FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

RAPPORT

RISIKO- OG SÅRBARHETSANALYSE (ROS)

2011

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)



Risiko- og sårbarhetsanalyse (ROS) 2011

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Finanstilsynet, 28. mars 2012

Innhold

1 Innledning

Finanstilsynet foretar årlig en risiko- og sårbarhetsanalyse (ROS-analyse) av finanssektorens bruk av IKT. Rapporten er basert på en rekke interne og eksterne kilder og inneholder vurderinger av hvordan identifiserte risikoer globalt kan få innvirkning på finanssektoren i Norge. Den teknologiske utviklingen og finanssektorens innføring og bruk av mer komplekse tjenester gjør arbeidet med risiko mer krevende både for den enkelte virksomhet og for myndighetene. Ny teknologi inneholder ofte ukjente sårbarheter som i en tidlig fase både kan utnyttes av kriminelle og føre til feilsituasjoner.

Internett åpner for global elektronisk kriminalitet. For at finanssektoren skal ligge i forkant, må den ha tilgang til korrekt informasjon om internasjonale utviklingstrekk og opplegg for håndtering og reaksjon på uønskede hendelser både juridisk og teknologisk.

For å forstå hva som kan gi økt risiko i framtiden er det viktig å ha fakta om risikosituasjonen og være i stand til å tolke hvilke faktorer som kan endre seg over tid og gi høyere risiko.

2 Utviklingstrekk

Endringer som følge av samarbeid, fusjoner, økt grensekryssende konkurranse, produktutvikling, kostnadsreduksjonsprogrammer og tilgang til ny teknologi stiller store krav til endringshåndtering. Endringer betyr økt risiko. Derfor er det effektivt å ha kunnskap om hva som driver endringene, slik at gjennomføringen kan skje på en kontrollert måte.

2.1 Ny internettprotokoll

Det arbeides nå med å innføre Internet Protocol version 6 (IPv61) som supplement og etter hvert erstatning av IPv4. Dette fordi det begynner å bli mangel på IPv4-adresser. Overgang til IPv6 har vært forberedt over mange år. Likevel er det bare en liten del av internettrafikken (ca. 1 prosent) som går over IPv6 i dag. Levetiden til IPv4 har vært forlenget ved hjelp av ulike tekniske løsninger som dynamisk adressetildeling og deling av adresser, men nå begynner behovet for overgang til IPv6 å bli kritisk av flere årsaker:

- Noen steder i verden er man i praksis tom for IPv4-adresser.
- Teknisk livsforlengelse av IPv4 kan føre til at brukere på ulike steder kan få samme IP-adresse med manglende sporbarhet og andre komplikasjoner som konsekvens.
- Livsforlengelse av IPv4 fører til store unødvendige utstyrsinvesteringer som kan være bortkastet ved overgang til IPv6.
- IPv6 inneholder forbedringer og nye fordeler som brukerne er interessert i.
- En stor og økende utbredelse av mobile enheter (tale, video og data) og utstrakt bruk av maskin til maskin-kommunikasjon (M2M) kan bare bli realisert med det større adresserommet til IPv6.
- Store tjenesteytere, som for eksempel Google, legger om sine tjenester til IPv6. Dominerende operatører internasjonalt, som AT&T, har besluttet en «IPv6 only policy».
- Det offentlige Norge, ved Direktoratet for forvaltning og IKT (Difi) vil innføre IPv6 som en sideordnet standard.

[1] IPv6 er versjon 6 av Internett-protokollen og er etterfølgeren til IPv4. Hovedgrunnen for å utvikle en ny standard var å håndtere mangelen på IP-adresser. Samtidig er flere mangler ved IPv4 utbedret.

IPv6 innebærer en rekke forbedringer. Adresserommet er økt fra 32 bits til 128 bits, pakkesvitsjing er mer effektiv, adressetildeling er mer dynamisk, det er forbedret en til mange-kommunikasjon, mulighet for kryptering og autentisering som del av protokollen, forbedring av QoS (Quality of Service) samt andre forbedringer.

Overgang fra IPv4 til IPv6 er forutsatt å være sømløs sett fra brukernes side. Det er utviklet en rekke overgangsmekanismer som skal sørge for at IPv4-noder og IPv6-noder kan snakke sammen over IPv4- og IPv6-nettverk. Dette er nødvendig fordi utrustning (maskiner og programmer) som krever IPv4, vil eksistere i mange år – kanskje 10 år eller mer. I overgangsmekanismene ligger det også mulige svakheter som kan være utgangspunkt for feil, tjeneste-degradering, stopp og sårbarhet for angrep.

Situasjonen hos de større nettleverandørene i Norge er at noen allerede i hovedsak leverer IPv6, noen vil innføre IPv6 i løpet av 2012, og noen planlegger for en større utrulling i 2013. Brukere i finanssektoren må ta stilling til hvordan man skal forholde seg til dette. Det er sannsynlig at en rekke tjenestetilbydere internasjonalt vil bytte til IPv6 som standard for sine tjenester i løpet av 2012.

2.2 Internett som kritisk infrastruktur

Stadig flere tjenester benytter Internett, og samfunnet som sådan blir mer avhengig av internett. Helse, tele, politi, strøm og finans er avhengig av Internett. Tidligere fungerte telefoni selv om strømnettet gikk ned, men slik er det ikke nødvendigvis i dag.

Å få til et systemsikkert Internett er en utfordring, blant annet fordi følgende sider ved sikkerheten ikke er avklart:

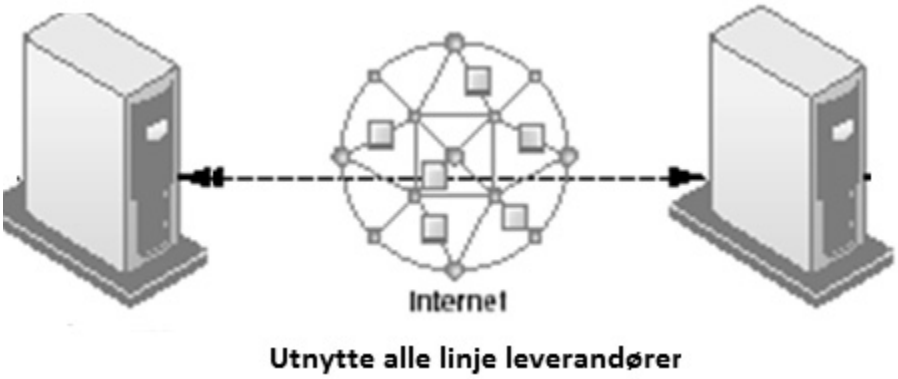
- Topologiene er ikke kjent. Noen få er forsøkt analysert, enda færre offentliggjort.
- Verken peering points[2] eller Service Level Agreements (SLA) mellom operatørene er kjent.
- Ruting-strategiene[3] er ikke kjent.
- Hvilke ruting-policyer[4] som er benyttet, er ikke kjent.
- Korrelerte sårbarheter som stammer fra samlokalisering av kabler og rutere er ikke kjent.

Siste punktet ble til fulle illustrert ved brannen ved Oslo Sentralbanestasjon i 2007 der reserveløsningen lå fysisk samme sted som hovedløsningen.

[2] Peering points på Internett er en samling av nettverk der alle er knyttet sammen så data kan bli transportert fra et nettverk til et annet. Ofte er ikke to nettverk knyttet sammen direkte, men via en tredjeparts nettverk.
[3] Ruting-strategi som gjelder for alle datapakker. Eksempler på dette er: «minste antall hopp», «statisk ruting», «dynamisk ruting».
[4] Datapakkenes ruting, prioritering, service-flagg etc. bestemmes ut i fra aksesslister, pakkestørrelse og andre egenskaper ved pakkene. Reglene er satt av nettverksadministrator.

NorNet[5] er eksempel på eksperimentell nettverksforskning. NorNet er et sett med nettverksnoder der virtuelle nett med egendefinerte ruting-protokoller og applikasjoner kan testes ut. Et sentralt spørsmål som slik forskning kan besvare, er om robusthet og ytelse kan økes ved å utnytte flere nett dynamisk.

Figur 1: Det er flere veier fram



En forutsetning for å kunne besvare spørsmålet er at det er kjent i hvilken grad linjene er uavhengige og selvstendige, det vil si at ikke én hendelse ødelegger linjene fra flere av leverandørene. Etter det Finanstilsynet kjenner til, er det ingen samlet oversikt på området.

Alvorlige hendelser i telenettet våren 2011 rammet store deler av teleinfrastrukturen i Norge. Noen operatører hadde ikke tilgang til alternative rutingsveier og ble hardt rammet.

Det er likevel de mange små hendelsene som er en hovedutfordring. Statistikk over mobilt bredbånd viser at 1 av 3 forbindelser er nede mer enn 10 minutter per dag. Det er mange noder involvert i en forbindelse, og nedetiden kan komme opp i rundt 1,5 prosent. Dette er betydelig mer nedetid enn det som er vanlig for kritiske komponenter i en IKT-infrastruktur, der det ofte er krav om nedetid på mindre enn 0,05 prosent.

Betalinger som benytter mobilt bredbånd, for eksempel billettsalg på busser eller oppgjør for drosjetransport, vil ikke fungere i slike situasjoner. Manglende tilgjengelighet, som nevnt ovenfor, vil kunne være uforenlig med visse mobile tjenester, som for eksempel helsetjenester. Men målinger viser at mobilleverandørene feiler uavhengig av hverandre. De er svært sjeldent (0,02 prosent) nede samtidig. Det vil si at det er stort potensial for økt robusthet hvis man kan bruke flere operatørers nett. For bruk som forutsetter høy tilgjengelighet, kan det være tjenlig å tilby ett abonnement som benytter alle nett. Laboratorieforsøk viser at dette er fullt mulig rent teknisk. Etter det Finanstilsynet kjenner til, eksisterer det ikke et slikt tilbud i dag.

[5] NorNet er en nasjonal infrastruktur for eksperimentell nettverksforskning finansiert av Forskningsrådet.

2.3 Teleleveranser i Norge

Finanssektoren er helt avhengig av teletjenester for den delen av virksomheten som i dag er tilnærmet 100 prosent basert på digitale løsninger og datakommunikasjon. Dette gjelder innenfor det enkelte finansforetak, mellom finansforetak og IKT-leverandører og med leverandører og samarbeidspartnere utenfor Norge.

Dersom telekommunikasjonen svikter, vil dette merkes umiddelbart siden banktjenestene i dagens løsninger i stor grad går helt ut til kundebetjeningspunkter. Dette gjelder i finansforetakenes egne filialnett, minibanker som er plassert i banken eller på offentlige plasser, EFT/POS-systemer[6] på brukersteder (butikker mv.), og tjenester som distribueres via Internett og telefoni til der kunden er.

Det er få leverandører av landbasert infrastruktur via kopper eller fiberoptisk kabling. I praksis er det kun Telenor, Ventelo, TeliaSonera og noen mindre lokale operatører som er leverandører på dette området. De fleste kommunikasjonsløsningene i Norge vil i et eller annet ledd være avhengig av at denne fysiske infrastrukturen fungerer.

Gjennom hendelsesrapportering til Finanstilsynet er tilsynet kjent med at det stadig oppstår hendelser som bryter kommunikasjonsforbindelser selv om kommunikasjonen var ment å være sikret med reserveløsninger. Det viser seg ofte at en teleleverandør som selv ikke leverer selve kablingen, kjøper denne av andre, og at topografien er slik at to ulike leverandører benytter samme fysiske kabel.

Det er vanskelig for finansforetakene å unngå dette siden leverandørene av det fysiske nettet av ulike grunner ikke synliggjør topografien. En løsning for finansforetaket kan da være å be teleleverandøren bekrefte at den aktuelle leveransen er redundant.[7]

Når det gjelder finansforetakenes kommunikasjon med kundene, skjer det en gradvis overgang fra tradisjonelle faste linjer til trådløs kommunikasjon. Kundens enhet er ofte en portabel enhet knyttet opp via trådløs kommunikasjon til et fastnett eller direkte via 3G mobilnett. Det pågår også en gradvis overgang til IP-kommunikasjon gjennom et datanettverk som Internett. Utviklingen gjør kommunikasjonsleddet mer komplekst og sammensatt, og vanskelig for den enkelte sluttbruker å ha kontroll med.

Det er problemstillinger knyttet til tilgjengelighet, konfidensialitet og integritet ved bruk av dagens teleløsninger. I 2011 oppsto en rekke alvorlige tilgjengelighetsproblemer på kommunikasjonsområdet i Norge, for eksempel under uværet i desember 2011. Sammen med problemer som oppsto i IKT-

[6] EFT/POS electronic funds transfer – point of sale
[7] Redundant – Redundans bygges ofte inn i systemer som krever høy pålitelighet. I datasystemer kan to eller flere datamaskiner jobbe parallelt med samme oppgaver og speile hverandre, slik at dersom en av dem skulle gå ned, så kan den andre ta over.

leverandørenes stamnett, har dette blitt et område som krever mer oppmerksomhet for å sikre akseptabel operasjonell risiko og tilgjengelighet.

