FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

RAPPORT

RISIKO- OG SÅRBARHETSANALYSE (ROS)

2010

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Risiko- og sårbarhetsanalyse (ROS) 2010

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Finanstilsynet, 21. mars 2011

Innhold

1 Innledning

Finanstilsynet foretar årlig en risiko- og sårbarhetsanalyse (ROS-analyse) av finanssektorens bruk av informasjons- og kommunikasjonsteknologi (IKT).

Et viktig utgangspunkt for arbeidet med ROS-analysen er å sikre at Finanstilsynet har tilstrekkelig informasjon om risiko knyttet til finanssektorens bruk av IKT og systemer for betalingstjenester.

Det har vært viktig å identifisere muligheter for å sikre mer informasjon om kvantitative data som sammen med kvalitative data gir grunnlag for risikovurderinger. Et viktig element i dette arbeidet har vært å etablere pliktig rapportering av IKT-hendelser til Finanstilsynet.

I samarbeid med fellesorganer i finanssektoren, har Finanstilsynet i 2010 arbeidet med å skaffe til veie korrekt informasjon om tap knyttet til utvalgte betalingstjenesteområder, noe som bidrar til å forstå risikonivået og behov for tiltak.

Samtidig som ROS-analysen er et viktig virkemiddel for Finanstilsynet, kan den også benyttes som informasjonskilde i arbeidet med risiko hos det enkelte finansforetak og av bransjeorganisasjoner. I tillegg representerer ROS-analysen et nyttig bidrag til internasjonalt samarbeid på IKT-området.

2 Utviklingstrekk

2.1 IT Governance

Foretaksledelsens styring og kontroll med IKT er vesentlig når det gjelder finansforetak fordi IKT utgjør viktige forutsetninger for hele virksomheten. Styring og kontroll med IKT har internasjonalt blitt synonymt med begrepet IT Governance. Dette omfatter også forankring i forretningsledelsens virksomhetsstyring. Erfaring hittil viser at det fortsatt er utfordringer knyttet til å sikre relevant involvering fra forretningsledelsen og til synliggjøring av koblingen mellom IKT-virksomheten og den totale forretningsvirksomheten.

Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT-forskriften) definerer forhold og krav som må ivaretas for å sikre hensiktsmessig styring og kontroll med IKT-virksomheten.

Tilstrekkelig styring og kontroll er viktig ut fra forretningsmessige krav, for håndtering av risiko og for å etterleve reguleringsmessige krav. Det finnes god faglig veiledning og gode metoder på dette området. Det er derfor bekymringsfullt at det fortsatt oppstår problemer som skyldes mangel på helhetlig styring og kontroll av IKT-virksomheten.

2.2 Mangelfull ledelse i store prosjekter

Vi ser fortsatt at store prosjekter i finanssektoren feiler, og at ledelsens mangel på kunnskap om styring og kontroll av IKT-prosjekter får konsekvenser for fremdrift, kostnadskontroll, kvalitet og realisering av forutsatte gevinster. Dette kan gi svært alvorlige konsekvenser som ikke alltid blir rapportert og fulgt opp på en hensiktsmessig måte.

God styring krever at ledelsen er involvert og stiller krav til rapportering om fremdrift og avvik. Under estimerings- og budsjetteringsprosessen kan virksomheten støtte seg på erfaringer fra lignende prosjekter. Men dette er kun mulig hvis foretaket har et kvalitetssystem som kan samle opp disse

erfaringene. En såkalt WBS[1] fra et lignende prosjekt kan sikre oversikt over alle nødvendige aktiviteter. Mangel på oversikt kan føre til at aktiviteter utelates og at både kostnader og ressursbehov underestimeres.

Oppfølgingsprosessen er essensiell i alle prosjekter. Det er vesentlig å benytte målepunkter som er godt definert i forhold til alle leveranser som skal komme ut fra aktiviteten. Manglende definisjon kan lede til en situasjon hvor aktiviteten meldes som 90 prosent ferdig, men hvor de siste 10 prosentene i praksis viser seg å være langt mer omfattende. Uten nøyaktige framdriftsmål og tilstrekkelig detaljering av oppgaver i omfang og tid, kan både kalendertid og budsjetter være brukt opp før avvik blir oppdaget.

Framdrift, forutsetninger, risiko og avhengigheter må følges tett gjennom prosjektperioden. Hvis dette blir oversett, ender det ofte med akutte situasjoner hvor tiltak ikke er klargjort. Det krever innsats av ressurser som det kan ta tid å skaffe, og det kan hindre oppstart av andre aktiviteter.
Prosjektledelse har utviklet seg mye de siste tiårene. Det finnes flere lett tilgjengelige prosjektmetoder som er lagt opp i henhold til anerkjente standarder, for eksempel IPMA (International Project Management Association) eller PMI (Project Management Institute).
God prosjektledelse sikres ved å benytte anerkjent prosjektmetodikk som blir fulgt av kvalifiserte prosjektledere.

2.3 Endringer fører ofte til feil

Krav til store kostnadsbesparelser fører ofte til behov for å endre systemporteføljen og resulterer dermed i endringstiltak. Manglende styring og kontroll i gjennomføring av slike tiltak kan medføre redusert kvalitet og økt operasjonell risiko.

Samtidig med krav til kostnadsreduksjon og økt inntjening, er deler av næringen underlagt betydelige regelverksendringer både gjennom internasjonale anbefalinger, EU-direktiver og nasjonale reguleringer. Summen av dette kan stille krav til store endringer av IKT-løsninger i samme tidsperiode og kan representere en risiko. Eksempler på slike regelverksendringer er Pensjonsreformen, Basel III-regelverket og Solvens II for forsikringsområdet.

Det er vesentlig at risikovurderinger og styring av operasjonell risiko blir en integrert del av foretakenes arbeid med tilpasning til nye regler, kostnadsreduksjoner og effektivisering.

[1] Work Breakdown Structure: En trestruktur som viser en inndeling av arbeidet som må gjøres for å nå et mål.

2.4 Leverandørutviklingen på IKT-området

På leverandørsiden pågår en ytterligere konsolidering ved at allerede store aktører har slått seg sammen. I Norge gjelder dette EDB Business Partner ASA og ErgoGroup AS som har dannet selskapet EDB ErgoGroup ASA (EDB). Det norske selskapet BBS og danske PBS har etablert et felles selskap med hovedkontor i Danmark, NETS, og et norsk datterselskap som heter NETS Norge AS. SDC (Skandinavisk Data Center), som er driftsleverandør til Terrabankene, har iverksatt prosesser med BEC (Bankernes EDB Central) for å etablere selskapet Nordisk Finans IT, som vil samle driften hos JB/NK-data (Jyske Bank og Nykredit). SDCs IT-drift flyttes da fra IBM til JN-Data gjennom et strategisk samarbeid.

Viktige grunner for fusjonene er ønsket om å oppnå stordriftsfordeler og andre synergier. Likeledes kan applikasjonsporteføljen samordnes og rasjonaliseres. Størrelse er også viktig ved nyutvikling/kjøp av løsninger.

Det er også en klar tendens at IT-leverandører utnytter mulighetene for kostnadsreduksjoner og større tilgang på ressurser ved å flytte viktige deler av virksomheten til lavkostland. Samlet sett kan disse endringene over tid medføre risiko gjennom redusert evne til egen styring og kontroll og gjennom økt konsentrasjonsrisiko. Det blir derfor viktig å overvåke utviklingen på leverandørsiden.

2.5 Utkontraktering og offshoring

2.5.1 Utvikling og risikoforhold

Både innenfor finanssektoren generelt og banksektoren spesielt er det lang tradisjon i Norge for utstrakt bruk av utkontraktering av IKT. For bankene ble dette tidligere i stor grad vurdert som en del av egen virksomhet mht. risikovurderinger siden bankene var både eiere og brukere av de aktuelle leverandørene. Senere har dette endret seg til at de fleste IKT-leverandører i dag er frittstående virksomheter, ofte børsnoterte og med eiere utenfor Norge.

Leverandørene er utsatt for krav til kostnadseffektivitet fra både eiere og kunder. For å møte disse kravene, benytter leverandørene i økende grad offshoring. Dette skjer både gjennom oppkjøp av selskaper i lavkostland og ulike andre samarbeidsopplegg. Hensikten er å få tilgang til mer ressurser, både kompetanse- og kapasitetsmessig, til en lavere kostnad.

Denne utviklingen medfører en kompleks og krevende situasjon både for kundene og leverandørene når det gjelder styring og kontroll, håndtering av risiko og etterlevelse av regelverk. Dersom denne typen utkontraktering, med utstrakt bruk av offshoring, får et stort omfang i finanssektoren, kan dette bety et økt risikonivå. Dette gjelder både for det enkelte foretak og finanssektoren samlet. Krav til risikohåndtering må vurderes ut fra dette helhetsbildet.

Med visse unntak er det ikke regler som direkte begrenser mulighetene til utkontraktering annet enn nærmere definerte krav som skal være oppfylt. Et eksempel er at det skal utføres en risikovurdering. Det enkelte finansforetak må sikre etterlevelse av lover, forskrifter, annet aktuelt regelverk (f.eks. egenregulering som benyttes mellom bankene) og egne retningslinjer. Det blir derfor viktig at foretaket som skal utkontraktere sikrer at alle nødvendige vurderinger blir gjennomført, dokumentert og legges til grunn for en eventuell beslutning. Om foretaket vil gjennomføre en utkontraktering, vil det være bestemmelser i avtalen mellom kunden og leverandøren som skal sikre forsvarlig kontroll med de utkontrakterte aktivitetene.

I Rundskriv 14/2010 om "Utflytting av bankenes IKT-oppgaver", legger Finanstilsynet til grunn klare begrensninger i utkontraktering til områder som betegnes som høyrisikoområder. Begrensningene er knyttet til nærmere bestemte funksjoner/områder av bankenes virksomhet. Finanstilsynets klare inntrykk er at bankene har innrettet seg etter disse vurderingene.

2.5.2 Kontroll ved utkontraktering av IKT-tjenester

For å ivareta leveransen og etterleve lovpålagte oppgaver, er det nødvendig for tjenestekjøper å ha egen kompetanse på det området som utkontrakteres (IKT-forskriften § 12). Slik egenkompetanse kan ivaretas i egen organisasjon eller den kan kjøpes inn fra for eksempel et konsulentselskap. Det er også vanlig at institusjonene samarbeider med hverandre, enten bilateralt eller gjennom for eksempel bransjeorganisasjoner, for å ivareta denne kompetansen.

For å kunne kontrollere en omfattende leveranse, er det nødvendig å dele den opp i hensiktsmessige enheter og foreta en detaljering som kan sikre mulighetene til kontroll. Dette må omfatte både kvantitet, kvalitet og sikkerhet. For best å kunne opprettholde fokus på kvalitet, bør man tydeliggjøre overfor leverandøren at dette blir fulgt med på og at det er viktig for kjøper.

Avtalene mellom kunde og leverandør er etterhvert blitt gode og spesifikke med krav til kvalitet og prising på detaljert nivå. Men det finnes fortsatt eksempler hvor kvaliteten ikke er god nok. Måling av ytelse innenfor sikkerhet er foreløpig et umodent område, men det finnes en del spesifikke krav. ISO 27002 gir oversikt over sikkerhetsområdet, og ISO 27004 angir en standard for måling innenfor dette området.

Erfaring viser at slike målinger må legges opp slik at de ikke koster for mye. Da vil de ikke bli utført. Det er ønskelig med automatiserte målinger slik at systemene selv rapporterer. Målinger skal være tallfesting av forhold, tellinger, prosent av, eller henvisning til en på forhånd fastsatt skala. Subjektive

vurderinger som for eksempel "høy", "middels" eller "lav" er ikke reproduserbare og gir lite mening annet enn ved eventuell rapportering til neste nivå internt i organisasjonen.

Avtalene må revideres med jevne mellomrom for å tilpasses nye krav og nye systemer. Videre vil det trolig være ønskelig med nye former for rapportering og målinger det pr. i dag ikke finnes noen standard eller noe etablert rammeverk for. Avtalen bør inneholde klausuler om at dette området skal videreutvikles i avtaleperioden.

Ytelser ved oppsigelse må reguleres spesielt. Tjenesteyter må ha plikt til å stille opp med kompetent personell for overlevering/konvertering til annen leverandør. Ved overgang til andre systemer, må man stille krav om nødvendig faglig assistanse for utlisting eller konvertering av registre.

2.6 IKT-infrastruktur

Den lange tradisjonen for at manuell behandling erstattes av programmessig behandling fortsetter med uforminsket kraft. I 2010 fikk vi en utvikling der IKT-tjenester ble knyttet tettere sammen i realtid. Elektronisk lånesøknad på nettet og etterfølgende maskinell behandling er et eksempel på dette. Algoritmehandel for handel i verdipapirer, valuta m.m. er et annet eksempel. IKT-virksomheten blir mer omfattende.

Finanstilsynet erfarer at foretakene ikke alltid har dokumentert oversikt over sammenhengen i IKT-systemene. En del hendelser som rammer foretakene og som rapporteres til Finanstilsynet viser hvordan IKT-systemene henger sammen og i hvilke situasjoner systemene kan påvirke hverandre negativt – enten ved at de "smitter hverandre" eller at én skade rammer flere systemer. Det virker som disse sammenhengene ikke alltid har tilstrekkelig oppmerksomhet i foretakene. Manglende oversikt kan føre til at feil får større konsekvenser enn forutsatt og at arbeid med å redusere sårbarheten ikke får høy nok prioritet.

