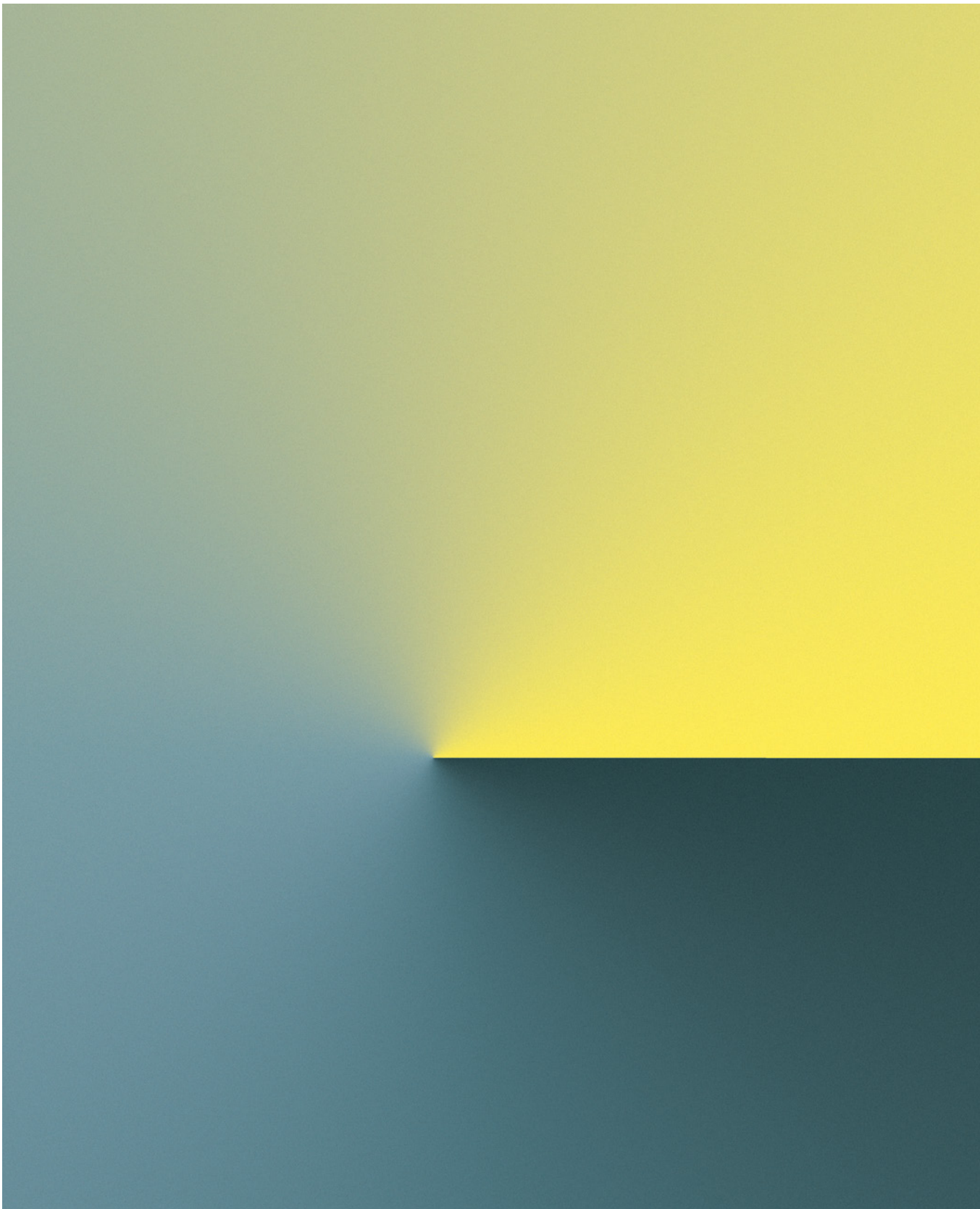
FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

RISIKO- OG SÅRBARHETSANALYSE (ROS)

2014



Risiko- og sårbarhetsanalyse (ROS) 2014

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

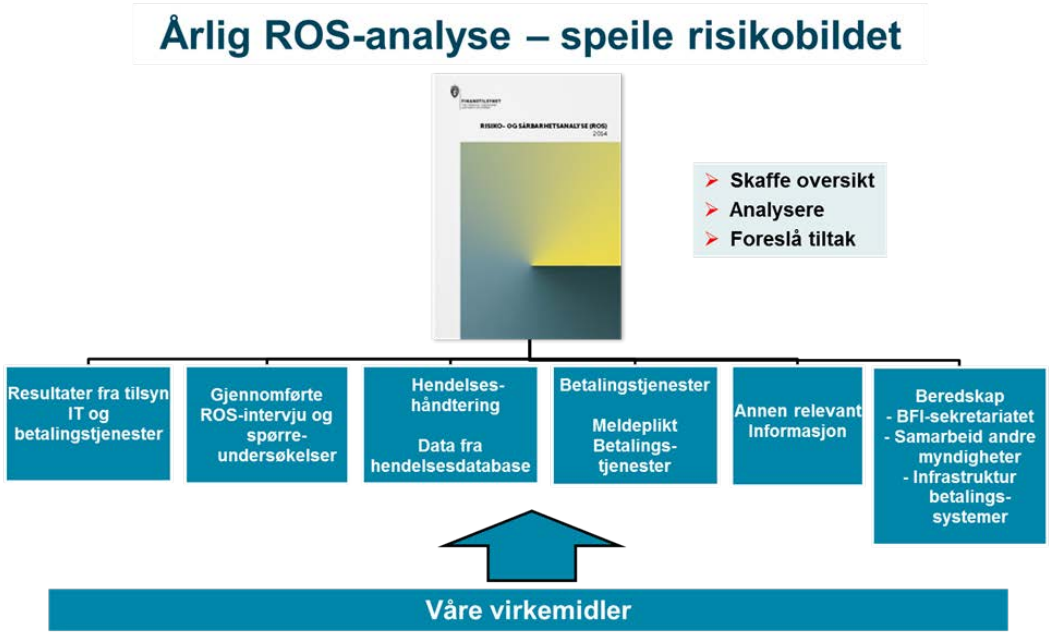
Finanstilsynet, 8. april 2015

INNHOLD

1 Innledning

Finanstilsynet utarbeider hvert år en risiko- og sårbarhetsanalyse (ROS-analyse) av finanssektorens bruk av IKT og betalingstjenester. Gjennom tilsynsarbeidet har Finanstilsynet en bred kontaktflate med finansforetak, bransjeforeninger, leverandører, standardiseringsorganer og nasjonale og internasjonale myndigheter. Basert på disse kildene gir rapporten en vurdering av hvordan identifiserte risikoer kan få innvirkning på finanssektoren i Norge.

Figur 1



Kilde: Finanstilsynet

Rapporten reflekterer risikoen og sårbarheten både med hensyn til finansiell stabilitet og det enkelte foretak og med hensyn til den enkelte forbruker.

Kjernen i årets rapport er kapittel 3, 4 og 5. Kapittel 3 gir et bilde av funn og observasjoner gjennom Finanstilsynets aktiviteter i 2014. Kapittel 4 refererer finansforetakenes egne vurderinger basert på bruk av et spørreskjema og intervjuer. I tillegg er noen sentrale aktører for sikkerhetsløsninger intervjuet og årsrapporter fra internasjonale sikkerhetsselskaper gjennomgått. Kapittel 5 beskriver utviklingstrekk og trender innenfor eller med relevans for finanssektoren og deres bruk av IKT.

Formålet med den årlige ROS-analysen er å gi et oppdatert bilde av risikoen for finanssektorens bruk av IKT og betalingstjenester. Noen risikoer og sårbarheter har fått gjentakende årlig oppmerksomhet. Omtalte risikoer og sårbarheter har imidlertid ikke vært uttømmende, og det har ikke vært slik at risikoer som ikke er nevnt, er ensbetydende med at Finanstilsynet ikke vurderer disse som viktige for foretakene. I kapittel 6 oppsummeres Finanstilsynets vurdering av risikobildet i 2014. I årets rapport er dette gjort gjennom en faktisk vurdering av risikoen sammen med en vurdering av utviklingstrenden knyttet til de omtalte truslene, sårbarhetene og kontrolltiltakene.

Kapittel 7 beskriver de områdene som Finanstilsynets vil ha særskilt oppmerksomhet på, og bakerst i rapporten er det en ordliste som forklarer ord og begreper.

2 Oppsummering

2.1 Finanstilsynets funn

Foretakene er pålagt å rapportere til Finanstilsynet vesentlige avvik som oppstår i driften av IKT-systemene. Gjennom oppfølging av rapporterte hendelser, funn fra tilsyn og annen oppfølging mot næringen får tilsynet god innsikt i foretakenes bruk av IKT, betalingsløsninger og i aktuelle risikoområder.

Det ble rapportert noen flere hendelser i 2014 enn i 2013, og den positivt synkende trenden de siste årene ble brutt midtveis i året. Gjennom året var det noen alvorlige hendelser som gjaldt integritet og konfidensialitet. Det ble rapportert om få ondsinnede angrep.

Observasjoner viser at foretakene har forbedringspotensial når det gjelder oppfølging og kontroll av tilganger til applikasjoner og data.

Betalingssystemer

Den finansielle stabiliteten er avhengig av velfungerende og tilgjengelige betalingstjenester og -systemer. Svikt i disse, enten det skjer gjennom planlagte ondartede hendelser eller som ikke-planlagte hendelser, kan true stabilitet og kvalitet.

Finanstilsynets vurdering er at betalingstjenestene generelt er stabile og har tilfredsstillende kvalitet, selv om det i 2014 var en økning i alvorlige hendelser, og utilgjengeligheten til betalingssystemet økte og var tilbake på 2011-nivå. Hendelsene i seg selv truet ikke finansiell stabilitet, men det var noen hendelser som, dersom de fikk utvikle seg, kunne skapt uro for den finansielle stabiliteten.

Selv om angrep mot betalingstjenestene inntreffer, er de direkte tapene fortsatt små. Mye av årsaken til de lave tapene skyldes tiltak som enkeltforetak og finanssektoren har iverksatt. Det viktige arbeidet med forebyggende tiltak må fortsette. Det er derfor viktig at styring og kontroll blir prioritert og at tiltak for å sikre samhandling om fellesløsninger og infrastruktur fortsetter.

Tap ved handel med betalingskort der det ikke er krav til PIN-kode ("Card-Not-Present"), øker prosentvis mye og har nær tredoblet seg i løpet av de tre siste årene, men tapene er likevel små sett i internasjonal sammenheng.

Bank

Observasjoner viste at foretak hadde svakheter i sine driftsløsninger ved at det har vært mangler i etablerte løsninger for å sikre kontinuitet. Særlig rammer dette betalingsformidlingen. Det er også observert forbedringspotensial knyttet til katastrofeløsninger.

Ved tilsyn om etterlevelse av forskrift om krav til datasystemer og rapportering til Bankenes sikringsfond ble det konstatert at ikke alle banker hadde etablert løsninger for å rapportere i henhold til forskriftens krav. Informasjonsleveransene viste store kvalitetsmessige variasjoner.

Verdipapirområdet

Helhetsbildet på verdipapirområdet viser både høy stabilitet og god kvalitet innenfor denne sektoren i Norge. Dette understrekes ved at det i 2014 var få hendelser, men noen var alvorlige ettersom de førte til brudd på konfidensialitet.

Det kan være en utfordring å sikre akseptabel risiko på gamle systemer. VPS' kjernesystemer er en av de mest kritiske komponentene i verdipapiromsetningen i Norge. For å sikre fortsatt høy stabilitet og god kvalitet pågår det nå et omfattende prosjekt for å erstatte disse med nye og mer moderne løsninger.

Forsikringsområdet

Forsikringsområdet viser høy stabilitet og god kvalitet. Imidlertid var det i 2014 noen alvorlige hendelser ettersom de førte til brudd på konfidensialitet.

Det ble observert at enkelte forsikringsforetak har et forbedringspotensial knyttet til test av beredskapsløsninger og at de i for liten grad involverer seg i leverandørenes beredskaps- og katastrofetesting.

Forbrukerområdet

Finanstilsynet observerer at utviklingen i digital kriminalitet gjør forbrukerne mer sårbare. Det er derfor viktig at tjenesteleverandører lager sikre og trygge løsninger som er enkle å bruke og forstå, etablerer kvalitetsmessige gode prosesser der tjenester utkontrakteres (som f.eks. ved utlevering av kodebrikker) og er proaktive i sitt arbeid med å formidle kunnskap om tjenester og hvordan forbrukerne skal beskytte seg mot digital kriminalitet.

2.2 Observasjoner fra intervjuer og spørreundersøkelser

Intervjuer og spørreundersøkelse med foretakene viser at de mest fremtredende truslene synes å være at inntrengere får tilgang til IKT-infrastruktur og applikasjoner gjennom målrettede angrep.

Andre trusselområder som representerer betydelig risiko, er økningen i IKT- og cyberkriminalitet, sikkerhetshull i programvare som kan utnyttes av kriminelle, den sterke avhengigheten til Internett, ansattes bruk av sosiale medier og informasjon som kommer på avveie.

Kompleksitet i IKT-løsninger utgjør også en høy risiko for datakvalitet og stabil drift, og kan hindre nyutvikling.

2.3 Utviklingstrekk

Den teknologiske utviklingen og sikring av finansiell stabilitet i finanssektoren medfører et behov for endringer i tjenester, infrastruktur og regelverk innenfor alle deler av sektoren. Samlet representerer endringene en økt risiko. Ny teknologi kan introdusere nye ukjente sårbarheter og gi økt risiko. Særlig innen betalingsformidlingen skjer det store endringer i kampen om det internettbaserte og mobile betalingstjenestemarkedet, og det er en fare for at sikkerhetsløsninger ikke vektlegges tilstrekkelig i konkurransen om markedsandeler.

Økningen i IKT- og internettbasert kriminalitet og det økte trusselbildet som følger med dette for både foretak og forbrukere har ført til en betydelig økt oppmerksomhet på IT-sikkerhet, nasjonalt, internasjonalt og fra myndighetene. Nye aktører som ikke er underlagt norsk lovgivning og opptrer i et grenseløst Internett, skaper utfordringer for kunder, norske finansforetak og myndigheter. Villede hendelser kan også få konsekvenser for finansiell stabilitet. Angrepene blir stadig mer målrettede og sofistikerte, og finansbransjen vil kunne utsettes for angrep av samme karakter som andre næringer har blitt utsatt for, som for eksempel telekombransjen.

Det har skjedd endringer i eierforhold hos viktige tjenesteleverandører til finanssektoren og i foretakenes valg av leverandører. Endringene kan tilføre forbedringer, men de kan også skape nye sårbarheter. Generelt fører endringer til økt operasjonell risiko når samhandlingskonstellasjoner endres. Det er viktig at foretakene har kontroll på sine endringer og risikoer, ettersom endringene samlet kan utgjøre en betydelig risiko for norsk finansiell infrastruktur.

Flere steder i rapporten pekes det på teknologiske utviklingstrekk, som brukt på den rette måten kan bidra til å redusere sårbarhet i de nasjonale betalingssystemene.

2.4 Aktuelle risikoområder fra analysene i 2014

Aktuelle risikoområder er vurdert ut fra kontrollmålene integritet, konfidensialitet, tilgjengelighet og at IT fungerer tilfredsstillende som støtte for forretningsdriften.

Finanstilsynet vurderer at risikoen knyttet til integritet er høy og økende, risikoen knyttet til konfidensialitet er middels og stabil, risikoen knyttet til tilgjengelighet er middels og økende og risikoen knyttet til at IT fungerer tilfredsstillende som støtte for forretningsdriften er middels og stabil.

Finansforetak var under angrep i 2014. Virkningen av angrepene har vært dempet som følge av tiltak fra foretakene. Digitale angrep mot finanssektoren kan føre til at markedene og finansiell stabilitet kan

bli truet.

I likhet med tidligere år ser endringer i systemer og omgivelser ut til å være den hyppigste feilårsaken eller risikodriveren hos foretakene, og de må fortsatt ha særlig oppmerksomhet rettet mot dette området.

Det er krevende for forbrukere å forholde seg til trusler og sårbarheter i finansielle tjenester på en kvalifisert måte, og finansnæringen har et stort ansvar for å bygge inn tilstrekkelig sikkerhet i løsningene.

2.5 Finanstilsynets videre oppfølging

Finanstilsynet vil fortsatt prioritere å ha en nær dialog med viktige aktører i sektoren, både for å sikre forståelse av risikonivået og for å forstå utfordringene som foretakene møter. Det blir lagt vekt på å ha innsyn i foretakenes beredskapsløsninger, foretakenes utkontrakteringer, deres tilgangsstyring og arbeid med IT-sikkerhet. Dette vil hovedsakelig skje gjennom IT-tilsyn.

Finanstilsynet vil legge vekt på å følge opp hendelser, trusselbildet knyttet til digital kriminalitet og å følge med i utviklingen av betalingstjenester. Tilsynet er sekretariat og leder for Beredskapsutvalget for finansiell infrastruktur (BFI), og dette arbeidet vil fortsette.

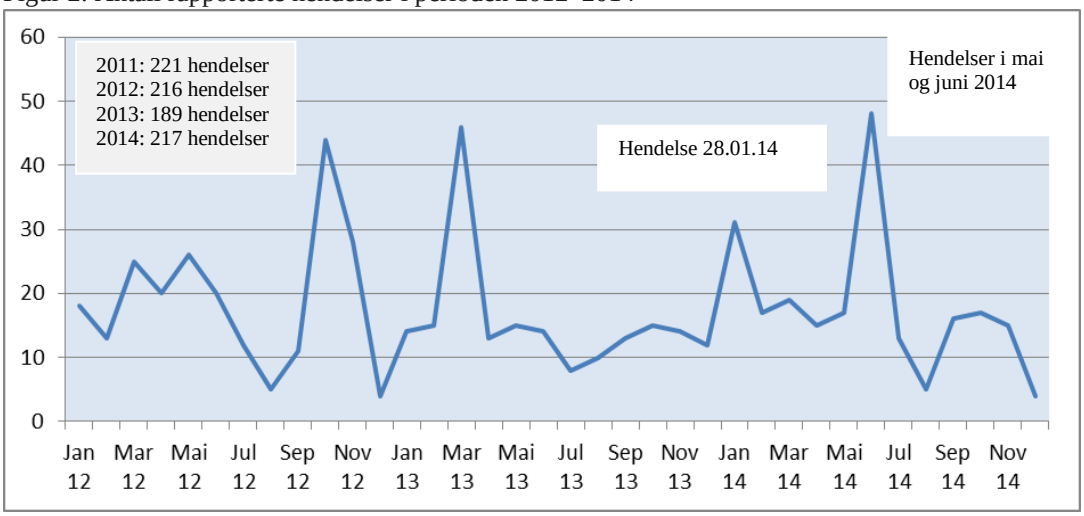
3 Finanstilsynets funn

Dette kapitlet viser funn og observasjoner basert på gjennomførte IT-tilsyn, mottatte hendelsesrapporter og meldinger om nye og endrede betalingstjenester. Videre omtaler det oppfølgingen av IT-prosjekter, utkontrakteringsavtaler og deltakelse i nasjonale og internasjonale arbeidsgrupper og organisasjoner i 2014. Betalingssystemer, verdipapirområdet, bank og forsikring er omtalt i underkapitler.

3.1 Rapporterte hendelser i 2014

Foretakene skal rapportere avvik som medfører vesentlig reduksjon i funksjonalitet som følge av brudd på konfidensialitet (beskyttelse av data), integritet (sikring mot uautoriserte endringer) eller tilgjengelighet til IKT-systemer og/eller data til Finanstilsynet. Rapporteringen skal normalt omfatte hendelser som foretaket selv kategoriserer til alvorlighetsgrad svært alvorlig eller kritisk, men kan også omfatte andre avvik dersom disse avdekker spesielle sårbarheter i applikasjon, arkitektur, infrastruktur eller forsvarsverk.

Figur 2: Antall rapporterte hendelser i perioden 2012–2014



Kilde: Finanstilsynet

Antall rapporterte hendelser i 2014 var omtrent på nivå med årene før. Med unntak av en alvorlig driftshendelse som rammet mange banker i januar, fortsatte den positive utviklingen fra 2013 i første

halvdel av 2014 med færre driftshendelser enn årene før. I mai og juni var det flere driftshendelser med få dagers mellomrom. Disse hendelsene rammet mange banker. Gjennom året var det noen alvorlige hendelser som gjaldt integritet og konfidensialitet. Det var få rapporter om ondsinnede angrep.

Finanstilsynet etablerte i 2014 en rutine for å varsle Finansdepartementet om særlig alvorlige hendelser, eller hendelser som kan få stor mediedekning. Finansdepartementet ble varslet om ni hendelser i 2014.

3.1.1 Driftshendelser som rammet mange banker

Det er særlig på to områder at driftsmiljøet er sårbart med vidtgående konsekvenser ved feilsituasjoner, og det er nettverk og sentrale systemer. Særlig er nettverket sårbart, noe som ble vist gjennom hendelser i 2013 og 2014. Da ble en rekke banker rammet samtidig av samme hendelse i nettverket. Ytterligere separasjon av nettverket kan være et tiltak for å sikre at etablerte kontinuitetsløsninger virker som de skal.

3.1.2 Driftshendelser som rammet enkeltbanker

Det var noen alvorlige hendelser som rammet enkeltforetak i 2014. Svikt i strømforsyningen i en datahall førte til nedetid og forsinkelser i kjøremønsteret i flere dager. Det fikk konsekvenser for tjenestene rettet mot publikum. En driftshendelse 17. februar gjorde denne bankens publikumstjenester mer eller mindre utilgjengelige denne dagen. I oktober rammet en ny hendelse kunder med VISA-kort. Samme transaksjoner ble belastet to dager på rad. Ved den planlagte reverseringen påfølgende natt ble transaksjonen feilaktig belastet en tredje gang.

Det var også alvorlige enkelthendelser ved flytting av systemer og/eller drift til ny tjenesteleverandør, hvorav noen fikk betydelige kundekonsekvenser som blant annet manglende tilgang til nettbank for gjennomføring av betalinger.

Hendelser i 2014 avdekket også svakheter ved oppsettet for kontinuitets- og katastrofeløsninger. Det er viktig at terskelen for å sette i gang katastrofeløsningen ikke blir så høy at den i realiteten ikke representerer et alternativ.

