KREDITTILSYNET
The Financial Supervisory Authority of Norway

Rapport

Risiko- og sårbarhetsanalyse (ROS)

2007

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Risiko- og sårbarhetsanalyse (ROS) 2007

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Kredittilsynet, 13. mars 2008

Innhold

1 Innledning

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

Kredittilsynet kan gjennom analysene se utviklingen over tid og på tvers av det enkelte foretaket, noe som gir et godt grunnlag for å planlegge tiltak. Det er også en målsetting å legge til rette for tilgang til kvantitative data som grunnlag for å se utviklingstrender på ulike områder. Kredittilsynets ROS-analyse kan også være nyttig for bransjeorganisasjoner og enkeltforetak som referanseramme og underlag for egne vurderinger og tiltak på ROS-området.

Resultatet av ROS-analysen kan gi indikasjoner på hvordan sektoren overholder gjeldende lover, forskrifter, bransjerelaterte vedtatte regelverk og forholdet til bruk av standarder og bransjemessige normer.

Arbeidet med ROS-analyser over tid har gitt tilsynet verdifull oversikt og gradvis bedre innsikt og forståelse for risikosituasjonen.

Hendelsesrapportering, som ble etablert som en frivillig ordning fra november 2007, er ett eksempel på dette.[1] Beslutningen om å starte en kartlegging og analyse av fysisk og logisk infrastruktur og hvordan styring og kontroll ivaretas på infrastrukturområdet, er et annet eksempel på tiltak iverksatt som følge av større oppmerksomhet knyttet til operasjonell risiko.

Et tema som får oppmerksomhet i årets rapport, er utkontraktering over landegrenser. Dette er et viktig tema som har vært oppe tidligere, men erkjennelsen av mangler i regelverket når det gjelder håndtering av risiko knyttet til data, systemer som prosesseres, driftes og oppbevares utenfor landets grenser, gjør dette til prioritert tema i risikoarbeidet. Blant annet som en følge av internasjonalt samarbeid om regelverk for kapitaldekning og soliditet innen finans og forsikring (Basel II og Solvens II), gis operasjonell risiko større oppmerksomhet. Det kommer også nye nasjonale krav som prioriterer arbeidet med risikoforståelse og håndtering av denne, jf. NOU 2006: 6 *Når sikkerhet er viktigst – Beskyttelse av landets kritiske infrastruktur og kritiske samfunnsfunksjoner* og "Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007–2010".

[1] Se Kredittilsynets rundskriv 31/2007: "Rapportering av IKT-hendingar til Kredittilsynet"

Norge har velfungerende betalingssystemer. En av grunnene er at finansnæringen er enig om å følge standarder for å få til god samhandling. Standarder finnes på mange nivåer og utvikles i flere organisasjoner. Se nærmere omtale av nasjonale standarder i kapittel 0. COBIT[2], ISO 27001[3] Information technology – Security techniques – Information security management systems – Requirements, ISO 27005 Information security risk management, ITIL[4] og "god praksis på området" er eksempler på generelle standarder som brukes av næringen. Likevel finnes det flere områder som ikke har ferdige standarder. For eksempel mangler det standarder innen interoperabilitet og back-up for finansnæringen internasjonalt.[5] Det hindrer delvis effektiv samhandling, og delvis representerer det en risiko.

[2] Control Objectives for Information and related Technology
[3] International Standards Organization/IEC FDIS 27001:2005-06-30 – Information technology – Security techniques – Information security management systems – Requirements.
[4] Information Technology Infrastructure Library
[5] ISO/TR 17944:2002(E) Banking – Security and other financial services – Framework for security in financial systems

2 Utviklingstrekk, risiko og sårbarhet

2.1 Viktige drivere som påvirker risikoen i finanssektorens bruk av IKT

Det er mange generelle utviklingstrekk i finanssektoren som påvirker foretakenes bruk av informasjonsteknologi. Kredittilsynet har identifisert følgende drivere som er viktige for å forstå effekten på operasjonell risiko.

- Organisert kriminalitet som søker å utnytte sårbare områder i finansnæringens bruk av informasjonsteknologi. Dette er et område med sterk økning og dynamikk.
- Samlet økt bruk av åpen infrastruktur for datakommunikasjon (Internett) gir mer avhengighet og kan medføre større sårbarhet om det ikke iverksettes tilstrekkelige tiltak for å sikre tilgjengelige og trygge tjenester.
- Nye forretningsmuligheter som åpner seg gjennom bruk av ny teknologi og som kan medføre økt eksponering av risiko på områder som ikke er forstått tilstrekkelig.
- Teknologisk utvikling som krever inn- og utfasing av teknologi for å følge IT-leverandørindustriens utvikling.
- Utkontraktering utenfor landet (såkalt offshoring) er en problemstilling som kan innebære ukjent operasjonell risiko.
- Tjenester, produkter og teknologi integreres ytterligere, øke kompleksiteten og gi mer sårbarhet om ikke relevante tiltak etableres.
- Press på priser og krav om kostnadsreduksjoner, også direkte på IT-området (for banker kan dette utgjøre fra 15 til 25 prosent av totale kostnader), stiller krav til effektivisering og rasjonalisering som igjen fører til press på behov for endringer i bruk av informasjonsteknologi.
- Etablering av nye distribusjonskanaler til kundene og behov for produktutvikling for å utnytte dette potensialet krever ofte etablering av nye IT-løsninger eller større endringer i eksisterende.
- I finansnæringen er det stadig strukturelle endringer, fusjoner og nye samarbeidskonstellasjoner som har stor innvirkning på IKT-området. Dette gjelder både for bank, forsikring og i verdipapirsektoren. Ofte medfører dette plattformendringer på IKT-

området og påvirkning på gjeldende opplegg for utkontraktering. De endringsprosessene som følger av dette, medfører ofte økt risiko og krever kompetent håndtering.

- Samarbeidskonstellasjoner kan gi nyttige effekter på mange områder, men kan også føre til mer komplekse organisasjoner og økt risiko for manglende styring og kontroll.
- Økt konkurranse i markedene lokalt og nasjonalt, og videre i det nordiske, europeiske og internasjonale markedene skaper behov for tiltak og endringer. Dette kombinert med store endringer i regelverk, gir samlet store krav til endringer i informasjonsteknologien og dermed fare for økt operasjonell risiko.
- "Time to market" er fortsatt en nøkkelfaktor i en økende konkurransesituasjon, og kan gjøre levetiden på produktene kortere og behovet for endringer i eksisterende produkter større. Også dette gir et press på endringshåndteringen og kan både gå ut over kvaliteten på de løsningene som settes i produksjon og samtidig gi økt sårbarhet.
- Applikasjonsporteføljen i enkelte typer finansforetak følger ikke helt med på den teknologiske utviklingen på en slik måte at deler av applikasjonsporteføljen blir stadig mer utdatert (for eksempel kjernesystemer i bank). Det blir kun et tidsspørsmål før det må foretas utskifting. Representerer dette en for stor del av applikasjonsporteføljen, kan det resultere i en høy operasjonell risiko.

2.1.1 Bruk av standarder

Standarder trygger bruk av IKT og reduserer risikoen for dårlig kommunikasjon mellom partene i næringen. Utviklingen går i retning av internasjonale standarder på bekostning av spesialutviklete norske. Samtidig må standarder tilpasses de faktiske behovene hver bruker har.

Finansnæringens infrastruktur fungerer ved hjelp av etablerte standarder i utformingen av kommuniserte meldingstyper. Historisk har ulike meldingsstandarder vært utviklet og drevet av enkeltinstitusjoner i forhold til deres markedsmakt. I stor grad har utviklingen skjedd i samarbeid mellom institusjoner med like transaksjonstyper basert på nasjonale protokoller.

Norske banker arbeider i dag med tre hovedtyper av transaksjonsstandarder. NIBE[6] for massetransaksjoner interbank i NOK, BOLS for interbank korttransaksjoner og SWIFT for interbank høyverdibetalinger. I tillegg brukes ulike typer åpne standarder for kommunikasjon mellom kunde og bank. Verdipapirhandel og oppgjør bruker ISO 15022[7].

FN og ISO har over lang tid søkt å utvikle en global standard som er egnet for å øke effektiviteten i finansnæringen både nasjonalt og globalt.

Arbeidet fra FN og ISOs side har i løpet av de siste årene fokusert på XML[8] som en ny syntaks med

[6] Norsk interbankstandard basert på EDIFact.
[7] Internasjonal standard for elektronisk transaksjons- og meldingsutveksling.
[8] The Extensible Markup Language

potensial for å utvikle en global standard med tilstrekkelig fleksibilitet. Målet er å sikre kvaliteten på transaksjonene samtidig med muligheten for mer kostnadseffektiv multilateral transaksjonsutveksling på tvers av nasjonale og spesielle bransjestandarder. Dette initiativet omfatter både betalingstransaksjoner, kontanthåndtering, verdipapirhandel, fondshandel, oppgjørs- og avregningssentraler samt dominerende bedrifter med høyt transaksjonsvolum.

ISO 20022 XML er grunnstandarden som finansnæringen selv administrerer gjennom ISO med SWIFT som forvalter av standarden. I arbeidet med et mer integrert EU/EØS gjennom SEPA[9], vil denne standarden brukes i alle meldingstyper som går via interbank. Dette omfatter også TARGET 2 som behandler alle sentralbankoppgjør. I tillegg er samarbeid innen verdipapirrelaterte organisasjoner kommet langt for å lage fellesstandarder og videreutvikle ISO 15022 mot en ISO 200022[10] XML-base.

Utviklingen i Norge vil i første rekke berøre de transaksjonene som kommuniseres gjennom SWIFT. Her omfatter dette i stor grad verdipapirhandel, verdipapiroppgjør, investortjenester, høyverdibetalinger, betalinger fra og til utenlandske aktører samt sentralbankoppgjøret.

2.2 Utkontraktering

2.2.1 Trender innen utkontraktering

2.2.1.1 Fra lokal til globalisert leveransemodell

Innenfor banksektoren i Norge har utkontraktering av IKT-virksomheten utgjort en viktig del av totalbildet gjennom mange år. Nye trekk i dette er at:

a) forholdet mellom kunde (finansforetak) og leverandør i dag har mer rene kommersielle trekk enn tidligere samarbeidsmodeller
b) utkontraktering foregår i økende grad ut av Norge (såkalt offshoring)

Det nye risikobildet er globaliseringen som skjer på dette området med leveranser og bruk av ressurser fra flere steder i verden, eksempelvis fra lavkostland som India, Ukraina, Baltikum og andre områder i østlige deler av Europa. Internasjonalt utgjør dette stadig økte forretningsvolumer, men også for Norge har dette blitt en realitet av betydelig omfang. Riktignok har det i størst grad vært flytting av IT-drift til naboland som Sverige og Danmark, men det er klare tendenser til at Norge nå blir en del av det totale bildet på offshore-området. Det kan være den lokale leverandøren i Norge som er del av dette, slik at kunden får utenlandseffekten indirekte. Risikoelementene kan i stor grad være de samme siden

[9] Single Euro Payments Area
[10] Financial services. UNIversal Financial Industry message scheme. Roles and responsibilities of the registration bodies

leverandøren utfører deler av oppgaven utenfor landet.

IT-leveransene kan komme fra fire kilder i kombinasjon:

- *På stedet*, det vil si leverandøren utfører arbeidet hos kunden.
- *Innenlandsk*, det vil si i det landet der kunden holder til.
- *Naboland*, normalt i et lavkostland i nærheten (for eksempel Baltikum), mens det først og fremst for Norge har vært til Sverige og Danmark, og lavere kostnader kan ikke være hele forklaringen
- *Oversjøisk*, det vil si langt unna, og det har i hovedsak vært relatert til systemutvikling og ressurskjøp for forvaltning og utvikling av systemer, hvor Ukraina, Baltikum og India allerede utgjør betydelige forretningsvolumer.

Målsettingen med globalisering er å oppnå markante reduksjoner i både driftskostnader og utviklings-/ forvaltningskostnader. Internasjonale leverandører i markedet, som IBM, CSC, HP, EDS og Accenture har en høy aktivitet på dette området, men også mer lokale leverandører er nå en del av dette bildet. I Norge er det spesielt EDB Business Partner som er aktiv med Ukraina og India som satsingsland for denne virksomheten, men også IBM, SDC, ErgoGroup og TietoEnator er betydelige aktører. På sikt har dette risikoelementer som også kan påvirke leverandørens kunder.

I følge Gartner Group ser det ut til at globalisering av leveransemodellen innen IKT er en irreversibel og varig trend, og det antas at den politiske og følelsesmessige motstanden vil avta. Forskjeller både i tilgjengelig kapasitet og lønnskostnader vil være en varig trend som representerer en underliggende påvirkning, men det tar nok tid før globalisering blir den helt dominerende leveransemodellen på IKT-området.

2.2.1.2 Fra produkteierskap til IT-tjenester etter behov

Bortsett fra stormaskiner, som rutinemessig brukes til flere oppgaver samtidig, har det vært vanlig at en datamaskin er reservert for bare én kunde. En av årsakene har vært at de fleste maskiner ikke lot seg dele mellom flere oppgaver/kunder på en effektiv og sikker måte.

En "IT-utility", en IT-tjeneste, er et sett "virtualiserte" datamaskiner som tilbyr fleksible tjenester, som er tilgjengelige ved behov, med prising basert på forbruk. Dette kan bety at en "IT-utility" betraktes som en globalisert ressurs som består av maskiner "både her og der" og det er likegyldig for kundene hvor produksjonen foregår. Produksjonen kan bli flyttet dit det finnes ledig kapasitet, uten at kundene er oppmerksomme på det. Et reservested i et annet land kan tas i bruk hvis nødvendig. De dominerende maskinprodusentene, som IBM og HP, har lansert løsninger med meget stor kapasitet som kan utvides/innskrenkes raskt etter kundens skiftende behov. Kapasiteten er allerede på plass og åpnes opp av leverandøren ved kundens bestilling (dette skjer innenfor betydelige kapasitetstrinn og da før ny installasjon og oppgradering må foretas). En målsetting med dette er å redusere driftskostnadene og samtidig kunne gjøre utkontraktering mer attraktiv.

