2019-01-14

josefin.gibson@sakerhetspolisen.se
sofie.klahr@sakerhetspolisen.se

Bankföreningens synpunkter och frågor på *Säkerhetspolisens utkast på nya säkerhetsskyddsföreskrifter*

Bankföreningen har den 19 december beretts tillfälle att yttra sig över Säkerhetspolisens nya säkerhetsskyddsföreskrifter. Bankföreningen anser att det är logiskt att finanssektorn omfattas av de nya säkerhetsskyddsföreskrifterna. Föreskrifterna kan verka som en hävstång för att skapa en ännu mer robust säkerhetskultur och awareness i alla delar av verksamheten vilket är positivt.

Hänsyn har, så vitt Bankföreningen kan bedöma, inte tagits till att föreskriften ska implementeras i näringsverksamheter. Bankföreningens bedömning är att många krav inte kommer att kunna tillgodoses med den typen av formuleringar.

Synpunkterna och frågorna sammanfattas i två delar: 1) väsentliga synpunkter och, 2) mindre synpunkter på föreskrifterna. Några av de väsentliga synpunkterna har framförts till Säkerhetspolisen på mötet den 14 januari medan de mindre synpunkterna på föreskrifterna inte har framförts på mötet.

1. Väsentliga synpunkter

Nedan lyfter vi de synpunkter som Bankföreningen bedömer som de mest väsentliga för Säkerhetspolisen att beakta i utvecklande och fastställande av föreskrifterna.

1. <u>Tillkommande krav på informationssäkerhetsområdet skapar oklarheter</u>
   Angående 4 kap. Informationssäkerhet i informationssystem kan Bankföreningen konstatera att åtminstone tre regleringar kommer att gälla för samma område vilket inte framstår som en transparent och tydlig väg att gå. Det kan leda till en svårgenomtränglig tillsynsmassa för både myndigheterna och verksamhetsutövarna. Det måste säkerställas att olika lagkrav inte medför kollisioner eller på annat sätt skapar oklarheter för verksamhetsutövarna.

   Informationssäkerhet regleras genom Finansinspektionens föreskrifter FFFS 2014:5 och, för större aktörer beträffande betaltjänster gäller Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (SFS 2018:1174 (NIS-

direktivet)). Utöver detta kan utvalda delar av verksamheten i en bank komma att klassas som extra skyddsvärd enligt säkerhetsskyddsföreskrifterna och då omfattas av den regleringen.

Gränsdragningen mellan lagen om informationssäkerhet för samhällsviktiga och digitala tjänster är i praktiken svår att förstå eftersom MSB (med hjälp av Finansinspektionen) särskilt har pekat ut betaltjänster som samhällsviktiga. Samtidigt gäller inte den lagen för verksamheter som omfattas av krav på säkerhetsskydd enligt säkerhetsskyddslagen (SFS 2018:1174 / SFS 2018:1176 8 §. Lagen gäller inte för verksamhet som omfattas av krav på säkerhetsskydd enligt säkerhetsskyddslagen). Bankföreningen ser behov av stöd och vägledande diskussioner från de tre tillsynsmyndigheterna (MSB, FI och SÄPO) rörande dessa gränsdragningsfrågor.

Nya aktörer och branscher kommer att omfattas av den nya Säkerhetsskyddslagen, förordningen och föreskriften. Många av dem är inte bekanta med området och begreppsapparaten. Bland annat introduceras nya begrepp som den finansiella sektorn inte är bekant med i regleringssammanhang t ex konsekvensnivåer, säkerhetsskyddsklassificerad, säkerhetsklass, säkerhetsskyddsklass, säkerhetsskyddsavtalsnivåer, dimensionerande hotbeskrivning, säkerhetsskyddsanalys, säkerhetsskyddsplan, särskild säkerhetsskyddsbedömning, säkerhetsskyddsåtgärder mm. Föreskriften bör därför inledas med definitioner av relevanta begrepp för ökad tydlighet även om vi förstod på hearing den 14 januari att det inte är aktuellt.