Finanstilsynet hadde særskilt oppfølging av totalt ni alvorlige hendelser i løpet av 2014.

3.1.3 Hendelser med konfidensialitetsbrudd

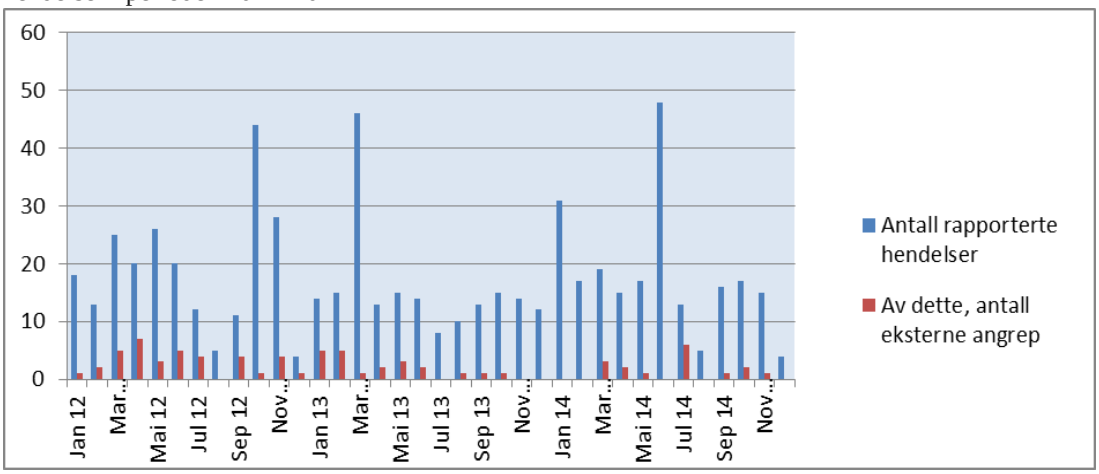
Hvert år er det en betydelig andel hendelser som gjelder konfidensialitetsbrudd. Etter endringer i nettbankløsningene er sesjonshåndteringen et gjentakende problem. Kunder har under gitte omstendigheter kunnet komme inn på en annen kundes engasjementer. Det kan ta lang tid før banken blir oppmerksom på problemet, og det er vanskelig å kartlegge hvor mange og hvem som er blitt eksponert. Det er en risiko for at den eksponerte kundeinformasjonen kan være grunnlag for svindelforsøk. Finanstilsynet etterlyser bedre applikasjonstesting når det gjelder sesjonshåndtering.

Konfidensialitetsbrudd er det som oftest utløser rapportering fra verdipapirforetak og forsikringsselskaper.

3.1.4 Få ondsinnede angrep

Finanstilsynet mottok få rapporter om ondsinnede angrep i 2014. Mest oppmerksomhet fikk DDoS-angrepet 8. juli. Angrepet rammet en del norske banker sammen med andre typer bedrifter, men ble effektivt håndtert og raskt slått ned. Det ble også rapportert noen flere DDoS-angrep i 2014, og det var fortsatt en del phishing der svindleren ga seg ut for å være en bank. Det ble observert forsøk på å tilegne seg informasjon på innsiden, noe som kan være varsel om planlegging av såkalte Advanced Persistent Threat-lignende angrep (APT).

Figur 3: Antall rapporterte eksterne angrep (ondsinnede angrep) i forhold til totalt antall rapporterte hendelser i perioden 2012–2014



Kilde: Finanstilsynet

3.1.5 Lite rapportering fra andre finansforetak enn banker

Finanstilsynet oppfatter at hendelsesrapporteringen fra bankene er på et relativt tilfredsstillende nivå. Dette gjelder både norske banker og utenlandske banker med filial i Norge. Hendelser som rammer mange banker samtidig, er en indikator på dette. I 2014 mottok Finanstilsynet om lag 20 rapporter fra ulike banker og bankgrupperinger om samme hendelse hos felles leverandør. Selv om utgangshendelsen er den samme, rammes bankene på ulike måter.

I 2014 var 197 av 217 rapporter fra banker. De resterende 20 fordelte seg på verdipapirområdet med 11 rapporter og forsikringsområdet med 9. Dette kan indikere en underrapportering fra de andre typene finansforetak, og på hendelsesseminaret i 2014 la Finanstilsynet vekt på forsikringsselskapenes rapportering av hendelser.

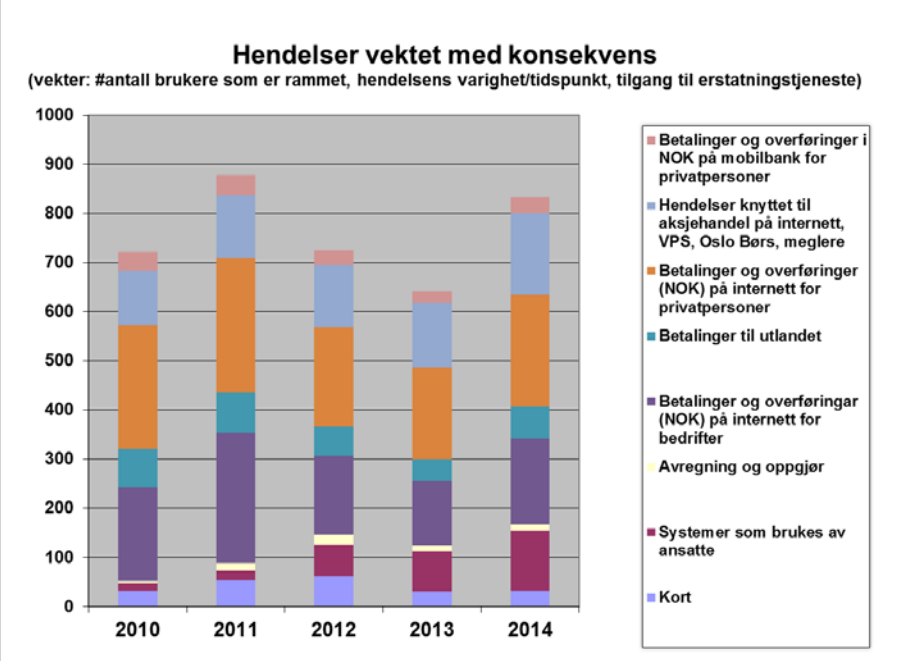
Inkassoselskaper er foreløpig ikke pålagt hendelsesrapportering.

3.1.6 Analyse av hendelsene som mål på tilgjengelighet

For hver hendelse som har rammet tilgjengeligheten, har Finanstilsynet vurdert avbruddets lengde, antall foretak som er berørt, anslagsvis hvor mange kunder som er rammet og om det eksisterer erstatningstjenester som kunden kan benytte. På denne måten får Finanstilsynet en indeks for utilgjengelighet til betalingssystemet år for år, og kan dermed følge utviklingen over tid.

Figur 4 viser at betalingssystemet var mer utilgjengelig for publikum i 2014 enn i 2013. Frem til juni 2014 var det mindre utilgjengelighet enn i tilsvarende periode i 2013, men hendelser i resten av 2014 gjorde at denne positive trenden tilbake til 2012 ble snudd.

Figur 4: Hendelser vektet med konsekvens



Kilde: Finanstilsynet

3.2 Betalingssystemer og utvikling

3.2.1 Generelt om betalingssystemer

Effektive, robuste og stabile betalingssystemer er grunnleggende for finansiell stabilitet og velfungerende markeder. I Norge blir betalingssystemene regulert gjennom lover og forskrifter og gjennom finansnæringens selvregulering, forvaltet av Finans Norge.

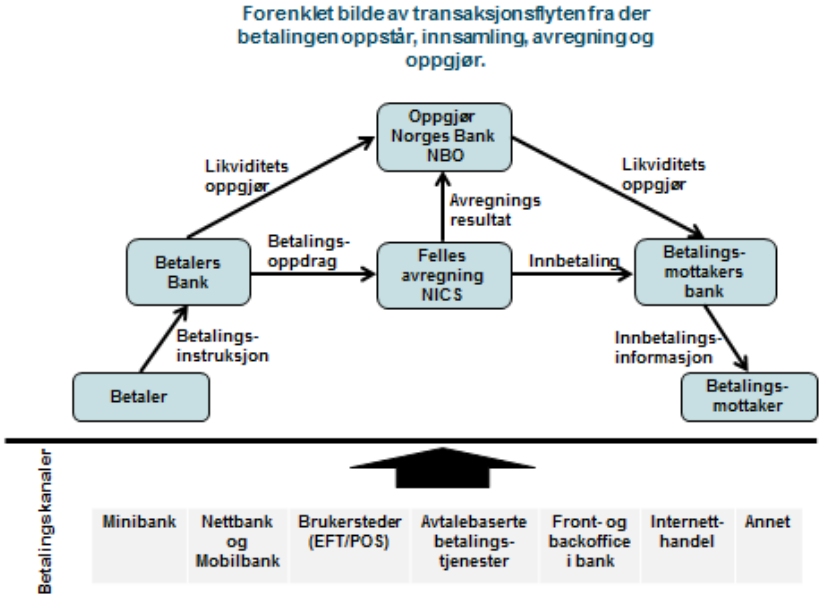
Finansavtaleloven og EUs betalingstjenestedirektiv er etablert som sentrale forsvarsverk for å ivareta forbrukerhensyn og best mulig sikre forbrukernes sikkerhet og rettigheter.

I økende grad blir lover og forskrifter harmonisert i takt med regelverksutviklingen innenfor EU, og i noen grad utfordrer dette etablerte og velfungerende nasjonale løsninger som prioriteringsregelen, når flere kortordninger er samlet i samme fysiske betalingskort (eksempelvis BankAxept og Visa) og de tradisjonelle verdikjedene mellom bank og forbruker.

Et betalingssystem defineres som et system basert på felles regler for avregning, oppgjør og overføring av betalinger mellom to parter som samhandler økonomisk. Juridisk blir det skilt mellom et interbanksystem som behandler transaksjoner mellom banker og en betalingstjeneste som behandler transaksjoner mellom kunde og bank. Figur 5 viser transaksjonsflyten i det norske betalingssystemet. Nederst i figuren er det en illustrasjon av de ulike betalingskanalene som kundene benytter.

Norges Bank ivaretar, med hjemmel i sentralbankloven og betalingssystemloven, sammen med Finanstilsynet viktige oppgaver på betalingssystemområdet, og det er etablert en samarbeids- og ansvarsdeling[1] for å oppnå et best mulig samspill på området.

Figur 5: Transaksjonsflyten i det norske betalingssystemet



Kilde: Finanstilsynet

3.2.2 Styring med og risiko og sårbarhet i betalingssystemene

Finansiell stabilitet innebærer at det finansielle systemet er solid nok til å formidle finansiering, utføre betalinger og fordele risiko på en tilfredsstillende måte. Betalingsformidlingen er gjennom det en viktig bærebjelke for finansiell stabilitet.

[1] http://www.finanstilsynet.no/Global/Venstremeny/Om_tilsynet/Samarbeid/Betalingssystemloven_samarbeid_og_ansvarsdeling_Finanstilsynet_og_Norges_Bank.pdf

Finanstilsynet har konstatert redusert tilgjengelighet for betalingsløsninger i 2014. Det er også observert at robustheten i enkelte sammenhenger ikke samsvarer med betalingsformidlingens sentrale rolle, enten det nå er knyttet til enkeltforetaks løsninger, løsninger benyttet av flere foretak eller sentral felles infrastruktur. Hendelser som oppstår i, eller treffer betalingsinfrastrukturen, rammer bredt og medfører raskt store konsekvenser.

Betalingsformidlingen er under stadig forandring, og det vil være løpende behov for endringer i eksisterende betalingsformidlingsløsninger i tillegg til utvikling av nye løsninger, noe som innebærer en høy endringstakt. Endringene gjøres i både applikasjoner, teknologi og kommunikasjonsløsninger og skjer med bakgrunn i et mangfold av endringsdrivere. Endringer er en hyppig årsak til at feil og avvik oppstår i betalingsformidlingen, og det er derfor knyttet betydelig risiko til dette. Derfor er det vesentlig at risikovurderinger og styring av risiko, i tillegg til god ende til ende-testing og etablering av en god sikkerhetskultur i alle ledd, er en sentral del av foretakenes utviklings- og endringsprosesser.

Det er et ledelsesansvar å sørge for at det enkelte foretak har et etablert rammeverk for styring og kontroll med hele betalingsformidlingen, som samsvarer med den sentrale rollen den utgjør i en velfungerende økonomi, og med fastlagte prosedyrer for viktige funksjoner. Det må derfor etableres kontrollordninger som sikrer etterlevelse av regelverk og av foretakets fastlagte kvalitetsnivå. Gjennomføring av regelmessige verdikjedebaserte risiko- og sårbarhetsanalyser er nødvendig, ikke minst ved utvikling av nye tjenester og løsninger, for å redusere sårbarhet og risiko til definert og akseptabelt nivå, sikre tiltak mot kriminelle angrep og for å unngå alvorlige hendelser. I dette inngår etablering av et drifts-, beredskaps- og sikkerhetsopplegg i tråd med foretakets dokumenterte krav for betalingstjenesten og regelmessig øving for å være i stand til effektiv håndtering når hendelser inntreffer.

Alle aktører i verdikjeden har et selvstendig ansvar for å styre og kontrollere driften i egne operasjoner, hos IKT-leverandører og ikke minst hos (eventuelle) underleverandører. Selv om store deler av den elektroniske infrastrukturen som betalingssystemene benytter er utkontraktert til IKT-leverandører, er det betalingstjenestetilbyder som har ansvaret – et ansvar som ikke kan utkontrakteres. Betalingssystemer vil derfor til enhver tid gi risiko- og sårbarhetsutfordringer som krever en bevisst holdning til sikkerhet, oppfølging og iverksettelse av tiltak der det er nødvendig.

3.2.3 Funn og observasjoner

Som omtalt under rapporterte hendelser, var det i 2014 flere alvorlige hendelser som rammet betalingsformidlingen. Det er mange bakenforliggende årsaker til hendelsene, og det ses ingen fremtredende likhetstrekk utover endringer.

Enkelte foretak har hatt svakheter i sine driftsløsninger som skal sikre kontinuitet for betalingsformidlingen. Det er også observert forbedringspotensial knyttet til katastrofeløsninger.

I 2014 var det noen nettverkshendelser, og den typen hendelser rammer betalingsløsningene spesielt hardt. De medfører oftest avbrudd samtidig hos flere banker og betalingstjenester som nettbank,

kortautorisasjoner, minibank og kassefunksjon i filialer og i post- og banktjenester i butikk. Konsekvensen av nettverkshendelsene tydeliggjør sårbarheten i nettverksinfrastrukturen.

Gjennom tilsynsaktiviteten er det konstatert at enkelte foretak har mangler i sine avtaler knyttet til betalingsformidlingen. Blant annet er det gjort funn hvor avtaler ikke oppfyller kravene i IKT-forskriftens regler om utkontraktering, noe Finanstilsynet har fulgt tett opp.

3.2.4 Meldinger om systemer for betalingstjenester

I lov om betalingssystemer stilles det krav til at det uten unødig opphold skal gis melding til Finanstilsynet om etablering og drift av betalingstjenester.

I 2014 mottak Finanstilsynet 13 meldinger, hvorav de fleste er knyttet til mobile betalingsløsninger. Ni av meldingene gjaldt nye løsninger, mens fire meldinger gjaldt nye versjoner av eksisterende løsninger. Med bakgrunn i de mottatte meldingene, har enkelte foretak blitt fulgt særskilt opp og har blitt bedt om supplerende informasjon eller å endre sine avtaler med underleverandører.

3.2.5 Mobile betalingsløsninger

Som det fremgår av meldeplikten for systemer for betalingstjenester, var de fleste meldinger i 2014 knyttet til mobile løsninger.

Det er en rask utvikling innen mobile betalingsløsninger, både nasjonalt og internasjonalt. Nasjonalt ble løsninger som betalingsapplikasjonen til mCASH[2] og NFC betalingsapplikasjonen Valyou[3] offisielt lansert i 2014. Eika Gruppen har under utvikling sin mobile kontaktløse betalingsløsning[4]. Internasjonalt har Apple lansert sin Apple Pay[5] (foreløpig bare i USA), og Snapchat sin Snapcash[6]. Visa Europa lanserte sin paneuropeiske digitale lommebok V.me[7] senhøsten 2013.

Danske Banks MobilePay-app har i Danmark fått nærmere 2 millioner brukere, mens en rekke andre danske banker har samarbeidet om mobilbanktjenesten Swipe. I Sverige er den mobile betalingstjenesten Swish dominerende med rundt 2 millioner brukere.

Fellesnevneren for de mobile betalingsløsningene er at de skal bidra til økt hastighet på og forenkling av elektroniske betalinger, samt erstatte kontanter.

Finanstilsynet har gjort følgende vurderinger[8] knyttet til mobilbaserte betalingsløsninger, som også omfatter NFC:

[2] https://www.bnbank.no/Omoss/Generell-informasjon/For-pressen/Pressemelding-03032014/
[3] http://www.digi.no/931241/naa-er-valyou-lansert
[4] http://www.cw.no/artikkel/it-bransjen/kontaktlos-betaling-fra-eika
[5] https://www.apple.com/no/pr/library/2014/09/09Apple-Announces-Apple-Pay.html
[6] http://techcrunch.com/2014/11/17/snapcash/
[7] http://www.visa.no/media/pdf/11068.pdf
[8] Vurderingene må ikke anses som uttømmende.

- Økt bruk av elektroniske betalinger gjør at brukeren legger igjen flere elektroniske spor, noe som utfordrer personvernet.
- Mobile lommebøker gjør at enda mer av "brukerens liv" ligger samlet på ett sted, og brukeren vil kunne få store praktiske utfordringer dersom mobiltelefonen kommer på avveie eller på annen måte går tapt.
- Flere sensitive operasjoner i mobiltelefonen stiller krav til brukeren når det gjelder å beskytte telefonen og bruken av den, og ikke alle brukere er tilstrekkelig bevisste når det gjelder dette.
- Mobiltelefonen er utsatt for virus og svakheter i programvaren, og brukeren må oppdatere telefonen med virusbeskyttelse og siste versjon av programvare. Dette blir ikke alltid gjort.
- Mobiltelefoner kan "jailbreakes" av bruker eller andre hvor mobiltelefonens sikkerhet blir ødelagt og gjør den sårbar.
- Det er nødvendig at tilbyder benytter kjente skadebegrensningsteknikker, som blant annet beløpsgrenser, omsetningsgrenser og gradert sikkerhet.
- Tilbydere av slike betalingsløsninger vil enten selv eller gjennom samarbeidspartnere lagre store mengder personlige og betalingsrelaterte data, hvilket stiller høye krav til tilbyders sikkerhet.

Det kan argumenteres for at det er like sikkert eller sikrere å betale fra mobiltelefonen sammenlignet med å "dra kortet", forutsatt at sikkerheten i telefonen ikke har blitt ødelagt (for eksempel ved såkalt jailbreaking) av brukeren eller andre:

- Det kan være sikrere at betalingsdata (kortnummer, kontonummer, utløpsdato osv.) ligger beskyttet på mobiltelefonen, sammenlignet med at de forekommer i klartekst, for eksempel på et bankkort.
- Løsninger som innebærer sentral lagring av betalingsdata slik at de ikke ligger lagret i telefonen, reduserer sårbarheten knyttet til den mobile tjenesten ytterligere, men skaper derimot en ny konsentrasjonsrisiko på lagringsstedet. Eksempel på dette er "tokenization", hvor betalingsdata blir konvertert til en "token" som fungerer som en alias slik at betalingsdata verken lagres i mobiltelefonen eller overføres.
- Transaksjonene kan beskyttes med PIN og/eller fingeravtrykk.
- Betalingene vil ofte bli logget i mobiltelefonen, og kan avstemmes mot banken.
- Det kan være en utfordring å samle og oppbevare papirkvitteringer ved tradisjonell kortbruk. Transaksjonsloggen i mobiltelefonen kan gjøre det mindre påkrevet for brukeren å ta vare på papirkvitteringer.
- Det kan være mulig å fjernslette innholdet i mobiltelefonen, dersom denne kommer på avveie.
- Det kan benyttes kjente skadebegrensningsteknikker, som beløpsgrenser, omsetningsgrenser og gradert sikkerhet (liten autentisering, middels autentisering, stor autentisering).
- Mobile løsninger har gjerne flere lag med sikkerhet, inkludert beløpsgrenser, og det er grunn til å tro at misbruk kan begrenses og ytterligere tiltak settes inn før skaden eventuelt skulle bli omfattende.
- Mobilbetaling kan gjøre at du slipper å taste PIN-kode i trengsel, for eksempel på bussen.

3.2.6 Angrep mot betalingstjenester

I 2014 ble det observert en del DDoS-angrep som var rettet mot bankers nettsider og nettbanker og som dermed også hindret tilgangen til betalingstjenester og sikkerhetstjenester, selv om betalings- eller sikkerhetstjenesten i seg selv ikke var det primære målet. Generelt er trenden at slike angrep opptrer hyppigere, og med større tyngde.

Gjennom 2014 ble det fortsatt observert en rekke phishing-angrep der kriminelle søker å tilegne seg informasjon som kan benyttes for å få tilgang til forbrukernes verdier, og de er særlig rettet mot betalingskort. Phishingen foregår som oftest via e-post der kriminelle utgir seg for å være et reelt foretak. Phishing er på samme måte brukt for å lure forbruker til internettsider som er infisert av ondsinnet programvare. Det er også observert forsøk på phishing via SMS på mobiltelefon. Finanstilsynet synes det er positivt at enkelte foretak[9] har opprettet egne nettsider med informasjon til forbrukerne om hvordan de skal forholde seg ved mistanke om falsk e-post og hvordan de skal beskytte seg selv. Her er det også en oversikt over falske e-poster i foretakets navn som foretaket har kjennskap til.

Selv om det ikke er rapportert om tap som følge av trojanere rettet mot nettbanker og betalingsformidling i 2014, betyr det ikke at det ikke er aktivitet. Den internasjonale trenden er at denne typen angrep går i bølger og flyttes fra land til land. Angrepene har blitt mer målrettede, og man må legge til grunn at Norge igjen kan bli rammet og av mer målrettede angrep enn tidligere.

Selv med det økende omfanget av mobile betalingsløsninger og en global økning av infiserte mobiltelefoner[10], er Finanstilsynet ikke kjent med svindelforsøk via mobiltelefon i Norge.

