FI-tillsyn

Bankernas arbete med informations- och cybersäkerhet

Nr 9

7 december 2018

7 december 2018
Dnr 18-18413

INNEHÅLL

FI-tillsyn

Finansinspektionen publicerar återkommande tillsynsrapporter i en numrerad rapportserie. Tillsynsrapporterna är en del av FI:s kommunikation. Rapporterna behandlar genomförda undersökningar och annan tillsyn som FI utför. Genom rapporterna informerar FI om vilka iakttagelser och bedömningar som FI har gjort och om sina förväntningar i olika frågor. Detta kan vara till stöd för företagen i deras verksamhet.

Sammanfattning

Flera banker gör satsningar i arbetet med informations- och cybersäkerhet. Men många har ännu inte fullt ut anpassat sitt arbete till de förändrade förutsättningarna som en ökad digitalisering och ett ökat cyberhot från omvärlden innebär. FI förväntar sig att bankerna fortsatt fokuserar på att utveckla sina förmågor, och att man hanterar och följer upp sina informations- och cybersäkerhetsrisker.

Den finansiella stabiliteten, både nationellt och globalt, är beroende av en fungerande finansiell infrastruktur och banker som stöder och tillhandahåller kritiska funktioner inom finanssektorn. I dag är verksamheten hos finansiella företag helt baserad på it-system. Många it-system har genom åren blivit mer komplexa och sammankopplade, både internt och externt, dels genom integration med andra finansiella aktörer men även genom att verksamhet läggs ut till tredjepartsleverantörer.

Denna förändring pågår samtidigt som antalet aktörer som har resurser och förmåga att genomföra avancerade it-angrepp mot banker ökar, både i Sverige och internationellt. Det är i detta skeende av ständigt förändrade förutsättningar som bankerna behöver hantera informations- och cyberrisker.

Finansinspektionens (FI) tillsyn visar att bankerna har fokus på dessa risker. Tillsynen visar samtidigt på ett antal områden där bankerna kan göra mer. Det kan sammanfattas i följande allmänna rekommendationer till bankernas ledningar:

- Säkerställ att ledningssystemet för informationssäkerhet – organisation, säkerhetshöjande processer, rutiner och kontroller – som beslutats också införs i praktiken och i hela bankens verksamhet.
- Etablera en god förmåga att kontinuerligt analysera och bedöma aktuella cyberhot och vilka aktörer som ligger bakom dessa så att riskhanteringen löpande kan anpassas. Detta arbete kan stärkas genom att förbättra och utöka formerna för samverkan och informationsdelning mellan bankerna och andra intressenter.
- Prioritera utbildning av personalen för att lyfta medvetandenivån om informations- och cybersäkerhet.

I denna rapport redogör FI för slutsatserna av den tillsyn som genomförts de senaste åren samt FI:s syn på hur detta hör samman med pågående förändringar inom finansmarknaden. Bankernas arbete med informations- och cybersäkerhet kommer att fortsätta vara ett prioriterat område inom FI:s tillsyn. FI kommer löpande att följa upp de brister som noterats och fortsätta genomföra undersökningar på området.

Bakgrund till FI:s tillsyn av informations- och cybersäkerhet

I denna rapport redogör FI för slutsatserna av den tillsyn som genomförts på bankerna under 2017 och 2018 av informations- och cybersäkerhet. FI ger också sin syn på hur detta hör samman med pågående förändringar inom finansmarknaden.

CENTRALA BEGREPP I TILLSYNSRAPPORTEN

Begrepp som cybersäkerhet, cyberhot och cyberrisker används i allt högre grad. FI tar i denna rapport avstamp i den begreppsapparat som Financial Stability Board (FSB) sammanställt i ett cyberlexikon, vars slutversion publicerades i november 2018[1].

Cybersäkerhet definieras där som bevarande av konfidentialitet och riktighet hos, samt tillgänglighet till, information och/eller informationssystem i cyberrymden. En cyberincident är en händelse som äventyrar informationssystemens cybersäkerhet eller den information som de hanterar, lagrar eller sänder. Med cyberrisk menas sannolikheten för, och konsekvensen av, en cyberincident sammantaget. Slutligen fastslås cyberhot vara en omständighet med potential att utnyttja en eller flera sårbarheter som påverkar cybersäkerheten negativt.

Begreppet informationssäkerhet följer i denna rapport den definition som ges i Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:5) om informationssäkerhet, it-verksamhet och insättnings-system. Det vill säga: skydd av konfidentialitet, riktighet och tillgänglighet hos information.