2.4 Tjenesteutvikling i betalingssystemer

2.4.1 Nettbank på mobil

Sikker bruk av banktjenester på Internett krever at følgende klassiske sikringselementene er ivaretatt:

- Autentisering: hvem er jeg?
- Autorisasjon: har jeg rettighet til å gjøre dette?
- Ekthetsbevis: sporbarhet, ikke-benekting
- Konfidensialitet: ingen uvedkommende kan avlese informasjon
- Integritet: ingen ting kan endres ubemerket
- Tilgjengelighet: vissheten om at kommunikasjon mellom to eller flere parter faktisk er mulig

Før mobilteknologien ble allment tilgjengelig, var nettbank i nettleser på pc-teknologi (Windows eller gjerne en Unix/Linux-variant) eller Mac den vanlige brukte applikasjonen. Teknologien har vært kjent i mange år, og svakheter og sårbarheter er gradvis luket ut. Med oppgradert operativsystem, virusbeskyttelse og brannmurer samt oppgraderte nettlesere, ser man få eller ingen tap forårsaket av sikkerhetssvikt i selve nettbankapplikasjonene. Dette fritar ikke brukerne fra å utvise egen aktsomhet i bruken av nettbanken. Det advares mot å gjennomføre sensitive transaksjoner i åpne trådløse offentlige nett (Wi-Fi hotspots).

Et første skritt i å gjøre banktjenester på Internett mobile, var å gjøre BankID tilgjengelig på mobiltelefon. Her er brukerens private nøkkel lagret på SIM-kortet. For øvrig brukes nettbank i nettleser som før, forutsatt at nettbanken tilbyr innlogging med mobil.

SIM-kort utstedes av mobiloperatørene. BankID på mobil tilbys fra flere operatører. Det viser seg at med stadig mer avanserte komponenter, 3G- og 4G-teknologi, SIM-kortenes økte lagringskapasitet og programmerbarhet, og smarttelefoner og nettbrett – som også kan være mobiltelefoner, blir det stadig vanskeligere å levere et konsistent produkt. Det som virket på én mobiltelefonmodell, virker ikke nødvendigvis på en annen.

Utviklingen av mobilteknologien og markedsutviklingen med stadig mer sofistikert utstyr, fører til at internettapplikasjoner flytter fra den tradisjonelle pc-en og ut på mobilutstyr som smarttelefoner og nettbrett – iPad og andre typer. Dette utstyret leveres med egne operativsystemer (OS) for å styre de mange funksjonene og programmene på utstyret. I dag er det følgende tre operativsystemer som har vunnet fram i markedet:

- iOS for Apples utstyr (iPad, iPhone, og iPod Touch)
- Android, et Linux-basert OS, eid av Google, for smarttelefoner og nettbrett
- Windows Phone, en videreutvikling av Windows Mobile fra Microsoft, for smarttelefoner og nettbrett

Det finnes også andre OS-er i markedet, men med mindre markedsandeler:

- BlackBerry OS for BlackBerry smarttelefoner
- Symbian OS – tidligere mye brukt på blant annet Nokia smarttelefoner
- Palm OS for smarttelefoner
- Bada OS fra Samsung for deres smarttelefoner

Mobilutstyr som smarttelefoner og nettbrett har vanligvis en eller flere nettlesere tilgjengelig, men de er ofte av en annen oppbygning enn tilsvarende på pc. Ofte er nettleserne nedskalerte versjoner av pc-utgavene; Opera har Opera Mini og Opera mobil, Dolphin er laget spesielt for mobilverdenen osv. Mobil-utstyr har vanligvis ikke antivirusprogrammer og brannmurer i den form som er kjent fra pc-verdenen. Hvilke sikkerhetsrisikoer som kan ligge i en enkelt nettleser på en mobilenhet, synes i mindre grad å være avklart.

Om nettbanken kan kjøre på en nettleser på et mobilutstyr, er avhengig av om kombinasjonen av utstyr og nettleser tilbyr et kjøremiljø med en sikkerhet som aksepteres av den enkelte nettbank. Tofaktor-autentisering (2FA) kan oppnås både med kodekort og mobil BankID, hvor mobilen kan være utstyret selv eller en separat mobiltelefon. Mange banker har egne nettbankapplikasjoner for mobilutstyr og nettleser, som nås ved å skrive «m.bankensnavn.no», eller «mobil.bankensnavn.no» i nettleserens URL-felt.

2.4.2 Mobilbank på «app»

Markedsutviklingen for smarttelefoner og nettbrett, med stadig mer avanserte muligheter og en svært stor markedsutbredelse, har åpnet et helt nytt marked for programutvikling. Små applikasjoner kan lastes ned fra Internett til mobilutstyret, enten gratis eller for en meget lav pris. Applikasjonene, eller «apper», kan løse de forskjelligste oppgaver, fra spill og underholdning til forretningstransaksjoner og banktjenester. Banker har åpenbart ment at de må være i dette markedet, og har utviklet mobilbank-apper for de ulike segmentene. iPhone, iPad, Android smarttelefoner og nettbrett og Windows Phone er kommende konkurrenter i det samme markedet.

Noen eksempler på mobilbank-apper som er i markedet i dag:

Figur 1: iPhone-app fra DnB

Figur 2: Android-app fra Nordea

Figur 3: Windows Phone 7-app fra SpareBank 1

Figur 4: iPad-app fra Fokus Bank

En interessant app er en kodebrikke-app fra Encap som tilbys av blant annet Storebrand Bank som erstatning for den tradisjonelle kodebrikken (for eksempel DigiPass fra Vasco). Kodebrikke-appen er uavhengig av teleleverandør, men krever tilgang til bredbåndkommunikasjon. Appen aktiveres med en selvvalgt PIN-kode på samme måte som BankID på mobil.

Den raske utviklingen på dette feltet, fører til at man ikke har oversikt over hvilke risikoelementer som kan være til stede i dette sammensatte «miljøet» av SIM-teknologi, maskinvare, operativsystem, bank-apper, andre applikasjoner på utstyret, kommunikasjon (Wi-Fi eller mobilt) og brukerinteraksjon. Datatilsynet peker på at det er flere hundre tusen apper tilgjengelig fra ulike «app-butikker». Appene

håndterer store mengder personopplysninger om brukerne, ofte uten at brukerne selv er klar over det. Det synes opplagt at når apper kan lastes ned gratis, må det ligge andre forhold bak som gjør dette til en lønnsom forretning. Det er nærliggende å tro at «tappet» informasjon kan være handelsvare. Om dette markedet er legalt eller ikke, er et åpent spørsmål. Datatilsynet har lagt vekt på personvernet og hvordan appen håndterer personopplysninger. Datatilsynet er opptatt av at app-leverandøren skal legge ut informasjon om hvordan appen håndterer persondata. Tilsynets rapport viser tydelig at det kan være flere sider ved utbredelsen av apper som bør kartlegges og risikovurderes i tillegg til personvernet.[8]

BankID Norge planlegger å utgi sin egen app for BankID. Med BankID-appen vil kundene kunne bruke BankID slik de er vant til på pc-en. Målet er å lage en app som har samme funksjonalitet som BankID på pc. Første app-versjon vil gjøre det mulig å logge på i nettbankene og handle på nett med mobile enheter. Senere vil man også kunne signere dokumenter (publisert 3.2.2012 på BankIDs nettsider).

Det er all mulig grunn for bankene til å ha denne utviklingen under observasjon og utøve sitt ansvar for sikkerheten i hele transaksjonskjeden når kundene bruker nettbank-tjenester på mobile enheter.

2.4.3 Skyggetjenester på Internett

2.4.3.1 Bitcoin

Bitcoin[9] er en digital valuta opprettet i 2009. Navnet på valutaen refererer også til «open source»-programmet Bitcoin som brukes for å sende penger. Maksgrensen på antall bitcoins som kan være i omløp, er satt på 21 millioner. Det er altså en statisk valuta etter at alle bitcoins er delt ut. Bitcoin er basert på person to person-teknologi (P2P), og opererer uten noen form for sentral server eller mellommenn. Alle betalinger verifiseres automatisk gjennom noder i P2P-nettverket, og systemet er bygd opp slik at man ikke kan opprette flere penger eller stjele andres. Dette sikres gjennom en «blockchain» som lagres av alle nodene i nettverket.

Bitcoin kan gjerne sammenlignes med «Monopolpenger» hvor den enkelte aktør kjøper virtuelle pengeverdier kalt bitcoin for å gjøre kommersielle transaksjoner i et lukket handelsmiljø. Likviditet i «reelle» penger må alltid ligge til disposisjon dersom aktørene ønsker å veksle fra bitcoins til for eksempel US dollar eller euro. Foreløpig foregår denne virksomheten utenfor kontroll av myndighetene, og risikoen er ukjent.

Systemet er virtuelt og amerikanske myndigheter har signalisert at de ønsker å fjerne dette systemet før godtroende brukere blir for mye involvert. For at et slikt system skal kunne fungere, må det ha en «rik» sponsor.

[8] Datatilsynets rapport *Hva vet appen om deg? Kartlegging av personvernutfordringer knyttet til mobilapplikasjoner*, september 2011: http://www.datatilsynet.no/Global/04_veiledere/app_rapport_DT2011.pdf
[9] http://bitcoin.org/

2.4.3.2 Mikrolån/SMS-lån

Flere foretak tilbyr nå kunder å kunne ta opp mikro- eller sms-lån. Dette er ofte mindre lånebeløp på for eksempel 1000–3000 kroner. Lånets løpetid er som regel 30 dager og renteregnes ikke, men det tillegges en fast avgift. Et lån på for eksempel 3000 kroner, gir en fast avgift på 565 kroner, og renten vil da utgjøre 18,8 prosent per måned.

2.4.3.3 Elektronisk lommebok

Elektronisk lommebok er en form for elektronisk betalingssystem som flere land prøver ut. Kjøperen overfører beløp fra sin bankkonto til et elektronisk kort, ved en spesiell terminal eller ved egen datamaskin. Kjøpsbeløpet overføres fra kortet til en egen «elektronisk saldo» i butikken. Elektronisk saldo behøver ikke tømmes ved hver transaksjon, men summeres over tid og overfører beløp til bank etter fastlagte rutiner.

Fordelene ved elektronisk lommebok sammenlignet med bankkort er at bankenes systemer belastes mindre, at det ikke etterlates spor som knytter kunden til en bestemt transaksjon (som for kontanter) og at det kan brukes i situasjoner der bankkortsystemets identifiseringsprosess kan være mindre egnet (som ved kollektivreiser). På den annen side må det stilles store krav både til kortet, som må inneholde en egen prosessor og et sikrere lagringsmedium enn bankkortenes magnetiske stripe, samt til butikkterminalen som ikke må kunne tømmes av uvedkommende og heller ikke miste penger ved strømbrudd.

2.5 Bruk av sosiale medier

Bruk av sosiale medier har økt sterkt de siste årene. Fordeler, som informasjonsdeling og effektiv samhandling og kommunikasjon har gjort at mange finansforetak har tatt sosiale medier i bruk, både internt og i sin kundedialog.

Ved bruk av sosiale medier kan grensen mellom det private og det profesjonelle være utydelig. Ubevisst eller ufornuftig bruk kan eksempelvis føre til at uvedkommende kan skaffe seg informasjon om både ansatte og virksomheten ved å sette sammen informasjon. Den ansattes bruk av sosiale medier i jobbsammenheng kan innebære en risiko som forutsetter at arbeidsgiver etablerer retningslinjer og rutiner for oppfølging.

2.6 Utkontraktering

2.6.1 Offshoring

Viktige begrunnelser for at foretak utkontrakterer IKT-tjenester er økonomiske og ressursmessige innsparinger, at det øker foretakenes fleksibilitet. Høye kostnader og/eller mangel på ressurser i Norge resulterer ofte i kjøp av IKT-løsninger og -tjenester utenfor Norge. Dette har ført til prispress på leverandører i Norge. Det er viktig at forventningene klargjøres mest mulig hos begge parter slik at avtalen reflekterer kundens forventninger til funksjonalitet, kvalitet og sikkerhet.

Utkontraktering, og spesielt til leverandører utenfor Norge (offshoring), gir fleksibilitet til å kjøpe tjenester ved behov og å avslutte tjenesten når behovet opphører.

Identifisering og behandling av risiko er viktig ved utkontraktering. Det kan være en utfordring å sikre at leverandøren har de ressursene og kvalitetene som er nødvendig for å kunne levere etter avtalen.

Andre utfordringer er regelverks- og rettsrisiko man får ved å flytte IKT-tjenester til land som man ikke har inngående kjennskap til. Tjenestekjøper kan ikke forutsette at tjenesteleverandøren har kunnskap om ulikheter i de nasjonale regelverkene. Det er kjøper av tjenesten som må identifisere de ulike risikoene og sammen med leverandøren iverksette tiltak for å oppnå et tilstrekkelig lavt risikonivå.