Finanstilsynets erfaring er at foretakene har god beredskap, at de har etablert godt forsvarsverk og at de iverksetter effektive tiltak som reduserer både skadeomfang og kunders tapsomfang.

3.2.7 Oversikt over årlige tap knyttet til betalingstjenester

Nedenfor er det gjengitt tapstall i Norge for henholdsvis kort- og nettbanksvindel for de fire siste årene. Tallene er innhentet av Finans Norge (FNO) og Bankenes Standardiseringskontor (BSK) i samarbeid med Finanstilsynet.

Det er også tatt med tapstall fra en del andre land for å sammenligne trender. Utviklingen i Norge i 2014 var på linje med utviklingen i de fleste andre europeiske landene. Det er økende tap på kortbetalinger ved varekjøp på Internett, og synkende tap på bruk av nettbank.

3.2.7.1 Tapstall i Norge for kortbruk

Svindel av typen Card-Not-Present (CNP) er den største tapskategorien. Tapene øker stadig og økte med ca. 39 % i Norge i 2014. Tapene på CNP er doblet i løpet av to år, og tredoblet i løpet av de tre

[9] http://www.danskebank.no/nb-no/Privat/Nettbank-og-Mobil/nettbank/Sikkerhet/falsk-e-post/Pages/falsk-e-post.aspx
[10] http://www.eetimes.com/document.asp?doc_id=1325677

siste årene. Tapt originalkort og PIN brukt utenfor Norge økte med 37 %. Annen type svindel med betalingskort er omtrent uforandret. Totalt er det 17 % økning i tap på kortbetalinger.

Tabell 1: Tap ved bruk av betalingskort (tall i hele tusen kroner)

Svindeltype betalingskort	**2011**	**2012**	**2013**	**2014**
Misbruk av kortinformasjon, Card-Not-Present (CNP) (internetthandel m.m.)	24 190	35 701	51 954	72 056
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort i Norge	468	2 308	762	524
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort utenfor Norge	57 340	55 869	51 534	51 685
Originalkort tapt eller stjålet, misbrukt med PIN i Norge	32 224	28 128	21 274	21 266
Originalkort tapt eller stjålet, misbrukt med PIN utenfor Norge	7 008	8 544	9 570	13 071
Originalkort tapt eller stjålet, misbrukt uten PIN	4 488	4 603	4 9 49	5 510
TOTALT	**125 718**	**135 153**	**140 043**	**164 113**

Kilde: Finanstilsynet

Volumet av kortbetalinger for varekjøp på Internett i Norge økte med 13 % fra 2012 til 2013 (tall fra Norges Bank 2013[11]). Andelen svindel økte fra 2013 til 2014 med 39 % (fra ca. 52 millioner til ca. 72 millioner). Av det totale transaksjonsvolumet på kortbetalinger i Norge utgjorde svindel om lag 0,026 %. For handel på Internett med kort utstedt i Norge, er svindelandelen vel 0,1 % (1 promille).

Tabell 2: Antall betalingskort rammet av misbruk

Svindeltype betalingskort	**2011**	**2012**	**2013**	**2014**
Antall kort rammet av misbruk	16 784	20 332	22 531	38 541

Kilde: Finanstilsynet

Antall kort rammet av misbruk økte i 2014 med 71 %. Dette er en større økning enn økningen i tapsbeløp og vil si at det gjennomsnittlige misbruket pr. kort sank.

3.2.7.2 Kortmisbruk og datatyveri

Kortsvindel er en av de høyeste teknologirisikoene som finansnæringen står overfor. Tyveri av kortdata har i flere år vært omfattende og lønnsomt, og trenden er fortsatt økende. De mest sårbare stedene er der hvor det oppbevares eller videreformidles store mengder kortrelatert informasjon.

[11] Svindel i kroner er ca. 72 millioner. Tall fra Norges Bank 2013 viser et volum på 59,7 milliarder kortbetalinger på Internett. Dette vil si om lag 0,12 %, eller vel 1 promille.
http://static.norges-bank.no/pages/99263/NB_memo_1_14_2_no.pdf

Det er en økning i tap ved Card-Not-Present (CNP) både nasjonalt og globalt, som hovedsakelig er tap gjennom misbruk av stjålet kortinformasjon i nettbutikker som ikke stiller krav til 3-D Secure-autentisering. Manglende krav til 3-D Secure-autentisering fra netthandelsstedet, men kun krav til bruk av CVC-kode, utgjør en forbrukerrisiko i betalingsformidlingen. Ved tyveri av kortinformasjon er det lett å misbruke denne i netthandelbutikker som ikke stiller krav til 3-D Secure-autentisering.

Tap ved CNP var en av driverne for at SecuRe Pays retningslinjer for sikkerhet for internettbaserte betalinger nå er etablert som retningslinjer fra den europeiske banktilsynsmyndigheten (EBA)[12], og disse vil etter planen gjelde fra 1. august 2015. I det nye betalingstjenestedirektivet[13] (PSD2) stilles det krav til sterk autentisering, som blir tatt inn i retningslinjene når direktivet er vedtatt.

Internasjonalt er det stadig nye og omfattende tyverier av kortinformasjon, som hos Home Depot og Staples[14]. Verizon 2014 PCI Compliance Report[15] fant en sterk sammenheng mellom non-compliance med PCI DSS[16] og sannsynlighet for å bli rammet av datainnbrudd. Det er også frykt for at stjålet informasjon kan bli benyttet til målrettet phishing for å innhente mer sensitive data.

Selv om næringen i Norge gjør mange tiltak og globalt ligger langt fremme i arbeidet med å redusere sårbarhet, er det nasjonalt behov for å følge opp brukersteder tettere når det gjelder sikkerhet ved internettbasert betaling, for eksempel ved krav om at netthandelssteder skal implementere 3-D Secure-autentisering. Ved lagring av store mengder kortdata er det viktig at internasjonalt anerkjente sikkerhetsstandarder, som PCI DSS, følges.

Fortsatt bruk av magnetstripe mange steder gjør svindel med stjålet kortinformasjon lett for kriminelle. En interessant observasjon fra Nederland er at tap på skimming er redusert betydelig fra 2012 til 2013 på bakgrunn av etablert regionsperre hvor magnetstripen deaktiveres for bruk utenfor Europa, se nedenfor.

3.2.7.3 Tapstall knyttet til bruk av nettbank

Tap ved bruk av nettbank grunnet angrep med ondsinnet kode var svært lavt i 2014. Det var derimot flere tilfeller av tapt/stjålet sikkerhetsmekanisme som økte det totale svindelvolumet for nettbank. En del av disse var knyttet til svindel med utlevering av BankID (kodebrikke) gjennom Postens utleveringstjeneste i Post i butikk, se omtale i kapittel 3.8.1.

[12] https://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments
[13] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ecofin/146078.pdf
[14] http://www.tomsguide.com/us/home-depot-data-breach-theft,news-19577.html
http://techcrunch.com/2014/10/21/staples-becomes-the-latest-retailer-affected-by-a-payment-card-data-breach/
[15] http://www.verizonenterprise.com/pcireport/2014/
[16] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

Tabell 3: Tap ved bruk av nettbank (tall i hele tusen kroner)

Svindeltype nettbank	**2011**	**2012**	**2013**	**2014**
Angrep ved bruk av ondartet programkode på kundens PC (trojaner)	664	5 064	1 327	552
Tapt/stålet sikkerhetsmekanisme	3 321	3 367	1 321	6 655
TOTALT	**3 985**	**8 431**	**2 648**	**7 207**

Kilde: Finanstilsynet

3.2.7.4 Tapstall i andre europeiske land

Tapstall fra andre land er interessante for å sammenligne trender i svindelutviklingen. Det er imidlertid et begrenset antall europeiske land som publiserer tapstall, og det er ulike publiseringstidspunkt. Det er få land som publiserer foregående års tapstall så tidlig som Norge. Nedenfor refereres tapstall fra andre land. På grunn av forsinkelser i publiserte tapstall, er ikke disse tallene og tallene for Norge for 2014 helt sammenlignbare, men gir likevel indikasjoner på utviklingstrender.

Betalingskort

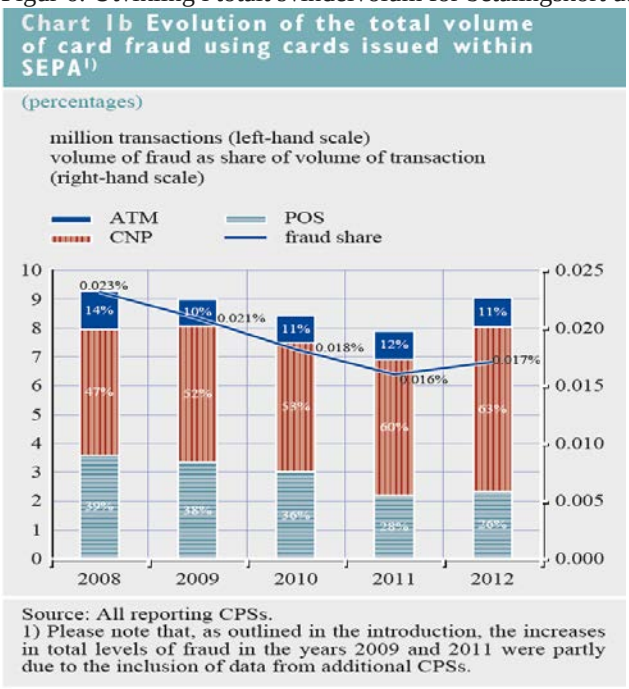
"Third report on card fraud"[17] fra februar 2014 fra Den europeiske sentralbanken (ECB) viste at etter flere år med synkende tap, økte samlet tap med betalingskort for de europeiske landene med 14,8 % fra 2011 til 2012 og svindel av typen CNP med 21,2 %. Alle kategorier tap økte, men andelen CNP var størst i absolutte tapstall med en andel på 60 %, og økte også mest. Innenlandstransaksjoner utgjorde 93 % av totalvolumet av korttransaksjoner, men bare rundt 50 % av svindelvolumet. 5 % av SEPA-transaksjonene er grensekryssende, mens 25 % av svindeltransaksjonene er grensekryssende. Rundt 2 % av transaksjonene innløses utenfor SEPA, men står for 25 % av svindeltransaksjonene. Svindel med POS og ATM med kort utstedt i SEPA-land foregår nesten utelukkende i land utenfor SEPA. Tilsvarende som i Norge, skimmes magnetstripen og brukes i land der magnetstripedelen av kortet fortsatt kan benyttes.

I Storbritannia[18] økte tap med betalingskort med 16 % fra 2012 til 2013 og svindel av typen CNP med nær 22 %. Samtidig økte også det totale volumet av kortbetalinger, så andelen svindel av totalvolumet økte bare med 0,003 %.

I Nederland er skimming av betalingskort redusert med 76 % fra 2012 til 2013, se figur 7 under. Tiltaket har vært regionsperre hvor magnetstripen deaktiveres for bruk utenfor Europa.[19]

[17] http://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201402en.pdf
[18] http://www.financialfraudaction.org.uk/Fraud-the-Facts-2014.asp
[19] http://www.nvb.nl/thema-s/veiligheid-fraude/166/fraude.html

Figur 6: Utvikling i totalt svindelvolum for betalingskort utstedt i SEPA-land (land som bruker euro)



Kilde: ECB: Third report on card fraud

Nettbank

Det er generelt lave tap fra trojanerangrep mot nettbank i Norge og i flere andre europeiske land.

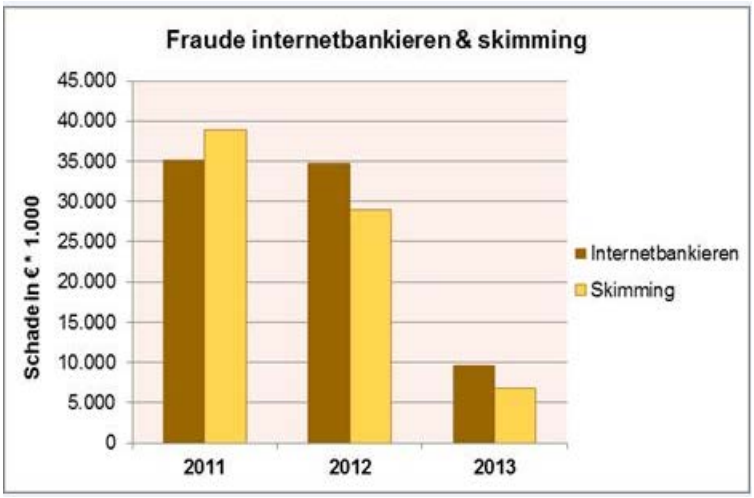
Danmark[20] har hatt omtrent samme utvikling i nettbankangrep som Norge, med en topp i 2012, deretter lavere aktivitet frem til svært lave tapstall i 2014. Tapstall for Nederland[21] viser en nedgang i tap på nettbank på 72 % i 2013.

Tapstall fra Belgia[22] viser en nedgang på 85 % i antall svindeltilfeller i 2014. Dette er en like markant nedgang som i Nederland, men nedgangen kom ett år senere. Nedgangen skyldes en kombinasjon av flere faktorer, blant annet økt årvåkenhet blant forbrukerne. Det er laget flere publikumsvennlige kampanjer i Belgia som advarer mot uvettig bruk av Internett og nettbank.

I Storbritannia[23] økte tapstall på nettbank med 4 % fra 2012 til 2013. Volumet på tap på bruk av nettbank (40,9 millioner pund) var i 2013 i underkant av en tiendedel av volumet på tap med betalingskort (450 millioner pund).

[20] http://www.finansraadet.dk/tal--fakta/Pages/statistik-og-tal/netbankindbrud---statistik.aspx
[21] http://www.nvb.nl/thema-s/veiligheid-fraude/166/fraude.html
[22] https://www.febelfin.be/nl/fraudegevallen-internetbankieren-dalen-sterk
[23] http://www.financialfraudaction.org.uk/Fraud-the-Facts-2014.asp

Figur 7: Utvikling i skimming av betalingskort og nettbanksvindel i Nederland



Kilde: Den nederlandske bankforeningen, http://www.nvb.nl

3.3 Verdipapirområdet

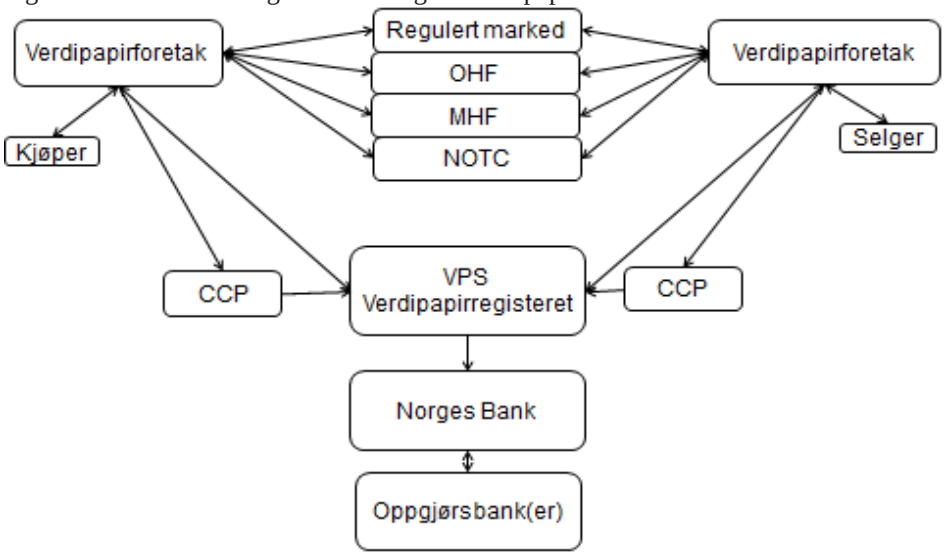
På verdipapirområdet skjer det endringer i et betydelig omfang som innebærer risiko og behov for kvalitetssikring. Også her kan gamle såkalte legacy-systemer representere en utfordring, og en fornyelse innebærer risiko under gjennomføringen.

I denne sektoren er det en endringsbølge på regelverksområdet som vil påvirke infrastruktur og aktører i et stadig mer grenseløst EU. Nye markedsplasser for handel med verdipapirer basert på elektronisk handel på tvers av grenser påvirker de eksisterende markedsplassene både med volum og inntekt og bidrar til å skape endringsbehov.

Fortsatt er helhetsbildet at det er både høy stabilitet og god kvalitet innenfor denne sektoren i Norge, men det kan være en utfordring å sikre akseptabel risiko med de endringene som antas å komme i denne sektoren fremover.

Figur 8 viser hvilke enheter/aktører som er involvert i verdipapirtransaksjoner avhengig av hvilken type verdipapir som handles. Den øverste delen av figuren viser gjennomføringen av selve handelen mens den nedre delen omhandler oppgjøret.

Figur 8: Sentrale roller og sammenhenger i verdipapirsektoren



OHF: Organisert handelsfasilitet
MHF: Multilateral handelsfasilitet
NOTC: Verdipapirforetakenes forbunds handelsløsning for unoterte papirer
CCP: Sentral motpart

Kilde: Finanstilsynet

3.3.1 Verdipapirforetakenes bruk av skybaserte tjenester

Finanstilsynet observerte i 2014 at utkontraktering av kontorapplikasjoner har aktualisert seg også blant verdipapirforetak. Ved bruk av tilgjengelig teknologi kan foretak oppnå stordriftsfordeler, og behovet for egne IT-ansatte med kompetanse på området begrenses til innkjøpskompetanse.

Applikasjoner og lagringssystemer hos IKT-tjenesteleverandører administreres gjennomgående av dedikerte og profesjonelle ressurser. Dette vil kunne bidra til redusert risiko for driftsavbrudd og er med på å gjøre bruk av skyteknologi attraktivt for verdipapirforetakene.

Store selskaper som Google, Microsoft og Amazon tilbyr skybaserte tjenester med standardiserte kontrakter. Kjøp av skytjenester er å betrakte som en utkontraktering, og foretakene må sørge for å beholde styring og kontroll med tjenesteleveransen slik at foretaket har kontroll på egen IKT-virksomhet og at IKT-forskriften etterleves. Dette gjelder for eksempel områder som katastrofetester, årlige risikovurderinger av leveransene, endringshåndteringer og hendelsesrapportering.

Standardiserte og rimelige IKT-tjenesteleveranser kan gi nye utfordringer. Oppsett av tradisjonelle løsninger for lagring og applikasjonsdrift er tradisjonelt sett ressurskrevende. Det kan være fristende for forretningsansvarlige i foretak å gå til innkjøp av IKT-tjenester uten å gå via egen IT-avdeling. Dette kan medføre at det ikke blir gjennomført relevante risikovurderinger for løsningene, og at løsningene ikke samsvarer med foretakets strategi og løsningsarkitektur.

3.3.2 Administrasjon av brukere med tilgang til sensitive selskapsdata på IT-systemer

Verdipapirforetak behandler i stor grad sensitiv informasjon, og det er derfor viktig at informasjon om selskapshendelser og annen kurssensitiv selskapsinformasjon må beskyttes. Foretakene må sikre at informasjonen er tilstrekkelig beskyttet både ved lagring, under transport, i forbindelse med utskrift og e-post (kryptering), samt ved bruk av minnepinner. Når det gjelder tilganger er det foretakenes ansvar å sikre tilstrekkelig kontroll. Dette gjelder også bruk av utkontrakterte filutvekslingsløsninger og distribusjon av sensitiv informasjon.

Det er observert tilfeller med mangelfull kontroll, og Finanstilsynet vil fremover vektlegge tilsyn med prosessene for tilgangshåndtering av sensitiv informasjon med tilhørende applikasjonstilganger.

3.3.3 Konsentrasjonsrisiko på nettverksinfrastrukturen

Aktørene i verdipapirmarkedet benytter i stor utstrekning den samme nettverksinfrastrukturen mot handelsplasser og oppgjørssentraler. Denne infrastrukturen har hittil vist seg å være både robust og kostnadseffektiv. Finanstilsynet er likevel opptatt av at dette representerer en konsentrasjonsrisiko der konsekvensen ved en feilsituasjon er stor, og at dette derfor må gjenspeiles i risikoanalyser og preventive tiltak på området.

3.3.4 Risiko ved endringer av sentrale infrastrukturkomponenter for verdipapiromsetning

VPS er i ferd med å bytte store deler av sine kjernesystemer. Dette er et omfattende prosjekt som fortsatt vil innebære betydelig risiko. Finanstilsynet vurderer VPS' systemer og data som del av den kritiske finansielle infrastrukturen i Norge. VPS' kjernesystemer er av de mest kritiske komponentene i verdipapiromsetningen i Norge. Finanstilsynet følger prosjektet og forventer at VPS gjennomfører kvalitetsmessig gode risikovurderinger og følger beste praksis for prosjektstyring og endringshåndtering ved innføringen av nye løsninger.

3.4 Bank

3.4.1 Endringer på driftsleverandørsiden

Utviklingen i 2014 viste at stadig flere banker bytter leverandører og løsninger innen sentrale deler av IKT-virksomheten. De frigjør seg fra leverandører gjennom mange år, og velger gjerne flere leverandører. Foretakene inntar en mer tilbaketrukket rolle når det gjelder IT-utvikling og daglig drift.

Organisasjonsmessig har det skjedd store endringer de siste to årene. I 2014 fortsatte Finanstilsynet oppfølgingen av endringer i organiseringen av Nets med spesiell vekt på avtalesiden mellom Finans Norge (bankene) og Nets. Nets ble i 2014 solgt til Advent International og Bain Capital. Videre ble Evry lagt ut for salg.

I 2014 ble krav til datahallutrustning aktualisert både gjennom nye utkontrakteringspartnere, bygging av nye datasentre og driftshendelser, se omtale i kapittel 5.2.

Endringer i leverandøravtaler og driftsopplegg kan øke risikoen, spesielt i endringsperioden. Det er foretaket som har ansvaret for egen drift, og dette inkluderer også de delene av forretningsfunksjonene som er utkontraktert, som for eksempel IKT (jf. IKT-forskriften § 12). Det er derfor viktig at foretakets risikovurdering også omfatter de utkontrakterte delene for å kunne ha oversikt over den totale risikoen for forretningsområdene.