Ledningssystem för informationssäkerhet är ytterligare ett centralt begrepp i rapporten och syftar till att upprätta, införa, driva, övervaka, granska, underhålla och utveckla företagets informationssäkerhet. Kraven på ledningssystemet beskrivs närmare i 2 kap. i Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:5) om informationssäkerhet, it-verksamhet och insättningssystem.

UTVECKLINGEN I OMVÄRLDEN

Risken för cyberattacker – där externa eller interna aktörer utför angrepp mot bankerna och deras kunder via internet för att sabotera finansiella tjänster, stjäla, manipulera eller sprida känslig information – har ökat. Det finns flera aktörer som är resursstarka och kapabla att genomföra avancerade it-angrepp i Sverige och internationellt. En rad allvarliga angrepp har skett globalt de senaste åren och detta har fortsatt under 2018.

Ett större angrepp mot it-systemen i den svenska banksektorn kan få omfattande konsekvenser för konsumenter och företag. Exempelvis kan information om kunder och deras engagemang hos banker raderas eller förvanskas. Viktiga tjänster kan också bli otillgängliga för kunder och marknaden. Ett sådant scenario kan allvarligt skada förtroendet

1 FSB Cyber Lexicon, se http://www.fsb.org/2018/11/cyber-lexicon/

för det finansiella systemet och i värsta fall orsaka problem som hotar den finansiella stabiliteten.

Till detta kommer en omvandling inom sektorn där innovation och utveckling utmanar de etablerade bankernas befintliga tjänster. Bankerna själva satsar på egen utveckling av innovativa tjänster och digitala kanaler samtidigt som de genomför ett omfattande utvecklingsarbete för att anpassa sig till befintliga och nya regelverk. Allt detta leder till en ökad nivå av komplexitet i en redan komplex it-miljö, där nya lösningar tillkommer samtidigt som det finns behov av att byta ut gammal teknik.

Sammantaget kan FI konstatera att cyberhoten i kombination med att bankerna arbetar under ett högt förändringstryck, ökar risken för it-avbrott i affärskritiska system.

REGLER OCH STANDARDER INOM INFORMATIONS- OCH CYBERSÄKERHET

De krav på informations- och cybersäkerhet som ställs på banker utgår från de regler om riskhantering som beskrivs i 6 kap. 2 § lagen (2004:297) om bank och finansieringsrörelse.

Till det kommer de föreskrifter och allmänna råd som FI utfärdat:

- Föreskrifter och allmänna råd (FFFS 2014:1) om styrning, riskhantering och kontroll i kreditinstitut
- Föreskrifter och allmänna råd (FFFS 2014:4) om hantering av operativa risker
- Föreskrifter och allmänna råd (FFFS 2014:5) om informationssäkerhet, it-verksamhet och insättningssystem.

FI valde att beakta den svenska standarden ”Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Krav (ISO/IEC 27001:2006, IDT)” i samband med att kraven på informationssäkerhet utformades i föreskrifterna.

FI ser positivt på att bankerna till stor del också baserar sitt arbete med informations- och cybersäkerhet på standarder som de som ingår i ISO 27000-serien, The ISF Standard of Good Practice for Information Security och NIST Cybersecurity Framework.

Bland internationella branschorganisationer och tillsynsmyndigheter inom den finansiella sektorn pågår ett allt intensivare arbete med informations- och cyberrelaterade risker. Inventeringar av befintliga regelverk och sammanställningar av riktlinjer och principer görs av flera organisationer[2] och arbetsgrupper som ägnar sig åt it- och cyberrisker. Tanken är att på lång sikt nå fram till en mer enhetlig reglering och tillsynspraxis i en allt mer sammanlänkad finansiell marknad.

2 Bl.a. Committee on Payments and Market Infrastructures, International Organisation of Securities Commissions (CPMI-IOSCO), Financial Stability Board (FSB), Group of 7 (G7), International Monetary Fund (IMF), Organisation for Economic Co-operation and Development (OECD) , World Bank, European Systemic Cyber Group (ESRB-ESCG), European Bank Authority (EBA), Basel Committee on Banking Supervision (BCBS)

Iakttagelser från tillsynen

I detta kapitel beskrivs ett antal viktiga delområden med de förväntningar som finns på informations- och cybersäkerhet och de iakttagelser som FI gjort i tillsynen. Beskrivningen av vad bankerna förväntas leva upp till, i form av processer och kontroller, baseras på FI:s föreskrifter och internationella standarder[3]. Beskrivningen är dock endast ett urval och ger inte en fullständig bild av alla krav. Bankerna behöver också ta hänsyn till sin storlek samt verksamhetens art, omfattning och komplexitet i arbetet för en tillräckligt god informations- och cybersäkerhet.