Flere land som er mye benyttet til offshoring av tjenester, er mye mindre lovregulert enn Norge. Dette gjelder for eksempel innen personvern. Mangel på lovregulering bør kompenseres ved at tilsvarende bestemmelser tas inn i avtalen med den eksterne leverandøren. Men samtidig blir det rapportert at de samme landene i begrenset grad evner å håndheve avtalebestemmelser. Se mer om dette på nettstedet www.doingbusiness.org/rankings, der for eksempel India rangeres som nummer 182 av 183 når det gjelder å håndheve avtalebestemmelser. I enkelte offshore-land kan det også være tradisjon for å favorisere kunder som er villige til å gi oppgjør i utradisjonelle former. Dette kan gå ut over leveransen til kunder som ikke er villig til dette.

2.6.2 Cloud computing

Begrepet «cloud computing» benyttes ofte om leveranse av en service fra nettet, for eksempel systemer for ekstern lagring av data. Det har fått stor oppmerksomhet og er en variant av utkontrakterte tjenester. Ut fra tilgjengelig litteratur og undersøkelser ser man at de største risikoene for både leverandører og kjøpere av cloud computing-tjenester er knyttet til sikkerhetsbrudd, styring og kontroll. Også når det gjelder cloud computing er det avgjørende å ivareta behovet for konfidensialitet, integritet og tilgjengelighet.

Leverandører av cloud computing har ofte infrastruktur tilgjengelig som kan konkurrere med tradisjonell utkontraktering i både pris og ytelse. Men den samme infrastrukturen kan føre til at data forlater kundens hjemland, at data blir borte og at kjøperen av cloud computing-tjenesten ikke har

kontroll over hvor dataene er eller hvem som har tilgang til disse.

Cloud computing i sin nåværende form er ikke tilpasset slik at det er særlig aktuelt for finansinstitusjoner å ta i bruk denne tjenesten for løsninger som er av betydning for institusjonen, som kunde- og reskontroforhold. For at cloud computing skal kunne benyttes for viktige deler av finanssektorens løsninger, må det foretas en avklaring av styring og kontroll, transparens når det gjelder hvor data blir lagret, hvem som har tilgang, oversikt og kontroll med infrastruktur, intern kontroll, revisjon og tilsyn.

India har de siste 20 årene opplevd en eventyrlig vekst i sin IT-industri. Alle de større IT-selskapene har etablert seg der med egne kontorer eller har inngått partnerskap med indiske selskaper. Også tjenesteleverandører i India er nå under press på pris og kvalitet. Nye land konkurrerer om kundene. For eksempel har land i Øst-Europa i dag lavere kostnadsnivå enn det som er i deler av India. En trend er også at leverandørene i større grad ønsker å komme lenger opp i verdikjeden hos kundene ved å ta over driften og vedlikeholdet av kundenes forretningsprosesser.

2.7 Internettkriminalitet

Norske nettbanker ble utsatt for angrep i økende grad fra ulike nettbank-trojanere i løpet av 2011. Mottiltak fra bankene resulterte i minimale tap. Samme trend ser man i andre land, men med varierende tapstall. Nederlandske banker hadde i 2010 ti ganger så store tap fra trojanerangrep som i 2009, og antallet angrep ble doblet fra 2010 til 2011. Trojanerangrepene utvikler seg til å bli mer automatisert ved at det er lagt mer logikk inn i programmene. Transaksjoner kan genereres uten bruk av et «on-site» overvåkings- og kommandosenter. Utviklingen er urovekkende fordi det åpner for massegenerering av transaksjoner i et omfang man hittil ikke har sett. «Phishing»[10] er en del av konseptet. Phishing benyttes i stadig nye scenarier. Fellesnevner er at den som blir avlurt informasjon, taper verdier og/eller kan bli mistenkt som skyldig i et svindelscenario når den frastålne informasjonen blir benyttet som betaling i ulike situasjoner iscenesatt av svindleren.

E-post brukes til å rekruttere «mules» (muldyr) som kan stille kontoen til disposisjon som mottakerkonto ved nettbankangrep. Henvendelsen blir gjerne kamuflert som rekruttering til en lukrativ stilling i et internasjonalt selskap. Den som avgir kontoopplysninger, gjør det kanskje i god tro og kan forbli uvitende om at kontoen benyttes som transittkonto for nettbanksvindel.

Phishing i en rekke ulike varianter brukes til å be om kredittkortinformasjon via e-post der avsender oppgis å være din bankforbindelse, kortselskap eller lignende. I et eksempel fra utlandet hadde svindleren opprettet et reisebyrå. Kredittkortinformasjon han hadde phishet, ble blant annet brukt til å

[10] «Phishing» vil si å avlure informasjon gjennom ulike former for henvendelser mot enkeltpersoner. Eksempel på dette er å be om informasjon i en annens navn.

kjøpe dyre reiser til eksotiske reisemål. Svindleren,solgte reisene raskt videre fra sitt eget reisebyrå, men nå med kampanjepriser som ble betalt til «phisheren» gjennom Western Union.

Et annet eksempel er at «phishet» kredittkortinformasjon blir brukt til å kjøpe annonseplass i en nettbutikk der fiktive varer blir solgt mot forhåndsbetaling. Det er en form for ID-tyveri der rettmessig eier av kredittkortet blir stående som skyldig når varen ikke blir levert.

I andre land i Europa har man sett svindel med SIM-kort der mobiltelefonen brukes til to-kanal pålogging til nettbank. Svakheter knyttet til krav til autentisering ved bestilling av nytt SIM-kort blir utnyttet. Svindlere bestiller nytt SIM-kort i telefoneierens navn. I en kort periode virker både nytt og gammelt SIM-kort, og dette er den tiden svindlerne trenger til å angripe nettbanken. I Nederland er det inngått et samarbeid mellom mobiltelefonleverandører og banker om informasjonsutveksling når mobilkunder ber om nytt SIM-kort.

I 2011 var det et massivt DDOS[11]-angrep mot Rabobank i Nederland. Angrepet varierte i styrke og varte i til sammen mer enn tre uker.

2.8 Identitetstyveri

Finanstilsynet bruker begrepet identitetstyveri der noen på uærlig vis har tilegnet seg personrelatert informasjon som misbrukes med for å oppnå urettmessig økonomiske gevinster eller andre fordeler uten den rettmessige eiers kjennskap.

ID-tyveri omfatter for eksempel «skimming» av kortinformasjon fra kortbruk i minibanker og EFT/POS-butikksystemer, hoteller, restauranter m.m. Kopiering av informasjon fra kortinnsamlingssentraler har foreløpig i større omfang kun skjedd internasjonalt. I tillegg omfatter det kopiering og misbruk av informasjon fra annen brukers pc, særlig bruk av nettbank.

Problemområdet kan deles inn i en innsamlingsfase, hvor datainnsamling om en person skjer målrettet, og en angrepsfase, hvor informasjonselementer som er samlet inn settes sammen for å utføre et målrettet angrep.

Det er i Norge også kjent at data/informasjon fra ID-tyveri er benyttet som elementer i større angrep, hvor både utro tjener og bruk av data fra ID-tyveri inngår i de kriminelle handlingene som har ført til store tap.

Internasjonale kilder rapporterer at ID-tyveri er et økende problem. Særlig den engelsktalende del av

[11] Distributed Denial-of-Service Attacks betyr i praksis å sende digitale forespørsler til et nettsted i et omfang som bryter ned systemet.

verden ser foreløpig ut til å være mest utsatt. I USA er ID-tyveri allerede et betydelig og økende økonomisk samfunnsproblem.

ID-tyveri som kriminalitetsform har også kommet til Norge, og for de som blir utsatt for dette, er det et alvorlig problem. Det finnes lite formell statistikk på dette området, men det er grunn til å tro at problemet er økende, og belastningen for den som utsettes for ID-tyveri er forskjellig.

For finanssektoren og myndighetene er det viktig å følge utviklingen nøye og arbeide med å finne fram til effektive mottiltak før ID-tyveri blir for omfattende og får økte negative effekter på områdene som er angitt ovenfor. Innenfor finanssektoren skjer det allerede et viktig samarbeid på dette området både gjennom bransjeorganisasjonene og med enkeltinstitusjoner. Finanstilsynet har også et nært samarbeid med Datatilsynet og andre relevante myndigheter.

2.9 Interne misligheter

Interne misligheter kan være utro tjenere og svake kontrollsystemer. Informasjonen som Finanstilsynet har fra Norge og internasjonalt tilsier at interne misligheter i finansinstitusjoner er et økende problem. Finanstilsynet antar at det er en underrapportering av slike misligheter, særlig når de fører til begrensede tap. Derimot ser det ut til at saker som fører til større tap, blir anmeldt til politiet og rapportert til tilsynet.

Den generelle globaliseringen med større arbeidstakermobilitet kan være en grunn til at det er vanskeligere å kjenne sine ansatte tilstrekkelig. Det er heller ikke usannsynlig at kriminelle grupper kjenner til personer fra sitt miljø som er ansatt i finansforetak og som på ulik måte kan presse den ansatte til å delta i kriminelle handlinger. Det er grunn til å tro at det i perioder pågår aktiviteter for å få ansatt personer som senere skal bidra til kriminelle handlinger.

Det er særlig bekymringsfullt om en ansatt (utro tjener internt) i et finansforetak inngår i et internasjonalt organisert digitalt angrep mot betalingstjenester, for eksempel på området nettbank, noe som kan medføre store tap.

Det er viktig at finanssektoren har oppmerksomheten rettet mot dette problemet framover, særlig gjelder dette for bankene. Gode rutiner ved ansettelser og effektiv kontroll med tilgangsrettigheter er viktige tiltaksområder for å avgrense dette problemet som ser ut til å være økende.

2.10 Verdipapirområdet

2.10.1 Felles oppgjørsregler i EØS-området

I EU arbeides det med et felles europeisk oppgjørssystem omtalt som TARGET2-Securities (T2S). Arbeidet ledes av Den europeiske sentralbanken (ECB), og målet er å sentralisere avregning og oppgjør av verdipapirtransaksjoner for å oppnå et større felles marked og bedre mulighet for å oppnå høyere effektivitet, lavere transaksjonskostnader og bedre sikkerhet. T2S skal dekke verdipapirtransaksjoner i alle valutatyper innenfor EØS. Det er ikke bestemt når eller om Norge vil knytte seg til T2S.

Det pågår også endringsprosesser som i stor grad er markedsdrevet når det gjelder etablering av nye markedsplasser og teknologibaserte løsninger på handel og investorenes tilknytning til markedet.

Summen av de ulike prosessene i EU på finansområdet krever endringer og tilpasninger som kan gi risiko som det er viktig at finanssektoren har evne til å håndtere. Betydningen for verdipapirregisterrollen i Verdipapirsentralen ASA (VPS) er ikke klarlagt.

2.10.2 Maskinhandel

Markedsaktører kan oppnå store gevinster ved hjelp av programmerte algoritmer som automatisk foretar handler basert på bestemte markedssignaler og er grunnlaget for såkalt høyfrekvenshandel (High-frequency trading – HFT). Databasert aksjehandel utgjør en stadig større andel av handelen i aksjemarkeder verden over. I Sverige står HFT for ca. 10–20 prosent av børsens omsetning, og på de amerikanske børsene står den for ca. 60 prosent.

Mange mener HFT tilfører likviditet til markedet, reduserer personalkostnadene og øker konkurransen mellom børsene. Andre peker på risikoen for at HFT driver markedet i stedet for å følge det, og at HFT skaper «støy» for investorer som ønsker å investere basert på selskapenes substansverdi, noe som kan redusere likviditeten.

For raskest mulig å kunne utnytte en mulighet i markedet, er det viktig at datamaskinene som drifter HFT er plassert nær børsen. Helst må de være samlokalisert med børsen. Bare de største har råd til dette. En viktig gruppe av mindre aktører vil dermed kunne bli presset ut av markedet.

Det er blitt hevdet at HFT kan gjøre markedet ustabilt av flere grunner. Algoritmene tenderer mot å være temmelig like, slik at de forsterker hverandre. Mange av dem vil selge eller kjøpe samme aksje samtidig, og dette kan skape store, uforutsette svingninger. Videre kan feilprogrammerte maskiner trigge andre maskiner til å selge og kjøpe aksjer, noe som øker risikoen for store svingninger. Det såkalte flash crash i New York 6. mai 2010 der Dow Jones-indeksen falt 9 prosent på 10 minutter, er forklart med at et dataprogram overreagerte på et markedssignal. Et annet eksempel er løsningene til et sveitsisk høyfrekvensfirma notert på Stockholmsbørsen, som plasserte automatisk en stor salgsordre og oppdaterte prisgrensen mange ganger for å matche kjøpsordre og dermed drev prisen ned til et uvanlig

lavt nivå.