3.4.2 Katastrofeberedskap

Funn i 2014 indikerer at reetablering av IKT-tjenester i en katastrofesituasjon vil ta lenger tid enn antatt. Det er to områder som har særlig innvirkning på dette: 1) manglende koordinering av foretakets egen katastrofeplan med katastrofeplan for de utkontrakterte tjenestene og 2) mangelfullt omfang av katastrofetest og dokumentasjon av testresultater både i foretaket og hos leverandør. Finanstilsynet har også observert at det mangler planer for ulike situasjoner, som hva foretaket kan gjøre for å drive virksomheten uten IKT i en periode, og for å informere kunder og ansatte.

For å utarbeide katastrofeplaner, bør det gjennomføres konsekvensanalyser og risikovurderinger som tar utgangspunkt i foretakets forretningsfunksjoner. Katastrofeplanen må peke på kritisk infrastruktur, nødvendig personell og tjenester som forretningsfunksjonene er avhengige av for å kunne fungere som planlagt. For de ulike systemene som inngår i katastrofeløsningen, må det dokumenteres krav til hvor lang tid forretningsdriften kan være uten systemstøtte og hvor mye data man kan tåle å tape.

3.4.3 Utkontrakteringsavtaler

Det er foretaket selv som har ansvaret for egen drift, og dette inkluderer også de delene av forretningsfunksjonene som er utkontraktert. Finanstilsynet vil peke på at selv om tjenesteleverandøren er sertifisert, for eksempel etter ISO/IEC 27001: 2005, er det ingen automatikk i at bestemmelsene i Finanstilsynets IKT-forskrift dermed er oppfylt. Særlig gjelder dette for styring og kontroll av IKT-virksomheten. Foretakets styring og kontroll av egen virksomhet skal sikre at gjeldende regelverk overholdes og avtaler oppfylles. Dette stiller særlig krav til at foretakene får tilstrekkelig tilgang til informasjon om, og kontroll av tjenesteleveransene til å kunne kontrollere at IKT-forskriften overholdes. Dette gjelder blant annet forhold som katastrofetest, årlig risikovurdering av leveransen, endringshåndtering og hendelsesrapportering.

Finanstilsynet vurderer innsyn i tjenesteleveranse som helt avgjørende for at foretak skal kunne vurdere risiko og føre styring og kontroll med egen virksomhet.

3.4.4 Forskrift om krav til datasystemer og rapportering til Bankenes sikringsfond

Forskrift om krav til datasystemer og rapportering til Bankenes sikringsfond med hjemmel i finanstilsynsloven trådte i kraft 1. juli 2013. Finanstilsynet og Bankenes sikringsfond gjennomførte i 2014 tilsyn med fire banker for å vurdere bankenes etterlevelse av forskriften. Tema for tilsynene var å

undersøke hvor raskt bankene, Finanstilsynet og sikringsfondet kan klargjøre informasjonsgrunnlaget for utbetaling av sikrede midler dersom banken blir satt under offentlig administrasjon. Ikke alle bankene hadde etablert løsninger for å rapportere i henhold til kravene i forskriften. Informasjonsleveransene viste også store kvalitetsmessige variasjoner. Temaet vil bli fulgt opp med tilsvarende tilsyn i 2015. Bankene har kommet med gode innspill og påpekt uklarheter i forskriftsteksten. Finanstilsynet og Bankenes sikringsfond tar med seg disse innspillene og har blant annet besluttet å utarbeide en veiledning til forskriften.

Det er viktig at foretakene utvikler løsninger i tråd med forskriftens krav, innarbeider rapporteringen i sine beredskapsplaner og sikrer at den blir testet regelmessig.

3.4.5 Tilgangskontroll

Finanstilsynet har merket seg at bankene i sine prosesser og prosedyrer i stor grad har definert hvilke oppgaver som er tillagt funksjonene som linjeledere, systemeiere og forretningsfaglige eiere. Dette omfatter blant annet tildeling og overvåking av tilganger til systemene. Linjelederne er ofte ansvarlige for gjennomgang av tilgangene til de enkelte ansatte, og vanligvis stilles det krav til at dette skal gjøres minst én gang i året. Det er viktig at informasjonen om tilgangene er av en slik kvalitet og i et slikt format at den som skal gjennomgå dem, har et godt grunnlag for å kunne overholde kravene til kontroll.

De fleste bankene har en svært omfattende applikasjonsportefølje. Innen hver enkelt applikasjon er tilgangsrettigheter basert på den enkelte brukers rolle. Det er derfor viktig at det tas ut oversikter som viser tilganger for den enkelte bruker på applikasjonsnivå og at det gjennomføres samme undersøkelse av applikasjonstilganger som for brukeridenter, domener og filområder.

Finanstilsynet har i sine funn funnet at gjennomgangen av den enkelte medarbeiders tilganger i flere tilfeller har vært mangelfull, og dette gjelder særlig for området der hvor den enkelte applikasjon har egen tilgangsstyring.

3.4.6 Klassifisering av informasjon

Finanstilsynet ble i 2014 informert om at foretak klassifiserer sine IT-systemer for å sikre konfidensialitet, integritet og tilgjengelighet. Ofte er det den enkelte systemeier som utfører klassifiseringen. Strengt konfidensielt, konfidensielt eller til internt bruk er en inndeling som foretakene klassifiserer sine IT-systemer etter. Inndelingen baseres på behovet for å sikre bruken av informasjon og knyttes til tilgangskontrollen.

Finanstilsynet har sett at det er utfordrende for foretakene å styre og kontrollere at klassifiseringsregler operasjonaliseres. Særlig gjelder dette for håndtering av tilganger til graderte data og systemer.

3.5 Forsikring

3.5.1 Generelt

Norske forsikringsselskaper er svært ulike, blant annet i organisering, størrelse og hva de tilbyr av produkter. Noen forsikringsselskaper er del av større norske eller utenlandske finans- eller forsikringskonsern, mens andre forsikringsselskaper er frittstående og selvstendige aksjeselskaper. Enkelte livsforsikrings- og skadeforsikringsselskaper har tett samarbeid, blant annet på IKT-siden, og kan fremstå som ett selskap, selv om de formelt er separate aksjeselskaper. Flere selskaper har nært samarbeid med banker og benytter bankenes distribusjons- og salgsnett. Noen aktører i det norske markedet er norske filialer av utenlandske selskaper (NUF – norskregistrert utenlandsk foretak). Disse er ikke direkte underlagt Finanstilsynets tilsyn.

Forsikringsselskapene som er medlem av Finans Norge, benytter seg av Finans Norges fellesløsninger. Forskjellene på forsikringsselskapene gjenspeiles i selskapenes virksomhet, utfordringer og risikoer på IKT-området. Det er likevel noen fellestrekk, som beskrives nedenfor.

3.5.2 Komplekse forsikringssystemer

Forsikringsselskaper er generelt IKT-avanserte virksomheter. Selskapene, og spesielt tradisjonelle livsforsikringsselskaper, har som regel flere ulike forretningskritiske kjernesystemer, som ofte er store og inneholder mange kompliserte forsikringstekniske beregninger, og som er krevende å forvalte. Systemene inneholder ofte sensitive personopplysninger. Det er vesentlig for virksomheten at systemene forvaltes og brukes på en sikker og betryggende måte og at reserveløsninger, basert på en forretningsmessig risikovurdering, er etablert og blir regelmessig testet.

3.5.3 Endringskontroll

Det siste tiåret har livsforsikringsselskapene vært underlagt store regulatoriske endringer, blant annet innføring av obligatorisk tjenestepensjon, ny forsikringsvirksomhetslov og pensjonsreformen. Det har også vært flere og større endringer på tarifferingssiden. Endringer pågår stadig, jf. omtale i kapittel 5.1.3. Skadeforsikringsselskapene har, som følge av forsikringsvirksomhetsloven, måttet endre sine pristariffer. Endringene har medført betydelig IKT-arbeid i selskapenes kjernesystemer, som er komplekse og krevende å endre.

Både livsforsikrings- og skadeforsikringsselskapene har i lang tid forberedt innføringen av Solvens II-regelverket, som etter mange utsettelser skal gjelde fra 1. januar 2016. Regelverket medfører til dels omfattende IKT-utvikling. Blant annet medfører modellberegninger og økte krav til intern og ekstern rapportering store krav til data og datakvalitet.

I tillegg til myndighetspålagte endringer nedlegger selskapene mye arbeid i å tilpasse IKT-virksomheten til stadig nye teknologiske løsninger, nye produkter og funksjoner, samt automatisering og effektivisering av forretningsprosesser.

Finansforetakene er etter IKT-forskriften § 9 pålagt å rapportere vesentlige hendelser til Finanstilsynet. Tilsynet har mottatt få hendelser fra forsikringsselskaper. Et flertall av hendelsene gjelder

konfidensialitetsbrudd som ikke er direkte relatert til systemendringer. Dette kan tyde på at selskapene har bra endringskontroll. Det kan også skyldes uklarhet i forståelsen av hvilke hendelser som skal rapporteres, jf. omtale av hendelsesrapportering i kapittel 3.1.5.

Endringer generelt fører til økt operasjonell risiko, og det er viktig at selskapene har etablert og benytter gode endringshåndteringsprosesser, og at risikoer relatert til endringene kontrolleres og styres.

3.5.4 Utkontraktert IKT-virksomhet

Nesten alle forsikringsselskaper har utkontraktert IKT-virksomhet, i mer eller mindre grad, og med ulike løsninger. Det finnes imidlertid selskaper som ut fra en kostnadsvurdering og et uttalt ønske om å ha bedre styring og kontroll med IKT-virksomheten, har valgt å gjøre alt IKT-arbeidet internt, både systemutvikling og drift.

Etter forskrift om risikostyring og internkontroll § 5 og IKT-forskriften § 12 har forsikringsselskapet ansvaret for risikostyring og internkontroll også der deler av virksomheten er utkontraktert. Selskapet skal ha tilstrekkelig kompetanse til å forvalte avtalen, noe som blant annet innebærer å kunne kontrollere leveransene. Kravene gjelder uansett forsikringsselskapets størrelse og hvem som er leverandøren.

Finanstilsynet har gjennom tilsyn observert at enkelte forsikringsselskaper ikke fullt ut etterlever forskriftenes krav ved utkontraktering. Manglende etterlevelse kan medføre mangelfull oversikt over, og kontroll med, selskapets IKT-virksomhet og IKT-risikoer.

3.5.5 Risikostyring

Risikovurderinger og risikostyring skal være integrert i selskapets daglige arbeid. Dette er viktige virkemidler for å forhindre tap og sikre at selskapet, også på IKT-området, kan gjennomføre sine strategier og når sine mål. Dette fremkommer også av forskrift om risikostyring og internkontroll § 6 Risikostyring: "Med utgangspunkt i definerte mål og strategier for virksomheten skal det minst én gang årlig foretas en gjennomgang av vesentlige risikoer for alle virksomhetsområder". Også IKT-forskriften § 3 krever at det minst årlig eller ved endringer av betydning gjennomføres risikovurderinger.

Finanstilsynets observasjoner er at selskapenes dokumenterte risikoanalyser jevnt over er fragmenterte, mangelfulle og ikke dekker selskapets samlede IKT-virksomhet. Det er dermed fare for at risikoanalysene ikke blir et reelt virkemiddel for å styre selskapets IKT-risikoer innenfor definerte rammer, og et bidrag til å sikre selskapets måloppnåelse.

3.5.6 Testing av beredskapsløsninger

I tilfelle driftsavbrudd og bortfall av tjenester skal foretakene ha etablert kontinuitets- og katastrofeplaner. For å sikre at katastrofeløsningen virker som forutsatt, skal kontinuitets- og katastrofeplanene testes minst årlig.

Ved tilsyn har Finanstilsynet funnet at testing av kontinuitets- og katastrofeplaner gjennomgående synes å være et forbedringsområde. Blant annet har Finanstilsynet observert at forsikringsselskapene ikke tar tilstrekkelig ansvar for, eller blir tilstrekkelig involvert i, leverandørenes testing av planer som berører forsikringsselskapet.

3.5.7 Eksterne dataangrep

Forsikringsselskaper oppbevarer personopplysninger og ofte også helseopplysninger og kontoopplysninger om sine kunder. Dette er opplysninger som på flere måter kan være interessante for inntrengere. Et eksempel på dette er det amerikanske forsikringsselskapet Anthem Inc[24], som i februar 2015 ble hacket, noe som førte til at personopplysninger fra flere titalls millioner kunder kom på avveie. Konkrete helseopplysninger kom antakeligvis ikke på avveie, og heller ikke kortdata.

Generelt har forsikringsselskapene, som alle andre finansforetak, mye oppmerksomhet på og bruker mye ressurser på å forhindre og oppdage eksterne dataangrep. Imidlertid har det vært angrep i norske forsikringsselskaper, blant annet DDoS-angrep, og Finanstilsynet er kjent med at noen forsikringsselskaper frykter industrispionasje, for eksempel i forbindelse med prissetting av produkter.

3.6 Funn i andre foretak

Finanstilsynet gjør enkelte stedlige IT-tilsyn i inkassoselskaper og eiendomsmeglingsforetak. I tillegg må eiendomsmeglingsforetakene og inkassoselskapene svare på et forenklet egenevalueringsskjema med spørsmål om IT-virksomheten ved ordinære fagtilsyn. Finanstilsynet hadde i 2014 merknader til manglende beredskapsløsninger, sikring av konfidensiell informasjon, manglende rutiner for å håndtere sikkerhetshendelser og at foretaket peker på IT-leverandøren som ansvarlig for IT-prosessene.

3.7 Prioritering av strøm og tele for kritisk finansiell infrastruktur

Finanstilsynet har vært en pådriver i arbeidet med å forankre finanssektorens prioritering av tilgang til strøm og tele i en beredskapssituasjon og for å sikre tverrsektorielt samarbeid. Møter med de prioriterte finansaktørene viste at de i stor grad bruker samme strøm- og teleleverandører. Det er gjennomført møter mellom de prioriterte finansaktørene og de sentrale strøm- og teleleverandørene for å informere de sistnevnte om hvilke installasjoner som understøtter de prioriterte systemene. Strøm- og teleleverandørene skal dermed være i stand til å prioritere de kritiske finanstjenestene i en krisesituasjon. Finansaktørene har etablert rutiner som sikrer at strøm- og teleleverandørene blir

[24] http://www.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925/, http://www.anthemfacts.com/

oppdatert ved endringer, og Finanstilsynet vil følge opp at rutinene kommer til anvendelse ved systemendringer som påvirker strøm- og teleleveransene.

3.8 Forbrukerområdet

3.8.1 Mangelfull ID-sjekk ved utlevering av BankID

Det rapporteres om et antall feilutleveringer av kodebrikken som benyttes sammen med BankID. Dette gjaldt 15 av 150 000 utleveringer i 2014. Det har vist seg å kunne få meget store konsekvenser for den enkelte forbruker som blir rammet av slike feil. Finanstilsynet har grunn til å tro at identitetskontrollen i en del tilfeller har vært mangelfull. Slike utleveringsfeil skjer gjerne i Post i butikk, hvor uerfarne ekspeditører ikke gjør god nok identitetssjekk. Dette utnyttes av kriminelle som har fått tak i en bankkundes data, og har bestilt ny BankID som banken sender i posten. Mangelfull ID-kontroll kan da forekomme.[25]

For en kunde som blir kompromittert (stilt i dårlig lys) på denne måten, kan dette være både en vanskelig og ubehagelig situasjon hvor innskuddskontoer kan tømmes urettmessig ved at uvedkommende får tilgang til for eksempel vedkommendes nettbank. Det er bankenes ansvar å sørge for riktig utlevering av BankID, og banken må i slike tilfeller ta ansvar for å rydde opp i forholdet og holde kunden skadefri. Rutinene for utlevering av kodebrikke, som ved utlevering i for eksempel i Post eller Bank i butikk der banker velger dette, bør være av minst samme kvalitet og gjennomføring som ved tradisjonelle bankfilialer.

3.8.2 Svindel ved netthandel

Mange forbrukere har opplevd å bli svindlet ved netthandel mellom private parter. Det er mange eksempler på situasjoner der selger burde reagere, og ikke tenker på at de kan bli svindlet. Varer overleveres uten betaling, og sendes i enkelte tilfeller til ukjente utenlandske adresser uten noen form for betalingsgaranti. Handelsstedene på nettet tilbyr betalingstjenester, men en stor del av brukerne tar seg ikke bryet med å benytte disse. For tilbyderne av handelsplassene blir det en avveining mellom brukervennlighet og sikkerhet hvordan oppgjørstjenester tilbys. Finanstilsynet kjenner ikke til at noen av netthandelsstedene for private har obligatorisk bruk av oppgjørstjenester.

3.8.3 Nettbutikker og informasjonssikkerhet

Bruken av nettbutikker har økt mye de siste årene, og det er noen risikoer forbundet med det. I de fleste tilfeller er det relativt enkelt å se om et nettsted har nødvendig sikkerhet, som for eksempel kryptering. Dette kan forbrukere se ved at det kommer opp et lite bilde av en hengelås i adressefeltet, sammen med navnet til nettstedet. På noen nettlesere vil denne være grønn, se eksempel under på Microsofts sertifikat.

[25] http://www.dn.no/nyheter/2014/07/18/2156/Finans/det-er-grunn-til-a-vaere-bekymret

Figur 9: Eksempel ved bruk av Microsofts Internet Explorer

En tilleggskontroll kan være å kontrollere at navnet i adressefeltet stemmer overens med brukerstedet som brukeren ønsker å besøke.

Ved valg av vare, innlogging, betaling og leveringsadresse bør nettsteder ha en løsning som krypterer informasjonen som forbruker taster inn. Krypteringen er der for at ingen andre enn forbrukeren og butikken skal kjenne informasjonen. Dersom et nettsted ikke har en slik løsning, skal en være svært forsiktig med å skrive inn informasjon som kan brukes av andre. Svært ofte sier det mye om kvaliteten på nettbutikkløsningen dersom det ikke benyttes krypteringsløsning. Dette kan for eksempel gjøre det enklere å gjennomføre "Man-in-the-middle"-angrep, ettersom det vil være vanskelig å oppdage om en har direkte kontakt med nettbutikken eller ikke.

3.8.4 Kort og PIN-kode

Finanstilsynet vurderte i 2014 enkelte aspekter ved sikkerheten i kortsystemene, med spesiell vekt på integritetsbeskyttelse knyttet til PIN-kode. Finanstilsynet konkluderer med at i saker der kortet har vært misbrukt med PIN-kode, og kunden hevder å ha holdt PIN-kode hemmelig, bør disse sakene følges opp med grundige, uavhengige, tekniske undersøkelser i hvert enkelt tilfelle for å avdekke hendelsesforløp og årsaksforhold.

4 Andre observasjoner

Dette kapitlet tar opp de mest fremtredende truslene foretakene selv tar opp i intervjuer og besvarelser av Finanstilsynets spørreskjema. Videre omtaler det vesentlige trusler fremkommet gjennom intervjuer med sentrale aktører for sikkerhetsløsninger og de mest alvorlige truslene ut fra enkelte internasjonale sikkerhetsselskapers vurderinger.

4.1 Foretakenes vurdering av risiko

4.1.1 Intervjuer

Finanstilsynet intervjuet i 2014 ulike finansforetak som et ledd i kartlegging av IKT-risikoer. Enkelte trusler rapporteres av mange av foretakene. Visse trusler kan gjøre stor skade for foretaket dersom de inntreffer, og enkelte trusler kan påføre forbrukere betydelig skade og ulempe. Under omtales trusler som foretakene er bekymret for. I enkelte tilfeller beskrives kontrolltiltak som er trukket frem.

4.1.1.1 Inntrengere får tilgang til IKT-infrastruktur og applikasjoner

Foretakene rapporterer at angrepene etter hvert blir spesialsydd og rettet mot et bestemt foretak. Angrepene starter med phishing, infiserte minnepinner (USB), eller sosial manipulering[26]. Angrepskoden er svært vanskelig å oppdage. Angriperen tar seg god tid og går skrittvis frem. Et typisk angrep kan innlede med at angrepskoden kartlegger de ulike segmentene i nettverket. Deretter leter skadevaren etter høyrettighetsbrukere. Skadevaren bruker rettighetene og legger inn selvsignerte sertifikater i hvitelisten i operativsystemet og kopierer deretter innloggingssider for å få tak i brukerens påloggings-ID og passord.

For å møte disse truslene må foretakene ha gode tilgangskontroller. Tilgangskontrollene må være oppdatert og aktuelle. Administratorrettigheter skal benyttes av et fåtall navngitte personer og kun i forbindelse med nærmere definerte oppgaver. Foretaket må logge og analysere aktivitet utført med administratorbrukere og andre høyrettighetsbrukere. Foretaket må fremtvinge arbeidsdeling så godt det lar seg gjøre, slik at ikke angriperen ved å benytte én og samme bruker er i stand til å utsette foretaket for store tap eller stor fare. Foretaket må best mulig kjenne sitt trafikkmønster (volum, tjenester, porter, protokoller) gjennom driftsdøgnet, og handle ved avvik fra driftsmønsteret ("fingeravtrykket"), slik at en potensiell inntrenger blir stoppet.

[26] Angriperen lykkes i å utgi seg for å være en betrodd person, og misbruker tilliten og infiserer foretaket.

Angripere foretrekker å benytte sine egne, skreddersydde verktøy. Dersom foretaket har hvitelister, det vil si lister over godkjente programmer, er angriperen tvunget til å ty til script eller benytte systemverktøy som går på maskinen. Bruk av slike verktøy og teknikker gjør det vanskeligere for angriperen å kamuflere seg og øker "støyen" knyttet til angrepet, noe som kan gjøre angrepet lettere å oppdage.

4.1.1.2 Kompleksitet

Mange foretak gir uttrykk for at IKT-systemene er så komplekse at de utgjør en risiko for stabil drift og bremser nyutvikling. Kompleksiteten oppstår som følge av at funksjoner som ikke lenger er i bruk, er erstattet av ny funksjonalitet eller er inkorporert i andre funksjoner ikke blir slettet fra produksjonsmiljøet. Dette kan gi en rekke ulemper og kostnader, for eksempel fordi funksjonene

- okkuperer ressurser (minne, disk) i test og produksjon
- må administreres (JCL, produksjonsplanlegging)
- inngår i sikkerhetskopiering samt katastrofe- og kontinuitetsplaner og testing
- medfører unødige oppdateringer
- medfører unødige lisenskostnader
- inneholder sikkerhetshull som angripere kan tenkes å utnytte

I tillegg kommer kompleksiteten som følger av at en rekke kjernesystemer er bygget på teknologi som er 20–40 år gammel.