STYRNING, RISKHANTERING OCH KONTROLL

Styrning av informations- och cybersäkerhet har som mål att säkerställa att informations- och cybersäkerhetsrisker analyseras och hanteras i bankens affärs- och riskhanteringsprocesser, för att uppnå affärsmålen inom ramen för bankens riskaptit.

Ledningssystem för informationssäkerhet

Ett metodiskt och strukturerat arbete med informationssäkerhet förutsätter ett klart och tydligt etablerat ansvar och ägarskap. Den som utsetts som ansvarig för att leda och koordinera informations-säkerhetsarbetet behöver ha tillräckliga resurser och befogenheter samt ett tydligt formulerat ansvar. Personen bör också ha en tillräcklig senioritet och en position på tillräckligt hög nivå i bankens organisation för att på ett effektivt sätt kunna vidta åtgärder och fatta nödvändiga beslut.

FI föreskriver att bankerna ska genomföra arbetet genom att använda sig av ett ledningssystem för informationssäkerhet. Ledningssystemet ska borga för att det finns ett dokumenterat mål och en inriktning för informationssäkerhet, rutiner för hur banken identifierar och hanterar sina informations- och cybersäkerhetsrisker samt hur informationssäkerhetsarbetet ska följas upp, granskas och förbättras. I förlängningen är det viktigt att bankernas planer för informations- och cybersäkerhet är beslutade och tidsatta samt att de beskriver de säkerhetshöjande åtgärder som ska genomföras.

Organisation och ansvarsfördelning

Inom informations- och cybersäkerhetsområdet är det viktigt att roller och ansvar är tydliga och att organisationen har de befogenheter, kompetenser och personalresurser som krävs för riskhanteringen. Här anser FI att det är viktigt att bankernas styrelser och ledningar engagerar sig och bidrar till att skapa och upprätthålla en hög medvetenhet om dessa frågor.

FI ser positivt på att flera banker har inrättat en centralt placerad grupp av informationssäkerhetsspecialister med operativt ansvar för hotbildsanalyser och hantering av säkerhetsincidenter. Eftersom dessa

3 Bl.a. Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut (FFFS 2014:1), om hantering av operativa risker (FFFS 2014:4) och om informationssäkerhet, it-verksamhet och insättningssystem (FFFS 2014:5) samt NIST Cybersecurity Framework och ISO 27000-serien.

individer ofta hanterar mycket känslig information bör en utökad säkerhetskontroll göras när de anställs eller när konsulter anlitas. Vidare är det viktigt att både informationssäkerhetsspecialister och övrig personal får tillgång till regelbunden och relevant utbildning inom området och att aktiviteter genomförs för att höja medvetandet om dessa frågor.

Riskanalys
Ytterligare en viktig faktor i styrning av informations- och cybersäkerhet är att risker analyseras årligen och vid förändringar som kan påverka informationssäkerheten, samt att analysen omfattar såväl människor och processer som teknik. Ett tydligt exempel där risker kopplade till informations- och cybersäkerhet alltid bör beaktas är i samband med uppdragsavtal när verksamhet läggs ut på en utomstående part, liksom vid kontinuerlig riskhantering av redan ingångna avtal om utlagd verksamhet. Detsamma gäller angränsande områden som kontinuitetshantering och processen för godkännande[4].

Kontrollfunktionerna
Informations- och cybersäkerhetsrisker bör hanteras som en integrerad del av bankernas ramverk för riskhantering. Det innebär att bankens funktioner för riskkontroll och regelefterlevnad ska ha tillräckliga resurser och relevant kompetens samt arbeta på ett aktivt och oberoende sätt för att övervaka och kontrollera hanteringen av informations- och cybersäkerhetsrisker i verksamheten. Funktionen för riskkontroll bör, i samråd med verksamheten, etablera lämpliga mätetal och tröskelnivåer för bankens informations- och cybersäkerhetsrisker samt säkerställa att dessa risker är inkluderade i bankens riskaptit.