Med omfattende IKT-virksomhet oppstår behov for god kontroll med den daglige driften. Gode rutiner når det gjelder overvåking og varsling er påkrevet. Tidligere var det vanlig å benytte måleverktøy som målte egenskaper ved én ressurs, eksempelvis fyllingsgraden til et datasett, utnyttelse av en kanal osv. Transaksjonskjedene er blitt lengre, og utfordringer som f.eks. kapasitetsproblemer ett sted i kjeden kan forplante seg og få store konsekvenser for tjenester andre steder i kjeden. Oftest er det også slik at flere tjenester deler de samme ressursene. Dette betyr at problemer i én tjeneste, for eksempel en uønsket loop eller heng-situasjon, kan ha negative følger for andre tjenester. Foretakene er, av økonomiske grunner, ikke i en situasjon der de på alle områder har tilstrekkelige IKT-ressurser til å dekke ethvert tenkelig behov som måtte oppstå. Det er derfor bruk for verktøy som optimaliserer utnyttelsen av ressursene. Såkalte intelligente programvareagenter benyttes mer og mer. Disse tar "temperaturen" en rekke steder i transaksjonskjeden under ulike forhold med hensyn til trafikkmengde, type transaksjoner som dominerer på de forskjellige tider av døgnet osv., og analyserer seg frem til

mulige aktuelle eller fremtidige ressursproblemer eller andre problemer. Det finnes eksempler på slike agenter som går enda lengre ved at de omallokerer IKT-ressurser "i fart".

Finanstilsynet observerte flere hendelser i 2010 som tyder på at rutiner for overvåking og varsling kan bli bedre. De fleste foretak har tilfredsstillende overvåking og varsling i de senere fasene av en hendelse under utvikling. Men tilsynet har registrert flere hendelser som indikerer fundamentale svakheter når det gjelder overvåking også i disse sene fasene.

Fremdeles er det slik at foretak oppdager mange av hendelsene først når tjenesten er utilgjengelig. Etter dette tidspunktet skal de analysere seg frem til feilårsak, kontakte leverandør, innhente programvareutbedringer (fixer/patcher), installere disse og teste. Til slutt må rettelsen settes i produksjon. Sein varsling gjør at verdifull tid går tapt. Preventiv overvåking av den art som beskrives ovenfor, jf. eksempelet med intelligente programvareagenter, kunne i større grad vært benyttet i foretakene.

Finansforetakene har i 2010 fortsatt trenden med å ta i bruk tilgjengelige kommunikasjonsmuligheter for å kunne tilby tjenester. Nye former for mobilbank ser dagens lys, og stadig flere tjenester tilbys over mobilkanalen. Bank i butikk får stadig større utbredelse. Dette betyr at distribusjonen av tjenestene er blitt mer robust. Dersom én kanal er utilgjengelig, vil kunden kunne benytte en annen kanal. Dette er en positiv utvikling. Men dersom den sentrale tjenesten er utilgjengelig, den som betjener alle kanalene, vil situasjonen være alvorlig.

Det har vært en rekke systemendringer i Norge i 2010. Norges Bank innførte et nytt system for oppgjør i mai 2010. I november innførte NICS (Norwegian Interbank Clearing System) et nytt 3. oppgjør for avregning. I august startet Oslo Clearing opp et nytt system der Oslo Clearing er sentral motpart når det gjelder avregning og oppgjør i verdipapirmarkedet. Innføring av disse endringene har stort sett gått etter planen.

2.7 Cloud Computing (Nettskyen[2])

Såkalt Cloud Computing (CC) er antagelig det mest omtalte og presenterte temaet innen IKT-teknologi i 2010. NIST[3] definerer, fritt oversatt, CC som en modell for leveranse over nettverk av lett tilgjengelige, delte IT-ressurser som f.eks. nettverk, tjenere, datalagring, applikasjoner og tjenester, og som raskt kan gjøres tilgjengelig ved behov og med minimal leverandørinteraksjon.

[2] Nettskyen (eng: cloud computing) er en betegnelse for alt fra dataprosessering og datalagring til programvare på servere som står i eksterne serverparker tilknyttet internett.
[3] National Institute of Standards and Technology, USA: http://csrc.nist.gov/groups/SNS/cloud-computing/

CC representerer ikke ny funksjonalitet eller ny teknologi. Tjenestene og ressursene som tilbys gjennom CC er de samme som tradisjonelle datasentra tilbyr, men leveransemodellen er ny. Forskjellen er at kunden, som i denne forbindelse er tilbyderen av en internettbasert tjeneste driftet gjennom CC, ikke lenger vet hvor egne applikasjoner og data prosesseres. At foretakene betaler for faktisk bruk, kan på sikt gjøre det billigere å bruke CC enn å skalere egen kapasitet. Den økonomiske risikoen ved å tilby nye tjenester foretaket på forhånd ikke kjenner bruksmønsteret til, kan også dermed reduseres.

NIST trekker fram de essensielle karakteristikkene ved CC:

- Kunden er sikret automatisk tilgang til dataressurser som server- og nettverkskapasitet uten at det kreves direkte interaksjon med den enkelte tjenestetilbyder.

- Dataressurser er tilgjengelige over nettverket, og kan aksesseres gjennom bruk av ulike tynne og tykke klientplattformer som mobiltelefoner, laptop-er, PDA-er m.m.

- Tilbyderen av CC har en pool av dataressurser som kan betjene mange kunder. Fysiske og virtuelle ressurser blir dynamisk allokert og deallokert basert på kundens behov. Kunden har vanligvis ikke kontroll med eller kjennskap til den eksakte lokasjonen til ressursene som benyttes, men kan stille krav til lokasjon (plassering i nettet) på et høyere abstraksjonsnivå – for eksempel land, stat eller datasenter. Eksempler på ressurser CC tilbyr, er datalagringsplass, prosessorkraft, minne, båndbredde og virtuelle maskiner.

- Tilgangen til dataressurser er dynamisk. Man kan raskt skalere opp ved å øke ressursbruken og raskt skalere ned ved å frigi ressurser. Kunden opplever kapasiteten som ubegrenset; dataressurser kan skaffes til veie i ethvert omfang til enhver tid.

- Ressursbruk kontrolleres og optimaliseres automatisk ved måling på et abstraksjonsnivå som passer til typen tjeneste, eksempelvis lagringskapasitet, prosessorkraft, båndbredde og aktive brukerkontoer. Det blir rapportert på en måte som sikrer innsikt både for leverandør og bruker av tjenesten.

Driftsoperasjonene som leveres i henhold til en tradisjonell driftsavtale mellom en større bedrift og en dataleverandør vil også kjennetegnes av de fleste egenskapene nevnt over. Sånn sett betyr ikke CC noe grunnleggende nytt. Men CC innebærer at kunden må godta at driftsoperasjonen utføres et sted i ”skyen” uten at kunden vet nøyaktig hvor data og funksjoner er lagret. Begrepet “private clouds” brukes om CC der det stilles krav til driftsoperasjoner innenfor ulike områder spesielt for én kunde, blant annet for å sikre etterlevelse av nasjonalt regelverk og direkte kontroll på data og program og også der bedriften selv eier og driver løsningen. Da blir forskjellene til tradisjonell utkontraktering liten.

CC utgjør antagelig størst forskjell for små og mellomstore bedrifter, og tilbydere av CC henvender seg i stor grad til dette segmentet. CC kan bestilles over internett, f.eks. som e-post-tjeneste og CRM-tjeneste, og leveres på dagen uten at kunden må forholde seg til hvor og hvordan tjenesten produseres. Man inngår avtaler uten noen form for menneskelig interaksjon avtalepartene imellom. Ofte benyttes standardkontrakter og produktpakker samt forhåndsdefinerte SLA-krav knyttet til disse.

For små bedrifter kan sikkerhetsnivået som tilbys gjennom en CC-tjeneste være høyere enn det bedriften selv vil kunne etablere. Men CC er et umodent område hvor sikkerhetsspørsmål foreløpig ikke er mye belyst.

ISO/IEC JTC 1[4] / SC 38[5] omhandler bl.a. sikkerhetsaspektet ved CC. Her omtales kort noen av problemstillingene rundt forsendelse av informasjon over internett vedrørende sikring av datastrømmen og sikkerhet for data så lenge de befinner seg i skyen.

- Konfidensialitet
  Brukerne har ikke full kontroll med sine data. CC-modellen kan eksponere data som vises for tjenestetilbyder. Disse datastrømmene, for eksempel logger, kan bli brukt til andre formål enn tjenestekjøperen eller sluttbrukeren ønsker. CC-tilbyderne benytter sjelden kryptering slik som f.eks. nettbankene. Sluttbrukerne har ikke kontroll med hvordan tilbyderne autoriserer sine ansatte. Det kan også være vanskelig, i verste fall umulig, å kontrollere at tilbyder ikke benytter data for å utvide sin egen forretningsvirksomhet.

- Integritet
  Data kan bli overvåket eller manipulert av ulike ytre krefter. Dette kan være myndigheter eller ansatte hos tilbyder. Databaser i skyen kan være fristende mål for kriminelle, spesielt ved mangelfull sikring. I slike tilfeller kan det være umulig for bruker å vite om dataene har blitt utsatt for uautorisert innsyn eller om de er på avveie.

- Tilgjengelighet
  Tilgjengeligheten i nettet kan være både tregere og dårligere enn i et intranett. I tillegg kan nettet blokkeres av ulike eksterne krefter. Data kan korrumperes av ansatte hos tilbyder, og det kan tenkes at myndigheter stenger nettet for å hindre uønsket informasjonsspredning, altså utøve sensur. Domstoler kan også gi adgang til beslag eller innsyn. Slike tiltak kan ramme en tredjepart som benytter samme CC som kunden som i utgangspunktet blir utsatt for tiltak fordi det kan være vanskelig å skille på brukere i en slik situasjon.

- Oppfyllelse av lover og regler
  Uten kontroll på hvor data befinner seg, har man heller ikke kontroll med, eller oversikt over, hvilke lover som regulerer tilgang og bruk av dataene. Beskyttelse av data reguleres

[4] ISO/IEC JTC 1 is Joint Technical Committee 1 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
[5] Reaching for the Clouds: Privacy Issues related to Cloud Computing - Canadian National Body

lovmessig ofte i forhold til hvem som eier dataene. Det kan til tider være uklart hvem som eier data som har oppstått i skyen, ikke minst avledede data og ulike logger. Det er vanskelig for myndighetene å kontrollere at lover og forskrifter følges når de ikke vet hvor data lagres og behandles, og hvordan de er sikret. Det kan også ha betydning hvor den fysiske lagringsenheten er plassert. Bruk av CC må ses på som en form for utkontraktering/offshoring. Sikkerhetsspørsmål må da vurderes på samme måte både for datainnbrudd og i form av backup og gjenskaping av data ved katastrofer og i beredskapssituasjoner.

Enkelhet, anvendelighet og fleksibilitet er drivkreftene bak CC. Som påpekt ovenfor, er det også en rekke ulemper forbundet med CC. For å oppnå samme grad av sikkerhet i en grenseløs sky som utenfor, kreves det særskilte sikkerhetstiltak. De tunge aktørene blant CC-tilbyderne er i ferd med å utvikle løsninger for sikker tilgangskontroll, kryptert kommunikasjon, kunders kontroll med egne data og monitorering av CC-løsninger. Det er likevel langt igjen før CC er modent for banksektorens kjernevirksomhet.

2.8 Algoritmehandel

De siste årene har det kommet en rekke nye teknologiske løsninger i markedene for kjøp og salg av verdipapirer. De nye teknologiske løsningene har medført nye risikoer og utfordringer for kontrollmyndighetene. Eksemplene nedenfor illustrerer enkelte av utfordringene.

Nye løsninger for frekvenshandel og ultrafrekvenshandel åpner for kortsiktig spekulasjon. Algoritmehandel skjer ved at algoritmer er programmert og oppdatert i et datasystem til å ta beslutninger om kjøp/salg basert på markedsinformasjon, for så å legge inn ordre. Dette skjer med høy frekvens.

Enkelte undersøkelser avdekker at mange av algoritmene er nokså like, det vil si at algoritmene vil gi likeartede konklusjoner når det gjelder beslutning om kjøp eller salg. Algoritmehandel kan forsterke svingninger i markedet og føre til ustabilitet. Men det kan også være slik at algoritmene er flinkere enn mennesker til å fange registrerte svingninger og "handle på dem". I undersøkelsen "Rise of the Machines: Algorithmic Trading in the Foreign Exchange Market", analyseres forholdet mellom andelen handler som er utført av algoritmer og volatilitet i valutamarkedet. Undersøkelsen konkluderer med at det ikke er positiv korrelasjon mellom volatilitet og andelen handler utført av algoritmer. Konklusjonene indikerer at algoritmehandel innenfor valutamarkedet ikke innebærer ustabilitet i form av økt volatilitet.

Høyfrekvenshandel, ultra høyfrekvenshandel, algoritmehandel og "dark pools" er begreper benyttet på nye teknologiske handelsløsninger. Verdipapirtilsynet i USA, U.S. Securities and Exchange Commission (SEC), gjorde i 2008 en analyse av risikoer forbundet med den nye teknologien.

6. mai 2010 skjedde det mye omtalte "flash crash". Dow Jones-indeksen falt først med 300 punkter. Dernest falt den 600 punkter på fem minutter. 20 minutter senere var det meste av de 600 punktene hentet inn igjen. U.S. Securities and Exchange Commission og Commodity Futures Trading Commission (CFTC) undersøkte hendelsesforløpet og ga et bilde av et marked som var så fragmentert og følsomt at en stor handel kunne gjøre at aksjemarkedet falt dramatisk. Hendelsen startet med at et fond prøvde å selge et uvanlig stort antall verdipapirer. Til slutt var det ingen kjøpere. Dernest startet høyfrekvensselgere et aggressivt salg, noe som forsterket nedgangen.