- IT-utility vil flytte eierskap av og kontroll med produksjonsutstyret helt i leverandørenes (først og fremst IBMs) hender slik som det for eksempel er med strømforsyning der ingen er opptatt av hvor strømmen produseres.
- Med IT-utility vil, sett fra kundens perspektiv, kostnadene på maskinvare forsvinne som kostnadsart, tjenestene vil komme i forgrunnen og betaling vil i større grad kunne skje ut fra forbruk og kvalitetskrav.
- Det er grunn til å tro at både driftskostnadene og investeringskostnadene for dem som utkontrakterer kan bli redusert, og faste kostnader vil bli erstattet med variable kostnader på bakgrunn av forbruk.
- En IT-utility forutsetter betydelig båndbredde (kommunikasjonskapasitet) mellom produksjonsstedene og de som kjøper tjenester. En vil i stor grad være avhengig av at kommunikasjonsløsningene er stabile og sikre løsninger. Med den utbyggingen en ser i markedet i dag, vil denne kapasiteten være tilgjengelig til og fra knutepunktene i de fleste aktuelle geografiske områder.
- I følge Gartner Group regner en med at IT-utilities vil være i allmenn bruk om ca. ti år og de vil få sterk påvirkning på hvordan tjenestene vil bli levert.

2.2.1.3 Fra "vertikal" til "horisontal" deling av tjenestene

"Vertikal utkontraktering" betyr at én leverandør, ofte kalt hovedleverandør, tar ansvar for alle oppgaver utkontrakteringen omfatter, også for alle tjenester som leveres av underleverandører. Fordelen med dette er at oppgaven for oppfølging av helheten av IT-leveransen er klart plassert. Dessuten har foretakene kun én motpart å følge opp. Dette har langt på vei vært en leverandørmodell for mindre banker og andre typer små finansforetak.

For større finansforetak går trenden mer i retning av en "horisontal deling" der spesialistselskaper tar seg av de ulike oppgavene en IT-leveranse består av, for eksempel å drifte nettverk eller utvikle applikasjoner. Fordelen kan være at økt konkurranse blant spesialistselskapene vil gi gunstigere pris og bedre kvalitet på hver av oppgavene i en IT-leveranse, men det krever samtidig større kompetanse, oversikt og kapasitet hos kunden.

2.2.2 Fra "fritt frem" til regulert utkontraktering

Finanssektoren er regulert og med direkte myndighetsoppfølging i de fleste land. Dette inkluderer utkontraktering. I stor grad har det vært opp til det enkelte foretaket å ta sine utkontrakteringsbeslutninger utelukkende ut fra egne forretningsmessige betraktninger. Denne praksisen er strammet betydelig inn i lys av at uheldig utformet utkontraktering kan få sterke negative virkninger på foretakenes operasjonelle risiko. Målsettingen er å gjøre utkontraktering til en tryggere forretningsmodell. Utstrakt utkontraktering i finanssektoren til andre land kan innebære en nasjonal risiko som det enkelte foretaket ikke kan håndtere. Det er grunn til å tro at regulering av dette området vil øke internasjonalt, både i USA og i Europa (EU) som følge av økt oppmerksomhet på sikkerhet og

operasjonell risiko (Basel II og Solvens II). I flere land er IT-leverandører til banksektoren underlagt direkte regulering.

2.2.3 Fra helhetlig til komponentbaserte kjernesystemer for banker

De fleste banker bruker kjernesystemer som er 10–20 år gamle. Nye, komponentbaserte kjernesystemer er gradvis mer tilgjengelige på markedet og vil sannsynligvis bidra til en utskiftingsbølge i det internasjonale bankmarkedet. Fordelen med disse løsningene er at de kan være enklere og billigere å vedlikeholde. De komponentbaserte løsningene kan ha lengre levetid og mer standardiserte grenseflater for tilknytning av nye kundenære løsninger. Utviklingen rundt Web-baserte løsninger er en viktig bidragsyter siden det benyttes standarder som gjør det enklere å knytte sammen gamle og nye løsninger. Målsettingen er å redusere de store forvaltningskostnadene som gamle komplekse kjernesystemer utgjør, og problemer knyttet til en offensiv utviklingsstrategi av nye produkter og digitale distribusjonsopplegg til kundene. Ved å gjennomføre en modernisering av gamle kjernesystemer vil en kunne redusere sårbarheten og samtidig øke fleksibiliteten i IT-løsningene, forutsatt at prosjektet blir profesjonelt håndtert. Det er en stor risiko i seg selv å skifte kjernesystem, noe som nok er en del av årsaken til at dette skjer i et langsomt tempo. Det er sannsynlig at å bytte kjernesystemer i stor grad vil bli utkontraktert, siden dette er komplekse og kostbare prosjekter. Det er kun større banker som vil ha kompetanse og kapasitet til å foreta dette i egen regi.

2.2.4 Vesentlige risikomomenter i forbindelse med utkontraktering

Risiko i forbindelse med sikkerhets- og konfidensialitetsbrudd (person- og bedriftsopplysninger på avveie) klassifiseres som en del av den operasjonelle risikoen. Det er ofte slik at en risiko faller inn i mer enn en kategori; for eksempel en kodingsfeil (som er en operasjonell risiko) kan resultere i feilaktig ”credit score”, det vil si en kredittrisiko.

Utkontraktering innebærer å gjøre seg avhengig av IT-leverandører i den daglige driften, som igjen kan bidra til dårligere kontroll. Det øker den operasjonelle risikoen på flere måter:

- Påvirkningsmulighetene (makten) blir redusert i forhold til å beholde ansvaret internt. Leverandørene har egne målsettinger som kan være i konflikt med kundenes.
- Eksterne leverandører kan svekkes, eventuelt gå konkurs hvis de ikke klarer å styre sin økonomi, blir overambisiøse eller få problemer hvis markedsutviklingen tar en ikke planlagt retning. Konkurslovgivningen kan representere en stor risiko for kunden om tilgang til leverandørens løsninger og operasjon blir stengt for tilgang. Denne problemstillingen blir ikke enklere når oppgavene utføres i et annet land enn der kunden er plassert.
- Utkontraktering til flere leverandører (“horisontalt”) kan tilrettelegge for å senke kundens kostnader, men det innfører et betydelig nytt risikoelement knyttet til koordinering, og ansvarsforholdene kan bli uklare.

- Ved en feil eller avbrudd kan leverandørene peke på hverandre og begynne å tolke kontrakten istedenfor å gå i gang med å løse problemet.
- Lovgivningen i det landet hvor oppgavene utføres kan være annerledes enn lovreguleringen i Norge, og dette kan gi kunden manglende kontroll over hva som skjer lokalt. For eksempel kan dette gjelde innsyn til data.
- Kriselignende situasjoner kan oppstå hos leverandøren, i landet der oppgavene utføres, og derfor føre til manglende innsikt og kontroll over situasjonen for kunden. Likeledes kan norske myndigheter risikere å ikke komme i en nødvendig posisjon for å bli informert om krisen og involvert i tiltak for å løse krisen, på tross av at dette kanskje kan ha store samfunnsmessige konsekvenser for Norge.

Utkontraktering senker også risikoen fordi eksterne IT-leverandører ofte betjener mange kunder, og derfor har det finansielle grunnlaget for å bygge opp prosesser, kompetanse, kapasitet, teknologi og fasiliteter som gjør disse mindre sårbare enn hva enkeltforetak ville vært på egen hånd.

Mange kunder er lite bevisste på hvor stor kapasitet og kompetanse det innebærer å leve i et velfungerende utkontrakteringsforhold. Dette gjelder både for ledelse og operative enheter. Juridiske og leveransemessige avtaler må være etablert og fulgt opp. Dersom avtalene er dårlige eller ikke følges opp, kan dette medføre problemer som ofte fører til misnøye og uventede kostnadsøkninger.

Foretakene er generelt sett lite flinke til å bygge inn fleksibilitet i sine kontrakter, og det betyr uventede, store kostnadsøkninger og behov for reforhandlinger. Kontraktene er statiske og lite fleksible mens forholdene i markedet forandrer seg hyppig og på uforutsette måter. I en reforhandlingssituasjon er foretakene i en ufordelaktig posisjon, og de har liten forhandlingsstyrke fordi det å forlate leverandøren kan bli kostbart. Tilsynelatende økonomisk fordelaktige utkontrakteringsavtaler kan derfor vise seg ikke å være det. Oppsigelse av avtalen er som oftest ikke en realistisk opsjon fordi konvertering er kostbart, tidkrevende og risikofylt å utføre.

2.2.5 Tilleggsrisikoer i forbindelse med utkontraktering over landegrensene

Globaliserte leveransemodeller har som tidligere nevnt flere fordeler, men innebærer risikomomenter i forhold til det å bruke hjemlige leverandører, og det krever derfor ekstra risikoreduserende tiltak. Det er utarbeidet flere rapporter hvor det klart fremkommer at foretak som vurderer utkontraktering over landegrenser spesielt må undersøke hvordan den konkrete risikoen i vedkommende land kan vurderes og reduseres på følgende hovedområder:

- Geopolitiske og landrelaterte risikoer (uroligheter, krigshandlinger m.m.)
- Kulturelle og språklige hindre i forbindelse med løpende kommunikasjon
- Risikoer i forbindelse med sikring av fysiske ressurser og intellektuell kapital
- Risikoer i forbindelse med infrastrukturen (strøm, telekommunikasjon o.l.)

- Hvilke virkemidler vil være tilgjengelige hvis en krise skulle oppstå?

Videre må avtale- og forretningsmessige forhold vurderes:

- Leverandørens soliditet på kort og lang sikt
- Prisrisiko og økonomisk stabilitet i de landene der produksjonen skal foregå
- Juridiske og regulatoriske forhold sammenlignet med tilsvarende forhold som norske banker er pålagt å følge.

2.2.6 Hovedleverandør med underleverandører

Det er i dag ingen norske foretak som har basert sin forretningsdrift på en avtale med en oversjøisk hovedleverandør. Derimot ser vi en tendens til at det inngås avtaler med veletablerte norske eller nordiske hovedleverandører som leverer sine tjenester gjennom en globalisert leveransemodell. Denne trenden er allerede synlig i USA, og den er økende. Det er de store bankene som leder an, men også de mellomstore bankene kommer etter for å beholde sin konkurranseposisjon. Ved å ha lokal hovedleverandør forenkler dette kommunikasjonen språklig, kulturelt og praktisk og skaper tydelighet. Kunde og leverandør(er) er da underlagt samme jurisdiksjon og tilsynsregime.

Utenlandske leverandører og globaliserte leveransekjeder kan øke risikoeksponeringen. I det følgende blir tre ulike situasjoner analysert:

1) Hovedleverandøren er norsk, underleverandørene utenlandske

- Kontrakten blir inngått med en ansvarlig norsk hovedleverandør som har ansvar for koordinering og oppfølging av sine utenlandske underleverandører (kan være datterselskaper i et internasjonalt konsern).
- Den spesielle risikoen er om underleverandørene vil være tilstrekkelig leveringsdyktige slik at kontrakten faktisk kan etterleves.

En viktig underleverandør vil være leverandøren av kommunikasjonstjenester i de landene som er aktuelle.

2) Hovedleverandøren er utenlandsk, underleverandørene fra samme land

Hvis leverandøren blir hindret i å levere på grunn av forhold i det landet han opererer i, kan kundens produksjon i Norge stoppe opp. I beslutningsgrunnlaget bør følgende områder undersøkes enda nøyere enn vanlig:

- Hovedleverandørens økonomiske soliditet, kompetanse/kapasitet, omdømme
- Kontraktsforhold, skal norsk retts- og forretningspraksis gjelde?

- Finnes det formelle påvirkningsmuligheter mot hovedleverandøren utenom kontrakten?
- Hvordan er forretningsforholdet mellom hovedleverandør og underleverandører formelt etablert?
- Imøtekommer den utenlandske hovedleverandøren alle de lovpålagte kravene og andre krav som norske banker er forpliktet til å etterleve? Hva med beskyttelse av intellektuelle aktiva?
- Er det tilfredsstillende teknisk infrastruktur og reserve driftssteder i de landene som leverandøren opererer i?
- Stabil strømforsyning, tilfredsstillende kommunikasjonslinjer m.m.

I visse tilfeller kan reservedriftssted i et annet land enn der IT-leverandørene opererer, være en fordel – spesielt hvis reservedriftsstedet er i Norge.

3) Hovedleverandøren er utenlandsk, leveransekjeden blir "usynlig" for kunden

Et godt eksempel på dette er Internett der ingen behøver å tenke på hvor de enkelte serverne er plassert og der oppgaver blir flyttet dit det finnes ledig kapasitet. Følgelig vil foretakets muligheter til styring i kriser bli svekket. Det vil også kunne være vanskeligere å følge opp avtalene og IT-leveransene som utkontrakteringen består av. IT-utility-modellen er et stort skritt i retning av å gjøre leveransemodellen usynlig i den forstand at oppgaven løses på ulike steder i et totalt nettverk, men som leveranse betraktet presenteres som en helhet.

Her er det viktig å skille mellom hvor supportpersonell er lokalisert og hvor maskinkapasiteten er lokalisert. Det er plasseringen av tjenesteyterne som vanligvis er viktigst fordi de må bygge opp kunnskaper om hvordan de enkelte applikasjonene oppfører seg og skal betjenes, og slik kunnskap bygges opp over tid gjennom erfaring.

Med dagens og morgendagens teknologiske løsninger kan tjenesteytere fra et geografisk sted drifte maskiner som står helt andre steder, det vil si at plasseringen av maskiner ikke lenger er så viktig, men den tekniske infrastrukturen som driften er avhengig av (strøm og telekommunikasjon), er fortsatt et viktig vurderingselement.

I finansnæringen har det skjedd og skjer stadig strukturelle endringer på IKT-området. Dette gjelder både for banker, i forsikringsforetak og i verdipapirsektoren. Alle de nevnte områdene benytter i stor grad utkontraktering for å ivareta sin IKT-virksomhet.

2.2.7 Situasjonsvurdering

I de senere årene har flere banker i Norge flyttet, eller har besluttet å flytte, store deler av sin IKT-virksomhet ut av landet. Det er ulike grunner til at dette skjer, men samlet sett har dette et betydelig omfang med de samfunnsmessige konsekvenser dette kan få.

I et nordisk perspektiv ser vi at IBM er i ferd med å få en svært sterk posisjon innen leveranser av IT-tjenester til foretak innen bank og finans. Samlet representerer dette betydelige endringer som også betyr et endret risikobilde, og gir nye utfordringer for det enkelte foretak og for myndighetene ut fra en samlet risikovurdering for det norske samfunnet og ut fra et reguleringsmessig synspunkt.

Dette er en utvikling som Kredittilsynet vil følge nøye fordi stor konsentrasjon ut fra en risikobetrakting kan være uheldig. IBM er allerede dominerende på salg av stormaskinløsninger med tilhørende programvare, og sammen med en offensiv internasjonal strategi på industrialisering av IT-driften kan dette bety store endringer på dette markedsområdet og få konsekvenser som det kan være vanskelig å overskue i dag.