Bankens funktion för internrevision har också en viktig roll att fylla. Den ska genomföra oberoende granskningar och bör bedöma och rapportera till bankens styrelse och ledning om hur ledningssystemet för informationssäkerhet är utformat och efterföljs.

Erfarenheter från tillsynen av styrning, riskhantering och kontroll
En slutsats FI drar av tillsynen är att bankerna behöver förbättra sin styrning, kontroll och organisation ytterligare. Det handlar om att öka förståelsen hos ledningen och att sätta av mer tid där för att diskutera och fatta välgrundade beslut om bankens ledningssystem för informationssäkerhet.

Det finns också utrymme för funktionen för riskkontroll att ta en tydligare roll i att rapportera väsentliga brister och risker samt avvikelser mot tröskelvärden för informations- och cyberrisker. Detta ger förutsättningar för ledningen och styrelsen att bättre kunna förstå omfattningen av dessa risker. Det förutsätter rimligen i sin tur att funktionen för riskkontroll har resurser med relevant it- och informationssäkerhetskompetens.

4 Kraven på kontinuitetshantering och processen för godkännande beskrivs närmare i FI:s föreskrifter och allmänna råd (FFFS 2014:4) om hantering av operativa risker.

Flera typer av attacker utnyttjar den mänskliga faktorn (phishing[5], vishing[6], social engineering[7]). Detta drabbar även banker och deras kunder. Även här finns en förbättringspotential i bankernas riskhantering. Det gäller att åstadkomma en bättre struktur och uppföljning av utbildningen av personalen. Det skulle öka medvetandet om informations- och cybersäkerhet och vilket ansvar varje enskild medarbetare har i skyddet av bankens information och tjänster.

Cyberattacker som lett till driftstörningar och incidenter och som uppmärksammats i media har i vissa fall kunnat spåras till brister i den interna kontrollen. Avvikelser från företagens interna styrdokument, etablerade processer och arbetsrutiner samt kända brister som inte åtgärdats leder till sårbarheter som utnyttjats av hotaktörer. Med en mer aktiv styrning, kontroll och uppföljning hade många incidenter sannolikt kunna förebyggas.

Tillsynen har också visat att det saknas tillräckligt med personalresurser med informations- och cybersäkerhetskompetens i funktionerna för riskkontroll och regelefterlevnad. Dessutom utför internrevisionen generellt sett för få revisioner av hur arbetet med informations- och cybersäkerhetsrisker hanteras av funktionerna för riskkontroll och regelefterlevnad.

KUNSKAP OM DEN EGNA VERKSAMHETEN OCH CYBERHOT

Banker bör ha en strukturerad och uppdaterad kunskapsdatabas över användare, enheter, it-system och deras inbördes beroenden. Det behövs bland annat för att kunna identifiera verksamhetens mest kritiska tillgångar som kräver ytterligare skydd, till exempel de som lagrar, överför eller behandlar känslig kund- eller affärsinformation men också andra tillgångar som kan vara ett mål för cyberattacker.

Dessutom bör bankerna ha realtidsövervakning och analysera säkerhetshändelser för att kunna identifiera potentiella cyberattacker. Detta kan också skapa bättre förutsättningar för att dela informationen så att hela sektorn kan lära sig av säkerhetsrelaterade händelser. FI rekommenderar bankerna att både delta i samarbeten för operativ informationsdelning om cyberhot och sårbarheter och att löpande ta del av information från öppna källor.

FI har i sin tillsyn sett att bankerna ofta har en fragmenterad kunskapsbas över användare, enheter, applikationer och deras relationer. Dock har flera banker pågående projekt som syftar till att samla informationen i ett för detta ändamål avsett it-system.

SÄKER SYSTEMUTVECKLING OCH KONTINUERLIGA SÄKERHETSUPPDATERINGAR

För att säkerställa att banken är skyddad mot kända säkerhetsbrister i programvaror behöver den följa en framtagen process för att ta emot,

5 Phishing, lösenordsfiske, är en form av social manipulation och en olaglig metod att lura innehavare av bankkonton och andra elektroniska resurser att delge kreditkortsnummer, lösenord eller annan känslig information via internet (epost).