Foretakene bør ha rutiner som løpende sikrer at funksjoner som ikke lenger benyttes, eller som benyttes i liten grad, blir fjernet, avvikles over tid eller slås sammen med andre funksjoner. Finanstilsynet mener at enkelte foretak bør gå gjennom og rydde på dette feltet.

4.1.1.3 Katastrofe

I 2014 ble enkelte store foretak av betydning for finanssektoren rammet av skadevare eller andre forhold som satte deler av virksomhetene ut av spill, og som dermed avdekket sårbarheter i foretakene.

For et foretak som er under angrep, har skadebegrensning høy prioritet, og det forutsetter at foretaket har oversikt over hvilke funksjoner og brukere som er rammet. Dette fremgår av loggene, og e-postlogger kan fortelle hvilke brukere som har åpnet et infisert vedlegg. Brannmurlogger kan gi indikasjoner på innbrudd. E-postlogger og brannmurlogger sett i sammenheng kan styrke antakelsen om angrep. E-postlogger viser at brukeren har åpnet et skadelig vedlegg, og brannmuren viser at det går meldinger til en ukjent adresse som viser seg å være angriperens kontrollsenter. Serverlogger kan gi ytterligere indikasjoner på skadevare hos brukeren. Logger vil være primærkilden for informasjon også ved avbrudd som skyldes andre forhold enn angrep. Flere foretak rapporterer at oppdagende kontroller i foretaket bør bli bedre. Flere foretak rapporterer at de prioriterer arbeidet med logganalyse, både for å forebygge og for å være i stand til begrense skadene etter angrep.

Foretakene erfarer at tilbakelegging av data og programmer tar lengre tid enn antatt. I denne

situasjonen ønsker foretakene å reetablere de viktigste funksjonene/tjenestene først. Dette forutsetter at det er en omforent prioritering av funksjoner/tjenester.

Videre forutsetter det kunnskap om hvilke systemer som understøtter hvilke forretningsfunksjoner. Kunnskap om systemer vil si at foretaket vet navnet på de relevante eksekverbare moduler og tilhørende datasettnavn, som i sin tur angis i programmet som utfører selve tilbakeleggingen av disse.

4.1.1.4 Sosiale medier

Flere foretak uttrykte bekymring for den økende bruken av sosiale medier. Konfidensiell informasjon, negativ omtale, informasjon som ikke er korrekt og informasjon om foretakets kunder kan komme uvedkommende i hende.

Angripere benytter informasjon om foretakets medarbeidere som fremkommer på sosiale medier til å utforme en "personlig" e-postmelding med lenke til ondartet kode. Innholdet i e-posten gir inntrykk av at avsender kjenner mottakeren, og tilliten som mottaker får, gjør at hun åpner vedlegget som viser seg å inneholde ondartet kode.

Det kan være utfordrende for foretakene å beskytte seg på en effektiv måte mot spredning av informasjon på sosiale medier. Opplæring av ansatte kan i noen grad virke forebyggende.

4.1.1.5 EMV/chip

Minibanker og butikkterminaler er spesialbygget for å håndtere korttransaksjoner og PIN på en sikker måte. Terminalene og programvaren i terminalene er vanskelig tilgjengelig for angripere. Nå lanseres løsninger hvor mobiltelefon fungerer som butikkterminal på brukerstedet, og kortinformasjon ligger på brukerens mobil. Da ligger terminalen, kortet og protokollene som benyttes, åpent for angrep i større grad enn før. Dette representerer en betydelig risiko og en stor utfordring som foretakene må ta hensyn til ved utforming av nye løsninger.

4.1.1.6 Cyberangrep

En rekke foretak anser eksterne angrep som en økende trussel. Senere tid har vist at en rekke interessegrupper angriper enkeltforetak, infrastrukturforetak og nasjonal IKT-infrastruktur for å oppnå politisk og/eller økonomisk vinning.

IKT-drift kan skje over leide linjer eller over Internett, eller en kombinasjon. Offshoredrift skjer over Internett. Trafikk på Internett er utsatt for angrep fra et globalt samfunn av angripere. Fjerndrift over Internett kan i tillegg gi økt sannsynlighet for avbrudd sammenlignet med lokale, leide linjer.

Enkelte land i konflikt er stengt ute fra kredittkortsystemene. Dersom den sentrale kortinfrastrukturen angripes, er det en risiko for at alle land mister tilgangen. I en slik situasjon kan det norske, nasjonale kortsystemet (BankAxept) være viktig.

4.1.1.7 Avhengighet av Internett

Finansforetak gir uttrykk for at driften er helt avhengig av internettforbindelse.

- Bruk av digitale sertifikater forutsetter at det gjøres oppslag mot sperrelister.
- Bruk av programvare forutsetter kommunikasjon knyttet til kontroll av lisenser.
- Oppdatering av programvare skjer over Internett.

Listen gjengir noen eksempler. Foretakene er sårbare for bortfall av internettforbindelse.

4.1.1.8 Utlevering av BankID-kodebrikke

I kapittel 3.8.1 er det redegjort for feilutlevering av BankID-kodebrikker. Enkelte foretak opplyser at de har gått bort fra denne utleveringsformen.

BankID kan benyttes for å få tilgang til en rekke personlige, offentlige tjenester. Dersom BankID kommer uvedkommende i hende, kan offeret påføres stor skade. BankID virker slik at BankID utstedt av enhver norsk bank, kan benyttes i enhver annen norsk bank. Det har lykkes svindlere å opprette et kundeforhold i ny bank i offerets navn og benytte BankID i ny bank til å tappe offerets konto i offerets bank. Offeret har ingen mulighet til å sperre for opprettelse av BankID i ny bank. BankID, slik den er konstruert, har på denne måten påført norske bankkunder en potensiell risiko.

I dag har en ingen mulighet for å reservere seg mot opprettelse av BankID. Det bør vurderes om det skal lages en funksjon der bankkunden kan reservere seg mot at det opprettes BankID i kundens navn. Ettersom BankID i en svindlers besittelse kan medføre slike alvorlig konsekvenser for offeret, må bankene vurdere om utlevering i post og bank i butikk skal benyttes ved utlevering. I tilfelle banken fortsatt velger dette, må den ha gode rutiner både for utlevering og for å avhjelpe skader og ulemper som offer kan bli påført ved en svindel.

4.1.2 Spørreundersøkelse

I desember 2014 foretok Finanstilsynet en spørreundersøkelse blant 26 foretak. I spørreundersøkelsen ber Finanstilsynet foretakene vurdere i hvilken grad foretaket anser seg for å være sårbare for aktuelle trusler og har manglende/mangelfulle kontrolltiltak. Truslene og kontrolltiltakene er listet i kolonne 2 i tabellene nedenfor. Sårbarhetene faller naturlig i seks risikoområder. Resultatene fremgår av tabellene nedenfor. *Grønt* gir uttrykk for lav sårbarhet for foretaket, *gult* innebærer middels sårbarhet og *rødt* uttrykker høy sårbarhet. *Ingen farge* innebærer at foretaket ikke har svart.

Videre ble foretakene bedt om å vurdere om sårbarhetene anses å være økende, stabile eller minkende. Trenden som kommer til uttrykk i kolonnen lengst til høyre i tabellene nedenfor, er uttrykk for gjennomsnittet av de vurderingene som ble gitt, der intervallet –0,2 til +0,2 angis av en horisontal pil og innebærer en stabil trend. Piler som peker opp, indikerer at sårbarheten anses å være økende (intervallet +0,2 til +1), og piler som peker nedover, indikerer at sårbarheten anses å være minkende (intervallet –0,2 til –1).

Gjennomgående er trenden stabil, eller minkende. Mulige forklaringer på dette kan være at foretakene anser at de har adekvate tiltak som vil gjøre dem mindre sårbare, eller at foretakene anser at enkelte trusler vil avta "av seg selv" fremover. Dette kan gjelde trusselen fra ondartet kode, som i følge en del foretak har avtatt i den senere tid.

En del av foretakene gir utfyllende og svært gode kommentarer til truslene og kontrolltiltakene. Kommentarene gir Finanstilsynet innsikt når det gjelder foretakenes vurdering av trusler og tiltak, og er gode innspill til oppfølging fremover.

4.1.2.1 Støtte for strategiske beslutninger

Risikoen er at IT ikke fungerer tilfredsstillende som støtte for strategiske beslutninger, kundebehandling eller saksbehandling.

Tabell 4: Støtte for strategiske beslutninger

	Sårbarhet	Foretakenes svar	Trend
1	Systemenes evne til å innhente og sammenstiller all relevant informasjon fra interne og eksterne kilder for beslutningsformål		↘
2	Systemer for beslutningsstøtte og rapportering henter relevant informasjon fra foretakets produksjonssystemer og sammenstiller og synkroniserer informasjonen til et bilde av foretakets risiko til bruk i styringsøyemed og til myndighetsrapportering.		↘
3	Systemene gir automatisk et totalbilde av risikoen, for eksempel slik at hvis en hjørnestensbedrift går konkurs, så varsler systemet automatisk om lån til ansatte i bedriften og lån til leverandører til bedriften, slik at vi kan vurdere å tapsavskrive på disse.		↘
4	Systemene identifiserer automatisk muligheter for mersalg.		↘
5	Datakvalitet		↘
6	Integrasjon og synkronisering mellom systemene		
7	Når nye IT-løsninger skal utvikles, tar vi i betraktning behovene og løsningene til alle relevante avdelinger. Dette for å unngå utfordringer forbundet med "silo-løsninger" slik som omfattende vedlikehold av programmer, komplisert drift og utfordringer med synkronisering av data.		↘
8	Grad av kompleksitet i IT-systemene		→
9	Grad av mangler og feil i systemene		→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet.		

Kilde: Finanstilsynet

En del foretak mener at det er høy risiko knyttet til mangel på kvalitet i dataene. Manglende datakvalitet kan føre til gale beslutninger.

Flere foretak mener at IT-systemene er komplekse. Manglende oversikt over sammenhenger i systemene gjør det vanskelig å forutse konsekvensene ved endringer i systemene. Dette er

sannsynligvis grunnen til at foretakene mener at det er feil og mangler i systemene, jf. nr. 9 i tabellen over.

4.1.2.2 Avvik i driften

Tabell 5: Avvik driften

	Sårbarhet	Foretakenes svar	Trend
1	Organisering, rutiner, stillingsbeskrivelse, rapportering og kontroll		↘
2	Grad av kompleksitet i driften		→
3	Test-systemene er "produksjonslike", dvs. at systemene har testdata, applikasjoner, programvare, styresystemer (SW) og annet som sikrer mot "overraskelser" når nye applikasjoner skal i produksjon.		↘
4	Vi gjør endringer i infrastrukturen ("ikke- funksjonelle" endringer) i trafikkstille perioder, og kan reversere endringen og rulle tilbake på kort tid hvis nødvendig.		→
5	Vår evne til å avdekke alle svakheter		↘
6	Kontroller som skal sikre at alle maskiner og programmer er inkludert i IDS/IDP, brannmur og virus og andre tiltak for å sikre stabil drift		→
7	"Tikkende miner", dvs. komponenter som gradvis slites eller verdier som gradvis når terskelverdien uten at vi er oppmerksom på det, for eksempel minnelekkasje, elektroniske komponenter som slites, energiforsyning som "slites" (batterier eller annet)		→
8	Logger og vår evne til å reagere på loggene		↘
9	Vår evne til å avdekke avvik i driftsmønsteret og ta aksjon før skade (avvik når det gjelder trafikkmønster, porter, protokoller, avvikende svarstider osv.)		↘
10	Dataangrep (Advanced persistence threat, trojaner, ransomware, DDoS)		→
11	Kvaliteten på kontinuitet- og katastrofeløsningene våre		↘
12	Samarbeidsrutiner med leverandører		→
13	Leveransepress		→
14	Kompetansen vi besitter		↘
15	Mengden av endringer (ny leverandør, nye grunnsystemer)		→
16	Vår kunnskap om hvor datalinjene går og redundans når det gjelder datalinjer		→
17	Tilgangskontroll, adgangskontroll og tjenestedeling ("segregation of duty")		→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet.		

Kilde: Finanstilsynet

Flere foretak ga uttrykk for at det er komplekst å drifte foretakets IKT-løsninger. Det er etter hvert svært mange tjenester som skal driftes, og forventningen er at tjenestene er tilgjengelige nærmest hele døgnet. Dette stiller store krav til kvalitet i driften, og det blir lite tilgjengelig tid til oppgradering og vedlikehold. Se også omtale under 4.1.1.2.

Flere foretak står foran større endringer når det gjelder leverandører av drifts- og/eller utviklingstjenester og markerer dette med høy risiko i besvarelsen.

Leveransepress synes å gi stor risiko for flere foretak. Den senere tid har vist at tjenester som har kommet på markedet, inneholder sikkerhetsfeil og mangler. Det kan tyde på et ikke ubetydelig press når det gjelder "time-to-market".

Dataangrep anses å være en betydelig risiko. Den senere tid har vist at spionasje og "ransomware" øker.

4.1.2.3 Data er ikke tilstrekkelig beskyttet

Tabell 6: Data er ikke tilstrekkelig beskyttet

	Sårbarhet	Foretakenes svar	Trend
1	Våre retningslinjer for klassifisering av informasjon og beskyttelse av informasjonen		→
2	Kvaliteten på våre tilgangskontroller		→
3	Våre systemer for logging		→
4	Mulig inntrenging i våre systemer		→
5	Sikring av data på bærbart utstyr (fjernsletting av mobildata osv.)		→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet.		

Kilde: Finanstilsynet

Beskyttelse av data er en økende utfordring. Nyere regler knyttet til personvern gjør området utfordrende. Flere foretak anser inntrenging i foretakets systemer som en stor risiko i relasjon til beskyttelse av data.

4.1.2.4 ID-tyveri

Tabell 7: ID-tyveri

	Sårbarhet	Foretakenes svar	Trend
1	Skadevare som infiserer en bruker og misbruker den infiserte brukeren sine rettigheter		→
2	Kontroll når det gjelder utlevering og bruk av logon-id og passord til kunder og medarbeidere (BankID, ansatte-id, systembrukere, admin-brukere)		→
3	Innsyn i kundedata		→
4	Kort ("Card not present, skimming")		→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet.		

Kilde: Finanstilsynet

Skadevare og misbruk av rettigheter i forbindelse med IT-tyveri anses som en stor risiko av flere foretak. Se også omtale under 4.1.1.1.

4.1.2.5 Misbruk av tilgang til datasystemene

Trussel når det gjelder misbruk omfatter at tilgang til datasystemene misbrukes for personlig vinning, for eksempel innsidehandel, ta penger fra foreningskontoer, interne kontoer eller fra kontoer med liten bevegelse.

Trussel knyttet til misbruk for innsidehandel er ikke ansett å være særlig høy.

Tabell 8: Misbruk av tilgang til datasystemene

	Sårbarhet	Foretakenes svar	Trend
1	Tilgangskontroll		→
2	Tjenestedeling		→
3	Logging		→
4	Markedsovervåking		→
5	Analyse av "mistenkelige" transaksjoner som tilbakevalutering, bevegelser på interne kontoer, overføring fra kunde til ansatt og tilbake		→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet.		

Kilde: Finanstilsynet

4.1.2.6 Hvitvasking

Flere foretak mener at det er utfordrende å lage systemer som har høy presisjon når det gjelder å flagge mistenkelig transaksjoner.

Tabell 9: Hvitvasking

	Sårbarhet	Foretakenes svar	Trend
1	Markedsovervåking		→
2	IT-systemenes evne til å samle informasjon om kunde, kunderelasjoner og kundeadferd (KYC– Know Your Customer)		→
3	Elektronisk overvåkning av transaksjoner – presisjon i flagging av mistenkelig transaksjoner		→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet.		

Kilde: Finanstilsynet

4.2 Risikoområder påpekt av sikkerhetsselskaper og internettjenesteleverandører (ISP)

4.2.1 Intervjuer

Høsten 2014 hadde Finanstilsynet samtaler med noen sentrale aktører for sikkerhetsløsninger og overvåking i Norge, og har omtalt de mest fremtredende trusselområdene tilsynet merket seg fra disse samtalene.

4.2.1.1 Lavt antall infiserte PC-er i Norge

Det er en generell nedgang i tradisjonelle virusangrep på verdensbasis, og Norge er et av de minst infiserte land når det gjelder PC-virus. Også DDoS-angrep har medført mindre konsekvenser det siste året. Det er likevel all grunn til å holde oppe forsvaret mot ondsinnede angrep fra nettet, ettersom feil her kan medføre alvorlige konsekvenser både for foretaket og kundene. Det kan være både direkte økonomiske tap, og tap av renommé og forretningsmuligheter.

Mindre konsekvenser fra DDoS-angrep skyldes at foretakene har fått på plass gode beskyttelses-mekanismer mot slike angrep. I Norge har det generelt vært lagt vekt på virusbeskyttelse overfor forbrukerne, og både software-, nettverks- og tjenesteleverandører har kommet med forbedret beskyttelse og lagt til rette for at forbrukerne holder sine PC-er oppdatert. Selv om infeksjonsraten er lav her til lands, er Java fortsatt dominerende blant infiserte systemer. Her er det fortsatt dårlig sikkerhet, selv om det har blitt vesentlig bedre de siste årene. BankIDs overgang bort fra Java er en stor forbedring for banksektoren.

Selv om det ikke har manifestert seg i Norge, er det internasjonalt registrert en utvikling, som for eksempel bruk av "reflection[27]"-angrep. Her benyttes svakheter/hull i blant annet NTP-tjenesten på en måte som gjør at DNS-servere kan forsterke angrepet. Slike angrep kan gjøres på en relativt enkel måte når angriperen først finner slike svakheter som også omtales på hackerfora på nettet.

Internettjenesteleverandører ("Internet Service Providers" – ISP-er) burde ta en mer aktiv rolle når det gjelder bekjempelse av DDoS og spam. Foretakene bør ta opp dette når de inngår avtaler om kjøp av tjenester fra disse leverandørene.

DDoS-angrep kan benyttes som avledning for andre typer nettangrep.

4.2.1.2 Advanced Persistent Threat (APT)

Advanced Persistent Threat (APT) oppleves som den største trusselen fra nettet, og her er det økning. Økningen har spesielt vært rettet mot avansert industri, men også finansinstitusjoner må være på vakt mot slike angrep. I 2014 har det helst vært større internasjonale banker som har vært målet innen finansområdet, siden man her får større "kundegrunnlag" for svindelen. Etter hvert som metodene raffineres, kan dette endres. Fremover er det ventet at små og mellomstore bedrifter (SMB-er) vil bli et viktig mål for kriminelle, ut fra en antakelse om at de har mindre omfattende sikkerhetstiltak. Dette gjelder også mindre foretak, som må påse at de har god sikring på sine lokale nettverk selv om hoveddelen av systemene er utkontraktert til eksterne leverandører og sikret av disse. Firmaer som aktivt følger markedet, registrerte i 2014 en økning fra 40 til 80 målrettede angrep i Norge.

For å komme inn i et foretak, skjer dette ofte ved tilgang gjennom ansattes PC-er. Det gjøres enklest ved "brukermedvirkning" ved at den ansatte har klikket på lenke, latt seg lure til å åpne et vedlegg,

[27] NTP-tjenesten sender synkroniseringsmeldinger til enheter eller servere i lokalnettet. Angriperen sender en melding til denne tjenestern, og benytter denne til å sende meldingen videre til aktuelle enheter og servere, slik at angrepet forsterkes.

eller svart på en phishing-e-post. Brukermedvirkning finnes i nesten 50 prosent av tilfellene der slik inntrenging er påvist. Her er bevisstgjøring av ansatte det viktigste mottiltaket, noe som både krever opplæring, holdningsskapende arbeid og tester. Kriminelle utnytter også utro tjenere som kan være rekruttert både ved fristelser og ved bruk av trusler.

Etter å ha kommet seg inn på en PC koblet til intranettet, vil angriper lete etter "sikre" steder å parkere skadevaren. Det er enheter som blir mindre overvåket, eller ikke overvåket. Foretaket må derfor sikre at skadevarebeskyttelsen også kan kontrollere alle tilkoblede enheter, for eksempel skrivere. "Internet of Things" kommer mer og mer inn i nettene til foretakene, og alle enheter som kobles opp i foretakenes nettverk, må sikres.

Oppbygging av bransjevise CERT-er er et godt bidrag til forsvar mot nettangrep. Det er likevel ønskelig med bedre samarbeid mellom de ulike sektorene på dette området, siden man har mye å lære av hverandre. Et utvidet samarbeid mellom alle parter (myndigheter, politi, ISP-er, eiere av internettsider og sikkerhetsaktører) vil trolig gi forbedringer. Det viser seg at land med myndigheter som er bevisste på disse truslene og legger vekt på sikkerhet, har generelt lav infeksjonsrate.

4.2.1.3 Mobiltelefoner – smarttelefoner og nettbrett smelter sammen

Mobile enheter som smarttelefoner og nettbrett er i seg selv ganske sikre. Applikasjonen kjører i "sandbox", som hindrer at en applikasjon infiltrerer eller henter data fra andre applikasjoner. Merk likevel at dette krever at utviklerne er kompetente og følger et strengt sikkerhetsopplegg.

Det er en allmenn oppfatning at skadevare kommer ca. fem år senere på mobiler enn på PC-er. Det er likevel ikke kjente tilfeller av skadevare i Norge, men internasjonalt er det sterk utvikling i skadevare for Android- og Windows-telefoner. Apple har et strengere regime for applikasjoner, og er foreløpig mindre utsatt for skadevare. Smarttelefoner og nettbrett nærmer seg i operativsystemer og funksjoner. Også i størrelse er det en viss tilnærming.

4.2.1.4 Foretakene må sikre at informasjon ikke kommer på avveie

For å unngå svindel er det viktig at sensitiv informasjon ikke kommer på avveie. Uaktsomhet fra ansatte kan føre til slike lekkasjer, også uten at den ansatte er klar over det. Mange foretak prioriterer å få produktene sine raskt ut på markedet, og enkelte utviklingsgrupper har ikke alltid prioritert sikkerhet. Ansatte i foretaket kan da søke etter enkle måter å dele informasjon på, og å ta med arbeid hjem. Her er enkle skytjenester tilgjengelige på en måte som gjør at en medarbeider eller gruppe enkelt kan ta disse i bruk uten at det er klarert med foretakets sikkerhetsansvarlige, noe som fort kan medføre at informasjon eksponeres for uvedkommende.