Nye teknologiske løsninger har ført til at en rekke nye markedsplasser har vokst frem de siste årene, slik som f.eks. OTC[6] og "dark pools". Disse markedsplassene er mindre transparente enn børser og andre regulerte markeder. Mangel på transparens gjør at det er vanskelig å spore handlene. I enkelte tilfeller er ikke ordrebøkene tilgjengelige, noe som gjør det vanskelig å avdekke aktivitet som skjer umiddelbart før handel og som eventuelt kunne indikere forsøk på kursmanipuleringer.

Finanstilsynet registrerer at det er ulike oppfatninger om risikoer forbundet med de nye tekniske løsningene og de nye markedsplassene. Dette kan tyde på at risikoene ikke er fullt ut avklart. Finanstilsynet følger derfor dette området med betydelig oppmerksomhet.

2.9 Bruk av mobile enheter

Mobile enheter har blitt en stadig viktigere del av IKT-infrastrukturen. Disse løsningene byr på sikkerhetsutfordringer når de mobile enhetene har tilgang til foretakenes interne systemer, deriblant kontorstøttesystemer som e-post og kalender.

Flere av de risikoer som oppstår er med bakgrunn i portabilitet og den utstrakte bruken av åpne trådløse nettverk. Ved bruk av åpne trådløse nettverk øker risikoen for at sensitiv informasjon kan komme på avveie.

Siden de fleste moderne mobile enheter kan lagre store mengder av informasjon, er det viktig at enhetene har tilstrekkelige sikkerhetsmekanismer samt sentrale administrasjonsløsninger. At enheten har sikkerhetsmekanismer som muliggjør kryptering av sensitiv informasjon, bør være en forutsetning for at enheten kan være en del av et foretaks IKT-infrastruktur.

Dersom et foretak bruker mobile enheter i sin IKT-infrastruktur, skal det også være omhandlet i foretakets sikkerhetspolicy. Områder som autentisering, kryptering, oppdateringer og sikkerhetsadministrasjon bør være sentrale elementer i retningslinjene for bruk av mobile enheter.

[6] OTC = "over the counter", det vil si et marked der papirene ikke er notert.

2.10 Tjenesteutvikling innenfor betalingssystemer

En betalingstjeneste omfatter alle elementer i transaksjonskjeden mellom betaler og betalingsmottaker. Dette gjelder i alle markeder, privat og bedrift, og i alle betalingssystemer nasjonalt og internasjonalt.

I finansieringsvirksomhetsloven er det angitt hvilke foretak som kan drive med betalingstjenestevirksomhet, og ingen kan drive betalingstjenestevirksomhet uten konsesjon. Det er nå åpnet for en ny gruppe foretak kalt betalingsforetak. Det forventes at flere foretak vil søke konsesjon som betalingsforetak, og gjennom dette tilby betalingstjenester til både privatkunder og bedriftskunder.

All betalingstjenestevirksomhet er avhengig av en infrastruktur som kan deles i to hovedgrupper. Den ene delen er den kommunikasjonsmessige infrastrukturen, hvor en bank eller et betalingsforetak kommuniserer med betaler på den ene siden og betalingsmottaker på den andre siden. Den andre delen er det pengemessige oppgjøret som krever en bokføring av betalingstransaksjonen på betalers konto (debet) og på betalingsmottakers konto (kredit). Bokføringen kan skje innenfor samme betalingsforetak eller bank uten at det flyttes penger, men bare når begge parter har konto hos samme foretak. Har partene konti i ulike foretak, vil transaksjonen bli avregnet i avregningssentral og ikke bli ferdigbehandlet før endelig pengeoppgjør er foretatt mellom foretakenes oppgjørskonti i sentralbanken eller en annen godkjent oppgjørsbank.

Normalt omfatter tjenesteutviklingen hvordan kunder kan kommunisere med en bank eller et betalingsforetak. Men like viktig er det hvordan den felles infrastrukturen fungerer.

PayPal er det mest kjente betalingsforetaket internasjonalt. Dette foretaket ble etablert i USA på basis av handel på internett, men har senere blitt overtatt av eBay og ekspandert videre globalt. I dag har foretaket ca. 220 mill. konti. Tjenestekonseptet som tilbys er at betaler belastes på et kredittkort eller PayPal-konto, og mottaker godskrives på en intern PayPal-konto. PayPal bruker en vanlig bank som oppgjørs- og likviditetsleverandør i forvaltningen av PayPal-kundenes penger. PayPal er en stor kontofører hvor det er mulig å gjøre raske transaksjoner mellom to parter som begge har konto hos PayPal. PayPal deltar følgelig ikke i det tradisjonelle interbankmarkedet. Ønsker en betalingsmottaker å få pengene på sin konto i en vanlig bank, må denne formidles ut av PayPal-systemet og inn i det tradisjonelle bankmarkedet.

Konkurransefortrinnet til PayPal er at det gjennom interne transaksjoner i eget system kan flytte penger på sekundet. Med denne funksjonen kan brukere enkelt overføre penger mellom iPhone-er. Programmet kan lastes ned gratis på Apple i iTunes Store eller Apples App Store for iPhone eller iPod Touch. Overføringen mellom PayPal-konti skjer umiddelbart ved at brukerne holder sine iPhone-er mot hverandre.

Ved at transaksjonene gjøres i eget system, flyttes imidlertid ikke penger. Det er bare en debet/kredit-transaksjon eller -informasjon mellom to kunders konti i PayPal-systemet. Lignende transaksjoner gjøres også innenfor Western Union, Hawala-systemet og tradisjonelle banker for enkle overførsler

og/eller mellom egne konti. Effektiviteten, både uttrykt gjennom transaksjonstid og bruk av likviditet, øker med de enkelte institusjoners størrelse, hvor det i et stort foretak finnes en større sannsynlighet for at flere kunder vil kunne samhandle. Andre eksempler på nye tjenester som kan innebære risiko er såkalt "overlay payment services" som i enkelte tilfeller opererer mellom kunden og banken. Denne type løsninger må vurderes nøye både mht. risiko, sikkerhet og etterlevelse av regelverk før det bør introduseres.

I den senere tid har internettportaler og internettforetak som Facebook, Google og Twitter kommet opp som potensielle markedsplasser og tilbydere av betalingstjenester og enkle utlån. Deltakere på slike internettområder kan enten organisert eller individuelt gjøre bilaterale betalingstransaksjoner og eventuelt andre finansielle transaksjoner som innebærer overføring av likviditet eller også risikotagning gjennom direkte utlån. Facebook, Google og Twitter utnytter nettverkseffektene ved at de har mange brukere som ønsker å samhandle. Transaksjonsvolumet kan være meget høyt, men hver enkelt transaksjon er pengemessig relativt liten. Det er uklart på det nåværende tidspunkt hvordan dette vil utvikle seg, og særlig hvordan transaksjonssikkerheten og muligheten for økonomisk kriminalitet på disse markedsplassene skal håndteres.

Tjenesteutviklingen i bedriftsmarkedet er mest synlig for tjenester rettet mot større og gjerne internasjonale bedrifter. Ofte er det her nye tjenester utvikles først som et markedskrav. Etter en tid videreutvikles disse for bruk også av mellomstore og mindre bedrifter.

I løpet av de siste årene har det skjedd en gradvis tilnærming til mer bruk av standardiserte internasjonale meldingstyper på basis av ISO 20022 XML, hvor også bedrifter er direkte brukere. Det startet med at Swift åpnet for at bedrifter kunne gjøre alle typer transaksjoner mot banker eller andre finansforetak. I dag er det ca. 800 bedrifter som er direkte brukere av betalings- eller andre oppgjørstjenester gjennom Swift-nettverket. Dette har medført en betydelig effektivisering av bedriftenes likviditetshåndtering samt all administrasjon knyttet til dette.

Swift har nå lansert produktet eBAM (electronic Bank Account Management). Denne tjenesten omfatter åpning av konti, endring av kontoforhold og innmelding av autorisasjoner og signaturer direkte mot de enkelte banker som bedriftene benytter. Bedriftene måtte tidligere gå veien om manuelle tjenester hos sine bankforbindelser, men nå kan de effektivisere ved å gjøre dette "back-office"-arbeidet selv. Bankene kan også spare kostnader ved å forenkle eksisterende grensesnitt mot sine bedriftskunder.

2.11 Internettkriminalitet

2.11.1 Kriminalitetsutviklingen

Aktører i finansbransjen rapporterer om et økende trusselnivå innenfor internettkriminalitet. Hewlett Packard (HP)-studien *"Cyber Security Readiness"* indikerer at mer enn halvparten av foretak i USA (56 prosent) og over en tredel av europeiske foretak (38 prosent) mener at de har vært utsatt for et nasjonalt cyberangrep. 78 prosent av organisasjonene i USA og 60 prosent av de europeiske mener at et cyberangrep i vesentlig grad vil påvirke kritisk nasjonal infrastruktur i de nærmeste to årene. Et stort flertall mener at cyberangrep er vanskelige å oppdage (88,5 prosent), ikke lar seg rette opp raskt (86,5 prosent) og at det ikke eksisterer gode mottiltak mot slike (82,5 prosent).

I Symantecs undersøkelse *"2010 Critical Information Infrastructure Protection"*, fremgår det at 53 prosent av leverandørene av kritisk infrastruktur sier at deres nettverk har vært utsatt for politisk motiverte cyberangrep. Deltakerne opplyser at de har opplevd angrep i gjennomsnitt ti ganger de siste fem årene, og at disse har kostet dem gjennomsnittlig USD 850.000.

Ifølge HP-studien mener 80 prosent av foretakene i undersøkelsen at de er en del av kritisk infrastruktur. Dette gjelder foretak innenfor bransjer som olje og gass, telekom, finans, strøm og vann. Foretakene gir uttrykk for at de innser alvoret og behovet for å være forberedt. Men undersøkelsen viser at under halvparten rent faktisk er i stand til å motstå et cyberangrep, ifølge HP.

Myndighetene i en rekke land, deriblant Norge, har vært utsatt for angrep med svært alvorlige konsekvenser. Angrep i kjølvannet av Wikileaks-avsløringene viser med all tydelighet at angripere kan gjøre stor skade og legge betydelig press på myndigheter og tjenestetilbydere på nett. Enkelte av angrepene har vært rettet mot finansbransjens informasjonsnett som reaksjon på at finansforetakene stengte tilgangen til Wikileaks-kontoer.

Facebook og Twitter er eksempler på enorme sosiale nettverk hvor deltagerne kommuniserer over internett. Det er en åpenbar fare for at disse nettverkene kan bli eksponert for ulike former for cyberangrep. For eksempel meldte NTB 06.08.2009 følgende*: "Mikrobloggtjenesten Twitter ble torsdag slått ut av et ondskapsfullt cyberangrep"*.

De sosiale nettverkene kan være arenaer for "social engineering" (avluring av informasjon) med sofistikert innsamling av personlige data som i neste omgang kan være basis for misbruk. Ved organiserte, planlagte angrep vil slik datainnsamling ofte utgjøre en av flere kilder til informasjon. Trenden ser ut til å være at angriperne kombinerer ulike teknikker for å maksimere utbytte. Både "social engineering", ondsinnet kode og teknisk manipulering av utstyr kan inngå som ledd i id-tyveri

som brukes til å åpne konto i en annen persons navn og benytte tjenester under en annen identitet i ulike elektronisk kanaler.

Mye tyder på at angriperne er godt organisert. Bot-farmeren som kontrollerer botnettet er den som dyrker og kultiverer botnettet[7], dvs. maskinene som benyttes til å utføre angrepene. De kriminelle leier og bruker nettet. Medhjelpere blir utstyrt med falske pass og benytter passene for å få opprettet bankkontoer. I mange tilfeller oppretter én person flere kontoer under flere forskjellige identiteter. Stjålne identiteter blir misbrukt i vinnings hensikt. Senere tids arrestasjoner i USA og Storbritannia indikerer at organiserte grupper står bak svindelen, og at disse har midler til å drive lønnsom internettkriminalitet i stor stil.

I 2010 har det vært økt aktivitet fra kjente trojanere som Zeus og Torpig mot nettbanker i Norge. Kjennetegn ved angrepene er at kundens PC blir infisert med ondsinnet trojaner-kode ved at de åpner spam-e-post, klikker på lenker eller laster ned fra nettsider. Den ondsinnede koden sørger for at brukerens PC blir koblet til et botnett og en server i et kontrollsenter operert av dem som har distribuert koden. Kontrollsenteret kan avlese brukerens tastetrykk på PC-en. Trojaneren går så inn i hvilemodus. Når brukeren taster nettadressen (url) til sin nettbank, starter trojanerprogrammet. Angrepet videre er ofte basert på "phishing". Brukeren blir presentert for et påloggingsvindu som til forveksling er lik bankens, men inneholder flere felter for å fylle inn påloggingsinformasjon. Ofte kan man se dårlig norsk i denne brukerdialogen. Nettadressen som kommer fram i det falske påloggingsvinduet er forfalsket og mangler ofte sikkerhetsmarkeringen som er i en ekte nettbank, nemlig hengelås til høyre for nettadressen i url-feltet. Kontrollsenteret i botnettet overvåker de infiserte PC-ene i sanntid. Kundens påloggingsdata blir stjålet og kontrollsenteret logger seg inn som kunden i kundens nettbank og legger inn transaksjoner. Mottakerkonti – såkalte "mules" – er oftest i en bank i utlandet.