6 Vishing, sociala manipulation med samma syfte som Phishing beskrivet ovan, via telefon.

7 Social engineering är inom informationssäkerhet metoder för att manipulera personer till att utföra handlingar eller avslöja konfidentiell information.

testa och distribuera säkerhetsuppdateringar i rätt tid, baserat på hur kritisk en uppdatering är. Säkerhetsuppdateringar ska verifieras och justeras vid eventuella fel. Automatiska säkerhetsuppdateringar kan underlätta för att säkerställa att it-system och nätverkskomponenter uppdateras i tid. Bankerna bör också ta hänsyn till och hantera eventuella cyberrisker som uppstår när de använder programvara som inte stöds längre.

Processer för säker systemutveckling och programmering, samt metoder för att testa säkerheten ska användas när en bank utvecklar programvara. Syftet med detta är att säkerheten ska verifieras inom ramen för bankens systemutvecklingsprocess, inklusive agila systemutvecklingsmetoder.

FI har i sin tillsyn observerat att flera banker har pågående projekt för att förbättra sina processer för hantering av säkerhetsuppdateringar, ofta för att öka automatiseringen. I skiftet mellan traditionella systemutvecklingsmetoder och agila metoder har skilda angreppssätt för verifiering av säkerhet i mjukvara observerats. Hos flera banker pågår det arbete för att förbättra processerna för säker systemutveckling.

IDENTITETS- OCH BEHÖRIGHETSHANTERING

Identitets- och behörighetshantering syftar ytterst till att göra det möjligt för rätt personer att få tillgång till rätt information och it-system vid rätt tidpunkt och av de rätta skälen.

Det bör utses ett tydligt ägarskap för identitets- och behörighets-processer. Processägaren bör ha mandat att ställa krav på dessa processer och få rätt förutsättningar för att kunna se till att de införs och efterlevs.

Det är viktigt att definiera strukturerade processer och kontroller som hanterar användarnas identiteter och behörigheter genom en identitets alla faser i en livscykel. En sådan livscykel infattar ofta hur identiteter till nätverk och it-system skapas, hur behörigheter tilldelas, hur de ska ändras vid behov och hur de tas bort, till exempel när personal slutar.

Det är också viktigt att regelbundet följa upp och kontrollera befintliga behörigheter samt att eventuella avvikelser som upptäcks i uppföljningen åtgärdas.

Inom identitets- och behörighetsområdet är hanteringen av höga behörigheter speciellt viktig. Med höga behörigheter menas här användare som har fullständiga behörigheter eller nära fullständiga behörigheter till kritiska it-system eller infrastrukturkomponenter. Det innebär att de exempelvis kan ändra och ta bort information direkt i it-produktionssystemen.

När bankerna utformar processer och kontroller för hantering av höga behörigheter behöver de bland annat beakta

- hur behörigheterna kan begränsas så långt som möjligt
- om stark autentisering[8] bör införas
- hur separering av otillåtna kombinationer av behörigheter ska kontrolleras
- hur övervakning och uppföljning av nyttjandet av behörigheterna ska gå till för att säkerställa spårbarhet.

Många av de incidenter och cyberattacker som uppmärksammats globalt de senaste åren har visat på brister i behörighetshantering och att höga behörigheter som inte skyddats av stark autentisering tagits över och använts vid attacker.

En iakttagelse FI gjort i sin tillsyn är att hanteringen av identiteter och behörigheter ofta är en utmaning för framför allt de banker som har en omfattande systemflora, komplexa systemsamband och flera användare som byter arbetsuppgifter inom företaget. På samma sätt har tillsynen visat att det är en utmaning att kartlägga och därmed få en komplett bild över vilka höga behörigheter som behöver hanteras.

Ytterligare en erfarenhet från tillsynen är att det är en utmaning att införa de strukturerade processer och kontroller som tagits fram. Införandeprojekten är ofta försenade. Det är därför viktigt att införandet ges ett tydligt mandat, de resurser och befogenheter som krävs samt fullt stöd från ledningen.

FI:s krav på interna regler för behörighetshantering beskrivs i 2 kap. 8 § i Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:5) om informationssäkerhet, it-verksamhet och insättningssystem.

SÄKERHETSÅTGÄRDER I IT-SYSTEM OCH NÄTVERK

Skydd av information och data

Banker hanterar stora mängder information i sin verksamhet, exempelvis om kunder, transaktioner och interna affärsförhållanden. För att kunna skydda informationen från obehörig åtkomst eller stöld finns det ett antal åtgärder att ta i beaktande. Det kan handla om att övervaka data som lämnar företagets nätverk och att kryptera data som transporteras i nätverket och lagras i servrar, datorer och olika mobila enheter. Rutiner ska också finnas för säkerhetskopiering och test av återläsning av säkerhetskopierad data. Ytterligare behöver företagen ha rutiner för hur uttjänade lagringsmedier, som till exempel hårddiskar, ska förstöras på ett tillräckligt säkert sätt.