Hänsyn har, så vitt Bankföreningen kan bedöma, inte tagits till att föreskriften ska implementeras i näringsverksamheter utan utgår från ett myndighetsperspektiv. Bankföreningens bedömning är att många krav inte kommer att kunna tillgodoses med den typen av formuleringar. Bankföreningen undrar om något stöd eller vägledning (”översättning”) av föreskriften kommer att tillhandahållas av någon av myndigheterna. Särskilt viktigt är vägledning i ett tidigt skede och av begreppet ”säkerhetskänslig verksamhet”, eftersom sådan verksamhet kan vara integrerad i annan del av bankernas verksamhet.

Vid sidan om säkerhetsskyddsföreskrifterna kan ytterligare komplexitet vara på väg att skapas för bankverksamhet på temat informationssäkerhet. EBA (europeiska banktillsynsmyndigheten) skickade den 19 december EBA draft Guidelines on ICT and security risk management (EBA/CP/2018/15) på remiss, med sista svarsdatum den 13 mars.

Diskussionen om säkerhetsskyddslagen, påverkan av lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-direktivet) och EBA/CP/2018/15 och hur dessa förhåller sig till FFFS 2014:5 kan alltså behöva

fördjupas ytterligare mellan bankerna och tillsynsmyndigheterna. Bankerna vill förstå och veta vilka delar av bankverksamheten som berörs av respektive lag.

MSB har angett vilka branscher och typ av aktörer som berörs av NIS-direktivet och förtydligat vilka banktjänster som omfattas. I den förteckningen framgår att MSB anser att betaltjänster är samhällsviktiga när de tillhandahålls av de större bankerna i landet. Kommer ansvarig tillsynsmyndighet att presentera något liknande avseende säkerhetsskyddslagen/säkerhetsskyddsföreskrifterna?

Bankerna efterfrågar specifikt definitioner och vägledning inom följande områden:

- Vilken/vilka verksamhet/er inom bankområdet omfattas?

- Vilka konsekvenskategorier är relevanta för bankbranschen och för vilken verksamhet?

- Kan det vara så att bankbranschen hanterar kvalificerat hemlig och hemlig information? Eller är bedömningen att bankerna endast hanterar konfidentiell och/eller begränsat hemlig information. Bedömningen och vägvalet kan ha stor inverkan avseende föreskriftens omfattande krav på informationssäkerhetsåtgärder, försvarsmaktsgodkända krypton etc.

- Utan definition av scope riskerar risk att flyttas mellan banker och lagens syfte inte uppnås. Omfattas t ex transaktioner och tillgångar för privatpersoner, företag, myndigheter eller endast en del av dessa? Vilka bankområden omfattas? Är t ex trading en del av nationell betalningsförmåga? Det är avgörande vilka bankområden och produkter som omfattas av föreskrifterna som en del eller som en helhet.

I föreskriftens inledning anges att verksamhetsutövaren ska anpassa skyddsåtgärder i relation till hotbilden. Vid genomgång av hela föreskriften är det endast i avsnittet om Fysisk säkerhet som man tar upp ” i den omfattning som skyddsdimensioneringen kräver”. I övrigt tycks den, för banker så viktiga principen, riskbaserad bedömning (”risk-based approach”) inte vara tillämpbart. Risk-based approach är helt central i bankverksamhet och genomsyrar allt i affärsdrivande verksamhet. Det tycks inte ingå i myndigheternas begreppsapparat och vissa krav avseende kvalificerat hemlig och hemlig information ter sig helt orimliga för en affärsdrivande verksamhet.

2. Angående incidentrapportering (2 kap 22 §)
   Angående incidentrapportering anger föreskriften att verksamhetsutövaren ska ”snarast, dock senast i samband med att en anmälan görs till Säkerhetspolisen, påbörja arbetet med en skadebedömning”. Begreppet ”skadebedömning” är nytt för bankerna och kan behöva förtydligas.

