KREDITTILSYNET
The Financial Supervisory Authority of Norway

Rapport

Risiko- og sårbarhetsanalyse (ROS)

2008

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Risiko- og sårbarhetsanalyse (ROS) 2008

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Kredittilsynet, 17. februar 2009

Innhold

1 Innledning

Det finansielle systemet er av stor betydning for effektiviteten i et moderne samfunn og for landets økonomi. Bruk av informasjons- og kommunikasjonsteknologi (IKT) i finanssektoren er i dag altomfattende og alvorlige brudd på konfidensialitet, integritet og tilgjengelighet i denne sektoren virker svært negativt og kan få store negative samfunnsmessige effekter. Denne erkjennelsen er en hovedgrunn til at det er økende fokus på operasjonell risiko i finanssektoren, både internasjonalt, nasjonalt, i bransjeorganisasjoner, hos forbrukermyndigheter og i det enkelte finansforetak. Det er mange eksempler på denne utviklingen, men her gjengis noen viktige påvirkningsprosesser:

- Internasjonalt gjennom samarbeidsopplegg, for eksempel det nye kapitaldekningsregelverket (Basel II), som for første gang gir føringer for håndtering av operasjonell risiko. Tilsvarende prosess er i gang innenfor forsikringsområdet gjennom arbeidet med Solvens II, som har adoptert mange av elementene fra Basel II. Dette er kun noen eksempler på en mangeartet prosess som legger vekt på risiko knyttet til samfunnsviktige områder. Det pågår flere andre tiltak på området initiert av OECD, G8-landene og FN som adresserer risiko knyttet til IKT og finanssektoren.

- Nasjonalt gjennom NOU 2006: 6 *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*, hvor finanssektoren er definert som kritisk samfunnsfunksjon. I St.meld. nr. 17 (2005–2006) *Eit informasjonssamfunn for alle* og i *Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007–2010* er IKT-sikkerhet gitt bred omtale. Likeledes gjennom St.meld. nr. 22 (2007–2008) *Samfunnssikkerhet. Samvirke og samordning*, hvor det er redegjort for flere sikkerhetstiltak som berører finanssektoren. Det er også grunn til å nevne forskningsprosjektet "Beskyttelse av samfunnet 5" (BAS5), som spesielt undersøkte risiko- og sårbarhetsanalyse som metode og leverte rapportene *BAS5 Casestudie – risikoanalyse av et finansforetaks IKT-system*, Tilsynsmetodikk og måling av informasjonssikkerhet i finans- og kraftsektoren samt sluttrapporten *Beskyttelse av samfunnet 5: Sårbarhet i kritiske IKT-systemer – sluttrapport*[1].

Finanssektoren i Norge har vært tidlig ute med å ta i bruk IKT på stadig nye områder, og dette er noe av grunnen til at det blir lagt stor vekt på IKT-sikkerhet og -risiko i denne sektoren. Det er etablert samarbeidsarenaer og felles organisasjoner for standardisering av krav til IKT-sikkerhet og -risiko på en rekke forskjellige områder. Dette opplegget utfordres nå av krav til europeiske tilpasninger, hvor

[1] http://rapporter.ffi.no/rapporter/2007/01204.pdf (lastet ned feb. 2009)

det blir en oppgave å opprettholde det nasjonale sikkerhetsnivået i europeiske løsninger. Med bakgrunn i finanssektorens offensive bruk av IKT, er det fra myndighetenes side laget regelverk på dette området. IKT-forskriften stiller krav til at foretakene minst én gang per år gjennomfører risiko- og sårbarhetsanalyser og dokumenterer resultatet av dette. Det er først når det enkelte foretak selv fokuserer på risiko og sikrer seg kunnskap om egen risikosituasjon, at håndteringen av risiko kan skje på en akseptabel måte.

Kredittilsynets årlige risiko- og sårbarhetsanalyse (ROS-analyse) oppsummer arbeidet med IKT-sikkerhet i finanssektoren i det foregående året og hvordan enkeltforetak og bransjen etterlever regelverket. Dette gjør det mulig å se utviklingen over tid for hele finanssektoren. Resultatene danner noe av grunnlaget for å iverksette tiltak på særlig utsatte områder. Det er også relevant å nevne Norges Banks *Årsrapport om betalingssystemer* hvor det er etablert et samarbeid med Kredittilsynet for å samordne fokus på risikoområder knyttet til IKT-sikkerhet og -risiko i betalingsformidlingen.

Det er lenge siden man ble oppmerksom på risiko og vanskelighetene med å kjenne alle problemer som kan oppstå på forhånd:

> ”Det er sannsynlig at noe usannsynlig vil skje.” *Aristoteles, 384–322 f.Kr.*

Om vi skal ta sitatet på alvor, understreker det viktigheten av arbeidet med å forebygge risiko og at dette i praksis aldri opphører eller er noe man kan bli ferdig med. Det er derfor viktig at arbeidet med å forebygge risiko ikke blir ren rutine, men at det gis tilstrekkelig oppmerksomhet, prioritet og tyngde for å oppnå hensikten, nemlig å kunne oppdage et problem og iverksette tiltak før det materialiserer seg.

2 Teknologi og utviklingstrekk

2.1 Generelt om teknologiske utviklingstrekk

Det er mange generelle utviklingstrekk i finanssektoren som påvirker foretakenes bruk av IKT. Kredittilsynet har identifisert følgende drivere som er viktige for IKT-utviklingen og som påvirker operasjonell risiko.

- Området elektronisk kommunikasjon er i sterk utvikling. De forskjellige kommunikasjonsnettene kan i økende grad utnyttes i kombinasjon (konvergens). Telefoni i kombinasjon med Internett er et eksempel på dette. Nettene har blitt multimediabærende, det vil si at de formidler tekst, lyd og bilde. De elektroniske kommunikasjonsnettene vil være tilgjengelige overalt til enhver tid. Slik kan de samme elektroniske banktjenestene benyttes fra Norge og Australia. Det som trengs er tilgang til en Internett-terminal eller en mobiltelefon med nettleser.

- Mobiliteten har økt ved utviklingen av mobiltelefonen og de mulighetene som mobiltelefonens grensesnitt kan tilby sine brukere. Ved at de mobile enhetene får stadig flere funksjoner og større kapasitet, vil enhetene langt på vei ikke bare erstatte den stasjonære kontor PC-en, men også bærbare PC-er. Denne typen avanserte mobiltelefoner har både personlige støttefunksjoner, tradisjonelle PC-egenskaper og mulighet for høyhastighet Internett-tilgang.

- Såkalte kontaktløse betalingsmetoder er en trend vi ser særlig på områder der kontanthåndtering fortsatt er dominerende. Teknisk sett gjennomføres en kontaktløs betaling uten at det er fysisk kontakt mellom leseren og kort. Flere teknologier kan brukes til dette, blant annet bluetooth, infrarød eller radio frequency identification (RFID).

- Til forskjell fra de trådløse enhetene som baserer seg på bluetooth eller infrarød behøver ikke RFID-senderen å være drevet av et batteri, men av signaler som er sendt fra RFID-leseren. Dette gjør det mulig å pakke en RFID-brikke i en chip, og det gir denne teknologien stor fleksibilitet. RFID-brikker kan legges inn i nøkkelringer, mobiltelefoner, kredittkort, klokker, brev og andre ID-brikker. Den store fleksibiliteten kan føre til lavere enhetskostnader og

forenkling for forbrukerne.

- Mange forbrukere har allerede stiftet bekjentskap med bruken av kontaktløse betalinger. I Norge er det særlig Autopass-brikkene som har stor utbredelse. I USA har man over lang tid hatt løsninger som for eksempel ExxonMobiles Speedpass og flere bomstasjonsløsninger. I England er det mest kjente prosjektet OysterCard som benyttes til betaling i Londons tunnelbanesystem. De store aktørene som American Express, Visa og MasterCard har siden 2005 hatt RFID-kort tilgjengelig for forbrukerne.

- RFID-betalingsløsninger er som nevnt ovenfor utviklet særlig for det tradisjonelle kontantsegmentet innenfor betalinger. For brukersted og bank er dette en utvikling i positiv retning når det gjelder håndtering av kontanter. Behandling av kontanter er en stor kostnad for bankene. Ved å redusere mengden av kontanter, reduseres også bankenes kostnader.

- Nettbanken er den klart dominerende kanalen nordmenn benytter for å håndtere egen økonomi. Med løsninger som stadig blir mer avanserte, ser en at ønsker om nye tjenester og bruksmuligheter øker. Det er derfor grunn til å anta at dagens nettbankløsninger vil endre seg. De fleste løsningene som tilbys norske kunder, er i regelen utformet etter samme mønster. Den største ulikheten mellom løsningene er ikke innholdet i løsningene, men hva det koster for forbrukerne å benytte disse. De fremtidige løsningene vil trolig kunne tilpasses hver enkelt bruker, slik at en kan skreddersy egen grenseflate. Særlig er det områdene innenfor mer direkte kommunikasjon med banken der en vil se endringer. Med muligheter til chat og direkte kontakt mellom kunde og bank vil en kunne videreutvikle kundeforholdet. På denne måten kan leverandørene av nettbankløsninger bidra til å øke tjenestetilbudet og følgelig også konkurransen mellom bankene.

- Store deler av norske nettbankbrukere er i dag avhengige av sikkerhetsinstrumenter som for eksempel DigiPass eller kodekort for å logge seg på nettbanken sin. Nye løsninger utvikles stadig for å forenkle kunders bruk av finansielle tjenester. Sikkerhetstjenester som tidligere ble gjennomført ved hjelp av tradisjonelle sikkerhetsinstrumenter, som nevnt ovenfor, utføres i stedet gjennom bruk av mobiltelefonen. Dette bidrar til å gjøre tjenestene mer tilgjengelige, siden en ”alltid” har med mobiltelefonen.

2.2 Infrastruktur

2.2.1 Generelt

Med infrastruktur mener vi fysiske komponenter, operativsystem, nettverk, standarder, systemer for overvåking, organisering, avtaler, oppfølging, dokumentasjon og kontroll når det gjelder drift av et foretaks IKT, enten det skjer i egen organisasjon, eller er delvis eller helt utkontraktert, for eksempel som del av en samarbeidskonstellasjon.

Det pågår en rekke initiativer som også øker oppmerksomheten knyttet til å sikre vital internasjonal og nasjonal infrastruktur.

2.2.2 Nettverk

Det enkelte foretaket er selv ansvarlig for å sikre tilgjengeligheten på egen infrastruktur. Nasjonal prioritering i telenettet ivaretas av Post- og teletilsynet. Aktører som ivaretar oppgaver av nasjonal betydning, kan få midler gjennom den såkalte tilskuddsordningen, som forvaltes av Post- og teletilsynet.

Ut over dette er det den enkelte tjenestetilbyder som må sikre at foretakets krav til tilgjengelighet, sikkerhetskopiering, redundans mv. blir oppfylt.

Mange finansforetak arbeidet i 2008 med å kartlegge sårbarheter og trusler i foretakets nettverksinfrastruktur i detalj med tanke på å finne løsninger som kan gi større grad av sikkerhet for at foretakets tjeneste kan fortsette dersom det skjer uplanlagte hendelser.

Flere foretak melder at det i mange tilfeller kan være vanskelig å få oversikt over nettverksinfrastrukturen. Det har vist seg vanskelig å få teleleverandørene til å redegjøre for hvordan topografien i nettet er. I enkelte tilfeller kan det virke som det ikke er tilstrekkelig vilje til å gi kunden nødvendig innsyn. I andre tilfeller kan det se ut som om nettleverandøren ikke har tilstrekkelig oversikt selv.

Kredittilsynet vurderer det som uakseptabelt at finansforetakene ikke får innsyn i denne viktige delen av sin virksomhetskritiske infrastruktur. Alternativet er at Post- og teletilsynet eller teleleverandøren formelt må bekrefte redundans i infrastrukturen.

2.3 Integrasjon mellom sentral og desentral programvare

Finansielle tjenester blir i stadig større grad automatisert. Omfanget av og bruken av finansielle tjenester på Internett øker sterkt. Økt bruk av elektroniske tjenester gjør samfunnet stadig mer avhengig av kvaliteten på tjenestene – vi tåler i mindre grad avbrudd og feil.

