FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

RISIKO- OG SÅRBARHETSANALYSE (ROS)
2013

RAPPORT

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Risiko- og sårbarhetsanalyse (ROS) 2013

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Finanstilsynet, 2. april 2014

Innhold

1 Innledning

Finanstilsynet foretar årlig en risiko- og sårbarhetsanalyse (ROS-analyse) av finanssektorens bruk av IKT og løsninger for tilbudet av betalingstjenester. Rapporten er basert på en rekke kilder og inneholder vurderinger av hvordan identifiserte risikoer kan få innvirkning på finanssektoren i Norge.

Den teknologiske utviklingen innen finanssektoren skjer raskt, og den gir grunnlag for nye tjenester. Men ny teknologi inneholder ofte ukjente sårbarheter. Den enkelte virksomhet møter krav om å bedre kvaliteten på tjenester og løsninger, effektivisere og redusere kostnader. Kravene kommer fra eiere, ledelse, kunder og myndigheter, og det stilles krav til endringsledelse og risikohåndtering.

Bruk av Internett representerer en rekke muligheter, men åpner samtidig for global elektronisk basert kriminalitet. Dette har hittil blitt håndtert på en forsvarlig måte av enkeltforetak og en samlet finanssektor i Norge. Trusselen vil vedvare globalt, og angrep kan komme både uventet og med bruk av ukjente framgangsmåter til Norge. Det er viktig fortsatt å prioritere det forebyggende arbeidet og raskt håndtere sårbarheter og risiko på en hensiktsmessig måte.

Finanstilsynets årlige ROS-analyse har som mål å gi et bilde av endringer i risikobildet av finanssektorens bruk av IKT og betalingstjenester. Bakerst i rapporten er det en ordliste som forklarer begreper og institusjoner.

2 Oppsummering

Utviklingstrekk

Den teknologiske utviklingen i finanssektoren medfører et behov for endringer i regelverk, tjenester og infrastruktur som samlet representerer en økt risiko. Ny teknologi kan introdusere nye ukjente sårbarheter og gi økt risiko. Det skjer også endringer på det organisatoriske området hos finansforetak, infrastrukturforetak og viktige IKT-leverandører, og dette kan øke sårbarheten.

Digitale markedsplasser for handel og distribusjon av elektroniske tjenester gir finanssektoren en rekke muligheter, men tiltrekker seg samtidig grupper av organisert kriminalitet som i stor grad retter angrep mot betalingstjenester. Denne kriminaliteten er internasjonal og har ikke landegrenser som noen barriere. Nye aktører som ikke er underlagt norsk lovgivning og som opptrer i et grenseløst Internett, skaper utfordringer for kunder, norske finansforetak og myndigheter.

Gjennom EØS-avtalen innføres nytt EU-regelverk der hensikten er å gi en tryggere finanssektor. Samlet kan endringene imidlertid gi utfordringer både for finansforetak og myndigheter. Gjennomføring av endringene, også systemtekniske, kan medføre risiko.

Bruk av smarttelefon og nettbrett øker sterkt, og finansforetakene lanserer mange nye tjenester som kan betjenes gjennom disse enhetene. Endringene kan føre til økt risiko som ikke i tilstrekkelig grad er identifisert og håndtert, og finansforetakene må tilpasse seg denne utviklingen.

Finanstilsynets funn og observasjoner

Finanstilsynet benytter i stor grad egne datakilder til ROS-analysen. Den viktigste kilden er resultatene fra gjennomførte tilsyn, dernest fra rapportering av hendelser på IT-området fra finansforetakene. Finanstilsynet har bygd opp en omfattende database med informasjon om registrerte hendelser, og analyse av denne informasjonen gir innsikt i aktuelle risikoområder. Hvert år foretar Finanstilsynet intervjuer med større finansforetak og viktige leverandører og operatører av infrastruktur. I tillegg gjennomfører Finanstilsynet målrettede spørreundersøkelser på områder som involverer bruk av ny teknologi og tjenester og som kan representere ukjent risiko.

Aktuelle risikoområder fra analysene i 2013

1) Omfattende endringer i finanssektorens IT-virksomhet

Flere av de store finansforetakene gjennomfører, eller vil gjennomføre, omfattende endringer i sin IKT-virksomhet, både på system- og driftssiden. Utskifting av leverandører og driftssteder, endringer

av driftsopplegg og driftsarkitektur, insourcing og økt bruk av offshoring er eksempler på endringer. Flere av endringene medfører personellendringer, som omstilling og nedbemanning.

Generelt fører endringer til økt operasjonell risiko. I intervjuene framkommer det at nettopp endringshåndtering vurderes å være en av de største risikoene. Finanstilsynet har erfart at de fleste og mest betydelige innrapporterte hendelsene har skjedd i forbindelse med endringer. Det er av vesentlig betydning at foretakene kontrollerer og styrer risikoene relatert til de pågående og omfattende endringene.

Selv om det enkelte foretak mener å ha kontroll på sine endringer og risikoer, er det Finanstilsynets vurdering at endringene samlet utgjør en betydelig risiko for norsk finansiell infrastruktur og stabilitet. Det er viktig at denne risikoen blir forstått og forsøkt redusert.

2) Samhandling mellom flere aktører

Mange endringer innebærer at forskjellige leverandører blir involvert i verdikjeden til ett og samme foretak. Der det tidligere har vært én hovedleverandør på IT-siden, splittes nå tjenester og leveranser mellom flere leverandører (multisourcing).

Det kan være fordeler med en slik modell. Finanstilsynet mener imidlertid at modellen kan gi opphav til uklare ansvarsforhold og mangelfull samhandling og koordinering, noe som kan medføre økt risiko, spesielt i en krisesituasjon. Finanstilsynet viser til "påskehendelsen" i 2011, der nettopp mangel på samhandling var en sentral problemstilling. Multisourcing kan gjøre det utfordrende for foretaket å skaffe tilstrekkelig oversikt og kontroll av risikoen i den totale utkontrakterte IT-virksomheten. Risikostyring og klart avtaleverk er derfor helt nødvendig.

3) Mangelfulle risikovurderinger

Finanstilsynet har i tidligere ROS-analyser påpekt at risikovurderinger og risikostyring er et klart forbedringsområde i finansforetakene. Området synes fremdeles å være en utfordring. De fleste finansforetakene utarbeider årlige risikovurderinger etter bestemmelsene i risikostyrings- og internkontrollforskriften og IKT-forskriften, men arbeidet er av varierende kvalitet. Generelt er Finanstilsynets erfaring at risikovurderinger og risikoreduserende tiltak ikke blir fulgt opp på en systematisk måte. Det framkommer ikke alltid at tiltakene er gjennomført og at de har hatt forventet effekt på risikoen.

4) Angrep mot betalingstjenestene

Betalingstjenestene er fortsatt under angrep av kriminelle. Dette gjelder for de fleste elektroniske kanaler der betalingstjenestene er digitalt distribuert helt ut til kundene. Bankenes tap viste på en rekke områder en klar nedgang i 2013. Det var imidlertid en klar økning i tapene ved kortbruk i nettbutikk, såkalt card-not-present. Dette kan ha sammenheng med de store datainnbruddene som har skjedd i internasjonale aktørers databaser som inneholder kortnummer.

5) Risiko fra eldre design

Finanstilsynet har i tidligere års ROS-analyser pekt på et stadig mer påtrengende behov for å erstatte eldre såkalte legacy-systemer med nye. En av grunnene er behovet for fleksibilitet og kobling av opplysninger. En annen grunn er utfordringene med å holde à jour kopier av grunndata og kunne gi et samlet korrekt kundebilde.

Moderne systemer derimot, består av lag med likeartede funksjoner som kobles til tjenestene ved hjelp av programkall (tjenestebuss). Programkallene gjenbrukes på tvers av tjenester.

Kompetansen på gamle systemer forsvinner også etter hvert, slik at vedlikehold og drift blir mer utfordrende.

Finanstilsynets videre oppfølging

Finanstilsynet vil fortsatt prioritere å ha et nært samarbeid med viktige aktører i sektoren, både for å sikre forståelse av risikonivået og for å forstå utfordringene som virksomhetene må møte. Det blir vektlagt å sikre innsyn i foretakenes beredskapsløsninger og at foretakene gjør nødvendige tiltak for å sikre at disse er virksomme.

Betalingssystemer og utvikling

Rapporten vurderer risiko knyttet til enkelttjenester i betalingssystemene, endringsprosesser og nye produkter og tjenester som kan representere en risiko. Det omfatter særlig planlagte ondartede hendelser, men også ikke-planlagte hendelser som kan true stabilitet og kvalitet. Tilsynets vurdering er at betalingstjenestene generelt er stabile og har tilfredsstillende kvalitet. Likevel inntreffer det alvorlige avvik.

Arbeidet med å bidra til økt kvalitetsnivå både hos finansforetakene og deres leverandører vil fortsette. Selv om angrep mot betalingstjenestene inntreffer, er tapene fortsatt moderate. Dette skyldes i stor grad tiltak som enkeltforetak og en samlet sektor har iverksatt, som etableringen av FinansCERT. Dersom næringen ikke hadde gjennomført relevante forebyggende tiltak, viser estimater at tapene ville vært svært høye. Det viktige arbeidet med forebyggende tiltak og andre tiltak må fortsette. Betalingssystemene i Norge forutsetter et nært samarbeid mellom ulike aktører, fellesskapsløsninger og involverte leverandører. Det er derfor viktig at styring og kontroll blir prioritert og at tiltak for å sikre samhandling om fellesløsninger og infrastruktur fortsetter. Det er videre viktig med korrekt og åpen informasjon om tap knyttet til betalingstjenester og følge utviklingen over tid. Dette gir også informasjon til forbrukere og aktører i næringen.

Verdipapirområdet

I rapporten er verdipapirområdet omtalt spesielt siden det skjer omfattende endringer i denne sektoren som samlet kan utgjøre en risiko. Disse endringene som skjer, påvirker også inntektsmulighetene og kan redusere midler til nødvendige tiltak for å fornye og sikre kvalitet. Eldre systemer kan være en utfordring, samtidig som en fornyelse kan innebære risiko. Det er betydelige endringer i regelverket som vil påvirke infrastruktur og verdipapirforetakene i EU. Nye elektroniske markedsplasser for

verdipapirhandel på tvers av landegrenser påvirker også de tradisjonelle aktørenes volum og inntekter. Behovet for endringer på området er derfor stort.

3 Utviklingstrekk

Kapitlet viser endringer i regelverk, teknologi og tjenestetrender i Norge og internasjonalt.

3.1 Utviklingstrekk for skytjenester i EU

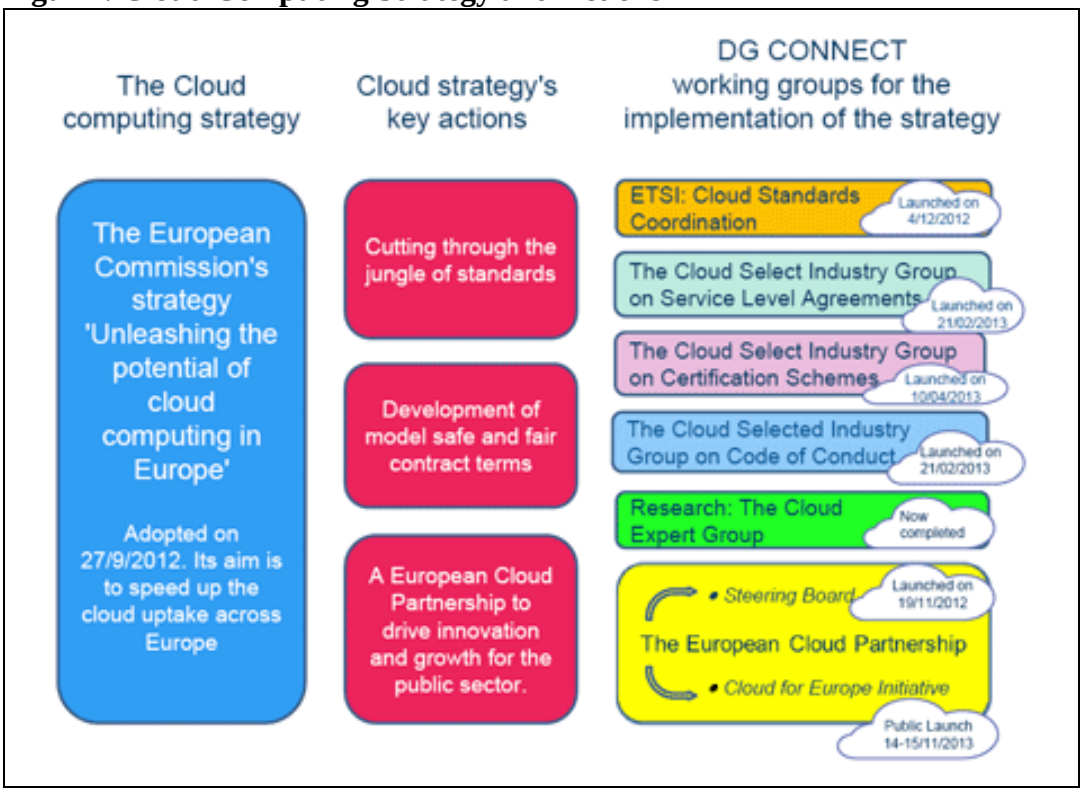
I september 2012 lanserte EU-kommisjonen sin strategi for skytjenester: "Unleashing the Potential of Cloud Computing in Europe".[1] Strategien har som målsetning å øke antall jobber og gi økt brutto nasjonalprodukt i Europa. Strategien skal fremme skytjenester i alle økonomiske sektorer, og det er opprettet arbeidsgrupper for å gjennomføre ulike påpekte tiltak.

Strategien har tre nøkkelområder:

1. Forenkle standarder
2. Anbefale avtalestandarder som ivaretar sikkerhet og rettferdige avtalebetingelser
3. Fremme partnerskap, innovasjon og vekst fra offentlig sektor i EØS-området

[1] Digital Agenda for Europe – European Commission:
http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy

Figur 1: Cloud Computing Strategy and Actions



Kilde: EU-kommisjonen[2]

De viktigste arbeidsgruppene som kan få konsekvenser for elektroniske finansielle tjenester, er:

- ETSI (European Telecommunications Standards Institute) koordinerer standarder for skytjenester og elektroniske signaturer og skal sammen med interessenter etablere standarder som kan støtte EUs strategi på området.
- Ekspertgruppe for SLA-er innen skytjenester. Målområdet er konsumenter og SMB-er.
- Arbeidsgruppe for sertifiseringsopplegg innen skytjenester. Med hjelp fra ENISA (European Network and Information Security Agency) og andre institusjoner skal den støtte utviklingen av et frivillig sertifiseringsopplegg innen skytjenester.
- Arbeidsgruppe for metoder og rutiner som skal støtte en enhetlig anvendelse av beskyttelse og behandlingsregler for data.
- Ekspertgruppe for forskning innen skytjenester. Gruppen har levert premisser for strategien, også føringer for forskningsområder.
- European Cloud Partnership, som gir EU-kommisjonen råd om muligheter for ny vekst innen området. En skal bringe sammen industripartnere med den offentlige sektor for å skape et enhetlig marked for skytjenester i Europa.

[2] http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy

Kartleggingen av standarder er fullført, og endelig rapport, Cloud Standards Coordination,[3] ble publisert i november 2013. Rapporten gir en samlet oversikt over ulike standarder og spesifikasjoner for skytjenester. Rapporten er rettet mot tjenesteleverandører, kjøpere av skytjenester og regulerende myndigheter.

Selv om det er etablert en viss standardisering for skytjenester, forventes det en videre utvikling innen området.

Ett av områdene som rapporten peker på som en utfordring, er å etablere standarder for avtaler som skal regulere forholdet mellom tjenesteleverandør og kjøper av skytjenester. Rapporten har i sin oppstilling av livsløpene i en avtale henvist til relevante rapporter og standarder om de ulike fasene i avtaleperioden. Rapporten har forsøkt å kartlegge alle initiativ som går på standardisering og spesifikasjoner av skytjenester. Siden infrastrukturen som skytjenestene er basert på, er kompleks og har mange bestanddeler, så er det også mange ulike organisasjoner innen sikkerhet, telekommunikasjon, strømleveranser og andre som har etablert eller er i ferd med å utarbeide standarder, spesifikasjoner og oversikter på dette området.

3.2 Samordning og endring i EUs regelverk

I løpet av 2013 fremmet EU flere forslag til endringer eller nye direktiver, forordninger, tekniske standarder og veiledninger innen betalingsformidlingen. Forslagene er på høring. Slik som forslagene foreligger, vil noen av forslagene trolig medføre endringer i finanssektorens og betalingstjeneste-leverandørenes IT-løsninger. 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.

Endringene er omfattende og representerer således en potensiell compliance-risiko. Endringer i systemporteføljen er generelt en av de viktigste kildene til systemfeil. Omfattende regelverksendringer gjennomført over en kort tidsperiode kan medføre en risiko.

3.2.1 Forordning om elektronisk ID

Det er foreslått en forordning om elektronisk ID og elektroniske signaturer. Selv om den i hovedsak dreier seg om elektronisk samhandling med forvaltningen, vil bl.a. sikkerhetsteknologien gi ringvirkninger til hele samfunnet, f.eks. til identifisering og sikkerhetsnivåer i betalingstjenestene. Det er foreslått at høyeste sikkerhetsnivå skal kunne bestemmes av EU-kommisjonen der verken de enkelte statene eller Norge har regelfestet påvirkningskraft. Justis- og beredskapsdepartementet uttrykker bekymring for alvorlige konsekvenser for kriminalitetsbildet og samfunnssikkerheten i Norge hvis

[3] http://ec.europa.eu/digital-agenda/en/news/cloud-standards-coordination-final-report

sikkerhetsnivået i forordningene settes for lavt og Norge ikke skal kunne bestemme nivået selv.[4]

3.2.2 Nytt betalingstjenestedirektiv – PSD2

EU har foreslått nytt betalingstjenestedirektiv – PSD2.[5] Ett av hovedformålene er å regulere "Third Party Providers" (TPP) inn under direktivet. TPP-er tilbyr ikke selv kontoføring, men tilbyr kunder å utføre betalingstjenester ved å opptre som en formidler mellom kunden og kundens bank. Kunden gir på den måten TPP-er i oppdrag å initiere betalingsoppdrag på sine vegne. TPP-ene baserer sine tjenester på kunders eksisterende bankkontoer. Å legge til rette for slik virksomhet gjennom regulering skaper nye og kompliserte operasjonelle og rettslige interaksjoner i verdikjedene innen betalings-formidlingen (mellom TPP-er, banker og kunder). Disse interaksjonene vil introdusere nye grensesnitt og kan innebære nye risiko- og sårbarheter. Dette kan føre til at kunder opplever redusert trygghet ved bruk av betalingstjenester og at tilliten blir svekket.