Nätverkssegmentering

För att skydda information och it-system i det interna nätverket – inklusive eventuella trådlösa nätverk – från obehörig åtkomst är det viktigt att utforma nätverket utifrån kraven på informationssäkerhet. Detta kan bland annat ske genom att etablera nätverkszoner. En fungerande nätverkszonsarkitektur begränsar riskerna för obehörig

8 Stark autentisering, ofta multifaktorautentisering (MFA) är en metod för åtkomstkontroll där användare endast beviljas åtkomst efter att framgångsrikt ha presenterat flera separata bevis för en autentiseringsmekanism – vanligtvis inom minst två av följande tre kategorier: kunskap (något de vet), innehav (något de har) och inneboende (något de är).

åtkomst och bidrar också till att begränsa konsekvenserna av en cyberattack genom att zoner under angrepp kan isoleras från resten av nätverket.

Den slutsats som FI drar från tillsynen är att bankerna aktivt arbetar med nätverkssegmentering men att de behöver färdigställa åtgärderna.

Säker konfiguration av hård- och mjukvara
Hård- och mjukvara som bankerna använder i it-verksamheten levereras ofta standardkonfigurerade och anpassas därefter till bankernas specifika säkerhetskrav. Därför är det viktigt att upprätta en standard för säkerhetskonfiguration som exempelvis reglerar vilka tjänster och nätverksportar som tillåts vara öppna samt hur autentisering ska utformas.

Det är viktigt att löpande uppdatera sådana standardkonfigurationer i takt med att nya hot och sårbarheter identifieras. Rutiner för att säkerställa att alla relevanta it-system och nätverkskomponenter har den godkända standardkonfigurationen installerad bör införas.

Skydd av nätverk från externa hot
Riskerna ökar för direkta intrång i bankernas it-system och infrastruktur där målet är att orsaka driftsavbrott, förstöra information eller förbereda för bedrägerier. Överbelastningsattacker mot bankernas internetkanaler förekommer också. Det är viktigt att på ett tillräckligt sätt skydda det interna nätverket från externa hot. De typiska skyddsåtgärderna innefattar brandväggar, system för upptäckt av intrång (IDS), förhindrande av intrång (IPS) samt skydd mot skadlig programvara och kod (anti-virus).

Även inom detta område är det tydligt att bankerna arbetar aktivt med frågorna, men att de behöver slutföra åtgärderna.

INCIDENTHANTERING

Det framgår av Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:4) om hantering av operativa risker att ett företag ska ha interna regler för att hantera de incidenter som uppstår i verksamheten. Kravet gäller också informations- och cybersäkerhetsrelaterade incidenter. För att direkt kunna ingripa mot informations- och cybersäkerhetsrelaterade incidenter är det viktigt att roller och ansvar för den operativa hanteringen av incidenter är bestämda i förväg.

Principer för att hantera och fatta beslut om åtgärder bör finnas på plats, liksom interna och externa kommunikationsplaner. Innan incidenthanteringen avslutas är det viktigt att säkerställa att återställningen av it-system och data är fullständig. Den efterföljande incidentutredningen bör inbegripa en analys av orsaken till incidenten. Händelseförloppet under incidenten bör också dokumenteras. Handlingsplaner bör upprättas för att åtgärda de brister som låg till grund för incidenten.

TESTER

Av Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:5) om informationssäkerhet, it-verksamhet och insättningssystem framgår att ett företag ska klassificera sin information för att den ska få rätt skyddsnivå. Klassificeringen ska utgå från de krav som ställs på

informationens konfidentialitet, riktighet och tillgänglighet i verksamheten. De interna reglerna bör ange krav på regelbunden kontroll av företagets it-system mot den fastställda skyddsnivån för informationen.

För att genomföra den regelbundna kontrollen finns det ett antal olika angreppssätt, exempelvis:

- regelbundna automatiska genomsökningar av it-system och it-infrastruktur efter kända sårbarheter
- regelbundna penetrationstester av det yttre nätverksskyddet – testerna kan också göras i samband med att förändringar har genomförts i it-system i företagets internetkanaler, exempelvis internetbanken
- avancerade penetrationstester där specifik hotbildsinformation används för att utforma testet och där personalen som utför testerna är oberoende från den funktion som testas.