Mange tjenester har i dag en sentral (server) og en desentral (klient) programvarekomponent. Klienten kan være flyktig, enten som et program (”applet”) som lastes ned hver gang tjenesten benyttes, eller den kan være permanent, som programvarekomponenter installert hos kunden. Kunden ønsker integrasjon mot egne systemer, og dette løses ofte ved en persistent komponent hos kunden. Det å utvikle grensesnitt mot kundens systemer er ofte en stor utfordring, ikke minst fordi de tekniske omgivelsene varierer fra kunde til kunde. Kundene har ulike portalkonfigurasjoner, brannmurkonfigurasjoner av ulik art, er ulikt satt opp programvaremessig og så videre. Variantene er mange, og leverandøren får problemer med å vedlikeholde funksjoner for å sikre grensesnittene mot de

mange ulike konfigurasjonene. Leverandøren løser dette problemet ved å tilby åpne ”Application Programming Interface” (API), der kunden selv setter sikkerhetsparametrene og skrur på sikkerheten, i henhold til sin spesifikke infrastruktur. Dette medfører en stor og økende risiko. Kunden kan ha mangelfull sikkerhetsforståelse og sikkerheten blir deretter. Leverandøren har mange kunder og kan ikke kontrollere at alle kundene har satt opp sikkerheten slik den skal være.

Enkelte tjenester er slik at tiltak på klientsiden er av administrativ art, slik at klientsiden oppfordres til å følge nærmere beskrevne sikkerhetsoppsett og prosedyrer. Andre tiltak er ”hardkodet”, det vil si at klienten ikke har valgmuligheter og sikkerhetsoppsettet er dermed tvunget.

Innenfor kredittkortområdet gjelder de såkalte PCI-kravene (Payment Card Industry). Disse er tiltak av administrativ art. Til tross for kravene, har det vært flere ulykker der store mengder kortdata har kommet på avveie. Det kan være grunn til å tro at PCI-kravene ikke har vært fulgt fullt ut på brukerstedene som har ”lekket” kortdata. Det er en stor utfordring for kortselskapene å kontroller at PCI-kravene følges på alle brukersteder til enhver tid.

2.4 Testing

Samtidig som at IKT-infrastrukturen blir mer kompleks og ulike parter må samarbeide, er det en større utfordring å sikre tilstrekkelig testing før endringer og nye systemer settes i drift.

Tidligere var banktransaksjoner delt i atskilte ”etapper”. En brevgirotransaksjon for eksempel, involverer ”Brukeren”, Posten Norge AS, OCR-giro på BBS AS, avregning i oppgjørssystemet Norwegian Interbank Clearing System (NICS) og bokføring i ”Banken AS”, i isolerte og avgrensede prosesser. Feil i ett ledd innebar ikke at transaksjonen måtte starte forfra (hos brukeren) igjen, og det var ikke sikkert feilen en gang var synlig for brukeren. I dag er tjenestene gjerne online og i sanntid. Brukeren sitter ved PC-en og ser alt som foregår fra registrering til beløpet er reservert på konto. Transaksjonen gjennomføres i en integrert operasjon. Feil i ett eneste av leddene gjør at hele transaksjonen må gjennomføres på nytt. Feilen er umiddelbart synlig for brukeren og skader banken. Risikoen og skaden for foretaket ved at systemet feiler i ett ledd, er derfor mye større i dag enn tidligere. Foretaksledelsen bør derfor ha en policy for å utvikle opplegg som sikrer en testing som gjenspeiler dette (IT-governance-standarder).

2.5 Effekter av finanskrisen

Alle finansforetak har i dag en teknisk infrastruktur som inkluderer leveranser fra en rekke IKT-leverandører. I lys av den globale finanskrisen oppstår spørsmålet om IKT-leverandørene står i fare for å gå konkurs eller av andre årsaker må innstille sin virksomhet. Mange leverandører kan ha foretatt

lånefinansierte oppkjøp. Vanskeligheter i kredittmarkedet kan gi høyere rente og belaste likviditeten og følgelig redusere handlefriheten. Dersom oppkjøpet er et ledd i en virksomhetssammenslutning, kan det på kort sikt være vanskelig å få ut ønskede gevinster, og i krisetider kan omsetningen gå ned.

I denne situasjonen er det viktig at finansforetaket (kunden) går nærmere inn på sin leverandør. Det kan være aktuelt å få bedre kontroll over leveransen med tanke på, i ytterste konsekvens, å måtte ta over videreutviklingen eller overlevere denne til en ny leverandør. Hva som er status for dokumentasjon, kildekode, opplæring og så videre, er nærliggende spørsmål i denne sammenheng. Videre kan det være aktuelt å kontrollere eierrettigheter, det vil si Intellectual Property Rights (IPR), bruksretter, videresalgsrettigheter, rett til å videreutvikle produktet og andre relevante forhold. Dersom foretaket i egen regi bidrar til å sluttføre produktet uten å ha nødvendige eierrettigheter, kan dette gi uheldige følger.

2.6 Utskifting av systemer

Med bakgrunn i det utstrakte samarbeidet som har vært i norsk finanssektor og gjennom etablering av felles løsninger på mange områder, eksisterer det i dag også felles infrastrukturer for å understøtte dette. Det er særlig på områdene betalingsformidling, verdipapirområdet, avregning og oppgjør og på spesielle tjenesteområder, for eksempel Public Key Infrastructure (PKI). Videre er det etablert ulike felles løsninger og infrastruktur. Den norske infrastrukturen er sammenkoblet. Mange sentrale systemer som inngår i samarbeidet, skal byttes ut i 2009 eller følgende år (Norges Bank, VPS, Oslo Børs, NICS/BBS, Teller). Systemene er sentrale for den norske finansielle infrastrukturen, og de har grensesnitt mot hverandre. Det innebærer en risiko at mange systemer skal byttes ut noenlunde samtidig. Dette stiller store krav til testing, kvalitetssikring og håndtering av risiko.

2.7 Internettkriminalitet

2.7.1 Generelt om utviklingen i internettkriminalitet

Mange land rapporterer om økning i antall angrep på nettbanken. Dette gjelder også vellykkede angrep, det vil si angrep som har ført til tap. Flere banker er bekymret og har etablert ”taskforces” for raskt å finne mottiltak.

Siden 2006 har internettpenetrasjonen økt i mange land. USA og Kina har omtrent 200 millioner internettbrukere. Svindelforsøk og svindlere på Internett øker tilsvarende. Noen land antas å ha uforholdsmessig mange svindlere, men ofte kan dette være vanskelig å identifisere da den aktuelle serveren som sender transaksjoner ofte styres fra et annet sted. Likevel antas det at Russland, Nigeria, Kina og Ukraina er eksempler på land som er kilder til stor internettkriminalitet.

Phishing, det vil si ondsinnet programvare som avlurer identitetsinformasjon fra kunden, er en alvorlig trussel. Trusselen setter grenser når det gjelder hvilke tjenester som det er forsvarlig å tilby på Internett, gitt at de kjente ID-løsningene forutsetter at brukeren registrerer passord og bruker-ID på sin PC.

2.7.2 Mulige fremtidige angrepsformer

2.7.2.1 Angriperne trenger inn i bedriftsinterne nettverk

Angripere har lykkes å trenge inn i foretakets interne nettverk. Kredittilsynet tror at dette problemet vil øke. En rekke muligheter åpner seg da for angriperne.

- Angriperne kan utføre uautoriserte transaksjoner fra innsiden av foretakene og ut mot banker og lignende.
- Angriperne kan ta ned systemet (operasjonen) og presse foretaket for penger.
- Angriperne kan stjele kundeinformasjon og presse foretaket for penger eller selge informasjonen.
- Angriperne kan plante programvare som gjør at det lekker informasjon, eller som gir angriperne kontroll over installasjonen.

Som et eksempel på dette kan vi vise til innbruddet i World Bank som representerer en tankevekkende hendelse som skjedde på dette området i 2008. Angripere lykkes i å trenge inn i bankens nettverk og å få tilgang til passord som med høy sannsynlighet ble benyttet til å få ut sensitiv informasjon, se artikken "World Bank Hacked, Sensitive Data Exposed"[2], publisert 10. oktober 2008 på nettstedet Darkreading.com.

2.7.2.2 Mer avanserte former for trojanere

Det har vært registrert flere eksempler på angrep der ondsinnet kode (trojanere) endrer det brukeren ser når hun er i nettbanken. Teknikken er kjent som persistent MitB (Man-in-the-Browser).

Poenget er at brukeren ikke ser den falske transaksjonen og slår derfor ikke alarm. Brukeren blir presentert for sider som viser at transaksjonen tilsynelatende ble utført som ønsket. Dette gir angriperen bedre tid til å overføre pengene før svindelen blir oppdaget.

Ingen av de kjente angrepene ble avdekket av antivirusprogramvare. Dette samsvarer godt med resultatene av en offentlig undersøkelse som er gjort i Spania.

[2] http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=211201265 (lastet ned feb. 2009)

2.7.2.3 Distributed Denial of Service (DDoS)

DDoS[3] (Distributed Denial of Service) vurderes fortsatt å være en av de store truslene på Internett.

DDoS består i angrep som kommer fra et stort antall infiserte PC-er som er sammenkoblet i et såkalt Botnet. PC-ene i nettet er i utgangspunktet ukjent for offeret. Angriperen kan aktivere/deaktivere PC-ene, slik at PC-er som har vært benyttet i angrepet og som offeret etter hvert sperrer for i brannmuren sin, erstattes av andre PC-er som angriperen aktiverer. For offeret er det vanskelig å skille nyttetrafikk fra ond trafikk før den onde trafikken gjør skade. For offeret er det en stor jobb løpende å sperre for PC-er i brannmuren, eventuelt anmode den som er internettvert for angrepsmaskinen(e) om å sperre disse for adgang til nettet. Enkelte internettverter er kjent for ikke å etterkomme sperreanmodninger – disse er populære blant DDoS-angripere.

Det mest bekymringsfulle er at det er lite læring i å bli angrepet. Det er begrenset hva offeret kan gjøre for å forberede seg på neste angrep og beskytte seg. Det er likevel viktig at foretaket har tenkt gjennom situasjonen som oppstår dersom foretaket utsettes for DDoS-angrep. Kontinuitets- og beredskapsløsninger må være på plass.

2.8 Web-applikasjonsutvikling

Bruken av web-applikasjoner er antakelig det området med størst sikkerhetsutfordringer. Det er mange grunner til dette. Trusselbildet er svært dynamisk. Det er snarere regelen enn unntaket at programvare for Internett inneholder alvorlige sikkerhetshull. Internett samler angripere. Stadig mer nyttetrafikk går på Internett og flere finansforetak rapporterer at de vil få en økende eksponering mot Internett.

Selv velrenommerte programvareutviklere ser ikke ut til å være i stand til å utvikle kode uten sikkerhetshull, og vi er blitt vant til å måtte akseptere en stor mengde sikkerhetsoppdateringer. I lys av risikoene på Internett er det underlig at applikasjoner i større grad enn tilfellet er, ikke undergis selvstendig sikkerhetstesting og sikkerhetsgjennomgang før de settes i produksjon. Finnes det en risikoanalyse, er denne som regel på overordnet nivå. I få tilfeller er analysene trukket ned til applikasjonen og driftsomgivelsene, med kartlegging av applikasjonens evne til å beskytte mot truslene.

Kredittilsynet har i tidligere ROS-analyser pekt på sårbarheter når det gjelder web-utvikling. Begreper som ”SQL-injection”, ”header poisoning” mv. er kjente begreper i utviklingsavdelingene. Etter hvert er det utviklet en ”best practice” på området web-utvikling. Det har dukket opp organisasjoner som utvikler og forvalter disse. Open Web Application Security Project (OWASP) er en slik organisasjon, som fikk sin norske gren i 2008.

[3] Distributed Denial of Service (DDoS) er en teknikk der angriperen sender tilstrekkelig mange henvendelser til en tjeneste til at tjenesten går ned, eller at angriperen foretar mange påloggingsforsøk med feil kombinasjon av bruker-ID og passord slik at brukeren blir sperret ute.

OWASP Guide er et dokument på over 300 sider som er en veiledning i hvordan man utvikler sikre web-applikasjoner og web-services. Det er et løpende prosjekt som oppdateres hele tiden. Det dekker "rike applikasjoner" som Asynchronous JavaScript and XML (Ajax). Det dekker hele utviklingsprosessen fra policy, sikker koding, trussel og risikomodellering til konfigurasjon, utrulling og vedlikehold, og dekker i detalj mange tema som autentisering, autorisering, sesjonshåndtering, datavalidering etc.[4]

Sårbarhetene som omtales, gjør at truslene på Internett er vanskeligere å oppdage for brukeren og tilsvarende vanskelig å beskytte seg mot. Selv velrenommerte nettsteder har vist seg å ha en eller flere av de omtalte svakhetene som gjør at brukeren, uten at hun oppdager det, får ondsinnet programvare installert på PC-en.

Det å skape sikkerhet i alle ledd er en utfordring når det gjelder Web-utvikling. I særdeleshet i de tilfeller der tjenestene inkluderer programvare som installeres på klienten ("tykk klient"). Leverandøren må i disse tilfellene forholde seg til mange ulike klientkonfigurasjoner. Enkelte klientkonfigurasjoner har egen DNS[5], andre har ikke det, noen er bak brannmur, andre har ulike former for portalløsninger og så videre. Det er en for omfattende oppgave for leverandøren å lage spesialsøm for alle variantene. Leverandøren leverer i stedet standardiserte sikkerhets API-er[6], og legger opp til at kunden benytter flest mulig av disse.