Europeiske børser har fattet en felles beslutning om å samordne den minste mulige prisdifferansen mellom to ordrer, såkalt tick size, i en ordrebok på de europeiske markedene nettopp for å øke likviditeten i handelen og minske transaksjonskostnadene. Dette har gjort det billigere å gå ut og inn av en posisjon og mer attraktivt for HFT-handlere siden det lettere oppstår prisdifferanser mellom markedsplasser, og at det er billigere å gjennomføre kjøp og salg.

HFT er et relativt nytt fenomen og under stadig endring og utvikling. Risikoen og konsekvensene forbundet med HFT er ikke fullt ut analysert. Finanstilsynet vil følge utviklingen.

3 Systemer for betalingstjenester

3.1 Generelt om betalingssystemer

Betalingssystemene er sentrale for all økonomisk aktivitet. All handel med kommersielle eller finansielle produkter resulterer i et avtalt pengemessig oppgjør. I Norge reguleres betalingssystemene gjennom lover og forskrifter og gjennom finansnæringens selvregulering som blir forvaltet av Finansnæringens Fellesorganisasjon (FNO).

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

I 2011 formidlet norske betalingssystemer ca. 2 milliarder transaksjoner (giro og kort). Over 95 prosent av betalingene skjer elektronisk i en digitalisert sømløs transaksjonskjede mellom to samhandlende parter. Kun 1,1 prosent av betalingene utføres via papirbaserte blanketter.

Personkunders bruk av nettbank utgjør 59 prosent av alle betalingstransaksjoner. Det utgjør 13,4 prosent av volumene i milliarder kroner som blir overført. Bedriftskundenes bruk utgjør 41 prosent av antall transaksjoner, hvilket står for 86 prosent av verdiene (beløpet).

For kortbetalinger har BankAxept 87 prosent av privatmarkedet målt i verdi. Norge er i verdenstoppen når det gjelder bruk av betalingskort.

En stor del av den elektroniske infrastrukturen som betalingssystemene anvender operasjonelt, er utkontraktert til IKT-leverandører. De konsesjonspliktige foretakenes ansvar berøres ikke av utkontrakteringen. Det er viktig å sikre at alle elementer og aktører i hele transaksjonskjeden mellom betaler og betalingsmottaker inngår i styringen av operasjonell risiko. Det er viktig å sikre nødvendig kompetanse og tid til fullt ut å kunne styre og kontrollere det driftsmessige forholdet både til egne operasjonelle ressurser og til IT-leverandører med eventuelle underleverandører. Finanstilsynet tok denne problemstillingen opp i rundskriv 20/2011.

Rammebetingelsene for betalingssystemer i Norge påvirkes av harmonisering innen EØS. Betalingstjenestedirektivet er fullt ut implementert i norsk lovgivning. 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 etablering av betalingsforetak.

I Norges Banks *Årsrapport om betalingssystem 2011* er det mer informasjon og statistiske data om dette feltet.

3.2 Risiko og sårbarhet i betalingssystemene

Transaksjonskjedene utvides, og kompleksiteten øker med nye elektroniske tjenester, nye grensesnitt og flere underleverandører som samarbeider. Dette kan medføre økt risiko for feil.

Gjennom Finanstilsynets system for hendelsesrapportering blir det innmeldt alvorlige hendelser i betalingssystemene. Se nærmere omtale i punkt 4.3.

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.

I Norge er det et lite antall operatører av kjernesystemer for banker og finansforetak. Dette kan representere en ikke ubetydelig konsentrasjonsrisiko, men kan også bidra til bedre styring og kontroll.

Etablerte beredskapsløsninger for betalingssystemene er viktig for å forebygge uønskede 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 beslutter og fastsetter norske meldingsstandarder og forpliktende sikkerhetskrav som skal anvendes i betalingstjenestene. De fleste kontraktørene i markedet følger dessuten kortselskapenes internasjonale sikkerhetsstandard PCI DSS, som stiller krav til blant annet brukerstedene. Standarden krever at man minst en gang i året evaluerer og sjekker at kravene etterleves.

Risiko for kriminelle angrep er foreløpig størst i grensesnittene mellom kunde og bank. Dette gjelder både svindel med betalingskort og angrep mot nettbanken.

3.3 Styring og kontroll med betalingssystemene

Systemer for betalingsformidling og betalingstjenester utgjør en vesentlig del av samfunnets kritiske infrastruktur og funksjoner.

Styring og kontroll av IKT-virksomheten relatert til betalingsformidling må følgelig være en prioritert oppgave. Forretningssidens eierskap og involvering når det gjelder funksjonalitet, endringer, problemstillinger og risikoer er nødvendig. Det må stilles krav til struktur, orden, kvalitet 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. Store deler av IKT-virksomheten relatert til betalingsformidling i Norge er utkontraktert, og mye er utkontraktert til de samme leverandørene. Som omtalt tidligere representerer dette en konsentrasjonsrisiko hos driftsleverandørene av både IKT-drift og applikasjonsutvikling. Det er viktig at de enkelte finansforetakene samarbeider om tiltak for å sikre at konsentrasjonsrisikoen er akseptabel og vurdert i risikoanalysene.

Det kan være en utfordring å få effektuert sine krav overfor en stor IT-leverandør som i realiteten har få konkurrenter. I forbindelse med utkontraktering må foretaket sikre at de selv har tilstrekkelig kompetanse til å forvalte slike avtaler, og til å stille krav i forbindelse med utkontrakteringen. Det kan være utfordrende å stille krav til og følge opp en leverandør som er etablert utenfor Norge.

Ved enkelte tilsyn har Finanstilsynet registrert manglende kompetanse hos styrende organer og øverste ledelse i finansinstitusjoner. Dette gjelder både innen IT generelt, og utkontraktering spesielt. Dette kan gjøre det vanskelig å få en helhetlig oversikt over alle elementene i transaksjonskjeden.

Styring og kontroll av betalingssystemene er en vesentlig del av den totale styring og kontroll av foretakenes IKT-virksomhet.

3.3.1 Risiko knyttet til fellessystemer

I tillegg til de kravene som følger av lovverket, driver særlig bankene under en avtalt form for selvregulering. Denne selvreguleringen berører primært transaksjonsbanken og omfatter felles utviklede tjenester og systemer som anvendes av hele banksektoren for å kunne ha en effektiv transaksjonskjede. Dette utgjør en vesentlig del av den finansielle infrastruktur som i de senere årene er blitt mer kompleks.

Selvreguleringen er dokumentert i «Blåboka» og forvaltes av FNO. Regelverket er tilgjengelig på FNOs nettsted, http://www.fno.no/blaboka.

I 2011 utviklet FNO og Finanstilsynet i en felles prosess en mer grunnleggende forståelse for hvordan det operasjonelle risikobildet ser ut, og hvem som har det operasjonelle primæransvaret. Basert på dette har FNO oppdatert relevant dokumentasjon.

3.4 Oversikt over tap knyttet til betalingstjenester

Tabellene viser tap for de tre siste halve årene. Tallene er innhentet av FNO og Bankenes Standardiseringskontor (BSK) i samarbeid med Finanstilsynet.

Det er først og fremst bruk av betalingskort som står for større tap. Nedenfor er de ulike tapskategoriene kommentert.

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

Svindeltype betalingskort	2010 2. halvår	2011 1. halvår	2011 2. halvår
Misbruk av kortinformasjon, kort ikke til stede (internetthandel)	9 401	9 358	14 832
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort i Norge	1 765	97	371
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort utenfor Norge	31 740	24 890	32 450
Originalkort tapt eller stjålet, misbrukt med PIN i Norge	14 395	15 913	16 311
Originalkort tapt eller stjålet, misbrukt med PIN utenfor Norge	5 149	2 135	4 873
Originalkort tapt eller stjålet, misbrukt uten PIN	4 239	2 254	2 234
Totalt	**66 689**	**54 647**	**71 071**

Tap i kategorien «Misbruk av kortinformasjon, kort ikke til stede (internetthandel)» gjelder hovedsakelig datainnbrudd, men også phishing er en kilde til disse tapene.

Kategorien «Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort i Norge» ble sterkt redusert i 2011 i forhold til 2010. Sommeren og høsten 2010 var det flere tilfeller av skimming mot norske minibanker. Noe tilsvarende var det ikke i 2011. Norske betalingskort blir skimmet i utlandet, og informasjon i magnetstripa blir kopiert og benyttet til produksjon av falske kort. Skimming av norske betalingskort i utlandet innebærer oftest også avlesing av PIN-koden, og de falske kortene brukes sammen med PIN. Falske kort kan også brukes uten PIN til enkelte betalingstjenester som ikke krever PIN.

Når det gjelder skimming av kort i Norge og i utlandet ble de falske kortene nesten utelukkende benyttet i utlandet i 2011. POS-terminaler og minibanker i Norge krever chip på norske debetkort, og dette utelukker bruk av falske norske betalingskort med kun magnetstripe.

Den største årsaken til kategorien «Originalkort tapt eller stjålet, misbrukt med PIN i Norge» er lommetyveri og såkalt skuldersurfing. Personer følger med og avleser PIN-koden som brukeren taster

inn på betalingsterminal eller minibank og stjeler deretter kortet, eller at det skjer i omvendt rekkefølge; noen stjeler kortet og tvinger offeret til å avgi PIN-koden. I tillegg blir fortsatt også noen kort og PIN-koder borte i posten.

Tabell 2: Tap ved bruk av nettbank (tall i hele tusen kr)

Svindeltype nettbank	**2010 2. halvår**	**2011 1. halvår**	**2011 2. halvår**
Angrep ved bruk av ondartet programkode på kundens PC (trojaner)	0	658	6
Angrep som utnytter sårbarheter i nettbankapplikasjon (hacking)	0	0	0
Tapt/stålet sikkerhetsmekanisme	2 398	602	2 719
Totalt	**2 398**	**1 260**	**2 725**

Til tross for massive trojanerangrep mot norske nettbanker i 2011, er tapene små. Imidlertid er kostnadene knyttet til tiltak økt betydelig. Et større beløp er tapt som følge av at passord og engangskodekalkulator er stjålet. Spesielt i andre halvår 2011 var det enkelte større svindelsaker som gjorde utslag på dette tapsområdet.

4 Funn og observasjoner

4.1 Noen funn fra IT-tilsyn i 2011

4.1.1 Mangelfull leveranseevne hos IT-leverandør

Flere av foretakene som Finanstilsynet har gjennomført IT-tilsyn hos, har uttrykt at de ikke er tilfreds med leverandørens evne til å levere applikasjonsutvikling og -forvaltning. Ofte er det samme leverandør som drifter systemene og forvalter mange av applikasjonene. Foretakene er frustrert over manglende gjennomslag for ønske om ny funksjonalitet. Gjentakende forsinkelser og fravær av bidrag til analyser og kreativitet fra leverandøren stopper foretakenes ønske om innovasjon og nyutvikling av produkter. Mange foretak ser seg etter hvert om etter andre samarbeidspartnere.

4.1.2 Utilstrekkelig kontroll med hele transaksjonskjeder der det er flere aktører

De fleste finansforetak har utkontraktert driften av IT-løsningene, og mange har også utkontraktert applikasjonsutvikling og -forvaltning. Finanstilsynet har gjennom tilsyn sett at flere driftsmodeller har gjort det vanskeligere for foretakene å sikre kontroll med transaksjonskjeden. Betalingskort-transaksjoner og nettbanktransaksjoner passerer gjennom den norske betalingsinfrastrukturen som driftes av flere ulike leverandører. For å møte konkurransen fra andre aktører og redusere kostnader, velger de primære IT-leverandørene å utkontraktere deler av sine oppgaver til underleverandører.

4.1.3 Mangelfull styring og kontroll med det totale risikobildet

Å sammenfatte resultatene fra gjennomførte risikoanalyser viser seg å være en utfordring. Dette gjelder særlig i større foretak der risikoanalyser blir utført på ulike forretningsområder og nivåer i organisasjonen. Risikoanalysene framstår som løsrevede deler som ikke har noen knytning til hverandre eller reflekterer hverandre. I større organisasjoner er det ofte både en «bottom up»- og en «top down»-tilnærming til risikoanalysen. Det er ikke alltid resultatene fra disse blir sammenstilt.

Generelt kan det synes som om foretakene bør avsette mer tid og ressurser til gjennomføring av risikovurderinger. Å utarbeide gode risikovurderinger krever kompetanse og erfaring. Det er mange

veiledninger, men ingen fasit, som sier hvordan det skal gjøres i det enkelte tilfellet, hvilket nivå det skal ligge på og hvordan risikoer og tiltak skal dokumenteres og følges opp.

Det er viktig å gjennomføre risikovurderinger i forkant av større IT-endringer. Likeledes at det framkommer i risikovurderingen hvem som har ansvar for risikoreduserende tiltak.

Mange foretak har ikke etablert rutiner for å følge opp at IT-prosesser og -rutiner etterleves. For å sikre god internkontroll er det ikke bare nødvendig å ha gode og dokumenterte rutiner, men det må også sikres at disse blir fulgt.

