cybersäkerhet

Inledning

Detta dokument beskriver forum, riktlinjer och rutiner för informationsdelning om cyberrisker som tillämpas idag av olika organisationer i samhället och inom finansiell sektor. Innehållet är en lägesbeskrivning inom ett område som utvecklas snabbt eftersom behovet av information ökar och förändras som en följd av att hotbilden och riskerna förändras.

Företag och organisationer som bedriver finansiell verksamhet använder olika metoder och verktyg för att identifiera, bedöma och hantera cyberrisker. Olika forum och nätverk är en viktig del i detta informationsflöde, inte minst utifrån det faktum att det finns beroenden mellan system och aktörer. De hot som en organisation möter delas därför ofta även av andra organisationer. Det är därför viktigt att bygga förtroende mellan organisationer och etablera metoder för att dela information och erfarenheter så att risker kan hanteras effektivt.

FSPOS är ett nätverk för samverkan mellan organisationer i finansiell sektor och har bland annat till uppgift att sprida kunskap om hur operativa risker kan hanteras för att samhällsviktiga finansiella tjänster ska fungera. Detta dokument, med fokus på cyberrelaterade risker, är ett led i denna kunskapsspridning.

Dokumentet kan även utgöra en grund för fortsatt analys inom området, exempelvis gällande behov av att utveckla befintlig informationsdelning inom den finansiella sektorn. En sådan analys kan även omfatta behoven av forum och plattformar för informationsdelning och rapportering utanför den finansiella sektorn.

Bakgrund

Cybersäkerhet inriktar sig på att skydda de system som hanterar, bearbetar, lagrar eller transporterar information. En hög grad av komplexitet i den finansiella sektorn medför, som noterats ovan, gemensamma beroenden till information och den infrastruktur som stödjer informationen. Genom att skapa nätverk och forum, kan finansiella aktörer dela relevant information inom sektorn och med andra aktörer, såväl nationellt som internationellt. Därigenom kan risker bedömas, incidenter upptäckas eller förebyggas och erfarenheter kan delas så att förmågan att motstå och hantera cyberhot ökar, både för individuella organisationer och för den finansiella sektorn som helhet.

Vilken information som är relevant och värdefull beror till stor del på om den är ”handlingsbar”, ”läglig” och ”specifik”. Med andra ord ska organisationer som tar del av informationen kunna använda den för egna åtgärder och informationen ska vara tidsmässigt tillgänglig då den ger nytta. Olika sorts information kan även delas på olika organisatoriska nivåer mellan den finansiella sektorns aktörer. Informationsdelningen behöver därför anpassas till och koordineras mellan

exempelvis strategisk, taktisk, operationell och teknisk nivå inom sektorns organisationer.

I syfte att hantera cyberrisker ställs krav på informationsdelning för den finansiella sektorn från såväl ett svenskt som ett internationellt perspektiv. Under 2017 lade även Finansinspektionen särskild vikt vid området cybersäkerhet i sin rapport om tillsyn över bankerna och lyfter där fram forum för operativ informationsdelning samt förbättrade former för samverkan mellan bankerna och andra intressenter.[1]

CPMI (Committee on Payments and Market Infrastructures) och IOSCO (International Organization of Securities Commissions) har utvecklat särskilda riktlinjer, som bland annat riktar in sig på hur finansiella infrastrukturaktörer bör dela information om cybersäkerhet.[2] Under 2016 upprättade FSPOS en särskild projektgrupp som tog fram en rapport om tolkning och tillämpning av riktlinjerna. Under 2017 har gruppens arbete fortsatt i form av en fokusgrupp, FG Cybersäkerhet. Ett område från 2016 års analys som bedömts som särskilt viktigt och utmanande är just informationsdelning. En av gruppens aktiviteter för 2017 har därför varit att utveckla detta PM om informationsdelning av cyberrisker.

Syfte

Syftet med detta dokument är att stärka den finansiella sektorns förmåga att dela information mellan aktörer gällande cyberrisker. Målet är att beskriva forum, riktlinjer och rutiner för sådan informationsdelning, med utgångspunkt i god praxis. Beskrivningarna har dels utgått från en genomgång av relevanta rapporter och vägledningar, dels från diskussioner med representanter som arbetar med berörda frågor inom sina respektive organisationer.

Informationsdelning gällande cyberrisker sker på olika sätt för aktörer i den finansiella sektorn. I denna rapport ligger tyngdpunkten på användning av *forum* för informationsdelning, bland annat då detta har bedömts ligga närmast FSPOS verksamhet gällande privat-offentlig samverkan. En annan utgångspunkt har varit nämnda riktlinjer från CPMI och IOSCO som i hög grad talar om forum och grupperingar där riktlinjerna mer konkret hänvisar till informationsdelning.[3]

Utöver att använda och delta i forum för informationsdelning så använder företag och organisationer som bedriver finansiell verksamhet även andra verktyg och metoder för att få information om cyberrisker. Bland annat så tillhandahåller specialiserade företag t.ex. prenumerationer, analyser och access till särskilda portaler och nätverk för teknisk och strategisk information.

---

[1] Finansinspektionen (2017), *Tillsynen över bankerna*.

[2] CPMI/IOSCO (2016), *Guidance on cyber resilience for financial market infrastructures*.

[3] CPMI/IOSCO (2016), *Guidance on cyber resilience for financial market infrastructures*, avsnitt 8, sida 21.

Nyttan av informationsdelning av cyberrelaterade risker

Behovet av informationsdelning av cyberrisker understryks i många sammanhang. Förutom explicita och implicita krav på utbyte av information för privata och offentliga aktörer, så betonade Regeringen under 2016 att ”samverkan och informationsdelning på informations- och cybersäkerhetsområdet ska stärkas”.[4] Behoven utvecklas i takt med en ökad komplexitet i samhällets beroende av informations- och kommunikationsteknologi. Med denna utveckling följer samtidigt nya former av cyberattacker.

I sammanhanget framhålls ofta att angriparna delar information och erfarenheter och att även de som behöver försvara sig mot angrepp borde upprätta forum och former för informationsdelning. Informationsdelning, t.ex. inom den finansiella sektorn och i form av privat-offentlig samverkan, kan stärka förmågan att hantera cyberrelaterade risker. Utbyte av information kan på så vis upprätta ett ”kollektivt försvar”, som minskar dubbelarbete och innebär att en organisations detektion kan bli en del av en annan organisations förebyggande arbete.

FSPOS Arbetsgrupp Information (AG INFO) betonar nyttan av att sektorns aktörer delar information om cyberrisker. I en vägledning från 2017 – *Kriskommunikation i finanssektorn– en vägledning vid större störningar* - lyfts bland annat fram att aktörer i den finansiella sektorn kan stärka sin förmåga att kommunikativt hantera cyberrisker genom att samverka kring kommunikation gällande cyberangrepp. Enligt vägledningen behöver sektorns aktörer kunna vara transparenta med vad man vet och inte vet vid en inträffad händelse, för att stärka såväl den egna som sektorns motståndskraft. I vägledningen betonas även att sektorn behöver skapa förtroende och hantera tendenser till slutenhet för att fullt ut kunna dra nytta av informationsdelning.