2.9 Identitetstyveri

Identitetstyveri som skjer på Internett brer om seg, og sikring av systemer som gjør det mulig for samhandlende parter å identifisere seg, blir viktigere.

Finansforetak tilbyr i dag ulike former for identitetskontroll på nett. Alle er kjennetegnet ved at kunden må oppgi hemmelige koder. Kunden registrerer kodene på sin PC og kodene fraktes til foretaket og kontrolleres der. Det vil være kjent at en PC kan være infisert med ondartete dataprogrammer, programmer som gjør at en angriper kan få tak i kodene. Angriperen kan i neste omgang misbruke kodene.

[4] Kilde: OWASP, http://www.owasp.org/images/7/76/20080528_hva-er-owasp.pdf

[5] Domain Name System (DNS) er Internetts navnetjeneste som oversetter navn til maskinnummer (IP-adresse) og gjør det mulig å sende informasjon til riktig sted på nettet.

[6] Application Programming Interface (API) betegner et grensesnitt for kommunikasjon mellom programvare.

Ingen av identitetskontrollene som benyttes innenfor finanstjenester på Internett i dag, beskytter på en effektiv måte mot den største identitetstyven på Internett, nemlig phishing[7]. Dette er aktuell risiko etter som angrep på nettbank som fører til tap, viser en økende tendens i andre land.

På denne bakgrunn er det grunn til å spørre hvorvidt dagens identitetsløsninger er sikre nok til at det er forsvarlig å benytte dem i forbindelse med transaksjoner, avtaler mv. på Internett. I særdeleshet gjelder dette for transaksjoner som er av en slik art, at det kan ha betydelige negative konsekvenser dersom en identitetstyv gjennomfører blant annet transaksjoner og avtaler i en annen brukers navn.

2.10 Regelverk knyttet til IKT-sikkerhet

Mye av utviklingen som skjer i Norge knyttet til informasjonssikkerhet, er styrt av internasjonale beslutninger og påvirkes av regelverk utviklet utenfor Norge. Nedenfor gir vi noen viktige eksempler på denne utviklingen som bidrar til bedre håndtering av risiko, men som samtidig også stiller krav til endringer som kan være krevende.

Basel II
Hensikten med Basel II var å etablere en internasjonal standard som banktilsynsmyndighetene kunne bruke i sitt arbeid med å utarbeide regelverk for å bestemme bankenes kapitaldekningskrav som sikkerhet for finansielle eller operasjonelle risikoer som kan oppstå. Videre er hensikten at denne type internasjonale standard kan verne det internasjonale finansielle systemet fra å få problemer dersom en eller flere større banker ikke lenger greier å overholde sine forpliktelser.

Med de erfaringene som en allerede ser, er det grunn til å tro at en igjen vil se på Basel II-regelverket og sikre at regelverket i en krisesituasjon ikke forsterker krisen (prosyklisk), men at det bidrar til å minske skadeomfanget dersom en eller flere banker går overende.

Solvens II
Solvens II er et sett med regulatoriske krav for forsikringsbransjen som er etablert innenfor EU og EØS. Solvens II er basert på økonomiske prinsipper for å kunne måle verdier og forpliktelser. Det vil også være risikobasert slik at risiko blir målt ut fra fastsatte prinsipper og at kapitaldekningsbehovet vil direkte avspeile dette. Arbeidet med Solvens II har pågått en tid, og direktivet forventes å bli gjennomført i 2012.

Datalagringsdirektivet
EU-parlamentet vedtok i februar 2006 et nytt europeisk rammeverk for lagring av tele- og internettopplysninger i arbeidet med kriminalitetsbekjempelse.

[7] Teknikk for å "stjele" identitetskoder som består i at angriper utgir seg for å være banken, for eksempel ved å presentere kunden for en kopi av bankens innloggingsside på nett, og lurer kunden til å oppgi identitetskoder.

Direktivet er ansett som EØS-relevant, og dermed bindende for Norge. Direktivet omfatter lagring av en mengde informasjon knyttet til data- og telekommunikasjon, slik som telefonnummer eller bruker-ID, navn og adresse for den som ringer og den man ringer til, dato, tidspunkt og varighet for kommunikasjonen, samt hvor utstyret befant seg. Informasjonen kan lagres fra seks måneder til to år.

Direktivet har skapt stor debatt i Norge, og skepsisen til direktivet er stor. Datatilsynet er blant de sterkeste kritikerne av direktivet, og hevder at en innføring av direktivet vil føre med seg flere endringer som kan true personvernet.

Nasjonale retningslinjer
I 2007 ble *Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007–2010*, utarbeidet. Formålet med retningslinjene er å skape en felles forståelse for hvilke utfordringer en står overfor, og identifisere områder der det er behov for å gjøre en ekstra innsats. Retningslinjene skal bidra til å fremme en bedre forståelse for hvordan alle brukere, utviklere og tilbydere av IKT kan bidra til utviklingen av og nyttiggjøre seg av en sikkerhetskultur på området.

I St.meld. nr. 17 (2006-2007) pekes det på behovet for å sørge for godt vern av den norske informasjonsinfrastrukturen gjennom forebyggende tiltak. Dette innebærer å være forberedt på IKT-sikkerhetshendelser gjennom beredskapstiltak og å sørge for å opprettholde og styrke sikkerhetsarbeidet gjennom blant annet kompetanseutvikling og standardisering.

Europa/EU
Det er satt i verk flere tiltak som også vil gjelde Norge. Blant annet er det etablert en europeisk strategigruppe innen sikkerhetsforskning (European Security Research and Innovation Forum – ESRIF) som er ventet å gi positive virkning på sikt. ESRIF er både etablert og støttet av EU, og Norge er representert i gruppen. ESRIF ble etablert for å bidra til samarbeid om sikkerhetsrelatert forskning og utarbeidelse av strategier og policies – og iverksettelse av tiltak. Målet er å sørge for en styrking av den generelle sikkerheten i Europa, og sikkerhet knyttet til IKT. Sikkerhetstrusselen i Europa blir mer og mer kompleks, og de europeiske landene må i økende grad stole på hvert enkelt lands sikkerhetsregime.

3 Kredittilsynets funn og observasjoner

Grunnlaget for ROS-analysen er som for tidligere år kunnskap og informasjon som 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 Generelt om IT-tilsyn gjennomført i 2008

I 2008 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 viser i stadig større grad til prosesser som understøtter kravene i forskriften. Samtidig skjer det uheldige hendelser på IT-området i finansnæringen som enkelte ganger er lite forutsett til tross for foretakenes egne 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 tilstrekkelig. Prosessene må være under konstant evaluering og forbedring, og ikke minst, de må etterleves.

Følgende er viktige funn fra IT-tilsynene som ble gjennomført i 2008:

1. Utilstrekkelig konfigurasjonsstyring
2. Ufullstendig gjennomføring av kontinuitet og katastrofetester
3. Manglende eller ufullstendige ROS-analyser
4. Manglende etterlevelse av egne endringsprosesser

I tillegg kommer også andre funn, som er relevante, men som det ikke redegjøres nærmere for her. Disse omfatter blant annet manglende kvalitetsmål og kvalitetsmåloppfølging, ikke tilstrekkelig tilgjengelige ressurser, for svake på kompetansemessig back-up (nøkkelmannsrisiko) og manglende basisdokumentasjon, manglende dokumentert IT-strategi, ufullstendig gjennomførte ROS-analyser i foretakene og manglende eller utilstrekkelig sikkerhetspolicy. Nedenfor utdypes hovedfunnene:

3.1.1 Konfigurasjonsstyring

Foretakenes IKT-infrastruktur innbefatter alle fysiske komponenter, operativsystem, nettverk, systemer for overvåking og drift. Særlig for større foretak er den tekniske infrastrukturen kompleks og omfattende, slik at det å ha tilstrekkelig oversikt over hele infrastrukturen til enhver tid er en stor utfordring. Til tross for dette er foretakene avhengige av å ha denne oversikten for å kunne sikre god og stabil IKT-drift. Ut fra erfaringer ser en at langt de fleste feil skjer på grunn av feil som oppstår i planlagte endringer. Dersom foretakene ikke har tilstrekkelig oversikt over egen infrastruktur, er det ved hver endring stor risiko siden mange av komponentene i infrastrukturen er avhengige av hverandre. Kompatibiliteten mellom komponentene må derfor sikres ved å ha oppdaterte konfigurasjonsoversikter over foretakets IKT-infrastruktur.

3.1.2 Katastrofetest

Katastrofetesting er et avgjørende element for å sikre at foretaket har evne til å videreføre egen drift ved en katastrofesituasjon. Særlig gjennom testing av planverket kan en avdekke mangler og svakheter.

I IKT-forskriftens §§ 10 og 11 stilles det krav til at det skal gjennomføres opplæring, øvelse og testing av reserveløsningene minst én gang årlig og i et omfang som gir trygghet for at reserveløsningene fungerer tilfredsstillende. Testene skal dokumenteres slik at gjennomføring og resultat kan vurderes i ettertid.

Kredittilsynets funn ved gjennomførte IT-tilsyn kan tyde på at ikke alle foretak gjennomfører tester som kan anses å være tilstrekkelige, og særlig gjelder dette graden av dokumentasjon av resultatene av testene. Kredittilsynets vurdering er at det uten dokumentasjon av resultatene vanskelig kan gjennomføres oppfølging og forbedring av det katastrofeplanverket testen er gjennomført med bakgrunn i.

3.1.3 Risikostyring

Risikovurderinger har i økende grad blitt et hjelpemiddel for foretakene for å avdekke sårbarheter i IT-systemene og ved bruken av IKT. Risikoanalyser og tiltak som følge av disse, kan gjøre foretaket i stand til å gjøre IT-systemene mer robuste. Dette vil bidra til å redusere sannsynligheten for at uønskede hendelser inntreffer. Hovedhensikten med risikovurderinger er først og fremst å bli klar over egen risikosituasjon, og basert på denne kunnskapen, iverksette risikoreduserende tiltak eller på annen måte sikre en forsvarlig håndtering av egen risiko. Det er viktig for foretaket å klargjøre hva som er et akseptabelt risikonivå med utgangspunkt i foretakets forretningsstrategi og virksomhetens omfang og viktighet.

En ønsket effekt er at risikoanalysen "beskytter" mot tap og skade på renommé. Risikoanalysene er et viktig verktøy for å sikre at virksomhetsmålene nås, og skal være en integrert del av den daglige driften. En forutsetning for å sikre kvaliteten på risikoanalysen er at den må være utarbeidet av personell som har forutsetning for å vurdere risikoen på et tilstrekkelig detaljert nivå.

Erfaringer fra gjennomførte tilsyn viser at mange uønskede hendelser sannsynligvis kunne vært unngått dersom foretaket hadde gjennomført risikoanalyse med tilstrekkelig kvalitet. Særlig gjelder dette i forbindelse med risikovurderinger knyttet til endringer.

3.1.4 Endringshåndtering

Kredittilsynet har sett en klar forbedring i foretakenes arbeid med å forbedre prosesser og rutiner som bygger opp under endringshåndtering i foretakene. Særlig i større organisasjoner hvor endringstakten er svært høy, er prosessene og rutinene godt etablert. Også risikoprosessen har fått en sentral plass i endringsprosessene. Som kjent kan "liten tue velte stort lass", og dette gjelder også endringer. Små endringer som i utgangspunktet ikke kan påvirke andre systemer, har ført til langvarige situasjoner med manglende tilgjengelighet.

Årsakene til feil som Kredittilsynet har funnet, er todelt. Den ene er at risikoprosessen når en endring meldes inn, ikke er tilstrekkelig grundig gjennomført, slik at en har nødvendig kunnskap om den risiko endringen medfører til å kunne ta riktig beslutning om endringen bør gjennomføres eller ikke. Den andre er at etablerte prosesser og rutiner ikke følges i tilstrekkelig grad. Dette er etter Kredittilsynets vurdering de to hovedgrunnene til at endringer feiler, og dette går i særlig grad utover endringer i den tekniske infrastrukturen.

3.2 Foretakenes vurderinger

I 2008 ble det gjennomført 12 intervjuer med nøkkelpersoner i sentrale finansforetak, hovedsakelig med personer som representerer IKT-området. Denne type intervjuer 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 er blitt regulære årlige samtaler.