Banker bör anta en riskbaserad ansats när de väljer i vilken omfattning och hur ofta testerna ska genomföras. I detta sammanhang bör man beakta att avancerade penetrationstester av specifika hotbilder är ett relativt omfattande och resurskrävande sätt att testa skyddsnivån. De passar bäst för företag som har kommit längre i sitt arbete med informations- och cybersäkerhet. Företag med kritiska internetkanaler bör prioritera regelbundna penetrationstester av dessa samt regelbundna automatiska genomsökningar av it-system och it-infrastruktur efter kända sårbarheter.

Slutsatser

FI konstaterar att bankerna gör väsentliga satsningar och investeringar inom informations- och cybersäkerhetsområdet. Samtidigt har flera banker ännu inte fullt ut anpassat sitt informationssäkerhetsarbete till de förändrade förutsättningar som en ökad digitalisering och ett ökat cyberhot från omvärlden innebär.

ARBETET MED ATT INFÖRA LEDNINGSYSTEM FÖR INFORMATIONSSÄKERHET

Baserat på den information som framkommit i tillsynen bedömer FI att bankerna generellt kommit långt i att utveckla sina ledningssystem för informationssäkerhet. Genomgående behöver dock engagemanget hos bankernas ledningar öka när det gäller att kontrollera, och vid behov vidta lämpliga åtgärder, i samband med att ledningssystemet införs i bankens alla områden.

I det här arbetet finns en förväntan från FI på funktionerna för riskkontroll och regelefterlevnad att ta en tydligare roll i att övervaka och kontrollera införandet av ledningssystemet i verksamheten. Hos flera banker kräver det sannolikt ökade personalresurser med it- och informationssäkerhetskompetens i dessa funktioner. Internrevisionen kan bidra med granskningar av hur informations- och cybersäkerhetsarbetet hanteras av funktionerna.

KONTINUERLIG RISKANALYS

FI:s tillsyn visar att det finns utmaningar när det gäller att nå hela vägen fram med att genomföra kontinuerliga riskanalyser och bedömningar av aktuella cyberhot som omfattar bankens väsentliga processer. Detta trots att de flesta banker har upprättat både generella och informationssäkerhetsspecifika riskidentifieringsprocesser.

FI vill uppmärksamma bankerna på att det är viktigt att de har processer på plats där det ingår att säkerställa att cyberrisker kontinuerligt analyseras och hanteras för bankens alla väsentliga processer.

ÖKAD MÅLMEDVETENHET

Cyberattacker som lett till driftstörningar och incidenter och som uppmärksammats i media har i vissa fall kunnat spåras till brister i den interna kontrollen. Även den mänskliga faktorn spelar in här. Erfarenheter från tillsynen indikerar att effekterna av denna typ av störningar kan minskas genom att se till att de processer och arbetsrutiner som bankerna har tagit fram införs fullt ut.

En ökad målmedvetenhet och en mer aktiv styrning, kontroll och uppföljning för att säkerställa att bankens alla områden efterlever etablerade processer kan sannolikt förebygga många incidenter och – när incidenter ändå inträffar – minimera konsekvenserna och korta ledtiderna för att återgå till normal verksamhet.

I det sammanhanget är identitets- och behörighetshantering samt kunskapsbasen över användare, enheter, applikationer och deras relationer avgörande. FI har observerat att införandet och hanteringen