Vägledningen lyfter även fram att 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. [5]

Genom att dela information kan man dra nytta av andra organisationers kunskap, erfarenhet och förmågor. Informationen som delas kan bidra till större förståelse för hot och risker, exempelvis om informationen inkluderar god praxis eller metoder och angreppssätt som används av angriparna och därför kan användas för att bättre skydda sig mot cyberrelaterade risker som drabbar enskilda aktörer eller en sektor som helhet. I slutändan kan därmed en effektiv informationsdelning bidra till stärkt förmåga att upprätthålla kontinuitet i verksamheten, skydd mot ekonomisk skada eller skydd mot negativ påverkan på allmänhetens förtroende m.m. Med informationsdelningen kan deltagande aktörer bidra till att

---

[4] *Nationell strategi för samhällets informations- och cybersäkerhet* (2016), sida 11.

[5] *Kriskommunikation i finanssektorn– en vägledning vid större störningar,* FSPOS (2017), sida 6, 8, 15

- *avskräcka* angripare
- *skydda* mot angrepp genom förebyggande arbete
- *upptäcka* nya hot som därmed kan hanteras bättre
- *reagera* mer effektivt på angrepp för att hantera de omedelbara konsekvenserna bättre
- *återställa* verksamheten bättre efter att ett angrepp har skett.

Framgångsrik informationsdelning bygger därigenom förmågor att hantera cyberrelaterade risker både i det förebyggande arbetet och i den reaktiva hanteringen. Inom den finansiella sektorn finns flera goda exempel på informationsdelningsforum, exempelvis inom ramen för FI-ISAC, FIDI-Finans och Bankföreningen. Bankernas SIRT-team genomför därutöver har veckomöten sedan ett par år där även CERT.SE deltar.[6]

Riktlinjer som ställer krav på informationsdelning i den finansiella sektorn

Guidance on cyber resilience for financial market infrastructures från CPMI/IOSCO ställer direkta eller indirekta krav på informationsdelning mellan finansiella aktörer avseende bl.a. beroenden, hot och risker.[7] Kraven berör såväl förebyggande analysarbete som en mer reaktiv hantering av incidenter. Forum och rutiner för informationsdelning bör, enligt riktlinjerna, vara etablerade på förhand och därigenom stötta det preventiva arbetet och vara tillgängliga när incidenter väl inträffar. Formerna för informationsdelning bör bl.a. inkludera vilken information som delas och hur.

Flera utmaningar har identifierats av FSPOS Fokusgrupp Cybersäkerhet. På en övergripande nivå har konstaterats att förmåga att hantera cyberrisker påverkas av tillgång till information i realtid. De ömsesidiga beroenden som finns i finansiell sektor medför uppenbara behov av att dela information.

Det finns flera nationella och internationella rapporteringskrav som berör området, bl.a. från dataskyddsförordningen som anger att intrång ska rapporteras till Datainspektionen inom 72 timmar.[8] Därtill är EU:s direktiv om nätverks- och informationssäkerhet (NIS-direktivet) under införande, vilket medför obligatorisk rapportering för aktörer som bedriver samhällsviktig verksamhet.[9] Med samhällsviktig

---

[6] Se bland annat https://www.fsisac.com/

[7] Guidance on cyber resilience for financial market infrastructures, CPMI-IOSCO (2016), bl.a. avsnitt 3.3 (sid. 11), 6.4 (sid. 17), 8.3 (sid. 21), m.m.

[8] 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). Se särskilt Artikel 33 "Anmälan av en personuppgiftsincident till tillsynsmyndigheten".

[9] SOU 2017:36 Informationssäkerhet för samhällsviktiga och digitala tjänster (2017), se bl.a. sid. 30-31 och sid. 74-75.

verksamhet avses enligt NIS-direktivet bankverksamhet och finansmarknadsinfrastruktur.[10]

CERT-SE (som är Sveriges nationella CSIRT, Computer Security Incident Response Team) vid MSB (Myndigheten för samhällsskydd och beredskap) är en central aktör aktör för mottagande av IT-incidentrapporter. CERT-SE har genom MSB ett nationellt uppdrag av regeringen att svara för en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera IT-incidenter. Exempel på medvetandehöjande insatser från CERT-SE inkluderar omvärldsbevakning, blogg, månadsbrev, alert-funktion, m.m. Hittills har kunskapshöjande rapporter från CERT-SE, baserade på bl.a. den obligatoriska IT-incidentrapporteringen för myndigheter, endast riktats mot just myndigheter. På sikt kan detta stöd dock komma att ändras i takt med att CERT-SE breddar sin målgrupp för sina analysrapporter. Ett utökat utbyte mellan CERT-SE och aktörer i den finansiella sektorn kan även bli en följd av tillämpningen av NIS inom Sverige, beroende på vilka finansiella aktörer som blir föremål för direktivets rapporteringskrav. CERT-SE deltar även i ett flertal forum för informationsdelning, där aktörer i den finansiella sektorn deltar.

FSPOS Fokusgrupp Cybersäkerhet har konstaterat att det finns många krav på rapportering inom cyberområdet, inom och utanför den egna organisationen, men att formerna för rapportering ofta inte är helt tydliga. I vissa fall kan det vara utmanande att möta tidskrav på rapportering om man är beroende av indata, som i sin tur kan ta tid att få inrapporterad till sig. Särskilt utmanande kan kravställning om informationsdelning bli om organisationen och aktörer som är sammankopplade med organisationen – såsom kunder, partners och leverantörer – är baserade utanför Sverige, där andra regelverk gäller. En framgångsfaktor är att inkludera krav om informationsdelning i avtal och att arbeta med uppföljning avseende cyberfrågor.