Finanstilsynet har videre merket seg at enkelte foretak som har utkontraktert IKT-virksomhet, ikke har tilstrekkelig oversikt over leverandørens risikostyring og internkontroll. Dette kan skyldes mangelfulle avtaler, eller at det ikke er tilstrekkelig bemanning i foretaket til å stille krav, bestille og følge opp IT-leverandøren. Dette kan spesielt være en utfordring for små foretak som kjøper vesentlige deler av sin IKT-virksomhet, og som ikke har tilstrekkelig intern bemanning.

4.1.4 Krevende risikoanalyser ved utkontraktering av IT-oppgaver til lavkostland

Utkontraktering til lavkostland introduserer nye problemstillinger og risikoer det kan være vanskelig å kartlegge. Aktuelle land og regioner kan befinne seg langt borte med ukjent kultur, språk og lovgivning. Finansforetak baserer seg ofte på risikoanalyser utført av store IT-aktører som Gartner, Accenture og Capgemini som har etablert seg i aktuelle land, og på målinger som for eksempel viser landrisiko. Målinger utført av Transparency International eller Gartner gis ut i en liste over landenes korrupsjonsgrad. Det er viktig å analysere nærmere hva høy korrupsjonsgrad kan bety av risiko og eventuelt hvilke tiltak som kan være relevante for å håndtere dette forsvarlig. Noen få foretak gjør egne landanalyser. En aktuell problemstilling er å sikre at regelverket i landet der oppgavene utføres ikke er til hinder for etterlevelse av det norske regelverket og at risikoen er akseptabel.

Finanstilsynet ga i rundskriv 14/2010 retningslinjer for utkontraktering av IT-oppgaver i bankene til lavkostland. Generelt er det høy risiko forbundet med utflytting av oppgaver knyttet til drift av betalingstjenester og kjerneløsninger. Etter Finanstilsynets oppfatning er det en forutsetning at finansforetaket ikke utelukkende baserer seg på risikoanalyser utført av nevnte aktører, men gjør egne analyser.

4.1.5 Manglende testing av at reserveløsninger fungerer

Også IT-tilsyn gjennomført i 2011 avdekker mangelfull testing og verifisering av at kontinuitets- og katastrofeløsninger virker som forutsatt. Fortsatt er det mange som på grunn av manglende testing og verifisering ikke har sikret at reserveløsningen vil fungere i en avbruddssituasjon. Det virker som om enkelte finansforetak i større grad legger mer vekt på testing av kontinuitetsløsninger enn på katastrofeløsninger.

Kontinuitet blir ofte testet gjennom dupliserte løsninger som periodisk skifter mellom å være primær og sekundær produksjonslokasjon. Utfordringen er å teste alle ledd i transaksjonskjeden. I de ytterste leddene ser man fortsatt at reserveløsninger, for eksempel på nettverkssiden, ikke virker som forutsatt i en avbruddssituasjon. Test av kontinuitet omfatter også test av nettverk.

Katastrofeløsninger er komplekse å teste. Også her må alle ledd i transaksjonskjeden tas hensyn til. Foretakenes dokumentasjon fra gjennomførte katastrofetester viser hvor viktig slike tester er. Finanstilsynet vurderer tester som avgjørende for at katastrofeløsningen skal bli det reelle alternativet den er ment å være i en krisesituasjon.

4.2 Foretakenes egne vurderinger

For å få innblikk i finansforetakenes egne vurderinger av sin IKT-risiko, har Finanstilsynet hatt samtaler med fjorten finansforetak av ulik type og størrelse. Samtalene omhandlet erfarte problemer og utfordringer i 2011, og hva som vurderes å være de største risikoene i 2012 og som derfor vil få oppmerksomhet.

De største problemene/utfordringene i 2011:

- Hendelsen på kortområdet i påsken 2011 vurderes av de fleste bankene som det mest alvorlige problemet i 2011. I etterkant av hendelsen ble det iverksatt tiltak for å redusere sannsynligheten for at en slik hendelse skal skje på nytt og få så omfattende konsekvenser. Det opplyses blant annet at avtaler, grensesnitt og rutiner er gjennomgått og forbedret, i tillegg til den pålagte kartleggingen av kritiske komponenter.
- Mangelfull driftsstabilitet påpekes av flere av foretakene som en risiko og et erfart problem i 2011. Driftsleverandører tillegges mye av ansvaret i denne sammenheng.
- Mangelfull leveransekvalitet fra leverandørenes side, både på prosjekter og i forbindelse med daglig drift.
- Angrep på nettbanken med tilhørende tjenester. Få andre foretakstyper synes å ha erfart alvorlig nettkriminalitet.
- Stabilitet og tilgjengelighet i etterkant av store endringer er erfart å være en problemstilling i enkelte foretak.

Risikoområder i 2012:

- Driftskvalitet og -stabilitet på løsninger og infrastruktur
- Konfidensialitet og integritet i kundedata
- Nettkriminalitet
- Konsentrasjonsrisiko på fellesfunksjoner, som Norwegian Interbank Clearing System (NICS) og BankID

- Kvalitet på foretakenes egne leveranser og løsninger
- Kvalitet på leverandørenes tjenester og leveranser, samt oversikt over og kontroll med leverandørens risikoer og internkontroll
- Krav til kostnadseffektive løsninger, «time to market», og de konsekvensene dette kan få for IT-arbeid og IT-løsninger
- Nye tjenester og enheter (mobiltelefontjenester, nettbrettløsninger etc.)
- Ansattes bruk av sosiale medier
- Risiko for tilsiktet eller utilsiktet misbruk av data i forbindelse med økt bruk av konsulenter som er gitt tilganger for å kunne utføre sitt arbeid

Problemstillinger som gis oppmerksomhet i 2012:

- Tiltak mot nettkriminalitet, blant annet overvåking av nettverksbaserte tjenester
- Sikkerheten rundt selvbetjeningskanalene, inklusive mobile enheter
- Forbedrede prosesser og rutiner, blant annet endringshåndtering, kvalitetssikring, prosjektledelse, porteføljestyring og implementering
- Gjennomføre vurderinger av leverandører og sourcing-muligheter
- Forbedre risikoanalyser

4.3 Rapporterte hendelser i 2011

I 2011 var det flere alvorlige hendelser. I februar ble norske nettbanker rammet av et koordinert ondsinnet angrep fra trojanerkode. I påsken var det avbrudd i mange bankers kortautorisasjonstjeneste, slik at mange kortkunder fikk problemer med varebetalingen i butikker, samt at hendelsen fikk uheldige ettervirkninger for hva som ble oppfattet som disponibelt beløp på kontoer. Disse to hendelsene er beskrevet nærmere i punkt 4.4.1 og 4.4.2.

I juli var det avbrudd i BankID-tjenesten. Det varte i seks timer og lammet det meste av pålogging til norske nettbanker, samt andre tjenester hvor BankID blir brukt til autentisering. Minst rammet ble banker med en alternativ autentiseringsmekanisme tilgjengelig i sin nettbankportal.

Terroraksjonen 22. juli fikk liten innvirkning på finanssektoren. Noen bankkontorer og pensjonskasser i Oslo sentrum fikk materielle skader.

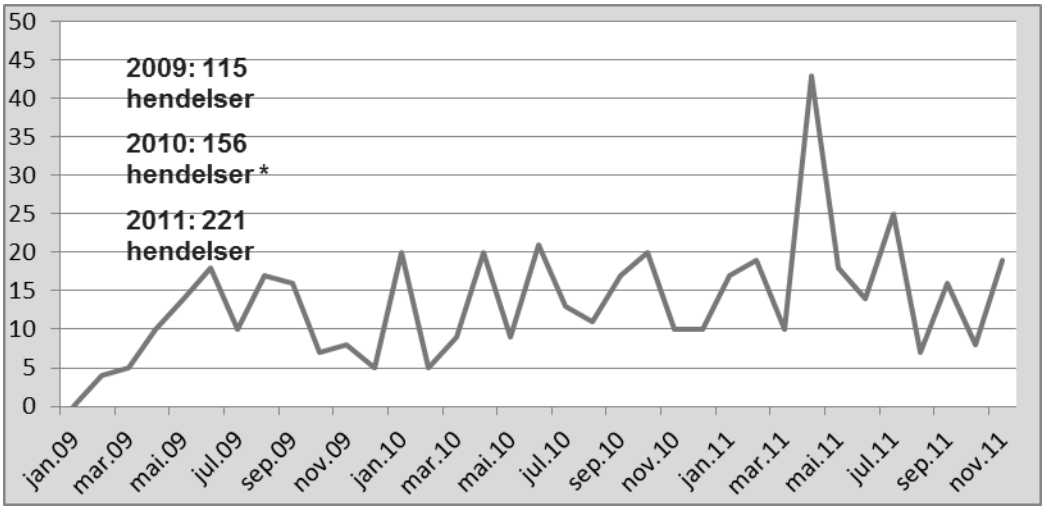
I september måtte Oslo Børs stenge handelen i vel tre timer på grunn av driftsproblemer hos børsens leverandør London Stock Exchange.

Brudd i tilgjengeligheten til norske nettbanker ser ut til å være omtrent på samme nivå som tidligere år. Finanstilsynet observerer at hvilke nettbanker som er mest rammet av driftsproblemer og avbrudd, varierer fra år til år. Årsaken kan være grad av oppmerksomhet fra felles leverandør eller delvis

utdaterte plattformer som krever stadig mer arbeid å holde oppdatert. Gjengangere blant feilårsaker er oppgradering av brannmurløsninger og sekundærløsninger. Bankene opplever det paradoksale i at de nettopp i sitt arbeid med å sikre kontinuitet i nettbanken, påfører avbrudd i tilgjengeligheten til nettbanken.

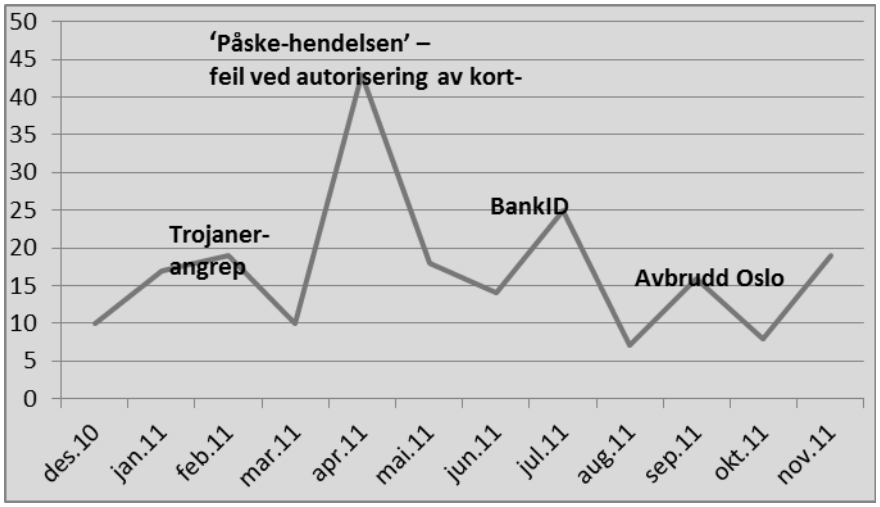
Finanstilsynet har mottatt flere meldinger om uønskede hendelser i 2011 enn tidligere, mye på grunn av hendelser som rammet mange finansforetak samtidig. Hendelsesrapporteringen er en vel etablert ordning. Banker og deres leverandører rapporterer raskt etter at en hendelse har oppstått. Andre typer finansforetak rapporterer i mindre grad.