Sikkerhetsansvarlige kan ha ensidig vektlegging av prosess uten å jobbe med praktisk implementering. Selv godt dokumenterte prosesser må etterprøves praktisk med testing, og for nettsikkerhet bør penetrasjonstester utføres. Prosesser og løsninger er ikke troverdige før de er testet, og slik testing bør gjøres regelmessig. Foretaket må også ha øvd på planer for hva som skal gjøres hvis det skulle bli utsatt for et angrep, eller at data er kommet på avveier. Innen dette området er det behov for en

kombinasjon av sikkerhetskunnskap og nettverkskompetanse for å se sammenhenger og designe gode løsninger. Personell som kombinerer disse kunnskapsområdene, er en knapphetsfaktor for mange foretak. Heller ikke utdanningsinstitusjonene tilbyr en slik kombinasjon i sine kursopplegg. Her må foretakene ofte selv sørge for opplæring. Enkelte har god erfaring med at det er hensiktsmessig å ta utgangspunkt i god nettverkskompetanse, og så bygge på med sikkerhetskompetanse.

Dagens tilgangsløsninger autoriserer på lagringssted eller domener. Disse "lagerplassene" holder store mengder data, og den enkelte bruker får dermed oftest tilgang til mer data enn nødvendig, eller til data som burde vært skjermet for vedkommende bruker. Nettverkstopografien er vesentlig for sikkerheten. Foretakene må ha en oppdeling som er slik at autorisasjon kan gis på hensiktsmessige områder/måter.

Det kommer nå lagringssystemer/tilgangssystemer som tar utgangspunkt i hvem som trenger hva, og så er det systemet som henter autoriserte data frem uten at bruker skal ha et forhold til lagringsområdet og hvordan dette er organisert, eller hvor det befinner seg.

Sikkerhetsatferd er viktig. 80–20-regelen kan benyttes i fordeling mellom menneskelige og teknologiske svakheter. Det er viktig at alle ansatte har god sikkerhetsforståelse og er bevisst om trusler fra Internett. Opplæring og bevisstgjøring må bli faste poster i foretakenes årsplaner.

4.2.1.5 Utarming av IKT-kompetanse hos finansforetakene

Det har tradisjonelt vært stor bruk av utkontraktering i norsk finansnæring. Likevel er det nå en tendens til at stadig mer av IKT-oppgavene utkontrakteres, og i større grad enn tidligere skjer det til utenlandske foretak. Samtidig blir tjenesteytere som tidligere var eid av foretakene eller innenlandske interesser, solgt til utenlandske (ikke-industrielle) eiere. Utviklingen setter IKT-kompetansen både i foretakene og i Norge under press.

I undersøkelser av store industriprosjekter blir det påpekt nødvendighet både av tilgang til fagkompetanse og innkjøpskompetanse, og manglende kompetanse på dette feltet hos utbyggerne har medført store overskridelser. Hvis den interne kompetansen utarmes, vil en også bli mindre i stand til å stille de rette kravene til leverandørene, og også kontrollen med leveransene vil kunne bli mangelfull. I prosjektsammenheng er det fare for at det blir stilt krav til kjøper som vedkommende ikke er i stand til å oppfylle, for eksempel krav til funksjonsspesifikasjoner, testkrav og andre ressurskrav. Resultatet kan bli at utkontrakteringen blir dyrere enn utførelse i egen regi, og at foretakets handlingsrom og evne til markedstilpasning blir negativt påvirket.

4.2.2 Rapporter fra sikkerhetsorganisasjoner

Finanstilsynet vil fremheve de mest typiske sårbarhetene som er relevante for finanssektoren, slik større internasjonale sikkerhetsselskaper som ENISA[28], som jobber tett med EU-institusjoner som den europeiske banktilsynsmyndigheten (EBA), den europeiske verdipapir- og markedstilsynsmyndigheten

[28] EUs enhet for nettverks- og informasjonssikkerhet, og som jobber for EU-institusjoner og medlemslandene.

(ESMA) og den europeiske tilsynsmyndigheten for forsikring og tjenestepensjon (EIOPA), og Cisco, som stor teknologileverandør til finansbransjen, vurderer dette.

4.2.2.1 ENISA Threat Landscape 2014

Ifølge ENISAs rapport "Threat Landscape 2014" har det vært mange positive signaler om bekjempelse av cyberkriminalitet i løpet av 2014. Nedstenging av sentrale "botnet" og arrestasjonen av utviklerne av Blackhole førte til en markant nedgang i angrep relatert til bruken av sammenstillingen av botnet og Blackhole-kode. I fremstillingen under viser ENISA endring i omfang for ulike trusseltyper, samt rangering av alvorlighetsgrad og endring i rangeringen fra året før.

Tabell 10: Oversikt over og sammenligning av trussellandskapet i 2013 og 2014

Top Threats 2013	Assessed Trends 2013	Top Threats 2014	Assessed Trends 2014	Change in ranking
1. Drive-by downloads (renamed to Web-based attacks)	↑	1. Malicious code: Worms/Trojans	↑	↑
2. Worms/Trojans	↑	2. Web-based attacks	↑	↓
3. Code Injection	↑	3. Web application /Injection attacks	↑	→
4. Exploit Kits	↑	4. Botnets	↓	↑
5. Botnets	→	5. Denial of service	↑	↑
6. Physical Damage/Theft/Loss	↑	6. Spam	↓	↑
7. Identify Theft/Fraud	↑	7. Phishing	↑	↑
8. Denial of Service	↑	8. Exploit kits	↓	↓
9. Phishing	↑	9. Data breaches	↑	↑
10. Spam	→	10. Physical damage/theft /loss	↑	↓
11. Rogueware/Ransomware / Scareware	↑	11. Insider threat	→	(NA. new threat)
12. Data Breaches	↑	12. Information leakage	↑	↑
13. Information Leakage	↑	13. Identity theft/fraud	↑	↓
14. Targeted Attacks (renamed to Cyber espionage, merged with Watering Hole)	↑	14. Cyber espionage	↑	→
15. Watering Hole (threat consolidated with other threats/attack vector)	↑	15. Ransomware/Rogueware/ Scareware	↓	↓

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Table 2: Overview and comparison of Current Threat Landscapes 2014 and 2013

Kilde: ENISA[29]

I 2014 var det stor økning i datainnbrudd, og ifølge ENISAs rapporteringssystem har datainnbrudd økt i frekvens med 25 prosent siste året. Innbruddene har i stor grad hatt som formål å hente ut kundedata eller annen forretningskritisk informasjon fra foretakene. Måten datainnbruddene er gjennomført på, er ulike. Et eksempel kan være at foretakene har dårlig passordkvalitet, som relativt enkelt gjør det mulig

[29] ENISA Threat Landscape 2014

at uautoriserte kan komme inn i et foretaks datasystemer. Det kan være sårbare nettverk, ikke oppdatert standard programvare eller sårbare applikasjoner.

En undersøkelse viste at mer enn 50 prosent av datainnbruddene skyldtes manglende sikkerhet i sluttbrukerleddet. Det er ofte der phishing og skadevare kan gjøre størst skade.

I 2014 var det stadig mer sofistikerte angrep og stadig stigende kvalitet på rettede angrep.

4.2.2.2 Cisco – Annual Security Report 2015

Ciscos sikkerhetsrapport tar for seg det pågående kappløpet mellom angripere og forsvarere, sikkerhetsselskaper og -funksjoner i foretakene, og hvordan brukerne stadig blir et svakere ledd i sikkerhetskjeden.

Noen hovedtrekk:

- I 2014 ble kun én prosent av kjente sikkerhetshull aktivt utnyttet til cyberkriminalitet.
- Selv om man benytter de beste sikkerhetssystemene, må man fortsatt sørge for at kvaliteten i prosessene for overvåking og tiltakene mot sårbarheter er god.
- Kjente sårbarheter i Java ble redusert med 34 prosent i 2014.
- Spam-volumet økte med 250 prosent fra januar til november 2014.
- Sikkerhetshullet i SSL-protokollen som ble omtalt som "Heartbleed", representerer i et globalt perspektiv fortsatt en stor risiko. Cisco melder at 56 prosent av alle SSL-installasjoner fortsatt ikke er oppgradert.
- Skadevareutviklere benytter nå tilleggsfunksjoner på nettleser til å distribuere kode, noe som til nå har vært effektivt fordi brukere ikke tenker på dette som en risiko.

4.2.2.3 Finanstilsynets oppsummering

Basert på blant annet rapportene nevnt over, er det Finanstilsynets oppfatning at trusselen fra cyberangrep øker ved at verktøyene som benyttes, blir mer sofistikerte og at metodene som benyttes, blir mer varierte. Angrepene som gjøres, er målrettede og utføres ofte av organisasjoner som baserer forretningsdriften sin på kriminell virksomhet. Denne typen organisasjoner har gjerne tilgang til ressurser med stor kunnskap innenfor IKT-området, nødvendig datakapasitet og god tilgang på finansiering av virksomheten.

5 Utviklingstrekk

Finanstilsynet vil her trekke frem utviklingstrekk som vil få, eller som antas å kunne få betydning for foretakenes bruk at IKT og medføre endringer i risiko- og sårbarhetsforhold både for foretakene, for forbrukerne og for finansiell stabilitet.

5.1 Digital kriminalitet

Cyberkriminalitet og IT-sikkerhet vies stadig mer oppmerksomhet nasjonalt og internasjonalt i tråd med den økende utviklingen i IKT- og internettbasert kriminalitet. EBA vurderer den operasjonelle risikoen knyttet til foretakenes bruk av IKT som høy, og den forventes å være høy fremover[30]. Det samme gjør også EIOPA og ESMA.

EBA gir klare anbefalinger om at finansinstitusjonene må gi økt prioritet til IT-relaterte risikoer og forsterke IKT-kontroller og -gjennomganger, og de må dekke alle deler av verdikjeden (for eksempel IKT-tjenesteleverandører og tredjepartsleverandører). EBA ber også nasjonale tilsynsmyndigheter sørge for at banker, forsikringsselskaper, investorer og andre aktører avsetter tilstrekkelige ressurser og viser den nødvendig aktsomheten for en forsvarlig forvaltning av sine digitale miljøer og sikrer mot kriminelle digitale angrep.

Målrettet angrep mot norske bedrifter økte i 2014, og finanssektoren var en av flere utsatte sektorer. Målrettet phishing i kombinasjon med APT og andre metoder brukes for å komme på innsiden av bedriftens nettverk for å hente ut informasjon. Et scenario som illustrerer metodene, er angrepene kjent under navnene Carbanak eller Anunak, som spesielt rammet russiske banker i 2014. Angrepene førte til store tap[31].

Det finnes resolusjoner og samarbeidsavtaler gjennom FN og i regional regi (EU, APEC, ASEAN m.fl.) samt Interpol-samarbeidet. Utfordringen er nasjonalstater som ikke er med i samarbeidene og at løsninger med kriminelle hensikter raskt kan flyttes til liberale steder, som land med mangelfullt lovverk på området, for å unngå vanskeligheter.

Det er en økende utfordring å definere et fysisk sted for systemer og data, spesielt etter inntoget av

[30] Se kapittel 7.2. https://www.eba.europa.eu/documents/10180/934862/EBA+2014.6941+RAR+web.pdf
[31] Angrepsscenariene er grundig beskrevet og dokumentert både av Kaspersky og FoxIT: https://www.fox-it.com/en/press-releases/anunak-aka-carbanak-update/

skybaserte systemer. Data kan være mange steder samtidig, og avgjørelsen for hvilke rettsregler som benyttes, problematiseres. Cyberkriminalitet er et internasjonalt problem som blir gjort mulig av nasjonalstater som ikke har lovverk og/eller utøvende makt til å håndheve et lovverk for dette området, eller selv tar del i dette.

Potensialet for cyberkriminalitet vil øke med fremveksten av sammenkoblinger av "objekter" med sensorer og styresystemer ("Internet of Things") gjennom Internett. Teoretisk vil man nå alle "objekter" fra et hvilket som helst sted i "cyberspace", kun begrenset av kvaliteten på objektets sikkerhetssystemer og rutiner.

5.2 Endringer i tjenesteleverandørmarkedet, organisering og eierskap og utkontrakteringslandskapet

I 2014 skjedde det store endringer både når det gjelder eierforhold hos viktige tjenesteleverandør til finanssektoren og ved valg av leverandører (utkontrakteringspartnere) hos noen av finansforetakene. Det er redegjort for endringene nedenfor.

Finanstilsynet har ikke rangert tjenestetilbyderne etter dyktighet, produkttilbud eller sikkerhet. Tilsynet er opptatt av at tilbyderne følger lover og forskrifter og tilbyr sikre tjenester i henhold til beste praksis. Vurdering utover dette er et ansvar for foretakene som setter ut sine tjenester. Tilbyderne er likevel ulike, og det er viktig at foretakene i en slik prosess får med seg mulige nye fordeler. Riktig utført kan derfor et bytte også tilføre forbedringer på ulike områder, både funksjonelt og sikkerhetsmessig.

Leverandørbytte betyr at foretaket får nye kontraktpartnere. Det er da viktig at foretaket forhandler inn moderne og feiltolerant infrastruktur, og sørger for at det er mulighet for senere endringer slik at foretaket får ta del i den tekniske utviklingen som fortsatt forventes å komme.

Nye driftsleverandører medfører spredning av risiko for samtidige driftshendelser, og minsker derved konsentrasjonsrisikoen som foretaket har hatt ved et fåtall sentrale leverandører. Dette kan være en styrke ved at kunden i en feilsituasjon har mulighet til å få tjenester utført hos en alternativ leverandør.

I forbindelse med salg/eierbytte hos tjenesteleverandørene er det viktig at etablerte kontakter og samarbeidsrutiner også blir ivaretatt, og at avtaler mellom selskapene også forankres hos nye eiere. Primært er det foretakene som utkontrakterer oppgaver, som må se til at dette blir fulgt opp.

Erfaringsmessig er endringer og flyttinger en betydelig kilde til feil. Foretakene må i forbindelse med disse endringene nøye følge opp med tilpasning i rutiner og tester av nye løsninger og konfigurasjoner.

Det er ikke klart hva disse endringene vil få av konkret betydning for foretakenes kompetanse og styring av IT-virksomheten, eller for kompetansen på banksystemer som helhet i Norge. Finanstilsynet er bekymret for at utkontraktering til utenlandske foretak kan utarme norsk kompetanse på IT-

løsninger til finanssektoren.

Nets er en betydelig og sentral leverandør innenfor norsk betalingsformidling. Tjenestene omfatter både felles operasjonell infrastruktur (FOI) som NICS, BankAxept og BankID og tjenester på kontrakter med enkeltforetak (for eksempel faktureringstjenester og minibanktjenester). Nets er markedsdominerende på betalingstjenester, og foretaket er systemkritisk for slike tjenester i Norge. Nets er også en sentral aktør for betalingstjenester i Danmark.

Bankene solgte Nets til et internasjonalt konsortium bestående av Advent International[32], Bain Capital[33] og ATP[34]. Det har hittil medført noen endringer i styre og ledelse, men ingen flyttinger av viktige driftsoppgaver.

Evry er gjennom oppkjøp og fusjoner blitt en dominerende leverandør til norske banker, og er også stor innenfor andre industrier. Flere sparebanker fornyet i 2014 sine avtaler med Evry. De bankene som ikke benytter Evry, har utkontraktert driften til utenlandske aktører. Eierne i Evry ga høsten 2014 signaler om at selskapet ble vurdert solgt. I desember 2014 ble det annonsert en intensjonsavtale med Lyngen Bidco AS, som indirekte kontrolleres av Apax Partners LLP.

Evry har, uavhengig av eiere, vedtatt å flytte driften til et nytt datasenter, Greenfield Data Center på Fet, som er under oppbygging. Flytteprosjektet vil starte i 2015.

Storebrand Bank har flyttet driften til SDC i Danmark. Det var en del driftsforstyrrelser med nettbanken i en overgangsperiode.

Sandnes Sparebank besluttet høsten 2014 å gå inn i Eika Alliansen, og planlegger å flytte IT-driften til SDC.

DNB valgte i 2013 HCL som ny driftspartner for drift av desentral plattform. Serverne flyttes til datasenteret Green Mountain. Tata Consulting Services er leverandør av forvaltnings- og utviklingstjenester. Flytteprosessen pågår. Mainframe driftes fortsatt av Evry.

Nordea har innkontraktert sine "midrange"-systemer (blant annet minimaskiner og servere) fra Nordic Prosessor. Flytteprosessen pågår.

[32] Advent International er et amerikansk globalt "private equity"-selskap med vekt på oppkjøp av selskaper i Vest- og Sentral-Europa, Nord-Amerika, Latin-Amerika og Asia.
[33] Bain Capital er et globalt verdipapirforetak med base i Boston, Massachusetts. Det har spesialisert seg på blant annet "private equity", "venture kapital" og kredittprodukter**.**
[34] ATP er det danske pensjonsfondet.

5.3 Utviklingstrekk innen betalingsformidling

Som omtalt i kapittel 3.2 påvirker teknologiutviklingen i vesentlig grad utviklingen av betalingstjenester og betalingssystemer gjennom foretakenes bruk av teknologi, at nye aktører etablerer seg, eller ved inntreden av utenlandske aktører.

Særlig skjer denne utviklingen innenfor mobilbaserte betalingstjenester, men også innenfor utviklingen i sikkerhetsløsninger, hvor utviklingen i teknologi åpner for utvikling av mer effektive og brukervennlige tjenester. Teknologien gir også mulighet for samtidig å gjøre tjenestene mer sikre i bruk, men trusselbildet øker også i takt med utbredelsen. Et av de største vekstområdene innenfor skadevare er nå innenfor mobiltelefoni, og det antas at dette bare vil øke i takt med at mobiltelefonen i stadig større grad tas i bruk for daglige aktiviteter. Det blir viktig å etablere løsninger som antivirus og anti-phishing for "proaktiv sikkerhet", og ikke bare reaktiv sikkerhet som "sandbox" gir. Det er forventet en fortsatt høy utviklingstakt innenfor mobile betalingsløsninger i de kommende årene.

Bruk av QR-koder[35] slik mCASH gjør i sin mobile betalingsløsning, er et eksempel på hvordan ny teknologi er tatt i bruk i mobile betalingsløsninger, og skanning av QR-koder er benyttet i stedet for NFC.

Også store internasjonale aktører etablerer seg i Norge etter hvert som konkurransearenaen er blitt mer åpen, hovedsakelig som filialer eller via agentvirksomhet eller samarbeid med eksisterende aktører. Eksempel på dette er Visa med sin paneuropeiske mobile digitale lommebok V.me, hvor de sammen med partnere startet testing (pilot)[36] i Norge i slutten av 2014 og har planer om lansering i slutten av 2015[37].

Eika Gruppen er allerede godt etablert med sin løsning for kontaktløse kort, "swipe and go"[38], og vil starte testing av sin mobile løsning for kontaktløs betaling i begynnelsen av 2015[39]. Også BankAxept, som er det dominerende betalingskortet i Norge, vil komme med løsning for kontaktløs betaling i 2015.[40]

Innenfor kort og sikkerhet skjer det også endringer. Zwipe[41] lanserte høsten 2014 sitt samarbeid med Mastercard sammen med pilotprosjektet Sparebanken Din. Dette er en prototype for identifisering via fingeravtrykk for kontaktløse betalingskort, og det forventes kommersiell lansering i markedet i løpet av 2015. Her erstattes pinkoden med biometriske data lagret direkte på kortet. Etter hvert må det forventes at teknologien også vil bli implementert for mobil bruk.

Det antas at andre aktører fremover vil forsøke å etablere seg i det norske markedet med sine

[35] QR-kode (Quick Response code) er en todimensjonal strekkode, http://no.wikipedia.org/wiki/QR-kode
[36] http://www.visaeurope.com/newsroom/news/vme-pilots-in-4-new-european-markets
[37] http://annualreport.visaeurope.com/
[38] https://eika.no/om-oss/kontaklosbetaling
[39] http://www.aftenposten.no/digital/Kampen-om-mobilbetaling-hardner-til-7721564.html
[40] https://www.fno.no/contentassets/9f9e2dc2b5a4464ea0b60ac1ba451cd6/oyvind-apelland--bankaxept-as.pdf
[41] http://www.tek.no/artikler/dette-norskutviklede-betalingskortet-gjor-pinkoder-til-en-saga-blott/164531

løsninger, og aktører med stor dominans i markedet kan fort skape store endringer i landskapet. Når det reviderte betalingstjenestedirektivet trer i kraft, vil det redusere etableringshindringer som tilgang til betalingskonto og gjøre etableringen for nye betalingstjenesteaktører lettere. Samtidig vil slike endringer skape nye risiko- og sårbarheter ved betalingsformidling som må håndteres.

Mobile løsninger vil få en betydelig rolle innenfor betalingsformidlingen, både som medium for gjennomføring av betalinger, som bærer av digitale lommebøker og som bærer av sikkerhetsløsninger. Når kontaktløs kortbetaling og kontaktløs mobil betaling vil bli dominerende, vil i stor grad avhenge av betalingsmottakernes implementering av nødvendig teknologi.

Brukervennlighet, enkelhet og hastighet synes å være dominerende i kampen om det mobile betalingstjenestemarkedet. Det er en fare for at denne vektleggingen kan medføre at vektleggingen av sikkerhet kan bli skadelidende.

Finanstilsynet mener det er viktig at foretakene stiller minst samme krav til sikkerhet for mobile betalingsløsninger som for de tradisjonelle nettbankløsningene, det vil si at de gjør grundige sikkerhets- og sårbarhetsanalyser, iverksetter tiltak og tar grep for å kvalitetssikre sine utviklingsprosesser og sikrer at sensitiv informasjon ikke fraktes over nettet og beskyttes på en tilstrekkelig måte. Det er viktig at foretakene gjør risiko- og sårbarhetsvurderinger av hele verdikjeden, inklusive lagring av informasjon. Sårbarheten er knyttet til verdikjeden, som til selve mobilapplikasjonen, noe en hendelse i USA-baserte CHARGE Anywhere LLC[42] viser tydelig.

For å møte disse utfordringene har Finanstilsynet under utarbeidelse en forskrift til lov om betalingssystemer som stiller krav til gjennomføring av risiko- og sårbarhetsanalyser. Det foreslås en rekke krav til sikkerhet.