Utkontraktering er et stort og veletablert område innen IT-tjenesteyting, og området er i kraftig vekst. I følge eksterne analyser utgjorde leveranser av eksterne IT-tjenester i EMEA (Europa, Midt-Østen og Afrika) i 2003 et marked på ca 194 milliarder USD. Foreløpige beregninger viser at markedet trolig vil øke med 6,3 prosent i snitt pr. år til 230 milliarder USD i 2007. I dette markedet er bank og finans det største kundesegmentet.

Etter hva Kredittilsynet har kunnet bringe på det rene, er Norge et av få land i verden hvor store deler av systemene til den finansielle IKT-virksomheten er utkontraktert ut over landegrensene. Oslo Børs, Fokus Bank, Nordea Bank Norge, SEB Kort, SEB Enskilda AS, TrygVesta Forsikring og sparebankene i Terra-Gruppen er eksempler på dette. Dette kan representere et paradoks ved økt oppmerksomhet på nasjonal infrastruktur, og dens betydning, samtidig som en stadig større del av infrastrukturen er utenfor landet. Det er derfor viktig å ha kontroll med IKT-aktiviteter av betydning for finanssektoren som foregår utenfor Norge på samme måte som for den som foregår innenfor landets grenser.

Så lenge utkontraktering foregår til naboland hvor myndighetene allerede har et nært samarbeid, vurderes risikoen å være begrenset. Det er imidlertid et spørsmål om det enkelte foretaket i Norge eller norske myndigheter har tilstrekkelig oversikt over reguleringssiden i det landet som utkontrakteringen foregår til. Det kan være reguleringsmessige forhold som er i konflikt med norsk lovgivning og som verken foretaket som utkontrakterer eller norske myndigheter har tilstrekkelig innsikt i, og kanskje enda mindre den aktuelle IT-leverandøren.

Eksempel på dette er USA hvor lovgivningen gir myndighetene rett til å få tilgang til data, for eksempel hos en IT-leverandør som kun har en leveranserolle til et finansforetak i Europa som er kunden (Dette er en aktuell situasjon i forbindelse med SWIFT-operasjonen i USA.). Et annet forhold kan være nasjonale konfidensialitetsregler som begrenser norske myndigheters mulige behov for innsikt så lenge dataene fysisk er lagret i det aktuelle landet. Et tredje forhold er hvilke muligheter norske myndigheter har for styring i en katastrofelignende situasjon som rammer kunder av finansforetaket i Norge med manglende tilgang for finansforetakets kunder og begrenset styringsrett, både for finansforetaket og norske myndigheter som resultat.

Dette er samlet forhold som innholder risikoelementer det er vanskelig å overskue i en risikoanalyse. I tilegg til utkontrakteringsavtalen vil offentlig regelverk regulere hva foretaket og norske myndigheter har av rettigheter.

2.3 Datakriminalitet rettet mot finanssektoren

Finansnæringen har i stadig økende grad blitt utsatt for svindelforsøk gjennom å utnytte svakheter i datateknologien som foretakene benytter seg av i sine løsninger. I stadig større grad ser vi at de kriminelle miljøene organiseres stadig bedre, og at personer i disse miljøene ofte er svært kvalifiserte og har høyere akademisk utdanning og til dels erfaring innen finansnæringen. Angrepene mot finansnæringen er stadig mer sofistikerte og bedre planlagt. Det er i hovedsak bruken av nettbank som har fått den aller største oppmerksomheten når det gjelder svindelforsøk. I 2007 ble det avdekket relativt komplekse organisasjoner med mange lag av bidragsytere. Ikke minst er det betenkelig at menigmann lar seg lure til å delta i kriminelle handlinger gjennom å delta i verdikjeden som pengeinnsamlere (stille konto til rådighet for kriminelle). Det at folk fremdeles lar seg lure av både Nigeria-brev og det å stille egne kontoer til rådighet for å kunne flytte penger mellom kontoer for så å eksportere pengene ut av landet til bakmennene i de kriminelle miljøene, krever at det settes inn flere mottiltak på dette området. Eksempler på dette kan være bedre generell informasjon om problemet og mer aktiv bruk av spam-filtre.

Den økende bruken av Internett som transportør av tjenestene som finansforetakene tilbyr, medfører en økende trussel. Trusselen som det primært snakkes om, er at Internett ikke lenger kan benyttes som transportør av våre finansielle tjenester. Dette gjelder både for personkundemarkedet, men også for bedriftskundegruppen. Det er grunn til å tro at de angrepene som er gjennomført mot både bank, verdipapir og andre foretak innen finansnæringen så langt er satt opp som mindre test-scenarioer siden omfanget har vært relativt begrenset. Grunnen til denne antakelsen er at det er relativt enkle tilgjengelige ressurser som er benyttet, og en kan derfor anta at forsøkene er i en tidlig start- eller testfase.

Ser en på ulike trusler innenfor datakriminalitet, representerer angrep mot telekommunikasjonsleverandører de største utfordringene i tiden som kommer. En ser ut i fra erfaringer både i Norge og i andre land at angrep i stor grad er rettet mot utstyr som er en del av finansnæringens tjenesteleveranse via Internett. Dette er en utvikling som antas å øke, siden flere og flere tjenester tilbys gjennom internettbaserte selvbetjeningsløsninger.

Mange land som ligger i forkant av å ta i bruk hensiktsmessige sikkerhetsløsninger har likevel erfart omfattende svindelforsøk. Årsaken kan bero i at det i de samme landene er store volumer på bruk av slike tjenester og høy prosent av befolkningen som benytter tjenestene.

Den økte bruken av åpne nettverk i foretakenes distribusjonsnett av tjenester, øker også den eksterne

trusselen. Dette gjelder selvfølgelig ikke bare bruk av nettbank, men også for alle andre tjenester som tilbys via Internett. De eksterne truslene er i hovedsak organisert og gjennomført av etablerte kriminelle grupper. Internett er hovedredskapen som disse gruppene bruker for å få tilgang inn i foretakenes systemer. Så langt er det få angrep fra kriminelle grupper som går direkte mot finansforetakene. Det er fortsatt slik at det er sluttbrukerne som kompromitteres, og de kriminelle benytter sluttbrukernes tilganger for å gjennomføre kriminelle handlinger. I 2007 kunne en se en stadig forbedring i organiseringen av de aktivitetene som de kriminelle grupperingene gjennomførte. Særlig gjaldt det verving av bankkunder til å stille sine kontoer til disposisjon for å få penger overført til seg for så å ta disse pengene fra kontoen og sende pengene til en på forhånd avtalt konto utenfor Norge. Vervingen skjer i hovedsak via Internett, enten som phishing, spam-post eller via et nettsted som er satt opp spesielt med verving som hovedformål. Det at norske forbrukere tilsynelatende ikke er klar over at oppgaven de påtar seg er en del av kriminell virksomhet, gir grunn til bekymring.

3 Kilder og informasjonsbearbeiding

Grunnlaget for ROS-analysen er som tidligere år kunnskap og informasjon Kredittilsynet får gjennom sine IT-tilsyn, intervjuer med sentrale aktører, rapporter om IKT-hendelser og oppfølging av meldeplikten for systemer for betalingstjenester. I tillegg er informasjon fra nasjonale og internasjonale organisasjoner og virksomheter viktige bidrag til denne ROS-analysen. I kapittel 5 blir de største risikoene drøftet nærmere.

3.1 Viktige funn fra IT-tilsyn

I 2007 ble det gjennomført 20 stedlige IT-tilsyn. I tillegg var det 35 foretak som i forbindelse med ordinær inspeksjon leverte egenevalueringsskjema for foretakets IT-virksomhet og ble vurdert i henhold til prosedyre for forenklet IT-tilsyn.

I løpet av fem år med stor tilsynsaktivitet har alle større foretak og mange mindre foretak vært gjenstand for en eller flere IT-inspeksjoner. Gjennom disse har Kredittilsynet opparbeidet betydelig erfaring med stedlige IT-tilsyn, og vi kan observere en utvikling i hvordan foretakene organiserer IT-virksomheten. IKT-forskriften er nå vel kjent i finansnæringen, og foretakene kan i stadig større grad vise til prosesser som understøtter kravene i forskriften. Samtidig skjer det uheldige hendelser på IT-området i finansnæringen som enkelte ganger er forbausende lite forutsett tatt i betrakting gjennomføring av ROS-analyser og andre forebyggende tiltak. Dette er hendelser som kunne vært unngått hvis relativt enkle forebyggende tiltak hadde blitt iverksatt. Etablerte og dokumenterte prosesser er ikke alltid nok. Prosessene må være under konstant evaluering og forbedring, og ikke minst, de må gjennomføres.

3.1.1 Noen funn fra IT-tilsyn i 2007

Følgende er viktige funn fra IT-tilsynene som ble gjennomført i 2007:

- Manglende eller ufullstendige ROS-analyser.
- Kompetanse til gjennomføring av ROS-analyser er et gjennomgående problem.
- Manglende styring og kontroll ved gjennomføring av større IT-prosjekter.

- Fortsatt problemer knyttet til endringshåndtering, samt for dårlig grunnlag ved beslutning om å iverksette drift av nye løsninger.
- Mer oppmerksomhet må rettes mot infrastruktur og felles løsninger – kompetansen i det enkelte foretaket kan svekkes når oppgaver ivaretas utenfor foretaket.
- Problematisk å opprettholde tilstrekkelig nøkkelkompetanse ved utkontraktering og på områder med manglende industristandarder.
- Mangelfulle prosessbeskrivelser og dokumentasjon i foretak med stor grad av egenutvikling.
- Ikke tilstrekkelig kontroll med og test av katastrofeløsninger.

Nedenfor utdypes noen av disse områdene nærmere.

3.1.1.1 IT-tilsyn i større foretak – utilstrekkelige ROS-analyser

Ved generelle IT-tilsyn av større foretak kan det være en utfordring å få konstatert den nødvendige forståelsen av IT-virksomheten. Selv om foretaket kan vise til implementerte IT-prosesser, kan disse være for overordnede og lite detaljerte. Det kan vise seg at prosessene mangler forankring i de operasjonelle delene av organisasjonen. Et område med varierende kvalitet i de større foretakene, er gjennomføring av risikoanalyser. Enten foretaket er stort eller lite, forretningsområdene mange eller få, må risikoanalyser alltid gjøres på et detaljeringsnivå som sikrer at sårbarheter blir avdekket og trusler og tiltak identifisert. I et større foretak må dette nødvendigvis føre til at omfanget av risikoanalyser blir stort og i prinsippet proporsjonalt med størrelsen på foretaket.

3.1.1.2 Innkontraktering av IT-kompetanse

Som eksempler på en motstrøm til hovedstrømmen når det gjelder utkontraktering, så Kredittilsynet i 2007 eksempler på foretak som justerte IT-strategien i retning av å ta tilbake områder av IT-virksomheten som hadde vært utkontraktert. Misnøye med leverandøravtaler grunnet manglende muligheter for innsikt og dyre reforhandlinger lå bak disse beslutningene. I 2007 fikk tilsynet bekreftet dette bildet, og spesielt gjelder dette forsikringsområdet. Her er det mange regelendringer og nye produkter som fører til stadig behov for videreutvikling, som igjen fører til at avtaler med leverandører må reforhandles. Bransjen har ikke tradisjon for fellesløsninger på samme måte som bank, og hvert selskap håndterer egen systemportefølje. Det er en tendens til at flere av forsikringsselskapene dreier IT-løsningene over på teknologiske plattformer som i større grad kan driftes og forvaltes med egen kompetanse for slik å sikre bedre kontroll med IT-virksomheten.

3.1.1.3 Lav modenhet på bruk av IKT

Ennå finnes det finansforetak som utvikler programvaren selv, drifter selv og ikke baserer seg på noen form for utkontraktering. Kredittilsynet hadde i 2007 flere IT-tilsyn i foretak som opererer IT-virksomheten på denne måten. Typisk for disse foretakene er at det operasjonelle står i hovedsetet. Foretakene har oppmerksomheten rettet mot rask tilpasning av applikasjonene, og det er ofte nært slektskap mellom utvikling, drift og brukerstøtte. Foretakene er effektive og kan ofte vise til høy brukertilfredshet, blant annet fordi det er færre hierarkier, noe som gjør det enkelt for brukere å kommunisere innenfor foretaket. Kvaliteten på dokumentasjon og rutinebeskrivelser er ikke like god. Reelle rutiner ligger ofte foran dokumenterte rutiner. Dette kan gjelde risikoanalyse, endrings- og

avvikshåndtering eller kontinuitets- og katastrofeplanlegging. Ofte har foretaket etablert rutiner som blir benyttet, men som ikke er systematisert og dokumentert på en ordentlig måte. Problemet synliggjøres i sterkere grad når foretakene vokser. Det er grenser for hvor lenge et foretak kan klare seg uten dokumenterte prosesser. Samtidig sikrer foretak som håndterer IT-virksomheten selv, kontroll og styring i en helt annen grad enn foretak som er prisgitt en eller flere leverandører. Etter Kredittilsynets vurdering er det ingen motsetning mellom å operere IT-virksomheten i eget hus og å ha IT-prosesser som kvalitetsmessig holder mål og skalerer i forhold til vekst i virksomheten.

3.2 Bruk av intervjuer

Det ble i 2007 gjennomført ni intervjuer med nøkkelpersoner i sentrale finansforetak, hovedsakelig med personer som representerer IKT-området. Erfaringer med å gjennomføre denne typen intervjuer, er at det gir et godt bilde av hva foretaket vurderer som de største utfordringene og risikoene på IKT-området. Spesielt godt fungerer intervjuene i foretak der intervjuene har fått en regularitet gjennom årlige samtaler.

En nærmere bearbeiding av resultatene viser følgende hovedtrekk relatert til svarene på de enkelte spørsmålene:

1) Hva ser foretaket som den/de største risikoen/e ved foretakets bruk av IKT?

- Stadig større eksponering mot Internett
- Økt bruk av bærbart datautstyr
- Manglende eller dårlige prosjektprosesser
- Stor utfordring å få tak i tilstrekkelig og riktig kompetanse, slitasje på IT-organisasjonen
- Vanskelig å oppfylle stadig større krav til nøyaktighet ved driftssetting av nye eller endrede løsninger
- Ikke tilstrekkelig kontroll på IT-tjenesteleverandører
- Manglende sikring av sensitive data

2) Hva har vært de største problemene knyttet til IKT-området i 2007?

- Driftsproblemer, særlig knyttet til nettbank
- Kvalitet på endringshåndtering
- Stadig mer avanserte phishing-angrep der avansert ”social engineering” tas i bruk
- Driftsforstyrrelser i sentral teknisk infrastruktur og særlig telekommunikasjonsleveranser
- Stadig økte krav til sluttbrukernes kunnskap og datautstyr

3) Hva er grunnlaget for å kunne identifisere dette?