En nærmere bearbeiding av resultatene fra intervjuene viser følgende hovedtrekk:

1) Hva ser foretaket som den/de største risikoen(e) ved foretakets bruk av IKT?
Mange foretak melder om stort leveringspress. Kravene kommer fra kunder og fra myndigheter. Flere av foretakene mener at IT-avdelingen strekker seg langt, og at kundene etter hvert har fått for høye forventninger. For eksempel forventer kundene i dag at banken og aksjehandel skal være døgnåpne tjenester. Tidligere var banken åpen fra 09:00–15:00 (15:45). Forventninger om slike åpningstider stiller betydelige krav til drift og utvikling av IT-systemer. I tillegg blir IT-avdelingen i praksis belastes i faser som forutsetningsvis skal leveres av andre, for eksempel i fasene spesifikasjon,

definisjon og prototyping, samt utvikling av brukerdokumentasjon. Følgene av urealistiske leveransekrav og forventninger er en stor risiko knyttet til IKT.

I og med publikums forventing om døgnåpne tjenester, blir ledig tid til programvedlikehold, maskinvedlikehold og implementering av endringer tilsvarende liten. Dette stiller økte krav til testing og kvalitet forut for implementering av endringer. Det er simpelthen ikke tid til å gjøre feil og eventuelt rulle tilbake til gammel versjon innenfor implementeringsvinduet.

Styring og kontroll av utkontraktert IT er en økende utfordring i lys av økt utkontraktering og derav følgende reduksjon i kompetansen internt.

2) Hva har vært de største problemene knyttet til IKT-området i 2008?
Mange av foretakene mener det er en utfordring å vedlikeholde og kontrollere basisplattformen, det vil si basis infrastruktur. Plattformen er blitt for komplisert å vedlikeholde. Dette gir mye feil og nedetid. Dersom det dreier seg om en online-tjeneste, kan feilen gi stor renomméskade.

Overvåking og kapasitetsplanlegging rapporteres å være en stor utfordring. Dette gjelder for eksempel diskplass, allokert plass i databaser, antall tråder i applikasjonsserveren, antall samtidige brukere, time out-parametre i kommunikasjonsenheter osv. Alt skal spille sammen og være tilpasset installasjonen og lasten til enhver tid. Det er en utfordring å kontrollere dette kompliserte samspillet.

Leveransepresset, jf. pkt. 1, var stort også i 2008. Presset medvirket til at systemer som var satt i produksjon, viste seg å ikke ha tilstrekkelig kvalitet. Dette medførte et stort omfang av feilretting, som igjen gikk på bekostning av nyutvikling og forbedring. Enkelte foretak kom på denne måten i en ond sirkel av feilretting og nye implementeringsforsøk. Den reelle nyutviklingen ble dermed lidende.

Det å få til en god dialog og samhandling mellom forretningssiden og IT-siden er stadig en utfordring.

3) Hva er grunnlaget for å kunne identifisere dette?
Hendelser i foretaket gir godt grunnlag for å identifisere de største problemene. Utfordringen ligger i å analysere hendelsen og finne rotårsaken. Uten grundig analyse, får ofte det som er synlig "skylden" for hendelsen. Et typisk utsagn vi har hørt fra kunder i 2008 er: "Nå er det noe i veien med nettbanken igjen". En nærmere analyse kan vise at nettbankapplikasjonen i og for seg går helt normalt, men at det er en softwarekomponent eller hardwarekomponent "lenger bak" som feiler. Det er svært viktig å gjøre grundig analyse slik at man finner den virkelige årsaken.

4) Hva ser foretaket på som de største utfordringene i 2009 med hensyn til risiko ved bruk av IKT?
Det er en stor utfordring å møte publikums krav til tilgjengelighet på systemene. Høy oppetid er kostbart. Å øke oppetiden med 0,2 prosent fra 99,6 prosent, koster betydelig mer enn å øke oppetiden med 0,2 prosent fra 99,4 prosent.

Høye oppetidskrav utfordrer endringshåndteringsfunksjonen, jf. pkt. 1 ovenfor. Å skape et driftsmiljø (testmiljø) for kvalitetssikring av nye tjenester anses som en utfordring for 2009.

Nesten alle foretakene rapporterer at mangel på helhetlig IT-arkitektur og infrastruktur er en utfordring. Kjernesystemene er kanskje fra 1980-tallet. Systemet avgir data til et datavarehus som ble implementert på 1990-tallet. Kjernesystemene får inndata ikke lenger fra filer, men fra web-basert realtidssystem som er utviklet på 2000-tallet. Systemene gjenspeiler arkitektur mv. som var gjeldende på det tidspunktet de ble utviklet, og som er vesentlig forskjellig. Det må lages mellomvare som syr det hele sammen. Dette gir risiko og vedlikehold i mellomvarekomponentene. I tillegg er mange av foretakene innfusjonert og del av et konsern. De øvrige konsernselskapene har gjort andre valg enn foretaket opp gjennom tiden. Sett fra konsernets ståsted er IT en omfattende og mangeartet samling systemer. Det å kontrollere systemporteføljen og få systemene til å "snakke sammen", er en stor utfordring og risiko som vil bli ytterligere adressert i 2009.

5) Hva ser foretaket på som viktige problemstillinger med hensyn til IKT-risikoen i 2009 hvor det kreves iverksatt egne tiltak?

a) Endringskontroll knyttet til implementering av nye systemer
Mange viktige aktører i finans har planer om å bytte ut sentrale systemer i 2009. Det å kvalitetssikre implementeringen anses som viktig siden disse systemene "snakker sammen". Dette stiller store krav til kvalitetssikring og kontroll i alle ledd.

b) Arkitektur
Nesten alle foretakene har planer om å kartlegge sin arkitektur og arbeide for å forenkle arkitekturen slik at den konvergerer mot noe mer stabilt. Nesten alle foretakene har i den senere tid etablerte egne stillinger og/eller funksjoner, og prosjekter innenfor dette viktige området.

c) Testmiljø
Mange foretak rapporterer om utfordringer knyttet til test. I og med at tjenester i dag er integrerte elektroniske funksjoner ende-til-ende som går i realtid, så må selv små funksjonsendringer regresjonstestes nøye mot resten av funksjonskjeden. Dette er en utfordring å få til, spesielt i de tilfeller der tjenesten har en (tykk) klientdel som det må testes mot. Tilstrekkelig test er en av forutsetningene for å nå oppetidsmålene.

d) Risiko knyttet til leveranser fra leverandørene
Flere foretak har utfordringer med kvaliteten på leveransene fra sentrale leverandører. Flere går så langt som å si at det er uvanlig at leveransen ikke har feil. Enkelte føler at de, etter at tjenesten er satt i produksjon, nærmest er en del av leverandørens test av tjenesten.

De fleste av foretakene har utkontraktert IT-tjenester til et fåtall leverandører. Dette gir konsentrasjonsrisiko. I og med økt utkontraktering, forvitrer IT-kunnskapen internt i foretaket, noe som gjør at oppfølgingen av leverandøren kanskje ikke blir ivaretatt på en tilstrekkelig god måte.

Enkelte foretak har satt i gang tiltak for å tiltrekke seg og beholde dyktige medarbeidere, ikke minst innenfor området IT-sikkerhet.

Oppfølging på dette området er en forutsetning for å nå oppetidsmålene, jf. pkt. 4.

e) Tilgangskontroll
Flere foretak rapporterer om "slitasje" når det gjelder tilgangskontroller og manglende oversikt over tilgangskontroller. Dette har flere sider.

Tilgangskontroller ligger spredt: i kode, i tilgangskontrollsystemer, i programvare, som nøkler i software osv. Flere foretak melder at de ikke har en totaloversikt og kontroll.

De personlige tilgangsrettighetene er ikke alltid tilpasset den enkelte medarbeiders aktuelle oppgaver og ansvar. Flere foretak har identifisert utfordringer innenfor området. Flere melder også at det har vært altfor mange som har hatt administratorrettigheter i systemet. Foretakene har satt i gang aktiviteter for å få bedre kontroll, og vil videreføre dette arbeidet i 2009.

Årsaken til at flere foretak ønsker å fokusere på tilgangskontroller nå, kan være at økt uro i arbeidslivet kan slite på den ansattes lojalitet. Den ansatte som står foran en oppsigelse kan ønske å ta med seg informasjon om kunder etc. for å ha noe å leve av fremover. Vi har sett eksempler på at dette har skjedd. Men like viktig er det å beskytte den enkelte ansatte mot mistanker om uregelmessigheter – det er vanskelig for den ansatte å begå misligheter innenfor et område hun ikke har tilgang til.

f) Opphør av virksomheten hos én eller flere sentrale leverandører
Flere finansforetak frykter for den situasjonen som kan oppstå dersom en viktig leverandør må opphøre eller innstille sin virksomhet for kortere eller lengre periode. Dette kan skje som følge av finanskrisen. Vi vet at flere store leverandører har foretatt lånefinansierte oppkjøp, og finanskostnadene har steget betydelig og belaster likviditeten. Virksomhetsstans kan også skje som følge av arbeidskonflikter.

g) Nettverksutstyr
Flere av foretakene melder om mindre nedetid som skyldtes feil i én eller flere nettverkskomponenter enn tidligere år. Det er et viktig mål å fortsette denne gode trenden i 2009.

h) Fare for spredning av virus
Etter som brukere blir mer og mer mobile, er det også økt risiko for å bli smittet av virus eller annen ondsinnet programvare. Kildene til infisering er etter hvert mange, og flere foretak ser dette som en trussel som det vil bli arbeidet ytterligere med å forebygge i 2009. Blant annet øker bruken av hjemmekontor, og bærbare PC-er er kanskje ikke regelmessig i kontakt med nettverket og får dermed ikke nødvendige sikkerhetsoppdateringer. Videre er det en fare for å bli smittet av virus eller annen ondsinnet programvare via minnepinner og e-post. Bruk av Facebook og andre møteplasser øker, og med det også faren for spredning av virus.

i) Internett
Virusproduksjon er blitt industrialisert. Angrepene er i økende grad rettet mot brukere og ikke maskiner. Engelskspråklige tjenester utgjorde angrepsmålene tidligere. Dette har endret seg. Nå kan angriperen velge språk når hun kjøper ondsinnet programvare. Flere av foretakene mener at sikring av nettbank og andre viktige internettbaserte tjenester er en prioritert oppgave i 2009.

Flere foretak rapporterer at de har en økende eksponering mot Internett.

j) Prosessetterlevelse og kultur
Uønskede IT-hendelser skyldtes ofte mangelfull etterlevelse av fastlagte prosesser. Flere av foretakene vil adressere dette i 2009.

Enkelte foretak har programmer for å skape en kultur der risiko og sårbarhet blir mer synlig internt. Det å oppdage og bringe opp sårbarheter skal bli honorert. Det å forbedre risikoanalyseprosessen inngår i flere tilfeller i programmet.

3.3 Rapporterte hendelser til Kredittilsynet

3.3.1 Generelt om rapporterte hendelser og kategorisering av disse

I november 2007 ble det etablert en frivillig rapporteringsrutine for hendelser i rundskriv 31/2007 "Rapportering av IKT-hendingar til Kredittilsynet". Ved utgangen av 2008 kan vi oppsummere erfaringer etter ca. 13 måneders rapportering. Sparebanker, forretningsbanker og filialer av utenlandske banker i Norge, VPS, Oslo Børs og BBS har deltatt i rapporteringen, og fra september 2008 sluttet EDB Business Partner ASA seg til rapporteringen.

Kredittilsynet mottok rapport om 136 hendelser i 2008. Dette er fem ganger så mange som året før. I tillegg blir Kredittilsynet informert om hendelsen tidligere i forløpet enn før, og hovedsakelig fra foretaket selv fremfor fra media eller kunder. I vel 80 prosent av tilfellene blir Kredittilsynet informert gjennom e-post til adressen hendelse@kredittilsynet.no. I de resterende tilfellene varsles Kredittilsynet pr. telefon eller brev fra foretaket eller blir informert om hendelsen gjennom media eller e-post direkte fra kunder. Der Kredittilsynet er gjort kjent med hendelsen gjennom andre kanaler, har Kredittilsynet rutiner for å etterspørre rapportering på hendelsen.

Kredittilsynet gjør en første grovkategorisering av hendelsene ved å benytte tapskategoriene til Basel II (såkalte 7 eksponeringsfaktorer). Hendelsene fordeler seg slik:

1. Basel II: Interne misligheter	1
2. Basel II: Eksterne misligheter	5
3. Basel II: Ansatte og arbeidsmiljø	–
4. Basel II: Produkter og forretningspraksis	–
5. Basel II: Fysisk skadeverk	–
6. Basel II: Driftsavbrudd og systemfeil	124
7. Basel II: Prosess og rutinefeil	6

Det er viktig å understreke at tabellen kun viser IKT-relaterte hendelser, og vi ser at de fleste hendelser kommer under driftsavbrudd og systemfeil. Det betyr at vi har behov for en ytterligere nedbrytning på dette området. Hendelsesrapportering gir oss et faktagrunnlag som er vesentlig bedre enn fra tidligere år og som danner grunnlag for tiltak.