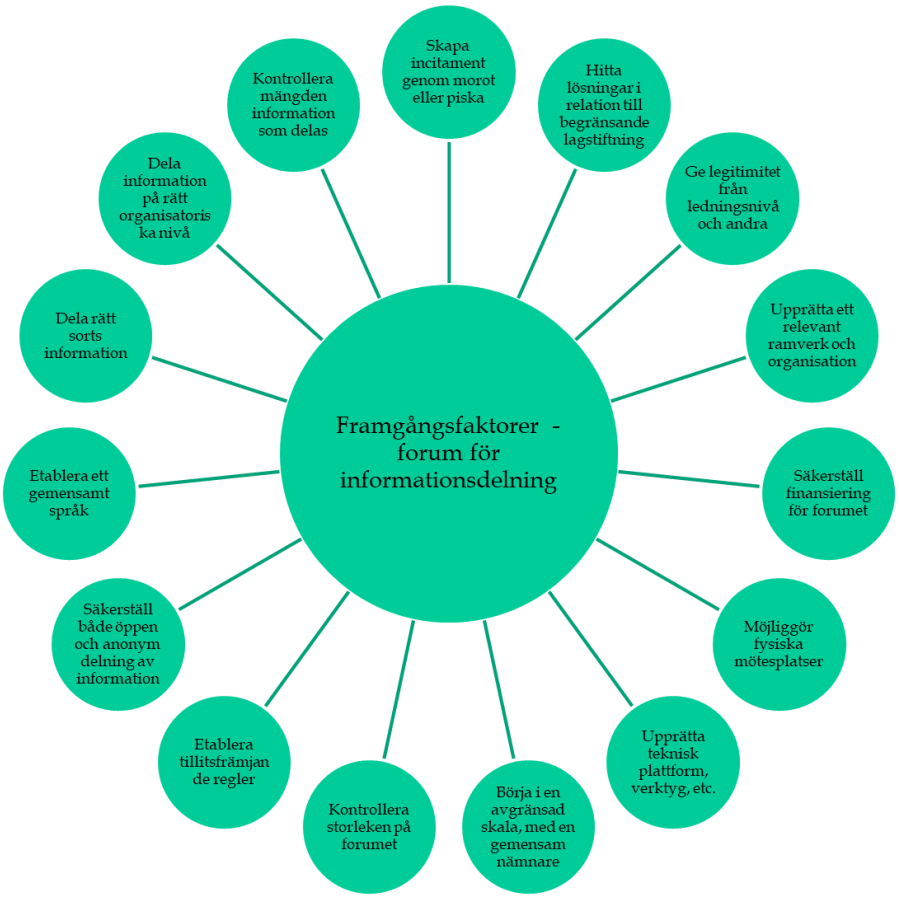
En möjlig källa till information skulle i framtiden kunna vara MSB, baserat på inrapporterade incidenter. En annan framtida framgångsfaktor för att dela information i sektorn är sannolikt Nordic Financial CERT, som grundar sig på det tidigare norska samarbetet FinansCERT. Till en början deltar ett antal nordiska banker i samarbetet, men man har poängterat att ambitionen är att bredda deltagarkretsen. Nordic Financial CERT skulle även kunna skicka ut meddelanden till deltagare för att snabbt sprida relevant information till sektorns aktörer. En finansiell CERT kan få till stånd bilateralt eller multilateralt informationsutbyte mellan finansiella aktörer, där CERT:en fungerar som en mellanhand och kan därigenom skapa en övergripande riskbild, baserat på inrapporterade risker, sårbarheter och incidenter. CERT:en kan dock bara beskriva hotbilden. Risken måste varje aktör själv bedöma, då CERT:en inte vet vilka sårbarheter varje enskild aktör har, eller värdet av informationstillgångar/tjänster som skulle kunna bli föremål för hotbilden.

---

[10] Se bilaga II i NIS-direktivet, *Förslag till EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen.*

Rutiner och former för informationsdelningsforum

Rapporter och vägledningar som beskriver informationsdelningsforum avseende cybersäkerhetsrelaterade frågor beskriver ett flertal framgångsfaktorer, vilka summeras i nedanstående avsnitt och återges i översiktsbilden nedan. Det pågår även ett arbete inom ISO på att ta fram ett internationellt standardförslag (ISO 22396) som ska ge vägledning i frågan om processer för informationsutbyte mellan organisationer. Standarden väntas kunna publiceras under 2019.[11] Därutöver kan nämnas att Europeiska unionens byrå för nät- och informationssäkerhet (ENISA) utvecklar en rapport om informationsdelning, som publiceras under 2018. I sammanhanget kan även nämnas att EU-kommissionen under hösten 2017 har föreslagit att en europeisk IT-säkerhetsmyndighet inrättas, baserad på ENISA. Dess uppdrag och organisation är dock inte klarlagt i dagsläget.[12]



Figur 1. Framgångsfaktorer för forum för informationsdelning av cyberrisker

[11] https://www.sis.se/nyheter-och-press/nyheter2017/samverkan-ger-battre-krisberedskap/
[12] https://www.europaportalen.se/2017/09/strangare-straff-och-ny-eu-byra-mot-natattacker

Skapa incitament genom morot eller piska

Mycket av diskussioner kring informationsdelning av cyberrisker handlar om utmaningarna med att skapa incitament. De potentiella nyttorna med informationsutbyte utgör en ”morot” för aktörer i sektorn. Sådana nyttor kan bland annat få uttryck i minskade avbrott eller minskad ekonomisk skada, till följd av att användbar information kan stärka förmågan att hantera cyberrelaterade risker. En annan fördel som har poängterats är att deltagande i informationsdelningsforum skulle kunna möjliggöra lägre försäkringspremier.[13]

Andra understryker vikten av att införa en mer tvingande ”piska” via lagar, riktlinjer eller avtal. Forumets medlemmar kan därigenom upprätta egna tydliga regler, uppförandekod (code of conduct), rutin för sanktioner mot avsteg från regler, eller övergripande samarbetsavtal (Memorandum of Understanding, MoU). Trots att flera nationella, lagstiftade initiativ, har ökat i antal så är ”självreglering” av olika sektorer den vanligaste formen av informationsdelningsforum inom Europa. I studier har den finansiella sektorn nämnts som den mest utvecklade i detta avseende, med flera exempel på branschinitiativ.[14]

Hitta lösningar i relation till begränsande lagstiftning

Offentlighets- och sekretessfrågor lyfts ofta fram som legala aspekter som medför begräsningar av viljan att dela information, då information som delas kan komma att begäras som offentlig handling eller utgöra sekretessbrott. Potentiella utmaningar kan även finnas i form av konkurrenslagstiftning, om informationsdelningen anses begränsa konkurrensen. Även personuppgiftslagstiftning kan utgöra ett hinder, exempelvis IP-adresser som klassas som personuppgift. I detta fall kan forumet för informationsdelning behöva hitta möjligheter att ”tvätta” informationen innan den delas och därmed anonymisera informationen.[15]

En framgångsfaktor kan i detta avseende vara att sådan information undantas från möjlighet att begäras ut. Ett exempel på detta är *Cybersecurity Information Sharing Act* i USA från 2015. Denna lagstiftning undantar frivilligt delad cyber-information från att röjas, när information delas med myndigheter som kan skydda kritisk infrastruktur från cyberrelaterade hot.[16][17] Andra möjliga lösningar är att använda säkra system, som i sig är undantagna från att utlämna information, för informationsutbytet.[18] Avslutningsvis kan den tekniska lösningens design möjliggöra anonymisering av information som delas. Utformning av processer, rutiner och tekniska lösningar kan således ha ”privacy by design” som utgångspunkt.[19]

---

[13] *Sharing Cyber Security Information* (2015), sida 34.
[14] *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches* (2015), sida 7.
[15] *Sharing Cyber Security Information* (2015), sida 34.
[16] Biztech (2016), ”Financial Industry Looks to Automate Information Sharing for Cybersecurity Risks”.
[17] *Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation* (2016).
[18] *Sharing Cyber Security Information* (2015), sida 31.
[19] *Building an informed community – New cyber threat landscape makes sharing intelligence imperative* (2015), sida 5.