Norske nettbankkunder er også utsatt for ulike forsøk på phishing gjennom e-poster fra avsendere som utgir seg for å være en bank eller en annen relevant institusjon.

Det viser seg at antivirusprogrammene er lite effektive mot trojanere som ikke allerede er kjent på nettet. I tillegg vil en trojanerkode, når den har infisert en PC, kunne bli endret via masterserveren slik at et antivirusprogram som har fått fatt i den opprinnelige profilen, allikevel ikke vil gjenkjenne trojanerkoden.

[7] BOT (utgjør siste ledd i det engelske ordet Robot) står for en type ondsinnet kode som lar angriperen ta kontrollen over datamaskinen. De er også kjent som "webroboter" og er som regel en del av et helt nettverk av infiserte maskiner, også kalt "botnett", som ofte er skapt av infiserte maskinen fra hele verden. Siden en botinfisert datamaskin er underkastet sin mester, er det mange mennesker som kaller slike maskiner for "zombier". De kriminelle som kontrollerer disse kalles bothyrder eller botmestere. Noen botnett kan bestå av noen hundre eller noen tusen datamaskiner, men andre har både ti- og hundretusen "zombier" til sin disposisjon. Mange av disse datamaskinene er infiserte uten at eieren vet om det. Noen mulige symptomer? En bot kan få datamaskinen til å gå saktere, vise merkelige meldinger eller helt enkelt krasje.

2.11.2 Tiltak for å redusere risiko

Banker både i og utenfor Norge prøver å øke sikkerheten ettersom trusselnivået øker. Santander tilbyr alle kunder gratis programvare som begrenser funksjonaliteten i nettleseren. Ifølge leverandøren opprettes det en tunnel for sikker kommunikasjon med nettstedet. Dette skal hindre ondartet programvare fra å sette inn data og stjele informasjon som presenteres for nettleseren. Ondartet kode blir automatisk fjernet. Programmet oppretter en direkte forbindelse mellom banken og en døgnkontinuerlig analysetjeneste som sjekker både for kjente trusler og trusler under oppseiling.

National Westminster Bank har de senere årene gradvis innført nye tiltak knyttet til kundens bruk av nettbank. En tid tilbake krevde banken at kunden installerte programvare med sikkerhetsfunksjoner. I den senere tid har banken knyttet sentrale kundefunksjoner til en forutsetning om at kunden har installert bankens sikkerhetskort og kortleser på sin PC.

I 2010 kom et gjennombrudd når det gjelder internasjonalt samarbeid for å bekjempe internettkriminalitet. Samarbeid mellom flere lands politimyndigheter førte til opprulling av en avansert ring av cyberkriminelle. De kriminelle var i ferd med å stjele inntil USD 220 millioner fra bankkontoer som var kompromittert ved bruk av Zeus-viruset.

Finanstilsynet registrerer at det nasjonalt og internasjonalt foregår et mer eller mindre uformelt samarbeid mellom finansinstitusjonene. På denne måten ble norske banker varslet om at kunder var kompromittert av Zeus-viruset. På europeisk nivå er det ønskelig at varsling kan inngå i en mer formell, strukturert samarbeidsform som vil gi mulighet for å reagere raskere og som vil være bedre egnet til å håndtere mer omfattende angrep. Et EU-støttet utviklingstiltak, CoMiFin[8] (www.comifin.eu) har utviklet en IT-plattform som støtte for samarbeid av denne art. CoMiFin-løsningen skal gjøre det enkelt å sette opp en desentral (peer to peer) IT-plattform som støtter analyse av trafikkdata fra deltakende finansforetak, og som varsler disse om angrep. Det foregår også annen type samarbeid på dette området i Europa gjennom myndigheter og aktører i finanssektoren, nemlig FI-ISAC – en europeisk internettrelatert organisasjon knyttet til finanssektoren. ISAC står for "Information Sharing and Analysis Center".

Finanstilsynet er kjent med at norske banker vurderer flere mulige tiltak som vil kunne redusere risikoen innenfor internettkriminalitet. Aktuelle tiltak er at kunden avgrenser utvalget av kontoer som det kan overføres penger til, at alle overføringer kun kan gjøres mot et på forhånd oppdatert mottaksregister, og at hvert enkelt brukersted har unike engangskoder for hver kunde. Engangskoden ville da være gyldig kun mot et bestemt brukersted, noe som kunne gjøre det mindre interessant for en angriper å benytte den. Tiltak som raskt kan iverksettes er intelligent overvåking som gjenkjenner trojanermarkører, utveksling av informasjon om "mules"-kontoer og manuell kontroll av alle transaksjoner til utlandet.

[8] CoMiFin Et EU-støttet utviklingsprosjekt med betegnelsen: Communication Middleware for Monitoring Financial Infrastructures

2.12 Tyveri av informasjon – identitetstyveri

Data som uønsket kommer ut fra en organisasjons nettverk og registre kalles datalekkasje, og er et økende sikkerhetsproblem. Konsekvensene av lekkasjer fra store registre kan være betydelige. Eksempelvis ble tusenvis av kunder rammet, også norske, ved innbrudd i et dataregister hos en av Visas og Mastercards partnere i Spania sommeren 2009. Registeret inneholdt informasjon om kort og kortbruk. I Norge må vi flere år tilbake for å finne lekkasjer fra registre innenfor betalingsformidling. Det var da lekkasje fra et register som ble operert på en server på vegne av brukersteder som var restauranter og hoteller. Det er også registrert ulike lekkasjer fra små og store offentlige databaser og registre. Basert på erfaring fra land utenfor Norge, er lekkasjer fra datainnsamling og kortregistre utbredt og rammer også norske kunder.

Informasjon som blir stjålet er ofte informasjon som er tilstrekkelig til at inntrengeren kan tilegne seg og misbruke en annen persons eller et foretaks identitet. En stjålet identitet kan benyttes på mange måter, blant annet til produksjon av falske bankkort og tapping av bankkontoer. Den kan også brukes til kjøp av varer og tjenester, til å opprette nye kontoer, opptak av lån, og til å skaffe seg pass og annen legitimasjon. Det kan være en utfordring for enkeltpersoner å bevise overfor bankene at de ikke har handlet uaktsomt, slik at de ikke kan lastes for å ha tapt kontoopplysninger. Erfaringsmessig har norske banker i stor grad dekket kundenes økonomiske tap ved slike tilfeller.

I tillegg til kopiering av kortdata, som eksempelvis er fremskaffet ved en datalekkasje, er tyveri av bankkort, pass, lønnsslipper og annet der persondata fremkommer, eksempler på kilder til identitetstyveri.

Identitetstyverier blir mer og mer utbredt også i Norge. Norske identiteter synes å være attraktive. Omfanget av tyverier i antall og økonomiske tap som følge av disse er imidlertid uklart. Det finnes i dag ingen samlet rapportering og oversikt. Ikke alle saker blir politianmeldt, og ikke alle saker blir rapportert til Finansnæringens Fellesorganisasjon (FNO) da tapsrapportering fra bankene til FNO er på frivillig basis. Det verserer derfor dessverre tall på identitetstyverier som ikke kan verifiseres.

Informasjon til forbrukere og foretak er viktig, og finnes på Datatilsynets hjemmeside og på Datatilsynets nettsted www.slettmeg.no. Videre har NorSIS, en del av regjeringens helhetlige satsning på forebyggende informasjonssikkerhet, satt i gang et identitetstyveriprosjekt og har i den sammenheng etablert websiden www.idtyveri.no.

2.13 Interne misligheter

En utro tjener er en medarbeider som misbruker sin tillit eller tilgang til systemer og informasjon. Motivet vil typisk være å utøve skade eller oppnå personlig gevinst. Utro tjenere som har godt kjennskap til IKT-systemene kan representere en alvorlig trussel.

Utro tjenere er et økende globalt problem for både offentlig og privat sektor. Det som gjør dette så alvorlig for enkelte bedrifter er at mange hendelser kan ta lang tid å oppdage – nok tid til å sette en liten bedrift ut av virksomhet eller skade en bedrifts omdømme.

De to sektorene som er mest rammet av utro tjenere er to av de mest regulerte områdene som bank/finans og offentlig forvaltning. Utfordringene her er at kontrollmekanismene som er etablert for å avsløre svindel gjennom f.eks. interne revisjoner ikke alltid er like gode for å avdekke interne misligheter. Norge retter gjennom regelverket i finanssektoren stor oppmerksomhet mot styring og kontroll, og dette kan ha medvirket til at problemet antas å være moderat sammenlignet med andre land. Men hendelser indikerer at problemet kan være økende.

Ifølge ACFE (Association of Certified Fraud Examiners) viser funn i 2010 at misligheter er av samme type, uansett hvor de forekommer over hele verden. Undersøkelsen avdekket at mer enn 43 prosent av de rapporterte interne mislighetene var inntruffet utenfor USA.

Mer enn 80 prosent av hendelsene i studien ble begått av enkeltpersoner i en av seks avdelinger: regnskap, drift, salg, toppledelsen, kundeservice eller kjøper. Dessuten hadde mer enn 85 prosent av svindlerne ingen tidligere tiltaler eller dommer for svindelrelaterte lovbrudd. ACFE fant at snittet på tap forårsaket av yrkesmessige bedrageritilfeller i 2010 var USD 160 000.

3 Systemer for betalingstjenester

3.1 Generelt om betalingssystemer

Betalingssystemene er en sentral funksjon for all økonomisk aktivitet. All handel med kommersielle eller finansielle produkter resulterer i et avtalt pengemessig oppgjør. Strukturen i et lands betalingssystemer er tilnærmet lik innenfor OECD-området; en sentralbank, ulike typer banker, betalingsinstitusjoner eller andre finansforetak er aktive deltakere i en finansiell leverandørkjede hvor kjedens elementer omfattes av betalingssystemene. I Norge reguleres betalingssystemene gjennom lov om betalingssystemer, andre lover og forskrifter og gjennom finansnæringens selvregulering forvaltet av Finansnæringens Fellesorganisasjon (FNO).

I 2009 utgjorde bruk av betalingstjenester i Norge 11 568,6 milliarder kroner[9]. Over 98 prosent av oppgjørene skjer ved elektroniske betalingsformer. Kun 1,7 prosent av betalingene utføres via blanketter. I varehandelen, som utgjør anslagsvis 678 milliarder kroner, skjer ca. 70 prosent av betalingene elektronisk. Ca. 2/3 av kontantene hentes fra minibanker eller ved uttak knyttet til varekjøp. Kontanter utlevert over bankenes skranker utgjør om lag 10 prosent av omsetningen i varehandelen.

I Norge er det viktigste betalingsinstrumentet i bedriftsmarkedet nettbank med 61 prosent. Bedriftsterminalgiro utgjør 23 prosent. For kortbetalinger i privatmarkedet har BankAxept 80 prosent av markedet målt i verdi. Norge er i verdenstoppen når det gjelder bruk av betalingskort.

Et betalingssystem defineres som et system basert på felles regler for avregning, oppgjør og overføring av betalinger mellom to parter som samhandler økonomisk. I et slikt betalingssystem skilles det mellom transaksjoner mellom banker, et interbanksystem (mellom banker), og transaksjoner mellom private kunder (betalingstjeneste mellom kunde og bank). Ny teknologi har i stor grad påvirket systemene for betalingstjenester de seneste årene. Kostnadseffektiv drift, brukervennlighet og sikkerhet har vært sentrale elementer.

[9] Norges Banks Årsrapport om betalingssystem 2009.

En stor del av den anvendte elektroniske infrastrukturen er allerede utkontraktert til selvstendige IKT-leverandører med egne planer og mål. Ansvar som er gitt de konsesjonspliktige foretakene gjennom lover og forskrifter vil imidlertid alltid forbli hos foretakene. Dette omfatter alle elementer og aktører i hele transaksjonskjeden mellom betaler og betalingsmottaker. Finanstilsynet har avdekket at dette ansvaret i mange tilfeller er dårlig forstått, også hos sentrale ledere. Mange foretak må i større grad fokusere på dette ansvaret ved spesielt å sikre nødvendig kompetanse til fullt ut å kunne styre og kontrollere det driftsmessige forholdet til leverandøren, eventuelt underleverandøren, som betalingssystemene er utkontraktert til.

Rammebetingelsene for betalingssystemer i Norge er påvirket av økt grad av harmonisering innen EØS. Særlig gjelder dette standardisering og utformingen av tilbudet av betalingstjenester. Betalingstjenestedirektivet, som er et fullharmoniseringsdirektiv, er fullt ut implementert i norsk lovgivning fra og med 1. juli 2010. Etter de nye reglene er det nå konsesjonsplikt for alle typer foretak som ønsker å tilby betalingstjenester, nasjonalt og internasjonalt. Gjennomføringen av betalingstjenestedirektivet i norsk rett har åpnet for en ny type foretak, nemlig betalingsforetak. Bestemmelsene om betalingsforetak kommer til anvendelse for alle som driver blant annet pengeoverføringsvirksomhet, og bestemmelsene vil kunne omfatte foretak/personer som ikke oppfatter sin egen virksomhet som konsesjonspliktig. Det vil være en oppgave for alle banker å vurdere om for eksempel privatpersoner med stor og hyppig gjennomstrømming av likvider på sine konti faktisk driver konsesjonsbelagt virksomhet som betalingsforetak. Dersom slik virksomhet identifiseres, må bankene be disse selskapene eller personene søke om konsesjon som betalingsforetak siden slik virksomhet er ulovlig uten tillatelse.