- Hendelsesrapportering
- Risikostyring
- Forbedret regime for styring og kontroll
- Årvåkne kunder

4) Hva ser foretaket på som de største utfordringene i 2008 mht. risiko ved bruk av IKT?

- Sikre at løsninger testes i et tilstrekkelig omfang før de settes i produksjon
- Opparbeide seg tilstrekkelig kunnskap og kompetanse rundt ny teknologi og nye løsninger
- "Zero day exploits"[11]
- Etablere prosesser som sikrer at håndteringen av en uønsket hendelse følger rutinen for problem endringshåndtering og spiller sammen for å kunne opprettholde kvalitet og sikkerhet på løsninger som er under press
- Opplæring av brukere, både teknisk og holdningsmessig
- Økt bruk av bærbare PC-er internt i foretakene fordrer bedre sikkerhetsløsninger
- Etterlevelse av myndighetskrav

5) Hva ser foretaket på som viktige problemstillinger mht. IKT-risikoen i 2008 hvor det kreves iverksatt egne tiltak?

- Gjennomføring av stadige organisasjonsmessige endringer
- Konsentrasjonsrisiko på fellesløsninger
- Ny kjerneløsning
- Nytt oppgjørssystem
- Nytt avregningssystem
- Kontinuitets- og beredskapsløsninger for tjenestenektangrep (DDoS-angrep)[12]
- Sikring av teknisk infrastruktur og særlig telekommunikasjon
- Innføring av ny teknologi

[11] "Zero day exploits": Hackere utnytter tidsvinduet fra introduksjon av ondsinnet kode som kan angripe hull i programvare og til det er laget fix (patch) som tetter hullet. Maskiner med aktuell programvare er sårbare i denne perioden.
[12] Distributed Denial of Service, distribuert tjenestenekt.

3.3 Registrering av hendelser

3.3.1 Rapportering av hendelser til Kredittilsynet

Kredittilsynet skrev om temaet *manglende hendelsesrapportering* i ROS-analysen både for 2005 og 2006. I 2007 ble det etablert en frivillig rapporteringsrutine for hendelser i rundskriv 31/2007 "Rapportering av IKT-hendingar til Kredittilsynet". Rapporteringsrutinen gjelder anbefalt for banker, VPS, Oslo Børs og BBS.

Bak iverksettelsen av hendelsesrapporteringen ligger et langvarig forarbeid. Blant annet har det tatt tid å vurdere hvilke hendelser som bør rapporteres. I 2006 ble det gjennomført en undersøkelse som viste et stort sprik i måten bankene kategoriserer alvorlighetsgraden av hendelser på, noe som bekreftet hvor vanskelig det er å lage en generell beskrivelse av hvilke hendelser som bør rapporteres.

Rapporteringsrutinen er en prøveordning som skal evalueres etter 12 måneder. Da vil vi kunne se om nivået på hendelsesrapporteringen virker fornuftig.

Kredittilsynet har tilrettelagt et analyseverktøy for å registrere informasjon om hendelser. Verktøyet er benyttet fra våren 2007 til å registrere alle kjente hendelser. Allerede første måneden etter at rapporteringsrutinen ble iverksatt, var antall hendelser Kredittilsynet fikk informasjon om, betydelig større enn før rutinen ble etablert, og det kan spores sammenhenger mellom hendelsene som blir rapportert. Flere foretak rapporterer om det som bunner i samme hendelse hos felles leverandør. Dette gir merverdi til en felles rapporteringsrutine.

3.3.2 Hendelser i 2007

Virusangrep

Mediene omtalte i 2007 et virusangrep som var rettet mot en av de større bankene. Viruset infiserte både arbeidsstasjoner og servere og lammet store deler av bankens virksomhet de første dagene i mars 2007. Av ulike grunner ble ikke viruset gjenkjent av antivirusprogramvaren, og det slapp igjennom antiviruskontrollen. Da viruset først hadde passert ett punkt i bankens nettverk, spredde det seg i hele det interne nettverket og forårsaket at banken til de grader ble satt ut av spill. Store ressurser er siden satt inn på å styrke antivirusberedskap og andre tiltak for å forebygge en lignende situasjon.

Ondsinnede angrep mot nettbankkunder

Også i 2007, og spesielt i begynnelsen av året, var det samme type ondsinnede angrep mot nettbankkunder som det var på slutten av 2006 og som ble omtalt i ROS-analysen for 2006. Brukers PC ble infisert med ondsinnet kode, og falske transaksjoner ble produsert til kontonummer som blant annet mellommenn hadde stilt til disposisjon. Gjennom ulike tiltak har bankene i større grad klart å

avdekke slike falske transaksjoner før de blir gjennomført. Få av forsøkene har vært vellykket, og ennå har ingen norske kunder tapt penger. Måten disse angrepene gjennomføres på, avdekker imidlertid planlegging og oppfølging på et meget profesjonelt nivå. Velorganiserte aktører med et velsmurt driftsapparat står bak. Angrepene varsler om at organisasjonene som står bak har "muskler" til nye typer ondsinnede angrep i fremtiden.

Manglende tilgjengelighet til tjenester i nettbanken

En type hendelser Kredittilsynet blir gjort oppmerksom på oftere gjennom mediene enn gjennom melding fra foretaket, er manglende tilgjengelighet til nettbank. Bankene tilbyr en nettbanktjeneste som skal ha høy tilgjengelighet. Publikum reagerer raskt når dette ikke er tilfelle. Spesielt merkes det der nettbanken er inngangsport til verdipapirhandel hvor tidsmarginene for endringer i aksjeverdiene kan være små. I 2007 har det vært mange klager fra publikum på manglende og ustabil tilgang til enkelte av de store nettbankene som tilbyr nettbasert verdipapirhandel. Enkelte kunder har i denne forbindelse sett det nødvendig å opprette egen reserveløsning i form av kundeforhold hos flere nettmeglere.

Tjenestenektangrep

I 2007 fikk Kredittilsynet rapport om et vellykket tjenestenektangrep mot et større norsk finansforetak. Det var et Distributed Denial of Service (DDoS)-angrep fra et botnett[13] som besto av ca. 45 000 fjernstyrte PC-er i 65 land. Dette var altså et massivt angrep hvor det kan nevnes at teleleverandøren i løpet av én time stoppet tre milliarder enkeltangrep. Foretakets nettsted ble lammet. Denne gangen var det en sluttet brukergruppe som benyttet tjenestene fra foretakets nettsted. Foretaket kunne derfor nå ut med informasjon til dem som ble rammet om bruk av alternativt nettsted. Selve DDoS-angrepet pågikk i over en måned. Det var også et mindre foretak som ble utsatt for samme angrep.

Avanserte phishing-angrep

I 2007 var det eksempler på avanserte phishing-angrep. Betegnelsen phishing-angrep brukes fordi angriperne på ulike måter skaffet seg forhåndskunnskap om offeret (kontohaveren) som de siden bruker til å utgi seg for å være offeret. Typisk for disse angrepene er at klassisk bedrageri kombineres med bruk av elektroniske tjenestekanaler. Aktuelle scenarioer er at bedrageren ringer kundesenteret i banken og utgir seg for å være kunden, og bedrageren ringer kunden og utgir seg for å være kundesenteret i banken. Bedrageren bestiller adresseendring, telefonendring eller kode-kalkulator i offerets navn. Gradvis får bedrageren samlet så mye informasjon om offeret at en falsk transaksjon kan gjennomføres. I 2007 ble svindelen i noen tilfeller oppdaget av observante medarbeidere i bankens

[13] Botnet: Et nettverk av PC-er som er infisert av ondsinnet kode som gjør at PC-ene kan fjernstyres av en hacker. Via vedlegg til e-post eller nedlasting fra Internett, har brukeren fått PC-en infisert. Mange av dagens PC-er er kraftige og ofte konstant oppkoblet til nettet ved hjelp av bredbåndaksess. Under kommando av en hacker, kan et botnet brukes i et større angrep mot annen infrastruktur på Internett.

kundesenter. Andre ganger gikk svindelen gjennom og ble oppdaget av kunden først i ettertid.

Brannen på Oslo S

Den 28. november 2007 brant det i kabelnettet på Oslo S. Dette medførte at BaneTeles bredbåndstrafikk ble utilgjengelig for en rekke kunder. Hendelsen rammet mange foretak i finanssektoren. Mest berørt var en del meglerhus der virkningen på kundetjenestene var umiddelbar med utilgjengelige handelssystemer. Hendelsen avdekket at det foretakene trodde var redundante løsninger, viste seg ikke å være redundante fordi kablene fysisk gikk i de samme traseene. BaneTele hadde 490 kunder og sluttkunder som ble berørt av hendelsen, og flere av disse var operatørkunder som igjen hadde egne sluttkunder. Hendelsen viste at manglende innsikt i og informasjon om innholdet i leveranser fra underleverandører kan bety en operasjonell risiko for finansforetakene, og at testing av kontinuitetsløsninger er av vesentlig betydning for å verifisere at løsningene fungerer.

3.4 Systemer for betalingstjenester

Kredittilsynets arbeid med meldeplikten for systemer for betalingstjenester representerer også en viktig kilde til informasjon til arbeidet med ROS-analysen. I lov om betalingssystemer er begrepet ”systemer for betalingstjenester” benyttet på systemer som ivaretar transport av transaksjoner/meldinger fra kunde til bank og den funksjonaliteten som er nødvendig for å understøtte at dette foregår på en betryggende måte. Eksempler er nettbankløsninger, minibankløsninger og brukerstedsløsninger for betalingskort.

Generelt sett kan en definere et betalingssystem delvis 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, og transaksjoner mellom private kunder, et system for betalingstjenester (kunde og bank). Ny teknologi har i særdeles grad påvirket systemene for betalingstjenester de seneste årene, hvor kostnadseffektiv drift, brukervennlighet og sikkerhet har vært sentrale elementer.

Moderne betalingssystemer anvender IKT-systemer i alle ledd, og i mange sammenhenger er det vanskelig å skille mellom betalingssystemenes enkelte tjenester og IKT-funksjonen isolert sett. For å markere en forskjell mellom disse, kan det være relevant å definere betalingstjenester som anvendt IKT. IKT utgjør dermed den fysiske infrastrukturen i betalingssystemene, mens betalingstjenestene utgjør de aktuelle ulike meldingstypene som transporteres gjennom den digitaliserte fysiske infrastrukturen.

Med økt bruk av IKT øker også kompleksiteten i utførelsen av betalingstjenestene. Gjennomføringen av betalingstransaksjonene i de ulike betalingssystemene er sammensatt av ulike tjenester fra en rekke

underleverandører som hver for seg er kritiske aktører for at transaksjonsstrømmene skal fungere feilfritt i et sømløst nettverk.

En stor del av den digitaliserte infrastrukturen er allerede utkontraktert til selvstendige IKT-driftsselskap med egne planer og mål. Selv om finansnæringen har gjennomført slik utkontraktering i stor grad, er det viktig å holde fast ved at ansvaret for betalingssystemene og betalingstjenestene alltid vil ligge tilbake hos de institusjonene som har konsesjon til å drive betalingsformidling.

Ved økt kompleksitet i betalingssystemene og i de enkelte betalingstjenestene, øker også risikoen for feil. For å styre og kontrollere slike risikoer, har myndighetene etablert et lovmessig rammeverk under lov om betalingssystemer. Loven forvaltes tilsynsmessig av Norges Bank når det gjelder interbanksystem og av Kredittilsynet når det gjelder systemer for betalingstjenester. I praksis er det vanskelig å skille disse to hovedsystemene fra hverandre fordi at de sammen danner hele den finansielle leverandørkjeden hvor systemene er komplementære og gjensidig avhengige. Det er derfor etablert et nært samarbeid mellom Norges Bank og Kredittilsynet slik at tilsynsansvaret kan utøves mest mulig effektivt og sikkert.

Kredittilsynet økte i 2007 kapasiteten og kompetansen på området betalingssystemer. Målsettingen er å legge større vekt på tiltak relatert til lov om betalingssystemer, og samtidig øke den løpende kontakten med institusjoner som har konsesjon til å drive betalingsformidling. Oppfølging av meldeplikten er et viktig virkemiddel i dette arbeidet som kan avdekke mangler ved etablering av nye systemer for betalingstjenester.

Betalingssystemer i Norge er under stadig påvirkning av økt internasjonal aktivitet innen standardisering og tilpasning til EU/EØS-direktiv. I særdeleshet gjelder dette utviklingen innen SEPA (Single European Payment Area) hvor harmonisering av betalingstjenester i euro over landegrensene står sentralt, samt de forslagene som er inkludert i Betalingsdirektivet. Spesielt åpner direktivet for en ny gruppe betalingsinstitusjoner ved siden av de som i dag kan få konsesjon. Dette direktivet skal være gjennomført innen 1. november 2009.

3.5 Risikoområder identifisert av andre

3.5.1 Samfunnet blir mer avhengig av Internett, og tjenestene på Internett blir mer integrert

Det er et stadig større tilbud av finansielle tjenester på Internett, og bruken av disse øker sterkt. Økt bruk gir økt avhengighet av Internett, og samfunnet vil i mindre grad tåle avbrudd og feil. Finansielle tjenester knyttes sammen med relaterte tjenester. Begreper som ”one stop shopping” og ”straight through processing” gir uttrykk for systemer der alle konsekvenser og handlinger forbundet

med et forretningstilfelle, alt fra lageroppdatering til kundens betalinger, skjer i sanntid. Systemet oppfattes som ett system av brukeren, selv om mange foretak, datasystemer og datanettverk er involvert. Teknisk sett blir tjenestene mer og mer integrert. Feil i ett ledd gjør at brukeren ikke får gjennomført forretningen.

Stadig flere foretak drifter styrings- og produksjonssystemer over Internett. Lagerinformasjon, ordreinformasjon m.m., samles inn via Internett fra foretakets ulike forretningssteder og er styrende for produksjonsprosesser. Se omtale av dette i NOU 2006: 6 *Når sikkerhet er viktigst.*

Økt integrasjon gir økt sårbarhet og økt behov for sikring i alle ledd. Det er en særskilt utfordring å plassere ansvaret samt å utøve dette.

Internett er et åpent nett, i det vesentlige uorganisert og under stadige angrep. I og med at systemene og nettverkene er integrerte, kan skadelig programvare smitte og lamme store deler av den kritiske samfunnsinfrastrukturen.