Ge legitimitet från ledningsnivå och andra

En grundläggande utmaning med informationsdelning mellan olika aktörer i en sektor är som sagt att lyfta fram nyttorna med informationsdelning, att bygga förtroende och att få beslut om sådant utbyte från de som har nödvändigt mandat. Detta gäller såväl inom en organisation som mellan organisationer i en sektor. Det har betonats att lednings- och styrelsenivå behöver stödja och främja informationsdelning på sektorsnivå. Dessa behöver i sin tur beakta nyttan av informationsdelning, t.ex. i termer av att det främjar myndigheters uppdrag eller aktieägares intressen. För att informationsdelning ska kunna bli verklighet och få erforderlig effekt, så behöver ledningen därför efterfråga rapportering om cyberfrågor, verka för en kultur där information delas och röja hinder för informationsdelning på olika delar av organisationen.[20]

En framgångsfaktor som har lyfts fram för forum är därutöver att det finns aktörer som lägger grunden och är beredd att initiera informationsdelning för att skapa förtroende mellan sektorns aktörer. Sådana ”Champions” eller ”Key Sponsors” ger legitimitet åt fortsatt utbyte och är ofta aktörer som har relativt stor erfarenhet av och resurser för informationsdelning.[21]

Upprätta ett relevant ramverk och organisation

Återkommande grundförutsättningar som betonas för ett framgångsrikt forum för informationsdelning berör struktur och ramverk. Delar i detta som nämns är en fastställd organisation, t.ex. med styrelse och underliggande grupperingar. Därutöver kan daglig operativ personal behövas för t.ex. program management/administration. Ytterligare personella förutsättningar kan vara att forumet bemannas med sakområdesexperter, både för den löpande förvaltningen och för långsiktigt arbete, såsom utveckling av rapporter, identifiering av trender, m.m.[22] Sakområdesexperter kan komma från såväl mer teknisk eller operativ nivå, som mer taktisk eller strategisk nivå. En möjlig målgrupp på en strategisk nivå skulle kunna vara att inkludera organisationernas Chief Information Security Officer (CISO).[23]

Privat-Offentlig samverkan lyfts i flera fall fram som ett ramverk för informationsdelning av cyberrelaterade risker. Här understryks inte sällan behovet av att ta hänsyn till aktörers olika behov av sekretess. En framgångsfaktor som poängterats är även att deltagande ska hållas frivilligt, men med vissa förpliktelser såsom efterlevnad av principer och regler för forumet. En annan framgångsfaktor som nämnts är att myndigheter i vissa fall kan behöva hålla låg profil för att motivera

---

[20] *Sharing Cyber Security Information* (2015), sida 16-17.
[21] Techtarget (2015), ”Cybersecurity information sharing: Industries join forces”.
[22] *Building an informed community – New cyber threat landscape makes sharing intelligence imperative* (2015), sida 4.
[23] *NCSS Good Practice Guide, Designing and Implementing National Cyber Security Strategies* (2016), sida 21.

informationsdelning mellan privata aktörer.[24] I andra sammanhang är dock behovet som störst gällande informationsdelning från myndigheter till privata aktörer.

Säkerställ finansiering för forumet

För att kunna utveckla och förvalta rätt teknik, plattform och resurser för ett forum för informationsdelning, så krävs en finansieringsmodell. Om inte denna finansiering kommer från statliga medel, så behöver deltagarna sannolikt dela kostnaderna. Löpande medlemsavgifter eller fasta investeringar utgör alternativ för finansieringen.[25]

Möjliggör fysiska mötesplatser

Att deltagare i informationsdelningsforum träffas personligen har beskrivits som en framgångsfaktor för att bland annat bygga förtroende. Mötesplatser kan utgöras av möten i arbetsgrupper, paneldiskussioner, seminarier, m.m.[26] Framgångsrika forum möjliggör återkommande mötestillfällen för exempelvis utbyte av cyberrelaterad information på strategisk och taktisk nivå, såsom god praxis, trender och strategier. Personliga möten kan också bygga ett nödvändigt förtroende för mer automatiserad eller annat elektroniskt informationsutbyte.[27] Heltäckande möjligheter till informationsdelning av cyberrelaterade information kräver dessutom ofta en kombination av mänsklig granskning och elektroniskt utbyte och automatiserad informationsdelning.[28]

Upprätta teknisk plattform, verktyg, etc.

Viss information kan med fördel delas via telefon, SMS, eller e-post, alternativt laddas upp på en säker och gemensam lagringsplats.[29] Informationsutbyte av mer teknisk och automatiserad information underlättas där det finns rätt tekniska plattform, med underliggande infrastruktur och relevanta applikationer, i synnerhet om aktörerna är geografiskt separerade och när informationen behöver utbytas snabbt eller i stora mängder. Plattformen behöver kunna möta säkerhetskrav för att bevara deltagarnas integritet.[30] Ett exempel på plattform för informationsdelning är MISP, en öppet tillgänglig mjukvara som används inom bland annat NATO. Automatiserat och mer tekniskt informationsutbyte sker i högre grad på teknisk och operativ nivå mellan organisationerna.[31]

---

[24] *Sharing Cyber Security Information* (2015), sida 20.
[25] *Building an informed community – New cyber threat landscape maked sharing intelligence imperative* (2015), sida 5.
[26] *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches* (2015), sida 34.
[27] *Sharing Cyber Security Information* (2015), sida 31.
[28] *Biztech (2016)*, "Financial Industry Looks to Automate Information Sharing for Cybersecurity Risks".
[29] *Sharing Cyber Security Information* (2015), sida 31.
[30] *Building an informed community – New cyber threat landscape makes sharing intelligence imperative* (2015), sida 6.
[31] *Sharing Cyber Security Information* (2015), sida 31.

Börja i en avgränsad skala, med en gemensam nämnare

Ibland kan det räcka med att en aktör tar initiativet att dela värdefull information för att en kultur av tillit ska infinna sig och för att en spiral ska sättas igång av informationsdelning. Snabbt vunnen tillit försvinner dock minst lika snabbt om tilliten inte respekteras, och leder då istället till en negativ spiral av misstro.

En framgångsfaktor som har lyfts fram i beskrivningar av god praxis, är att hitta en gemensam nämnare med ett område som berör alla aktörer som deltar i informationsdelningsforumet, exempelvis molntjänster.[32]

Kontrollera storleken på forumet

Ett större forum, bestående av fler aktörer, möjliggör ett allt större utbud av information som delas. Samtidigt beaktar framgångsrika forum för informationsdelning att det finns risker med ett växande nätverk.[33] Fler aktörer kan medföra att gruppens behov och målsättningar skiljer sig avsevärt mellan aktörerna, så att nyttan av informationsdelning på sikt undermineras. Ett större antal deltagare kan också innebära att förtroendet mellan deltagare är svårare att upprätthålla. Framgångsrika forum undviker att deltagarkretsen blir för stor, om detta försvagar förtroende eller medför att deltagarna har avsevärt olika mål och syn på informationsdelningen.[34]