3.2 Risiko og sårbarhet i betalingssystemene

Økt bruk av elektroniske systemer fra mange leverandører i utformingen av fleksible betalingstjenester utvider selve transaksjonskjeden og øker kompleksiteten i betalingssystemene. Dette kan medføre økt risiko for feil.

I Finanstilsynets meldingssystem for hendelser, er det i 2010 innmeldt tre alvorlige hendelser i betalingssystemene. Se også kapittel 4 for detaljer. Disse skyldtes feil i kjernesystemene med betalingsforsinkelser som konsekvens.

For å styre og kontrollere slike risikoer, har myndighetene etablert et rammeverk gjennom ulike lover og forskrifter. Lov om betalingssystemer er den mest sentrale sammen med IKT-forskriften. Lov om betalingssystemer forvaltes tilsynsmessig av Norges Bank vedrørende interbanksystemer, og av Finanstilsynet vedrørende systemer for betalingstjenester og verdipapiroppgjøret. Det er etablert et nært og kontinuerlig samarbeid mellom Norges Bank og Finanstilsynet for at tilsynsansvaret kan utøves mest mulig effektivt og sikkert.

Privatkunder og bedrifter bruker nå flere kanaler inn mot banken for å få utført betalinger. Flere betalingskanaler reduserer risikoen for at bankkundene ikke får utført betalinger. Dersom én kanal er nede, vil det ofte være mulig å benytte en annen.

Tilbydere av nye betalingsmåter er ofte registrert utenfor Norge. De må nå følge de bestemmelser som ble implementert gjennom betalingstjenestedirektivet.

I Norge er det et lite antall operatører av kjernesystemer for banker og finansforetak. Dette kan representere en ikke ubetydelig konsentrasjonsrisiko.

Etablerte beredskapsløsninger for betalingssystemene er viktig for å sikre mot hendelser. Robuste løsninger for å unngå problemer som tekniske feil av type "single point of failure", regelmessig gjennomgang av kontinuitetskrav og testing av reserveløsninger er vesentlige ledd i preventivt arbeid. Det er Bankenes Standardiseringskontor (BSK) som fastsetter BSK-standarder og forpliktende sikkerhetskrav til EFT/POS-systemet[10] i Norge (BankAxept). De fleste kortaktørene i markedet følger dessuten kortselskapenes internasjonale sikkerhetsstandard PCI DSS[11], som stiller krav til bl.a. brukerstedene. Standarden krever at man minst en gang i året evaluerer og sjekker at kravene etterleves. Kontrollen på dette området kan være mangelfull.

Risiko for kriminelle angrep er størst i grensesnittene mellom kunde og bank. Når det gjelder betalingskort er det tyveri av informasjon i/om kort og kortholder, og tyveri av selve kortet med PIN-kode. Det første dreier seg om svindel ved hjelp av ulike metoder som er knyttet til kortbruk, men kan også f.eks. være informasjon på avveie internt i bankene. Dette adresseres ved sikkerhetstiltak i systemene. Tyveri av kort og PIN-kode kan ofte ha med kortholders adferd å gjøre.

I 2009 ble det registrert over 21 000 tilfeller av svindel med betalingskort i Norge[12].
Samlede tap var 215 millioner, opp 8 prosent fra året før. Svindelen utgjør om lag 30 øre pr. 1000 kroner omsatt. For nettbank var det i 2009 registrert null i tap. På papirbaserte girotjenester er tapene 6,1 millioner, som er 4,7 øre pr. 1000 kroner.

3.3 Styring og kontroll med betalingssystemene

Systemer og tjenester for betalingsformidling er en del av samfunnets kritiske funksjoner og infrastruktur.

[10] Electronic Funds Transfer/Point of Sale
[11] Payment Card Industry Data Security Standard (PCI DSS)
[12] Norges Banks Årsrapport om betalingssystem 2009

Styring og kontroll av IKT-virksomheten relatert til betalingsformidling må være en prioritert oppgave. Forretningssidens eierskap og involvering i forhold til funksjonalitet, endringer, problemstillinger og risikoer er nødvendig. Det må stilles krav til struktur, orden, kvalitet og formaliteter, og til at arbeid gjennomføres i henhold til anerkjente standarder og metoder. Finanstilsynet har erfart at mange finansforetak gjennomfører risikovurderinger én gang i året, oftest i forbindelse med internkontrollrapporteringen. Når det gjelder betalingsformidlingsområdet, er dette neppe tilstrekkelig. IKT-forskriften stiller krav til gjennomføring av risikovurdering i forkant av endringer som har betydning for IKT-sikkerheten, og forskrift om risikostyring og internkontroll setter blant annet krav til at foretaket løpende skal vurdere hvilke vesentlige risikoer som er knyttet til virksomheten. Dette gjelder også de deler av virksomheten som er utkontraktert.

Ifølge IKT-forskriften § 9 skal finansinstitusjonene rapportere IKT-hendelser til Finanstilsynet. Finanstilsynet registrerer at et flertall av rapporterte hendelser i 2010 skyldes feil eller ustabilitet i etterkant av utførte endringer. Dette gjelder systemendringer så vel som driftsendringer. Etter Finanstilsynets vurdering ser det ut til å være behov for økt fokus på endringshåndtering inklusive testing, kvalitetssikring, dokumentasjon og godkjenning før endringene settes i produksjon. I henhold til IKT-forskriften skal rutiner for endringshåndtering være etablert, dokumentert og følges opp. Dette er også i overensstemmelse med anerkjente internasjonale metoder, standarder og god praksis.
Store deler av IKT-virksomheten relatert til betalingsformidling i Norge er utkontraktert, og mye er utkontraktert til de samme leverandørene. Som omtalt tidligere foregår det en konsentrasjon hos driftsleverandørene. I tillegg til konsentrasjonsrisikoene som de nye, store aktørene kan representere, tilsier erfaring at finansielle forhold, inntjening og interne synergier ofte får mer fokus ved sammenslåinger enn det å ivareta kundenes krav, behov og forventninger.

Det kan være en utfordring å få effektuert sine krav overfor en stor leverandør som i realiteten knapt har konkurrenter. Foretakene må i forbindelse med utkontraktering sikre at de har tilstrekkelig kompetanse[13] til å forvalte slike avtaler, og til å stille krav i forbindelse med utkontraktering. Det er spesielt utfordrende å stille krav til og følge opp en leverandør etablert utenfor Norge. Risikokultur, risikovurderinger og risikostyring blir i denne sammenheng stadig viktigere både for banker og leverandører for å sikre stabiliteten i betalingsformidlingen. Det er viktig at de risikovurderingene som gjøres er knyttet opp til og dekker de områdene som foretakets retningslinjer[14] setter for IKT-virksomheten.

Ved all utkontraktering må foretaket som utkontrakterer ivareta sikkerheten[15] som beskrevet både i IKT-forskriften, forskrift for styring og kontroll (intern kontroll forskriften) og lov om betalingssystemer. Det er viktig å måle sikkerhet der dette er praktisk gjennomførbart, slik at det er mulig både å vurdere risiko og sette inn forebyggende tiltak der det er nødvendig.

[13] IKT-forskriften § 12
[14] IKT-forskriften § 2
[15] IKT-forskriften § 5

3.4 Meldeplikten - Systemer for betalingstjenester

Ifølge lov om betalingssystemer § 3-2 skal foretakene gi melding til Finanstilsynet dersom de etablerer systemer for betalingstjenester eller gjør endringer i slike systemer. Melding til Finanstilsynet er basert på en egenevaluering hvor foretakene svarer på 19 sentrale kontrollspørsmål. Bestemmelsen i loven er et risikoreduserende tiltak.

Finanstilsynet har i løpet av de fem siste årene mottatt et varierende antall årlige meldinger, og har i den sammenheng vurdert om dette kunne skyldes en undermelding av denne plikten. I løpet av de tre første kvartaler av 2010 mottok Finanstilsynet ingen meldinger om nye eller endrede systemer for betalingstjenester. I 2010 ba derfor Finanstilsynet finansforetakene om å gjennomføre en spesiell gjennomgang og vurdering av sårbare områder knyttet til betalingstjenester. Dette var rettet mot foretakenes egne interne utviklingsprosjekter som kunne omfattes av meldeplikten. Målsettingen med meldeplikten er å kunne identifisere risikoer som er knyttet til IKT-baserte systemer for betalingstjenester og gjennomføre tilsyn.

Basert på Finanstilsynets henvendelse, sendte finansforetakene inn 18 meldinger i siste kvartal 2010. Av disse kom ti meldinger fra ett foretak.

Finanstilsynet har på bakgrunn av undersøkelsen grunn til å tro at meldeplikten ikke er godt nok innarbeidet i bankenes administrative rutiner, og hos enhetene som har ansvar for foretakenes etterlevelse av myndighetenes lover og forskrifter (compliance-ansvarlige). Ansvaret for å melde nye og endrede systemer for betalingstjenester er lagt til ulike organisatoriske enheter hvor denne type rapportering ikke synes å være et primæransvar. I tillegg kan årsaken være at melding om nye og endrede systemer for betalingstjenester alltid gjøres reaktivt, og ofte samtidig med eller senere enn produksjonssetting og lansering i markedet.

Det vil i 2011 bli satt i verk tiltak for å bedre foretakenes oppfølging og etterlevelse av meldeplikten.

3.5 Oversikt over årlige tap knyttet til betalingstjenester

I samarbeid med Finansnæringens Fellesorganisasjon (FNO) og Bankenes Standardiseringskontor (BSK) ble det sendt brev til bankene for å innhente tapsdata som blant annet omfattet betalingstjenester. Hensikten er å følge opp dette videre slik at det kan presenteres tapsdata på de samme tjenestene over tid. Det vil da være mulig å se hvordan tapene utvikler seg, noe som vil gi et bedre grunnlag for å dimensjonere tiltakene både for enkeltforetak, bransjeorganisasjoner og myndigheter. I første omgang har Finanstilsynet valgt å presentere tapsdata på utvalgte

betalingstjenester innenfor områdene internettbank, bruk av kort i tjenestekanalene, minibanker, butikkterminaler (EFT/POS) og bruk av kort ved handel på internett via nettbutikker.

TAP VED BRUK AV BETALINGSKORT (tall i hele tusen kr)

Svindeltype betalingskort	**2010[1]**
Misbruk av kortinformasjon, kort ikke til stede (internetthandel)	9.401
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort i Norge	1.765
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort utenfor Norge	31.740
Kort tapt eller stjålet, misbrukt i Norge	14.395
Kort tapt eller stjålet, misbrukt utenfor Norge	5.149
Borte i posten	4.239
TOTAL	**66.689**

1) Tall innhentet av Finansnæringens Fellesorganisasjon og Bankenes Standardiseringskontor i samarbeid med Finanstilsynet.

TAP VED BRUK AV NETTBANK (tall i hele tusen kr)

Svindeltype nettbank	**2010**
Angrep ved bruk av ondartet programkode på kundens PC (trojaner)	0
Angrep som utnytter sårbarheter i nettbankapplikasjon (hacking)	0
Phishing (avluring av informasjon)	0
Andre former for angrep på nettbank	0
Annet (tyveri av kodekort og annen informasjon)	2.398
TOTAL	**2.398**

Som statistikken viser, er fortsatt tapene knyttet til virksomheten i Norge moderate i forhold til informasjon om tap fra andre sammenlignbare land. Men tapene på kortområdet er likevel ikke ubetydelige. Ut fra tidligere estimater er de også økende. Det ser ut til at tapene som skjer i Norge går noe i bølger knyttet til de kriminelles bruk av nye tekniske løsninger og næringens etablering av mottiltak. Tapene som skjer utenfor Norge er betydelige. Dette kan dreie seg om informasjon som kan være stjålet i Norge og sendt til mottaker utenfor Norge via internett. Tapene på nettbanktjenesten er

fortsatt svært lave. Generelt ser vi at tapene i 2010 er relatert til mer tradisjonelle tyverier og ikke internettbaserte angrep.

4 Finanstilsynets funn og observasjoner

På ulike måter har Finanstilsynet jevnlig kontakt med finansforetakene og er oppdatert om status på IKT-området. I 2010 var det mange kontaktpunkter mellom Finanstilsynet og finanssektoren som det vil fremgå av kapitlene under. Dette er tilsyn og avtalte samtaler som ledd i tilsynets planlagte virksomhet, men også møter iverksatt på kort varsel som reaksjon på informasjon Finanstilsynet er blitt kjent med om hendelser og spesielle utviklingstrekk.

4.1 Funn fra IT-tilsyn i 2010

Finanstilsynet opprettholdt et høyt aktivitetsnivå på IT-tilsyn i 2010. Det ble gjennomført 26 stedlige IT-tilsyn. I tillegg ble det gjennomført 31 dokumentbaserte IT-tilsyn. Tilsynene omfatter bank, forsikring, ulike typer foretak knyttet til verdipapirområdet, inkassoforetak, eiendomsmeglingsforetak og flere av de store dataleverandørene både i Norge og Norden.

IKT-forskriftens § 12 Utkontraktering gir Finanstilsynet adgang til å gjennomføre tilsyn hos leverandør som ledd i tilsyn med finansforetaket som har utkontraktert tjenester til leverandøren. Funn fra IT-tilsynene viser at noen områder krever spesiell oppmerksomhet.