   För bankerna är incidentrapportering en sedan länge etablerad process och i dagsläget är den både utmanande och på olika sätt resurskrävande. Vägledning från de relevanta myndigheterna har varit otydlig och begränsad. Bankföreningen efterfrågar vägledning, gärna med exempel, eftersom anmälningsplikt inträder.

   De senaste åren har ett flertal nya regleringar kommit gällande ny incidentrapportering; GDPR, PSD2 och NIS. Bankerna producerar en strid ström av incidentrapporter som efterfrågas av olika myndigheter, i flera fall kan orsaken vara samma händelse. Bankföreningen ifrågasätter inte att rapportering kan vara av vikt för att myndigheter ska få en bild av en verksamhetsutövares verksamhet. Vi anser dock att dubbelrapportering med olika format, definitioner, mallar och frekvens för likartade uppgifter bör undvikas. I den mån en myndighet har behov av information som en annan myndighet redan har så bör – i första hand – ett informationsutbyte mellan dessa myndigheter ske. För att skapa en administrativ effektivitet hos verksamhetsutövarna bör rapportering av incidenter ske till en myndighet och i redan upparbetade format och mallar.

   Branschen har många, och ibland omfattande, outsourcing- och leverantörsavtal med globala företag på IT-området. Avtal av betydelse skall anmälas till FI. Det måste säkerställas att samrådskravet för säkerhetsskyddad upphandling (PMFS 7 kap 1§) inte innebär orimligt långa handläggningstider från myndighetens sida. Om en stor del av bankers verksamhet kommer att omfattas kan handläggningstiderna få stor påverkan på branschens aktörer. Tydlighet och ”one point of entry” för finansiella institutioner efterfrågas i tillsynsfrågan mellan FI, MSB och SÄPO (PMFS 8 kap 1§).

3. Att gemensamt definiera scope, konsekvensnivåer och kategorier
   För att den befintliga metoden för systematisk säkerhetsskyddsanalys ska kunna tillämpas (§1) för en ny bransch behöver scope definieras, och konsekvensnivåer och kategorier gemensamt definieras (av tillsynsmyndighet eller SÄPO). Verksamhetsutövarna har därefter möjlighet och enskilt ansvar för att göra en säkerhetskyddsanalys och planera för åtgärder. Bankföreningens bedömning är att en gedigen säkerhetsskyddsanalys kan ta cirka ett år att göra. Utgångspunkten i det arbetet behöver bottna i kunskap om vilka konsekvensnivåerna och konsekvenskategorierna är. Utan den kunskapen är det svårt för verksamhetsutövarna att veta vilka åtgärder man bör och ska vidta.

En potentiell administrativ konsekvens av de nya säkerhetsskyddsföreskrifterna kan bli att verksamhetsutövare behöver upprätta ett stort antal ansökningar om säkerhetsskyddsklassning. Det kräver att det finns motsvarande resurser för att ta emot och handlägga ett eventuellt stort antal ansökningar hos Registerkontrolldelegationen och Säkerhets- och integritetsskyddsnämnden. Bankföreningen välkomnar beskedet den 14 januari att Säpo undersöker hur ansökningsprocessen för registerkontroll kan digitaliseras eftersom ett sådant verktyg kan minska handläggningstiden.

4. Att balansera föreskrifternas krav med krav i affärsdriven verksamhet
Syftet med nya säkerhetsskyddsföreskrifterna är att reducera sårbarheter och minska risk i verksamhet som är av central betydelse för Sveriges säkerhet samt att skydda säkerhetskänslig verksamhet från antagonistiska hot. Syftet med nya säkerhetsskyddsföreskrifterna riskerar dock att inte uppnås till fullo om inte samtliga aktörer i sektorn omfattas av kraven vilket framfördes av flera företrädare på mötet den 14 januari. Det riskerar att resultera i att sårbarheten flyttas från en aktör till en annan aktör vilket inte minskar sektorns aggregerade risk.