Etablera tillitsfrämjande regler

Tillit är en förutsättning för informationsdelning av cyberrelaterade risker mellan olika aktörer i den finansiella sektorn. Förtroende behöver finnas både för att andra aktörer hanterar integritetsaspekter och för att informationen som delas är verifierad och pålitlig. Framgångsrika informationsdelningsforum hittar därför relevanta lösningar för att bygga förtroende mellan sina medlemmar. Vissa informationsdelningsforum bygger på person-till-person-relationer, andra på en gemensam betrodd tredje part eller på någon form av feedback-/ryktesbaserat system där avvikelser märks i andra medlemmars omdömen/betyg eller öppet tillgängliga feedback. En återkommande erfarenhet som betonas är att förtroende ofta behöver byggas upp över en längre tidsperiod och genom ett långsiktigt samarbete.[35]

En brett formulerad princip som kan etableras för att bygga förtroende är att den som delar informationen bestämmer villkoren för hur informationen används, exempelvis hur informationen får delas vidare. En regel som kan användas är den så kallade *Chatham House Rule*, som förskriver att information som delas vid möten eller motsvarande kan användas fritt, med undantag av identiteten och organisationen för den som delat informationen eller andra som deltar i informationsutbytet. Regeln används vid ett möte om en deltagare vill dela information ”utanför protokollet” eller

---

[32] *Sharing Cyber Security Information* (2015), sida 20.
[33] *NCSS Good Practice Guide, Designing and Implementing National Cyber Security Strategies* (2016), sida 21.
[34] *Sharing Cyber Security Information* (2015), sida 27.
[35] *Sharing Cyber Security Information* (2015), sida 17.

vill behålla sin anonymitet. Chatham House Rule är en enkel och tydlig regel för att uppmuntra öppenhet och förtroende för informationsdelning.[36][37]

Säkerställ både öppen och anonym delning av information

Om information kan delas öppet och utan integritetsrisk inom en sektor, så kan informationsflödet sannolikt ske snabbare och med större tydlighet. När det är möjligt bör därför forum för informationsdelning främja dialoger där deltagarna öppet kan dela information utan att anonymisera den. Ett sätt att främja sådant informationsutbyte är öppna grupp-diskussioner vid fysiska träffar. Även tekniska plattformar som upprättas bör beakta denna möjlighet. Givet restriktioner från tillit, sekretess, m.m. så kan mycket information ändå vara till nytta om den anonymiseras innan den delas. Som har noterats ovan, så är ett sätt att hantera detta genom att med behörigheter styra vilka deltagare som har tillgång till vilken information och genom sekretessavtal (Non-disclosure Agreement, NDA) mellan medlemmarna. I många sammanhang poängteras även fördelarna med att upprätta en tredje-part-lösning, där en betrodd aktör agerar mellanhand för information som delas och vid behov även stå för målgruppsanpassning av information. Andra benämningar på en sådan lösning är ”Clearing House”, ”Fusion Cell”, ”Centre”, ”Information broker”, ”ISAC”.[38][39]

Etablera ett gemensamt språk

Ett gemensamt språk hjälper deltagare i informationsutbytet att bättre förstå och använda informationen. Om deltagande personer har olika nationaliteter, så behöver till att börja med kultur- och språkskillnader beaktas, exempelvis genom att enas om engelska som det språk man kommunicerar på. En vanlig del av ett gemensamt språk i forum för informationsdelning av cyberrisker är därutöver en tydlig och etablerad terminologi och kriterier för hur information klassificeras, i synnerhet vid automatiserad delning av teknisk och tidskritisk information.

Trafikljusprotokoll (TLP) är vanligt i dessa sammanhang, där man även styr vilka deltagare som har behörighet till vilken information. Trafikljusprotokoll möjliggör klassificering av informationen, där den som delar informationen märker den med någon av trafikljusfärgerna (*White, Green, Amber, Red*). Färgskalan innebär en stegring av informationens känslighet och innebär fördefinierade regler för spridning av informationen för respektive nivå. Med tydliga definitioner och regler för trafikljuset, så kan förväntningar och förtroende etableras mellan de som delar och tar del av information.[40][41] En annan del av ett gemensamt språk är att använda gradering av tillitsnivå på information som delas.[42][43]

---

[36] *Sharing Cyber Security Information* (2015), sida 25 och 38.
[37] *https://www.chathamhouse.org/about/chatham-house-rule#*
[38] *Sharing Cyber Security Information* (2015), sida 31.
[39] *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches* (2015), sida 39.
[40] *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches* (2015), sida 39.
[41] *NCSS Good Practice Guide, Designing and Implementing National Cyber Security Strategies* (2016), sida 35.
[42] *Building an informed community – New cyber threat landscape make sharing intelligence imperative* (2015), sida 6.

Standardisering krävs för att automatiserad, med teknisk, information, t.ex. för att IP-adresser m.m. ska kunna användas effektivt och för att man ska kunna jämföra med egna loggar. Delningen underlättas då av ett etablerat och gemensamt kommunikationsspråk/protokoll. Några exempel på sådana, som har använts av finansiella aktörer är STIX, TAXII och CybOX.[44]

Dela rätt sorts information

Det finns en stor mängd information som aktörer inom den finansiella sektorn skulle kunna dela med varandra. För att informationsflödet inte ska bli överväldigande och för att informationen ska vara relevant, så behöver avgränsningar och urval göras. ”Rätt sorts information” beror på flera olika faktorer och styrs av omständigheterna, något som bland annat har uttryckts som ”context is king” i dessa sammanhang.[45]Flera källor betonar vikten av att information som delas ska vara ”handlingsbar”, ”läglig” och ”specifik”.[46] Ett sätt att identifiera vilken information som är ”läglig”, är att utgå från olika faser i incidenthanteringscykeln, från *proaktiv hantering*, via *förebyggande*, *förberedande*, *responsiv* och *återhämtande* faser, till *efterarbete*. ”Rätt sorts information” beror på vilken del av hanteringen som informationen kan göra nytta. Framgångsrik informationsdelning av cyberrelaterade risker i den finansiella sektorn lyckas därför rikta rätt information till rätt mottagare för rätt tillfälle.[47]

Flera studier på ämnet har gjort ansatser att fastställa informationstyper, såsom information om risker, hot, sårbarheter och god praxis.[48] Andra talar om betydligt fler typer, som information från brottsbekämpning, bakgrunds- och referensinformation, compliance-status, information om detektion och mitigering, incidentinformation, god praxis, samt hot eller sårbarhetsinformation.[49] Andra texter beskriver en mer specifik klassificering som antyder hur informationen är ”handlingsbar” eller användbar. Exempel på detta kan vara ”underrättelse om potentiella mål och angripare”, ”metoder och konsekvenser från en framgångsrik attack” eller ”lärdomar och försvarsprinciper”.[50] På ett liknande sätt understryks inte sällan att underrättelse som kan användas för att skydda sig mot angrepp kan summeras i förkortningarna *TTP (tactics, techniques, procedures)* och *IOC (indicators of compromise)*. Denna information kan sprida lärdomar om angripare, deras metoder och hur framgångsrika attacker har genomförts. Finansiella aktörer behöver arbeta med alltifrån enklare IoC (såsom hashfunktioner, IP-adresser, domännamn, m.m.) till mer komplexa nätverk, verktyg och TTP. Genom att mitigera TTP, kan man försvåra angriparens arbete jämfört med om man exempelvis endast mitigerar hashfunkioner eller IP-adresser.