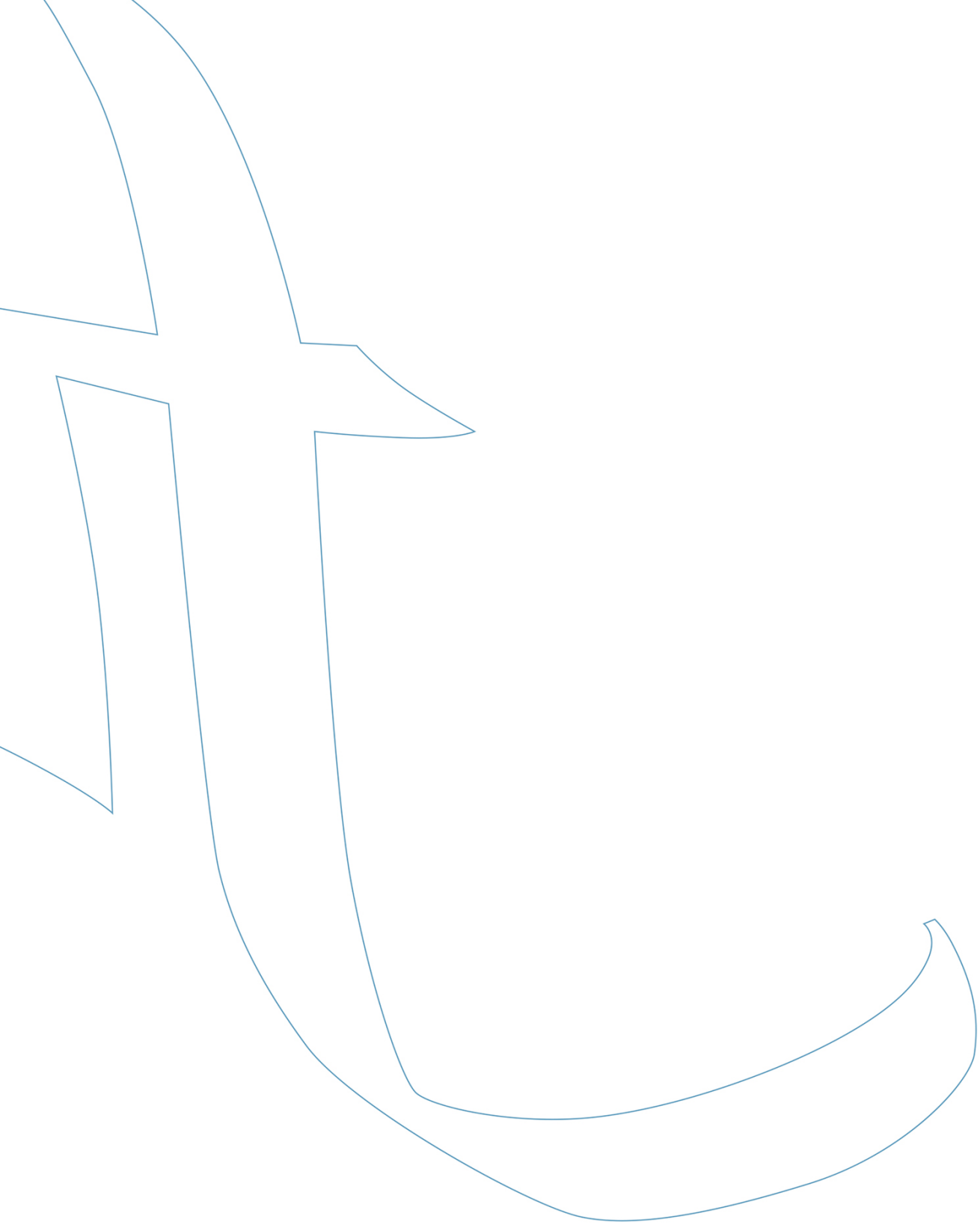
av dessa viktiga processer är fragmenterat och skiljer sig åt mellan bankernas affärsområden. Dessutom bedömer FI att det finns en stor potential i utbildning av personalen. På så sätt kan medvetandenivån om informations- och cybersäkerhet höjas, vilket kan bidra till att motverka att cyberattacker lyckas och att minska deras konsekvenser när de inträffar.

Ett annat viktigt område är att kontinuerligt testa verksamhetens beredskap och skyddsåtgärder samt i vilken mån incidenthanteringen är anpassad för att hantera cyberattacker.

SAMVERKA INOM SEKTORN BEHÖVER STÄRKAS

Genom att utbyta information om cyberhot och sårbarheter inom en grupp kan bankerna utnyttja samlad kunskap och erfarenheter för att få en mer komplett förståelse av de hot och attacker som förekommer. Företag som tar emot sådan information och använder den för att stävja eller avhjälpa exempelvis en cyberattack kan lindra eller hindra vidare spridning till andra företag.

Informationsutbyte ökar i sin tur möjligheterna för företagen att identifiera cyberattacker som är riktade specifikt mot en grupp företag eller mot den finansiella sektorn som helhet. FI ser därmed positivt på forum för operativ informationsdelning och förbättrade former för samverkan mellan bankerna och andra intressenter inom detta specifika område.



Finansinspektionen
Box 7821, 103 97 Stockholm
Besöksadress Brunnsgatan 3
Telefon +46 8 408 980 00
Fax +48 8 24 13 35
finansinspektionen@fi.se

www.fi.se