Forslaget til revidert betalingstjenestedirektiv innebærer at en TPP skal ha tilgang på kontoinformasjon på kundekontoer hos kontoførende bank eller betalingsforetak, og skal kunne levere betalingstransaksjoner på samme måte som om kunden leverte betalingsoppdraget direkte til egen bank. En slik tilgang, som medfører separasjon av kontoholdet og betalingstjenester, kan medføre redusert interesse for vedlikehold og utvikling av underliggende og effektive betalingsinfrastrukturer. Om tredjeparter også gis rett til tilgang til privat og hemmelig log in-informasjon, som kunde har fått fra sin bank, oppstår en rekke sikkerhets- og ansvarsmessige problemstillinger. At TPP-er skal ha tilgang til informasjon på kundekontoer kan reise personvernmessige problemstillinger. Om det i tillegg nedfelles bestemmelser som forbyr avtalerelasjon mellom bank og TPP, blir ansvarsforholdene ved tap og misbruk uoversiktlige.

Et annet sentralt område i forslaget omhandler krav til betalingstjenestetilbyderes styring og kontroll av risiko og hendelsesrapportering. En stor del av kravene knyttet til risikostyring og hendelsesrapportering[6] er allerede gjennomført i IKT-forskriften, men det er også krav som kan medføre økte rapporteringskrav i Norge.

3.2.3 Forslag til reviderte passporting-retningslinjer for betalingsforetak[7] og e-pengeforetak[8]

I forbindelse med revidering av betalingstjenestedirektivet er det foreslått en rekke forbedringer/endringer i retningslinjene 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. Hensikten er å standardisere og forenkle etableringsprosessen for foretak som opererer

[4] http://www.regjeringen.no/nb/sub/europaportalen/eos/eos-notatbasen/notatene/2012/okt/forslag-til-forordning-om-eid-og-esignat.html?id=728989
[5] Payment Services Directive: Norge er for øvrig godt forberedt på dette området gjennom eksisterende regulering, NorCERT-opplegget til Nasjonal sikkerhetsmyndighet (NSM) og etablering av egen FinansCERT.
[6] http://www.finanstilsynet.no/no/Artikkelarkiv/Rundskriv/2009/4-kvartal/Rapportering-av-IKT-hendelser-til-Kredittilsynet/
[7] http://ec.europa.eu/internal_market/payments/docs/framework/transposition/passporting_guidelines_en.pdf
[8] http://ec.europa.eu/internal_market/payments/docs/emoney/passporting_guidelines_en.pdf

innen EØS. Dette omfatter både foretak som tilbyr betalingstjenester og e-penger.

3.2.4 Regulering av formidlingsgebyrer for kortbaserte betalinger – MIF-forordningen[9]

EU har foreslått en regulering av formidlingsgebyrer for kortbaserte betalingstransaksjoner. Formålet er å øke konkurransen i markedet ved å regulere formidlingsgebyrer, organisere prosessering og regulere forretningsmodeller. Det er også foreslått bestemmelser som kan få konsekvenser for dagens "prioriteringsregel"[10] i det norske nasjonale kortsystemet (BankAxept), noe som igjen kan bety svekket effektivitet i det norske betalingssystemet og økt bruk av internasjonale kort med den økningen i kostnader som det vil kunne innebære for forbrukerne. Reguleringen kan føre til endringer som introduserer nye risiko- og sårbarhetsområder. På samme måte kan forslaget også føre til manglende vilje til å investere i å utvikle betalingsinfrastruktur som har stor betydning for handel.

3.2.5 Direktiv for nettverk og informasjonssikkerhet (NIS-direktivet[11])

Hensikten med direktivet er å sikre et høyt felles nivå på nettverks- og informasjonssikkerhet (NIS) for medlemslandene, og det er foreslått også å gjelde for finanssektoren og dens aktører.

Målet for det foreslåtte direktivet er tredelt:

1. Etablere nasjonale myndighetsorganer for NIS, etablere CERT-er (Computer Emergency Response Teams) og etablere nasjonale NIS-strategier.
2. Sikre samarbeid mellom de nasjonale myndighetene på NIS-området innenfor EU/EØS.
3. Sikre utvikling av en kultur for risikostyring og deling av informasjon mellom privat og offentlig sektor. Sentrale samfunnsaktører vil bli pålagt å iverksette nødvendige sikkerhetstiltak og rapportere alle alvorlige hendelser i nettverks- og informasjonssystemer.

Norge er for øvrig godt forberedt på dette området gjennom eksisterende regulering, NorCERT-opplegget til Nasjonal sikkerhetsmyndighet (NSM) og etablering av egen FinansCERT.

3.2.6 Endringer i hvitvaskingsreglene

Det foreligger forslag fra EU-parlamentet om krav til at opplysninger om betaler skal følge hele betalingskjeden. Det foreligger videre nytt forslag til hvitvaskingsdirektiv. Hovedreglene videreføres, men det er tatt inn en rekke presiseringer, utdypninger og endringer.

[9] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0550:FIN:EN:PDF
[10] Prioriteringsregelen innebærer at ved bruk av kombinerte kort i betalingsterminaler, prioriteres BankAxept.
[11] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf

3.3 Norske finansinstitusjoner og skytjenester

Norske banker har utkontraktert sine bankløsninger siden bankene tok i bruk IT i bankdriften. Også innenfor forsikringsområdet er det stor grad av utkontraktering. Det er kommet ny teknologi som gjør det enklere for tjenesteleverandørene å tilby både økt lagrings- og prosesseringskapasitet, og dette kan deles over flere datasentre på ulike steder.

Det er vanlig for de fleste store aktørenes løsninger at de er generelle og kan brukes av flere sektorer uten særlige tilpasninger. Dette skaper stordriftsfordeler og god kontroll i prosesser som problem- og endringshåndtering. I stor grad har de internasjonale tjenesteleverandørene som tilbyr skytjenester laget avtaler som er like for alle kunder. Avtalene er ofte skrevet slik at det for kjøper av tjenesten kan være vanskelig å ha kontroll over egne data og ha kunnskap om risikoen som er i infrastrukturen. Særlig gjelder dette dersom avtalen begrenser kundenes innsyn i den delen av tjenesteleverandørens infrastruktur som kundens løsninger benytter.

Bruk av skytjenester er å betrakte som utkontraktering, slik at IKT-forskriften § 12 Utkontraktering, som stiller klare krav til avtalene for utkontraktering, kommer til anvendelse uten unntak. Foretakene skal ha kunnskap om og kontroll over all risiko i egen bruk av IKT. Selv om hele eller deler av IKT-virksomheten er utkontraktert, er det foretaket som har ansvaret for tjenesteleveransen. Avtalene skal gi foretaket rett til å inspisere og kontrollere leverandørens aktiviteter som er knyttet til avtalt leveranse. I tillegg skal avtalen sikre at Finanstilsynet gis innsyn hos tjenesteleverandøren når Finanstilsynet finner det nødvendig som et ledd i tilsynet med foretaket.

Beredskap og foretakenes kontinuitets- og katastrofeløsninger har fått økt oppmerksomhet de senere årene. Forskriftens paragrafer om beredskap stiller konkrete krav som skal oppfylles også der oppgaven er utkontraktert.

3.4 Organisering og eierskap

I november 2012 varslet Nets Norway AS (Nets) endringer i organiseringen av Nets-konsernet. Sett i lys av en mulig filialisering av Nets' norske virksomhet, pekte Finanstilsynet overfor Nets på behovet for å klargjøre bankenes bruksrettigheter til løsningene for bankenes felles betalingstjenester og felles infrastruktur. Mange av fellesløsningene som Nets forvalter og drifter som leverandør til Finans Norge og bankene, eksempelvis sentrale elementer i BankAxept og BankID, er nødvendige for bankenes betalingssystemer. Finanstilsynet har også pekt på viktigheten av styring og kontroll med felles operativ infrastruktur, særlig i en beredskapssituasjon og den utfordringen dette kan være dersom deler av virksomheten foregår utenfor Norge. Finanstilsynet påpekte overfor bankene at de har ansvaret for leveransene fra Nets på sentrale områder av betalingssystemene i Norge og at det er bankenes ansvar å sikre nødvendig styring og kontroll slik at risikoen er akseptabel.

3.5 Endringer i sourcing-landskapet

Flere internasjonale leverandører er interessante for norske finansinstitusjoner. For finansinstitusjonene er lønnsomhet en driver i søken etter nye muligheter, men også stabilitet, kvalitet og fleksibilitet framheves som viktige faktorer. Leverandørene har sine sterke og svake sider, ofte på ulike produkter slik det vurderes fra kjøperne. Dette medfører at enkelte institusjoner benytter flere ulike leverandører. I 2013 varslet flere større finansforetak og enkelte leverandører at de skifter systemleverandør/systemer på viktige områder, eller at de var i en vurderingsfase for valg av ny leverandør.

Utviklingen fører til utfordrende endringer for aktørene, og omfattende avtaleverk må på plass. Erfaringsmessig er det endringer som er den største kilden til IKT-feil for finansinstitusjonene. Skifte av leverandør krever derfor grundige risikoanalyser. Ikke minst vil håndtering av feilsituasjoner i verdikjeder som berører flere leverandører bli utfordrende. Erfaringene fra hendelsen på kortområdet i påsken 2011 viste at det var krevende å iverksette skadebegrensende samhandling raskt når flere leverandører inngår i verdikjeden.

Tap av lokal teknisk kunnskap og erfaring kan også på sikt svekke finansforetakenes bestillerkompetanse for disse tjenestene.

3.6 Fellestiltak fra finansnæringen

Bankene, andre viktige 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.

Bankenes standardiseringskontor (BSK) har startet arbeidet med å modernisere "Baltus" (Bankenes online transaksjonsutvekslingssystem), som er nettverket for ruting og transport av transaksjonsrelatert finansiell informasjon/forespørsler mellom bankene i den felles norske infrastrukturen. "Baltus 2.0" er planlagt å bli et moderne nett hvor meldingsinnhold og header-informasjon er atskilt slik at det blir mulig med flere nivåer og veier i systemet. Omleggingen planlegges gjennomført innen utgangen av 2015. BSK har også startet opp arbeidet med et "veikart" for en overgang fra eksisterende nasjonale og internasjonale standarder innen betalingsformidling til ISO 20022. EU-regulering krever at ISO 20022 skal være obligatorisk format også for kunders innlevering av betalingsoppdrag. Begge disse tiltakene vil føre til endringer i felles infrastruktur og endringer i systemene til de enkelte finansforetakene. Krav om ISO 20022 vil også kreve endringer for bedrifters ERP-systemer for utveksling av betalinger og betalingsinformasjon med finansforetakene. På sikt vil dette kunne gi grunnlag for standardisering og forenkling hos bedriftskundene.

Finans Norge etablerte i 2013 felles operasjonell infrastruktur (FOI) for straksbetalinger,[12] og det ble

[12] http://www.sparebankforeningen.no/id/17811.0

startet en begrenset pilot. Straksbetalingsløsningen gjør det mulig for kunder å gjennomføre en betaling som oppfattes å skje i realtid når som helst på døgnet. De overførte pengene blir umiddelbart disponible på mottakers konto, mens oppgjøret mellom bankene skjer i etterkant gjennom de ordinære oppgjørssyklusene. Hver enkelt bank må selv utvikle sine kunderettede løsninger, enten via nettbank eller via mobilbank. Både betalers bank og betalingsmottakers bank må være tilknyttet den operasjonelle infrastrukturen for at betaler skal kunne nyttiggjøre seg tjenesten.

BankID Norge er i gang med BankID versjon 2.0, som vil bli en Java-fri BankID.[13] Den vil benytte nettleseren, uten installasjon av annen programvare eller nedlasting av apper, og den vil være tilgjengelig på et bredt utvalg av enheter. Den nye løsningen, som vil komme høsten 2014, vil innebære eliminering av sårbarheter og bortfall av brukeropplevde problemer knyttet til bruk av Java. Utfasing av Java-basert BankID forventes å skje relativt raskt, selv om det ikke er satt noen frist for utfasingen.

Finans Norge, sammen med aktuelle finansforetak, etablerte i 2013 FinansCERT Norge. Formålet er å videreføre og styrke arbeidet innenfor overvåking, reaksjon og informasjonsutveksling når det gjelder IT-sikkerhetshendelser i finansnæringen.

Gjennom Finans Norge skjer det også en forretningsorientering ved etablering av egne selskaper for felles tjenester som BankAxept og BankID. Felles tjenester omfatter også en felles infrastruktur og utgjør en sentral komponent i bankenes tilbud av betalings- og PKI-tjenester. Forretningsorienteringen av BankAxept gjøres for å møte den økte priskonkurransen i markedet, sikre en bærekraftig utvikling av tjenester og for å tilfredsstille markedets etterspørsel etter nye betalingsløsninger. Målet er fortsatt å levere et stabilt, effektivt og konkurransedyktig betalingssystem. Gjennom forretningsorientering av bankenes PKI-løsning ønsker man å sikre en fortsatt bærekraftig utvikling av BankID, utvikling av tilleggstjenester og utvidet bruk.

3.7 Tekniske utviklingstrekk og risikoer/trusler

3.7.1 Mobilbank

Ingen banktjeneste har noen gang økt så mye i bruk som mobilbank gjør nå. Mobilbank har en rekke "gamle" og "nye" sårbarheter. Disse kan etter hvert utgjøre en betydelig risiko for betalingssystemene.

De vanligste kildene for å få tak i applikasjoner er Apples App Store for iOS og Google Play for Android. I tillegg til disse har Android muligheten til å installere applikasjoner fra hvilken som helst kilde som inneholder en Android-applikasjon. Når det gjelder iOS, må telefonen være "jailbreaket"[14] for å kunne installere applikasjoner fra andre kilder. Mange uoffisielle applikasjonsbutikker inneholder både piratversjoner og infiserte versjoner av kjente applikasjoner. Bank-apper som er digitalt signert av

[13] https://www.bankid.no/Presse-og-nyheter/Nyhetsarkiv/2013/BankID-20-uten-Java-lanseres-hosten-2014/
[14] Endring i telefonens sikkerhetsopplegg.

banken, øker sikkerheten. Banken bør aktivt bidra til at kunden for egen del øker sikkerheten ved å kontrollere signaturen og sertifikatet for appen. Banken bør også legge opp til at brukeren gjør nedlasting fra lenke til App Store eller Google Play fra bankens nettsider.

For begge operativsystemer gjelder prinsippet om at en app kjører i en isolert kjøreomgivelse ("sandboksing"). Sikkerheten som sandboksing gir, forutsetter naturligvis at utvikleren utnytter dette, og holder kode og data innenfor "sandkassen". Undersøkelser viser imidlertid at apper kan "lekke", for eksempel ved at det skrives sensitiv informasjon til åpne logger. Det er en risiko at enkelte utviklingsmiljøer ikke er modne nok til å påse at alle sikkerhetsnormer blir fulgt.

Mobilen har sikkerhet og sikre lagringsområder som skal beskytte nøkler og programmer mot uautorisert bruk. Enkelte brukere fjerner denne beskyttelsen ved "jailbreaking" (Apple) og "rooting" (Android). Angripere kan dermed få tilgang til koder, nøkler, innloggingsdetaljer og informasjons-kapsler, og angriperen kan installere ondartet kode som stjeler innloggingskoder og annen sensitiv informasjon.

Undersøkelser tyder på at mobilbrukere har tilbøyelighet til å trykke på ondartede lenker, blant annet fordi de korte URL-ene på mobilen ikke avslører angriperen. Angripere har lykkes med å stjele både brukerens innloggingskoder sendt til brukeren som SMS-koder, og koder sendt over nettet. På den måten tilegner de seg kundens penger, jf. Euro-grabber, såkalt to-kanalsangrep.

Ved hjelp av MAC-adressen på brukerens PC kan banken knytte sammen bruker og PC. Banken kan stanse en angriper som logger inn fra sin PC med koder som er stjålet. Mobilen har ikke tilsvarende identifikator og kan ikke kontrolleres effektivt på denne måten. Det kan imidlertid legges funksjoner i appen som bygger en identifikator som kan brukes til tilsvarende kontroll. Prinsippet om gjensidig autentisering bør anvendes slik at kunden kan autentisere banken og omvendt.

Et risikoreduserende tiltak er å sette enhver banksesjon inn i en kontekst som gir en risikoscore. Banken bør vurdere telefonenes lokalisering (hvis bruker tillater dette), IP-adresse, sikkerhetsoppdateringer, innbrudd, systemkonfigurasjon, infeksjoner og bruk av usikret trådløst nett, før brukeren slipper inn i banken. Informasjonen bør krysskobles med bruksmønstret til kunden. Brukeren på sin side bør laste apper kun via bankens nettsider og holde mobilen oppdatert og virusfri.

Bruk av informasjonskapsler kan etter hvert representere en risiko. De blir mer og mer utbredt i appene, og bruken av apper øker også, slik at det blir et større nedslagsfelt. Informasjonskapsler som lagres på en bankkundes PC, kan leses, stjeles og kanskje endres. Dette gjelder også kapsler som benyttes under HTTPS-sesjoner. Nettbanker benytter informasjonskapsler både på PC-er og på mobiltelefoner. Dette krever årvåkenhet både fra bankene og brukerne.

Trojanerangrep er stadig en utfordring og da ofte sett i sammenheng med phishing og DDoS-angrep. Nettbrett og smarttelefoner har hatt en økning i antall virusinfeksjoner, og særlig er Android-løsningen utsatt. Siden det ikke er reelle antivirusprogram eller brannmurløsninger for denne type enheter, utgjør

dette en risiko ettersom stadig flere tjenester tilbys på telefonen. Ondsinnet programvare (malware) på mobile enheter ligger utviklingsmessig mange år etter utviklingen på PC-er. Selv om risikoen nå er lav, kan en forvente en økning i årene som kommer.

En ytterligere risiko er at det er svak kryptering i deler av mobilnettet.

3.7.2 Big data

"Big data"[15] er ingen hyllevare, og en må derfor være bevisst på hva en vil oppnå for å få forventet gevinst av en big data-satsing. Mange starter med det en har, som datavarehus, og tar i bruk business intelligence-verktøy som gjerne også kombineres med visualiseringsverktøy. Etter hvert finnes det gode løsninger på dette området. Datafangst fra nye kilder, som f.eks. kan være offentlige registre og sosiale medier, tas i bruk når en ser behov for det i spesifikke applikasjoner og for forretningsprosesser. Datamengden øker raskt, og det kan skape problemer med dataforvaltning framfor å støtte forretningsprosesser. Det er behov for rask databehandling av ferske data, og til det vil en trenge kraftig verktøy. Flere aktører er allerede på markedet, og det forventes å komme kraftige big data-søkemotorer i nær framtid.