---

[43] ”*How STIX, TAXII and CybOX Can Help With Standardizing Threat Information” (2015).*
[44] ”Financial Industry Looks to Automate Information Sharing for Cybersecurity Risks” (2016).
[45] SC Magazine (2016), ”Cybersecurity preparedness requires threat intelligence information sharing”.
[46] *Cyber Threat Information Sharing - Recommendations for Congress and the Administration*
[47] *Sharing Cyber Security Information* (2015), sida 22-23. Techtarget (2015), ”Cybersecurity information sharing: Industries join forces”
[48] Jfr. ”actionable”, ”timely” och ”specific”. *Incentives and Challenges for Information Sharing in the Context of Network and Information Security* (2010), sida 17 och sida 9.
[49] *Sharing Cyber Security Information* (2015), sida 23.
[50] *Building an informed community – New cyber threat landscape makes sharing intelligence imperative* (2015), sida 5.

Informationsdelning inom sektorn kan göra stor nytta i form av ett ”kollektivt försvar”, men behöver beakta riskerna med att dela information som äventyrar integritet, affärshemligheter, personuppgifter och exponering mot tillsynsmyndigheter. TTP/IOC i form av tekniska hot-indikatorer - exempelvis IP-adresser, koder eller mönster av tekniker och taktik - kan lättare anonymiseras och kan med mindre risk hjälpa andra liknade aktörer med liknande data att skydda sig mot attacker. Med mindre integritetsrisk, så lämpar sig denna sorts information bättre för automatiserad delning än information som är mer kontextuell och specifik, såsom drabbade mål, kundinformation eller särskilda sårbarheter. [51][52]

Dela information på rätt organisatoriska nivå

Flera källor framhäver vikten av att anpassa informationen som delas till olika delar av organisationen, exempelvis strategisk, taktisk, operationell och teknisk.[53] Informationsdelning behövs på samtliga av dessa nivåer och utbytet behöver ske koordinerat. Det poängteras inte sällan att informationen som delas mellan organisationer bör flöda horisontellt, t.ex. från strategisk nivå i en organisation till strategisk nivå i en annan organisation. Detta förhållningssätt motiveras av att en viss typ av information finns och behövs på samma nivå inom aktörer i en sektor. När information rör sig vertikalt är det oftast inom en organisation. Delning av information diagonalt, t.ex. mellan teknisk nivå i en organisation till strategisk nivå i en annan, tenderar enligt vägledningar och artiklar att leda till förvirring då informationskanaler, kommunikationssätt och språk kan skilja sig åt beroende på nivå. Forum för informationsdelning mellan aktörer i en sektor kan upprätta delning över flera nivåer eller upprättas endast för en nivå, t.ex. med deltagare på teknisk nivå. Det viktiga är att informationen är relevant för mottagaren.[54]

Kontrollera mängden information som delas

En lärdom som återkommer i beskrivningar av god praxis är att anpassa ”volymen” av information, dvs. stimulera rätt nivå på flödet. Risken är annars att deltagarna antingen bara bidrar med minsta möjliga insats (”minimum compliance”) eller för mycket information delas (spamming).[55] Risken är även en kombination av dessa, där deltagare delar en stor mängd information av lågt värde, i syfte att dela information för delandets skull.[56]

---

[51] *Cyber Threat Information Sharing - Recommendations for Congress and the Administration*, sida 7.
[52] Techtarget (2015), “Cybersecurity information sharing: Industries join forces”
[53] *Sharing Cyber Security Information* (2015), sida 21.
[54] *Incentives and Challenges for Information Sharing in the Context of Network and Information Security* (2010), sida 18
[55] *Building an informed community – New cyber threat landscape makes sharing intelligence imperative* (2015), sida 7. *Sharing Cyber Security Information* (2015), sida 19.
[56] *Sharing Cyber Security Information* (2015), sida 31.

Bilaga 1: Exempel på befintliga forum för informationsdelning

I denna bilaga beskrivs några forum och nätverk som används för spridning av information om cyberhot/incidenter och som används av aktörer inom den finansiella sektorn.

Forum	Sammanfattande beskrivning
FIDI-Finans	Drivs av MSB, med representanter från myndigheter, infrastrukturaktörer, banker, Polisen och FRA. Informationsdelning i samband med möten, som styrs av särskilda riktlinjer (bl.a. *Traffic Light Protocol*)
Svenskt CERT-Forum	Grundat av CERT-SE och PTS, med representanter från storbanker men inte från finansiella infrastrukturaktörer, försäkring m.fl. Informationsdelning löpande vid behov via e-post, telefon och krypterad chat. Fyra ordinarie möten genomförs årligen.
Informationssäkerhetsrådet	Drivs av MSB, med representanter från Riksbanken och Riksgälden, samt från ett antal andra offentliga och privata aktörer. Informationsledning i samband med möten, för att diskutera omvärldstrender och bistå med ingångsvärden till MSB:s arbete.
Informationssäkerhetsgruppen i Bankföreningen	Bankföreningens informationssäkerhetsgrupp, sammanträder regelbundet och samverkar även med externa parter, såsom polis och IT-leverantörer.
Bankernas SIRT-team	Bankernas SIRT-team (Security Incident Response Team) genomför veckovisa möten, med operationell delning mellan bankernas SIRT-team Många svenska bank-SIRT-team är certifierade och med i TF-CSIRT. EC3-portalen finns också för infodelning.
FI-ISAC (The European Financial Institutes – Information Sharing and Analysis Centre)	Nätverk inom EU, med representanter från t.ex. banker från medlemsländer men även nationella CERT och brottsbekämpande organ. Informationsdelning (med *Traffic Light Protocol)* via löpande direktkommunikation mellan deltagare, med samlade informationsutskick, samt vid möten två gånger årligen.

FS-ISAC (The Financial Services Information Sharing and Analysis Center)	Medlemsdrivet och har ett operativt fokus. Medlemmar är nationella, regionala och globala aktörer, såväl privata som offentliga. Deltagarna är banker, försäkringsbolag, betalningsförmedlare, kortutgivare, m.fl. Informationsdelning bl.a. genom varningsmeddelanden. Delningen styrs av ett *Traffic Light Protocol.* Tillhandahåller även en operativ krisgrupp för större incidenter samt ett dedikerat *Security Operations Center* för bl.a. eskalering av ärenden.
Nordic Financial CERT	Nordic Financial CERT grundar sig på det tidigare norska samarbetet FinansCERT och har som vision att stärka den nordiska finansiella sektorns motståndskraft mot cyberattacker för att säkerställa säkra och pålitliga finansiella tjänster. I samarbetet deltar Danske Bank, Nordea, DNB, m.fl, med målsättningen att utöka och bredda medlemkretsen under kommande år.
Financial Services Information Exchange (FSIE)	Forum för informationsdelning inom den finansiella sektorn i Storbritannien. Medlemmar, inkluderar banker, försäkringsbolag, fondhandlare och värdepappersmäklare. Informationsdelning genom möten för direkt utbyte av information. Utbyte styrs av sekretess och gradering av informations känslighet. FSIE genomför även telefonkonferenser och tillhandahåller anonymiserad e-postkorrespondens, samt fokuserat arbete i mindre grupper gällande specifika sakfrågor
Cyber-security Information Sharing Partnership (CiSP)	Privat-offentligt initiativ i Storbritannien för informationsutbyte om cyberhot. Medlemmar får information om hot och risker från en ”Fusion Cell”, en privat-offentlig grupp av analytiker. Informationen inkluderar varningsmeddelanden och rådgivning, samt skräddarsydd analys av misstänkt malware och phishing
Financial Intelligence Unit Netherlands (FIU-Netherlands	FIU-Netherlands är en fristående del inom den holländska polisen, med syfte att stärka såväl brottsförebyggande arbete som utredningsarbeten av genomförda brott.