Det er vanlig å dele inn prosesser i sikkerhetssoner, og å sette opp kontroller i sonegrensene, jf. brannmur, "Intrusion Detection-systemer" m.m. I og med at prosessene etter hvert er tett integrert, er det vanskelig å soneinndele prosessene ettersom det ikke er noen naturlige sonegrenser. Hele prosessen utgjør sonen, og sonen inkluderer altså et usikret, åpent ledd, nemlig Internett.

I 2007 så Kredittilsynet mange tilfeller der viktige forretningsprosesser var utilgjengelige som følge av skadevoldende handlinger på Internett eller som følge av rene ulykker. Samfunnskritiske infrastruktur som for eksempel betalingsformidling var i flere tilfeller lammet i lengre perioder som følge av angrep mot infrastrukturen eller feil i infrastrukturelementer.

En gjennomgående observasjon i 2007 er at det i praksis mangler en instans som erkjenner et totalansvar for å sikre hele prosessen, ende til ende. Den som leverer sluttbrukertjenesten, har mangelfull kunnskap om risiko i de ulike leddene. De mange instansene som er involvert, vet å begrense ansvaret til sin egen, avgrensede del av leveransen inn til prosessen. Det er mangel på totalansvar og oversikt, noe som må anses som en risiko.

3.5.2 Sårbarhet i protokoller og programvare øker

Utbudet av programvare øker, funksjonaliteten i programvaren blir stadig rikere og feil og mangler øker.

Mange programvarehus sliter med å levere til avtalt tid, og til avtalt kostnad og kvalitet. Vi vet at store programvarehus har som forretningsfilosofi å levere til avtalt tid og kostnad. Kvaliteten kommer senere i form av oppgraderinger som utbedrer feil – feil som brukere har avdekket og informert leverandøren om. Det er et økende omfang av svakheter i programvaren som kan utnyttes i skade- eller

bedragerihensikt. Det kan synes som om programvarehusene overlater deler av testing og "herding" til brukerne.

En stor internasjonal undersøkelse[14] konstaterer at tallet på nyoppdagede sårbarheter i programvare fortsatt er svært høyt, 3 400 i første halvår 2007, men at dette tallet for første gang siden 2003 er lavere enn i halvåret før. Utviklingen viser at sårbarhetene som ble oppdaget i første halvår i 2007, jevnt over er mer kritiske, og enklere for kriminelle å utnytte enn tidligere.

En enkel analyse av oppgraderinger fra to store programvarehus, viser at over 70 prosent av publiserte oppdateringer går på å tette sikkerhetshull.

Kredittilsynet observerte i 2007 en rekke tilfeller der personer hadde utnyttet svakheter i programvare som bankens standardtilbud på Internett benytter seg av, og på denne måten uberettiget forsøkte å få tilgang til midler.

3.5.3 Lover, lovvalg og annet regelverk holder ikke tritt med utviklingen i teknologi og i globaliseringen

Internett er i sin natur grenseløst. En rekke bestemmelser i norsk lov er knyttet til landet "… der foretaket har sin virksomhet …" eller "… der virksomheten skjer …". Disse og lignende formuleringer er svært vanskelige å forholde seg til i et grenseløst internettsamfunn.

Denne problemstillingen var relevant flere ganger i 2007. Ett tilfelle gjaldt et finansforetak hvor e-postkorrespondanse fra alle ansatte oppbevares på en server utenfor Norge. Det norske foretaket fikk ikke tilgang til e-postinformasjon som gjaldt egne ansatte under henvisning til at oppbevaringslandets lover ikke hjemlet slikt innsyn. En annen aktuell sak i 2007 gjaldt et foretak der medarbeidere, fra terminaler i Norge, registrerte bilag mot en server i utlandet. De registrerte bilagene og regnskapsdokumentasjonen for øvrig ble lagret på serveren i utlandet. Spørsmålet gjaldt om det skulle gis dispensasjon til å kunne lagre regnskapsdokumentasjon utenfor Norge. Vurdering av viktigheten av virksomheten ut fra en nasjonal betraktning, samt behovet for tilgang til opplysninger for norske myndigheter, er viktige elementer. Likeledes om de forutsetningene som stilles til slik dispensasjon i praksis er mulig å etterleve når problemer oppstår etter lang tid, og tidsaspektet for å få tilgang til opplysningene er viktig.

Internett gir en rekke utfordringer når det gjelder jurisdiksjon og lovanvendelse.[15] EUs databasedirektiv gir støtte til vurderingen av jurisdiksjon og lovanvendelse innenfor visse rettsforhold og avgrenset til EU. Men ofte etablerer en virksomhet seg der lovgivningen er minst "truende". Med Internetts grenseløse natur, er markedet det samme, uansett etableringsland.

[14] http://download.microsoft.com/download/a/a/1/aa1ac20e-514e-4ec1-a12e-022c35aa54cf/MS_Security_Report_Jan-Jun07.pdf (mars 2008)
[15] http://www.jus.uio.no/iri/gmlforskning/lib/rapporter/elektronisk_marked/juridiksjon.html#6 (mars 2008)

3.5.4 Utilstrekkelig sikkerhet hos sluttbruker en stadig økende risiko

Mangler og svakheter i programvare kan utnyttes i skadehensikt. De såkalte "Zero day exploits" utnytter tidsvinduet mellom introduksjon av ondsinnet kode og tiltaket som blir satt inn for å bekjempe den ondsinnede koden. Maskiner som er angrepet, er
sårbare i denne perioden.

Hackerutviklere tester den ondsinnede kodens resistens mot antivirus-programvare. På denne måten er hackeren rimelig sikker på at den ondsinnede koden vil ha en viss levetid.

Mange brukere har ikke oppdatert antivirus, brannmur mv. Men selv den mest oppdaterte PC, er altså ikke nødvendigvis beskyttet mot de nyeste angrepene.

De fleste PC-er som ble misbrukt i 2007, viste seg å ha svak sikring. Svak sikring har gjort det mulig for forbrytere å installere ondsinnet kode. Dette kan være kode som for eksempel leser av elektroniske identitetskjennetegn (koder til bank mv.) som offeret taster inn, eller som kopierer og overfører annen informasjon fra offerets PC.

Det må forventes at denne type kriminalitet vil øke fremover. Finansinstitusjoner må følge utviklingen nøye og ha mottiltak i beredskap. Kredittilsynet må påse at institusjonene vurderer risikoen på en adekvat måte. Institusjonene må være forberedt for en situasjon der de blir utsatt for et massivt angrep som gjør at nettjenestene må lukkes for en lengre periode.

3.5.5 Økning i bruk av trådløse og mobile nettverk og tjenester

Bærbare PC-er stjeles, og viktig/sensitiv informasjon går tapt. I Oslo gjenglemmes daglig omkring ti mobiltelefoner i taxier og en bærbar PC hver uke.[16] Mobiltelefonene kan programmeres og er langt på vei utsatt for de samme truslene som datamaskiner. De forholder seg til mange protokoller.

Brukte mobiltelefoner og datamaskiner inneholder konfidensiell informasjon, informasjon som i mange tilfeller den nye eieren "arver" eller som kommer på avveie i overgangen mellom gammel og ny eier.

Internettkafeer benyttes i stadig større grad. Som regel vet ikke brukeren om maskinen er sikret, for eksempel mot ondsinnet programvare som kan medføre at konfidensiell informasjon som kredittkort- og bankkortdetaljer kommer på avveie.

[16] http://www.jpr.no/archive.php?subaction=showfull&id=1164698882&archive=&start_from=&ucat=2& (mars 2008)

3.5.6 Internettkriminalitet er økende med egne markedsplasser

Økte utfordringer innenfor sikring og tilgjengelighet av tjenester på Internett oppstår samtidig som det skjer en profesjonalisering av det kriminelle miljøet. Tidligere dreide det seg ofte om "guttestreker" i form av enkle "hack", men de siste to årene har det skjedd en vesentlig profesjonalisering av kriminalitet knyttet til Internett. Det eksisterer nå tilsynelatende velorganisert markeder der det omsettes programvare og informasjon som kan benyttes i bedragersk hensikt. Identitetsinformasjon, kredittkortinformasjon mv. er blitt hyllevare. Prislister eksisterer der informasjonen har veiledende priser og volumrabatter.

Sikkerhetsselskapene rapporterte om dette i 2007.[17] Det dreier seg om avansert programvare og "big business". Det omfatter store beløp, og penger som gjør at de kriminelle får tilført ytterligere ressurser.

3.5.7 Identitetstyveri

Identitetstyveri der offerets digitale identitetskjennetegn kommer på avveie og blir misbrukt, er en alvorlig trussel som øker i omfang. En omfattende internasjonal undersøkelse[18] konkluderer med at ID-tyveri er det primære målet for kriminelle hackere.

Utviklingen viser en faretruende sterk økning. Som eksempel viser vi til en undersøkelse foretatt av APACS.[19]

Number of phishing incidents* targeted against UK banks and building societies by month 2005-2006

	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec
2006	606	669	1,074	947	919	872	970	1,484	1,513	1,596	1,993	1,513
2005	18	29	27	54	72	122	153	160	190	267	255	353

Vi må forvente at identitetstyverier vil øke i omfang i tiden fremover.

3.5.8 Angrep mot domenenavnsystemet

Domenenavnsystemet (DNS)[20] utgjør koblingssentralen i internettrafikken. Domenedata må ha høy grad av integritetsbeskyttelse. Uten slik beskyttelse kan nettsteder bli offer for såkalt pharming, det vil

[17] http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf (mars 2008)
[18] http://download.microsoft.com/download/a/a/1/aa1ac20e-514e-4ec1-a12e-022c35aa54cf/MS_Security_Report_Jan-Jun07.pdf (mars 2008)
[19] Association for Payment Clearing Services, Storbritannia.

si at trafikk som var ment for nettstedet, blir rutet til et annet nettsted der sensitiv trafikk avleses og misbrukes. Det er viktig at programvaren på domenenavnservere inneholder de siste sikkerhetsoppgraderingene.

Med de eksisterende tekniske løsningene kan ingen garantere at DNS-informasjonen som overføres er ekte eller kommer fra rett kilde. Internet Engineering Task Force (IETF) har arbeidet med å utvikle en standard for sikker DNS (DNSSEC). Standarden er nå vedtatt, noe som baner veien for en systematisk adopsjon av denne.

3.5.9 Kortsvindel

Magnetstripen på kortet inneholder informasjon som kan misbrukes. Informasjonen kan avleses med enkle midler. På enkelte brukersteder er den avleste informasjonen tilstrekkelig til at svindleren får gjennomført kjøp. I andre tilfeller lurer svindleren til seg PIN-koden også. Svindleren kan da produsere et kort og misbruke dette i butikker og minibanker. Kredittilsynet har avgitt en egen vurdering av dette i brev til Banklagenemnda datert 20. januar 2008. Brevet er tilgjengelig på Kredittilsynets nettsted.[21].

Dette er årsaken til at flere og flere land går over til bruk av chip. Informasjonen i chip-en lar seg ikke kopiere like enkelt. Om PIN-koden blir stjålet, er svindleren likevel ikke i stand til å kopiere innholdet i chip-en. Introduksjon av chip har medført at det internasjonalt har vært en betydelig reduksjon i svindel på brukersteder som krever at brukeren bruker kortet.

Brukersteder der kunden ikke behøver å bruke kortet, men en kunde oppgir informasjon fra kortet, opplever økt svindel. Dette er bakgrunnen for at flere og flere brukersteder på nettet krever at kunden identifiserer seg på sikker måte, jf. for eksempel Verified By Visa, og MasterCard SecureCode.

For 2007 er det rapportert om en årlig økning i svindel knyttet til internetthandel/e-handel med engelske kort på 32 prosent.[22]

3.5.10 Mangel på redundans i nasjonal og internasjonal infrastruktur

I dagliglivet forutsettes det at de elektroniske motorveiene er tilgjengelige til enhver tid. Samfunnet synes å leve på en illusjon om at det finnes nødløsninger og redundans i denne viktige nasjonale infrastrukturen.

[20] http://www.pts.se/Archive/Documents/SE/strategi_sakrare_internet_2006_12.pdf (mars 2008)
[21] http://www.kredittilsynet.no/wbch3.exe?ce=19907 (mars 2008)
[22] http://www.apacs.org.uk/resources_publications/documents/FraudtheFacts2007.pdf (mars 2008)

Avbruddshendelser som fant sted i 2007, kan tyde på at infrastrukturen er mer sårbar og mindre redundant enn vi antar. Tre alvorlige hendelser[23] i 2007 satte deler av viktig infrastruktur ut av drift. Utsagn fra berørte parter tyder på at det i alle de tre tilfellene var forutsatt at nødløsninger var på plass og at disse ville tre i kraft. I ingen av tilfellene var det nødløsninger som fungerte.

Det er urovekkende at reserveløsninger som forutsettes å være virksomme enten ikke eksisterer, eller ikke fungerer som forutsatt. På nasjonalt nivå er dette alvorlig. På internasjonalt nivå kan det være katastrofalt, for eksempel dersom en av de oversjøiske internettkablene skulle ryke, dette desto mer som utkontraktering over landegrensene brer om seg.

Hendelsene i 2007 indikerer et behov for å kartlegge graden av redundans, inkludert reserveløsninger, i den nasjonale infrastrukturen.

3.5.11 Ondsinnet sabotasje

IT-spesialister innenfor og utenfor en virksomhet kan komme i en situasjon der de har stor kunnskap om systemer og vidtrekkende rettigheter i systemer. Spesialistene har fullmakter som gjør dem i stand til å lamme en virksomhet.

Dersom spesialisten er en medarbeider i virksomheten, kan hun benytte sin makt til å få gjennom egne krav. "Gå sakte"-aksjon kan være en måte å markere krav på og konsekvensen ved ikke å innfri kravene.

Omstrukturering og nedbemanning kan gjøre at medarbeidere ønsker å hevne seg på sin arbeidsgiver. Ofte er det mulig å legge igjen skadelig kode som blir virksom i fremtiden og som legger igjen få spor som kunne lede til gjerningspersonen. Spesialister utenfor virksomheten kan ha fått tilgang til IT-systemene, og presser virksomheten for penger, se for øvrig omtale i kapittel 3.5.12.

Flere store foretak fant i 2007 grunn til å undersøke trusselen.[24] Det har vært flere tilfeller av sabotasje, og konsekvensene er svært store. Vi tror at omfanget er større enn rapportert og at problemet kommer til å øke i fremtiden.

[23] http://www.digi.no/tele/kommunikasjon/kabelbrudd+hos+telenor+rammer+telemark/art395063.html ; http://www.ranablad.no/nyheter/article2543283.ece og http://www.digi.no/php/art.php?id=395704 (mars 2008)
[24] http://www.digi.no/php/art.php?id=496413 (mars 2008)

3.5.12 Nye former for DDOS (Distributed Denial of Service) og Botnet[25]

DDOS-angrep går ut på å overbelaste en tjeneste på Internett i den hensikt å få tjenesten til å gå ned. Angrepene utføres ved at et stort antall PC-er er infisert med programvare som knytter PC-ene sammen i et virtuelt PC-nett, et såkalt botnet. Programvaren bomber tjenesten med forespørsler for å få denne til å gå ned.