Figur 6: Hendelser i perioden 2009–2011

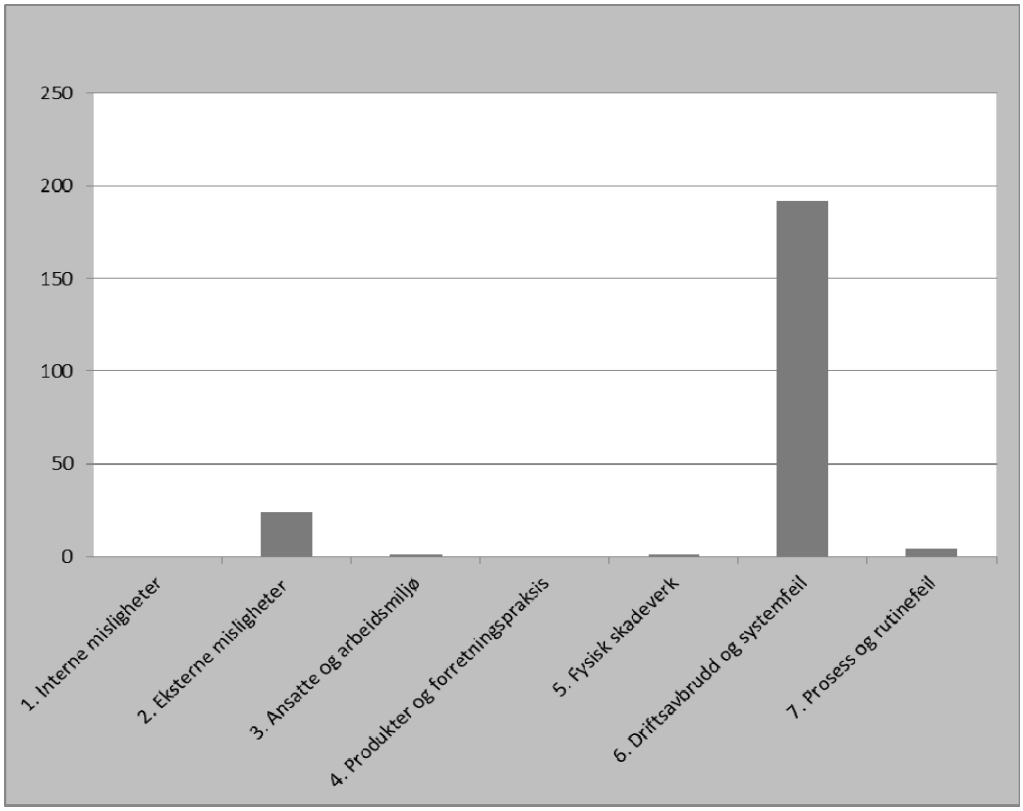


Hendelser rapportert i perioden januar 2009 til desember 2011.
* Skimming av minibanker er telt som én hendelse.

Figur 7: Hendelser i 2011 per måned



Figur 8: Hendelser rapportert i 2011 fordelt etter de sju tapskategoriene i Basel II-regelverket



4.3.1 Trojanerangrep

I hele 2011 har norske nettbanker vært utsatt for angrep med ondsinnet kode, spesielt trojanerne SpyEye og Zeus. Angrepene nådde toppen av intensitet i februar. Da ble de fleste url-ene til norske nettbanker (internettadresser) gjenfunnet i ondsinnet programkode, ment for spredning til norske bankkunders pc-er. Gjennom oppslag eller nedlasting fra en nettside eller en e-post ble kundens pc infisert med ondsinnet kode. Pc-er med dårlig oppdatert sikkerhet (virusbeskyttelse, spamfilter, brannmur etc.) er mest utsatt. Den ondsinnede koden fungerer slik at den legger seg på vent til kunden logger seg inn i nettbanken (taster nettbank-url). Kunden blir da presentert for en falsk side (phishing) som ligger over den ordinære siden og til forveksling er lik bankens side med bankens logo etc. Språket blir stadig bedre, men i angrepene i 2011 var det fortsatt tydelige skrivefeil. Påloggingskodene kunden taster inn, blir plukket opp av et kommandosenter med sanntids overvåking av infiserte pc-er og brukt til å lage falske transaksjoner. På grunn av samarbeid mellom bankene om utveksling av informasjon om infiserte pc-er og falske mottakere, har nesten alle transaksjonene blitt stoppet før de har blitt gjennomført. Tapene er lave, se tabell i punkt 3.5. De fleste transaksjonene har vært overføring til utlandet. Mindre banker fikk størst tapstall fordi de ikke var like raske med å bli inkludert i det etablerte samarbeidet mellom bankene, BSK og NorCERT.[12] Dette er nå endret.

4.3.2 «Påskehendelsen» 2011

Onsdag før påske, en av årets travleste handledager, oppsto det problemer med å bruke betalingskort. Kundene opplevde at betaling med kort i betalingsterminal og uttak i minibank ble avbrutt eller gikk særdeles tregt. Problemene gjaldt både BankAxept-transaksjoner og transaksjoner med internasjonale kort. Av totalt 4,3 millioner betalinger med kort ble 1,4 millioner i «stippet»[13] med over 4 sekunder ventetid på svar fra terminalen og ca. 200 000 transaksjoner ble avvist. Kunder med kort utstedt av banker som bruker autorisasjonsløsningen til EDB ErgoGroup ASA (EEG) ble verst rammet. Årsaken til problemet var en hardware-feil på primærserver for autorisasjonsmottak av kort i EEG. Det viste seg at reserveløsningen ikke var oppgradert med samme kapasitet som primærløsningen. Primærserver ble oppdatert høsten 2010 for å kunne behandle transaksjonsmengden i juletrafikken. Ved en feil ble ikke sekundærserver oppgradert tilsvarende.

Driftsavviket viste seg å få alvorlige følgefeil. På grunn av tregheten i behandlingen gjorde mange kunder flere forsøk på å bruke kortet. Dette førte til at det ble dupliserte reservasjoner på kunders kontoer, og i noen tilfeller ble transaksjoner gjennomført flere ganger ettersom de ble inntastet mer enn en gang på brukerstedet.

Siste reskontrokjøring med kapitaltransaksjoner før påske ble kjørt onsdag ettermiddag. Grunnet feilen med autorisasjonssystemet i EDB, ble det ettersendt reservasjoner fra Nets fra onsdag 20. april etter at kapitaloppdatering var kjørt. Dette foregikk helt fram til fredag formiddag. Transaksjonene ble altså

[12] NorCERT: Avdeling i Nasjonal sikkerhetsmyndighet (NSM) hvor «Nor» står for Norge.
CERT: Computer Emergency Response Team.
[13] STIP: Stand In Processing – inngår i et avtalt opplegg uten dekningskontroll

kjørt inn i feil rekkefølge og ble ikke nullet ut som normalt. Berørte kontoer ble bokført med riktig beløp, men fikk i tillegg redusert disponibel saldo med det samme beløpet (det vil si «dobbelt belastet»). Disponibel saldo framsto derfor som for lav for mange kunder, eller som tom for enkelte kunder.

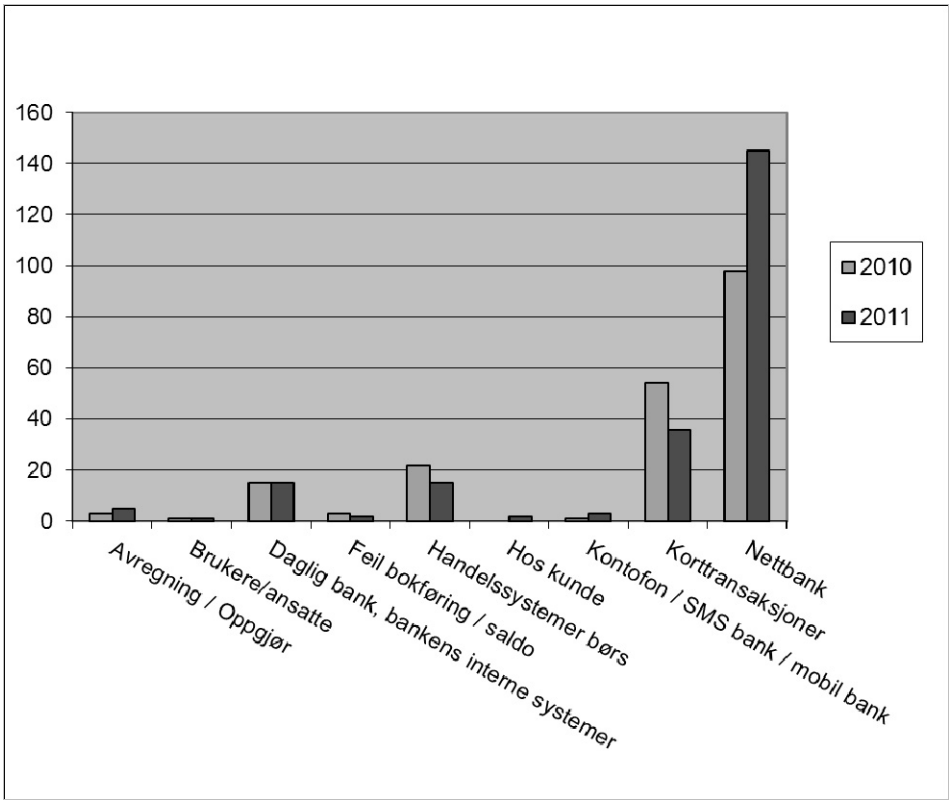
Det var ingen bankdager i påsken, og flere kontoer blir derfor ikke rettet opp før bankene kjørte reskontrooppdatering (oppgjør) første arbeidsdag etter påske.

Søndag 24. april kjørte EDB sletting av reservasjoner og fjernet majoriteten av reservasjonene. De resterende ble fjernet i flere påfølgende kjøringer fram til og med tirsdag 26. april.

4.3.3 Analyse av hendelsene

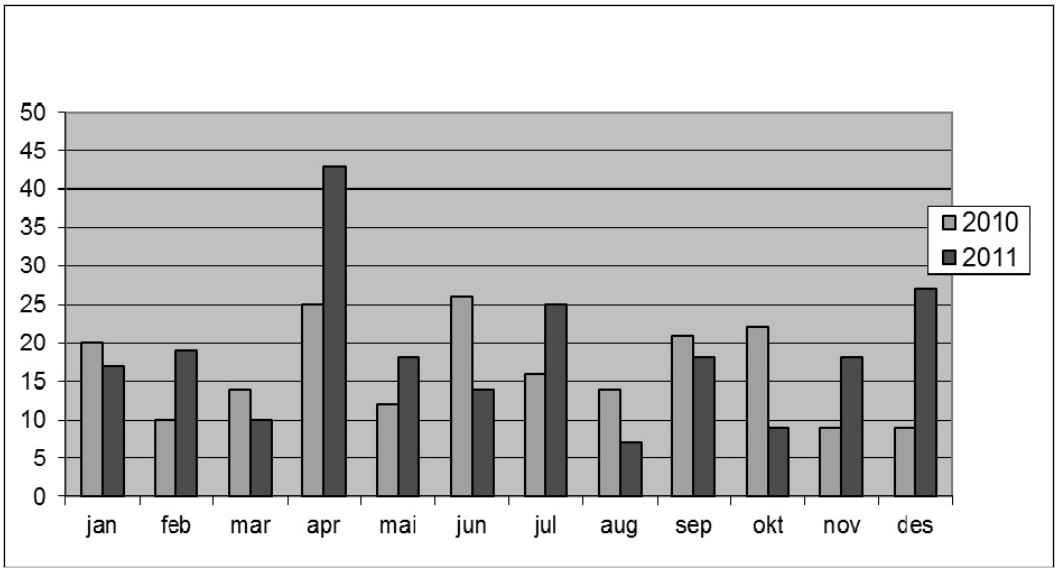
Figurene nedenfor viser utviklingen fra 2010 til 2011.

Figur 9: Hendelser fordelt på system/produkt 2010 vs. 2011



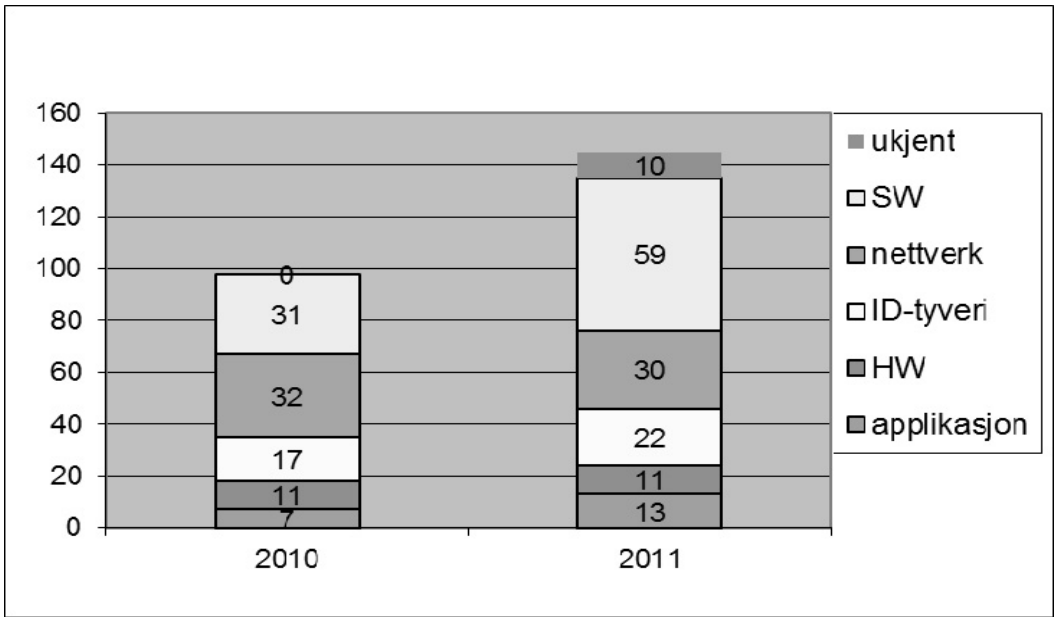
Det er ingen dramatisk negativ utvikling. Nettbank skiller seg ut med en økning i innrapporterte hendelser på ca. 40 prosent.