FIDI-Finans

Myndigheten för samhällsskydd och beredskap (MSB) driver ett antal nationella samverkanforum enligt konceptet FIDI - Forum för informationsdelning avseende informationssäkerhet. FIDI-konceptet bygger på riktlinjer och erfarenheter från Storbritannien[57] och går ut på att myndigheter och privata aktörer delar information om risker och sårbarheter. Syftet med samverkan är bland annat att höja enskilda organisationers beredskap genom att ta lärdomar av andra aktörers erfarenheter.[58]

En särskild FIDI-grupp för informationsdelning med inriktning på finanssektorn, FIDI-Finans, startades 2009. Denna grupp har till syfte att identifiera och initiera åtgärder för den finansiella sektorn som kan bidra till ökad säkerhet och minskad gemensam sårbarhet. Medlemmar i FIDI-Finans är MSB, Bankföreningen, Svensk Försäkring, Bankgirot, Handelsbanken, Nordea, Skandiabanken, Swedbank Euroclear, Finansinspektionen, Nasdaq OMX, Nordnet, Riksbanken, Riksgälden, SEB, Polisen NBC (Nationella Bedrägeri Centret), SÄPO, samt Försvarets radioanstalt (FRA).

Arbetet inom FIDI-Finans bygger på förtroende mellan de aktörer som deltar. För att uppnå denna tillit, finns ett flertal överenskommelser som styr informationsutbytet. Bland annat särskilda mötesregler, exempelvis om informationsdelning vid slutna möten och att endast personligt deltagande vid möten är tillåtet. Därigenom ställs krav på närvaro och ersättare är inte tillåtet. Informationsdelning sker genom ett så kallat *Traffic Light Protocol*, en överenskommelse för att säkerställa att känslig information delas enligt särskilda kriterier efter bedömning av den aktör som är källa till informationen som delas. Under 2018, så genomgår alla som deltar i forumet säkerhetsklassning.[59]

Svenskt CERT-Forum

Svenskt CERT-forum bildades 2003 av CERT-SE (då som Sveriges it-incidentcentrum, Sitic) och av PTS. De svenska storbankerna ingår i forumet, däremot inte försäkringsbolag, finansiella infrastrukturbolag, eller mindre banker. Det saknas därmed forum där samverkan sker mellan CERT-SE en bred representation av den finansiella sektorn. Svenskt CERT-forum upprättades för att skapa informations- och erfarenhetsutbyte inom cyberområdet. Årligen anordnas fyra gemensamma träffar för deltagarna. Därutöver sker löpande samverkan via telefon, mail och chat. Vid incidenter finns t.ex. möjlighet att kommunicera säkert med krypterad chat (med protokollet Jabber). Infrastruktur tillhandahålls även för säker delning av loggar.[60]

---

[57] Bygger på erfarenhet från Brittiska Centre for the Protection of National Infrastructure (CPNI) och arbete med Information Exchange (IE).

[58] MSB (2010), ”Åtgärder för att förbättra samhällets samlade förmåga att förebygga och hantera IT-incidenter”, s.15.

[59] Se Kungliga Krigsvetenskapsakademin (2013): http://kkrva.se/hot/2013:1/avd_V_kristalighet_genom_privat-offentlig_samverkan.pdf.

[60] Samverkansmöte mellan FSPOS och CERT-SE 10 juni 2015.

Informationssäkerhetsrådet

Myndigheten för samhällsskydd och beredskap (MSB) har, för att utnyttja samhällets samlade kompentens på informationssäkerhetsområdet, knutit till sig ett informationssäkerhetsråd med bred representation från både offentlig förvaltning och näringslivet. Informationssäkerhetsrådet består bl.a. av representanter från Riksbanken och Riksgälden.[61] Informationssäkerhetsrådet har i uppgift att bistå MSB med information om utvecklingstrender inom området informationssäkerhet, synpunkter på inriktning, prioritering och genomförande av MSB:s arbete inom området, samt att bidra till spridning av information om MSB:s arbete med informationssäkerhet i omvärlden.[62]

FI-ISAC (The European Financial Institutes – Information Sharing and Analysis Centre)

FI-ISAC är ett nätverk som grundades 2008, som syftar till att dela kunskap om de senaste hoten och riskerna och därigenom höja medvetandet hos europeiska finansiella aktörer. FI-ISAC främjar informationsutbyte gällande bl.a. cyber-kriminalitet som påverkar finansiell sektor, sårbarheter och hot, samt tekniska trender. Delning av erfarenheter sker även genom incidentbeskrivningar och fallstudier.[63]

Deltagare består av finansiella aktörer såsom banker från medlemsländer men även nationella CERT och brottsbekämpande organ. Andra organisationer som är representerade är ENISA (European Network and Information Security Agency), Europol, Europeiska centralbanken (ECB), European Payments Council (EPC) och Europeiska kommissionen. Europeiska FI-ISAC stöds aktivt av ENISA.

Deltagarna delar information genom möten som genomförs två gånger per år. Dessutom delas information kontinuerligt genom en särskild utskickslista (EU FI-ISAC list server). Utbyte sker även genom direkt kommunikation mellan deltagande aktörer.

Precis som beskrivits ovan för FIDI-Finans, är tillit en förutsättning för samarbetet mellan deltagande aktörer. Alla medlemmar måste underteckna Traffic Light Protocol, dvs. regler för informationsdelning. En särskild avsiktsförklaring finns även mellan FI-ISAC och Europol för att stärka informationsutbytet mellan finansiella aktörer och brottsbekämpande organ.

---

[61] Övriga medlemmar är Polismyndigheten, Post- och telestyrelsen, Säkerhetspolisen, Försvarets radioanstalt, Vattenfall, .SE (Stiftelsen för Internetinfrastruktur), Karlstads Universitet, Försvarsmakten, Ericsson, Västra Götalandsregionen, Försvarshögskolan, Försvarets materielverk och Scania.

[62] SOU 2015:23, *Informations- och cybersäkerhet i Sverige - Strategi och åtgärder för säker information i staten*, s.168.

[63] För ytterligare information, se https://www.enisa.europa.eu/activities/cert/support/information-sharing/european-fi-isac-a-public-private-partnership.