Fordelt på forretningsområde er det, ikke overraskende, i særklasse flest hendelser knyttet til nettbank. Nettbank for regningsbetaling, verdipapirhandel, mv. er sluttjenester til kundene med 24/7 åpningstid som umiddelbart representerer et problem for kundene, når tjenestene ikke fungerer.

Kortbetalingssystemet i butikk og minibank er også tjenester med 24/7 åpningstid, men disse er i større grad stabile med færre hendelser rapportert. For minibank rammer hendelsene ofte lokalt, og kundene kan benytte en annen banks minibank i stedet.

Hendelsesbildet er i mange tilfeller sammensatt. Hendelsen det rapporteres om rammer flere tjenester samtidig.

3.3.2 Nærmere om hendelser knyttet til nettbank fordelt på årsak

For å få en mer standardisert årsaksvurdering av hendelser relatert til nettbank, har Kredittilsynet laget et opplegg for å analysere og kategorisere de underliggende tekniske årsakene til hendelsene. Årsaksbildet for nettbankhendelsene (85 av våre 136 hendelser) er brutt ned og fordelt på følgende kategorier:

Nettbank-SW: Feil i programvare (operativsystem, databaseprogramvare, overvåkings-SW, brannmur-SW, kommunikasjonsservere, nettverksprogramvare, applikasjonsserver-SW osv.).

- Funksjonsfeil (programmeringsfeil)
- Parametere: uriktige/uhensiktsmessige verdier
- Programvaren ligger på disk i stedet for i lokalt minne – fører til lange svartider
- For liten kapasitet: Programvaren er ikke programmert for å håndtere trafikken (# samtidige brukere/tråder)

Nettbank-HW: Maskiner som banken drifter nettbanken på, og maskiner i banken som må til for å nå nettbanken, dvs. nettverk/kommunikasjonsutstyr i banken.

- Maskinen har ikke kapasitet til å håndtere trafikken (f.eks. for lite minne).
- Funksjonsfeil og full stopp (f.eks. som følge av strømbrudd).

Nettbank-nettverk: Kommunikasjonslinjer, rutere og annet kommunikasjonsutstyr (HW og SW) utenfor banken som kundene benytter for å nå frem til nettbanken, samt SW som benyttes i forbindelse med kommunikasjonslinjene, ruterne mv.

- Telelinjene går ned (f.eks. ved graveuhell).
- Utstyret til telecom-leverandøren feiler (f.eks. Telenor, BaneTele, Hafslund, Lyse).
- Brann på Oslo Sentralbanestasjon gjør at Tele2s og Telenors linjer går ned.
- Utstyret har for liten kapasitet.

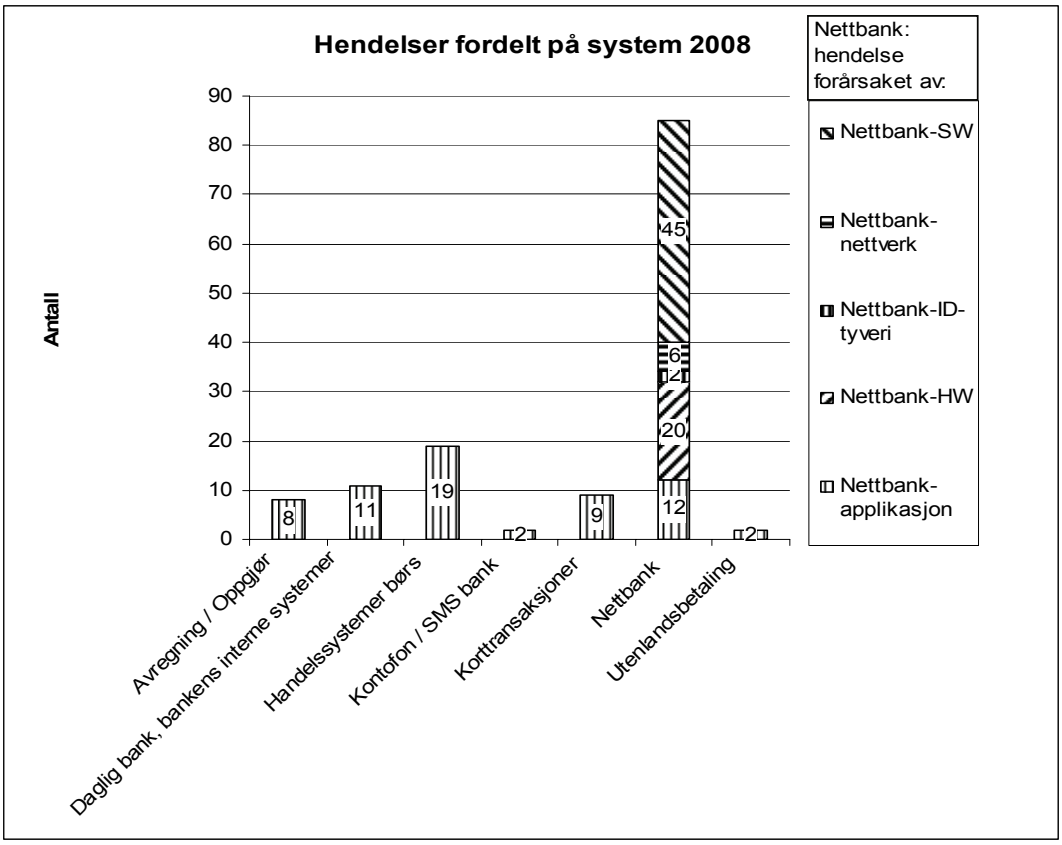
Nettbank-applikasjon: Bankens nettbankapplikasjon.

- For liten kapasitet. Applikasjonen er ikke programmert for å håndtere trafikken.
- Funksjonsfeil
- Feil i en applikasjon utenfor nettbanken får følger for nettbanken.
- Feil i BankID-applikasjonen(e) gjør at nettbanken ikke er tilgjengelig.

Nettbank-ID-tyveri:

- Man-in-the-Middle Attack (MITMA)
- Phishing
- Kombinasjon av phishing og MITMA
- Trojanske hester
- Banken sprer kundedata ved uhell

Aktuelle hendelser knyttet til nettbank fordeler seg da slik:



Rapportene viser at det bør gis større oppmerksomhet mot de tekniske omgivelsene til nettbanken og ikke kun til nettbankapplikasjonen. Dette er en ny kunnskap basert på den samlede hendelsesrapporteringen fra 2008.

3.3.3 Antall rapporterte hendelser målt mot antall faktiske hendelser

Ofte rapporterer flere forskjellige foretak omtrent samtidig om en hendelse, og det viser seg å være hendelser som har rot i samme tekniske feil hos felles leverandør. Det vil si at det i realiteten er færre hendelser enn de 134 hendelsene som er registrert. Det er likevel valgt å registrere hvert enkelt foretaks rapport om hendelsen som en egen hendelse (med unntak av der samme feil rammer alle banker i en bankgruppering som Terra-Gruppen eller SpareBank 1 Gruppen, men disse melder også med felles rapport for gruppen). Bakgrunnen for dette er en vurdering basert på at leverandørene har bilaterale avtaler om leveransen av IT-tjenester med den enkelte bank eller bankgruppering, og på tross av at det er samme tekniske feil som er årsak til hendelsene, kan hendelsene ramme tjenestene ulikt hos de ulike foretakene. I prøveperioden har vi ved ca. ti anledninger sett at samme tekniske feil hos leverandør har

rammet mer enn et foretak. Av våre 134 registrerte hendelsesrapporter kan mellom 30 og 40 spores tilbake til disse 10 faktiske hendelsene. De fleste skjedde hos IT-leverandører, men også feil hos nettverksleverandører forårsaket hendelser som ble rapportert fra flere foretak.

3.3.4 Generelle erfaringer med hendelsesrapportering

Kredittilsynet observerer stor ulikhet i antall rapporterte hendelser fra foretakene, noe som ikke bare kan tilbakeføres til foretakets størrelse eller antall IT-systemer. I forberedelsene til hendelsesrapporteringen var det en utfordring å lage en beskrivelse av hvilke hendelser som skulle rapporteres uten at det ble funnet noe fasitsvar på dette. Rundskrivet kom nærmest i å konkretisere dette ved å si at *"Rapporten skal normalt omfatte hendelser som foretaket selv kategoriserer som svært alvorlige eller kritiske, men kan også omfatte andre hendelser dersom de avdekker spesielt sårbare punkt i applikasjoner, arkitektur, infrastruktur eller forsvarsverk."* (Kredittilsynets rundskriv 31/2007). Dette må tas i betraktning når frekvensen på rapportering fra det enkelt foretak vurderes. Foretakene kan ha ulike skalaer å måle på om en hendelse er alvorlig nok til å kvalifisere for rapportering til Kredittilsynet.

Noen foretak har klart å få i gang en velfungerende hendelsesrapporteringsrutine, mens andre ser ut til å mangle dette. Den oppsummerte erfaringen er at Kredittilsynet har et forholdsvis oppdatert og riktig bilde av IT-virksomheten i foretak Kredittilsynet mottar regelmessig og rutinemessig rapportering fra, mens Kredittilsynet mangler et tilsvarende bilde av IT-virksomheten i foretak det mangler rapportering fra. De fleste foretak befinner seg et sted mellom disse ytterpunktene.

Det totale omfanget av hendelsesrapporter, inkludert underliggende dokumenter med beskrivelse av hendelsesårsak, er en nyttig kilde for å forstå hvordan systemer og nettverk henger sammen. Dette gjelder både innad i foretak, mellom foretak og mellom leverandør og foretak. Selv om den enkelte hendelsesrapport kun gir et fragmentert bilde, er hver rapport en bit i et stort puslespill. Som nevnt stammer mange hendelser fra de samme faktiske tekniske feilene hos felles leverandør. Det er blant annet observert at samme tekniske feil kan ramme ulike forretningsområder i ulike foretak, som for eksempel at hendelsen rammer nettbanktjenestene i en bank og minibanktjenesten i en annen. Samme hendelse kan beskrives ulikt i forskjellige foretak, noe som også fyller ut det totale bildet av situasjonen. Til sammen bidrar informasjon fra hendelsesrapportene som en kilde til kartlegging av infrastrukturen i finanssektoren i Norge.

En viktig del av oppfølgingen av hendelsesrapporteringen er håndteringen av hendelser som vurderes som særlig alvorlige. Hendelsesrapporteringen vil være en informasjonskanal for fortløpende statusoppdatering av situasjonen og danne grunnlag for Kredittilsynets vurdering av om en beredskapssituasjon skal identifiseres. Kredittilsynet vil benytte data fra hendelsesrapporteringen som grunnlag for rapportering til andre myndighetsinstanser som Beredskapsutvalget for finansiell infrastruktur (BFI) og Finansdepartementet.

3.3.5 Hendelser i 2008

I 2008 var hendelsene forholdsvis jevnt fordelt utover året med en liten topp i månedsskiftet juni/juli. Hendelsen som fikk mest oppmerksomhet i media i 2008 var problemene med handelssystemet på Oslo Børs 2. og 3. juni. Da ble Kredittilsynet varslet gjennom hendelsesrapporteringssystemet om morgenen både 2. og 3. juni. Kredittilsynet ble holdt løpende oppdatert om status på feilhåndteringen gjennom påfølgende meldinger begge dagene. Det ble iverksatt tiltak umiddelbart som senere har avdekket rotårsaken til hendelsen.

Det var mange tilfeller med utilgjengelig nettbank som har rammet mange banker samtidig. Det var også gjentakende problemer med handelssystemene i enkelte banker, noe som var særdeles uheldig sett i lys av de store svingningene i aksjekursene høsten 2008. Det var tilfeller av phishing og annen form for ID-tyveri, men ellers ikke registrert vellykkede trojanerangrep eller Man-in-the-Middle-angrep.

Hendelser som gir feil i saldo, er meget alvorlige. I 2008 var hadde slike hendelser rot i feil i applikasjon eller systemprogramvare etter programendring. Heldigvis ble bare et begrenset antall kunder berørt, og bankene klarte å korrigere saldo i ettertid. Opprettingsarbeidet etter denne typen hendelser er svært omfattende og krever ofte betydelig innsats fra involverte leverandører og banker.

Som figuren på side 26 viser, kan de fleste hendelser om nettbank som er innrapportert til Kredittilsynet føres tilbake til softwareproblemer. Det er derfor en stor utfordring å ha kontroll med ”kjøreomgivelsene” som applikasjonene opererer i. Programvaren har en rekke parametre som alle skal settes på riktig måte, og som kan hende må settes på nytt i lys av nytt trafikkmønster, endret konfigurasjon og eller på annen måte endret samspill med omgivelsene. Det å overvåke trafikken og konfigurasjonen og holde programvaren oppdatert slik at den speiler dette, er en stor utfordring.