   Å andra sidan skapar ökad regelverksbörda kostnader och det är inte lagstiftarens intention att snedvrida konkurrens eller att begränsa näringsverksamhetens utveckling och konkurrenskraft ur ett internationellt perspektiv. Det är inte alltid verksamhetsutövarens storlek som är avgörande för de risker verksamheten medför och det ligger i farans riktning att risker hos mindre verksamhetsutövare ignoreras. Det tycktes finnas en viss förståelse från Säpo på mötet den 14 januari för resonemangen från privata aktörer att ökade regelverkskostnader kan snedvrida konkurrensen. Det är angeläget att föreskriften och myndigheten tar hänsyn till att det är pågående, etablerad och affärsdriven verksamhet som ska anpassas till de nya kraven och inte myndigheter som etablerats och utvecklats över lång tid där säkerhetsskydd varit en känd parameter.

5. Tillsynsansvaret är otydligt
Tillsynsfrågan berörs i kap 8 men också i "Kompletteringar till den nya säkerhetsskyddslagen" (2018:82) som publicerades den 30 november: https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2018/11/sou-201882/

   Det finns idag en otydlighet gällande Finansinspektionens roll fram tills den 1 januari 2021. Av säkerhetsskyddsförordningen 7 kap 1§ 6p framgår att Länsstyrelserna utövar tillsyn över säkerhetsskyddet och, i bilagan till samma förordning, att Finansinspektionen beslutar om personals placering i säkerhetsklass. Förtydligande behövs gällande övriga uppgifter och det ansvar som är aktuella för Finansinspektionen.

En förutsättning för en väl fungerande tillsyn är att myndigheten har kunskap om både tjänster, produkter och system och bankverksamhet är dessutom omgärdad av mycket regler. Enligt Bankföreningen är det därför naturligt att (det långsiktiga, från 2021) tillsynsansvaret läggs på Finansinspektionen.

6. Bankföreningen efterlyser vägledning för gränsöverskridande verksamhet
   Bankföreningen efterlyser vägledning om hur lagen och föreskriften ska tillämpas i situationer då företag som omfattas av regelverket ingår i en koncern eller en finansiell grupp samt i situationer då företag som omfattas av regelverket bedriver gränsöverskridande verksamhet.

2. Mindre synpunkter på föreskrifterna

Nedan lyfter vi mindre synpunkter och noteringar som Bankföreningen och dess medlemsföretag har gjort i genomgången av utkastet på föreskrifter. Synpunkterna framfördes inte på mötet den 14 januari.

2 kap. Grundläggande bestämmelser om säkerhetsskydd
§1
Identifiering av säkerhetskänslig verksamhet i övrigt (2kap 1§ 3p.)
Konsekvensnivåer: Vägledning i scenarier för de olika nivåerna är helt avgörande för harmonisering av skyddet mellan aktörer i finansbranschen för att undvika att flytta risk. Nivåerna i matrisen vid klassificering enligt dels 1) PMFS 2019:xx 2 kap 3§ och bilagan om Identifiering och värdering av säkerhetskänslig verksamhet i övrigt i form av anläggningar, objekt eller system (konsekvensnivåer) och, 2) Säkerhetsskyddslagen 2 kap 5§ ang. uppgifters klassificering.)

Angående bilaga till PMFS 2019: xx har Bankföreningen två funderingar:

1. Varför finns fem (5) konsekvensnivåer men bara fyra (4) nivåer för uppgifter i Säkerhetsskyddslagen?
2. Varför är numreringen/skalan för allvarlighet omvänd jämfört med lagen? Det är inkonsekvent och kan skapa onödig svårighet att göra rätt.

§5
1.2 Konsekvensnivåerna är inkonsekventa
Konfidentialitet, riktighet och tillgänglighet är ett nytt fokusområde i den nya lagstiftningen. Tidigare har fokus varit konfidentialitet. Konsekvensnivåerna är beskrivna i föreskriften och inkluderar samtliga tre kriterier. Säkerhetsskyddslagen 2 kap 5§ om säkerhetsskyddsklassificering är formulerad så att endast hänsyn tas till konfidentialitet vad gäller ”uppgifter”. Är syftet att riktighet och tillgänglighet ej skall ha betydelse vid uppgiftsklassificeringen?