FS-ISAC (The Financial Services Information Sharing and Analysis Center)

FS-ISAC är en icke-vinstdrivande global organisation för finansiell sektor, som ägs av privata aktörer och som grundades 1998. Organisationens huvudfokus är operativ krishantering, framförallt gällande informationssäkerhet, där tjänster som erbjuds inkluderar varningsmeddelanden. Finansiella aktörer som deltar kan dela aktuell och korrekt information samt analyser gällande cyberhot[64]. Organisationen samarbetar med nationella, regionala och globala aktörer, såväl privata som offentliga. Bland deltagarna finns banker, försäkringsbolag, betalningsförmedlare, kortutgivare, m.fl. Förutom finansiella aktörer, finns även samarbete med aktörer såsom brottsbekämpande organisationer och CERT.

FS-ISAC är medlemsdrivet och erbjuder deltagarna möjlighet att bidra till att utforma gemensamma strategier, verktyg och samordning. Ett exempel på en tjänst som erbjuds medlemmar är anonym delning av de senaste incidenterna och hoten som uppmärksammats av medlemmar. Varningsmeddelanden delas med ett särskilt tekniskt stöd för att öka medvetenheten och stärka taktisk planering. En särskild krisledningsgrupp kan aktiveras vid större händelser som påverkar flera medlemmar och hotar kritisk finansiell infrastruktur, såsom DDoS-attacker eller kapning av konton. Ett dedikerat så kallat Security Operations Center finns dessutom tillgängligt dygnet runt för att besvara frågor, eskalera cybersäkerhetsärenden och tillhandahålla rapporter. FS-ISAC anordnar dessutom övningar, möten, regionala konferenser, utbildningar, m.m.

Precis som för andra forum för informationsutbyte, är tillit och förtroende en förutsättning, vilket skapas genom såväl fysiska möten med medlemmar som genom regler för hur information delas. Ett sätt att skapa ömsesidigt förtroende i informationsutbytet är användning av Traffic Light Protocol. I oktober 2016 meddelade FS-ISAC att man även kommer att etablera ett Financial Systemic Analysis & Resilience Center (FSARC), i syfte att ytterligare stärka samverkan mellan sektorns aktörer och med uppgift att proaktivt identifiera, analysera, bedöma och koordinera aktiviteter för att motverka cyberrelaterade hot och risker.

Nordic Financial CERT (NFCERT)

Nordic Financial CERT grundar sig på det tidigare norska samarbetet FinansCERT och har som vision att stärka den nordiska finansiella sektorns motståndskraft mot cyberattacker för att säkerställa säkra och pålitliga finansiella tjänster. NFCERT har som mission att möjliggöra för nordiska finansiella institutioner att hantera cyberhot och online-brott snabbt och effektivt. Detta uppnås bland annat genom att NFCERT faciliterar informationsdelning mellan medlemmar, partners och offentliga institutioner. Målet uppnås även genom publicering av information om cyberhot,

[64] För ytterligare information, se bl.a. https://www.fsisac.com/about.

erbjuda Threat Intelligence-tjänster, samt genom att koordinera och stödja mitigerande aktiviteter mot cyberhot och online-brott.

I nuläget erbjuder NFCERT ett antal grundläggande tjänster, såsom en medlemsportal för informationsutbyte och ett responsteam för att stödjda och koordinera cyberincidenter. Därutöver erbjuds anti-phishing och anti-malwaretjänster, samt fungerar som samverkansforum och nätverk. Planen är att kunna erbjuda mer komplexa tjänster runt 2019-2020, i form av exempelvis forensisk analys, cyberövningar, samt ett sensornätverk.

I samarbetet deltar Danske Bank, Nordea, DNB, m.fl. Nordic Financial CERT uppmuntrar fler aktörer i sektorn att delta. Målet är att expandera under de kommande åren, både genom att rekrytera nya medlemmar och genom att fördjupa och utvidga samarbetet mellan medlemsföretagen och till partners och nyckelleverantörer, myndigheter och nationella CERT-funktioner.[65] Alla licensierade finansiella institutioner som lyder under tillsyn från en nordisk tillsynsmyndighet kan ansöka om medlemskap.

Den tidigare norska FinansCERT upprättades 2013 för att stödja sektorn i övervakning och hantering av cyberrelaterade hot och risker. Funktionen fungerade dels som ett nätverk med etablerade kontaktuppgifter/kontaktvägar för informations- och erfarenhetsdelning, dels tillhandahålldes omvärldsbevakning och översiktliga analyser för sektorn. FinansCERT arbetade även med specialiststöd för hantering och begränsning av incidenter och hade en kommunikationscentral för samordning och tilldelning av gemensamma resurser.[66]

Financial Services Information Exchange (FSIE)

FSIE bildades 2003 för att dela känslig information rörande hot, risker och sårbarheter inom den finansiella sektorn i Storbritannien. FSIE:s medlemmar, som består av banker, försäkringsbolag, fondhandlare och värdepappersmäklare, träffas för att verbalt utbyta information om hot risker och sårbarheter i den nationella informationsinfrastrukturen. FSIE leds av National Infrastructure Security Co-ordination Center (NISCC) och alla medlemmar har skrivit under en överenskommelse om sekretess. All information som delas under möten bedöms och graderas beroende på hur känslig den är. På detta sätt blir medlemmarna medvetna om hur de kan hantera informationen. Den som lämnar information ska också förbli anonym utanför gruppen. Utöver möten genomför FSIE telefonkonferenser och tillhandahåller anonymiserad e-postkorrespondens, samt fokuserat arbete i mindre grupper gällande specifika sakfrågor.[67]

---

[65] Sak och Liv, ”Stoppa cybertjuven! Nytt nordiskt forum ska motverka cyberbrott”, 10 april 2017.

[66] FinansCERT (2015). *Digitale banktjenester – Et trusselbilde i rask endring*.

[67] Enisa (2015), *Regulatory and Non-regulatory Approaches to Information Sharing,* KBM (2005), *Informationsutbyte/Privat-offentlig samverkan, Storbritanien*.

Cyber-security Information Sharing Partnership (CiSP)

CiSP är ett privat-offentligt initiativ i Storbritannien för informationsutbyte om cyberhot. Medlemmar får information om hot och risker från en ”Fusion Cell”, en privat-offentlig grupp av analytiker. Informationen inkluderar varningsmeddelanden och rådgivning, samt skräddarsydd analys av misstänkt malware och phishing.[68]

Financial Intelligence Unit Netherlands (FIU-Netherlands)

FIU-Netherlands är en fristående del inom den holländska polisen, med syfte att stärka såväl brottsförebyggande arbete som utredningsarbeten av genomförda brott. FIU-Netherlands nyttjar den nationella polisens organisation, teknik och kommunikation som stöd för att dela data mellan ett hundratal organisationer från olika sektorer. Informationen delas framförallt på taktisk nivå.[69]

[68] https://www.ncsc.gov.uk/cisp

[69] *Building an informed community – New cyber threat landscape makes sharing intelligence imperative* (2015), sida 42.