Big data kan brukes i mange sammenhenger, både for å få bedre kjennskap til eksisterende kundemasse, oppdage trender og behov for nye produkter, og ikke minst for kryssalg. Beslutningsstøtte er også et område som framheves ved støtte fra data utenom egen forretningsvirksomhet, samt sammenligne lignende situasjoner, avdekke anomaliteter og eventuelle systematiske avvik for enkeltindivid eller grupper. Analyse av kundedata kan også deles med kunden og gi kunden en merverdi utover tradisjonell informasjon. Eksempel kan være analyse av kjøpemønster og hvordan pengene brukes (butikker, reiser, restauranter, opplevelser og lignende), utover rene kontoutskrifter. Enkelte banker har allerede slike tjenester.

Big data kan på den ene siden gi nyttig informasjon for virksomheter, men kan også medføre risiko på enkelte områder. Informasjon kan nå et metningspunkt hvor mer informasjon ikke gir noe merverdi. Enkelte advarer mot faren ved å stole for mye på analyser fra store datamengder. Hvis dataadministrasjonen ikke holder mål, kan en få systematiske feil i datagrunnlaget, eller det kan bli utdatert. Også i selve analysene kan det gjøres feil. En kan for eksempel få for mye utjevning til å oppdage avvik og anomaliteter, eller for lite slik at en mest har "støy" i resultatene. Hvis en på slikt grunnlag tror at en har all kunnskap, kan en ta alvorlige og feil beslutninger. Beslutninger som treffes av institusjonen, kan ha store og vidtrekkende konsekvenser for mange kunder, mens enkeltpersoners feil sjelden har betydning for andre enn dem selv. Slik kunnskap kan bare opparbeides over tid, og det trengs gode rutiner rundt bruk av big data-analyser.

Big data kan involvere bruk av personopplysninger, og det er lovregulert. EU arbeider med et nytt personverndirektiv som både vil samordne de europeiske lovverkene bedre, og endre krav til

[15] "Big data" er et begrep som benyttes innenfor IT for å beskrive innsamling, oppbevaring, analyse, prosessering og fortolkning av store mengder av data. Dataene kan omfatte både strukturerte og ustrukturerte data. Det benyttes ofte i markedssammenheng.

behandling av persondata. Et viktig prinsipp for innsamling av persondata, er prinsippet om formålsbestemthet. Når kunden gir sitt samtykke til innhenting av personopplysninger, skal kunden kjenne til formålet med innhenting av slike data. Ny EU-regulering kan endre dette slik at dataeier (foretaket) også kan bruke innhentede data til andre formål. Et annet viktig prinsipp er den enkelte kundes rett til innsyn i data som er registrert om kunden selv. Det kan bli omfattende å trekke ut slike data i big data-sammenheng, på grunn av mange indirekte avhengigheter. Datatilsynet publiserte høsten 2013 rapporten "Big Data – personvernprinsipper under press".[16] Her er personvern omfattende behandlet.

Big data holder også en verdi i seg selv. Ettersom slike data også inneholder interne data som ikke er tilgjengelige utenfor foretaket, kan det ha stor verdi for andre som dermed kan få et utvidet datagrunnlag. Slike data kan ikke overleveres, utveksles eller selges uten at de er anonymisert. De bør derfor gis god beskyttelse og sikkerhet mot misbruk. Det kan være fristende for utro tjenere å selge slike data til utenforstående, også til kriminelle nettverk.

I finanssektoren er det de store internasjonale finanskonsernene, spesielt amerikanske, som tar big data i bruk. Mange av de områdene som omtales i mediene, er grenseområder mellom finansielle tjenester og f.eks. handelskjeder. Dette er bruksområder som vil kunne hindres av gjeldene europeiske personvernlover som er mer restriktive til dette.

3.7.3 Katastrofeberedskap (datasenter og kvalitet)

Finanstilsynet stiller krav til foretakenes beredskapsløsninger gjennom IKT-forskriften § 10 Krav til kontinuitet og § 11 Driftsavbrudd og katastrofeberedskap. De ulike foretakene under tilsyn har ulik risikoprofil og har derfor også etablert ulike beredskapsløsninger. Stadig flere av de eksisterende datasentrene i Norge vil i de neste årene flytte inn i nye datahaller hvor infrastruktur som strøm, telekommunikasjon, kjøling og fysisk sikring av bygget er etablert. Leveransen blir som et datasenterhotell der tjenesteleverandører kjøper seg plass til egen teknisk infrastruktur. Hvilke standarder og beste praksis som er innarbeidet i et slikt datasenterhotell, må kjøper avstemme mot egen risikovurdering.

I Norden har det så langt ikke vært vanlig å sertifisere datasentrene, men likevel bruker mange sertifiseringskravene som f.eks. Uptime Institute stiller til de ulike Tier-nivåene[17] (kravnivåer) ved etablering. I Nord-Europa er det ingen datasentre som er sertifiserte, mens eksempelvis i Spania har de to største bankene, Santander og BBVA, samt forsikringsselskapet Mapfre, sertifisert sine datasenter til nivå Tier 4. For å sammenstille kvaliteten på datasentersertifiseringen med driften av løsningene plassert i datahallen, har Uptime Institute etablert en tredelt inndeling som sier noe om de løsningene som er installert i datasenteret, er satt opp slik at de utnytter datasenterets potensiale for kvalitet.

[16] http://www.datatilsynet.no/Global/04_planer_rapporter/Big%20Data_web.pdf
[17] Tier-nivåer og krav: Det er etablert ulike industristandarder for krav som settes til en datasentral. Disse er inndelt i såkalte Tier-nivåer hvor 1 er lavest og 4 er høyest. Nivå 4 inneholder alle de lavere kravene, samt at det kreves dublering av løsninger for å sikre robusthet.

Finanstilsynet vil se nærmere på dette i 2014 som del av arbeidet med å videreutvikle tilsynsverktøyene.

3.7.4 Ondsinnet programvare

Ondsinnet programkode (malware) som spres av enkeltpersoner og mindre hacker-miljøer kan være skadelig for dem det berører, men fører sjelden til vidtrekkende samfunnsmessige problemer. Malware fra kriminelle miljøer er en større risiko. Disse miljøene blir stadig mer profesjonelle, og legger etter hvert opp sine angrep på en profesjonell måte. Angrepene har gjerne flere faser. Det kan innebære en rekognoserings-/kartleggingsfase, utviklingsfase hvor malware tilpasses formålet, test som kan gjøres mot et lignende mindre foretak for ikke å røpe målet, før selve angrepet settes inn. Angrepet kan også ledsages av ulike avledninger.

I kartleggingsfasen benyttes gjerne "phishing". Det kan også benyttes under utvikling og uttesting for å tilpasse f.eks. websider med troverdig layout, og også for å få brukeren inn på "falske" websider for plassering av ulike andre virus som skal brukes i angrepet. Under selve angrepet kan en så avlede oppmerksomheten hos offeret med DDoS-angrep på noen servere slik at en holder sikkerhetsavdelingen beskjeftiget.

Phishing som fenomen har utviklet seg både kvalitativt og kvantitativt. Phishing økte i 2013, og mange nye innfallsvinkler ble utprøvd. Det blir stadig vanskeligere å skille phishing-e-post fra ordinær e-post. En rekke hendelser viser at angrepene etter hvert er blitt mer målrettede, såkalt "spear phishing", for å oppnå uautorisert tilgang til konfidensielle data. Phishing skjer også gjennom telefonsamtaler, sms-er og webdialoger.

Phishing passer i en tid der folk utleverer store mengder informasjon om seg selv på sosiale medier som LinkedIn, Facebook og Twitter. Phishing var en del av opplegget i det alvorlige hacker-angrepet mot ledere i Telenor i 2013.

I 2013 var det i Norge en bølge av phishing-angrep mot norske finansinstitusjoner. Store mengder falske e-poster ble sendt ut, angivelig med en finansinstitusjon som avsender. Men fortsatt er ikke e-postene som er skrevet på norsk godt nok formulert til å bli oppfattet som troverdige. E-poster skrevet på engelsk, angivelig fra internasjonale foretak som VISA, PayPal osv., har et bedre språk.

De falske e-postene forsøker å fiske betalingsinformasjon, men de kan også infisere datamaskinen med ondsinnet kode hvis mottakeren klikker på lenker eller vedlegg i e-posten. Det samme blir forsøkt gjennom phishing per telefon som også hadde en kraftig økning i 2012 og 2013. Gjennom veiledning på telefonen blir man dirigert inn på en webside hvor man blir bedt om å klikke på en lenke. Dette er lenker som laster opp ondsinnet kode på datamaskinen.

En indikasjon på omfanget av phishing er antallet falske websider som tas ned. I Storbritannia tallfestes phishing i finanssektoren på den måten, se kapittel 7.5 (tapstall).

DDoS-angrep har økt sterkt i omfang internasjonalt. Effektive mottiltak er etablert i Norge, og det kan forklare at det i siste del av 2013 var en nedgang. Tendensen internasjonalt er at disse angrepene blir mer sofistikerte, med riktig syntaks for innlogging, slik at angrepene kommer forbi de første sperrene og må stoppes lenger inne i systemene, eksempelvis på applikasjonsnivå. Flere norske aktører sier at de forventer en lignende utvikling i Norge.

På tross av omfattende angrep i Norge indikerer rapporter at Norge er et land med et relativt lavt antall infiserte PC-er. Uansett må foretakene fortsatt prioritere å beskytte seg mot malware.

3.8 Utfordringer for forbrukerne

Forslag til EU-direktiver referert under kapittel 3.2 vil omfordele ansvar mellom bank og kunde. Blant annet forslås det bestemmelser som kan frata medlemsland anledning til å sette grense for kunders egenandel ved misbruk som skyldes grov uaktsomhet. Slik grense er i dag gjeldende i norsk, svensk og dansk lovgivning. Fjerning eller vesentlig reduksjon av disse grensene vil forskyve risikoforholdet mellom bank og kunde. Dette vil kunne være uheldig dersom det leder til at det ikke blir samsvar mellom de som har ansvar for sikkerhet og de som tar risikoen. Konsekvensen kan være økt tap og svekkede incentiver for å ivareta god sikkerhet. Finansforetakene fastlegger det tekniske sikkerhetsnivået for sine tjenester, mens organisasjoner og personer kan oppleve problemer hvis informasjon om kundeforhold eller betalingsinformasjon blir tilgjengelig for uvedkommende.

Beskyttelse av kundens interesser er, i tillegg til gjeldende regelverk, også regulert i kundeavtalen. Dette kan stadig endres, og ikke alltid til kundens fordel. For øvrig er det i Norge høy forbrukerbeskyttelse i gjeldende regelverk. Dette kan måtte endres ved eventuelle forslag om samordnede regler for hele EØS-området.

Betalingskort med mulighet for kontaktløs betaling kan åpne for en sårbarhet fordi kundene ikke kan nok om sikker bruk. Betalingskort vil dermed virke på samme måte som NSBs og Ruters reisekort. Dersom hele lommeboka legges på kortleseren, i stedet for å ta ut det spesielle kortet, kan kortleseren registrere alle de andre kortene i lommeboka som har samme teknologi for betaling. Ved bedrag vil ikke kortholder få melding om betalingstransaksjonen før kontoen kontrolleres. Alle kort med RFID-chip er klar for lesing og kan ikke skrues av.[18] Det kommer stadig nye kort med denne funksjonaliteten.

Mange betalingskort har protokoll for bruk av PIN ved kontaktløs betaling, selv om det ikke benyttes i tjenestene. Testing for å finne PIN i denne sammenhengen har ikke begrensningen i antall forsøk. PIN kan testes over flere dager uten å overskride antall gyldige forsøk. PIN for kontaktløs betaling og vanlig betaling viser seg å være den samme.[19]

[18] http://www.rogerclarke.com/EC/CPS-12.html
[19] http://fc13.ifca.ai/proc/9-2.pdf

Noen konsekvenser for kundene kan bli:

- Økt bruk av kontaktløs betaling vil gjøre betalingsoversikten fra banken omfattende, og mange forbrukere vil aldri oppdage falske betalinger av små beløp.
- Når en forbruker oppdager en suspekt betaling, må de gjennom en relativt lang prosess for å få tilbake pengene samtidig som kunden ofte får lite informasjon som grunnlag for å kreve refusjon. Det kan også være tidsfrister og tungvinte rutiner ved klagebehandling.
- For å kunne vurdere bankutskriftene, må de ha noe å avstemme disse mot, f.eks. kvitteringer.

Sannsynligvis vil dette føre til at relativt få falske transaksjoner for småbetalinger blir oppdaget og fulgt opp.

3.9 Virtuelle valutaer

Det siste året har det vært mye oppmerksomhet knyttet til virtuelle valutaer, eller såkalte kryptovalutaer. Bitcoin[20] er den mest utbredte og omtalte virtuelle valutaen, men også LiteCoin, ZeroCoin og Linden Dollars er blant de mer kjente. Virtuelle valutaer kommer i mange former, og det finnes i dag mer enn 100 forskjellige varianter.[21] En virtuell valuta er en type uregulert, digital valuta som ikke er utstedt og garantert av en sentralbank, og som kan fungere som betalingsmiddel fordi den oppfattes å ha verdi så lenge andre aksepterer å motta den digitale valutaen som oppgjør i handel.

Virtuelle valutaer veksles og aksepteres på stadig flere steder, både på Internett og utenfor, i den "virkelige økonomien". Et økende antall detaljhandlere, restauranter, underholdningssteder, i tillegg til den utstrakte bruken i spillfora, sosiale medier og kriminelle fora, har begynt å akseptere virtuelle valutaer (bl.a. Bitcoin) som betalingsmiddel, ettersom de vanligvis ikke involverer en bank og derfor heller ikke legger igjen "spor" som myndigheter kan få innsyn i. I tillegg har de lave eller ingen transaksjonskostnader.

Ettersom de virtuelle valutaene verken er utstedt eller garantert av en sentralbank, og så langt ikke underlagt tilsyn, finnes det ikke beskyttelse i lovverket. Det innebærer at disse er beheftet med vesentlige risikoer. Den europeiske banktilsynsmyndigheten (EBA) advarte i desember 2013 forbrukere mot mulig risiko ved å kjøpe, handle med og eie virtuelle valutaer. Finanstilsynet var med på å utarbeide advarselen.[22]

[20] http://bitcoin.org
[21] http://coinmarketcap.com/
[22] http://www.finanstilsynet.no/no/Artikkelarkiv/Aktuelt/2013/4_kvartal/Advarsel-til-forbrukere---informasjon-om-virtuelle-valutaer/

Punkter i advarselen:

- Du kan tape pengene dine på vekslingsplattformen.
- Pengene dine kan stjeles fra den digitale lommeboken din.
- Du er ikke beskyttet når du bruker Bitcoins som betalingsmiddel.
- Verdien av dine Bitcoins kan endres raskt, og kan til og med falle ned til null.

Manglende regulering skaper også mulighet for svindel. Virtuelle valutaer kan ofte ikke spores, og det er høy grad av anonymitet rundt brukerne. Dette bidrar til at bruk av virtuelle valutaer kan være attraktive for kriminell aktivitet og hvitvasking.

Den svenske Finansinpektionen anser Bitcoin for å være et betalingsmiddel, hvilket betyr at betalingsformidlingsforetak som tilbyr Bitcoin som betalingsmiddel skal melde sin virksomhet til Finansinspektionen.

EBA vurderer nå om virtuelle valutaer kan og bør reguleres.

4 Finanstilsynets funn og observasjoner

Finanstilsynets hovedkilder til informasjon om IT-virksomheten i finansforetakene er tilsyn, intervjuer og hendelsesrapporter. I tillegg holder Finanstilsynet seg oppdatert om større utviklingsprosjekter og endringer gjennom regelmessige møter med de største foretakene og leverandørene, og tilsynet mottar meldinger fra foretakene om nye eller endrede betalingstjenester.

I forbindelse med arbeidet med denne ROS-analysen ble noen sikkerhetsselskaper og internettleverandører (ISP-er)[23] intervjuet, og Finanstilsynet gjennomførte en spørreundersøkelse knyttet til aktuelle områder av IT-utviklingen.

4.1 Funn fra IT-tilsyn i 2013

Utfordringer ved nye utkontrakteringsstrategier
Finanstilsynet ser en trend der de store finansaktørene søker konsolidering i store organisasjoner og inngår avtaler med globale partnere. Ofte er det vanskelig å se hvordan den norske virksomheten er plassert i organisasjonen/konsernet, og å forstå hvordan den norske virksomheten styres og drives. For Finanstilsynet framstår det som mer utfordrende for foretakene å sikre styring og kontroll ved denne typen "globalisert" utkontraktering.

Mangelfulle avtaler
Det å etablere et godt avtaleverk ser ut til å bli stadig viktigere. Finanstilsynet ser en utvikling der finansforetakene deler opp IKT-tjenesteleveransene i flere deler. Dette medfører flere avtaleparter. Avtalene må omfatte alle deler av den utkontrakterte virksomheten og beskrive samhandlingen mellom partene. Videre er det viktig for finansforetakene å få avtalefestet rettigheter til bruk og eierskap av løsninger og kildekode. Dersom en IKT-leverandør får økonomiske eller andre typer problemer, er det viktig å ha konkrete avtaler om disse forholdene slik at det er teknisk mulig å velge en annen leverandør.

[23] ISP: Internet Service Provider – internettleverandør

Beredskapsløsninger for betalingsformidling
I 2013 gjennomførte Finanstilsynet i samarbeid med Norges Bank et tematilsyn på beredskapsløsninger for innenlands betalingsformidling. For å kartlegge bankenes beredskap for kunders tilgang til betalingsmidler og hvordan kontanter inngår i dette, ble det gjennomført tilsyn med tre utvalgte banker og en avregningssentral.

Foreløpig vurdering er at en beredskapssituasjon der det mangler tilgang til felles infrastruktur, er lettere å håndtere med reserveløsninger enn en beredskapssituasjon der det mangler tilgang til bankens kjerneløsning. På den andre siden rammes flere brukere totalt sett når det mangler tilgang til felles infrastruktur. Drift av norske bankers kjerneløsninger er relativt spredt både teknologisk og geografisk slik at det sannsynligvis alltid vil være tilgang til noen bankers kjerneløsning. Tilsynet er ikke avsluttet, og resultatet vil bli oppsummert i en samlet rapport.

Mangelfulle risikovurderinger av IKT-virksomheten
Finanstilsynet fant gjennom tilsynene i 2013 at risikovurderingen av IKT-virksomheten i en del tilfeller er mangelfull. Ofte er den overordnet og basert på en "top-down"-tilnærming. Med mindre observasjonene til det operative personellet systematisk blir dokumentert og innarbeidet i grunnstrukturen i risikoarbeidet, kan de gå tapt i risikoanalysen. Det er viktig at deltakere i gjennomføring av risikoanalyser har tilstrekkelig kunnskap på de områdene som skal analyseres.

Finanstilsynet har også sett at det mangler en strukturert gjennomgang av at IKT-virksomheten drives i samsvar med regelverket. Dette gjelder både drift i samsvar med eget internt regelverk og drift i samsvar med aktuelle lover og forskrifter, slik som IKT-forskriften.