4.1.1 Test av katastrofeløsninger

Finanstilsynet har gjennom resultatene fra gjennomførte IT-tilsyn funnet at testing av foretakenes katastrofeløsninger ofte har mangler i omfang og kvalitet. Porteføljen av IT-systemer er sammensatt og basert på leveranser fra flere leverandører. Test av en katastrofeløsning krever en form for ende-til-ende-testing med deltagelse fra alle involverte parter for å sikre ønsket funksjonalitet i en krisesituasjon. Det er ikke tilstrekkelig at dataleverandør gjennomfører tester. Finansforetaket selv må også delta. Ved endringer av systemplattform eller leverandør, viser det seg å være en utfordring å sikre at katastrofeløsningen tilpasses nytt miljø. Test av katastrofeløsning på ny plattform foretas ofte for seint.

4.1.2 Koordinering av prosesser

De fleste foretakene har etablert gode og fungerende prosesser innenfor området IKT-drift. En gjennomgående trend er bruken av standarder, og særlig er ISO 20000 (ITIL) en standard som det ofte refereres til. Gjennom tilsyn i 2010 har Finanstilsynet merket seg at den enkelte driftsprosess i seg selv fungerer etter hensikten, men at driftsprosessene samlet ikke i tilstrekkelig grad kommuniserer med hverandre. Et eksempel på dette kan være at utviklings- og forvaltningsprosessene for applikasjoner ikke i tilstrekkelig grad ber om eller deler informasjonen med prosessene for endringshåndtering, testing og kapasitetsplanlegging.

4.1.3 Ressurssituasjonen

Flere av de løsningene som benyttes innenfor bank og finansnæringen i Norge er løsninger som har sitt opphav i en tid med en annen IT-arkitektur og andre programmeringsspråk enn de som brukes til utvikling i dag. Dette har medført at en stor del av applikasjonsporteføljen til finansnæringen forvaltes og driftes av personell som i løpet av få år vil avslutte sin arbeidskarriere. Det er få eller ingen av dagens nyutdannede IT-informatikere i Norge som søker seg til gamle og kanskje utdøende teknologier og programmeringsspråk. Finanstilsynet har derfor sett en tendens til at stadig flere ønsker å utkontraktere disse tjenestene til land der tilgangen på denne type ressurser er bedre enn i Norge. Dette kan medføre stor risiko ved at ansvaret i foretaket blir svekket samtidig som oppgavene blir ivaretatt av andre ressurser, ofte på lang avstand og med uvant kommunikasjon. På sikt kan dette øke risikoen.

4.1.4 Risiko og sårbarhetsanalyser

Som tidligere år ser Finanstilsynet at kvaliteten på risiko- og sårbarhetsanalyser er et gjennomgangstema. Fra Finanstilsynet innførte gjeldende IKT-forskrift i 2003, har næringen gjort store framskritt i forhold til å gjennomføre slike analyser. Gjennomgående for 2010 er manglende kvalitet på risikoanalysene som omhandler foretakenes ønske om å sette bort IKT-tjenester til land utenfor de områder det tradisjonelt har vært satt bort oppgaver til, slik som Sverige og Danmark. Finanstilsynet har ved flere anledninger i 2010 påpekt overfor tilsynsenheter viktigheten av å gjennomføre gode og tilstrekkelige risiko- og sårbarhetsanalyser. Finanstilsynet legger stor vekt på at det er de enkelte tilsynsenheter som har ansvaret for selv å utarbeide gode og fullstendige analyser.

4.1.5 Foretakenes IKT-kompetanse

Utkontraktering medfører at foretakenes egne IT-avdelinger gradvis er blitt endret, og kompetanse på IT-området er blitt konsentrert på færre ressurser. Dette kan ha medført at det i mange tilfeller er leverandøren av tjenestene som i stor grad styrer og bestemmer utviklingen av løsninger og leveranser til foretakenes applikasjonsportefølje. Denne fremgangsmåten kan være hensiktsmessig hvis leverandør og foretak utveksler og samordner sine strategier. Gjennom tilsyn har Finanstilsynet identifisert at mange foretak mangler tilstrekkelig bestillerkompetanse til å stille krav til og kontrollere tjenesteleverandørens IKT-leveranser.

4.2 Intervjuer – foretakenes egne vurderinger

Finanstilsynet intervjuet representanter fra 13 finansforetak i 2010, hvorav noen av intervjuene dekket flere foretak i samme konsern. Utgangspunktet for samtalene var spørsmål knyttet til hva foretakene vurderer som risikoer på IKT-området i inneværende år og i tiden framover. Ved å oppsummere og sammenstille svarene, ser man at flere foretak peker på de samme risikoområdene.

Her følger en oppsummering av foretakenes vurderinger:

Hva ser foretaket på som den/de største risiko/er ved foretakets bruk av IKT?

- Logiske feil i applikasjonene som medfører feil saldo/kontoføring er noe av det verste som kan skje.
- Sårbarhet i åpne nett og infrastruktur er en risiko. Fare for "malware" (ondartet programkode) / virus og svindel i nettbaserte betalingstjenester er en konstant bekymring.
- Det er vanskelig å skaffe tilstrekkelige ressurser. Nøkkelressurser med kombinert IT-faglig og forretningsmessig kompetanse er en flaskehals og gjenbrukes i alle prosjekter.
  Kompetanse på stormaskinmiljø kan bli en knapphet fordi mange nærmer seg pensjonsalderen og nye medarbeidere slutter raskere enn det som var normalt tidligere. Dette fører til et kompetanseproblem.
- Bankene deler opp oppgavene i avtaler med en rekke leverandører, og det er krevende å følge opp avtalene og koordinere leveransene både administrativt og teknisk. Fra leverandørens side er det tilsvarende en utfordring med multikundetilknytning, dvs. å levere sikre tjenester til kunder en rekke ulike steder.
- Mange finansforetak har en nordisk plattform, og det er en utfordring å sikre at IT-applikasjonene etterlever regelverket i alle de nordiske land.

Hva har vært de største problemer på IKT-området i 2010? Og hvordan er disse identifisert?

- Driftsavbrudd grunnet feil i applikasjon, system software og infrastruktur har vært en gjenganger i 2010. Fusjoner har gjort at finansforetak i stor grad er prisgitt én leverandør. Mange foretak opplever forsinkelser i leveranser fra leverandøren. Endret organisering og "støy" i den forbindelse medfører dårligere kvalitet på leveransene. Kompetanse på norsk betalingsinfrastruktur mangler i systemutviklingsmiljøet i andre nordiske land som skal forvalte applikasjoner for det norske markedet.
- Skimming av kort har vært et problem. Offline betalingsterminaler blir benyttet til å samle kredittkortdata. Brukersteder og deres leverandører i Norge og utlandet oppfyller fortsatt ikke PCI-kravene i tilstrekkelig grad.
- Sårbarheter i software-produkter som Adobe og Windows, og krav til patching under tidspress, er en risiko.

Hva ser foretaket på som de største utfordringene i 2011 mht. risiko ved bruk av IKT?

- Av forretningsmessige grunner er det prioritert å få fart på utvikling av nye produkter og oppfylle leveringsforventninger til nye digitale kundeløsninger som omfatter tjenester på mobile enheter. Samtidig skal informasjonssikkerhet i tilknytning til dette ivaretas.
- Det er en utfordring å håndtere strukturendringer og omstillinger samtidig med produktutvikling. Ressursene skal balanseres mellom utvikling og drift. Kvalitet og sikkerhet skal ivaretas. Ved prosjekter må det kartlegges hvordan disse vil påvirke infrastrukturen. Testmetodikk inkludert regresjonstesting må videreutvikles.
- Trusselen fra trojanere er økende ved inngangen til 2011. Organisert kriminalitet rettet mot elektroniske betalingstjenester må overvåkes.
- I mange foretak er det økt integrasjon mellom nasjonal og internasjonal virksomhet. Dette medfører kompleksitet forbundet med at systemer skal dekke betalingsprosesser og kontorapportering for mange land med ulike regelverk.
- Sikre stabilitet og kapasitet i WAN-nettverk mellom nordiske land er viktig.

Hva ser foretaket på som viktige problemstillinger som må adresseres (gjennomføre tiltak) i 2011 mht. IKT-sikkerhet?

- Tiltak mot trojanerangrep har høy prioritet.
- Løsninger for å redusere kriminalitet knyttet til betalingskort er viktig. Tiltak kan være å hindre misbruk av stjålne kort og falske kort gjennom å redusere antall offline-terminaler, bedre kommunikasjonen med potensielt svindlede kunder for raskere å blokkere kortet, etablere enda bedre analyseteam, bedre opplæring av brukersteder og fremtvinge PCI-etterlevelse (de internasjonale kortselskapenes standarder).
- Øke sikkerheten på mobile enheter står høyt på agendaen. PC-er kan krypteres, men ikke mobiltelefoner like lett. Samtidig samles mer informasjon på mobiltelefonene. Det trengs en gjennomgang av mulige sikkerhetstiltak som anti-virus, sentral administrasjon m.m.
- Parallelle prosjekter/system-releaser må koordineres og sikres kvalitet gjennom bedret testing og oppfølging. For å lykkes med utvikling og forvaltningsstyring, trengs ressurser med både forretningskompetanse og IT-faglig kompetanse. Kommunikasjon mellom forretningsside og utviklingsside om tolking av krav til format, koding etc. er viktig. Globale prosjekter og det å sikre et felles nordisk sikkerhetsnivå er en utfordring.

Andre problemstillinger foretaket er opptatt av og som kan ha betydning for virksomhetens bruk av IKT og operasjonell risiko?

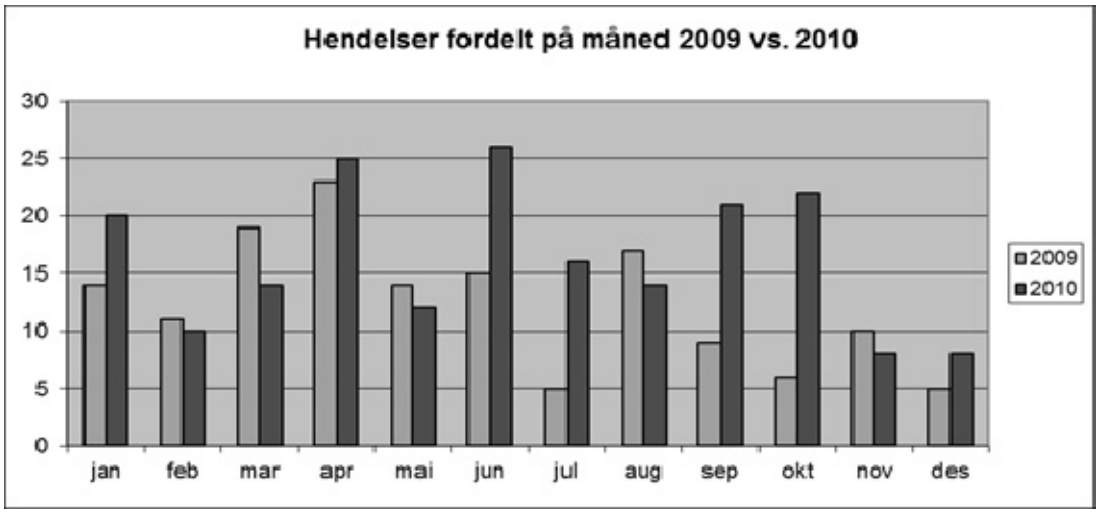
- Sikkerhetstiltak må forstås, følges opp og forankres på ledernivå.

- Kompleksitet i markedsinformasjonen øker stadig bl.a. grunnet økt antall markedsplasser (se mer om dette i kapittel 2).
- Det blir viktig å utvikle global forståelse for lokale ulikheter.
- Stamnettet (foretakets hovedløsning for kommunikasjon) må skiftes ut.
- Realøkonomiske og politiske forhold kan medføre internasjonal uro.

4.3 Rapportering av hendelser til Finanstilsynet

4.3.1 Hendelsesrapporteringen i 2010

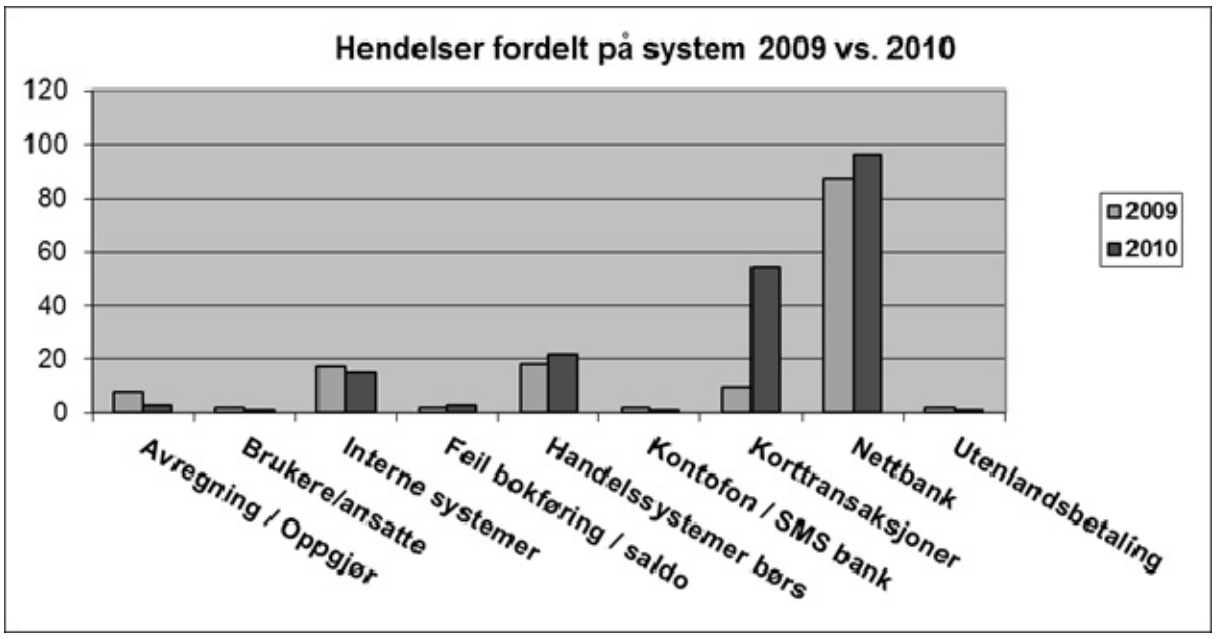
Antall hendelser som ble rapportert i 2010 økte med ca. 40 prosent sammenlignet med 2009. Det ble rapportert 198 hendelser i 2010. Av disse er 42 knyttet til skimming av minibanker. Fortsatt er det bankene som rapporterer flest hendelser.