Figur 10: Hendelser fordelt på måned i 2010 vs. 2011



Økningen i april skyldtes «påskehendelsen», se kapittel 4.3.2.

Figur 11: Hendelser i nettbank – antall fordelt på årsak



Figuren over viser hvor årsaken til hendelsene ligger for nettbank. 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 i seg selv virker slik den skal, men at SW er satt i drift på en uheldig måte, og at dette fører til at nettbanken ikke fungerer som forutsatt. Det kan for eksempel være parametre som er satt uheldig, som ikke lenger passer til omgivelsene, eller ikke er tilpasset trafikken e.l.

Grunnlaget for inndelingen i figuren over er:

Software (SW) er all støtteprogramvare som utgjør kjøreomgivelsen til nettbankapplikasjonen. Det kan være applikasjonsservere, webserver, databaseserver, CICS, programvare for overvåking av nettbanken, sertifikater, køsystemer (MQ eller andre), og annen standard hyllevare levert av tredjepart.

Nettverk dekker rutere, switcher, Domain Name System, gateway, Network Address Translation, Intrusion Prevention System/Intrusion Detection System, linjer, brannmur osv.

ID-tyveri er først og fremst phishing og trojanere. Det har også vært hendelser som går på at en kunde har fått innsyn i en annen kundes engasjement og at det har vært feil i autentiseringsfunksjonene. Disse er med her.

Hardware (HW) er maskinvaren som nettbankapplikasjonen kjører på og kan være mikrokodefeil, overbelastning, feil parametersetting, plutselige og uforklarlige stopp.

Applikasjon er hendelser knyttet til feil eller svakheter i selve nettbankapplikasjonen, det vil si den delen av koden som banken utvikler.

Figuren viser at det fremdeles er SW som er dominerende årsak til hendelser. Fortsatt synes det å være en utfordring å opprettholde en stabil kjøreomgivelse for nettbankapplikasjonene.

Det var 16 alvorlige eller kritiske hendelser knyttet til brannmur i 2011. Finanstilsynet registrerer at det er betydelig utfordringer å ha oversikt over konsekvensene av endringer knyttet til brannmurregler og oppdateringer av brannmurkonfigurasjon.

Det er verdt å merke seg at i og for seg uskyldige feil fører til følgefeil som kan ha svært alvorlige konsekvenser. Illustrerende i så måte er en hendelse knyttet til en minnelekkasje som førte til at både nettbank, mobilbank, telefonbank, sms-bank, låneløsning på Internett, system for avtaleinngåelse på Internett, kortsystemene, POS-systemene, bedriftsløsning på Internett og bankens interne systemer for salg og kundeoppfølging og løsning for kredittbehandling gikk ned.

4.4 Risikoområder identifisert fra andre kilder

4.4.1 Cloud Computing

Sony har lagt store deler av sin kundebase for online-spill ut på en Cloud Computing-løsning. Det er sagt at det ligger informasjon om ca. 100 millioner kunder som spiller online-spill på Sonys løsninger. Informasjonen som ligger ute, inneholder store deler av den personlige informasjonen som navn, adresse, kjønn og fødselsdato, samt påloggingsinformasjon, om enn kryptert. For noen av disse kundene ligger det også informasjon om betalinger og kortinformasjon. Sonys løsning ble kompromittert og måtte stenges ned over flere dager i 2011. Det kan se ut som om at de som har hacket seg inn på Sonys baser har benyttet styrken ved Cloud Computing, som gir den datakraften og lagringskapasiteten man trenger til oppgaven.

Eksemplet Sony viser risikoer ved Cloud Computing.

4.4.2 Angrepet på RSA

Datasikkerhetsmiljøene reagerte med overraskelse og usikkerhet da det viste seg at RSA, et selskap i EMC-gruppen, var blitt utsatt for et avansert dataangrep av typen APT («Advanced persistent threat») i mars 2011, og at informasjon om RSA SecureID var stjålet. Denne informasjonen ble i sin tur brukt til et forsøk på å angripe Lockheed Martin, en stor amerikansk produsent av forsvarsmateriell. RSA har siden vedgått at den stjålne informasjonen kunne gjøre et stort antall SecureID engangskodegeneratorer verdiløse, og de har tilbudt å skifte ut engangskodegenerator hos kunder som bruker disse i firmasammenheng.

Selve datainnbruddet ble gjennomført som en tre-trinns operasjon: Angrepet startet ved at en ansatt ble lurt til å åpne et infisert regneark fra en e-post med emnet som utga seg for å være rekrutteringsplaner for året. Det infiserte regnearket benyttet så en hittil ikke identifisert feil («zero-day flaw») i Adobe Flash til å installere et verktøy for fjernstyring. Deretter ble flere pc-er infisert for til sist å nå pc-er som hadde adgang til de sensitive informasjonene. De ble samlet, komprimert, og eksportert til ekstern maskin som også var overtatt, og deretter sendt til den som foretok innbruddet.

Slike APT-angrep som bruker en kombinasjon av tilsynelatende enkel svindel og høyteknologisk utnyttelse av «zero-day»-feil i en programvare, er svært vanskelig å oppdage og stoppe, ettersom antivirusprogrammene ikke gjenkjenner slike angrep.

RSA SecureID brukes som engangspassord (OTP)-generator, blant annet i to-faktor-autentisering (2FA) for online-tilgang til banktjenester. Det er derfor kritisk hvis systemet infiltreres.

5 Identifiserte risikoområder

5.1 Risiko ved utkontraktering

Det enkelte foretak er ansvarlig for egen IKT-virksomhet. Dette gjelder også der hele eller deler av IKT-virksomheten er utkontraktert. Gjennom hendelser som oppsto i 2011, har det kommet fram at enkelte foretak mangler et helhetlig bilde av transaksjonskjeden, for eksempel innenfor området betalingsformidling.

En forutsetning for å kunne ha den totale oversikten er at det er etablert avtaler med alle relevante aktører, og at avtalene er avstemt for å kunne levere ønsket resultat.

Kostnadene ved utkontraktering av IKT-tjenester gis stor oppmerksomhet. Det er viktig at avtalene ivaretar interessene både til kjøper og leverandør, slik at man sikrer at eventuelle besparinger ikke går på bekostning av sikkerhet og kvalitet i IKT-leveransene.

Finanstilsynet vurderer cloud computing på lik linje med utkontraktering av tjenester, og feltet behandles derfor på samme måte. Foretaket skal, i egen regi eller gjennom et formalisert samarbeid med andre foretak, sikre kontroll med egne data og ha tilstrekkelig kunnskap om IKT-infrastrukturen slik at alle IKT-forskriftens krav oppfylles.

Avtalen må sikre at foretak under tilsyn også gis rett til å kontrollere de av leverandørens aktiviteter som er knyttet til avtalen, og at Finanstilsynet gis tilgang til opplysninger fra og tilsyn hos IKT-leverandøren.

5.2 Mangler ved styring og kontroll

Finanstilsynet peker på tre forhold som er vesentlige for styring og kontroll av IKT-virksomheten, og som generelt ikke synes å være tilstrekkelig ivaretatt.

Et rammeverk, der blant annet prosesser, rutiner, prosedyrer, prosesser, verktøy, rolle- og

ansvarsavklaring er dokumentert, er nødvendig for at foretakene skal arbeide rasjonelt og effektivt innenfor virksomhetens rammer og krav, og mot de målene som er satt. Det er en forutsetning at prosesser og rutiner er gjennomarbeidet. Finanstilsynet har erfart at foretakene ikke alltid har et slikt rammeverk på plass, og at rammeverket ikke alltid er forankret og kjent i organisasjonen. Det er også nødvendig at foretakene etablerer rutiner og praksis for å påse at rammeverket etterleves.

Risikostyring skal bidra til at foretakene når sine mål og strategier. For å oppnå ønsket effekt er det nødvendig at risikovurderingene er gjennomarbeidet, at risikoreduserende tiltak blir identifisert og at ansvarlig og sluttdato for gjennomføring av tiltak blir tilordnet. Risikoene må følges opp og revurderes jevnlig. Dette gjelder også for IKT-virksomheten. Finanstilsynets erfarer at risikovurdering og risikostyring ofte ikke blir tilstrekkelig ivaretatt på IKT-området, og dermed ikke blir det styringshjelpemidlet det kan være.

Manglende eller mangelfulle risikovurderinger i forkant av beslutning om utkontraktering tilsier at flere foretak neppe har oversikt over risikoen de løper ved utkontraktering. Foretaket som utkontrakterer, har også ansvaret for risikostyring og internkontroll i den delen av virksomheten som er utkontraktert. Mange foretak har ikke tilstrekkelig innsikt i leverandørenes risikostyring og internkontroll.

5.3 Kriminelle angrep mot betalingssystemene

5.3.1 Antatt bakgrunn for kriminaliteten

Organisert kriminalitet rettet mot bankenes betalingssystemer er et pågående og økende problem. Det er sannsynlig at mange av angrepene som skjer i de nordlige og vestlige deler av Europa har sitt utspring i organisert kriminalitet. Disse miljøene benytter ofte en komplisert struktur med prosjektlignende form på angrepene. Det er derfor vanskelig å finne effektive midler for å stoppe denne formen på kriminalitet. Viktige tiltak for å bekjempe dette internasjonalt er samfunnsbygging og demokratisering i de aktuelle kjerneområdene, politisamarbeid, som allerede skjer gjennom Interpol og Europol, ulike tiltak og samarbeidsopplegg på tvers av land i Europa, eksempelvis CERT-samarbeidet, samarbeidsopplegg knyttet til utvikling og bruk av Internett, og konkrete samarbeidsopplegg innenfor finanssektoren.

5.3.2 Nettbankkriminalitet

I 2011 var flere av bankene i Norge utsatt for angrep mot nettbanken med bruk av såkalte trojaner-programmer. Det var ulike typer trojaner-program som ble benyttet:

a) Trojanerprogram som må kombineres med aktiv overvåking, det vil si nødvendig med en «Man in The Middle»-løsning, for å endre innholdet i kundens transaksjoner til banken, eksempelvis beløp og kontonummer med gjenbruk av engangs- og andre koder uten at kunden

selv kan merke dette.

b) Bruk av trojanerprogram hvor logikken allerede er programmert inn. Dette er kanskje den mest alvorlige typen med hensyn til mulige volumer i et angrep og som krever mindre kostnadsinnsats fra de kriminelles side. Det er mange metoder som benyttes for å infisere de enkelte brukeres pc-er med trojanerprogram. Bruk av phishing og spam er sannsynligvis noen av løsningene hvor det å klikke på en lenke i e-posten fører til at trojanerprogrammet blir oppdatert på pc-en. Besøk på ulike nettsider er en annen.

Bankenes bevissthet på dette problemet sammen med et nært samarbeid mellom de ulike aktørene er viktige elementer i kampen mot denne kriminalitetsformen. Myndighetenes oppmerksomhet på problemet kan også ha betydning.

Det er åpenbart at situasjonen må følges nøye og at det fortsatt må investeres i sikkerhetstiltak på dette området.

5.3.3 Svindel med betalingskort

Svindel med betalingskort er det området hvor finansnæringen har størst tap. I 2011 ble det meldt om nærmere 17 000 betalingskort som er misbrukt, og samlet tap for kortområdet var over 125 millioner norske kroner.

Skimming av betalingsterminaler og minibanker i Norge er redusert. Krav om chip på alle betalingskort og chip-leser i alle betalingsterminaler har bidratt til dette, og bruk av falske kort med magnetstripe er nesten eliminert i Norge. Men fortsatt kan skimmet informasjon fra magnetstripe på originalkort kopieres inn i magnetstripe på falske kort og nyttiggjøres i utlandet, og det er her de største tapene er. Selve skimmingen skjer også oftest i utlandet, både med og uten avlesing av PIN i tillegg. I Norge er det svært begrenset hvilke betalinger i betalingsterminaler som kan gjøres uten PIN, men i en del andre land er dette mer vanlig. Et nyttig tilbud fra mange banker er å sette regionsperre på kortet. Korteier kan til enhver tid avgrense mulig bruk av kortet til en ønsket geografisk region.

Det er også store tap knyttet til tap av originalkort med PIN. Dette knytter seg til mer tradisjonelle tyverier og overfall/ran.

Ikke ubetydelige tap knytter seg til misbruk av kortinformasjon uten bruk av kort, som ved internetthandel. Her er det mange uoversiktlige varianter. Ofte brukes en form for phishing til å avlure kredittkortinformasjon, men det kan også være datalekkasjer i form av innbrudd i butikksystemer eller annet. Man ser kredittkortinformasjon brukt i stadig mer sofistikerte «business cases» for å maksimere utbyttet, men også for å maskere svindelen. Rettmessig eier av kortet kan framstå som skyldig i tvilsomme transaksjoner som kortet har vært involvert i.

Finansforetakene følger opp kortsvindel blant annet gjennom avanserte overvåkingssystemer. For å ha kontroll med tapene, er det viktig å ha stor oppmerksomhet rettet mot kortsvindelen.