Bruk av ISAE 3402-rapporter
Resultatet av en gjennomgang av IKT-virksomheten hos IKT-leverandør, dokumentert gjennom en ISAE 3402-rapport,[24] kan være et hjelpemiddel for kunder som kjøper IKT-tjenester fra leverandøren. ISAE 3402 er imidlertid beregnet på kontroller som er relevante for internkontroll relatert til finansiell rapportering. I følge § 12 Utkontraktering i IKT-forskriften, har finansforetaket ansvar for å oppfylle alle krav i forskriften, også der hele eller deler av IKT-virksomheten er utkontraktert. Det skal avtalefestes at foretaket har adgang til å kontrollere leverandørens aktiviteter knyttet til avtalen. ISAE 3402-rapporten gir en generell oversikt over risikobildet basert på resultatet av utvalgte kontroller, men er normalt ikke dekkende for alle deler av IKT-virksomheten og følgelig heller ikke dekkende for om leverandøren etterlever IKT-forskriftens bestemmelser.

[24] Standard for attestasjonsoppdrag (ISAE) 3402: Attestasjonsuttalelser om kontroller hos en serviceorganisasjon http://www.revisorforeningen.no/arch/_img/9605549.pdf

4.2 Foretakenes egne vurderinger

4.2.1 Intervjuer

I november og desember 2013 hadde Finanstilsynet samtaler med 14 foretak og to interesseorganisasjoner innenfor finans om deres syn på risiko i 2013 og framover. De 14 foretakene omtalte risikoer knyttet til IT-tjenestene, mens de to interesseorganisasjonene la vekt på risikoer knyttet til leverandørrollen av sikkerhetsløsninger. I det følgende omtales begge gruppene som foretak.

Oppsummert synes kombinasjonen kostnadspress og leveransepress og utfordringer knyttet til endringshåndtering i kombinasjon med svært store krav til kvalitet og sikkerhet i tjenestene å utgjøre den største risikoen.

De fleste foretakene rapporterer at ulike former for svindel er muliggjort gjennom f.eks. phishing eller card-not-present er og vil være en risiko (se for øvrig tapstall i kapittel 7.5). Flere rapporterer at omfanget av trojanere var mindre i 2013 enn tidligere.

Foretakene peker også på at ID-tyveri fortsatt er en risiko.

Ti av foretakene framhevet endringshåndtering som en spesiell risiko for dem. Av disse meldte seks at endringsrisikoen er forbundet med innføring av nye regulatoriske krav. To av foretakene meldte at de har særskilt høy risiko forbundet med store endringer i systemene for øvrig.

Tre av foretakene mener at bruk av sosiale medier er en stor risiko. Av disse mente to at bruk av kundebetjening i form av chat er en betydelig risiko.

Såkalt "dårlig håndverk" i utviklingen av nye tjenester blir av fire foretak ansett som stor risiko. OWASPs[25] "Top Ten Project" viser eksempler på trusler i tjenestene.

Nettverksbortfall anses som en sårbarhet og risiko av fem foretak. Ett av foretakene peker dessuten på faren for avlytting og falske transaksjoner i offentlige nett.

To av foretakene mener at "Advanced Persistance Threat" (APT)[26] er en stor risiko.

Seks av foretakene mener at administrering og kontroll av data er en stor risiko. "Hvilke data eier vi og hvor er de", som et av foretakene uttrykker det.

To av foretakene mener at bestemmelser i PSD 2 og anbefalinger fra SecurePay er en risiko, jf. for eksempel "overlay services".[27]

[25] The Open Web Application Security Project (OWASP) – verdensomspennende ikke-kommersiell organisasjon som jobber for å fremme IT-sikkerhet: https://www.owasp.org/index.php/Main_Page
[26] Ondartet kode i foretakets systemer. Koden går ubemerket og over lengre tid.
[27] Tredjeparts tjenester i grensesnittet kunde-bank.

Fem av foretakene mener DDoS er og vil være en trussel. Betydelige tiltak er iverksatt, og risikoen for skade er redusert i betydelig grad.

Tre av foretakene melder at verdikjedene er lange, og at det er stor risiko knyttet til dette, når det gjelder testing, overvåking, ansvar og kontroll.

Ni av foretakene gir uttrykk for at kostnadspress og leveransepress er en stor risiko.

To av foretakene peker på innsidetrusselen.

Fire av foretakene peker på risikoen forbundet med gammel kjerneløsning (kundereskontro).

Ingen av foretakene mener at mobilbank er stor risiko, og to foretak mener at det foreløpig er liten risiko knyttet til mobilbank.

4.2.2 Spørreundersøkelse

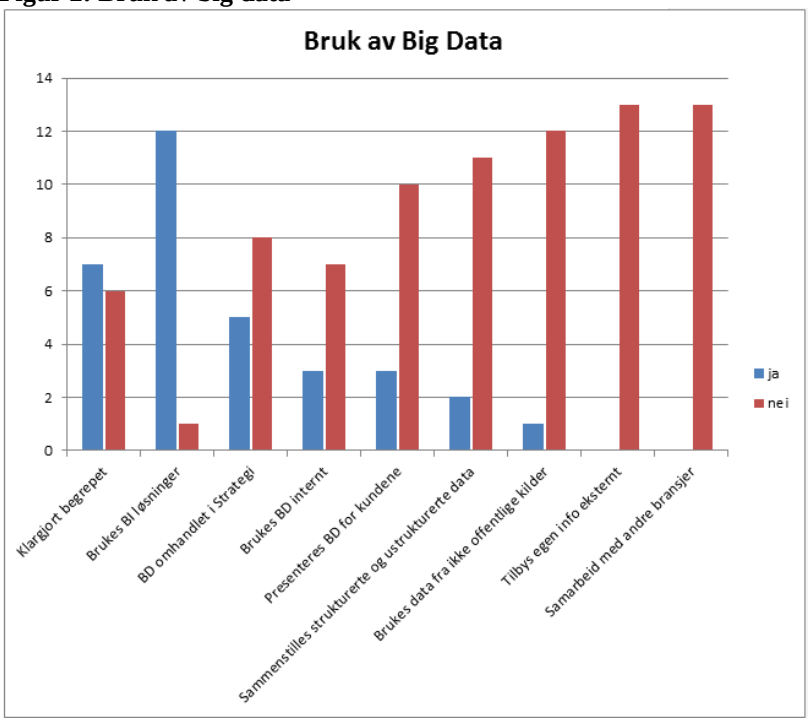
Som et ledd i å kartlegge noen områder som er i sterk utvikling og derfor kan representere en operasjonell risiko, gjennomførte Finanstilsynet en spørreundersøkelse. Banker og forsikringsselskaper ble bedt om å svare på spørsmål knyttet til temaene:

- bruk av big data
- bruk og utvikling av apper
- bruk/planer for bruk av skytjenester

Bruk av big data (BD)

Mange banker i Norge har tatt i bruk big data på enkelte områder. De fleste bankene benytter business intelligence-verktøy for å analysere data i sine datavarehus, og det er stort sett slike opplysninger som også deles med kundene. Noen har startet med datainnsamling også fra andre kilder, men ingen deler opplysninger med tredjeparter, eller samarbeider om slike løsninger.

Figur 2: Bruk av big data



Kilde: Finanstilsynet

Bruk og utvikling av applikasjoner (apper)

Foretakene svarer at apper behandles på lik linje med andre kanalløsninger, og at de utvikles gjennom standard metodeverk. De fleste foretakene kjøper utvikling av apper fra eksterne tjenesteleverandører, men det er foretakets krav til utvikling og test som følges i utviklingsløpet. Appene designes for å tilfredsstille samme krav til sikkerhet og kvalitet som andre webbaserte kanalløsninger.

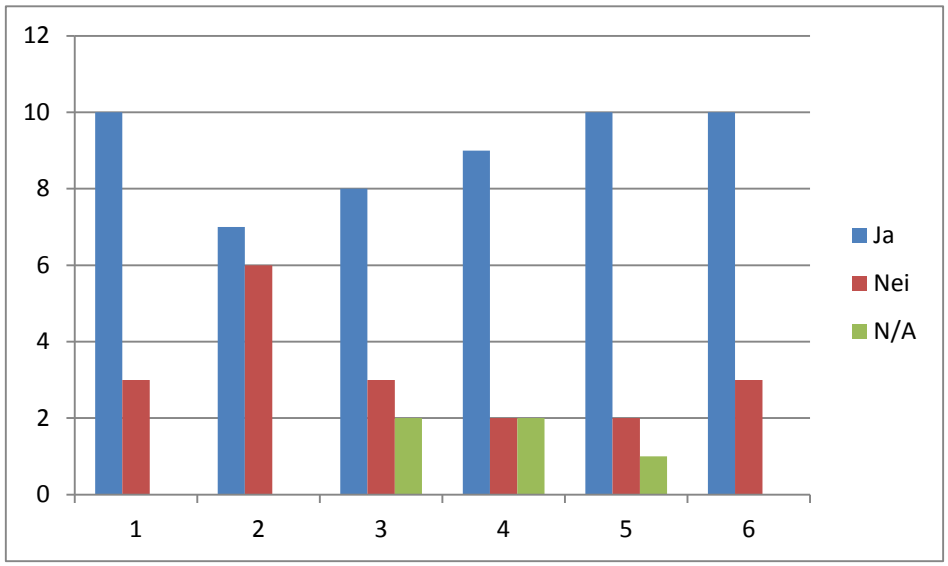
Flere foretak har utviklet apper som benytter GPS, kamera og kontaktliste for "hvor er vi", men funksjonen logger data kun lokalt på enheten.

Bruk/planer for bruk av skytjenester

Foretakene ble stilt disse spørsmålene:

1. Har foretaket tatt i bruk eller vurderer å ta i bruk skytjenester?
2. Har foretaket i sin strategi besluttet å ta i bruk skytjenester?
3. Før bruken av skytjenester ble tatt inn i strategien, ble det gjennomført risikoanalyser?
4. Omfattet risikoanalysene hensynet til overholdelse av lover og regler?
5. Er det områder i foretakets portefølje som er særlig egnet for bruk av skytjenester?
6. Har foretaket vurdert hvordan etterlevelse av konfidensialitet, integritet og tilgjengelighet skal sikres ved bruk av skytjenester?

Figur 3: Svarfordeling på bruk/planer for bruk av skytjenester



Kilde: Finanstilsynet

Svarene viser at foretakene har løftet problemstillingen rundt bruk av skytjenester opp på et strateginivå, gjennomført risikoanalyser og vurdert bruk av skytjenester opp mot lover og regler.

De områdene foretakene vurderer som best egnet for bruk av skytjenester, er åpne anonyme data som kan publiseres eksternt, kontorstøtteløsninger for intern samhandling og anonymiserte personopplysninger for kundebehandling. Utfra svarene å dømme er skytjenester ikke aktuelt å benytte for foretakenes kjernevirksomhet. Kontroll over egne kundedata er viktig.

Foretakene ble bedt om å rangere viktigheten av følgende temaer når det gjelder valg av skytjeneste:

1. Tilgjengelighet
2. Kostnadsårsaker
3. Sikkerhet
4. Enkelhet
5. Stabilitet
6. Tilgang på ressurser/kompetanse

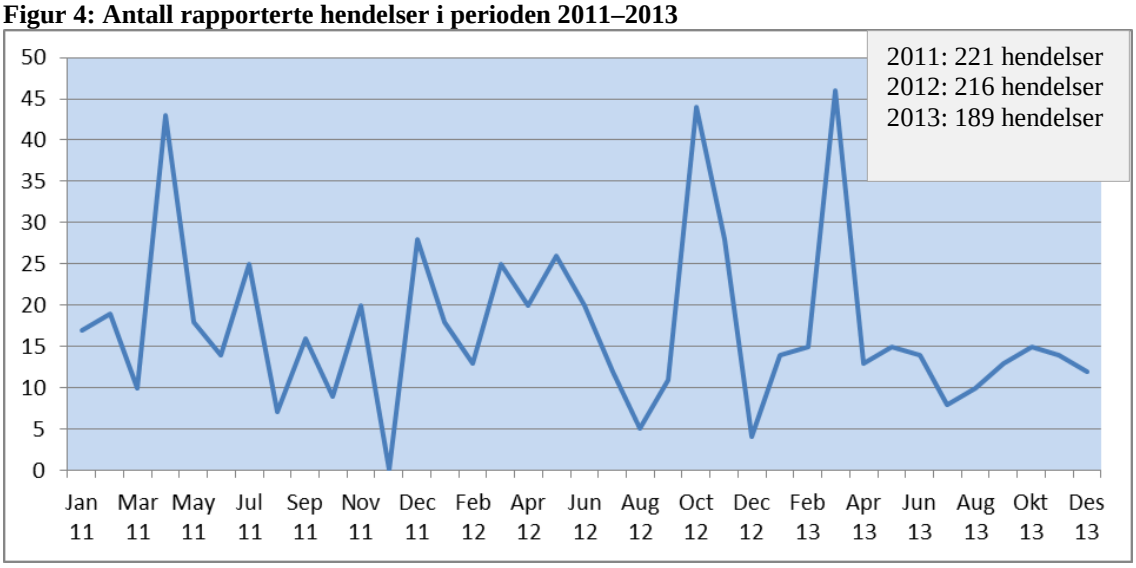
Sikkerhet i løsningen ble rangert høyest, dernest kom kostnader. Tilgang på ressurser/kompetanse kom ut som det minst viktige i følge denne spørreundersøkelsen.

4.3 Rapporterte hendelser i 2013

Svikt i den operasjonelle driften, utilsiktede hendelser eller tilsiktede angrep mot betalingstjenestene skal rapporteres til Finanstilsynet.

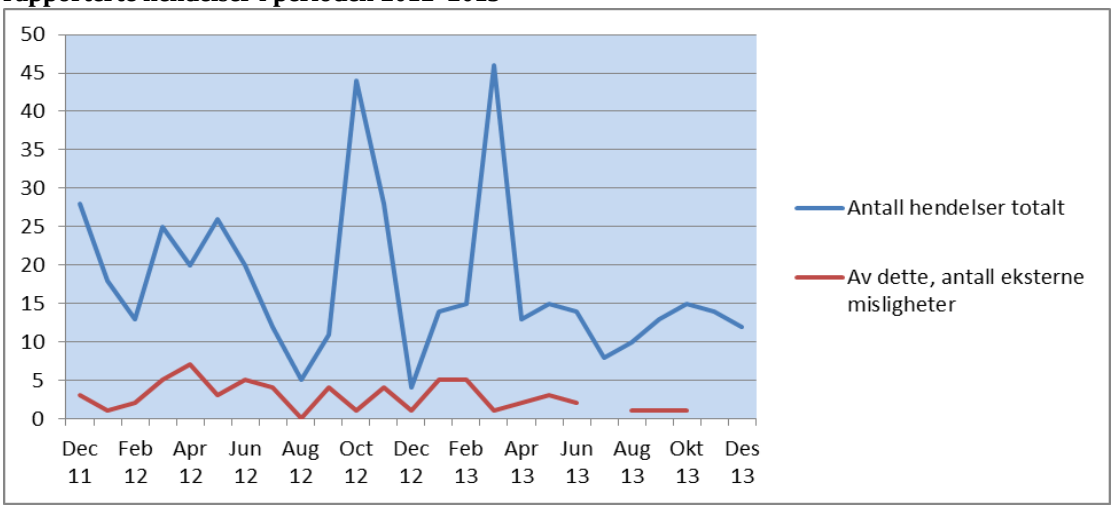
Det ble rapportert noe færre hendelser i 2013 enn i de to foregående årene. Driftsstabiliteten har jevnt over vært bedre, men alvorlige driftsavbrudd forekom i 2013 hos de fleste bankene. Trojanerangrepene var betydelig redusert i 2013 i forhold til i 2012. Phishing-angrep økte derimot både i omfang og i variasjon.

Figur 4: Antall rapporterte hendelser i perioden 2011–2013



Kilde: Finanstilsynet

Figur 5: Antall rapporterte eksterne misligheter (ondsinnede angrep) i forhold til totalt antall rapporterte hendelser i perioden 2012–2013



Kilde: Finanstilsynet

4.3.1 Driftshendelser i sårbar infrastruktur

Våren 2013 var det to alvorlige hendelser som viste sårbarheten ved svikt i felles infrastruktur. 4. mars var det et nettverksbrudd i Evry som varte ca. fire timer, og 18. mars var det et nettverksbrudd i Nets som varte ca. to timer. Ved begge hendelsene var det feil i en nettverkskomponent, og sekundær løsning fungerte ikke som den skulle.

Nettverkskomponenten var inngangsport til en lang rekke betalingstjenester. Finanstilsynet mener det er grunn til å gjennomgå nettverksarkitekturen hos leverandørene for å hindre at brudd i én komponent kan ramme mange kritiske tjenester samtidig og har tatt dette formelt opp med leverandørene.

4.3.2 Mangelfull test

Mange hendelser i 2013 var forårsaket av feil i applikasjon, implementering eller driftsoppsett og resulterte i feilaktig svar til bruker/kunde. Det var mange uheldige konsekvenser som f.eks. at kunder fikk tilsendt kontooversikter med feil i kontoopplysningene. Mange av disse hendelsene kunne vært unngått ved bedre test. Akseptansetest skal utføres av foretaket selv som en siste garanti for at produktet/tjenesten er i henhold til spesifikasjonen. Om avviket ikke blir oppdaget tidligere i testløpet, skal det fanges opp av foretakets akseptansetest.

4.3.3 Økning i phishing-angrep

I 2013 var det en økning i svindelforsøk av typen phishing for å lure folk til å gi fra seg sensitiv informasjon. Folk mottok svært mange e-poster, angivelig fra finansforetak som VISA, Teller, Western Union, Nets, DNB, SpareBank 1, andre banker eller fra teleleverandører som Telenor og Netcom. Stadig nye scenarier ble presentert. Ofte var det nødvendige sikkerhetsoppdateringer som var grunn til å be om betalingskort- eller kontonummer. De fleste var skrevet på et dårlig norsk språk,

mens e-poster som utga seg for å være fra internasjonale finansforetak som Western Union, VISA o.l., var skrevet på engelsk og var bedre formulert. Ved å klikke på en lenke i disse e-postene kunne datamaskinen bli infisert og dermed være sårbar for mer alvorlige trojaner-angrep. Det kan være at 2013 var et år hvor data og informasjon samles inn for å forberede angrep.

4.3.4 DDoS-angrep i 2013

Økningen i DDoS-angrepene i 2012 fortsatte gjennom 2013. Tiltakene både hos foretakene selv og hos internettleverandørene (ISP-ene) har blitt styrket, slik at til tross for flere angrep, påvirket angrepene i liten grad tilgjengeligheten. I 2013 var det en ny type målrettet DDoS-angrep, og i september ble et større forsikringsforetak utsatt for et DDoS-angrep der angriperne ga konkrete trusler.