Finanstilsynet utarbeidet i 2014 et eget egenevalueringsskjema for mobilbank[43] basert på Cobit for bruk i tilsynssammenheng og som foretakene selv kan benytte for å vurdere IKT-virksomheten sin knyttet til mobile løsninger og mobile betalingstjenester.

5.4 Endringer i norsk regelverk

5.4.1 Regulering av utkontraktering

I 2014 var det flere lovendringer som regulerte forhold knyttet til utkontraktering. Fra 1. juli 2014 trådte en ny hjemmel § 2-17a i finansvirksomhetsloven i kraft som regulerer hvilke oppgaver som kan/ikke kan utkontrakteres, og at bruk av oppdragstaker ikke fratar foretaket ansvaret for virksomheten som utkontrakteres. Fra samme dato trådte det også i kraft en ny hjemmel § 4c i finanstilsynsloven som regulerer meldeplikt til Finanstilsynet 60 dager før iverksettelse av avtale om

[42] http://www.itgovernanceusa.com/blog/electronic-payment-company-charge-anywhere-suffers-five-year-breach/?utm_source=Email&utm_medium=Macro&utm_campaign=S01&utm_content=2014-12-12
[43] http://www.finanstilsynet.no/no/Tverrgaende-temasider/IT-tilsyn/Egenevalueringssporsmal/

utkontraktering, og Finanstilsynets rett til å gripe inn i den planlagte utkontrakteringen. En ny forskrift ble deretter sendt på høring som regulerer unntak fra denne meldeplikten når det gjelder type finansforetak og virksomhet som skal utkontrakteres. Forskriften vil tre i kraft i 2015.

5.4.2 Endringer i og nye forskrifter

For IKT spesielt er det også planlagt endringer i IKT-forskriften som stiller krav til at avtaler om utkontraktering og endringer i slike avtaler skal behandles av styret. Inkassoselskaper som i dag ikke er pålagt hendelsesrapportering, vil bli pålagt dette. I tillegg planlegges en ny forskrift til lov om betalingssystemer som stiller krav om å gjennomføre risiko- og sårbarhetsanalyser, som en del av beslutningsgrunnlaget, før en ny betalingstjeneste lanseres og ved hendelser eller endringer av betydning for sikkerhetsnivået. Finanstilsynet vil sende regelendringene på høring i 2015.

5.4.3 Regelverksendringer på forsikringsområdet

Som nevnt i kapittel 3.5.3, har det gjennom flere år vært store regelverksendringer når det gjelder kollektiv tjenestepensjon. Dette omfatter både regelverksendringer som er trådt i kraft, som ny lov om tjenestepensjon og hvor pensjonsinnretningene arbeider med å tilpasse seg de nye endringene, og regelverksendringer som vil komme, som lovforslag om ny uførepensjon i skattefavoriserte private tjenestepensjonsordninger og ny form for ytelsesbasert alderspensjon tilpasset ny folketrygd. Regelverksendringene pågår fortsatt og medfører betydelig IKT-arbeid for pensjonsinnretningene. Som kapittel 3.5.3 viser, medfører endringer økt risiko, og samlet sett utgjør endringene en ikke ubetydelig risiko, som selskapene må håndtere.

5.4.4 Regelverksendringer på verdipapirområdet

Den amerikanske lovgivningen Foreign Account Tax Compliance Act (FATCA) vil generere endringer og nye systemløsninger. FATCA er en avtale mellom USAs skattemyndigheter og Finansdepartementet om utlevering av informasjon om amerikanske skattepliktige med kundeforhold til norske finansinstitusjoner.

5.5 Samordning og endringer i EUs regelverk

I løpet av 2014 var det en rekke prosesser under EU knyttet til forslag til nye, eller endring i eksisterende direktiver, forordninger, tekniske standarder og veiledninger som vil få betydning for norske forhold etter hvert som de blir tatt inn i norsk lovgivning.

Endringene er omfattende og representerer således en potensiell compliance-risiko. Endringer i systemporteføljen er generelt en betydelig kilde til feil. Omfattende regelverksendringer vil derfor medføre en risiko som foretakene må forebygge.

Forslagene kan også medføre endringer i ansvars- og risikoforhold mellom aktørene i verdikjeden innen betalingsformidling, og de kan introdusere nye risikoer. En uønsket konsekvens kan være at

kunder opplever redusert trygghet ved bruk av betalingstjenester, som igjen gir seg utslag i redusert tillit.

5.5.1 Nettverk og informasjonssikkerhet

Det har pågått omfattende og krevende diskusjoner i EU knyttet til flere av områdene i det foreslåtte direktivet for nettverks- og informasjonssikkerhet (NIS-direktivet)[44]. Det har skapt store utfordringer for fremdriften, og forhandlingene om det foreslåtte NIS-direktivet vil fortsette i 2015. Finanssektoren er en av flere sektorer som vil bli omfattet og påvirket. Temaet ble omtalt i Finanstilsynets ROS-rapport for 2013.

5.5.2 Betalingsformidling

På området betalingsformidling var det i 2014 en omfattende prosess med å ferdigstille det nye betalingstjenestedirektivet (PSD2)[45]. Dette arbeidet er ennå ikke helt sluttført, men er nå i sluttfasen da enigheten som ble oppnådd i Europarådet i slutten av november, gir grunnlag for oppstart av forhandlinger med Europaparlamentet. Det ene nye vesentlige området i direktivet omhandler tilbydere av betalingsinitiering og kontoinformasjon og deres rett til på vegne av den som betaler, å initiere betalinger og innhente kontoinformasjon. Det andre vesentlige området er krav til styring av operasjonell- og sikkerhetsrisiko knyttet til betalingsløsninger og krav til autentisering, der tidligere henvisninger til NIS-direktivet nå er erstattet med lovtekst i direktivet. EBA er tillagt et ansvar for å utarbeide nærmere retningslinjer for flere av direktivets områder.

Tilsvarende prosess har pågått for å ferdigstille reguleringen av formidlingsgebyrer for kortbaserte betalinger, den såkalte MIF-forordningen[46]. I desember 2014 ble det inngått kompromiss mellom Europaparlamentet og Europarådet, og formelt vedtak forventes i løpet av våren 2015. Det vil blant annet bety krav til tak på formidlingsgebyrer, krav til at kortordninger ("card schemes") skal separeres fra behandlingen av kortbetalingene og krav knyttet til co-branding (felles markedsføring) av kort.

Direktivet og forordningen ble begge omtalt i Finanstilsynets ROS-rapport 2013.

Under EBA er det etablert en arbeidsgruppe hvor Finanstilsynet deltar.
Arbeidsgruppen har mandat til å:

- utarbeide retningslinjer i tilknytning til den foreslåtte revisjonen av PSD2, blant annet retningslinjer for sikkerhet, retningslinjer for rapportering av hendelser og retningslinjer for melding fra et EØS-land (hjemland) til et annet om tillatelse for et foretak til å drive virksomhet i det andre EØS-landet basert på tillatelse gitt i hjemlandet.
- identifisere eventuelle risikoer som kan oppstå fra innovative betalingstjenester og som ikke er adressert i noen av de eksisterende eller foreslåtte direktivene, og der det er påkrevd å utarbeide retningslinjer eller anbefalinger for å håndtere disse.

[44] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf
[45] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ecofin/146078.pdf
[46] http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%205119%202015%20INIT

- utarbeide retningslinjer for sikkerhet for internettbaserte betalinger[47], med basis i de publiserte anbefalingene fra SecuRe Pay[48]. Disse ble vedtatt i desember 2014 og vil gjelde fra 1. august 2015.
- gjennomføre mandater gitt i den vedtatte MIF-forordningen, blant annet tekniske standarder for separasjon av kortordninger fra behandling av kortbetalingene.

EU-forordning som forlenger bankenes frist for overgang til kredittoverføringer og direkte debiteringer i euro, inkludert fullføring av overgangen til SEPA (Single Euro Payments Area), ble vedtatt innlemmet i EØS-avtalen 12. desember 2014. Innlemmelsen krever norsk lovendring og trer derfor først i kraft etter at dette er gjort. SEPA Direct Debit er en felles europeisk betalingsløsning for direkte debitering i euro, og vil på sikt kunne medføre endringer i nasjonale betalingsløsninger, som for eksempel avtalegiro og autogiro.

5.5.3 Forordning om elektronisk identifikasjon og tillitstjenester

Formålet med forordningen er å legge til rette for økt elektronisk samhandling, ved gjensidig aksept av løsninger for elektronisk identifikasjon (eID) og elektronisk signatur og andre tillitstjenester på tvers av landegrensene i EU/EØS. Dagens nasjonale regler er ikke harmoniserte og utgjør en barriere. Forordningen ble vedtatt i 2014, og nå arbeides det med regelverk for innføring som forventes besluttet i EUs organer i løpet av våren/høsten 2015. Fra nasjonalt hold er det uttrykt en bekymring for kriminalitetsbildet og samfunnssikkerheten i Norge hvis krav til aksept av sikkerhetsnivåer, som en følge av forordningen, settes for lavt og Norge selv ikke skal kunne bestemme nivået.

5.5.4 Bank

Single Supervisory Mechanism (SSM) ble etablert i november 2014 og består av ECB og nasjonale tilsynsmyndigheter i eurosonen. Gjennom SSM får Den europeiske sentralbanken (ECB) ansvar for tilsyn med de største bankene i eurosonen. Land som ikke er medlemmer i eurosamarbeidet, kan også velge å delta, men står foreløpig utenfor.

Det mest sentrale regelverket på bankområdet er CRD IV (Capital Requirements Directive – nytt kapitaldekningsregelverk), som trådte i kraft fra januar 2014. Regelverket innebærer ny omfattende rapportering med trolig behov for betydelige IKT-tilpasninger. Fra januar 2015 trådte krisehåndteringsdirektivet (BRRD) i kraft i EU med felles regler for håndtering av banker i krise. Alle banker skal utarbeide gjenopprettingsplaner med konkrete og gjennomførbare tiltak for håndtering av finansielle krisesituasjoner.

[47] https://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments
[48] https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf

5.5.5 Verdipapirområdet

Ny regulering for verdipapirvirksomheten i den finansielle infrastrukturen i Europa vil i løpet av de neste årene ha betydelig innvirkning på de norske verdipapirforetakene og den tilhørende infrastrukturen. De nye reglene må ventes å kreve mange systemtilpasninger og betydelige investeringer i utviklingen av nye løsninger. Implementeringstiden er ofte kort. Korte tidsfrister vil kunne sette betydelig press på utvikling av løsningsspesifikasjonene og de tilhørende løsningene. I tillegg vil det kreve betydelig ressursbruk i verdipapirforetakene for testing og implementering. Forsinkelser kan derfor lett oppstå, og resultatet kan bli en tidspresset utvikling slik at løsningene får feil og mangler.

Eksempler på de kommende reguleringsendringene i EU er EMIR (European Market Infrastructure Regulation) og MiFID II (Market in Financial Instruments Directive – nytt investeringstjeneste-direktiv). Disse endringene vil medføre nye rapporteringskrav for foretakene med utfordringer knyttet til felleseuropeisk løsningsvalg og trolig betydelig arbeid med tilhørende lokale tilpasninger. Videre vil det også komme nye rapporteringskrav ved shortsalg.

Verdipapirforetakene vil med MiFID II få flere plikter til å innrapportere data. Et av de mest utfordrende kravene vil sannsynligvis være at alle transaksjonsdata for finansielle instrumenter skal innrapporteres til det eksisterende transaksjonsrapporteringssystemet (TRS). Rapporteringen skal foretas til relevant finansiell myndighet i EU/EØS-land. TRS vil bli betydelig utvidet for å kunne dekke det nye rapporteringsbehovet. Et annet og helt nytt rapporteringskrav er posisjonsrapportering for varederivater og utslippskvoter/kvotederivater. Ved handler foretatt på markedsplass i EU/EØS-land vil markedsplassen normalt rapportere posisjonene på vegne av medlemmene deres.

5.5.6 Forsikring

Det nye europeiske soliditetsregelverket for forsikringsselskaper, Solvens II[49], trer i kraft 1. januar 2016. Blant annet stilles det økte krav til intern og ekstern rapportering og store krav til data og datakvalitet, noe som krever vesentlige endringer i IKT-løsningene.

5.5.7 Tiltak mot hvitvasking

I desember 2014 kom Europarådet og Europaparlamentet til enighet om forslaget til et fjerde hvitvaskingsdirektiv[50] og revisjon av forordningen om opplysninger som skal følge med pengeoverføringer. Formelt vedtak i EU forventes fattet i løpet av våren 2015. Forslaget gjennomfører blant annet de reviderte anbefalingene til Financial Action Task Force (FATF) fra februar 2012. Forslaget utvides også til å omfatte at opplysninger om betalingsmottaker (navn, kontonummer, eller tilsvarende) skal følge hele betalingskjeden i tillegg til dagens krav om betalers opplysninger (navn, kontonummer, adresse eller tilsvarende).

[49] http://www.finanstilsynet.no/no/Artikkelarkiv/Aktuelt/2014/4_kvartal/Finanstilsynets-forskriftsforslag-for-gjennomforing-av-Solvens-II/.

[50] http://www.consilium.europa.eu/en/press/press-releases/2015/02/150210-money-laundering-council-endorses-agreement-with-ep/

5.6 Fellestiltak fra finansnæringen

Banker, andre sentrale aktører i finanssektoren og Finans Norge samarbeider om sikkerhet, utvikling av felles infrastruktur, tjenester og felles standarder. Resultater fra hendelser, overvåking, analyser og statistikk utveksles og drøftes, og tiltak besluttes.

Finansnæringens selvregulering er under press gjennom endringer i lover og forskrifter, ikke minst påvirket av endringene som skjer i regi av EU, men også av nasjonale endringer. Endringene, som er ment å gi bedre forbrukerbeskyttelse og åpnere marked, kan gi økte eller nye trusler og sårbarheter som finansnæringen må forholde seg til. Eksempel på dette er krav i PSD2[51] om at tiltrodde tredjeparter skal kunne ha tilgang på kontoinformasjon hos kontoførende bank eller betalingsforetak, noe finansnæringen gjennom BSK har vurdert gjennom sitt arbeid med å se på sikkerhetsmessige aspekter.

BankAxept og BankID ble i 2014 etablert som egne AS som ledd i forretningsorienteringen av bankenes felles tjenester. Bankenes standardiseringskontor (BSK) har ansvar for kravstilling og oppfølging på sikkerhets- og standardiseringsområdet, på vegne av bankene. BSKs initiativ til etablering av en tverrsektoriell nasjonal løsning for standardisering innen blant annet IT-sikkerhet er et av tiltakene i arbeidet med IKT-sikkerhet for finansbransjen.

FinansCERT har gjennom sitt første år etter etableringen i 2013 fått på plass en operativ organisasjon. Finanstilsynets forståelse er at bankene gir uttrykk for viktigheten av etableringen og at den vil bidra til samarbeid og koordinering ved uønskede hendelser for å redusere sårbarheten i næringen. FinansCERT yter regelmessig informasjon til næringen om trusselbildet og utviklingen i dette. Finanstilsynet mener FinansCERTs samarbeid med NorCERT og andre sektor-CERT-er er viktig nasjonalt, og for finansnæringen. Det er ønskelig at flere virksomheter i finansnæringen blir med som deltakere i FinansCERT slik at FinansCERT kan ta rollen som sektor-CERT og dekke alle områder innen finansnæringen.

Høsten 2014 ble den Java-frie BankID-versjonen, BankID 2.0 levert. Problemene for brukerne knyttet til Java vil forsvinne etter hvert som tjenesteleverandørene legger om sine IT-løsninger, og med det sikkerhetsrisikoen fra Java-sårbarheter. Den nye løsningen gir imidlertid ikke bankene like gode muligheter som tidligere til å innhente informasjon om sikkerhetsnivået på brukerens PC. Dette må banken ta hensyn til ved utforming av tjenester og i form av kompenserende kontroller. BankID 2.1 skal etter planen lanseres første halvår 2015 og skal blant annet gjøre det lettere å signere dokumenter.

Finanstilsynet er kjent med at næringen har lagt vekt på kvaliteten i identitetskontrollen i Postens PUM-tjeneste ved utlevering av kodebrikken som benyttes sammen med BankID og at næringen planlegger gjennomføring av aktiviteter for å bedre denne.

Etter planen skal BSKs arbeid med å modernisere "Baltus" ferdigstilles i 2015, noe som vil gi en

[51] Payment Services Directive 2 (Betalingstjenestedirektivet)

fleksibel og sikker infrastruktur for ruting og transport av transaksjonsrelaterte finansielle forespørsler mellom bankene tilknyttet den felles norske infrastrukturen. Videre har bankene utarbeidet en plan i regi av BSK, for overgang til ISO 20022. Dette arbeidet vil medføre vesentlige endringer for norsk betalingsinfrastruktur de nærmeste årene, og det er viktig at dette arbeidet skjer på en koordinert og kontrollert måte slik at både sikkerhet og stabilitet blir ivaretatt på en god måte.

Næringen etablerte i 2014 felles konto- og adresseringsregister[52], som blant annet vil øke både sikkerheten og kvaliteten i norsk betalingsformidling og gi grunnlag for forenklede nye tjenester. Dette omfatter kobling mellom telefonnummer, eier og kontonummer, som benyttes i straksbetalingsløsninger[53] på mobil[54].

5.7 Virtuelle valutaer

Det er fortsatt oppmerksomhet på virtuelle valutaer, eller såkalte kryptovalutaer. I 2014 var det over 550 ulike typer virtuelle valutaer.

De virtuelle valutaene er verken utstedt eller garantert av noe offentlig myndighetsorgan eller underlagt tilsyn. Brukerne har derfor ingen rettsbeskyttelse utover allmenn lovgivning.

I desember 2013 advarte EBA forbrukere mot mulig risiko ved å kjøpe, handle med og eie virtuelle valutaer.[55] EBA fulgte opp risikoen med virtuelle valutaer i 2014 og utarbeidet, med deltakelse fra Finanstilsynet, en rapport[56] om virtuelle valutaer kan og bør reguleres.

EBAs konklusjonen fra rapporten var:

- Risikoen man ser, overstiger langt de fordelene man kan se, særlig i europeisk sammenheng.
- Mer enn 70 risikoområder ble identifisert, og deres bakgrunnsdrivere ble vurdert.
- For å adressere alle disse risikoene vil det kreves et omfattende reguleringssett med et vesentlig globalt preg, som vil være tidkrevende å utarbeide.
- Et hensiktsmessig kortsiktig tiltak vil være at nasjonale tilsynsmyndigheter fraråder finansinstitusjoner, betalingsforetak og e-pengeinstitusjoner fra å kjøpe, eie, eller selge virtuelle valutaer.
- Forslag om at vekslingssteder e.l. for virtuelle valutaer inkluderes i revisjonen av hvitvaskingsdirektivet (AMLD4).

[52] https://www.fno.no/verktoy/avtaler-og-regelverk/bank-og-betalingsformidling/betalingssystemer-og-felles-bankinfrastruktur-/Betalingstjenester-og-fellesfunksjoner/
[53] http://www.dinside.no/931446/endelig-kommer-straksbetalinger-i-nettbanken
[54] https://sn.no/om-oss/infoartikler/ny-mobilbank
[55] http://www.finanstilsynet.no/no/Artikkelarkiv/Aktuelt/2013/4_kvartal/Advarsel-til-forbrukere---informasjon-om-virtuelle-valutaer/
[56] http://www.eba.europa.eu/-/eba-proposes-potential-regulatory-regime-for-virtual-currencies-but-also-advises-that-financial-institutions-should-not-buy-hold-or-sell-them-whilst-n

I kjølvannet av offentliggjøringen av rapporten har flere lands myndigheter utstedt varsler og frarådet finansnæringen mot involvering i virtuelle valutaer. Noen steder har banker også avsluttet kontoforhold med Bitcoin-selskaper.

USA, som er et av landene med en liberal holdning til virtuelle valutaer, har ved The New York State Department of Financial Services (NYDFS) offentliggjort sin revisjon av forslag til kryptovalutaregulering[57]. Reguleringsforslaget inneholder blant annet krav om registrering, etterlevelse av regelverk, kapital, oppbevaring og beskyttelse av kundemidler, tilsyn, tiltak mot hvitvasking, cybersikkerhetsprogram og tiltak, kontinuitet og beredskapsløsninger og forbrukerbeskyttelse.

FAFT har fulgt risikoen knyttet til hvitvasking og terrorfinansiering ved bruk av virtuelle valutaer. FATF er i ferd med å utarbeide retningslinjer for en risikobasert tilnærming som tilsier bruk av allerede eksisterende anbefalinger også for virtuelle valutaer. Eksempler på dette kan bli at selskaper som driver med valutaveksling og lignende, skal lisensieres/registreres, utføre kundekontroller ("kjenne din kunde") og krav til informasjon om avsender og mottaker av overføringen.

5.8 Kontanter og elektroniske løsninger

Det er store insentiver og praktiske årsaker til at flere ønsker å gjøre Norge til et kontantfritt samfunn[58]. Behandling av kontanter er kostbart, og logistikken for kontantdistribusjon er omfattende. Dersom elektroniske løsninger fullt ut skal erstatte kontanter, må disse dekke de behovene som kontanter dekker i dag, som at kontanter er det eneste betalingsmidlet du kan kreve å få betale med. Ett av hovedpunktene som må oppfylles før en kan likestille kontanter og elektroniske penger, er tilgjengeligheten for forbrukerne. Beredskapsløsningene for de elektroniske tjenestene må være av en kvalitet som sikrer forbrukerne tilgang til å betale elektronisk på lik linje som med kontanter.

I Finanskomiteens innstilling til ny finansforetakslov[59] foreslås det en ny bestemmelse om bankers ansvar for kontanttjenester. Det er foreslått at banker pålegges en plikt i samsvar med kundenes forventninger og behov om å motta kontanter fra kundene og gjøre innskudd tilgjengelige for kundene i form av kontanter.

[57] http://insidebitcoins.com/news/nydfs-releases-revised-bitlicense-proposal/29578
http://www.dfs.ny.gov/legal/regulations/revised_vc_regulation.pdf
[58] http://www.hrrnett.no/kontantfritt-norge-i-2020/
http://www.nhoreiseliv.no/2013/08/09/ny-rapport-om-kontantfritt-reiseliv/
[59] https://www.stortinget.no/globalassets/pdf/innstillinger/stortinget/2014-2015/inns-201415-165.pdf

6 Risikoområder

6.1 Oversikt

Finanstilsynet har vurdert trusler, sårbarheter og kontrolltiltak som er omtalt i denne ROS-analysen. Tabell 11 nedenfor oppsummerer Finanstilsynets vurdering av risikoen innenfor det enkelte kontrollområdet eller kontrollmålet.