Foretakene rapporterer om utfordringer knyttet til å vedlikeholde grunnsystemene. Mange av foretakene har flere generasjoner av systemer, fra CICS/PL1, IMS/DL1 og Cobol, til mer moderne systemer. De ulike generasjonene gjenspeiler sannheten som var gjeldende på det tidspunktet de ble til. Det er ulikheter i implementering innenfor de fleste lag i OSI-modellen, med unntak av det fysiske laget, men ulikhetene mellom eldre og moderne teknologi kommer først og fremst til utrykk ved ulikheter i lagdelingen og i brukergrensesnitt. Det er en omfattende jobb å vedlikeholde systemene. Det krever bred kompetanse og god oversikt. Som oftest skal moderne systemer ”snakke” med eldre systemer. Et typisk eksempel er et kundereskontrosystem av eldre dato som fores med data fra et moderne system, og som kan rapportere til et moderne datavarehus. Dette betyr at det må lages mellomvare som knytter systemene sammen. Dette gir risiko i mellomvarekomponentene.

3.4 Andre funn

3.4.1 Grunnsystemene

Mange av foretakene rapporterer om utfordringer knyttet til å vedlikeholde grunnsystemene (de mest sentrale systemene for virksomheten) i sin infrastruktur. Mange av foretakene har flere generasjoner av systemer som gjenspeiler det tekniske utviklingsnivået, metoder, arkitektur mv. på ulike tidspunkter. Det er en utfordring å vedlikeholde systemene og å få dem til å "spille sammen". Observasjonene fra foretakene stemmer godt overens med hendelser som er innrapportert til Kredittilsynet. Av 85 hendelser som har rammet nettbanken, er 45 å henføre til programvare.

Utfordringen med å kontrollere en stadig mer komplisert driftsomgivelse kan løses ved å øke kompetanse og bemanning til man får kontroll, og/eller man kan sanere og forenkle programvareporteføljen.

Kredittilsynet noterer at mange av foretakene har offensive planer for å sanere, slå sammen og forenkle når det gjelder programvare. I noen tilfeller benytter foretaket bare en liten del av funksjonaliteten i en programvare. Men vedlikeholdet av programvaren er ikke tilsvarende liten. Programvaren må parametersettes, sikkerhetsoppdateres ("patches"), versjonsoppdateres mv. som om den var i fullskala bruk, og programvaren forutsetter at omgivelsene oppdateres til bestemte nivåer. Mange foretak går derfor kritisk gjennom programvareporteføljen. Kredittilsynet har sett mange eksempler på foretak som har avinstallert "marginal" programvare og erstattet nødvendig funksjonalitet med egen kode eller en mindre mellomvarekomponent skreddersydd for formålet. Etter det Kredittilsynet erfarer, har foretakene fått en betydelig bedre, mer stabil og mer oversiktlig driftsomgivelse. Kredittilsynet har stor tro på verdien av slik gjennomgang og sanering.

Inngripende og omfattende styreprogramvare gir bindinger og føringer på infrastrukturutvikling. Programvaren reduserer foretakets frihet når det gjelder fremtidig arkitektur. Programvareleverandøren ønsker naturligvis at programvaren i omfattende grad griper inn i foretakets infrastruktur for på den måten å "lime" foretaket fast i programvaren til leverandøren. En gjennomgang og sanering kan som nevnt løse opp i dette "limet" og gir foretaket større frihet med hensyn til fremtidig utvikling.

3.4.2 Tilgangskontroll

For et foretak av noe størrelse er det vanskelig å ha ett system for tilgangskontroller som dekker alle systemer og brukere. Alt avhengig av om det gjelder personlige tilganger, prosesstilganger, databasetilganger mv., så vil prinsippene for å kontrollere tilgangen variere. Prosesstilganger, det vil si tilgangsrettigheter som automatiserte prosesser trenger for å kjøre, kan være definert ved hjelp av brukerID og passord skrevet rett inn i programmet, ved digitale signaturer som verifiseres softwaremessig ved hjelp av nøkler som er mer eller mindre godt beskyttet og eventuelt andre løsninger. Personlige brukerrettigheter blir ofte mer oversiktlig styrt ved hjelp av et dertil egnet administrasjonssystem. Men personlige brukerrettigheter har gjerne vært gjenstand for slitasje, på den måten at brukeren typisk har flere rettigheter enn det som strengt tatt trengs i det aktuelle arbeid. Vi har

sett eksempler på at det er gitt administratorrettigheter til langt flere brukere enn det reelle behovet skulle tilsi.

Flere av foretakene ser det som en utfordring å holde oversikt over alle systemer og områder der det en gang i tiden er satt en rettighet. Mange av foretakene har identifisert dette som et risikoområde og har prosesser på gang for å rette opp i forholdet. Kredittilsynet vil følge opp foretakenes arbeid med dette i 2009.

3.4.3 Testing

Kredittilsynet har erfart at mange av hendelsene som skjedde i 2008, hadde sammenheng med at det i praksis er vanskelig å fullskalateste nye tjenester. Spesielt er fullskalatesting med regresjonstesting i praksis vanskelig å få til. Men enkelte av hendelsene medførte stor skade, og bedre testing hadde derfor lønt seg.

Flere av de nye eller oppgraderte tjenestene i 2008 var sentrale tjenester som i tillegg krevde forutgående oppgradering av programvaren hos brukeren. Ende-til-ende test i en slik omgivelse krever mye koordinering, og kan hende nøyer man seg med en funksjons-/regresjonstest og tester i mindre skala. Dersom implementeringen bærer galt av sted, kan det i praksis vise seg vanskelig å snu. Det å be samtlige kunder rulle tilbake til gammel versjon og koordinere en omstart med gammel versjon, er en temmelig håpløs utgave.

Kredittilsynet erkjenner at det ikke er en enkel oppgave å få til fullskala og produksjonslik test. Teknikere som arbeider på praktisk nivå med systemutvikling og drift, vet hvor viktig det er, men også hvor vanskelig det er å teste tilstrekkelig.

3.4.4 Utkontraktering

Kredittilsynet har i tidligere ROS-rapporter omtalt forholdet mellom finansforetak og IKT-leverandør. Kredittilsynet mener at det fremdeles er store utfordringer og til dels direkte misforståelser knyttet til ansvarsforholdet mellom foretaket og IKT-leverandøren.

Kredittilsynet er kjent med at nettverksleverandører hindrer at finansforetaket gis innsyn i sider ved leveransen som er regulert av IKT-forskriften. Dette er ikke akseptabelt. Det er finansforetaket som skal sikre at IKT-forskriften etterleves når det gjelder foretakets bruk av IKT. Det hviler et særskilt ansvar på finansforetaket når det gjelder IKT levert av underleverandører, jf. IKT-forskriftens § 12. Dersom finansforetaket ikke har tilstrekkelig grunnlag for å vurdere om IKT-forskriftens bestemmelser etterleves når det gjelder tjenesten fra underleverandøren, så kan finansforetaket ikke benytte tjenesten.

4 Systemer for betalingstjenester

4.1 Generelt om betalingssystemer

Betalingssystemloven (lov om betalingssystemer m.v. – 1999-12-17 nr. 95) fastsetter at systemer for betalingstjenester (§ 3-2) skal meldes til Kredittilsynet.

Ved nyutvikling, kjøp eller endringer av systemer for betalingstjenester, skal Kredittilsynet informeres gjennom "Egenmelding for systemer for betalingstjenester" (rundskriv 17/2004).

Meldingene representerer en viktig kilde til informasjon for arbeidet med ROS-analysen. I 2008 mottok Kredittilsynet åtte meldinger om endringer i systemer for betalingstjenester.

I betalingssystemloven er begrepene "interbanksystemer" og "systemer for betalingstjenester" benyttet på systemer som sammen ivaretar transport av pengemessige transaksjoner/meldinger mellom kunder i finansinstitusjoner og mellom banker i interbankmarkedet. Likeledes kravet til den funksjonaliteten som er nødvendig for å understøtte at dette foregår på en betryggende og effektiv måte. Eksempler på interbanksystem er NICS (Norwegian Interbank Clearing System) og NBO (Norges Bank Oppgjør). Systemer for betalingstjenester er for eksempel nettbankløsninger, mobilbankløsninger og brukerstedsløsninger for betalingskort. Betalingssystem kan anvendes som et samlebegrep for interbanksystem og systemer for betalingstjenester.

Handel med varer og tjenester i moderne velregulerte samfunn fungerer optimalt gjennom bruk av effektive betalingssystemer. Finanskrisen har vist at til tross for stor turbulens i de globale finansmarkedene, har betalingssystemene nasjonalt og internasjonalt fungert tilfredsstillende. I denne sammenheng er det viktig å understreke at betalingssystemene består både av transaksjonsinformasjon og pengemessige oppgjør.

Finansnæringens betalingssystemer er transportsystemer med pengemessig oppgjør som alltid er direkte knyttet til en kommersiell transaksjon enten basert på fysiske varer, tjenester eller handel med verdipapirer. Dette er en av finansnæringens grunnleggende funksjoner som i moderne tid har utviklet seg fra rene manuelle operasjoner til dagens elektroniske transaksjoner basert på avansert IKT og anvendte meldingsstandarder under administrasjon av FN, ISO og Bankenes Standardiseringskontor.

Interbanksystemer og systemer for betalingstjenester utgjør to deler i et betalingsoppgjør mellom ulike parter. Norges Bank har tilsynsansvar for interbanksystemer, og Kredittilsynet har ansvar for tilsynet med systemer for betalingstjenester. Samarbeidet er dermed nært i det operative tilsynet både med den løpende aktiviteten i betalingssystemene, og meldeplikten som utløses ved endringer av eksisterende systemer og tjenester, samt ved introduksjon av nye funksjoner og betalingstjenester. De anvendte systemene håndterer nødvendige prosesser mellom kunde og kundens bank, og mellom banker enten direkte eller gjennom oppgjørssentraler og Norges Bank.

I hovedsak omfatter betalingssystemloven alle systemer som gjør det mulig for kunder i finansforetak å overføre penger fra egne og til andres konti ved bruk av ulike betalingsinstrumenter.

Finansforetakenes drift av betalingssystemer er for det meste basert på bruk av IKT, som normalt er en kombinasjon av interne og utkontrakterte prosesser. Regelverket rundt drift og utvikling av slike prosesser dekkes av IKT-forskriften (Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT) – 2003-05-21 nr. 630).

Styring og kontroll av betalingssystemer inngår som et viktig element i vurderingen av operasjonell risiko basert på reglene i Basel II som er innarbeidet i norsk finanslovgivning.

Et nytt betalingsdirektiv som omfatter EU/EØS, vil ved sin ikrafttredelse 1. november 2009 også medføre endringer i eksisterende finanslovgivning, blant annet i betalingssystemloven. Arbeidet med å foreslå hvordan direktivet skal gjennomføres i norsk rett, er godt i gang under ledelse av Norges Bank.

4.1.1 Betalingsinfrastruktur

Betalingsinfrastrukturen bygger teknisk på IKT-infrastrukturen, se kapittel 2.2 Infrastruktur, samt ulike samhandlende foretak. Dette er sentralt for at et betalingssystem skal fungere etter hensikten.

Infrastrukturen vil kunne omfatte foretakets egen organisasjon inkludert avtaler om utkontraktering (datasentraler) og samarbeidsavtaler med andre foretak (andre finansinstitusjoner, avregningssentraler for betalingstransaksjoner, sentralbank).

Infrastrukturens ulike elementer og aktører må samarbeide for å oppnå kostnadseffektivitet og sikker transaksjonsflyt innenfor rammen av tilfredsstillende operasjonell risiko.

Betalingskanaler, betalingsinstrumenter og meldingsstandarder er elementene i betalingsinfrastrukturen som former betalingstjenestene, og som spiller sammen i den finansielle leverandørkjede når betalingstjenester utføres i betalingssystemene.

I hovedsak består betalingssystemene av tre hovedelementer slik de er definert av European Monetary Institute:

1) definisjon av deltakerne i betalingssystemet
2) et sett av betalingsinstrumenter
3) definerte prosedyrer som skal følges.

Når det gjelder den delen av betalingssystemet som i betalingssystemloven er definert som systemer for betalingstjenester, består denne av:

Betalingskanaler
a. Brev
b. Bankfilial/Bank i butikk
c. Elektronisk betalingsterminal (nettbank, mobilbank, butikkterminal mv.)
d. Elektronisk overførte datafiler

Betalingsinstrumenter
a. Koder (i forbindelse med nettbank, mobilbank, butikkterminal mv.)
b. Debetkort
c. Kredittkort
d. E-faktura
e. Avtalegiro
f. Brevgiro
g. Giro (enkel- og masseutsendelser)

Oversikt over meldingsstandarder i betalingsnettverk
a. Egenkontrollerte meldingsstandarder
b. Felleskontrollerte meldingsstandarder
    1. NIBE
    2. SWIFT MT og MX
    3. EMV (Internasjonale betalingskort)
    4. OCR
    5. BOLS
    6. Telepay
    7. EdiFact
    8. ISO (8583, 20022 XML)

4.2 Risiko og sårbarhet i betalingssystemene

På overordnet nivå fungerer NICS som det eneste komplette avregningssystemet for kundebaserte betalingstransaksjoner i norske kroner. Alle norske finansinstitusjoner som tilbyr betalingstjenester, leverer i løpet av dagen transaksjoner til NICS som leverer videre avregnede netto transaksjonsdata til

NBO til bruk for pengemessig oppgjør og kontoføring på finansinstitusjonenes konti i sentralbanken. Deretter oppdaterer de enkelte bankene kundenes konti.