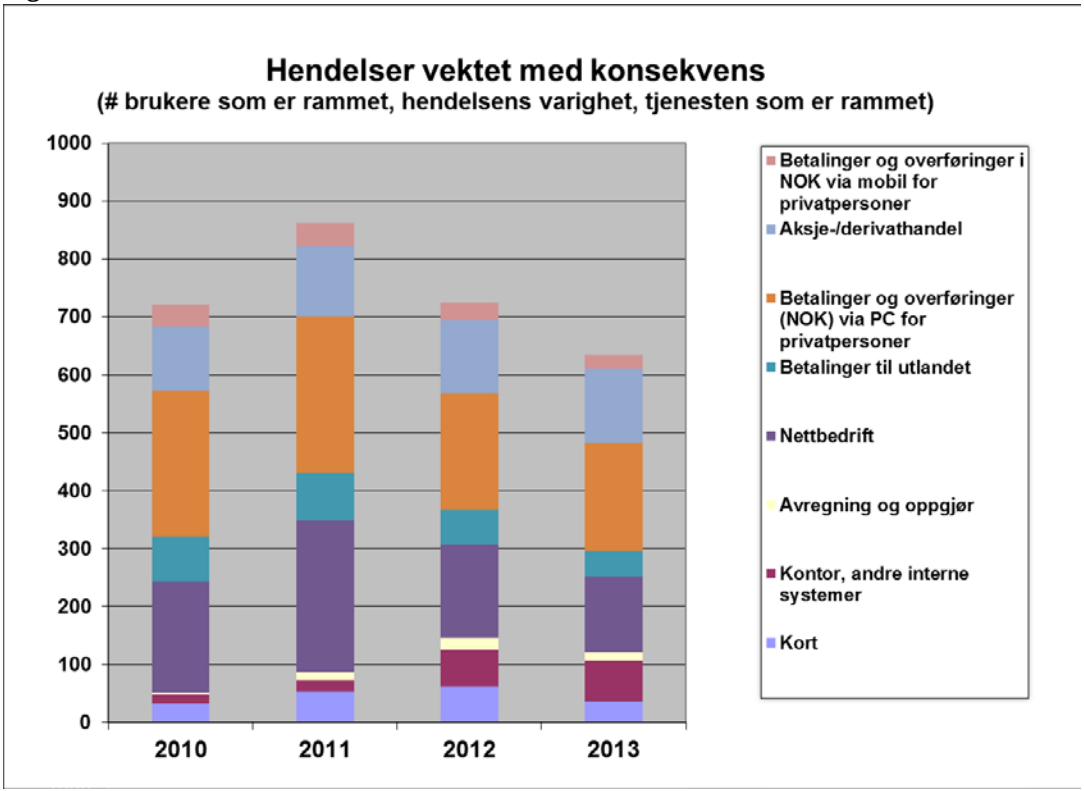
4.3.5 Analyse av hendelsene som et mål på tilgjengeligheten

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 følge med på utviklingen.

Figuren viser at betalingssystemet i mindre grad enn foregående år har vært utilgjengelig for publikum. Årsaken kan være at kvalitetsforbedringsarbeidet som gjøres hos viktige leverandører, har gitt resultater. Dersom tilfanget av nye tjenester var mindre i 2013 enn i foregående år, kan dette også være en medvirkende årsak. Foretakene har tidligere år iverksatt tiltak mot ID-tyveri, DDoS og APT (Advanced Persistent Threat), noe som kan ha medvirket til reduksjonen.[28]

[28] Dette er en samlet vurdering, og enkeltforetak kan derfor oppleve avvik fra det generelle bildet.

Figur 6: Hendelser vektet med konsekvens



Kilde: Finanstilsynet

4.4 Risikoområder identifisert fra andre kilder

4.4.1 Intervjuer med sikkerhetsselskaper og internettleverandører

Høsten 2013 hadde Finanstilsynet samtaler med noen sentrale aktører for sikkerhetsløsninger og overvåking i Norge.

Finanstilsynet merket seg noen punkter fra disse samtalene:

Etter avsløringene av angrepene mot Telenor i 2013 og bedre dokumentasjon av det som synes å være en internasjonal trend med økende digital industrispionasje, er det gitt høyere prioritet å avdekke og sette inn tiltak mot industrispionasje. Mørketallene for slike angrep har vært betydelige, trolig grunnet frykt for å offentliggjøre informasjon som kan gi negativ publisitet.

Antallet DDoS-angrep er økende, trolig på grunn av at slike angrep nå enkelt kan kjøpes som en service på "lysskye" markedsplasser. Konsekvensene er imidlertid mindre grunnet bedre overvåking, verktøy og rutiner for mottiltak både hos ISP-ene og hos det enkelte selskap.

Myndigheter og IT-brukere i de nordiske landene er blant de mest bevisste i verden når deg gjelder datasikkerhet, og har lavest infiseringsgrad av virus og ondsinnet programvare.

Koordinerte tiltak mellom myndigheter, internettleverandører, politi og etter hvert også de ulike CERT-ene har gitt en stadig bedre beskyttelse mot uønskede konsekvenser ved cyberangrep. Det vurderes som viktig at dette samarbeidet videreføres.

4.4.2 Rapporter fra internasjonale sikkerhetsorganisasjoner

ENISA (European Union Agency for Network and Information Security) vurderer i sin trusselsrapport for 2013[29] følgende trusler som de mest alvorlige:

1. Angriperne blir stadig mer sofistikerte i sine angrep og bruker stadig mer avanserte verktøy.
2. Verktøy som tidligere ble benyttet mot PC-plattformer er nå konvertert til å kunne benyttes mot mobile løsninger.
3. Ikke bare en håndfull, men ganske mange nasjonalstater har nå kapasitet til å utføre målrettede angrep, for eksempel av typen APT (Advanced Persistent Threat), både mot myndigheter, private og offentlige selskaper.

To nye områder som er i sterk utvikling kan utfordre sikkerheten:

4. Internet of Things (IoT) og big data.

ENISA viser også til positive trender i 2013:

5. Politiet har lykkes med å stenge flere viktige kriminelle nettsteder og arrestere nøkkelpersoner knyttet til disse miljøene.
6. Antall rapporter og data om cyber-angrep har steget, og det har også kvaliteten på tilgjengelig informasjon. Dette gjør det mulig å utføre bedre trusselanalyser og målrettet sikkerhetsarbeid.
7. Systemleverandørene har redusert responstiden mot nye trusler ved raskere tilgjengelighet til sikkerhetsoppgraderinger.
8. Samarbeid mellom en del relevante sikkerhetsorganisasjoner er i støpeskjeen og vil tilta i tiden som kommer.

Fortinet[30] (internasjonalt selskap for sikkerhetsprodukter) beskriver i "Cybercrime Report" for 2013 hvordan moderne datakriminalitet ligner på vanlig, legal IT-virksomhet. Godt organiserte virksomheter leverer delprodukter "as a service" med en ferdig prisliste. Man kan kjøpe konsulenttjenester, leie botnett, få tilpasset DDoS-angrep og kjøpe kode som utnytter svakheter for å infisere datamaskiner.

[29] http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats

[30] http://www.fortinet.com/resource_center/whitepapers/cybercrime_report_on_botnets_network_security_strategies.html

På den positive siden nevner Fortinet utviklingen med at myndigheter, software-leverandører og sikkerhetsorganisasjoner samarbeider om Computer Emergency Response Team (CERT). Slik har man klart å stanse de største botnettene.[31] Men de peker også på at en kritisk suksessfaktor er nødvendigheten av internasjonalt samarbeid.

[31] Botnett (Bot kommer av siste ledd i ordet Robot) er et nettverk av datamaskiner, knyttet opp til Internett, der datamaskinens eier selv ikke er klar over at datamaskinen er tatt over av utenforstående gjennom bruk av trojaner, datavirus eller på annen måte.

5 Risikoområder

I dette kapitlet beskrives de risikoene som Finanstilsynet vurderer som de mest alvorlige for finanssektoren.

5.1 Omfattende endringer i finanssektorens IT-virksomhet

Som beskrevet i kapittel 3.6, er Finanstilsynet kjent med at flere av de store finansforetakene gjennomfører, eller vil gjennomføre, omfattende endringer i sin IT-virksomhet, både på system- og driftssiden. Utskifting av leverandører og driftssteder, endringer av driftsopplegg og driftsarkitektur, insourcing og økt bruk av utkontraktering og offshoring er eksempler på endringer. Flere av endringene medfører også personellendringer, som omstilling og nedbemanning. Også hos flere av de sentrale IT-leverandørene pågår det eller planlegges det betydelige endringer. Dette gjelder særlig der leverandøren blir påvirket av finansforetakenes valg.

Endringene har ulikt omfang og har ulike begrunnelser. Kostnadsbesparelser, kvalitetsforbedringer og krav til økt effektivitet og fleksibilitet er blant hovedgrunnene. Det pekes også på at endringene, når de er gjennomført, vil redusere sårbarhet og risiko.

Generelt medfører endringer økt operasjonell risiko, noe også foretakene synes å være enig i. I intervjuene (jf. kapittel 4.2.1) framkommer det at nettopp endringshåndtering vurderes å være en av de største risikoene. Finanstilsynet har erfart at de fleste og største innrapporterte hendelsene faktisk har skjedd i forbindelse med endringer. Det er av vesentlig betydning at foretakene kontrollerer og styrer risikoene relatert til de pågående og omfattende endringene.

5.2 Samhandling mellom flere aktører

Mange av endringene, omtalt i avsnittet over, innebærer at flere leverandører blir involvert i verdikjeden til ett og samme foretak. Der det tidligere har vært én hovedleverandør på IT-siden, splittes nå tjenester og leveranser mellom flere leverandører (multisourcing).

Det kan være mange fordeler med en slik modell. Finanstilsynet mener imidlertid at modellen kan gi opphav til uklare ansvarsforhold og mangelfull samhandling og koordinering, noe som kan medføre økt risiko, spesielt ved en krisesituasjon. Finanstilsynet viser til "påskehendelsen" i 2011, der nettopp

manglende samhandling var en problemstilling for å redusere omfanget og konsekvensene av den utløsende hendelsen. Multisourcing kan også gjøre det utfordrende for foretaket å skaffe tilstrekkelig innsikt i internkontrollen og risikoen i den totale utkontrakterte IT-virksomheten. Risikostyring og omfattende avtaleverk er nødvendig.

5.3 Mangelfulle risikovurderinger

Finanstilsynet har i tidligere ROS-analyser påpekt at risikovurderinger og risikostyring er et forbedringsområde. Området synes fremdeles å være en utfordring. Jevnt over gjøres det riktignok årlige risikovurderinger etter bestemmelsene i risikostyringsforskriften og IKT-forskriften, men arbeidet er av ujevn kvalitet og kan ofte være mangelfullt. Finanstilsynets erfaring er at for mange risikovurderinger og risikoreduserende tiltak ikke blir fulgt opp på en tilstrekkelig systematisk måte. Det framkommer ofte ikke om tiltakene er gjennomført og om de har hatt forventet effekt på risikoen. Det kan være vanskelig å se hvordan risikoanalysene faktisk benyttes godt nok som et hjelpemiddel for å styre risikoen og bidra til at foretaket når sine mål.

Finanstilsynet har inntrykk av at foretakenes risikoanalyser i for stor grad har et overordnet perspektiv og ikke i tilstrekkelig grad sikrer seg kompetanse på områdene som skal analyseres. Personell som arbeider med daglig drift og utvikling har ofte best mulighet for å oppdage risikoer. Systematisk arbeid med risiko og tilstrekkelig dokumentasjon må innarbeides som del av den daglige driften. Risikoanalyser er et helt vesentlig virkemiddel for å sikre at det å ta i bruk nye løsninger eller endre eksisterende skjer på en hensiktsmessig måte og med akseptabel risiko.

5.4 Angrep mot betalingstjenestene

Betalingstjenestene er fortsatt under angrep av kriminelle. Dette gjelder for de fleste elektroniske kanaler der betalingstjenestene er distribuert helt ut til kunden direkte gjennom nettbank, eller via offentlig salgssted, minibank for kontantbetjening, handel i butikk eller via nettbutikk. Riktignok viser bankenes tap at det på en rekke områder var en klar nedgang i 2013, mens det på bruk av kort mot nettbutikk – card-not-present – var en klar økning i tapene. Det kan ikke utelukkes at dette kan ha sammenheng med de store datainnbruddene som skjedde hos internasjonale databaser for kortnummer.

Basert på informasjon fra ulike kilder har Finanstilsynet grunn til å tro at kriminelle grupper arbeider med å videreutvikle angrepsmetoder både mot nettbanker, minibanker og EFT/POS-terminaler og at det som skjer av angrep mot løsninger i det enkelte land, vil gå i bølger og kan komme uventet. Det er derfor all grunn til å opprettholde det viktige arbeidet som skjer med å bygge forsvar og tette sårbarheter. Det var stor phishing-aktivitet i 2013, og det kan ses på som en forfase til angrep. Om det skjer angrep, kan avhenge av de kriminelles vurderinger av muligheten for å lykkes ut fra informasjon de kan ha om forsvarsevnen. Selv om 2013 ikke var et år med økende tap generelt, er det likevel store beløp som blir tapt, og det er all grunn til å ha en målsetting om at tapene skal reduseres ytterligere.

5.5 Risiko fra eldre design

Finanstilsynet har i tidligere års ROS-rapporter pekt på et stadig mer påtrengende behov for å erstatte eldre, såkalte legacy-systemer. Kompetansen på gamle systemer vil etter hvert forsvinne, og vedlikehold og drift blir mer utfordrende.

Hver tjeneste ble bygd som en isolert vertikal silo, der brukergrensesnittet er øverst og grunndata nederst. Nye tjenester må for en stor del bygges på nytt fra bunn til topp.

Denne tidligere mangelen på innebygd fleksibilitet i systemene gjør det vanskelig å realisere dagens krav til stadig nye tjenester og nye kundekanaler. Man har kompensert for dette ved å løfte grunndata ut i kopier. Kunde og kontodata ligger etter hvert i flere kopiregistre, og det er krevende å holde disse oppdatert.

Moderne systemer derimot, består av funksjoner som kobles til tjenestene via en "tjenestebuss". Gjenbruk gjør at utviklingstiden ("time to market") blir redusert, og risikoen for feil blir mindre.

6 Finanstilsynets oppfølging

6.1 IT-tilsyn og annen kontakt med foretakene

Oppfølging av foretakenes IT-risikoer skjer primært gjennom tilsyn. Finanstilsynet vil i 2014 ha oppmerksomhet på de tilsynsenhetene og leverandørene som har størst innvirkning på finansiell stabilitet og velfungerende markeder.

Særlig oppmerksomhet vil være rettet mot operasjonell risiko i banksektoren når det gjelder tilsynsenhetenes sentrale IKT-systemer og utkontraktering. Finansforetak som gjennomfører større endringer, inkludert utkontrakteringer, på IT-området og dermed kan øke risikoen, vil vektlegges. 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.

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.

Finanstilsynet har løpende kontakt med de større foretakene, knyttet til den generelle IT-risikosituasjon, utviklings- og endringsprosjekter eller hendelser.

6.2 Arbeid med betalingssystemer

Finanstilsynets generelle tilsynsansvar er hjemlet i finanstilsynsloven og gjennom forskriftene om risikostyring og internkontroll og bruk av IKT. Oppgaver spesielt knyttet til systemer for betalingstjenester er i tillegg regulert gjennom lov om betalingssystemer, kapittel 3.

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 egen forskrift med hjemmel i betalingssystemloven for systemer for betalingstjenester og forslag om endringer til IKT-forskriften. Endret regelverk vil bli fulgt opp og eventuelt innarbeidet i

tilsynsopplegget.

Når det gjelder arbeidet med betalingssystemer har Finanstilsynet også her en oppmerksomhet på tilsynsenhetene og leverandørene som har størst innvirkning på finansiell stabilitet og velfungerende markeder, med særlig oppmerksomhet på operasjonell risiko. 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.

6.3 Regelverksutvikling i Norge

Basert på Finanstilsynets informasjon om utviklingstrekk og risikobilde arbeider tilsynet med forslag om regelverksendringer på områder knyttet til utkontraktering og risiko i betalingstjenestene:

Til finanstilsynsloven:

- en generell meldeplikt til Finanstilsynet ved utkontraktering
- et sterkere hjemmelsgrunnlag for nærmere vurderinger av utkontraktering som vurderes å ha for høy risiko

Til IKT-forskriften:

- en særlig meldeplikt til Finanstilsynet ved utkontraktering av IKT-systemer.
- utkontraktering av IKT som har betydning for foretakets virksomhet, skal godkjennes av styret i foretaket
- nye regler om sikkerhet og risiko ved etablering og endring av betalingstjenester

Til lov om betalingssystemer:

- Krav til sikkerhetsnivå ved bruk av elektroniske betalingstjenester. Meldeplikten beskrevet i rundskriv skal tas inn i forskriften. Forslaget til ny forskrift kan bidra til sikrere betalingstjenester for brukerne og stiller konkrete krav til utformingen slik at forbrukerne skal være bedre beskyttet mot svindel.

Forslag om endringer i finanstilsynsloven og betalingssystemloven er oversendt Finansdepartementet.

Meldeplikt om etablering og drift av systemer for betalingstjenester
Foretakene skal uten unødig opphold gi melding til Finanstilsynet om etablering og drift av systemer for betalingstjenester, jf. lov om betalingssystemer § 3-2. Meldeplikten er utdypet i Finanstilsynets rundskriv 17/2004 med tilhørende egenmeldingsskjema. Meldingene er viktige for at Finanstilsynet skal kunne følge med på endringer som skjer i betalingstjenester, fange opp bruk av ny teknologi og valg av nye tjenesteleverandører og ikke minst kunne følge de operasjonelle risikoene relatert til slike tjenester.

Finanstilsynet mottar generelt få meldinger. Det er derfor grunn til å anta en underrapportering, også basert på kontroll ved tilsyn, og at foretakene ikke i tilstrekkelig grad etterlever rapporteringsplikten. Finanstilsynet vil fremme forslag om å benytte forskriftshjemmelen i betalingssystemloven og erstatte Finanstilsynets rundskriv 17/2004 med en forskrift.

6.4 Hendelsesrapportering

Foretakene skal rapportere vesentlige hendelser til Finanstilsynet, jf. IKT-forskriften § 9. Innrapporterte hendelser samles i Finanstilsynets hendelsesdatabase, der de blir analysert og brukt som grunnlag for eventuelle tiltak. Hendelsesdatabasen er en verdifull kilde for analyse av trender og sammenhenger, den gir et godt innblikk i foretakenes operasjonelle risikoer og vil synliggjøre tema som Finanstilsynet eventuelt vil ha behov for å følge opp.