5.4 Risiko for driftsavbrudd og systemfeil

5.4.1 Reserveløsninger

Hendelser som rammer den finansielle IKT-infrastrukturen viser at reserveløsningen ikke alltid er tilgjengelig slik det er forutsatt av foretaket som rammes. Reserveløsningen blir ikke alltid vedlikeholdt i takt med produksjonsløsningen. Årlige tester, jf. IKT-forskriftens § 11, gir ofte nyttig informasjon som grunnlag for å ajourføre reserveløsningen.

Ny teknologi åpner for mer robusthet. I dag kan kunden få tilgang til finansielle tjenester mobilt, via Internett, via telefonbank, ved oppmøte i banken, eller ved hjelp av faste oppdrag som e-faktura og avtalegiro.

Kjernesystemene er imidlertid like sensitive som før og må dekkes av gode reserveløsninger.

5.4.2 Manglende helhetsbilde

Hendelser viser at enkelte foretak har utfordringer knyttet til at arkitekturen er uhensiktsmessig. Det kan være en lite hensiktsmessig datamodell der eierskap og definisjon av dataelementer og attributter er uklare. Det kan også være at IKT-arkitekturen ikke er lagdelt i tilstrekkelig grad, noe som kan gi utfordringer når det gjelder vedlikehold. Ny funksjonalitet kan ha uønskede og utilsiktede følger for andre systemer. For å være på den sikre siden defineres gjerne nye dataelementer for eget formål, noe som gir ytterligere utfordringer når det gjelder vedlikehold og oversikt.

Finansielle transaksjoner behandles automatisk i en behandlingskjede der flere aktører deltar. Hendelser i 2011 viser at aktørene med fordel kunne samhandlet bedre når det gjelder overvåking og varsling. Foretak B mottar transaksjoner fra foretak A etter et regelmessig mønster («kalender» og volum). B, som oppdager et avvik fra mønsteret, kan varsle A. A og B samarbeider etter dette om retting, opprydding etc. Det ble iverksatt gode initiativer på dette området i 2011.

5.4.3 Parametersetting, vanskelig å teste transaksjonskjeden og tilhørende infrastruktur

Hendelser som rammer den finansielle IKT-infrastrukturen tyder på at det kan være en utfordring å vedlikeholde driftsplattformen. Plattformen består av et omfattende sett med støttesystemer, både maskinvare og programvare, som sluttbrukertjenesten (eks. nettbank) er avhengig av. Det er en komplisert oppgave å konfigurere og vedlikeholde applikasjonsservere, databaseservere, web-servere,

kommunikasjonsprogramvare, overvåking, sertifikater, tilganger, brannmur osv. En rekke forhold, som endringer i belasting, antall brukere og ny sluttbrukerfunksjonalitet, kan medføre behov for å endre parametre i programvaren, noe som krever detaljert kunnskap og nøye overvåking.

Grundig testing er en forutsetning for stabil drift. Flere foretak har gode produksjonslike testmiljøer. Flere foretak benytter i utstrakt grad programmerte tester (scripts), og har stor nytte av dette i forbindelse med regresjonstesting av nye versjoner («releaser») av applikasjonene. Men Finanstilsynet ser også foretak som hyppig må kalle tilbake nye versjoner, gjøre rettelser, teste på nytt og starte produksjon på nytt. Foretakene taper tid og ressurser, og det skaper støy hos kundene. Grundig testing er en god investering.

Finansielle transaksjoner gjennomføres i sin helhet automatisk. All behandling skjer maskinmessig, fra og med kundens registrering til og med bokføring og arkivering. Flere finansforetak er involvert i behandlingen av en transaksjon. Det kan være behov for å regresjonsteste hele transaksjonskjeden, det vil si at det må testes også mot systemer som foretaket ikke direkte har kontroll over. Organisatorisk og teknisk kan det være en utfordring å få til slike omfattende tester. Det krever godt samarbeid mellom alle involverte.

6 Finanstilsynets videre oppfølging

6.1 IT-tilsyn

Finanstilsynet har utviklet et omfattende opplegg for gjennomføring av IT-tilsyn og tilsyn med betalingstjenester på ulike områder. Inndeling i områder følger i stor grad industristandarder. Bruk av modulene for det enkelte tilsyn velges ut fra en risikovurdering av det aktuelle foretaket. Hensikten er å forvalte og videreutvikle dette videre. Modulene er lagt tilgjengelig på Finanstilsynets nettsted for at også aktuelle foretak kan benytte modulene til eget arbeid.[14]

En videre utvikling av dette er planlagt gjennom valg av egne temaområder. Følgende områder er valgt ut:

a) Styring og kontroll (IT-governance)
b) Katastrofe- og beredskapsløsninger
c) Elektroniske betalingsløsninger
d) IKT-infrastruktur
e) Utkontraktering som omfatter outsourcing, offshoring og cloud computing

Planen er å benytte aktuelle temamoduler mot de mest systemkritiske foretakene og se dette i sammenheng med øvrige ordinære IT-tilsyn, hendelsesrapportering og meldeplikt på betalingstjenester som underlag til vurdering av nivået på operasjonell risiko for ICAAP[15]-prosessene.

[14] Se: www.finanstilsynet.no/no/Tverrgaende-temasider/IT-tilsyn/Egenevalueringssporsmal/
[15] Internal Capital Adequacy Assessment Process (ICAAP) stiller krav til regelmessig gjennomføring av en intern kapitalvurderingsprosess for å ta stilling til kapitalbehovet.

6.2 Betalingstjenester

6.2.1 Meldeplikten

Det er viktig for Finanstilsynet å holde seg oppdatert på endringer som skjer med betalingstjenestene. Det pågår en omfattende teknologisk utvikling på området mobile enheter som i stadig sterkere grad får samme egenskaper som personlige datamaskiner. Finanssektoren, særlig bankene, adopterer denne teknologien og tilbyr løsninger til sine kunder på nye mobile enheter. Risikobildet kan bli mer komplekst og krever høy kompetanse for å ha tilstrekkelig oversikt over risikobildet. For å sikre tilstrekkelig informasjon om utviklingen på dette området, vil tilsynet opprettholde meldeplikten.

6.2.2 Samarbeid

Det er mange aktører på betalingssystemområdet i Norge og som har ansvar og oppgaver som grenser tett opp til hverandre i regelverket, og til en viss grad overlapper hverandre. For å sikre på den ene siden at oppgaver ikke faller mellom to stoler, og på den andre siden sørge for samordning slik at det ikke blir gjort dobbelt arbeid, har Norges Bank og Finanstilsynet samarbeidet nært på betalingsområdet gjennom flere år. I 2011 ble det utarbeidet et felles dokument om samarbeid og ansvarsdeling mellom Finanstilsynet og Norges Bank som regulerer dette. Begge organisasjoner tror at det tette samarbeidet gir positive effekter og bidrar til effektiv ressursutnyttelse. Samarbeidet vil fortsette i 2012.

For banksektoren ivaretar FNO Servicekontor, seksjon for betalingssystemer og infrastruktur mange viktige oppgaver, særlig gjelder dette for fellesløsninger på betalingssystemområdet. Finanstilsynet har derfor lagt opp til et nært samarbeid med FNO på dette området. Samarbeidet omfatter også Bankenes Standardiseringskontor (BSK). Finanstilsynet tror at et tett samarbeid på betalingssystemområdet kan bidra til økt oppmerksomhet på problemområder og håndtering av risiko.

6.3 Risiko- og sårbarhetsanalyser

Finanstilsynet får informasjon fra mange finansforetak når det gjelder foretakenes etterlevelse av IKT-forskriften. Det gjør at Finanstilsynet kan danne seg en oppfatning av hva som er beste praksis innenfor områdene som IKT-forskriften dekker. På denne bakgrunn kan Finanstilsynet danne seg et bilde av hvilke foretak som har et forbedringspotensial og kan påvirke foretakene i retning av beste praksis.

Finanstilsynet mottar hendelsesrapporter, jf. IKT-forskriftens § 9. Det gjør at Finanstilsynet kan identifisere «single point of failure», det vil si IKT-komponenter som vil kunne ramme større deler av den finansielle IKT-infrastrukturen dersom de ikke fungerer som forutsett. Hvert foretak ser konsekvensen for eget foretak. Finanstilsynets utfordring er å vurdere konsekvensen for næringen totalt sett.

I arbeidet med risikoanalyser prioriterer finansforetakene det som de føler de har best kontroll over, det vil først og fremst si IKT-infrastrukturen som leveres og styres av foretaket selv. Finanstilsynet vurderer risikoanalysen til enkeltforetak i det løpende tilsynet. Dette bidrar til en vurdering av risikobildet totalt sett for næringen. I denne totalvurderingen er det også viktig at Finanstilsynet opprettholder kontakten med tilsynsmyndigheter. Dette gir nyttig innsikt i trusseltrender og sikringstiltak.

Finanstilsynet oppfordrer til kunnskapsdeling foretakene mellom når det gjelder sårbarheter og aktuelle trusler. Dels formidler Finanstilsynet aktuelle trusler til foretakene som del av tilsyn med foretakene. Finanstilsynet lager også oversikter i anonymisert form som deles mellom foretakene. Endelig samler Finanstilsynet foretakene årlig for å informere om funn og trender fra hendelsesrapporteringen.

6.4 Hendelsesregistrering og rapportering

Finanstilsynet har etter hvert bygd opp en betydelig hendelsesdatabase som representerer en verdifull kilde til analyse av trender og sammenhenger. Ved særlig alvorlige hendelser som rammer mange foretak samtidig samler Finanstilsynet bransjen til møte for å kartlegge situasjonen og avtale felles tiltak. Særlig gjelder dette ved sikkerhetshendelser der utveksling av informasjon er viktig for å kunne iverksette effektive tiltak.

Å sikre stabil og kvalitetsmessig god rapportering kan være en utfordring. Større banker/finansforetak følges derfor opp med møter om rapporteringen. For å rette oppmerksomheten mot og verdsette rapporteringen foretakene gjør, inviterer Finanstilsynet aktuelle kontaktpersoner i foretakene til et årlig hendelsesseminar med relevante temaer knyttet til hendelseshåndtering.

Bankene har i oppfølgingen av påskehendelsen identifisert en rekke forhold som kan forbedres. Mange av forslagene fra bankene har resultert i konkrete tiltak. Finanstilsynet arbeider med gjennomgang av dokumentasjonen fra bankene og vil følge opp resultatet av dette arbeidet mot den enkelte bank og bankenes hovedleverandører.

6.5 Beredskapsarbeid – Beredskapsutvalget for finansiell infrastruktur

Gjennom Beredskapsutvalget for Finansiell Infrastruktur (BFI), som ledes av Finanstilsynet, planlegges og gjennomføres beredskapsøvelser på tvers av finansinstitusjoner og leverandører. I 2011 ble det i regi av BFI gjennomført to beredskapsøvelser, en øvelse på betalingssystemområdet gjennomført i regi av DNB og en øvelse på organisasjon og prosedyrer gjennomført i regi av Finanstilsynet. Erfaringen er at det er nødvendig med regelmessige øvelser på beredskapsopplegget for

å sikre at dette fungerer i en reell beredskapssituasjon.

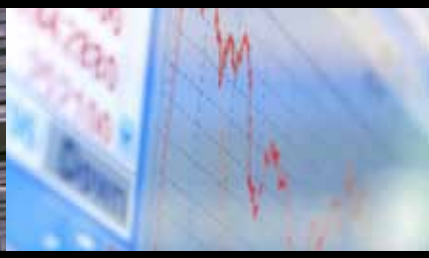
Basert på opprinnelige forslag utarbeidet i regi av BFI er det i samarbeid med Norges Bank utarbeidet forslag til prioritering av tele og strøm for nærmere definerte sentrale institusjoner og forslag til alternative betalingsmåter i en beredskapssituasjon. Forslagene inngår i det generelle beredskapsarbeidet for finanssektoren og er oversendt Finansdepartementet.

BFI representerer en viktig møteplass mellom ulike aktører i Norge som har oppgaver innenfor det norske betalingssystemet. Utvalget har mange oppgaver, men har særlig oppmerksomhet mot beredskapsarbeidet og er derfor opptatt av å følge opp hendelsesutviklingen. Gjennomføring av øvelser for å være best mulig forberedt om det skjer en alvorlig hendelse er viktig og gitt prioritet. Finanstilsynet vil fortsette arbeidet med å utvikle BFI og ivareta ansvaret for ledelse og sekretariat for utvalget.

Foto forside (fra venstre): Berit Roald/Scanpix, Scanpix Creative, Nina Berman/Noor/Felix Features.
Foto bakside (fra venstre): Rui Camilo/Scanpix, Johan Wingborg/Scanpix, Ilja Hendel/Scanpix.

Design omslag: miksmaster.no
Trykkeri: RK Grafisk
03.2012/700





FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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