I tillegg har to norske bankgrupper tillatelse fra Norges Bank til å tilby interbanksystem som en tjeneste for andre banker. Konstruksjonen av disse betalingssystemene fungerer som en hybrid ved at transaksjonsavregningen gjøres i NICS, mens det pengemessige oppgjøret gjennomføres på interbankkonti utenfor sentralbanken. I disse betalingssystemene oppdateres kundekonti i noen tilfeller før interbankoppgjør er gjennomført (kreditering før oppgjør). Dette kan både medføre likviditetsmessig risiko og muligheter for tap.

NICS er et robust system som fungerer meget godt innenfor en stabil infrastruktur basert på anerkjente typer meldingsstandarder. Risikoen og sårbarheten i dette avregningssystemet ligger i den enkelte finansinstitusjons kjerne- og kundesystemer og i NICS Drift hos BBS. Slike systemer skal sikre korrekt overføring av betalingsinformasjon og mottak av informasjon om gjennomførte transaksjoner.

I konseptet omkring såkalte nivå 1- og nivå 2-banker mener Kredittilsynet at det er viktig at den enkelte bank må klassifiseres på riktig måte overfor NICS. I motsatt fall kan dette medføre at ulike oppfatninger om eget ansvar for deltakelse i NICS vil kunne føre til at det enkelte foretak vurderer operasjonell risiko på feil måte, og har en misforstått oppfatning av hvor det endelige ansvaret for transaksjonene ligger. Kredittilsynet mener at det er nødvendig med en ny analyse og en klar presisering om hvordan ulike betalingssystemer skal oppfattes og drives i henhold til betalingssystemloven.

Økende risiko i betalingssystemene er også identifisert ved at særlig nyere mindre banker oppfatter deltakelse i betalingssystemer for enkelt. Troen på at disse bankenes tilbud av betalingstjenester kan basere seg på et ”plug and play”-konsept hvor banken raskt kan knytte seg til eksisterende systemer, kan føre til manglende håndtering av operasjonell risiko. Her hviler ansvaret for denne oppfatningen på flere aktører i betalingsinfrastrukturen. Kredittilsynet vil gjennom kontakt og tilsyn med ulike bankgrupper og enkeltbanker påpeke disse svakhetene for å bidra til en akseptabel håndtering av risiko.

Den økende konkurransen mellom finansinstitusjonene og deres tilbud til kunder om kontinuerlig døgnåpne elektroniske betalingskanaler, kan medføre økt risiko i betalingssystemene. Dette kommer delvis fra hyppige konseptuelt baserte krav fra forretningsområdene om produkt og tjenestetilpasninger. En annen faktor er mulighetene til operasjonelt å gjennomføre slike tilpasninger i en stadig mer kompleks IKT-infrastruktur hvor tid for tilstrekkelig testing blir utfordret. Risikobildet kan reduseres noe ved en mer formalisert horisontal organisatorisk fokusering, gjennom bedre samordning mellom bankenes inntektsfokuserte forretningsområder og de kostnadsbaserte operasjonelle områdene, i særdeleshet IKT.

5 Beredskap – Nasjonal øvelse IKT-08

5.1 Øvelse IKT-08

Direktoratet for samfunnssikkerhet og beredskap (DSB) og Nasjonal sikkerhetsmyndighet (NSM) gjennomførte i 2008 en nasjonal øvelse kalt Øvelse IKT-08. Øvelsen skulle fokusere på samfunnets evne til å være forberedt på, oppdage og håndtere et massivt angrep på digital infrastruktur i Norge og omfattet sektorene finans, tele, energi og olje og gass. Virksomheter innen disse sektorene ble invitert til å delta i øvelsen. Kredittilsynet deltok sammen med åtte finansinstitusjoner i øvelsen, og Kredittilsynet hadde rollen som koordinator for finanssektorens deltakelse i øvelsen. Foretak både fra verdipapirsektoren, banksektoren og IT-leverandørene var representert. Utenom foretakene som var direkte involvert i scenarioene, var også bankforeningene med i planlegging og gjennomføring av øvelsen.

Øvelsen var papirbasert uten tekniske inngrep i systemene og med følgende målsetninger for øvelsen:

- Ansvars- og rolleforståelse ved de ulike beslutningsnivåene før, under og etter en hendelse
- Hensiktsmessigheten ved etablert planverk
- Informasjonsdeling vertikalt og horisontalt for de ulike beslutningsnivåene før og etter en hendelse
- Mediehåndtering og krisekommunikasjon til kunder/befolkningen før, under og etter en hendelse.

Øvelsen la opp til å skape virkelighetsnærhet for deltakerne. Et øvingsteam dekket hendelsene som journalister, og produserte ulike nyhetsinnslag til en nettbasert mediasimulator.

Selve øvelsen fant sted 1.–3. desember 2008. En rekke hendelser rammet finanssektoren disse dagene hvor alvorlige tjenestenektangrep (Distributed Denial of Service) mot nettsteder for finansielle tjenester som nettbanker m.m. dominerte. I tillegg var det også andre former for ondsinnede angrep mot elektroniske tjenester.

5.2 Oppsummering etter øvelsen

Finansforetakene opplevde det som et stort pluss å få anledning til å øve sammen med andre foretak i egen og andre sektorer i et omfang det er vanskelig og komplisert å tilrettelegge alene. Dette ga finansforetakene muligheten til, i tillegg til å teste intern kommunikasjon, å teste kommunikasjon mot eksterne leverandører og myndigheter. Varslingslister og samarbeidspunkter/-kontakter ble oppdatert.

Finanssektoren fikk gjennom denne øvelsen trent på en situasjon der mange finansforetak blir rammet av samme hendelser iverksatt av eksterne angripere. Det viktigste for finansforetakene i en krisesituasjon er å gi korrekt informasjon og unngå panikk blant publikum. Øvelsen viste at i en krisesituasjon må det raskt kunne iverksettes kontinuerlig medieovervåking, og tilhørende oppbemanning i foretakenes kommunikasjonsenheter for å håndtere et forventet medietrykk.

Øvelsen viste videre at det er vanskelig å få et konsistent og riktig totalbilde av en situasjon der mange foretak er rammet av hendelser samtidig og informasjonen i media er sprikende. Det ble registrert underrapportering til Kredittilsynets rutine for hendelsesrapportering under øvelsen. Hovedsakelig skyldtes dette øvingsteknisk svikt, men det kan heller ikke utelukkes at det er en viss treghet i foretakenes rapportering til Kredittilsynet. Foruten hendelsesrapporteringen til Kredittilsynet, er det ingen automatikk i at informasjon fra finansforetak tilflyter andre finansforetak eller felles instanser.

Selve angrepene håndterte finanssektoren operativt, det vil si at det ble ikke behov for å be Finansdepartementet sette i verk tiltak. Internettbaserte tjenester i finanssektoren er ikke like kritiske som for eksempel butikkterminaler og minibanker. Finansforetakene fikk trent på iverksettelse av reserveløsninger ved tjenestenektangrep. Scenariene i finanssektoren trigget videre øvingsscenarier for NorCERT, Post- og teletilsynet samt teleleverandørene som deltok, i forhold til å overvåke angrepene mot nettet og iverksette tiltak fra deres side.

6 Identifiserte risikoområder

6.1 Gjennomføring av katastrofetest

IKT blir i stadig økende grad viktig for foretakets forretningskritiske prosesser. Dette sammen med at et økende behov for tjenester krever døgnkontinuerlig drift året rundt, gjør det viktig å sikre egen kontroll med organisasjons data og IKT-infrastruktur i tilfelle en katastrofesituasjon. Et omfattende og detaljert planverk er avgjørende for hvor raskt en kan gjenopprette de forretningskritiske prosessene. Et slikt planverk krever at det er etablert en prosess som sikrer at relevant dokumentasjon oppdateres ved endringer i IKT-infrastrukturen, endringer i ledelse, endringer i varslingslister, endringer i innkjøpsprosess og lignende.

I IKT-forskriftens §§ 10 og 11 stilles det krav til at det skal gjennomføres opplæring, øvelse og testing av reserveløsningene minst én gang årlig og i et omfang som gir trygghet for at reserveløsningene fungerer tilfredsstillende. Testene skal dokumenteres slik at gjennomføring og resultat kan vurderes i ettertid.

Kredittilsynet vurderer testing av katastrofeløsningen som et avgjørende element for å sikre at foretaket har evne til å videreføre egen drift i en katastrofesituasjon. Bare gjennom testing av planverket kan en avdekke mangler og svakheter. I større foretak kan det å gjennomføre omfattende katastrofetester i stor grad være ressurskrevende slik at en ikke hvert år gjennomfører "live" tester, men at de delene av foretakets planverk som ikke tas med i testen, gjennomgår særlig risiko- og sårbarhetsanalyse.

Kredittilsynets vurdering er at det å dokumentere resultatet av katastrofetester og tilhørende risikoanalyser, er avgjørende for å kunne gjennomføre oppfølging og forbedring av det testede katastrofeplanverket. Detaljeringsgraden i testene er avgjørende for kvaliteten. Løse og omtrentlige planer vil ikke være tilstrekkelig for foretak med strenge krav til tilgjengelighet av IKT-infrastrukturen. Kredittilsynet vil gjennom sine IT-tilsynsaktiviteter særlig legge vekt på foretakenes katastrofeplaner med tilhørende ROS-analyser og testresultater.

6.2 Konfigurasjonsstyring

Finansielle tjenester blir i stadig større grad automatisert. Omfanget av og bruken av finansielle tjenester på Internett øker, og økt bruk av elektroniske tjenester gjør samfunnet stadig mer avhengig av kvaliteten på tjenestene, og ulike typer hendelser kan få store konsekvenser.

Et foretaks IKT-infrastruktur omfatter alle fysiske komponenter, operativsystem, nettverk, systemer for overvåking og drift. Selv for mindre foretak kan den tekniske infrastrukturen være kompleks og omfattende. Med økende krav om tilgjengelighet til foretakenes IKT-infrastruktur, stilles det også strengere krav til kvalitet, og ofte forbindes konfigurasjonsstyring med kvalitetsbegrepet.

Hensikten med konfigurasjonsstyring er å holde oversikt over alle komponenter i en IKT-infrastruktur, sammenhengen mellom dem og hvilken versjon komponentene har. Dette er viktig informasjon, særlig for organisasjonen som står for driften av IKT-infrastruktur, for å kunne tilby høy grad av kvalitet i utførelsen av prosessene endringshåndtering og problemhåndtering. Foretak med høye krav til tilgjengelighet har i regelen strenge krav til konfigurasjonsstyring.

Av erfaring ser en at de fleste hendelser som fører til nedetid i komponenter i IKT-infrastrukturen, oppstår med bakgrunn i feil i planlagte endringer. Dette kan tyde på at IKT-infrastrukturen ikke i tilstrekkelig grad er kartlagt og dokumentert. Det er dermed uklart hvilke versjoner av ulike komponenter som er i bruk og hvilke avhengigheter de ulike komponentene har mot andre komponenter. Kredittilsynets vurdering er at dette er et område som med fordel kan vektlegges i større grad. IT Infrastructure Library (ITIL)'s rammeverk regnes av mange som beste praksis for leveranser av IKT-tjenester og kundestøtte.

6.3 Nettverk

Et nettverk er en infrastruktur som gjør at to eller flere datamaskiner kan snakke sammen. Et enkelt nettverk kan bestå av to datamaskiner som kommuniserer gjennom kabel, infrarød forbindelse, Bluetooth eller lignende. Større nettverk kan ha flere hundre tusen maskiner tilkoblet i en og samme IKT-infrastruktur. Tradisjonelt sett har også finansnæringen utkontraktert store deler av nettverksleveransene til leverandører av nettverkstjenester.

Kredittilsynet har gjennom § 3 i IKT-forskriften stilt krav til hvert enkelt foretak at det skal minst årlig gjennomføre ROS-analyser av hele IKT-infrastrukturen, og dette omfatter også nettverksleveranser. En rekke finansforetak arbeidet i 2008 med å kartlegge sårbarheter og trusler i foretakets nettverksinfrastruktur i detalj, nettopp med tanke på å finne løsninger som kan gi større grad av sikkerhet for tilgjengelighet av foretakets tjenester. For å kunne gjennomføre ROS-analyser som omfatter hele IKT-infrastrukturen, må kunnskap om foretakets nettverksløsninger være tilgjengelig.