Angrepet er meget vanskelig å avverge og å stoppe. Når tjenesten tar i mot forespørsler fra brukere på Internett, er det nærmest umulig å avgjøre om forespørselen er godartet eller om den har skadehensikt. Angrepene kommer fra tusenvis av PC-er i botnettet. Botnettet kan dynamisk aktivere PC-er i botnettet. Dersom tilbyder avdekker skadehensikt, må tilbyder i programvaren avvise forespørsler fra den enkelte PC, noe som i praksis kan vise seg å være en svært vanskelig oppgave. Alternativt kan tilbyder stenge ned alle adresser tilhørende en nærmere angitt Internet Service Provider. Sistnevnte er en betydelig administrativ operasjon.

Det mest alvorlige er at det er vanskelig å forberede seg mot DDOS i og med tjenestetilbyder ikke vet hva eller hvem som angriper tjenesten. DDOS er en av de alvorligste truslene mot tjenester på Internett. Samfunnskritiske funksjoner kan bli satt ut av spill.

[25] http://www.schneier.com/blog/archives/2007/10/the_storm_worm.html (mars 2008)

4 Risikoområder

4.1 Manglende oversikt, styring og kontroll for bruk av infrastruktur

Infrastruktur er en integrert del av det samarbeidet finanssektoren utvikler for å skape effektiv samhandling og enkelhet for brukerne av finanssektorens tjenester. Finanssektoren består av en rekke nettverksbaserte foretak i et marked hvor det enkelte foretaket knytter sammen to kundegrupper som ønsker å samhandle. Foretakenes egen infrastruktur er en del av den markedsplattformen med produkter og tjenester som tilbys kundene. For å øke verdien av de enkelte plattformene knyttes disse sammen enten direkte eller gjennom fellesforetak og avtaler. Foretakene konkurrerer innbyrdes med egne merkevarer, mens samarbeidet omfatter innsamling, avregning og oppgjør av transaksjoner.

4.1.1 Beskrivelse

Kompleksiteten i infrastrukturen øker med veksten i antall transaksjoner, samhandlende kunder, aktører og utstrakt bruk av IKT. Problemstillingene oppstår ofte innen samhandling hvor operasjonelle effektivitetsmål møtes av uventede koordineringsproblemer. Felles funksjonelle, organisatoriske og institusjonelle prosesser styres på tvers av de målene som settes av hver enkelt institusjon. Det er derfor viktig å legge vekt på både på strategiske og politiske utfordringer sammen med organisatoriske og operasjonelle effektivitetsmål.

4.1.2 Funn

Finansnæringens forretningsmodeller har stor oppmerksomhet rettet mot finansiell rådgivning og tilknyttede tjenester, og mindre oppmerksomhet mot transaksjonsbaserte tjenester. Mens finansiell rådgivning ofte representerer inntektssiden hos institusjonene, representerer transaksjonsbaserte tjenester store kostnader, men også inntekter. De bankoperasjonelle kostnadene er i stor grad knyttet til IKT. I tillegg representerer IKT en kompleksitet hvor både nødvendig kompetanse og kapasitet ofte ikke er tilstrekkelig dekket, verken operasjonelt eller ledelsesmessig. Kompleksiteten synes å øke

risiko og sårbarhet, mens sterkt kostnadsfokus reduserer muligheten for langsiktighet i å møte disse utfordringene. Resultatet kan føre til både ansvarsfraskrivning og problemløsninger i form av gjentatte brannslukkinger.

4.1.3 Analyse

Finansforetakenes økte avhengighet av IKT for å etablere og drive egen og felles infrastruktur, bør kartlegges bedre for å sikre god styring og kontroll, samt mulighet for identifisering av potensielle sårbare områder. I første rekke må operasjonelle forretningsmodeller basere seg på at infrastrukturen understøtter hele transaksjonsløpet ende til ende mellom markedsplattformens to samhandlende sider. Få institusjoner definerer i dag infrastruktur som en strategisk dimensjon. Å ha oversikt over kompleksiteten infrastrukturen representerer, kan innebære en utfordring for foretakene ettersom det stilles store krav til både administrativ og operasjonell kompetanse. Finansnæringen samlet og de enkelte institusjonene individuelt, bør i sterk grad legge vekt på infrastruktur som en verdiøkende tjeneste. På denne måten kan næringen øke felles verdiskaping og eliminere feil og tap av renommé.

4.2 Manglende kvalitet på utførte risikoanalyser

4.2.1 Beskrivelse

Finansiell stabilitet og velfungerende markeder er avhengig av at finansforetak har kontroll med egen operasjonell risiko. Risikovurderinger må være av en viss kvalitet, følge anerkjente metoder og være forståelige for styre og ledelse.

For at de ansvarlige i et foretak skal kunne ta begrunnede avgjørelser, bør risikovurderinger utføres med foretakets målsetning som virkeområde og danne grunnlag for å definere basiskriterier for akseptabel risiko. Det er mange som har kunnskap om risiko og sårbarheter i foretaket, og som bør bidra i prosessen. Risikoer oppstår i både organisasjon, datasystemer og rutinene rundt dem. Mange trusler og hendelser finnes det kontrolltiltak mot. Den raske utviklingen av IT-teknologien gjør at det alltid vil oppstå nye sikkerhetshull. Derfor er det viktig å gjøre jevnlige analyser, minst en gang pr. år, jf. IKT-forskriftens § 3 Risikoanalyse.

4.2.2 Funn

Risikovurderingsmetoder er under utvikling, og det har kommet flere som bør kunne brukes av finansinstitusjoner.

Kredittilsynet har erfart at institusjonenes evne og vilje til å gjennomføre risikoanalyser har blitt bedre. Samtidig indikerer våre funn at kvaliteten på risikoanalysene ikke er tilfredsstillende. Mange av risikoanalysene er overflatiske og ufullstendige. Det gjelder også blant de store institusjonene.

Årsaker til dette kan være at:

- Foretakene i liten grad kjenner til eller følger standarder innen området
- Foretakene ikke har tilstrekkelig kunnskap og fokus på risiko*prosessen*
- Få foretak har risikoanalyse som en vanlig del av virksomhetsplanen
- De ansvarlige for foretaket stiller ikke nok spørsmål
- De ansatte i IT-organisasjonen klarer ikke å forklare sårbarheter og konsekvenser av uønskede hendelser for ledere

Våre gjennomganger avdekker at mange driftsavbrudd skyldtes enkle, menneskelige feil. Foretakets renommé lider en uforholdsmessig og betydelig skade som følge av avbruddene. Risikoanalyser ville i mange tilfeller kunnet avdekke risikoen. Det viser seg at mange finansforetak "følger det de andre gjør" og bruker liten egen tid på å opprettholde egen kompetanse.

4.2.3 Analyse

Ufullstendige risikoanalyser medfører at de ansvarlige for foretakene tar avgjørelser på sviktende grunnlag, og at foretakene ikke klarer å reagere raskt hvis det inntreffer en uønsket hendelse.

Det er viktig at foretakene har gode rutiner og har tilstrekkelig kompetanse og kapasitet til å lage gode analyser. Manglende egen kompetanse kan føre til at rutinene svikter i kritiske situasjoner. En god analyseprosess forutsetter at prosessledelsen har erfaring i denne type arbeid. Foretakene må legge større vekt på arbeidet for å oppnå tilstrekkelig kvalitet.

4.3 Finansinstitusjonenes bruk av åpne nettverk (Internett)

4.3.1 Beskrivelse av nåsituasjonen

Bruk av åpne nettverk og risiko knyttet til dette er et generelt problem for alle brukere av Internett, men finanssektoren er særlig utsatt både på grunn av at den er en betydelig bruker av internettjenester samtidig som penger ofte er involvert i internettbruken.

Finansielle tjenester knyttes sammen med relaterte tjenester. Alle leverandørene som er involvert i et forretningstilfelle, oppdaterer sin informasjon i realtid. Teknisk sett blir tjenestene mer og mer

integrert. Feil i ett ledd gjør at brukeren ikke får gjennomført forretningen. I og med at prosessene, systemene og nettverkene er integrert, kan skade eller feil ett sted gi følgeskader i andre systemer.

En finanstjeneste på Internett består av et meget komplekst samspill av tjenester. I bunnen ligger bæretjenesten – den fysiske kabelen. "Oppå" kabelen ligger det 2–3 tjenestenivåer med sine respektive tilbydere (leverandører). Kabelen og tjenestene transportere i sin tur sluttbrukertjenesten. Alt må virke – svikt i ett av leddene rammer sluttbrukertjenesten. I 2007 ble det registrert hendelser på alle nivåer, noe som viser kompleksiteten og sårbarheten.

Samtidig er det et faktum at håndtering av risiko knyttet til funksjonalitet i Internett ligger utenfor norsk kontroll i større grad enn annen infrastruktur. Ingen enkeltland eller organisasjon er alene ansvarlig for sikkerhet på Internett. En rekke interesseorganisasjoner arbeider og påvirker ut fra sine egne, individuelle målsettinger.

Ved at alle har adgang og ingen bestemmer, defineres Internett som et åpent nett, i det vesentlige uorganisert og under stadig angrep, noe som gjør det komplisert å etablere effektive mottiltak.

Andre forhold er:

- Antallet sårbarheter i protokoller og programmer øker.
- Kompetansegapet øker i takt med økt kompleksitet.
- Lover, rettsforfølging og policy henger ikke med på den tekniske utviklingen og globaliseringen.
- Angripere blir bedre organisert, med egne markeder.

EU/EØS-landene (og dermed Norge) er underlagt bestemmelsene i "Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services". Direktivet er tolket og implementert på ulike vis i de enkelte land. Finland har en detaljert teknisk regulering med krav til vedlikehold, ytelse og tilgjengelighet. Andre land krever at operatørene gjør risiko og sårbarhetsanalyser. Atter andre stiller krav om at brukerne skal opplyses om servicegraden som de kan forvente. I Norge er direktivet ivaretatt gjennom ekomloven, eller lov om elektronisk kommunikasjon, hvor det blant annet er lagt vekt på kommunikasjonsvern, kvalitetskrav og leveransevilkår.

4.3.2 Funn/observasjoner

Samfunnskritisk infrastruktur, som for eksempel betalingsformidling, var i 2007 ved flere tilfeller lammet i lengre perioder som følge av angrep mot infrastrukturen og rene tekniske feil.

Volumet av aksjehandel på nett har økt vesentlig. I 2007 var det flere tilfeller av at aksjehandelstjenesten gjennom nettbank var utilgjengelig i lengre perioder. Dette førte til at kunder ble

innelåst i posisjoner de ønsket å komme ut av, med følbare tap som resultat. Kundene har vært henvist til å ringe fondsforetakets meglerbord, men dette har ikke vært dimensjonert for å ta i mot alle internettkundene i denne situasjonen.

I 2007 var det i Norge to alvorlige forsøk på å overbelaste en tjeneste i den hensikt å sette tjenesten ut av spill. Angrepene bekreftet at det i åpne nettet er svært vanskelig å skille vanlig trafikk og ondartet trafikk, og tilsvarende vanskelig å beskytte tjenesten. Slike angrep anses å være en svært alvorlig trussel generelt og i særdeleshet når det gjelder samfunnskritiske tjenester som går i åpne nett. Mange av angrepene mot tjenester på Internett kommer fra "uregulerte" land, land med mangelfull lovgivning og eller mangelfull håndhevelse av lovregler.

Samtaler og tilsyn hos foretakene i 2007 avdekket at foretakene har store ambisjoner om nye tjenester på nett. I 2007 ble bankenes nye sikkerhetstjeneste for autentisering og signering, BankID, rullet ut for alvor. BankID beskrives[26] slik:

> *BankID er en elektronisk legitimasjon for sikker identifisering og signatur på Internett. Tjenesten tilbys av bankene i Norge. På denne måten sikrer vi at butikker, banker og brukere kan stole på hvem de kommuniserer med elektronisk. En elektronisk signatur med BankID er like bindende som en håndskrevet signatur på papir.*

Bankkundens elektroniske legitimasjon ligger lagret i banken i sikre omgivelser der. Kunden får tilgang til denne gjennom å logge seg på tjenesten fra sin PC. Dette gjør hun ved å taste inn en engangskode fra kodekort samt et fast passord. Gjennom 2007 erfarte Kredittilsynet at kundens PC kan være er et usikkert ledd som kan kompromittere sikkerheten. Det er risiko for at en person kan utgi seg for å være en annen ved å utnytte sårbarheter i den delen av tjenesten som går over Internett, og at tjenestetilbyder ikke klarer å avdekke slike bedrag. Sikkerhet må ses i en totalsammenheng, og sikkerheten blir ikke sterkere enn det svakeste leddet. Mange leverandører (for eksempel Microsoft) velger å være åpne og oppfordrer brukere til å publisere sikkerhetshull i programvaren, slik at denne kan utbedres og herdes så raskt som mulig.

4.3.3 Analyse og tiltak

Økt bruk gir økt avhengighet av Internett, og mindre akseptanse for avbrudd og feil. Det at tjenestene blir mer integrert, øker sårbarheten, og det er derfor økt behov for sikring i alle ledd.

Det er særlig viktig at det nasjonale navnedomenet for internettadresser blir administrert på en sikker måte og at databaser som er grunnleggende for driften oppbevares sikkert. Uten slik sikring kan en blant tenke seg at nettsted utgir seg for et annet, noe som rokker ved selve fundamentet for tjenester på Internett. Dette vil kunne få alvorlige negative konsekvenser for samfunnet.

[26] DnB NORs bestillingsside for bestilling av BankID.

Det er tilsynelatende ulik oppfatning av hvilken risiko som knytter seg til virksomhet i åpne nett. En undersøkelse foretatt av Kredittilsynet viser nemlig at det er svært stort sprik mellom likeartede tjenester når det gjelder tiltak som er implementert for å sikre tjenesten. Det synes ikke å eksistere noen "best practice" når det gjelder vesentlige aspekter knyttet til sikkerheten i tjenester på Internett. Enkelte stiller spørsmål om det bør stilles krav om sertifisering av systemer og utviklingsprosessen, jf. SANS Institute,[27] og drift.