Finanstilsynet er generelt fornøyd med foretakenes innrapportering, men ser at det fortsatt er et forbedringspotensial i rapporteringen. Det vil derfor bli arbeidet videre med å sikre korrekt og rettidig informasjon som grunnlag for eventuell reaksjon og eventuelle tiltak.

For å sikre rapportering på et riktig nivå fra andre typer finansforetak enn bankene, planlegger Finanstilsynet å arrangere et miniseminar om hendelsesrapporteringen for forsikringsselskapene i 2014. Det årlige hendelsesrapporteringsseminaret for de rapporteringsansvarlige og bilaterale oppfølgingsmøter med enkeltforetak vil fortsette.

6.5 Beredskapsarbeid

Gjennom samarbeid med finansnæringen, Norges Bank, andre myndigheter og sentrale tjenesteleverandører er det lagt vekt på beredskapsarbeid, enten det er mot næringen som helhet, mot foretakene selv eller mot foretakenes underleverandører. Det er et arbeid som vil ha fortsatt oppmerksomhet, blant annet gjennom tilsyn, videre oppfølging av beredskaps- og katastrofeløsninger og egnede øvelser.

Finanstilsynet er også involvert i et nordisk, europeisk og internasjonalt tilsynssamarbeid, noe som vil videreføres. I sammenheng med hendelser på nettet deltar tilsynet også i et europeisk samarbeid om sikkerhet på nettet.

Etableringen av FinansCERT Norge, i regi av Finans Norge, vurderes som et hensiktsmessig tiltak i arbeidet med å sikre elektroniske betalingsløsninger. Likeledes er etableringen av egne forretningsenheter for viktige felles betalingstjenester og infrastruktur et hensiktsmessig tiltak.

Beredskapsutvalget for finansiell infrastruktur (BFI)
Finanstilsynet har ansvaret for å lede utvalget og er også sekretariat for utvalget, og tilsynet vil fortsette sitt arbeid med å utvikle BFIs rolle, både på vegne av myndighetene, bransjen og det enkelte finansforetak.

BFI representerer en viktig møteplass mellom ulike aktører i Norge som har oppgaver innenfor det norske betalingssystemet. Utvalget har en særlig oppmerksomhet mot beredskapsarbeidet og er derfor opptatt av å følge opp hendelsesutviklingen. Ett av tiltakene er planlegging og gjennomføring av årlige øvelser, med myndigheter, finansinstitusjoner og leverandører som deltakere, for å være best mulig forberedt om det skjer en alvorlig hendelse.

6.6 Videreutvikling av tilsynsverktøy

Internasjonal beste praksis som Cobit, ITIL og ISO er lagt til grunn for de 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 à jour med beste praksis, og Finanstilsynet vil løpende sørge for å videreutvikle tilsynsmetoder og verktøy gjennom erfaring fra gjennomførte tilsyn og kunnskap om beste praksis på området. I 2014 planlegges en større omarbeiding av metodeverket basert på siste beste praksis innen rammeverk på prosedyrenivå som blant annet Cobit. I tillegg vil det bli vurdert å utvikle et verktøy for målrettede innrapporteringer.

7 Betalingssystemer og utvikling

7.1 Generelt om betalingssystemer

Betalingssystemene er sentrale for all økonomisk aktivitet. I Norge blir betalingssystemene regulert gjennom lover og forskrifter og gjennom finansnæringens selvregulering, forvaltet av Finans Norge.

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 betalingstjenestetransaksjoner mellom kunde og bank.

Pålitelighet, tempo og effektivitet er hjørnesteiner i økonomien og hvor bankenes betalingssystemer med "4-kantmodellen" har vært helt sentrale. Teknologiutviklingen har i vesentlig grad påvirket systemene for betalingstjenester og gjort at mer og mer av betalingsformidlingen skjer helelektronisk, inklusive tilstøtende verdikjeder både i forkant og i etterkant av selve betalingsverdikjeden.

Teknologiutvikling kombinert med deregulering og nye lovregler, der særlig EU er en pådriver, i tillegg til forbrukernes og foretakenes forventninger/krav til enkelhet og valgfrihet, gjør at tradisjonelle modeller for betalingssystemer utfordres.

Nye og mer effektive betalingsmetoder, nye bærere av "penger", aktører som etablerer seg med forskjellige modeller i "man in the middle"-roller, virtuelle valutaer, nye "oppgjørsmekanismer" og kostnadseffektivisering er noe av det som skaper endringer innenfor betalingsformidlingslandskapet.

Markedet forventer raskere og mer effektive løsninger med økt brukervennlighet for å betale for varer og tjenester, der balansegangen mellom konkurranse og samarbeid påvirker markedets effektivitet og tilgjengelighet, og der brukervennlighet må balanseres mot krav til sikkerhet. Dette kan føre til at betalingsverdikjedene blir lengre, krav til ansvarsforhold mellom aktører blir viktig og nye sikkerhetsløsninger må introduseres. Dette kan føre til at risikoen øker.

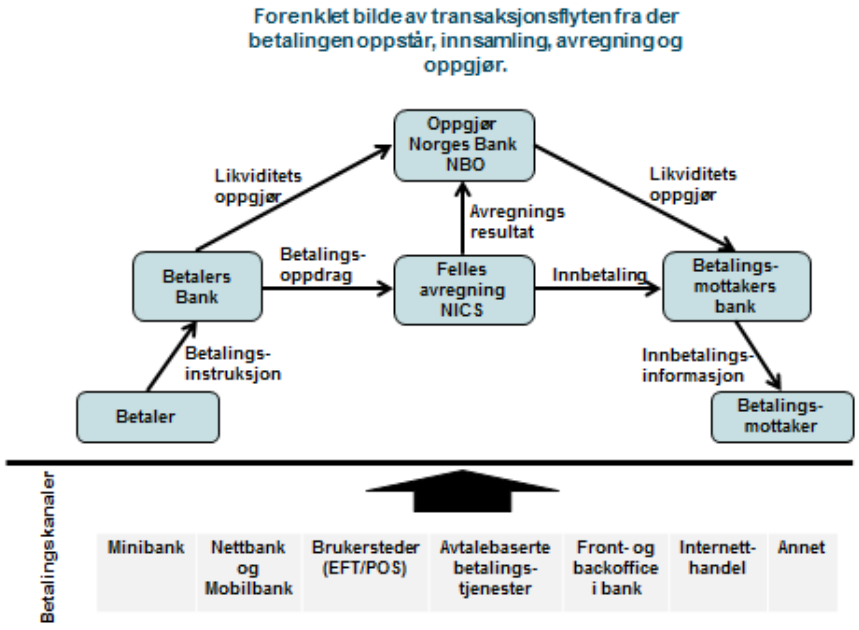
Finansavtaleloven[32] og EUs betalingstjenestedirektiv er sentrale forsvarsverk etablert for å ivareta

[32] http://lovdata.no/dokument/NL/lov/1999-06-25-46

forbrukerhensyn og best mulig sikre forbrukers sikkerhet og rettigheter.

Figur 7 viser transaksjonsflyten i det norske betalingssystemet. Nederst i figuren er det en illustrasjon av de ulike betalingskanalene som kundene benytter.

Figur 7: Transaksjonsflyten i det norske betalingssystemet



Kilde: Finanstilsynet

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

7.2 Risiko og sårbarhet i betalingssystemene

Teknologien vil bringe med seg nye og til dels ukjente bruksområder og muligheter, men også nye risiko- og sårbarhetsområder.

Aktørlandskapet endres, både på bakgrunn av dynamikken i markedet, myndighetsreguleringer, vekt på kostnadsreduksjon og strategiske grep hos enkeltaktører.

Brukervennlighet og hastighet synes å være dominerende i kampen om betalingstjenestemarkedet. Dette endrer seg raskt, slik at det som nå synes markedsledende, kan vise seg å bli akterutseilt. I dette kappløpet kan sikkerhet bli en konkurranseparameter, men det kan også bli skadelidende som følge av

for sterk vektlegging på brukervennlighet, kostnadsbesparelser og "time to market".

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.

7.2.1 Bruk av ondsinnet programvare mot betalingstjenester

Bruk av phishing, der svindler utgir seg for å være kjente finansforetak eller betalingstjenestetilbydere, er blitt en svært vanlig metode for ulovlig innsamling/tyveri av data. I 2013 hadde dette et økende omfang, selv om det var en nedgang i fjerde kvartal. Denne typen kriminalitet er særlig rettet mot betalingskort der misbruket ofte skjer gjennom betaling i nettbutikker som ikke stiller krav til sikkerhetsløsninger som BankID eller 3D-Secure, eller hvor svindlerne utnytter oppdagede svakheter hos betalingstjenesteleverandører. Finanstilsynets erfaring er at foretakene har god beredskap og iverksetter effektive tiltak som reduserer tapsomfang ved å informere kundene, og raskt få stengt ned falske websider, fange opp svar på henvendelser og overvåke transaksjoner.

Til tross for at trojanere blir stadig mer sofistikerte og dermed vanskeligere å oppdage av tradisjonell antivirus-programvare, var det en markert aktivitetsnedgang i Norge i 2013. Dette kan hovedsakelig tilskrives aktiv beredskap og godt forsvarsverk kombinert med beskjedne utbytter. Ettersom denne typen angrep har gått i bølger og det fortsatt er stor aktivitet internasjonalt, må man legge til grunn at Norge igjen kan bli rammet av målrettede angrep.

7.2.2 Kortmisbruk og datatyveri

Selv om næringen i Norge gjør mange tiltak og globalt ligger langt framme i arbeidet med å redusere sårbarheter, er kortsvindel en av de høyeste teknologirisikoene som finansnæringen står overfor. Bruk av norske kort skjer også fysisk i utlandet og ikke minst i den virtuelle netthandelen.

Tyveri av kortdata har blitt "big business", og de mest sårbare stedene er der hvor det oppbevares eller videreformidles store mengder kortrelatert informasjon.[33] Manglende sikring av kortdata kan resultere i at hackere får tak i konfidensiell informasjon som kan misbrukes. Informasjon som blir stjålet er ofte tilstrekkelig til at den kan misbrukes i betalingsformidlingen, enten direkte eller indirekte ved å tilegne tilganger eller rettighet som gjør misbruk mulig.

Trusselen om "cyber attacks" mot netthandelssteder har i økende grad blitt en realitet, noe som ble godt synlig da rundt 96 000 norske kortbrukere,[34] i tillegg til noen hundre tusen kortbrukere fra andre land, ble frastjålet sin kredittkort- og/eller kontaktinformasjon i et omfattende hacker-angrep.[35] Banker har i ettertid avdekket kortmisbruk som potensielt kan knyttes til innbruddet. Det er også en frykt for at den stjålne informasjonen kan bli benyttet til målrettet phishing for å innhente mer sensitive data.

Finanstilsynet observerer at det er en økning i tap ved card-not-present, som hovedsakelig er tap

[33] http://www.usatoday.com/story/money/personalfinance/2013/04/14/identity-theft-growing/2082179/
[34] http://coop-norge.mynewsdesk.com/pressreleases/hotellbestillingstjeneste-beroert-av-datainnbrudd-929230
[35] http://news.sky.com/story/1167656/loyaltybuild-hackers-steal-card-details

gjennom misbruk av stjålet kortinformasjon i nettbutikker som ikke stiller krav til 3-D Secure-autentisering, enten nasjonalt eller globalt.

Manglende krav til 3-D Secure-autentisering fra netthandelsstedet, men kun krav til bruk av CVC-kode, utgjør en risiko i betalingsformidlingen. Ved tyveri av kortinformasjon er det lett å misbruke denne i netthandelsbutikker som ikke stiller krav til 3-D Secure-autentisering.

Fortsatt bruk av magnetstripe mange steder gjør svindel med stjålet kortinformasjon lett for kriminelle. Selv om data kryptert på mikrobrikker er tatt i bruk mange steder, som i Norge og Europa, er det andre land som henger langt bak og dermed utgjør innganger for svindel med bruk av stjålet informasjon. Ett av verdens største og mest kjente datainnbrudd[36] ble gjort i fjorårets julehandel i USA. Informasjon ble stjålet fra anslagsvis over 110 millioner kunder.[37, 38 og 39] Dette var blant annet magnetstripeinformasjon fra minst 40 millioner kunder ved tapping av informasjon fra butikkenes kasseterminaler.

Det er også stjålet millioner av krypterte pinkoder uten at det er kjente tilfeller hvor pinkoder er knekket. Laboratorieforsøk[40] viser at pinkoder kan knekkes, men det er likevel usikkert om dette kan skje i praksis fordi det normalt vil være flere sikkerhetstiltak iverksatt enn det som er tatt hensyn til i et laboratorieforsøk.

Bankene har god overvåking for å fange opp misbruk, og kortholdere holdes skadesløse. Likevel vil slike datatyverier medføre mye ekstra arbeid både for kortinnløser, kortutsteder og korteier. Det er viktig at bankene forsetter med relevante tiltak som er mulig både enkeltvis og samlet i næringen.

Et tiltak som kan være effektivt, er krav fra banker og internasjonale betalingskortselskaper om at netthandelssteder skal implementere 3-D Secure-autentisering. Dette vil gjøre det mindre attraktivt med tyveri av kortinformasjon og redusere tap ved card-not-present. Brukersteder som kun opererer med magnetstripe, utgjør også en sårbarhet. I Norge utgjør det riktignok et beskjedent omfang. Det er viktig at magnetstripen blir erstattet av microchipen, men det forutsetter også at alle relevante land gjennomfører dette.

Diversifisering av kort, dvs. kort med og uten magnetstripe, engangskort og engangspassord via mobil er tiltak som bør vurderes.

Manglende etterlevelse av PCI-standarden (PCI DSS)[41] vil kunne skape sårbarheter som hackere leter

[36] http://www.bostonglobe.com/business/2014/01/11/information-million-taken-target-data-breach/J7kRpDwXaxkPk5amUgVdXI/igraphic.html
[37] http://www.usatoday.com/story/news/nation/2013/12/18/secret-service-target-data-breach/4119337/
[38] http://www.bostonglobe.com/business/2014/01/11/information-million-taken-target-data-breach/J7kRpDwXaxkPk5amUgVdXI/story.html
[39] http://www.digi.no/926377/datavirus-i-kassa-rappet-id-er
[40] http://www.jbonneau.com/doc/BPA12-FC-banking_pin_security.pdf
[41] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

etter, ikke minst der det er sannsynlig at store datamengder lagres. I tillegg er det viktig at etterlevelsen av standarden i seg selv er nok, og som et element i å redusere sårbarheter sammen med øvrige risikoreduserende tiltak. Tettere oppfølging av etterlevelsen av PCI-standarden vil være et godt tiltak.

Finanstilsynet erfarer at en del banker har etablert mulighet for regionsperrer. Dette kan gi økt beskyttelse mot misbruk av tappet kortinformasjon og er noe alle banker bør vurdere som tiltak. Riktignok gjelder regionsperre kun for bruk av bankkort i fysiske terminaler og ikke for kredittkort og handel på Internett, men vil likevel være ett element for å redusere mulighet for misbruk.

7.2.3 Mobile betalingsløsninger

Utvikling og bruk av mobile løsninger fortsatte å øke betydelig i 2013, i den grad at bruken er blitt større enn bruken av tradisjonell nettbank.[42 og 43] Det innebærer at mobile løsninger er i ferd med å få en betydelig rolle også innenfor betalingsformidlingen, både som medium for gjennomføring av betalinger, som bærer av digitale lommebøker[44] og som bærer av sikkerhetsløsninger som BankID.

I det norske markedet er det sterk konkurranse mellom aktører som vil sikre at deres teknologi blir normen. Mobile løsninger skal være brukervennlige, og det introduseres stadig nye løsninger. Mobilens små flater utgjør en betydelig mulighet for brukerfeil, og det er en fare for at krav om enkelhet, hurtighet og brukervennlighet kan gå på bekostning av sikkerhet.

De mobile løsningene er i stadig større utstrekning utsatt for de samme farene som tradisjonelle nettbanker. OWASP's (The Open Web Application Security Project) 10 på topp-risikooversikter for mobile og tradisjonelle webløsninger viser at mobile løsninger ligger fem år etter når det gjelder sårbarhetsutviklingen.[45] De samme sårbarhetene som man har hatt i webutviklingen dukker opp i mobilapplikasjoner, ikke nødvendigvis i selve applikasjonen, men på serversiden.

Utviklingen på mobil utgjør i stor grad bruk av ny teknologi, og det er en fare for at kompetansemodenheten ikke alltid er tilstrekkelig. Det er eksempler på at utvikling av mobile løsninger ikke har vært tilfredsstillende kvalitetssikret når det gjelder sikkerhet. Dette har avdekket manglende bevissthet og/eller dårlig koding ved utvikling av løsninger, blant annet ved at falsk informasjon kommer inn i apper og at informasjon lekker ut av apper.[46]

Et risikoaspekt ved mobilen er at den stadig skal dekke flere behov, der betalingsformidlingen bare blir ett av disse. Når mange funksjoner og opplysninger samles på ett sted, skapes det en sårbarhet som betalingstjenestetilbyderne må være bevisste på når de utvikler løsninger.

[42] https://pressesenter.sparebank1.no/2013/04/paskerush-i-mobilbanken/
[43] http://www.dagensit.no/article2582872.ece
[44] http://www.dinepenger.no/bruke/disse-slaass-om-din-mobile-lommebok/22599383
[45] https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks
[46] http://www.dinside.no/923295/nettbank-appene-er-saarbare

Selv om det ikke har vært kjente angrep mot mobile løsninger i Norge, er det viktig at foretakene stiller minst samme krav til sikkerhet for mobile betalingsløsninger som for de tradisjonelle nettbankløsningene, dvs. at de gjør grundige sikkerhets- og sårbarhetsanalyser og iverksetter tiltak, tar grep for å kvalitetssikre sine utviklingsprosesser og sikrer at sensitiv informasjon ikke fraktes over nettet.

7.2.4 Sårbarheter i felles infrastruktur

Flere finansielle tjenester er koblet sammen og deler tekniske ressurser. Feil på en av tjenestene kan føre til at en eller flere av de andre tjenestene også svikter.

Hendelser som oppstår i, eller treffer betalingsinfrastrukturen, rammer bredt og kan raskt medføre store konsekvenser. Det er derfor viktig med regelmessig gjennomgang av risiko- og sårbarhet i nettverksarkitekturen og iverksetting av tiltak for å hindre hendelser som kan ramme mange kritiske tjenester samtidig.

7.2.5 Endringsrisiko i betalingssystemer

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. Driverne omfatter funksjonell modernisering, bruk av ny teknologi, utskifting av delløsninger, etterlevelse av regulatoriske krav og selvpålagte krav i næringen, kostnadsbesparelser og tilfredstillelse av markedets etterspørsel etter effektive, enklere og mer brukervennlige tjenester.

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 gode ende-til-ende testprosesser og etablering av en god sikkerhetskultur i alle ledd, er en sentral del av foretakenes utviklings- og endringsprosesser.