Kilde: Finanstilsynet

Finanstilsynet følger opp hendelsesrapporteringen på ulike måter. I tillegg til den daglige oppfølgingen, har Finanstilsynet møter med de større foretakene for å drøfte trender i avviksbildet, form og nivå på rapporteringen. Alvorlige enkelthendelser følges opp spesielt. Dette er ofte hendelser knyttet til misligheter, nye former for sikkerhetsbrudd eller andre hendelser som har fått spesielt store konsekvenser.

4.3.2 Funn fra hendelsesrapporteringen i 2010

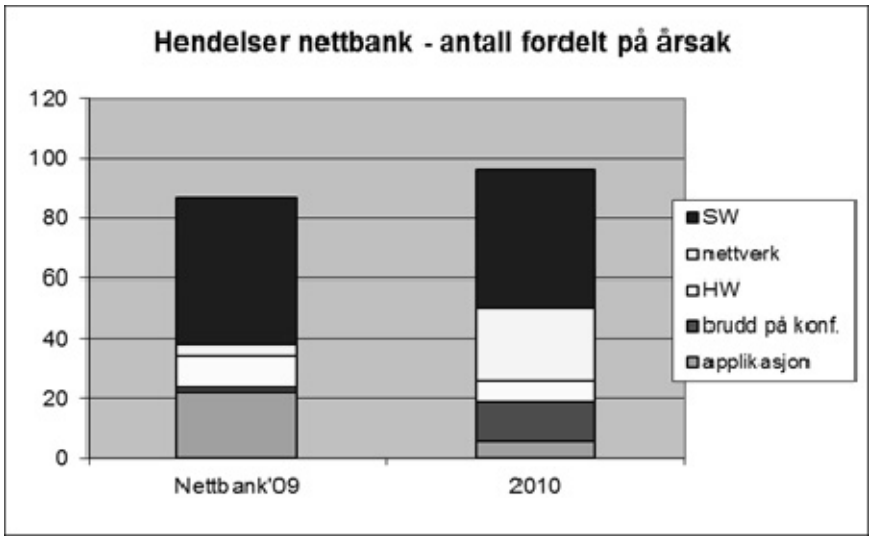


Figuren ovenfor viser hvordan hendelsene fordeler seg på forretnings-/funksjonsområder.
Kilde: Finanstilsynet

Korttransaksjoner - sårbarhet i bankenes betalingsløsninger på brukersteder i Norge
Det er en økning i hendelser knyttet til kortområdet. I 2010 har norske minibanker vært utsatt for alvorlige angrep gjennom ulovlig kopiering av innholdet i magnetstripen, såkalt skimming. Over 40 minibanker av totalt 2200 ble skimmet, og mange kort ble potensielt utsatt for misbruk. Det reelle antallet kort som ble misbrukt, var langt lavere. Alle aktuelle kortinnehavere fikk utstedt nye kort. En viktig oppgave i 2011 blir, i samarbeid med BSK, FNO og bankene, å sikre at relevante tiltak blir iverksatt. Det er allerede etablert et møteforum med bankene på dette området, både for å sikre relevant informasjon og for å drøfte aktuelle tiltak. Oslo politidistrikt har etablert en egen gruppe ved Sentrum politistasjon som arbeider med denne typen kriminalitet på tvers av fylker.

Feil bokføring/saldo
I 2010 har det vært to hendelser der feil i driftsoppsett har ført til doble transaksjoner/reservasjoner på kunders konti. Dette er alvorlige hendelser som har medført et betydelig arbeid for gjenoppretting.

Nettbank - sårbarhet i nettbankløsningen
Fortsatt er det fleste hendelser knyttet til nettbank.



Figuren over viser hvor årsaken til hendelsen ligger. Denne må leses slik at det ikke nødvendigvis er feil ved software (SW), nettverk, hardware (HW) osv. som er årsak til hendelsen. Når det gjelder SW er feilårsaken ofte at SW er satt opp på en uheldig måte, og at dette fører til at nettbanken ikke fungerer som forutsatt. Det kan for eksempel være parametere som er satt uheldig, som ikke lenger passer til omgivelsene eller ikke er tilpasset trafikken e.l.

Figuren viser at det fremdeles er system software-feil som dominerer årsaksbildet. Fortsatt synes det å være en utfordring å opprettholde en stabil kjøreomgivelse for nettbankapplikasjonene. Tjenestene i nettbanken trekker på den samme begrensede pool av tekniske ressurser. Nettbankene rommer etter hvert stadig flere tjenester som igjen gjerne har forbindelser til systemer utenfor nettbanken. Feil i en av de mange tjenestene eller i omkringliggende systemer kan medføre at hele eller større deler av nettbanken blir mindre tilgjengelig. I tillegg endrer trafikken og trafikkmønsteret seg, noe som fører til at parametere i SW må justeres i lys av dette. Det er et komplekst bilde som krever mye kunnskap og oppmerksomhet. Håndtering av SW i kompliserte kjøreomgivelser er ressurskrevende både med hensyn til teknisk kompetanse og koordinerende oppfølging. Slike ressurser kan være mangelvare.

Det er funnet spor av trojanerangrep mot nettbankene i Norge i 2010, men ingen kunder er svindlet. Angrep av større omfang foregår i mange andre land, slik at det er viktig å ha høy fokus på nettbankområdet både gjennom tilsynsvirksomheten, gjennom samarbeid med bransjeorganisasjonene og enkeltforetak, og ved iverksetting av hensiktsmessige tiltak. Det pågår også et samarbeid med

KRIPOS på dette området. Aktiviteten rundt trojanerangrep ser ut til å være oppadgående, slik at oppmerksomheten på dette området har økt noe ved inngangen til 2011.

Hendelser som har medført brudd på konfidensialitet
I 2010 har det vært flere tilfeller av brudd på konfidensialitet. 18 tilfeller ble rapportert i 2010 mot bare tre i 2009. Dette gjelder på tvers av type finansforetak. Dette er ikke hendelser med bakgrunn i misligheter, men hendelser forårsaket av driftsmessige feil, oftest grunnet det foretakene beskriver som "menneskelig svikt" som har oppstått i forbindelse med systemendringer. Dette skyldes oftest uheldig programmering som gjør at kunder i visse situasjoner får tilgang til en annen kundes kundeforhold i nettbanken, får kontooversikt som inneholder data om en annen kunde eller at fødselsnummer trykkes synlig på brev/konvolutter. Denne typen informasjonslekkasje skal også rapporteres til Datatilsynet.

4.4 Utkontraktering til land utenfor Norge

Finanstilsynet er kjent med at flere banker og andre finansforetak i Norge har utkontraktert hele eller deler av sin IKT-virksomhet til leverandører utenfor Norge.

En ny situasjon oppsto i 2010 ved at EDB hadde flyttet deler av sin virksomhet til et deleid selskap av EDB i Ukraina. Finanstilsynet foretok derfor en nærmere undersøkelse av forholdene. Dette viste at det ikke fullt ut var foretatt en formell avtalemessig regulering av oppgavene som var flyttet til Ukraina. Mange av bankene hadde heller ikke gjennomført risikovurdering som skal ligge til grunn for en slik endring i avtalen. Noen banker hadde basert sine vurderinger på de risikovurderinger som leverandøren hadde foretatt og som var svært mangelfulle. Finanstilsynets vurdering var at risikoen knyttet til den aktuelle flyttingen var for høy og at flere regelbestemte forhold var brutt. Finanstilsynets vurdering ble nærmere klargjort gjennom tilsynsmerknader til bankene. Et generelt tiltak var Rundskriv 14/2010 om "Utflytting av bankenes IKT-oppgaver", og som setter klare begrensninger i utkontraktering til områder som betegnes som høyrisikoområder, og er knyttet til nærmere bestemte funksjoner/områder av bankenes virksomhet. Rundskrivet er en klargjøring av Finanstilsynets vurdering av hva som er akseptabel risiko på dette området. Det er en oppfatning at både bankene og leverandøren har tatt rundskrivet til direkte følge og etterlevelse.

4.5 Gjennomførte spørreundersøkelser

4.5.1 Meldeplikten – lov om betalingssystemer § 3-2

I siste kvartal 2010 ble det gjennomført en undersøkelse hos de største finansforetakene om sårbare områder knyttet til betalingstjenester. Bakgrunnen for undersøkelsen var at Finanstilsynet antok at

finansforetak under tilsyn underrapporterte i forhold til meldeplikten. Resultatet av undersøkelsen bekreftet Finanstilsynets antakelse.

Finanstilsynet mottok 19 nye meldinger fra fem finansforetak i denne perioden.

Det ble svart på tre spørsmål med følgende resultat:

1. Har foretaket i 2010 etablert nytt(e) system(er) for betalingstjenester?
   12 ja og 7 nei

2. Har foretaket i 2010 utviklet ny versjon av systemer for betalingstjenester som vesentlig påvirker andre berørte parter som inngår i løsningen?
   12 ja og 7 nei

3. Har foretaket i 2010 utviklet ny versjon av systemer for betalingstjenester med vesentlig endret eller ny funksjonalitet?
   13 ja og 6 nei

Alle foretakene har svart ja på ett eller flere av de tre svaralternativene.

Finanstilsynets konklusjon er at foretakene gjennom denne undersøkelsen er blitt mer oppmerksomme på det som naturlig faller inn under meldeplikten. Dette vil føre til bedret kvalitet på rapporteringen og være et ledd i å redusere den operasjonelle risikoen.

4.5.2 Forskrift om krav til innretning av datasystemer for medlemmer av Bankenes sikringsfond

Finanstilsynet fastsatte 19. mai 2010 ”Forskrift om krav til innretning av datasystemer for medlemmer av Bankenes sikringsfond”. Formålet med forskriften var å beskrive hvordan administrasjonsstyret i en bank som er satt under offentlig administrasjon og Bankenes sikringsfond kan gjennomføre en rask og korrekt utbetaling av beløp som tilsvarer garantien til sikringsfondet.

For å sikre at bankene har implementert de nødvendige løsninger i egne IKT-systemer, har Finanstilsynet bedt de største bankene og bankgrupperingene om selv å vurdere om deres systemer overholder forskriftens krav.

Med bakgrunn i tilbakemeldingene fra bankene, kan Finanstilsynet legge til grunn at de fleste bankene i stor grad anser at de overholder forskriftens krav. Ett forbehold er meldt inn; det gjelder det tredje kravet om å kunne *”vise en reskontro over hvilke krav som er dekket ved utbetaling av midler skaffet til veie fra Bankenes sikringsfond og markere at sikringsfondet har trådt inn i den opprinnelige innskyters krav mot banken”*. Det ble bedt om noe mer tid for å kunne besvare dette spørsmålet.

Videre har noen banker signalisert at de vil oppfylle forskriftens krav innen 31. mars 2011. Prosjekter er i ferd med å bli gjennomført, og leverandør av løsninger har satt dato for implementering av nødvendige endringer.

4.6 Hendelser identifisert fra internasjonale kilder

Enkelte hendelser fra andre steder i verden er interessante å merke seg. Nedenfor er det beskrevet noen hendelser fra 2010.

4.6.1 Tyveri av data fra testsystem i Cleveland, USA

Det har ved anledninger i 2010 blitt stjålet data fra testsystemer hvor reelle produksjonsdata er brukt til test. Ved en anledning ble Federal Reserve Banks avdeling i Cleveland, Ohio, USA hacket, og informasjon fra 400 000 kreditt- og debetkort stjålet og forsøkt solgt. Vedkommende som stjal informasjonen var hjemmehørende i Malaysia, men reiste til USA for å møte en kjøper. Kjøperen var i dette tilfelle en federal agent som arresterte vedkommende etter at han hadde solgt kortinformasjon fra 31 kort for 1000 USD pr. kort.

4.6.2 National Bank of Australia

National Bank of Australia hadde i slutten av november og begynnelsen av desember 2010 store problemer med sine datasystemer. Ifølge offentlig tilgjengelig informasjon, var det en menneskelig svikt som forårsaket feilen. Feilen medførte at ingen av bankens kunder fikk tilgang til sine penger for å betale regninger eller bruke butikkterminaler. Oppgjørene mellom bankene ble også skadelidende. Oppryddingen etter hendelsen ble svært dyr og arbeidskrevende da over 60.000 transaksjoner ble ødelagt som følge av hendelsen.

4.6.3 Hendelse i DBS Singapore

DBS, en av Singapores største banker, hadde i 2010 en hendelse som medførte at minibanker, butikkterminaler og nettbank var utilgjengelig i flere timer. For Singapore er dette en større hendelse enn i andre land fordi retningslinjer fra myndighetene sier at dersom en bank tilbyr denne type tjenester, skal tjenestene være tilgjengelige 24 timer i døgnet året rundt og ha nødvendig infrastruktur til dette.