Internettkriminalitet har økt sterkt de siste årene. Tjenestetilbydere må være i stand til å reagere raskt dersom de er under angrep, eller dersom svakheter avdekkes. Kredittilsynet observerer at det skorter på bevissthet rundt kravet til reaksjonsevne. Tilbydere blir for opptatt av egen suksess og kanskje mindre opptatt av sikkerhetsproblematikk – de er ikke forberedt på raskt å kunne reparere en uønsket situasjon som oppstår. Kredittilsynet ønsker å påvirke foretakene til å stille seg spørsmålet: "Hva hvis tjenesten er nede, for eksempel som følge av et tjenestenektangrep, og en er tvunget å gå tilbake til 'gammelt' system?" Særlig for tjenester hvor det ikke er akseptabelt med nedetid, som for eksempel aksjehandel, er det viktig med tilstrekkelige reserveløsninger.

På Internett skjer hele forretningsprosessen i realtid, noe som gjør at nedetid er synlig for publikum. Tidligere tok banken imot et oppdrag og behandlet oppdraget i "back-office". Eventuelle stopp i prosessene internt i banken var ofte usynlige for kunden. Basert på kundereaksjoner som følge av nedetid i nettjenestene, virker det som om publikum nå forventer og innretter seg på at internettjenesten er tilgjengelig til enhver tid. Det er grunn til å stille spørsmål ved om dette er en realistisk forutsetning.

I 2007 så Kredittilsynet svakheter i tjenestene som ble utnyttet. Leverandørene har reagert med å lappe på med mer av den gamle sikkerheten, for eksempel slik at hver betaling nå må godkjennes med en engangskode. Denne formen for reaksjon er på mange måter et tveegget sverd. For det første går sikkerheten etter hvert ut over brukervennlighet i stor grad, og overdreven bruk av koder kan føre til at publikum blir skjødesløse i omgangen med dem. Sikkerheten mister da sin verdi.

Kredittilsynet vil peke på behovet for en grundig diskusjon i bransjen når det gjelder nye tiltak. Et slikt tiltak kan være å kreve at kunden på sikker måte definerer et mottakerregister, det vil si at kunden opplyser banken om de kontoene som hun tillater at det overføres penger til, og at banken kontrollerer mot dette registeret når betalinger skjer fra kundens konto.

[27] http://www.sans.org/gssp

4.4 Trusler og problemer knyttet til nettbanker

4.4.1 Risikostyring

Foretakene som tilbyr nettbankløsninger skal i følge IKT-forskriften ha en risikohåndteringsprosess som gjør det mulig å identifisere, måle, overvåke og kontrollere risikoen som nettbankløsningen innebærer. Ved innføring av nye løsninger og ny teknologi er det i hovedsak tre hovedområder:

- etablere en planleggingsprosess for hvordan å bruke ny teknologi,
- implementeringen av denne og
- evnen til å måle og overvåke risiko i løsningen

Ved leveranse av en nettbankløsning er en av hovedoppgavene å sikre at den løsningen som leveres er en løsning som fyller de krav til kvalitet, tilgjengelighet og risikonivå som foretaket har satt. Det forutsettes derfor at det i dette arbeidet er etablert strenge og rigorøse prosedyrer som sikrer at en i størst mulig grad kan identifisere, måle, overvåke og kontrollere risiko.

Nettkriminalitet

Ved den stadig økende bruken av Internett verden over blir også Internett i større grad benyttet som verktøy for å gjennomføre kriminelle handlinger. Dette medfører også at det i stadig større grad er en internasjonal dimensjon i gjennomført internettkriminalitet. En av de store utfordringene som myndighetene møter i den internasjonale arena er harmoniseringen av lovverkene landene i mellom for å kunne ha tilstrekkelig samarbeid til å kunne lokalisere og identifisere kriminelle over landegrensene og å sikre elektronisk bevismateriale slik at en kan få prøvd saken for retten.

Et stadig mer komplekst og spesialisert nettverk av nettkriminelle handler med hverandre i et internasjonalt marked. En del av miljøene kan sammenlignes med rene kjøpesentre, der virusskrivere og mellommenn selger og kjøper alt fra nye virusvarianter og trojanere til distribusjonsmuligheter, personopplysninger og kredittkortdetaljer

Såkalte botnets, fjernstyrte nettverk av infiserte PC-er, er også en tilgjengelig distribusjonskanal.[28] Disse er i stand til å sende ut millioner av spam-meldinger i løpet av svært kort tid. Når mellommenn deretter selger fullstendige sett med personopplysninger, går det for rundt 5 dollar pr. stykk. Kredittkortopplysninger koster gjerne mellom 2 og 5 prosent av kredittgrensen på kortet, ifølge rapporten.

Etter hvert som nye virus, trojanere og spionprogrammer dukker opp, legger antivirusleverandørene inn signaturene deres i sine neste oppdateringer. Problemet er at de kriminelle kan lage og distribuere nye varianter veldig raskt. Før antivirus er tilgjengelig, kan det ha skjedd stor skade. Det finnes

[28] http://www.tu.no/it/article112853.ece (mars 2008)

eksempler på virus som muterer, det vil si som selv endrer sin signatur og unnslipper antivirusprogrammet.

Antivirusselskapet F-Secure kunne i desember 2007 fortelle at de la til 250 000 nye virussignaturer i sine databaser i løpet av 2007. Det er like mange signaturer som selskapet hadde lagt til i alle sine 20 leveår frem til 2006.

4.4.2 Manglende tilgjengelighet

Stadig nye undersøkelser viser at bruken av internettbaserte bank- og meglertjenester har økt kraftig de siste årene. Kundene har i stadig større grad forutsatt at løsningene internettjenesten baserer seg på, til enhver tid er tilgjengelig. De mest tidskritiske IT-tjenestene ser ut til å være de tjenestene som går mot kjøp og salg av verdipapirer. En stadig større gruppe av day tradere bruker internettbaserte tjenester som sitt hovedverktøy for å utføre arbeidet sitt. I 2007 så Kredittilsynet ved flere anledninger at flere av de norske bankenes internettbaserte tjenester var ustabile og ikke tilgjengelige i perioder der dette kunne skape vanskelige situasjoner for kundene. Ustabilitet med manglende tilgjengelighet kan medføre at en kan handle på feil informasjon siden markedsinformasjonen i løsningene er feil, eller at en ikke kan komme seg ut av posisjoner da IT-løsningen ikke er tilgjengelig. Selv om brukere i slike tilfeller kan ringe bankforbindelsen sin for å få utført ordren, er dette i praksis en stor usikkerhet siden noen større aktører kan ha flere tusen kunder som trenger denne hjelpen. Det er ingen organisasjoner så vidt Kredittilsynet er kjent med som er dimensjonert for å kunne ta imot slike volum av kundehenvendelser samtidig. Også de mer tradisjonelle internettbaserte tjenestene som betaling av regninger, overførsel av penger mellom egne kontoer og kjøp av fondsandeler som ikke nødvendigvis er av samme tidskritiske karakter med tanke på tilgjengelighet, ble undersøkt i 2007 fordi publikums forventninger er at tjenestene alltid skal være tilgjengelige uansett tid på døgnet, alle dager i året. Det er viktig for bankene å klargjøre overfor kundene hvilket forventningsnivå som skal gjelde (alltid tilgjengelige tjenester (24/7), eller et lavere nivå), og deretter sikre opprettholdelse av tilbudet som gis.

Kredittilsynet mottok i 2007 langt flere henvendelser fra publikum om manglende tilgjengelighet på internettbaserte banktjenester. Kredittilsynet tar dette som en pekepinn på at løsningene blir en stadig viktigere del av bankkundenes grensesnitt mot egen bank og at forventningene til tilgjengelighet er, som nevnt over, svært høye. Kredittilsynet tar disse signalene på alvor og har iverksatt stadig tettere oppfølging av bankenes internettbaserte tjenester gjennom tilsyn, etablering av samarbeidsarenaer for bankene, spesielt for internettbaserte tjenester, og deltakelse i internasjonale tilsynsfora særlig for sikkerhet av banktjenester basert på Internett som transportkanal. Etter undersøkelser som ble gjort av enkelte bankers tilgjengelighet på nettbanktjenestene i 2007, er Kredittilsynet ikke tilfreds og har varslet dette overfor aktuelle banker. Det pågår en dialog med de aktuelle bankene for å sikre at foreslåtte tiltak får forutsatt virkning på tilgjengeligheten i 2008.

4.4.3 Informasjonstyveri

Etter hvert som handel på Internett og bruk av nettbank har blitt stadig mer vanlig, har også de kriminelle på nettet skiftet fokus fra å lage ødeleggende virus, til å lage programmer som kan stjele personlig informasjon og passord.

Ifølge tall fra Anti-Phishing Working Group var det i april 2006 hele 11 000 nettsteder dedikert til phishing (nettkriminalitet som spesialiserer seg på å lure ut konfidensiell informasjon eller penger fra enkeltpersoner). Det er en stadig økende trend at ondsinnede programvare i stadig større grad er designet for å stjele personlig informasjon.

Den store utbredelsen av bredbånd i Norge medfører at faren for å bli infisert av ondsinnet programvare øker. Alle PC-er som er oppkoblet mot Internett må ha antivirusprogram installert, virksom brannmur og et operativsystem som er oppdatert med aktuelle sikkerhetsoppdateringer. Ved å gjøre dette vil en kunne klare å unngå de fleste trojanere og virus.

Både banker, Kredittilsynet og Kripos melder om en økning i angrep mot norske nettbankkunder. Angrepene er i stor grad organisert, blant annet på den måten at de som gjennomfører angrepet, står i ledtog med de som samler inn pengene. Det er avdekket at nettsider rekrutterer innsamlere, såkalte money mules. Rekrutteringsmetodene kan sammenlignes med de som benyttes i forbindelse med de mye omtalte Nigeria-brevene. Personene som har stilt sin konto til disposisjon for bakmennene, tar ut pengene i kontanter, eller videreføre dem til bakmenn i utlandet.

Det er på det rene at disse personene har visst, eller burde ha forstått, at de har deltatt i kriminell virksomhet.

4.4.4 Innløsing av verdipapirfond

Bruk av internettbanken til annet enn gjennomføring av betalingstransaksjoner, krever at alle ledd i transaksjonskjeden er sikret tilstrekkelig. Svakheter hos sentrale finansforetak er oppdaget ved gjennomføring av kundetransaksjoner knyttet til innløsing av verdipapirfond. Her tilbys kundene å innløse fondsandeler ved å bekrefte transaksjonen med et enkelt tastetrykk. Kunden blir verken stilt kontrollspørsmål om gjennomføring av transaksjonen eller om bruk av sikkerheten som ligger i BankID. Denne svakheten øker muligheten for utilsiktede feiltransaksjoner hvor det ikke er mulig å angre. Dessuten blir det innløste beløpet automatisk overført til en predefinert konto. I verste fall kan en slik konto være kompromittert hvor oppgjørsbeløpet faller i feil hender.

Sikkerheten for denne type transaksjoner må bedres både med hensyn til krav til ekstra bekreftelse og på angrefunksjon, bruk av akseptable sikkerhetsløsninger og muligheten til å redefinere predestinerte konti.

4.5 Mangelfulle katastrofeløsninger

De aller fleste foretak under tilsyn fra Kredittilsynet har nå etablert katastrofeløsninger som også omfatter IKT-området. Den store utfordringen for foretakene er å teste løsningene i et omfang som gir trygghet for at løsningen kan fungere dersom et uhell inntreffer. Reelle DDOS-angrep (se kapittel 0), brann, virusangrep og programmeringsfeil gjorde at flere foretak innen finansnæringen i 2007 fikk prøve sine planverk i praksis. Vi må ha som utgangspunkt at en katastrofeløsning ikke er virksom når den ikke er testet og verifisert innenfor et tilstrekkelig kort tidsrom. IKT-forskriften § 11 krever at dette gjennomføres minst én gang årlig.

Alle IKT-tjenester som foretakene tilbyr sine kunder er avhengige av at telekommunikasjonslinjene er tilgjengelige. Mange foretak kjøper løsninger som forutsetter at dersom én linje er utilgjengelig, så rutes trafikken over til en alternativ, virksom linje. Dette forutsetter at linjene er fysisk adskilt på en slik måte at en hendelse som rammer den ene linjen ikke rammer den andre linjen. Hendelser i 2007 tyder på at foretakene ikke i tilstrekkelig grad har sikret seg at slike forutsetninger er til stede. Foretakene har stolt på at dersom de kjøper en redundant løsning, så vil leverandøren av tjenesten sikre at dette er i orden. Det kan være vanskelig å holde oversikt over tjenestene i et stadig voksende ekom-marked. Det som to forskjellige leverandører fremstiller som "leie av linje", kan vise seg å være logiske linjer, men i realiteten tjenester fra den samme fysiske kabel. Det er viktig at finansforetaket sikrer seg informasjon om hvem som leverer den fysiske delen av kommunikasjonsløsningen for å sikre seg at laveste nivå i kommunikasjonsløsningen faktisk kommer fra ulike leverandører.

4.6 Utkontraktering til land utenfor Norge

Tilsynene i 2007 viste at det gjennomgående er visse utfordringer knyttet til utkontraktering. Den største utfordringen synes å være å definere ansvar og å plassere ansvaret. I tilfeller der det har skjedd ulykker, og ansvar skal fordeles, viser det seg svært ofte at kunden mener at leverandøren har et ansvar, mens leverandøren mener at det ikke er avtalt et slikt ansvar.

Når virksomhet utkontrakteres, så vil ofte kompetansen internt i foretaket bli redusert. Foretaket har etter hvert ikke tilstrekkelig oversikt og kunnskap til å identifisere alle sider som bør ansvarsreguleres, og leverandøren er interessert i å minimere ansvaret sitt innenfor rammene av leveransen. Det oppstår fare for uregulerte soner.

Gjennom høringsuttalelser mv., kan norske virksomheter påvirke utviklingen i norsk lovgivning som er relevant for virksomhetene, herunder lovgivning knyttet til databehandlingen. I andre land kan interessene til norske foretak bli uvesentlige og forbisett. Dette kan skape usikkerhet og uforutsigbarhet med hensyn til de juridiske rammebetingelsene som det norske foretaket opererer innenfor. Harmonisering av regelverket innenfor EU/EØS kan på sikt motvirke dette problemet.

Det er ikke uvanlig at avtalebestemmelser suspenderes i tilfeller av force majeur, for eksempel dersom det skulle oppstå en omfattende avbruddssituasjon hos leverandøren. I disse tilfellene kan situasjonen bli den at myndighetene i leverandørlandet bestemmer hvilke kunder som skal prioriteres når det gjelder reetablering av normal drift. Den utenlandske (norske) kunden kan bli nedprioritert. En bestemmelse regulert i avtalen mellom leverandør og kunde kan bli oversett i en slik situasjon.