Betalingsformidling er under stadig forandring, og nye aktører etablerer seg. Endrede eller lengre verdikjeder gir behov for klare ansvarsforhold, enten det er mellom applikasjoner, mellom steg i verdikjedene eller mellom forskjellige aktører i verdikjeden. Det er derfor viktig at det gjøres løpende risiko- og sårbarhetsanalyser ved endringer.

7.2.6 DDoS kan ramme betalingsformidlingen og hindre tilgangen til betalingstjenester og sikkerhetstjenester

DDoS-angrep er ikke nødvendigvis det mest framtredende når det gjelder sårbarheter som kan ramme betalingsformidlingen, selv om det var en fortsatt økning i angrep i 2013. Massive målrettede angrep kan gjøre kunderettet betalingsformidling helt eller delvis utilgjengelig over en periode. Erfaringer fra Gartner viser at DDoS-angrep, såkalte lavintensitetsangrep, også er benyttet for å skjule andre angrep hvor betalingsformidlingen er rammet.[47, 48 og 49]

[47] http://www.itavisen.no/nyheter/bruker-ddos-til-%C3%A5-kamuflere-banksvindel-90002

Finanstilsynets erfaring er at foretakene selv og internettleverandørene (ISP-ene) har styrket tiltakene for at angrep i liten grad skal påvirke tilgjengeligheten. Det er likevel viktig at forsvaret mot DDoS-angrep fortsatt vies oppmerksomhet, ettersom DDoS-angrep både kan lamme kunderettede tjenester og kan være et tegn på at annen svindel kan være aktuell.

7.3 Styring og kontroll med betalingssystemene

Det er et ledelsesansvar å sørge for at det enkelte foretak har et etablert rammeverk for styring og kontroll med hele betalingsformidlingen og med fastlagte prosedyrer for viktige funksjoner. Det må etableres kontrollordninger som sikrer etterlevelse av regelverk og av fastlagt 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 akseptabelt nivå, sikre tiltak mot kriminelle angrep og for å unngå alvorlige hendelser. I dette inngår etablering av et kontinuitets- og beredskapsopplegg og regelmessig øving for å være i stand til effektiv håndtering når hendelser inntreffer.

Det er viktig å sikre at alle elementer og aktører i transaksjonskjeden mellom betaler og betalingsmottaker inngår i styringen av operasjonell risiko. Ikke minst blir dette viktig når betalingsformidlingen er i stadig forandring med nye aktører og forretningsmodeller, lengre verdikjeder og endrede ansvarsgrenser. Alle aktører i verdikjeden har et selvstendig ansvar for å sikre nødvendig kompetanse og tid til å kunne styre og kontrollere driften i egne operasjoner, hos IKT-leverandører og ikke minst hos (eventuelle) underleverandører.

Store deler av den elektroniske infrastrukturen som betalingssystemene benytter, er utkontraktert til IKT-leverandører, men foretakenes ansvar for styring og kontroll er det samme og kan ikke utkontrakteres. Sikkerhet er som hovedregel en integrert del av tjenestekjøpet og har de siste årene blitt en økende kostnadstyngende komponent for tjenesteleverandørene. Det er krevende for tjenesteleverandørene å få dette kompensert gjennom avtaleendringer, og det kan derfor være en risiko at sikkerhet ikke blir tilstrekkelig ivaretatt.

7.4 Meldeplikten – 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. Meldingen skal opplyse om at avtaler med deltakende institusjoner og med leverandører er inngått, om forhold knyttet til bruken av tjenesten er ivaretatt og annen risiko knyttet til systemet for betalingstjenesten.

[48] http://www.scmagazine.com/fraudsters-target-wire-payment-switch-at-banks-to-steal-millions/article/307755/
[49] http://blogs.gartner.com/avivah-litan/2013/08/12/ddos-diverts-attention-during-payment-switch-takeover/

Hovedhensikten med meldeplikten er å sikre at nødvendige risikovurderinger er gjort, at nødvendige tiltak for å sikre trygg og sikker operasjonell drift er iverksatt og at eventuelle avtaler mellom aktuelle parter er etablert før en ny betalingstjeneste tas i bruk.

I 2013 mottok Finanstilsynet 38 meldinger, hvorav 23 dreide seg om BankID på mobil, 4 om tilbud av tjenester på håndholdte enheter, 4 om endringer knyttet til utenlandsbetalinger, 2 om vesentlig endret bruk av betalingstjenesten og 2 for andre betalingsrelaterte tjenester. I tillegg mottok Finanstilsynet 3 meldinger som etterrapportering fra tidligere år. Det var i 2013 ikke behov for å følge opp foretakene basert på de mottatte meldingene.

Selv med en vesentlig økning i omfang av meldinger antas det fremdeles å være en underrapportering om endringer av systemer for betalingstjenester, og Finanstilsynet vil komme med tiltak for å sikre at meldeplikten blir overholdt.

7.5 Oversikt over årlige tap knyttet til betalingstjenester

7.5.1 Tapstall i Norge

Tabellene under viser tapstall i Norge for kort- og nettbanksvindel for de tre siste årene. Tapene representerer alle bankene i Norge og er innhentet av Finans Norge og Bankenes standardiseringskontor (BSK) i samarbeid med Finanstilsynet.

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

Svindeltype betalingskort	2011	2012	2013
Misbruk av kortinformasjon, kort ikke til stede (internetthandel)	24 190	35 701	51 954
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort i Norge	468	2 308	762
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort utenfor Norge	57 340	55 869	51 534
Originalkort tapt eller stjålet, misbrukt med PIN i Norge	32 224	28 128	21 274
Originalkort tapt eller stjålet, misbrukt med PIN utenfor Norge	7 008	8 544	9 570
Originalkort tapt eller stjålet, misbrukt uten PIN	4 488	4 603	4 9 49
Totalt	**125 718**	**135 153**	**140 043**

Kilde: Finanstilsynet

Tabell 2: Antall betalingskort rammet av misbruk

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

Kilde: Finanstilsynet

Totaltapet på kortsvindel økte noe i 2013. Det var en betydelig økning i svindel av typen card-not-present (CNP), mens det var en reduksjon i tapene knyttet til andre typer kortsvindel. CNP er handel

med bruk av betalingskort på Internett, telefon eller e-post. Kortinformasjonen kan ha blitt urettmessig ervervet gjennom phishing, eller gjennom datainnbrudd på brukersteder eller innsamlingssentraler for betalingskort. Som nevnt i kapittel 4.3.1, var det en stor økning i phishing i 2013 for å lure folk til å avgi bl.a. betalingskortinformasjon. Finanstilsynet kjenner ikke til at det var innbrudd på norske brukersteder eller innsamlingssentraler i 2013, men kjenner til store datainnbrudd i Irland og USA.

Av det totale transaksjonsvolumet på kortbetalinger i Norge utgjorde svindel omtrent 0,018 prosent. Dette er lavere enn i eurolandene (SEPA) hvor andelen i 2011 var 0,036 prosent.[50] Ser man derimot på handel på Internett med kort utstedt i Norge, som i 2012 utgjorde 53 milliarder,[51] nærmer svindelandelen seg 0,1 prosent (1 promille).

3D Secure (Verified by Visa / MasterCard SecureCode)
3D Secure er en sikkerhetsløsning VISA og MasterCard tilbyr for å gjøre internetthandel sikrere og for å redusere kortutsteders tap ved uautorisert bruk av kort på Internett. Løsningen gir også bedre rettighet til oppgjør for brukerstedet.

To forutsetninger må være oppfylt for at 3D Secure skal komme til anvendelse:

- Utstederbank må ha implementert 3D Secure på kortet.
- Brukerstedet må ha implementert 3D Secure på brukerstedet (handelsplassen).

Dersom begge forutsetningene er til stede, avkreves brukeren ekstra autentiseringsinformasjon gjennom 3D Secure før handelen på Internett kan gjennomføres. Den ekstra autentiseringsinformasjonen kan være et fast passord, bruk av BankID, kode mottatt på SMS fra kortutsteder eller tilsvarende.

Dersom enten utstederbank eller brukerstedet ikke har 3D Secure implementert, gjennomføres handelen uten denne ekstra sikkerheten. Innløser, som inngår avtale med brukerstedet om bruk av betalingskort, kan nekte å inngå avtaler med brukersteder som ikke etablerer 3D Secure.

Det er etablert en egen modell for håndtering av tap for å motivere til etablering av løsninger med 3D Secure. Hvis ingen av partene har 3D Secure, eller begge har det, er det utstederbank som bærer tapet. Ellers er det den parten som har dårligst sikkerhet, som bærer tapet.

[50] http://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201307en.pdf?1b8fb7a7abcf9c9f5a0dd8e6eada19e2
[51] Norges Banks årsrapport om betalingssystem 2012:
http://www.norges-bank.no/pages/94894/Betalingssystem_2012_o.pdf

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

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

Kilde: Finanstilsynet

Tapene for nettbank avtok i 2013. For å få et reelt bilde av svindelnivået, rapporterte bankene, i tillegg til tap, også på to andre parametere:

- Svindeltransaksjoner som er registrert i nettbanken med et gyldig kontonummer og et beløp, men avverget før de ble gjennomført.
- Antall kunder der banken har oppdaget at kundens datamaskin er infisert med en aktiv nettbanktrojaner.

Også disse tallene indikerte vesentlig lavere angrepsintensitet i 2013 enn i 2012.

Tiltak fra bankenes side, blant annet med å advare kundene, raskt stenge ned falske websider, fange opp svar og overvåke transaksjoner, var effektive.

Tap hvor phishing inngikk som et ledd i angrepet, inngår i tapstallene både til betalingskortsvindel og nettbanksvindel. Den økte phishing-aktiviteten i 2013 resulterte altså ikke i økte tap på nettbank. En medvirkende årsak til dette kan være, som nevnt tidligere, at IT-brukere i de nordiske landene er blant de mest bevisste i verden når det gjelder datasikkerhet, og de har lavest infiseringsgrad av virus og ondsinnet programvare.

Norges Banks statistikk over nettbankbruk i 2012 viser at det ble utført ca. 430 millioner nettbankbetalinger, og i Norge var det ca. 6 092 944 etablerte nettbankavtaler.

7.5.2 Tapstall i andre europeiske land

Oversikten Fraud the Facts 2013[52] fra Financial Fraud Action (FFA) i Storbritannia viser en økning i tap på kortområdet i 2012. Tap ved betaling uten fysisk bruk av kort (card-not-present) økte med 11 prosent, og utgjorde totalt 63 prosent (tilsvarende ca. 246 millioner pund) av tapene på kortområdet. Også tap knyttet til nettbank økte i 2012, noe som kan skyldes mer avanserte former for phishing.

Storbritannia kartlegger omfanget av phishing gjennom antall identifiserte falske websider i navn av finansforetak. Det er ingen direkte knytning mellom phishing og tapstall, men bak de falske websidene gjemmer det seg tap både knyttet til card-not-present og nettbank.

Fraud the Facts' figur 8 viser en voldsom økning over antall infiserte websider fram til november hvor det er en dramatisk nedgang (se pilen). Nedgangen skyldtes at den spesielle politimyndigheten for

[52] http://www.financialfraudaction.org.uk/downloads.asp?genre=consumer

elektronisk kriminalitet i Storbritannia, Police Central eCrime Unit (PceU), avslørte en liga av profesjonelle svindlere og fikk stoppet botnettet denne ligaen administrerte.

Figur 8: Phishing-angrep mot engelske banker

Number of phishing websites targeted against UK banks and building societies by month 2005-2012

	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec	TOTAL
2012	18,252	6,629	14,362	20,669	24,578	26,818	39,767	41,734	27,869	30,036	3,523	2,404	**256,641**
2011	5,803	5,757	6,828	5,698	6,216	6,896	7,402	8,062	23,083	9,397	15,395	10,749	**111,286**
2010	2,654	3,135	4,810	4,335	5,406	5,277	5,873	5,861	5,689	6,977	4,552	7,304	**61,873**
2009	4,206	5,161	5,004	3,422	3,917	4,335	4,415	4,845	3,900	4,903	4,191	5,864	**51,161**
2008	3,144	3,243	3,848	3,719	3,091	3,637	3,584	3,716	4,121	4,536	3,896	3,456	**43,991**
2007	1,290	974	1,130	1,188	1,274	1,368	3,066	3,268	2,597	3,170	3,277	3,195	**25,797**
2006	606	669	1,074	947	919	872	970	1,484	1,513	1,596	1,993	1,513	**14,156**
2005	18	29	27	54	72	122	153	160	190	267	255	353	**1,700**

Kilde: Financial Fraud Action UK

Tapstall fra Belgia publisert på Febelfin[53] viser at tap på nettbank økte med over 50 prosent fra 2012 til 2013.

Tapstall publisert av den nederlandske bankforeningen[54] viser derimot synkende tapstall. Her tilsvarte tapene i andre halvdel av 2013 bare en tredjedel av tapene første halvdel av 2012.

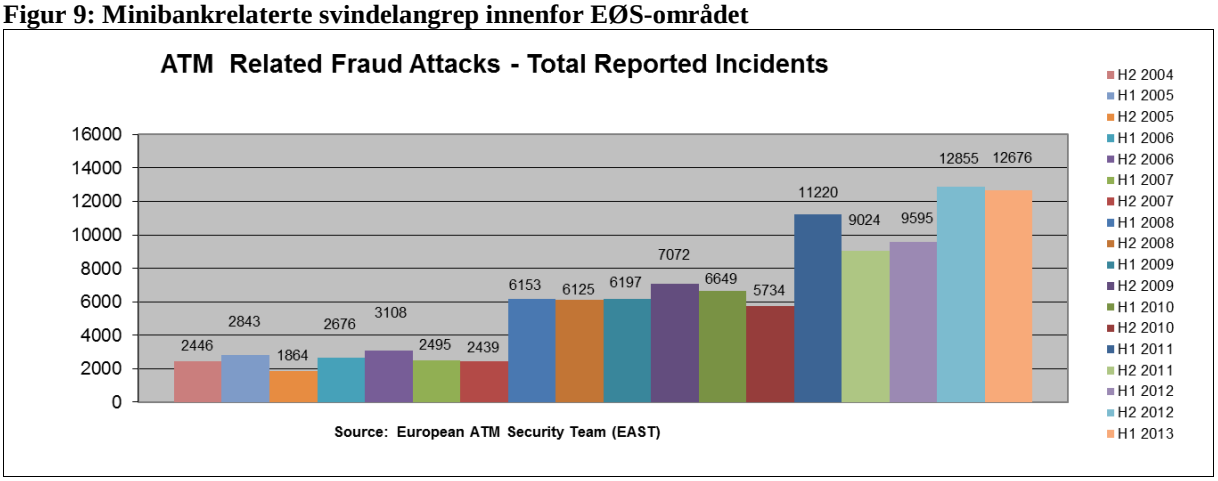
7.5.3 Svindelangrep og tap på minibanker (ATM) i EØS-området

EAST[55] utarbeider halvårlige rapporter som viser minibankrelaterte angrep og tap innenfor EØS-området.

Totalt sett har det de siste årene, bortsett fra i 2010, vært en økning i svindelangrep mot minibanker innenfor EØS-området, se figur 9. Tapene har imidlertid ligget på samme nivå de siste tre årene. Nær alle tap er knyttet til skimming. Fortsatt bruk av magnetstripe på betalingskort i en del land gjør at kortene er utsatt for skimming-angrep. Norske kort som er skimmet, blir nesten utelukkende misbrukt i utlandet.

[53] http://www.febelfin.be/nl/aantal-gevallen-van-phishingfraude-neemt-toe-1
[54] http://www.nvb.nl/thema-s/veiligheid-fraude/166/fraude.html
[55] Kilde er EASTs (European ATM Security Team) halvårlige European ATM Crime Report.

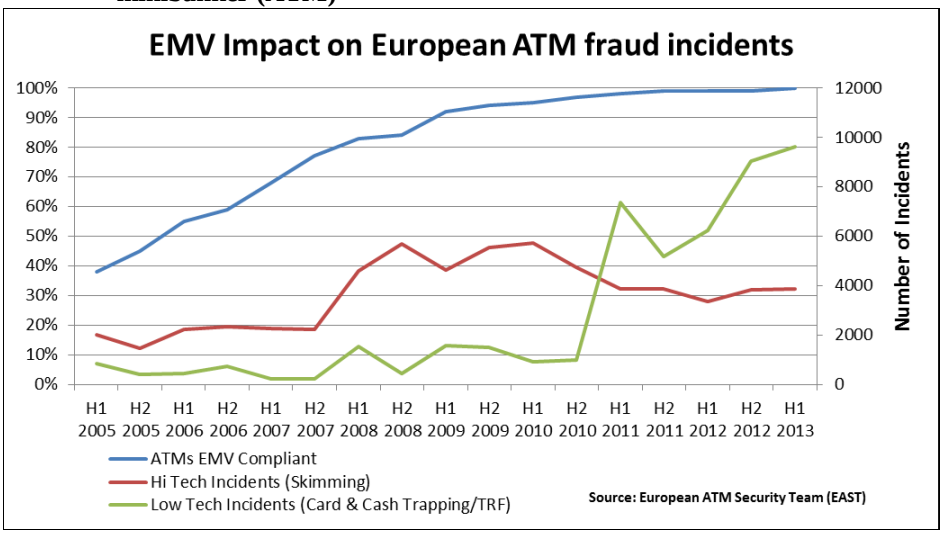
Figur 9: Minibankrelaterte svindelangrep innenfor EØS-området



Kilde: EAST

Som figuren nedenfor viser, har det fra 2011 skjedd et markant skifte fra såkalte "Hi Tech"-angrep (skimming) til "Low Tech"-angrep (kort og kontant fangst/transaksjonsreversering) uten tilsvarende vridning i tap, siden ca. 97,5 prosent av alle tap er knyttet til skimming.

Figur 10: Hvordan gjennomføring av EMV-standarden har påvirket svindelangrep mot minibanker (ATM)



Kilde: EAST

Antall fysiske angrep mot minibanker innenfor EØS-området har ligget på omtrent samme nivå, om lag 2000 per år de siste fem årene. RAM-angrep og innbrudd i minibanker utgjør hovedparten. Tapene viser imidlertid en nedadgående trend. Denne typen angrep er sjelden å se i Norge.

7.6 Nettvett, mobilvett og kortvett

Når stadig mer av bankens betalingsformidling og øvrige virksomhet skjer digitalt og elektronisk, er det viktig at finansforetakene har relevant og oppdatert "vett"-informasjon for sin tjenesteyting lett synlig og tilgjengelig for både kort, nettbank og mobil. Informasjonen bør være dekkende både for private kunder og bedrifter, og ha lenke til supplerende nettsider på en enkel måte. Finanstilsynet har observert at enkelte foretak har gjennomført sikkerhetsrelaterte kampanjer.