5 Identifiserte risikoområder

Basert på funn gjennom tilsyn, hendelser, samtaler med foretakene og eksterne nasjonale og internasjonale kilder er det noen områder som peker seg ut som spesielle risikoområder og som må vies ekstra oppmerksomhet i 2011.

5.1 Skimming-angrep mot minibanker

Skimming-angrep mot norske minibanker som skjedde i 2010, var basert på en annen teknologi enn den som ble benyttet ved skimming på midten av 2000-tallet. Mens det tidligere har vært såkalt digital skimming, ble det nå brukt en analog skimming-teknologi. Tiltak er iverksatt for å hindre videre utbredelse av denne typen skimming-angrep. Tapene er begrensede, ikke minst takket være at urettmessige transaksjoner ble oppdaget raskt og potensielt skimmede kort ble sperret raskt. Det er likevel ingen grunn til å tro at det ikke kan dukke opp nye former for skimming-angrep mot minibankene.
Tiltak mot skimming gjennomføres på to plan:

- Fysisk sikring av teknologien i minibanken og stedet minibanken er plassert
- Transaksjonsovervåking og analyse.

5.2 Angrep mot nettbankløsninger

Tjenestene i nettbanken er attraktive mål for svindel grunnet den direkte tilgangen til penger. Ved inngangen til 2011 er beredskapen styrket i forhold til angrep fra trojanere mot nettbankene. Høyt kvalifiserte hackere profesjonaliserer angrepsformene i stadig større grad og finner nye måter å "selge" trojanertjenestene på. For å lykkes med et nettbankangrep, må man ha et sted å overføre pengene, altså en mottakskonto. Ulike scenarier blir generert for å tåkelegge informasjon om hvem som mottar

pengene. Mottaker kan være en kunde som også er angrepet uten å være klar over det ved at kontoen blir benyttet som transittkonto med automatisk videreføring av pengene til en konto i utlandet. Angrep mot nettbanken blir ekstra farlige når ulike angrepsformer kombineres, som for eksempel phishing kombinert med trojaner. Finanstilsynets vurdering er at bankene i Norge har stor oppmerksomhet på trusler mot nettbanken og samarbeider både nasjonalt og internasjonalt om hensiktsmessige tiltak. Det er viktig å prioritere dette risikoområdet som utvikler seg såpass hurtig.

5.3 Mangelfull testing og verifisering av katastrofeløsninger

Foretakene skal i henhold til regelverket gjennomføre test av katastrofeløsningene minst årlig og resultatet skal dokumenteres. Foretakene i finansnæringen benytter IKT-løsninger som er komplekse, sammensatt av mange lag og basert på leveranser fra flere leverandører. Å gjennomføre katastrofetester krever kompetanse og ressurser. Det er viktig å involvere alle aktuelle aktører. Det er en arbeidskrevende prosess, men det er den eneste måten å sikre at beredskapsløsninger vil fungere i en krisesituasjon. Det er vanskelig å si når en katastrofeløsning er godt nok testet, men Finanstilsynets vurdering er at dette området har forbedringspotensial. Det er antakelig et behov for en veiledning om dette temaet.

5.4 Konsekvenser av organisasjonsmessige endringer hos dataleverandørene

I 2010 har det vært flere fusjoner mellom de store dataleverandørene. Fusjonene bidrar til færre leverandører og med det økt konsentrasjonsrisiko og mindre påvirkningskraft for kunden. Fusjoner skaper uro i organisasjonene i en omstillingsperiode, og det påvirker driften. Den nordiske dimensjonen blir stadig mer dominerende. Nordiske konsern skal levere tjenester til finansforetak i hele Norden. Hvert av de nordiske land har sin betalingsinfrastruktur og sitt regelverk. Kompetanse flyttes på og kan i den forbindelse gå tapt og være vanskelig å bygge opp igjen fordi kunnskap om betalingsinfrastruktur i et annet nordisk land er svakere enn kunnskap om strukturen i eget land. Flere foretak har pekt på dette som en utfordring. En potensiell risiko ligger også i at foretak som flytter driften ut av Norge i neste omgang blir en filial i Norge. Vertslandet har ikke helt de samme virkemidlene å bruke overfor en filial, og regelverket kan være forskjellig i moderlandet.

5.5 Mangel i styring og kontroll ved utkontraktering

Det er risiko forbundet med utkontraktering, enten det er til leverandør i eget land, i Norden eller i land lenger unna. Generelt gjelder at jo større avstand det er til leverandøren, jo større er utfordringene knyttet til å sikre tilstrekkelig styring og kontroll med de utkontrakterte tjenestene. Det er derfor grunnleggende at foretakene selv gjennomfører nødvendige risikovurderinger knyttet til utflytting av IKT-virksomhet. Risikovurderingene må omfatte både den operasjonelle risiko isolert, men også landrisikoen knyttet til det landet virksomheten skal flyttes til. Det er ledelsen som skal sørge for at risikosituasjonen er håndtert tilfredsstillende. Foretakene må ta høyde for en økt operasjonell risiko som følge av utkontraktering, og møte risikoen med å etablere relevante tiltak. Dette er områder hvor Finanstilsynet i sitt arbeid har påpekt mangler overfor bankene.

6 Finanstilsynets videre oppfølging

6.1 Generelt

Finanstilsynets arbeidsområder innenfor tilsyn med IKT og betalingstjenester har risiko og sårbarheter i finanssektoren som hovedfokus. Oppfølging av dette skjer ved:

- å sørge for å gjennomføre IT-tilsyn i et omfang og med en detaljering som gjør at tilsynet får et realistisk bilde av hvordan foretakene ivaretar IKT-virksomheten, håndterer risiko og etterlever regelverk

- å sikre registrering og oppfølging av informasjon fra rapportering om IKT-hendelser via e-post til: hendelse@finanstilsynet.no og oversikt på et område som er av vesentlig betydning for finansmarkedets stabilitet

- at tilsynet gjennom blant annet arbeidet med ROS-analyser innhenter informasjon for å ha en mest mulig riktig risikoforståelse på området

- å ha oppmerksomheten rettet mot betalingssystemene gjennom proaktive tiltak, men også gjennom tilsynsvirksomhet og annen oppfølging å sikre etterlevelse av regelverk samt at betaling skjer på en rask og effektiv måte

- å sikre etterlevelse av eksisterende regelverk og sørge for en hensiktsmessig utvikling basert på risikosituasjonen

- å bidra til å etablere samarbeidsarenaer knyttet til problemområder hvor det er viktig med deling av informasjon og drøfting av felles tiltak

6.2 Aktuelle tiltak rettet mot risikoområdene

6.2.1 Skimming

Finanstilsynet følger bankorganisasjonenes arbeid mot skimming og holder seg oppdatert på den teknologiske utviklingen, trusler og sårbarheter innen området. Tilsynet vil også sikre nødvendig informasjon om hendelser og tap som grunnlag for å vurdere potensielle konsekvenser og tiltak for å sikre akseptabel håndtering av risiko slik at man kan begrense eventuelle samfunnsmessige konsekvenser. Tillit til betalingstjenestene er viktig.

6.2.2 Nettbanker

Finanstilsynet følger nettbankløsningene nøye. Det er viktig at bankene har nye sikringstiltak tilgjengelig når konsekvensene av angrepene blir for store. Det er etablert tett kontakt med BSK, samarbeid med Nettbankutvalget og enkeltbanker. Finanstilsynet har også etablert et tett samarbeid på nordisk og internasjonalt plan med andre tilsynsmyndigheter på dette området. Dette bidrar til å sikre et bredt tilfang av informasjon om kriminelle angrep mot nettbanker i andre land og metodene som benyttes. Det er også etablert formelt samarbeid med NorCERT som bidrar til overvåking av nettet, og som er en viktig samarbeidspartner når det gjelder tiltak i nettverk utenfor Norge.

6.2.3 Katastrofeløsninger

Tilliten til katastrofeløsninger er vesentlig for samfunnet. Tilstrekkelig testing for å verifisere at beredskapsløsningen virker er nødvendig. Finanstilsynet vil derfor følge opp dette viktige området både gjennom tilsynsvirksomheten, direkte kontakt mot enkeltforetak og ny spørreundersøkelse i 2011.

6.2.4 Styring og kontroll ved utkontraktering

Det arbeides med denne problemstillingen som omfatter både utkontraktering generelt og offshoring spesielt både gjennom mulige regelverksendringer og gjennom utarbeidelse av egen veiledning til IKT-forskriftens § 12 Utkontraktering. Tilsynet vil følge denne utviklingen nøye gjennom 2011, og samtidig samarbeide med bransjeorganisasjoner og myndigheter i andre land for å sikre avstemming mot beste praksis og internasjonale standarder på dette området.

6.3 IT-tilsyn

Finanstilsynet gir fortsatt prioritet til IT-tilsyn, samtidig som det er en utfordring å videreutvikle tilsynsopplegget slik at relevante problemer og sårbarheter kan identifiseres.

I 2010 ble det eksisterende tilsynsopplegget forbedret og nye tilsynsmoduler etablert. Tilsynet arbeider med å ta i bruk en metodisk gradering av modenhetsnivået til foretakets IKT-organisasjon. Videre pågår det arbeid med å etablere en egen modul for transaksjonstest.

I 2011 vil det bli utarbeidet veiledninger til IKT-forskriften, bl.a. til § 2 Planlegging og organisering, § 5 Sikkerhet, § 10 Krav til kontinuitet, § 11 Driftsavbrudd og katastrofeberedskap og § 12 Utkontraktering.

6.4 Beredskapshåndtering

Finanstilsynet har fra 01.06.2010 fått ansvar for sekretariat og ledelse av Beredskapsutvalget for finansiell infrastruktur (BFI). Tilsynet vil arbeide aktivt for å ivareta og utvikle dette utvalget videre i samarbeid med Norges Bank og de andre deltagerorganisasjonene. Viktige oppgaver er løpende oppfølging av hendelsesutviklingen, stabilitet i den finansielle infrastrukturen og gjennomføring av hensiktsmessige beredskapsøvelser.

6.5 Håndtering av ID-tyveri

Datatilsynet og Finanstilsynet fortsetter samarbeidet når det gjelder ID-tyveri. I arbeidet deltar også NorSIS (Norsk Senter for Informasjonssikring) slik at det kan bygges videre på kartleggingen som tidligere er foretatt på dette området. Arbeidet er innrettet på å identifisere lekkasjekilder, analysere hvordan informasjonen kan benyttes i angrep blant annet innenfor finanssektoren, og hva som kan være effektive tiltak for å stoppe lekkasjer samt redusere mulighetene for misbruk av stjålet informasjon.

6.6 Brukerstedenes etterlevelse av regelverket

Mangelfull sikkerhetsforståelse hos brukersteder (butikker) generelt kan føre til sikkerhetsmangler ved utførelse av betalingstjenester. Finanstilsynet vil også følge opp de nye brukerstedene "bank i butikk" for å bidra til bedre forståelse for juss, ansvar, sikkerhet, kommunikasjon og opplæring.

6.7 Informasjon og kommunikasjon

Samhandling og tillit mellom Finanstilsynet og foretakene under tilsyn er vesentlig. I 2011 planlegges et dagsseminar om risikohåndtering knyttet til IKT-sårbare områder og betalingstjenester som er utsatt for angrep fra kriminelle.

Som et ledd i arbeidet med IKT-sikkerhet i finanssektoren, deltar Finanstilsynet i en rekke ulike fora. Blant de sentrale er Koordineringsorganet for forebyggende informasjonssikkerhet (KIS) og Beredskapsutvalget for finansiell infrastruktur (BFI). Tilsynet samarbeider også direkte med Norges Bank, Nasjonal sikkerhetsmyndighet (NSM), Datatilsynet, Post- og teletilsynet og bransjeorganisasjoner.

Finanstilsynet samarbeider nært med de øvrige nordiske IT-tilsynsenhetene, og er med i et internasjonalt IT-tilsynssamarbeid (Information Technology Supervisors Group) med en europeisk undergruppe. Likeledes deltar tilsynet i arbeidet med internasjonal standardisering i gruppene for bank- og sikkerhetsstandarder, standardisering for elektroniske signaturer (ETSI ESI) og i en gruppe for sikkerhet i den internasjonale dataforeningen, IFIP.

6.8 CoMiFin

CoMiFin er et forskningsprosjekt finansiert av EUs 7. rammeprogram. Leveranser fra CoMiFin kan bidra til at banker på praktisk måte kan koble sammen IT-ressurser mellom deltakerne i et delt, distribuert nettverk. Systemet inneholder funksjoner for å definere og måle tjenestekvalitet, ressursmåling og allokering/deallokering av ressurser, samt å analysere store datamengder. Systemet er ferdig utviklet og testet. Systemet kan benyttes for å avdekke trusler og sårbarheter (Denial of Service-angrep, Man In The Middle Attack mv.). Systemet kan også benyttes som felles utviklings- og testplattform for banker som ønsker å utvikle noe sammen, eksempelvis en felles rapporteringsapplikasjon for myndighetsrapportering. Det vil imidlertid være opp til banker og andre finansinstitusjoner på fritt grunnlag å adoptere en løsning som dette. Det er imidlertid positivt at det gjøres forskning og utvikling på dette risikoområdet.

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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

Design: www.miksmaster.no **Foto:** Jarle Nyttingnes **Origamikunstner:** Stine Walderhaug 02.2011/2 000