§6
Säkerhetspolisen tillhandahåller sektorsspecifika hotbilder till tillsynsmyndigheterna. Bankföreningen ställde en fråga på hearing den 14 januari huruvida skyldighet finns att lämna ut sektorsspecifika hotbilder och hur det sker, med vilken frekvens och vilket format. Om det inte framgår en uttrycklig skyldighet i föreskriften är risken stor att hotbilder inte kommer verksamhetsutövarna tillhanda, vilket är en förutsättning för att kunna göra den övergripande säkerhetsskyddsanalysen, samt för nya verksamheter, anläggningar, system och därmed skydda det skyddsvärda mot antagonistiskt hot. Vi fick inget uttömmande svar på den frågan. Vi anser att sektorsspecifika hotbilder skapar mest praktisk nytta för berörda verksamhetsutövare (bankerna) snarare än tillsynsmyndigheterna (i bankernas fall Finansinspektionen). För att uppnå syftet med säkerhetsskyddsföreskrifterna är det angeläget att de sektorsspecifika hotbilderna delas med både tillsynsmyndigheten och bankerna.

Sektorsspecifik hotbild skall tillhandahållas av SÄPO och DHB upprättas av SÄPO tillsammans med tillsynsmyndigheter enl. 2 kap 6–7§. När och på vilket sätt över tid får aktörerna del av detta? Det är en grundläggande input för säkerhetsskyddsanalysen. Hur hanteras de personer som redan nu behöver registerkontrolleras för att kunna 1, ta del av SÄPO:s hotbildsanalyser och 2, påbörja arbetet med säkerhetsskyddsanalysen. Hur ser processen ut från den 1 april?

<u>3 kap. Behandling av säkerhetsskyddsklassificerade uppgifter och handlingar</u>
§26
Förslag: radera ordet ”varken” så blir paragrafen förmodligen rättvisande.

<u>4 kap. Informationssäkerhet i informationssystem</u>
§13 och §15
§13 och §15 är överlappande. Överväg att slå ihop dem till en paragraf.

§28 och §29
§28 och §29 är överlappande. Överväg att slå ihop dem till en paragraf.

<u>6 kap. Personalsäkerhet</u>
§15 Angående avslutande säkerhetssamtal
Säkerhetspolisen får gärna förklara varför verksamhetsutövare ska ha avslutande säkerhetssamtal med medarbetare som slutar eftersom arbetstagarorganisationer kan ifrågasätta tillvägagångssätt. Samtalet behöver kunna fungera i förhållande till t ex kollektivavtal.

<u>7 kap. Säkerhetsskyddad upphandling med säkerhetsskyddsavtal</u>
§6–7
Verksamhetsutövare kommer inte att på plats kunna kontrollera säkerhetsskydd på alla lokaler eller kontrollera leverantörens ledning och övriga hos leverantören. Krav

kan ställas på att ledning och lokaler ska kontrolleras och genomföras (vilket görs inom ramen för nuvarande säkerhetsskyddslag och relaterade SUA-avtal med underleverantörer) men för globala mjuk- och hårdvaruleverantörer som används för bankernas tjänstedistribution etc. kan det visa sig bli mycket svårt.

Även om det avtalsmässigt skulle vara möjligt skulle det medföra en mängd praktiska problem. Om ett stort antal aktörer ska kontrollera samma byggnad kan risk och sårbarhet snarare öka än minska vilket skulle verka i motsatt riktning med föreskriftens intention. En alternativ riskreducerande åtgärd, eller alternativ skrivning, kan behövas om inte avsikten är att omöjliggöra all outsourcing av säkerhetskänslig information, oaktad nivå på informationen.

SVENSKA BANKFÖRENINGEN

Hans Lindberg Peter Göransson