Det finnes mye informasjon på en rekke nettsteder om nettvett, dvs. råd om hvordan man bør opptre på Internett. Tilsvarende finnes det også veiledninger om bruk av betalingskort og mobil. Mange av nettstedene har særlig vekt på personvern og generelt nettvett. Nettvett.no,[56] som Post- og teletilsynet er ansvarlig for, gir også råd om nettbank, netthandel og mobil.

Finanstilsynet har sett på en rekke foretaks informasjon om nettvett, mobilvett og kortvett. Det finnes mye informasjon på foretakenes nettsider, men graden av dekning, samlet informasjon og synlighet varierer. Omtaler av kortvett, nettvett og mobilvett finnes ofte på ulike nettsider hos det enkelte foretak. Å samle denne informasjonen gjør det lettere tilgjengelig for forbrukerne. Ofte er det også forskjellige nettsider for person og bedrift. Mange har også nyttige lenker til gode nettvettsider, som nettvett.no og norsis.no,[57] som igjen har lenker til andre sider, som f.eks. nettsidene til Forbrukerrådet[58] og Forbrukerombudet.[59]

Det er viktig at foretakene gir god informasjon og råd om varsomhet knyttet til sikkerhet i forbindelse med bruk av elektroniske banktjenester. Det vil kunne være krevende å etablere uttømmende informasjonssider og holde disse oppdatert, men samtidig vil de være et viktig supplement som del av tjenesteytingen.

7.7 Regelverksutvikling i EU

Forslag til nytt betalingstjenestedirektiv (PSD2)

Det er behov for å endre det eksisterende rammeverket i betalingsformidlingen. Bakgrunnen er at regulatoriske justeringer, avklaringer og innarbeiding av teknologisk og markedsmessig utvikling skal gi bedre samsvar mellom nasjonale regelverk. Forslaget skal også fremme økt samhandling og fjerne konkurransebegrensende og -vridende regelverk. Forslaget vil kunne innebære endringer i finansavtaleloven og finansieringsvirksomhetsloven, forskrift om betalingsforetak og IKT-forskriften og i finansnæringens bransjebestemte regelverk innenfor bl.a. betalingsformidling ("Blåboka").

[56] http://www.nettvett.no/
[57] https://norsis.no/
[58] http://www.forbrukerradet.no/
[59] http://www.forbrukerombudet.no/

Forslag til nytt betalingstjenestedirektiv innebærer blant annet

- at tredjeparts betalingstjenestetilbydere (TPP), som ikke holder betalers eller betalingsmottakers midler, blir regulert for å ivareta krav til sikkerhet, databeskyttelse og ansvar. TPP-er må bli registrert og overvåket som betalingsinstitusjon for å få lov til og tilby betalingstjenester. Det betyr at de vil bli underlagt de samme rettighetene og pliktene, og særskilte krav til sikkerhet som andre betalingstjenestetilbydere. Direktivet gir klare retningslinjer for tilgang til kontoinformasjon, krav til autentisering og korrigering av transaksjoner og ansvar for uautoriserte transaksjoner.
- at det også skal gjelde for grensekryssende transaksjoner, der den ene delen av transaksjonsgjennomføringen utføres innenfor EØS, og i visse sammenhenger også for alle valutaer
- en harmonisering av reglene for kunders objektive erstatningsansvar ved uautoriserte transaksjoner til 50 euro, hvis kunden ikke har overholdt sine sikkerhetsforpliktelser
- ingen begrensninger i ansvar ved grov uaktsomhet. Betaler kan innen åtte uker ubetinget kreve tilbakeføring av direkte debiterte beløp, forutsatt at varen ikke har blitt konsumert.
- oppdatert regelverk om hvilke betalingsrettede aktiviteter som kan unntas direktivet
- strømlinjeforming og harmonisering av krav til sikringstiltak av verdier som holdes i betalingsformidlingen
- utvidelse av regimet for begrensede tillatelser til å drive betalingstjenester, ved å redusere terskelen for slike tillatelser
- krav til betalingstjenestetilbyderes styring, kontroll og rapportering av risiko og varsling om og rapportering av hendelser

Forslaget til direktiv inneholder også endringer som innebærer at den europeiske banktilsynsmyndigheten (EBA) på flere områder forutsettes å bidra ved

- å sørge for et konsistent og enhetlig tilsyn
- å gi retningslinjer og utkast til regulatoriske og tekniske standarder på ulike områder, som f.eks. å sikre etablering av tilstrekkelige krav til sikkerhet eller klargjøre reglene om "passporting" for betalingstjenesteleverandører som opererer i flere medlemsstater. Passporting tillater at et foretak med lisens i et EØS-land fritt kan etablere seg med filialer og agenter i andre land, med mindre vertslandet har vesentlige innsigelser og at disse vil stå under tilsyn av tilsynsmyndighet i hjemlandet.
- å etablere et europeisk tilgangspunkt for informasjon om registrerte betalingsforetak for å sørge for økt åpenhet og innsyn

Forslag til regulering av formidlingsgebyrer for kortbaserte betalingstjenester
Som en del av arbeidet med nytt betalingstjenestedirektiv er det i en separat forordning foreslått regulering av formidlingsgebyrer for kortbetalinger (MIF-reguleringen).

Forslaget skisserer kortbruken i et regulert og i et ikke-regulert område. Det regulerte området omfatter

forbrukeres bruk av betalingskort i betalingsterminaler, betaling på Internett og mobilbetalinger, men det gjelder kun transaksjoner innenfor den såkalte 4-partsmodellen, samt "lisensierte" 3-partsmodeller. Det uregulerte området består av alle betalingskorttransaksjoner og kortbaserte betalingstransaksjoner som faller utenfor det regulerte området. Dette inkluderer såkalte kommersielle kort, kort utstedt av tredjeparts ordninger og uttak i automater.

Videre deles regulering inn i to hoveddeler: regler om formidlingsgebyrer og tilleggsgebyrer og regler for god forretningsskikk. Det regulerte området omfattes av hele reguleringen, og det ikke-regulerte området omfattes bare av regler for god forretningsskikk.

Forslag til regler om formidlingsgebyrer innebærer et tak på gebyrene knyttet til debet- og kredittkort på henholdsvis 0,2 prosent og 0,3 prosent. Det foreslås en totrinns gjennomføring der grensekryssende betalinger skal omfattes kort tid etter at lovverket er besluttet, mens alle nasjonale forbrukerkortbetalinger først blir omfattet etter to år. I tillegg foreslås det forbud mot tilleggsgebyrer.

Regler for god forretningsskikk omhandler

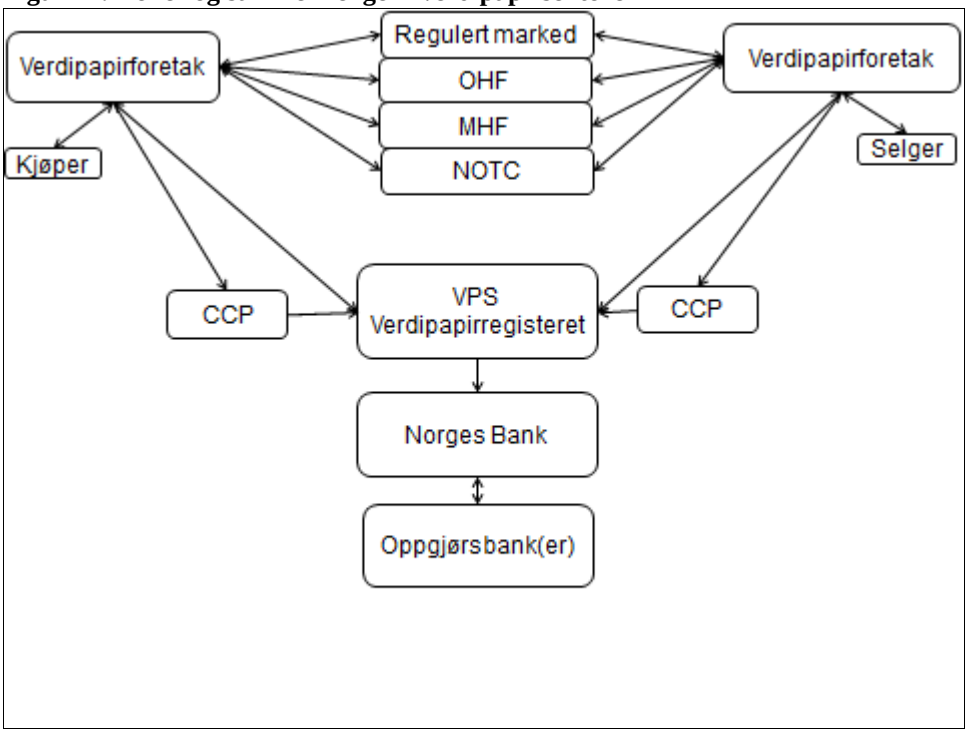
- retten til å utstede og innløse kort for hele EØS-området
- at "payments schemes" (kortordning) skal separeres fra behandlingen av kortbetalingene
- begrensninger på "Honour All Cards Rule", som innebærer at "like" typer kort må behandles likt
- utsteders rett til co-branding og brukers rett til å velge betalingsmåte, noe som bl.a. vil berøre co-branding av norske kort (BankAxept og Visa). Dagens prioriteringsregel vil da ikke lenger være lovlig.
- at utstederbanker skal tilby og gebyrlegge betalingsmottakere individuelt for de forskjellige kortmerkene og betalingskort
- betalingstjenesteleverandørers informasjonsplikt overfor betalingsmottaker for enhver gjennomført betalingstransaksjon
- forbud mot regler som hindrer forhandlere i å opplyse forbruker om faktiske kostnader ved den kortbaserte betalingstjenesten og regulering av forhandlers rett til å styre forbruker mot bruk av dennes foretrukne betalingsinstrument

8 Verdipapirområdet

På verdipapirområdet skjer det omfattende endringer som samlet kan representere en risiko knyttet til omfanget på endringene og kvalitetssikring av disse. Også her kan gamle legacy-systemer representere en utfordring, og en fornyelse vil innebære risiko under gjennomføringen. I denne sektoren er det flere regelverksendringer 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.

Nedenfor er det gitt et oversiktsbilde av viktige roller og sammenhenger som inngår i verdipapirsektoren. Fortsatt er helhetsbildet at det er både høy stabilitet og god kvalitet innenfor denne sektoren i Norge, men det har skjedd hendelser, og det kan være en utfordring å sikre akseptabel risiko med de endringene som antas å komme i denne sektoren framover.

Figur 11: Roller og sammenhenger i verdipapirsektoren



Kilde: Finanstilsynet

8.1 Risiko for underinvestering ved redusert inntjening

Den norske infrastrukturen for omsetning av verdipapirer har vært utsatt for store endringer i rammebetingelsene. Endringene i verdipapirhandelloven med bakgrunn i et ønske om økt konkurranseutsetting av verdipapirtjenester og lavere kostnader for investorer, har medført at Oslo Børs i dag står for mindre enn 50 prosent av omsetningen av aksjer som er primærnotert på Oslo Børs. Likviditeten i norske noterte aksjer er nå spredt på flere ulike handelsplasser som Chi-X, BATS og Nasdaq OMX.

For å kunne tilby en samlet likviditet fra disse handelsplassene har verdipapirforetakene satt opp IT-løsninger som kan handle simultant over flere handelsplasser. Resultatet av denne automatiseringen av handel er blant annet at markedsskjevheter og forsinkelser som tradere med investeringshorisont på mindre enn én dag tidligere utnyttet, er betydelig redusert. Dette innebærer at størstedelen av omsetningen som denne typen kunder representerte for verdiforetak, er falt bort. Kurtasjeinntektene for meglerhus som ikke er bank, sank fra 2,4 milliarder kroner i 2007 til 0,5 milliarder kroner i 2012. For mindre verdipapirforetak har konsekvensen av økte kostnader til infrastruktur og handelssystemer oversteget reduksjonen i transaksjonskostnadene. Når omsetningsvolumet i andrehåndsmarkedet samtidig er redusert, har også lønnsomheten for verdipapirforetak som har hatt dette som en vesentlig inntektskilde blitt borte.

Reduserte inntekter og økte kostnader kan medføre et press på IT-området for å redusere kostnadene, og dette kan ha negative konsekvenser for kvalitet og sikkerhet i forvaltningen av IT-løsningene.

8.2 Risikoer i forbindelse med algoritmehandel

De siste par årene har det vært tilfeller der algoritmer som benyttes til høyhastighetshandel i det norske aksjemarkedet som følge av programmeringsfeil har hatt et utilsiktet handelsmønster. Dette har ført til tap for verdipapirforetaket. Årsaken til feilene har vært svikt i, eller mangler ved selskapets endringsprosedyrer.

Konsekvensen ved slike feil i algoritmehandel kan være betydelige tap for selskapet som forestår handelen, og i tillegg kan markedspriser bli påvirket.

8.3 Back office-systemer i verdipapirmarkedet

Flesteparten av norske verdipapirforetak benytter i dag i stor grad samme back office-system. Dette har gjort det mulig for leverandøren å fordele de store kostnadene for utvikling av slike systemer på alle aktørene, og dermed oppnå en grad av stordriftsfordel. Risikoene er på den andre siden at kompetansen på dette området også blir konsentrert og man går glipp av fordeler som et marked med flere tilbydere gir.

8.4 Utkontraktering av kjernesystemer

Verdipapirforetakene har også økt sin grad av utkontraktering av systemer for front- og back-office-løsninger til systemleverandører. Dette senker på kort sikt totalkostnadene og vil trolig også redusere antall feilsituasjoner som skyldes driftsoperasjon lokalt hos hvert enkelt foretak. Konsentrasjonsrisikoen vil på den andre siden øke, og eventuelle feilsituasjoner vil få større konsekvenser for hele markedet. En av utfordringene med utkontraktering av kjernesystemer for verdipapirforetakene er å beholde tilstrekkelig kompetanse på systemområdet internt i foretakene slik at man kan gjennomføre styring og kontroll med leverandørene.

8.5 Konsentrasjonsrisiko på nettverksinfrastrukturen

Aktørene i verdipapirmarkedet benytter i stor grad samme nettverksinfrastruktur mot handelsplasser og oppgjørssentraler. Denne infrastrukturen har hittil vist seg å være både robust og kostnadseffektiv. Finanstilsynet er spesielt opptatt av at dette representerer en konsentrasjonsrisiko der konsekvensen ved en feilsituasjon er stor.

8.6 Regelverksutvikling

Ny regulering for virksomheten 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, ofte med kort implementeringstid. Dette vil igjen normalt kreve betydelig ressursbruk i verdipapirforetakene for testing og implementering. Korte tidsfrister vil i tillegg kunne sette betydelig press på utvikling av løsningsspesifikasjonene og tilhørende løsninger. Forsinkelser kan derfor lett oppstå, og resultatet kan bli en tidspresset utvikling slik at løsningene får feil og mangler, noe som kan medføre uheldige konsekvenser for produksjon og stabilitet i verdipapirmarkedet.

Som særlige eksempler på forestående reguleringsendringer i EU kan nevnes CRD IV (Capital Requirements Directive – nytt kapitaldekningsregelverk), EMIR (European Market Infrastructure Regulation) og MiFID II (Market in Financial Instruments Directive – nytt investeringstjenestedirektiv). Disse endringene vil medføre nye rapporteringskrav for foretakene med utfordringer knyttet til felleseuropeisk løsningsvalg og trolig betydelig arbeid med tilhørende lokale tilpasninger. Videre er nye rapporteringskrav ved shortsalg også på trappene.

I tillegg vil FATCA (Foreign Account Tax Compliance Act) 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.

8.7 Verdipapirforetakenes håndtering av sensitive selskapsdata på IT-systemer

En kjent risikofaktor er informasjon på avveie. Sensitiv selskapsinformasjon i verdipapirforetakene og informasjon som omhandler selskapshendelser kan gi betydelig skade. 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. Foretakene må også sørge for tilstrekkelig kontroll ved bruk av skybaserte filutvekslingsløsninger som Dropbox ved distribusjon av sensitiv informasjon.

Finanstilsynet vil framover vektlegge tilsyn med prosessene for tilgangshåndtering av slike dataområder, samt bruken av logger for å avdekke lekkasjer av kurssensitiv informasjon.

8.8 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 derfor vil innebære risiko. Finanstilsynet forventer at prosjektet gjennomfører kvalitetsmessig gode risikovurderinger, samt følger opp disse gjennom prosjektet.

9 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	Hvitvasking (Anti Money Laundering)
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 informerte og raske beslutninger i vanskelige saker.
Botnett	Konstruert ord fra robot og nettverk. 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 ofte via Internett.
Computer Emergency Response Team	Se CERT.
DDoS-angrep	Et internettangrep som overbelaster en server ved at stor trafikk rettes mot serveren, gjerne ved bruk at et botnett. Hensikten er å hindre normal tilgang fra ordinære brukere.
EBA	Den europeiske banktilsynsmyndigheten – European Banking Authority
EIOPA	Den europeiske tilsynsmyndigheten for forsikrings- og tjenestepensjon – European Insurance and Occupational Pensions Authority
ESMA	Den europeiske verdipapir- og markedstilsynsmyndigheten – European Securities and Markets Authority
FATCA	Foreign Account Tax Compliance Act
FI-ISAC	Financial Institutes – Information Sharing and Analysis Centre er et europeisk tiltak primært med deltakere fra CERT-er, bankorganisasjoner og politimyndighet. I Norge samarbeid mellom NSM, BSK og Finanstilsynet. Foreløpig et uformelt samarbeid mellom enkeltland og definerte myndigheter, bl.a. 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 inndras av automaten. Når kunden har gått, hentes pengene ut av svindler.
Internet of Things (IoT)	Foreløpig et noe udefinert begrep. Går på at ting kan knyttes til Internett på mange ulike måter. Som "tags" for å avlese identitet, eller mer avansert via f.eks. WiFi-nett. Mange enheter har innebygde datamaskiner og kan kommunisere med andre enheter og servicesentre. Også utplassering av sensorer for innhenting 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, nonprofit-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: endre telefonens sikkerhetsopplegg, f.eks. for å tillate at en benytter en annen operatør enn den telefonene er låst til (hvis den er låst til operatør). Leverandør vedlikeholder ikke slike endringer, og sikkerhetshull kan oppstå.
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
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	Tredjeparts tjenester i grensesnittet kunde – bank
Phishing	Det å gi seg ut for å være en annen og i dennes 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).
RAM-angrep	Ondsinnet kode som leser maskinvarens minne, og hvor informasjonen ikke er kryptert
Rooting	For Android: Som "jailbreaking" hos Apple/iPhone – se dette.
Sandbox	"Sandkasse". En virtuell beholder (beskyttet område) hvor en kan kjøre et program uten at det påvirker andre programmer.
Skytjenester	Norsk for engelsk "cloud computing" – se dette.
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

Foto omslag: Jetta Productions/Getty Images
Design omslag: Miksmaster Creative
04.2014

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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