Vurderingstemaene som ligger til grunn for oppsummeringen, er stikkordsmessig listet i kolonne 2 i tabellen nedenfor. Temaene er "nøytrale", det vil si at for eksempel "Tilgangskontroller" er en sårbarhet hvis tilgangskontrollene er mangelfulle. Omvendt vil god tilgangskontroll være en styrke for kontrollmålet. Merk også at et tema kan være relevant for flere kontrollmål, selv om det ikke er listet for alle kontrollmål i tabellen. Temaene som er listet for et kontrollmål, er ikke uttømmende for kontrollmålet, men er de som er mest omtalt i denne rapporten ut fra funn og observasjoner.

Kontrollmålene i tabellen er ikke satt i prioritert rekkefølge.

Kolonne 3 gjengir Finanstilsynets vurdering av risikoen for at kontrollmålet i kolonne 1 ikke nås. Kolonne 4 gir uttrykk for om risikoen anses å være økende, stabil eller avtakende.

Sikringen varierer mellom foretakene. Finanstilsynet er oppmerksom på at enkelte foretak, etter en nærmere vurdering, kan ha kommet til at kostnadene forbundet med ytterligere beskyttelse er for høye i forhold til sikringen som oppnås, og at foretaket velger å akseptere sårbarheten og risikoen som den innebærer.

Tabell 11

Kontrollmål	**Vurderingstema** **Sårbarhet/kontrolltiltak**	**Risiko:** **H(øy)** **M(iddels)** **L(av)**	**Trend**
Integritet Informasjon og informasjonssystemer er korrekte, gyldige og fullstendige.	Datakvalitet Datamodeller Endringsbeskyttelse (hash) Dobbeltlagring Strukturerte vs. ustrukturerte data Tilgangskontroller	H	↗
Konfidensialitet Informasjon og informasjonssystemer er tilgjengelige bare for dem som skal ha tilgang.	Autorisasjon Identitetskontroller Interne retningslinjer Kryptering (kvalitet) Logging Logisk/fysisk tilgang Nøkkelhåndtering Signering Sosiale medier ID-tyveri: tiltak	M	→
Tilgjengelighet Informasjon og informasjonssystemer er tilgjengelige innenfor de tilgjengelighetskravene som er satt.	Avhengighet av Internett Avviksøving og -testing Bytte av leverandør Endringer i programmer og data Flytte driften Komplisert kjøreomgivelse Maskinvarefeil Nettverksfeil Overvåking Redundans Sabotasje Sikkerhetskopier Sikring av nasjonal, sentral infrastruktur Tjenestenektangrep Utviklingen når det gjelder hendelser Vedlikehold, opprydding og sanering	M	↗

Kontrollmål	Vurderingstema Sårbarhet/kontrolltiltak	Risiko: H(øy) M(iddels) L(av)	Trend
Beslutningsstøtte: "IT fungerer tilfredsstillende som støtte for strategiske beslutninger, kundebehandling, saksbehandling og rapportering".	Avviksanalyse Integrasjon mellom dataelementer i ulike systemer Integrasjon mellom systemer Konsekvensanalyse Segmentanalyse Tidlig varsling Totalt kundebilde "What if"-analyse	M	→

Kilde: Finanstilsynet

6.2 Nasjonal finansiell stabilitet

Dersom betalinger og enkelte andre finansielle tjenester er utilgjengelige, vil viktige samfunnsfunksjoner etter kort tid ikke lenger fungere tilfredsstillende. Etter lengre tid vil viktige samfunnsfunksjoner kunne stoppe opp. Markedene fungerer ikke lenger som forutsatt. Manglende oversikter over finansielle posisjoner kan dermed true den finansielle stabiliteten. I slike situasjoner er nasjonen sårbar for påvirkning utenfra.

Foretak av betydning for finanssektoren var under angrep i 2014. Virkningen av angrepene ble redusert som følge av tiltak fra foretakene.

Erfaringene fra 2014 viser at én angriper alene, selv med begrensede ressurser, kan gjøre stor skade. Det finnes også svært ressurssterke grupper av mulige angripere. Angrep med stor og varig skade kan true finansiell stabilitet.

6.3 Foretak

I likhet med tidligere år synes endringer i systemer og omgivelser å være den hyppigste feilårsaken eller risikodriveren. Foretakene må fortsatt ha særlig oppmerksomhet rettet mot dette området. Mange foretak har kompliserte kjøreomgivelser samtidig som det forgår bytte av tjenesteleverandør. Dette medfører en økt risiko som må ivaretas i inn- og utkontrakteringsprosjekter. Samhandlingsprosedyrer må tilpasses og testes.

I 2014 var det situasjoner der katastrofeløsninger ble iverksatt eller planlagt iverksatt. Disse viste at det fremdeles oppstår uventede og uheldige forhold knyttet til løsningene. Dette viktige området må

fortsatt prioriteres høyt.

Sosial manipulering, målrettede angrep og Big Data truer konfidensialitet og integritet i systemer, og dette må det legges vekt på fremover.

Hendelser indikerer at ikke alle foretakene har tilstrekkelig kontroll på driften. Det forekommer situasjoner der datasett ikke lukkes og med den følge at batch-oppdateringene ikke går. En prosess som låser en database og stopper videre prosessering, eller manglende "Recovery"-punkter, gjør at det blir doble oppdateringer. Risikoen øker ytterligere fordi enkelte foretak synes å ha kommet på etterskudd når det gjelder "renholdet", det vil si at de ikke løpende har fjernet funksjoner fra driftsmiljøet som ikke lenger brukes, eller unngår å slå sammen funksjoner der dette er hensiktsmessig.

6.4 Forbruker

I løpet av gjennomføringen av en betaling må brukeren gjøre kontroller som er vesentlig for sikkerheten. Banken oppfordrer gjerne kunden til å forsikre seg om at det er en hengelås på nettsiden. Hengelåsen signaliserer at det er opprettet en kryptert forbindelse mellom kunden og nettsiden og at et sertifikat er benyttet for å oppnå dette. Dette er ikke en tilstrekkelig kontroll. For at kontrollen skal være effektiv, må kunden blant annet kontrollere at sertifikatet er utstedt til det brukerstedet som hun ønsker å benytte.

Dette er et eksempel på at det er utfordrende for forbrukeren å forstå sikkerhetsmekanismene og risikoen forbundet med digitale løsninger. Da er det vanskelig for forbrukeren å være tilstrekkelig årvåken.

Det oppstår fra tid til annen uenighet mellom forbruker og banken om årsaksforhold og ansvar knyttet til transaksjoner som er registrert på kundens konto og som forbrukeren ikke vedkjenner seg. Det kan kreves betydelige ressurser i form av undersøkelser og juridisk bistand for å klargjøre forholdet. Den enkelte forbruker har ofte ikke forutsetninger for å uttale seg om tekniske innretninger knyttet til transaksjonsforløpet i bankens tjenester, og forbrukeren har mindre ressurser enn banken til å innhente teknisk eller juridisk bistand. Dette kan medføre at årsaksforhold mv. ikke i tilstrekkelig grad blir belyst.

Bankene benytter posten for fysisk distribusjon. Banken krever i visse tilfeller at posten, eller dens underleverandør, tar kopi av forbrukerens pass. Hensikten er at banken ønsker å kunne dokumentere at forsendelsen er utlevert til rett person. På denne måten er forbrukeren av banken pålagt å legge igjen kopi av et viktig og personlig ID-dokument (passet), som kan bli misbrukt.

Forbruker som har fått sin identitet stjålet, risikerer at det blir foretatt kjøp og bestillinger i sitt navn. Ved større kjøp vil butikken foreta kredittsjekk. Forbrukere som ønsker å redusere konsekvensene av

ID-tyveri, oppfordres til å sperre for kredittsjekk.[60] Sperring skjer ved at forbruker overleverer en kopi av passet sitt til hvert kredittopplysningsforetak sammen med en instruks om at kredittsjekk ikke skal skje. Med dette har forbrukeren lagt igjen et antall kopier av et viktig og personlig ID-dokument (passet), som kan bli misbrukt. Forbrukeren ønsket å redusere sannsynligheten for å bli utsatt for konsekvensene av ID-tyveri. Resultatet kan imidlertid være at kunden øker risikoen for å bli utsatt for ID-tyveri.

Det er krevende for forbruker å forholde seg til trusler og sårbarheter i finansielle tjenester på en kvalifisert måte. Forbruker må i praksis følge rådene fra næringen og for øvrig gå ut fra at foretakene har bygget inn tilstrekkelig sikkerhet i løsningene. Det er derfor viktig at næringen opplyser brukerne godt og fullstendig om risikoen for ID-tyveri og konsekvensene av dette. Rådene næringen gir, må ivareta forbrukernes interesser på en god måte.

[60] https://idtyveri.info/min-id-er-misbrukt/

7 Finanstilsynets oppfølging

7.1 IT-tilsyn og annen kontakt med foretakene

Oppfølging av foretakenes IT-risikoer skjer primært gjennom tilsyn. Finanstilsynet vil i 2015 ha stor oppmerksomhet på de tilsynsenhetene og leverandørene som har størst innvirkning på finansiell stabilitet og velfungerende markeder.

Særlig oppmerksomhet vil være rettet mot utkontraktering av sentrale IKT-systemer i banksektoren. Finansforetak som gjennomfører større endringer på IT-området, inkludert utkontrakteringer, øker den operasjonelle risikoen.

Finanstilsynet vil fortsette sin oppfølging av beredskaps- og katastrofeløsninger, risikovurderinger, iverksettelse av tiltak knyttet til gamle kjernesystemer og driftsstabilitet og strukturelle endringer hos tilsynsenhetenes leverandører.

Det vil også bli rettet oppmerksomhet mot foretakenes styring med og oppfølging av tilgangskontroller.

Basert på risikovurderinger vil det bli gjennomført både generelle IT-tilsyn og IT-tilsyn med vekt på særskilte tema. Det viktigste grunnlaget for tilsyn er kontroll med etterlevelse av IKT-forskriften og bruk av ulike tilsynsmoduler (egenevalueringsskjemaer) basert på beste praksis. De mest vanlige tilsynsmodulene er tilgjengelige på Finanstilsynets nettsted.

7.2 Arbeid med betalingssystemer

Kontroll med etterlevelse av regelverket er en viktig oppgave samtidig som nødvendig utvikling av regelverket er viktig på et område hvor det er stor grad av dynamikk. Finanstilsynet arbeider med forslag om endringer til IKT-forskriften. Endret regelverk vil bli fulgt opp og eventuelt innarbeidet i tilsynsopplegget.

Der det gjennomføres større endringer på betalingssystemer, enten ved utvikling av nye løsninger og ved utkontraktering, vil dette vektlegges i arbeidet ettersom det kan medføre økt operasjonell risiko.

7.3 Oppfølging av hendelser

Omfang av alvorlige hendelser økte i 2014. Det er pågående store endringer i enkelte foretak, noe som medfører økt risiko for avvik. Finanstilsynet vil i 2015 følge nøye med på utviklingen av alvorlige hendelser, og legge vekt på at rotårsak blir funnet og tiltak iverksettes for å hindre gjentakelser.

7.4 Beredskapsarbeid

Arbeidet i BFI vil fortsette, blant annet med oppfølging av stabiliteten i betalingsinfrastrukturen, se på hendelsesscenarioer og vurdering av om ansvarsforhold ved krisesituasjoner er tilstrekkelig klare. Det er planlagt å gjennomføre to øvelser.

7.5 Videreutvikling av tilsynsverktøy

Internasjonal beste praksis som COBIT, ITIL og ISO er lagt til grunn for egenevalueringsmetodene som Finanstilsynet benytter i sine IT-tilsyn og tilsyn med betalingsformidlingen. Dette gir grunnlag for en ressursmessig effektiv gjennomføring av tilsyn. Det er vesentlig at tilsynsverktøyet er àjour med beste praksis.

I arbeidet med å utvikle tilsynsverktøy og -metodikk samarbeider Finanstilsynet tett internasjonalt med andre lands og EUs tilsynsorganer, blant annet med EBAs enhet for IT-tilsyn.

7.6 Oppfølging av trusselbildet knyttet til digital kriminalitet

Finanstilsynet vil fortsette sin tette oppfølging knyttet til utviklingen innen digital kriminalitet og ha særskilt oppmerksomhet rettet mot foretakenes tiltak og beredskap mot det økende trusselbildet og håndtering av hendelser.

8 Ordliste

Begrep/forkortelse	Betydning
3-D Secure	3-D Secure er en XML-basert protokoll som benyttes ved nettbetaling. Den gir et ekstra sikkerhetslag ved bruk av kort, ved at bruker autentiserer seg overfor kortutsteder, uavhengig av betalingsmottaker. Hos Visa, som utviklet protokollen, heter den "Verified by Visa".
Advanced Persistance Threat (APT)	Vedvarende angrep på systemer med formål å hente ut fortrolig informasjon. Normalt en kartleggingsfase hvor mange metoder benyttes, en gjennomføringsfase som foregår mest mulig skjult, ofte med lav intensitet, og gjerne en avslutningsfase for å skjule spor.
AML	Tiltak mot hvitvasking (Anti Money Laundering)
APEC	Asia-Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
BASH	Standard kommandotolk på mange GNU/Linux-systemer (gratis programvare)
BFI	Beredskapsutvalget for finansiell infrastruktur Koordineringsutvalg ved kriser i finanssektoren. Ledes av Finanstilsynet.
Big Data	Begrepet er ikke veldefinert, og det brukes litt ulikt av ulike aktører og i ulike sammenhenger. Det innbefatter store datamengder samlet fra både interne og eksterne kilder, og det er både i strukturert og ustrukturert form. Dette krever stor lagringskapasitet og stor prosesseringskraft for behandling om en skal trekke ut verdifull informasjon. Forventningene er at en derved skal kunne treffe velbegrunnede og raske beslutninger i vanskelige saker.
Botnet	Botnet – laget ord fra robot og network. Et nettverk av programmer på ulike servere knyttet sammen via Internett. Programmene samarbeider om en gitt oppgave.
Business Intelligence	Metoder og teknologier for å omforme rådata til nyttig og meningsfull informasjon om forretningen. Populært: Brukervennlig tolkning/presentasjon av store datamengder.

CERT	Computer Emergency Response Team. Ekspertgruppe som håndterer sikkerhetsbrudd på Internett.
Cloud Computing	Skytjeneste. Distribuert databehandling via et nettverk. Mulighet for å kjøre program på mange sammenknyttede servere. Skytjenester kan være både private og offentlige, eller en blanding av disse. Brukes ulikt av ulike leverandører, leveres via Internett.
CNP	Card Not Present. Svindel med hjelp av stjålne kortopplysninger, vesentlig ved netthandel.
Computer Emergency ResponseTeam	Se CERT.
CVC-kode	Card Verification Code. Verifiseringskode; de tre siste sifrene bak på de fleste kredittkortene.
DNS	Domain Name System
DDoS–angrep	Et internettangrep som overbelaster en server ved at stor trafikk rettes mot serveren, gjerne ved bruk av et botnet. Hensikten er å hindre normal tilgang fra ordinære brukere.
EBA	European Banking Authority. Den europeiske banktilsynsmyndigheten
EIOPA	European Insurance and Occupational Pensions Authority. Den europeiske tilsynsmyndigheten for forsikrings- og tjenestepensjon
Eksekverbar	Kjørbar, det vil si et program som kan kjøres på en datamaskin.
EMV	Står for Europay, Mastercard og Visa.
ENISA	European Union Agency for Network and Information Security. Den europeiske etaten for nettverks- og informasjonssikkerhet
ESMA	European Securities and Markets Authority. Den europeiske verdipapir- og markedstilsynsmyndigheten
FATCA	Foreign Account Tax Compliance Act
FS-ISAC	Financial Services – Information Sharing and Analysis Center (FS-ISAC) er et europeisk tiltak primært med deltakere fra CERT-er, bankorganisasjoner og politimyndighet. I Norge er det samarbeid mellom NSM, BSK og Finanstilsynet. Foreløpig er det et uformelt samarbeid mellom enkeltland og definerte myndigheter, blant annet støttet av ENISA. I USA er det etablert en myndighetsenhet på samme område. Utveksler til dels konfidensiell informasjon om sårbarheter, angrep og tiltak knyttet til bruk av de elektroniske betalingsløsningene.
Gafling	(engelsk: forking) – Fange penger i minibankene slik at de ikke utleveres, og heller ikke kan indras av automaten. Når kunden har gått, hentes pengene ut av svindler.
Hvitlisten	Liste over godkjente/aksepterte forekomster, som f.eks. sertifikater eller e-postadresser.

Internet of Things (IoT)	Foreløpig et noe udefinert begrep. Går på at ulike teknologiske enheter kan knyttes til Internett på mange ulike måter, blant annet for å avlese identitet, eller mer avansert via f.eks. Wi-Fi-nett. Mange enheter har innebygde datamaskiner og kan kommunisere med andre enheter og servicesentre. Også utplassering av sensorer for innhentig av data går under begrepet. Teknologien gjør det mulig å få utført tjenester fra hvor som helst, når som helst, av hvem som helst, gjennom en hvilken som helst kompatibel enhet.
ISACA	En uavhengig, non-profit-organisasjon. Arbeider med å utvikle og fremme bruk av globalt aksepterte og industriledende kunnskap og praksis for informasjonssystemer. ISACA står for Information Systems Audit and Control Association, men har nå endret profil til en IT Governance-organisasjon.
ISO 20022	ISO 20022 er ISO-standarden for finansielle meldinger. Den inneholder beskrivelser av meldingene og forretningsprosessen og dets vedlikehold.
Jailbreaking	For iPhone: Går inn og endrer telefonens sikkerhetsopplegg, f.eks. for å tillate bruk av en annen operatør enn den telefonen er låst til (hvis den er låst til operatør). Leverandør vedlikeholder ikke slike endringer, og sikkerhetshull kan oppstå.
JCL	Job Control Language; Navn for skriptspråk som brukes på IBM stormaskin operativsystemer for å instruere systemet når en skal kjøre en driftsjobb eller starte et delsystem.
NTP	Network Time Protocol. Brukes for å synkronisere klokkene i datamaskinene i et nettverk.
Man-in-the-middle- angrep	Et angrep hvor angriperen i hemmelighet videresender kommunikasjon mellom to parter som tror de kommuniserer direkte med hverandre.
MIF-forordningen	Forordning om formidlingsgebyr for kortbaserte betalingstransaksjoner
Miscalibration	Feiljustering. Ofte brukt om bedømming av informasjon ut fra feil utgangspunkt/grunnlag slik at en trekker feil slutninger.
Multisourcing	Oppdeling av leveransene på flere leverandører, men i denne sammenheng slik at en kjøper ulike produkter fra ulike leverandører.
NIS-direktivet	EU-direktiv som skal sikre høyt felles nivå på nettverks- og informasjonssikkerhet i EU.
NFC	Near Field Communication. Benyttes i enkelte betalingskort og mobiltelefoner (holde kort eller mobil nær betalingsterminalen).
Offshoring	Kjøp av tjenester utenfor landets grenser.
Outsourcing	Kjøp av tjenester utenfor eget foretak.

Overconfident	Selvsikker på grunnlag av stort tilfang på informasjon. Kan overse vitale forhold som ikke er med i informasjonsgrunnlaget.
Overlay services	Tredjepartstjenester i grensesnittet kunde-bank.
Passporting guidelines	Et betalingsforetak eller e-pengefortak i et EØS-land kan fritt etablere seg i annet EØS-land forutsatt at hjemlandets myndigheter ikke har vesentlige innvendinger eller vertslandets myndigheter har vesentlige innvendinger. Prosessen når et slikt foretak, med lisens i et EØS-land ønsker å etablere seg i et annet EØS-land, kalles passporting. Passporting betyr i korthet meddelelse fra hjemlandet til vertslandet om at et foretak ønsker å drive virksomhet i vertslandet i form av filial eller agent. "Passporting guidelines" er veiledninger til hvordan dette skal gjøres.
Phishing	Det å gi seg ut for å være en annen og i denne forkledning be en person om opplysninger. Personens tillit til den originale avsenderen blir forsøkt utnyttet.
PKI	Public-key infrastructure. Består av hardware, software, prosedyrer, retningslinjer og personell som er nødvendig for å lage, forvalte, distribuere, bruke, lagre og kunne tilbakekalle digitale sertifikater.
PSD2	Nytt betalingstjenestedirektiv fra EU (foreløpig et forslag).
Ransomware	Er en type skadevare som begrenser tilgang til IKT-løsninger som er infisert og krever en løsesum.
Recovery punkter	Gjenopprettelsespunkter
Rooting	For Android: Som jailbreaking hos Apple/iPhone. Se dette.
SSM	Single Supervision Mechanism. ECBs tilsyn for (system)viktige banker.
SSL	Secure Sockets Layer. Eldre krypteringsmetode, nå erstattet av TLS.
Sterk autentisering	Autentisering ved bruk av flere metoder, f.eks. pinkode + passord.
Sandbox	"Sandkasse". En virtuell beholder (beskyttet område) hvor en kan kjøre et program uten at det påvirker andre programmer.
SecuRe Pay	European Forum on the Security of Retail Payments
Skytjenester	Norsk for engelsk Cloud Computing. Se dette.
SSL	Secure Sockets Layer
Sterk autentisering	I autentisering finnes det tre metoder. Disse er noe man vet, noe man er og noe man har. For eksempel passord, fingeravtrykk og adgangskort. To-faktor-autentisering, også kalt sterk autentisering, benyttes når to av disse metodene benyttes i kombinasjon.
TLS	Transport Layer Security. En protokoll som brukes til å kryptere meldinger og levere dem trygt, og forhindrer tyvlytting og "forfalsking" mellom e-postservere.
Token/Tokenization	Token er en sekvens av tall og fungerer som en alias.

TPP / Third Party Providers	Begrep fra PSD2-direktivet. Dette er tjenesteleverandører som yter betalingsformidlingstjenester og som normalt ikke holder betalers eller betalingsmottakers kontoer.
Trojaner	Virus som utgir seg for et vanlig program, men som inneholder ondsinnet kode.

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00
Faks 22 63 02 26
post@finanstilsynet.no
finanstilsynet.no