Utkontraktering innebærer mer transport av data enn om databehandlingen skjedde sentralisert. Økt transport innebærer økt risiko knyttet til linjebrudd, feiltransmisjon etc. Dersom transporten skjer over Internett, er det vanskelig å gi garantier med hensyn til servicegrad, i og med Internett i det vesentlige er uregulert.

4.7 Stort press på håndtering av endringer

IT-organisasjonene i finansnæringen har vært utsatt for et stort endringspress de siste årene. Det er flere årsaker til dette.

I løpet av de to siste årene har finansnæringen vært utsatt for massive regelverksendringer. En rekke nye krav gjennom lover og forskrifter har trådt i kraft. Her kan nevnes ny lov om hvitvasking, ny verdipapirhandellov, ny børslov, ny lov om eiendomsmegling, nye forskrifter om kapitaldekning i tråd med Basel II, ny lov om virksomhetsregler for livsforsikringsselskaper og lov om obligatorisk tjenestepensjon (OTP). Endringer i lover og forskrifter indikerer ofte regelendringer som må implementeres gjennom endringer i IT-systemene. Av og til fremkaller regelendringene nye kommersielle produkter som for eksempel verktøy for elektronisk overvåkning av transaksjoner mot hvitvasking og verktøy for OTP-løsninger, men oftest implementeres endringene i hver enkelt IT-organisasjon.

Større volumer og økte krav til tilgjengelighet til elektroniske betalingskanaler, samt introduksjonen av nye typer elektroniske betalingskanaler, er også med å øke endringspresset. Dette er løsninger hvor flere lag i systemarkitekturen trenger kontinuerlig overvåkning for å optimalisere ytelse og responstid for å imøtekomme dagens funksjonelle krav.

Samtidig er også trusselbildet endret. Tjenester levert gjennom åpne nettverk som Internett, eksponerer for nye typer trusler som blir stadig mer sofistikerte og profesjonelt gjennomført. Mottiltaket er sikringstiltak i alle deler av infrastrukturen for å tette potensielle hull i forsvarsverket.

Videre gjennomføres det organisasjonsmessige endringer i finansforetakene gjennom salg, oppkjøp og fusjoner. Konsekvensen kan være splitting eller sammenslåing av IT-organisasjoner som igjen gir grunnlag for plattformskifter og større integrasjonsprosjekter.

I utgangspunktet utgjør nettopp disse faktorene selve grunnlaget til IT-virksomheten. Men i en periode hvor rekruttering av IT-kompetanse kan være vanskelig, og flere av de nevnte faktorene samtidig slår ut i sterk grad, kan endringspresset bli urimelig stort og innebære en større operasjonell risiko.

5 Hva kan Kredittilsynet gjøre?

5.1 Tilsynsopplegget

5.1.1 Utvikling av tilsynsmetodikk

Basert på den erfaringen Kredittilsynet gjør gjennom IT-tilsynene, arbeider tilsynet med å videreutvikle og forbedre tilsynsmetodikken. Det kan være vanskelig å tilpasse IT-tilsynene til så mange ulike foretakstyper. IT-tilsynet dekker foretak som driver bank, forsikring (liv og skade), verdipapirhandel, børs, fondsforvaltning, eiendomsmegling, inkassovirksomhet samt IT-leverandører. Dette kan spenne fra foretak med mange tusen ansatte til foretak med under 10 ansatte. En annen utfordring er å tilpasse tilsynsopplegget til endringer i trusselbildet. "Security"-hendelsene har i større grad fått oppmerksomhet etter tilsiktede, ondsinnede angrep mot IT-systemene.

Den prosessorienterte metodikken som CobiT representerer, sikrer at det blir gitt oppmerksomhet til alle deler av IT-virksomheten, og metoden kan skalere i forhold til størrelse på og type foretak. Det opplegget Kredittilsynet har utviklet med egenevalueringsskjemaer med kontrollspørsmål knyttet til hver CobiT-prosess, er derfor et verktøy vi vurderer som like viktig som tidligere. Samtidig ser vi at det er nødvendig å supplere tilsynsmetodikken med flere elementer for å oppnå tilstrekkelig innsikt i IT-virksomheten i foretakene vi skal gjennomføre tilsyn med. Basert på en risikovurdering er det også utviklet en rekke egne tilsynsmoduler som adresserer et avgrenset område. For eksempel antivirus, antihvitvasking, brannmur, nettbank og andre. Ved gjennomføring av tilsynene i 2007 ble det gjort noen justeringer i tilsynsopplegget, og erfaringer fra IT-tilsynene i 2007 vil bidra til ytterligere justeringer i året som kommer.

5.1.2 Tematilsyn

Et IT-tilsyn som i utgangspunktet er rettet mot foretakets generelle IT-virksomhet, kan etter en første gjennomgang dreies mot et spesifikt område av forretningsvirksomheten eller IT-virksomheten. De siste årene har vi gjennomført en del risikobaserte tematilsyn. Eksempler på dette er tilsyn rettet mot nettbank, utenlandsbetaling, prosjektgjennomføring, oppfølging av leverandører eller

sikkerhetsområder. Noen av disse temaene er det utviklet egne temamoduler med kontrollspørsmål for. Sikkerhetshendelser er blitt et stadig mer aktuelt område på grunn av økt operasjonell risiko knyttet til trusler om ondsinnede angrep. Med bistand fra flere anerkjente sikkerhetsselskaper i Norge, har Kredittilsynet laget en temamodul med kontrollspørsmål knyttet til foretakets sluttpunktsikkerhet (antivirus m.m.). Denne modulen ble benyttet første gang i 2007. Modulen er detaljert og har vist seg å være nyttig både for Kredittilsynet som tilsynsmyndighet og for foretaket som en sjekkliste og indikator på foretakets sikkerhetsbeskyttelse. Under arbeid har vi en tilsvarende modul med kontrollspørsmål for foretakets perimetersikring (brannmur m.m.).

5.1.3 Verifikasjon

IT-tilsynet har hittil benyttet de to tilnærmingsmåtene som er beskrevet over: den prosessbaserte med IT-tilsyn av hele IT-virksomheten på et overordnet nivå og den risikobaserte med tematilsyn på valgte områder. I begge tilfeller har Kredittilsynet innhentet informasjon gjennom foretakets dokumentasjon, foretakets svar på egenevalueringsskjemaer og samtaler med foretakets representanter for IT-virksomheten. Resultatet av tilsynet er basert på Kredittilsynets tillit til foretakets framlegging. Kredittilsynet har vurdert å lage et opplegg for å følge ulike transaksjonstyper gjennom livsløpet: en form for ende til ende-test som kan kalles en metode basert på transaksjonstest. Utformingen av dette opplegget er ikke klart ennå.

Kartleggingen av infrastrukturen som ble startet i 2007 og som fortsetter i 2008, kan bidra til å finne en fornuftig måte å starte en slik transaksjonstesting på. Transaksjonsverifikasjon kan gjøres på applikasjonsmessig nivå, men kan også suppleres med verifikasjon av basisteknologi som strøm og nettverkslinjer, samt knyttes til områder som kontinuitet og katastrofeplan.

5.2 Videreutvikling av opplegget for meldeplikt for systemer for betalingstjenester

I lov om betalingssystemer er det nevnt under § 3-2 at ”Det skal uten nødig opphold gis melding til Kredittilsynet om etablering og drift av system for betalingstjenester.”

Meldeplikten er senere presisert i rundskriv 17/2004 fra Kredittilsynet. Her understrekes det at innføring av nytt system eller nye systemversjoner for betalingstjenester som påvirker berørte parter i vesentlig grad, eller hvor nye funksjonsversjoner og andre funksjonelle endringer er vesentlig for etablerte systemer, vil utløse meldeplikt. I rundskrivets vedlegg er det et eget skjema til bruk for denne meldeplikten. Rundskrivet og skjemaet er tilgjengelige på Kredittilsynets nettsted.

Meldeplikten har hittil vært oppfylt med noe varierende kvalitet og oppmerksomhet. Kredittilsynet vurderer derfor å videreutvikle dette opplegget slik at meldeplikten og kvaliteten på denne kan bli

bedre til nytte for alle involverte parter. Kredittilsynet vil vurdere innholdet i det nåværende skjemaet for egenmelding, men i tillegg også starte tematilsyn rettet mot de ansvarlige enhetene for betalingstjenester i de enkelte foretakene. Tatt i betraktning foretaksstrukturen innen norsk finansnæring, vil slike tilsyn måtte tilrettelegges på individuelt tilpassede måter. Til bruk for slike tematilsyn, har Kredittilsynet utviklet et eget evalueringsskjema som bygger på den strukturen som nå brukes for våre vanlige IT-tilsyn.

5.3 Risiko- og sårbarhetsanalyser (ROS)

Som vi skrev om i kapittel 4.2, indikerer både Kredittilsynets egne funn og eksterne kilder at foretakene ikke har tilstrekkelig kunnskap om og legger nok vekt på risikoanalyser.

Risikoanalyse er ikke å definere tiltak som settes inn dersom det usannsynlige skjer, men snarere det motsatte. I arbeidet med risikoanalyser og tiltak som følge av disse, styrker man IT-systemene slik at de blir mer robuste og feilfrie, noe som reduserer sannsynligheten for at uønskede hendelser skal skje. Risikoanalysen "beskytter" mot tap og skade på renommé. Risikoanalysen gir *løpende* avkastning for virksomheten. Risikoanalysene er et viktig verktøy for å sikre at virksomhetsmålene nås og skal være en integrert del av den *daglige driften*, ikke et isolert, årlig "stunt". Med integrert mener vi at risikoanalysen må være utarbeidet av fagpersonell som har forutsetning for å vurdere risikoen på et detaljert, teknisk nivå og at analysen skjer som en integrert del av det daglige arbeidet.

Det foreligger en rekke ROS-veiledninger og metoder både på konseptuelt nivå og i form av datastøtte. Flere av disse er tilgjengelige som dokumentasjon eller fri programvare.

Erfarte feil, mangler og nestenulykker er viktige kilder i analyseprosessen. En oversikt over dette gir verdifulle assosiasjoner og koblinger til mulige likeartede feil. Kredittilsynet har ikke kommet over noen systematisk oppsamling av erfaring som er benyttet på denne måten. Kredittilsynet vil sterkt oppfordre til slik gjenbruk av egne og andres erfaringer.

IKT-forskriftens § 3 har bestemmelser om risikoanalyse, der det blant annet fremgår at "foretaket skal ha en dokumentert prosess for gjennomføring av risikoanalyser av IKT-virksomheten". Kredittilsynet vil fremover ha oppmerksomheten rettet mot foretakenes prosesser for risikoanalyse, blant annet gjennom utarbeidelse av en enkel veiledning til IKT-forskriftens § 3.

5.3.1 Kriterier for hva Kredittilsynet mener er akseptabel risiko

Tilsynsarbeidet bygger på at ansvaret for den forretningsmessige driften ligger hos styre og ledelse i foretakene selv.

Kriterier for evaluering:

- Den samfunnsmessige verdien finansiell informasjon representerer, og de delene av den som er kritisk. Her er konsekvenser ved utilgjengelighet, tap av konfidensialitet og integritet faktorer som vurderes.
- Avvik fra regelverk

Tap av tillit og renommé til finansnæringen er en vesentlig evalueringsfaktor. Bankene i Norge har ikke tapt store penger via angrep på nettbanker. Men deler av befolkningen er klar over at bankene tilbyr elektroniske tjenester som benytter PC-er som kan være korrumperte. Det kan skape en for stor risiko for samfunnet hvis deler av befolkningen ønsker å gå tilbake til mer manuelt baserte løsninger igjen, eksempel brevgiro, og bankene ikke har apparat til å takle dette.

Uakseptabel risiko

Uakseptabel risiko er områder der Kredittilsynet ikke ser det dokumentert at institusjonene eller andre parter har kontroll.

Kriterier for å akseptere restrisiko

Det vil alltid finnes risikoer på ulike områder. Restrisiko er kjent risiko der det ser ut for Kredittilsynet til at institusjonene har rimelig kontroll.

5.4 Hendelsesregistrering og rapportering

Hendelsesrapporteringen som ble etablert i 2007, vil etter 12 måneder bli evaluert for å bestemme om den skal videreføres eller ikke. Dersom hendelsesrapporteringen videreføres, kan det bli eventuelle justeringer i opplegget. Erfaringer så langt tyder på at en form for felles hendelsesrapportering for finansnæringen er nyttig. Hendelsesrapportene representerer kvantitative data. Når dataene sammenstilles og analyseres, kan de gi en totaloversikt over hvordan IKT-hendelser innvirker på tjenestenivået i finansnæringen. Sammenhenger i teknologisk infrastruktur kan synliggjøres når foretakene rapporterer om samme hendelse fra hvert sitt perspektiv. Feil som oppstår ett sted, kan gi følgefeil et helt annet sted og avdekke avhengigheter de færreste har vært klar over. Hendelsesregistreringen er nyttig, både som grunnlag for preventive tiltak og som grunnlag for aksjonering for å gjenopprette normal drift.

5.5 Informasjon og kommunikasjon

I tillegg til å føre tilsyn med og kontrollere IKT-virksomheten i finansnæringen, er Kredittilsynet opptatt av å kunne veilede og informere. Kredittilsynet har samme mål som foretakene om at IT-systemene skal fungere optimalt og sikkert. Kredittilsynet ønsker en åpen dialog med foretakene og bidra med informasjon der det er aktuelt. I noen grad vil Kredittilsynet også legge til rette for kommunikasjon foretakene imellom.

Temamodulene med kontrollspørsmål vil vi i større grad publisere og tilgjengeliggjøre på Kredittilsynets nettsted. I dag er det kun hovedmodulen med ca. 170 spørsmål som ligger tilgjengelig, men i løpet av 2008 vil vi publisere flere av modulene. I 2007 ble det utarbeidet en veiledning til etterlevelse av IKT-forskriften rettet mot mindre sparebanker. Denne ble publisert på Kredittilsynets nettsted i januar 2008. I 2008 vil det bli utarbeidet en veiledning spesielt rettet mot etterlevelse av § 3 Risikoanalyse i IKT-forskriften.

Kommunikasjon med foretakene skjer gjennom tilsynsmøter, intervjuer og ulike typer faglig relaterte møter. I 2007 tok Kredittilsynet initiativ til at bankene fikk en felles møteplass for å diskutere tiltak og beredskap mot nettbankkriminalitet.

Kredittilsynet holder også hvert år en rekke foredrag om emner knyttet til IT-tilsyn for næringen.

Kredittilsynet
Østensjøveien 43
Postboks 100 Bryn
NO-0611 Oslo

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

Innoventure Design Center

Foto: Jarle Nytrinqnes

03.2008/700