Flere foretak melder at det i mange tilfeller kan være vanskelig å få oversikt over nettverksinfrastrukturen.

Kredittilsynet er blitt informert om at det er tilfeller der det har vært vanskelig for foretak å få teleleverandørene til å redegjøre for hvordan topografien i foretakets nett er. Kredittilsynet vurderer det som viktig at foretakene har tilgang til tilstrekkelig informasjon om hele IKT-infrastrukturen for å kunne vurdere egen eksponering i forhold til risiko. Som nevnt tidligere dreier dette seg også om kunders rett og plikt til å undersøke det produktet en kjøper.

6.4 Offshoring

Kjøpere av utkontrakteringstjenester flytter i økende grad arbeid til land der prisene er lavere. Denne utviklingen er tydelig å se også i Norge, hos leverandører som Accenture, EDB Business Partner ASA og Capgemini. Selv om lavere kostnader forblir en viktig driver for fremveksten av såkalte Globale leveransemodeller (GLM), søker mer "modne" kjøpere også bedre dekning av sine behov for å få tak i den kapasiteten av arbeidskraft de behøver. GLM er fremdeles et ferskt konsept, derfor kan det være grunn til å anta at det å levere robust og konsistent service gjennom GLM kan by på utfordringer.

For om lag ti år siden startet store globale aktører som IBM og Accenture med utvidet virksomhet i India. India vil fortsatt være det viktigste GLM-landet på mellomlang sikt, men flere land er kommet etter, som landene i Baltikum, Ukraina og Filippinene. Både IT-tjenesteleverandører og kunder av disse har i en viss utstrekning valgt å etablere seg i India og noen andre land, ofte gjennom oppkjøp av lokale selskaper. I de siste årene har indiske leverandører økt sin årsomsetning med ca. 60 prosent i Europa.

Applikasjonstjenester var det første området som ble utkontraktert og flyttet til et annet land. Antall tjenester som kan anskaffes gjennom GLM er økende, og for eksempel testtjenester er blitt et standardtilbud. Enkelte tjenestetyper er i et tidlig stadium og vil etter Gartner Groups vurdering kunne ta noe tid for å modnes. Blant annet er infrastrukturtjenester (teknisk drift) og forretningsprosesser fortsatt relativt umodne områder sammenlignet med applikasjonstjenester.

Ujevn kvalitet, utfordrende håndtering av personalvekst og stor gjennomstrømning av ansatte skaper ofte store utfordringer for både kunder og leverandører. For å kunne takle denne type utfordringer, er det Kredittilsynets vurdering at det må eksistere sterke bedriftskulturer. Foretak som har lykkes i å etablere seg i India og andre land det er aktuelt å utkontraktere til, er i hovedsak foretak som tradisjonelt sett har sterke bedriftskulturer og overfører denne til organisasjonen i "offshoringslandet".

6.5 Endringshåndtering

Endringshåndteringsprosessen er en viktig prosess som omfatter det å motta endringsønsker, kategorisere, vurdere behov, planlegge, vurdere kost, analysere risiko, teste, godkjenne, implementere og rapportere status. Formålet med prosessen er at man ønsker å oppnå kontroll over alle endringer i foretakets IKT-infrastruktur og dermed også redusere risikoen ved endringer.

Kredittilsynet har sett en klar forbedring i foretakenes arbeid med prosesser og rutiner som bygger opp under en forbedret endringshåndtering i foretakene. Dette har også vært nødvendig siden endringstakten har økt. For at endringshåndteringsprosessen skal fungere etter hensikten med tilfredsstillende kvalitet, er det etter Kredittilsynets vurdering avgjørende å ha tilstrekkelig dokumentasjon og kunnskap om IKT-infrastrukturen.

Årsaken til at et relativt stort antall endringer feiler, er etter Kredittilsynets vurdering todelt. Den ene årsaken er kvaliteten på risikoprosessen og hvilke aktiviteter som denne prosessen iverksetter fra en endring meldes inn og til endringen er implementert. Den andre årsaken, og etter Kredittilsynets vurdering den mest vanlige, er at den etablerte prosessen med rutiner ikke følges i tilstrekkelig grad. Den sist beskrevne årsaken kan i stor grad spores tilbake til den kulturen foretakets IT-organisasjon har til etablerte prosesser.

7 Kredittilsynets videre oppfølging

7.1 Aktuelle tiltak

De viktigste tiltakene som kan gjøres for å håndtere operasjonell risiko er tiltak som ivaretas i det enkelte foretak under tilsyn. Det er først og fremst gjennom dette helt grunnleggende forholdet at vi kan oppnå en hensiktsmessig håndtering av risiko. De tiltakene som Kredittilsynet kan ivareta som tilsynsorgan, vil i hovedsak være:

- Sørge for gjennomføring av IT-tilsyn i et omfang og med en detaljering som gjør at Kredittilsynet får et realistisk bilde av hvordan foretakene benytter IKT, håndtering av risiko og etterlevelse av regelverk.

- Tiltak for å støtte foretakene i deres egne aktiviteter. Dette kan for eksempel være opplærings- og veiledningsmateriale. Kredittilsynet deltar aktivt i samarbeid internasjonalt og nasjonalt, på områder knyttet til IKT-risiko.

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

- Sørge for en aktiv forvaltning av regelverk knyttet til operasjonell risiko på IKT-området og til en hver tid formulere relevante krav til virksomhetsområder og bruk av IKT der dette kan være hensiktsmessig for å sikre en betryggende håndtering av risiko.

- Kredittilsynet vil i 2009 arbeide for at teleleverandørene stiller til disposisjon nødvendig og presis informasjon. Det dreier seg i bunn og grunn om kundens rett til å undersøke produktet som de kjøper. Denne retten er lovfestet, jf. kjøpsloven § 3, som gir kunden en rett og *plikt* til å undersøke leveransen.

I arbeidet med operasjonell risiko knyttet til finanssektorens bruk av IKT har Kredittilsynet etablert ulike virkemidler. Nedenfor vil vi redegjøre for hvordan det videre arbeidet med virkemidlene innrettes slik at dette kan bidra til en forsvarlig håndtering av operasjonell risiko.

7.2 IT-tilsyn

Arbeidet med gjennomføring av IT-tilsyn i tilstrekkelig omfang vil fortsette. Dette er et helt vesentlig virkemiddel og egnet til "temperaturmåling" av hvordan finanssektoren håndterer bruk av IKT og risiko knyttet til dette. Utfordringen blir å videreutvikle tilsynsopplegget slik at relevante problemer kan identifiseres gjennom mest mulig rasjonell resursbruk, både hos tilsynsenhetene og hos Kredittilsynet.

Erfaringen Kredittilsynet gjør gjennom IT-tilsynene må aktivt utnyttes som "temperaturmålinger" for å iverksette egnede tiltak og som grunnlag for gradering og sammenligning av relevante foretak.

Arbeidet med å videreutvikle IT-tilsynsopplegget i separate moduler vil fortsette slik at dette er best mulig egnet til behovet for å sette sammen hensiktsmessige moduler knyttet til det enkelte planlagte IT-tilsyn.

Det er et mål å legge de enkelte tilsynsmodulene tilgjengelige på Kredittilsynets nettsted slik at disse enkelt kan hentes og benyttes i foretakenes eget arbeid med operasjonell risiko og IKT-sikkerhet.

7.3 Videreutvikling av opplegget for meldeplikt for systemer for betalingstjenester

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

Meldeplikten er omtalt 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 vesentlige for etablerte systemer, vil utløse meldeplikt. Rundskrivet og skjemaet er tilgjengelige på Kredittilsynets nettsted.

Kredittilsynet arbeider med et opplegg for i større grad å kunne, uavhengig av de meldingene som mottas i medhold av loven, identifisere mulige problemer knyttet til systemer for betalingstjenester.

Likeledes er det nå laget en ny tilsynsmodul for systemer for betalingstjenester som vil benyttes i en kombinasjon av IT-tilsyn og oppfølging av arbeidet med å sikre kvalitet og risikohåndtering på betalingstjenestene. Denne modulen er planlagt å være tilgjengelig på Kredittilsynets nettsted i første halvår av 2009.

7.4 Risiko- og sårbarhetsanalyser (ROS)

Gjennomføring av regelmessige ROS-analyser for sikre seg forståelse av den risikoen som foreligger, og på det grunnlaget iverksette tiltak på områder der dette er nødvendig, er viktige forutsetninger for hensiktsmessig risikohåndtering.

Dette er hovedgrunnen til at IKT-forskriftens § 3 Risikoanalyse stiller krav om gjennomføring av årlige risikoanalyser.

Det viktigste tiltaket Kredittilsynet kan gjøre, er å påse at foretak under tilsyn etterlever § 3. Som nevnt tidligere, vurderer Kredittilsynet at det å gjennomføre ROS-analyser er en krevende oppgave og forutsetter kunnskap om gjennomføring av slike prosesser samtidig som det er nødvendig å ha tilgang på tilstrekkelig kompetanse på de forretnings-, og teknologiområdene som ROS-analysen skal omfatte.

For å bidra til dette, har Kredittilsynet utarbeidet en enkel veiledning til etterlevelse av § 3. Det finnes mange relevante standarder og metoder for å gjennomføre ROS-analyser. Det er derfor viktig at foretakene tilegner seg de kunnskapmessige forutsetningene for å sikre gjennomføring av ROS-analyser, noe som er et ledelsesansvar.

Kredittilsynet vil på sin side fortsette med å gjennomføre årlige ROS-analyser på tvers av finanssektoren for å skaffe seg innsikt og kunnskap som i neste omgang kan benyttes som grunnlag for videre oppfølging av foretakene. Videreutvikling av kompetanse og teknikker for å sikre en best mulig måte å gjennomføre ROS-analysene på, vil derfor være viktig.

Det internasjonale foretaket ECM, som har IKT-sikkerhet som viktig forretningsområde, har uttalt som en problemstilling at: *"Organizations cannot secure what they do not manage"*. Utsagnet er ment å adressere det grunnleggende. Har en virksomhet ikke sørget for å sikre en hensiktsmessig administrering, organisering, ansvarsklargjøring, dokumentert og skrevet aktuelle prosesser og prosedyrer, sikret ledelsesmessig kapasitet og kompetanse, blir det vanskelig å etablere sikkerhetsløsninger og hensiktsmessig håndtering av risiko. Det er de grunnleggende elementene som må på plass først for deretter å bygge nødvendig opplegg for håndtering av risiko og sikkerhet.

Et annet viktig arbeid som Kredittilsynet startet i 2008, er kartlegging av IKT-infrastruktur som benyttes i finanssektoren. Det foreligger allerede viktige konklusjoner fra arbeidet i 2008 knyttet til styring og kontroll, tekniske problemområder og leverandørforhold. En rapport fra arbeidet vil bli utarbeidet som foreløpig resultat og fulgt opp mot de aktuelle enkeltforetakene og samarbeidsopplegg, samtidig som arbeidet på dette området vil fortsette inn i 2009.

7.5 Hendelsesregistrering og rapportering

Prøveordningen for hendelsesrapportering, som ble etablert fra november 2007, er besluttet videreført inntil videre. Evalueringen har vist at dette er et nyttig tiltak for å sikre korrekt informasjon om hendelsesbildet i finanssektoren og som gir et godt grunnlag for analyser og tiltak. I 2009 vil nødvendig arbeid startes opp for å innarbeide fremtidig hendelsesrapportering i IKT-forskriften med sikte på at dette blir et forskriftsregulert opplegg.

I arbeidet med ROS-analysen for 2008 var hendelsesdatabasen en viktig kilde. Informasjon fra hendelsesdatabasen vil bli benyttet som et analysegrunnlag til aktivt å ta opp problemstillinger på IKT-områder som krever tiltak.

7.6 Informasjon og kommunikasjon

Arbeidet med å videreføre møteplasser og tett dialog med bransjeorganisasjoner og andre relevante samarbeidsparter vil fortsette. Sentrale rapporter og veiledninger publiseres på Kredittilsynets nettsted, blant annet for å bidra til økt kunnskap og forståelse for IKT-risikohåndtering og -sikkerhet i det enkelte foretak.

I 2008 holdt Kredittilsynet 30 eksterne foredrag om temaer knyttet til IKT-risiko og -sikkerhet. Utgangspunktet er å forsette den linjen vi har holdt til nå hvor vi på forespørsler fra enkeltforetak, bransjeorganisasjoner og andre relevante samarbeidspartnere stiller oss positive til å bidra.

Arbeidet med å utvikle veiledningsmateriell vil fortsette. Viktige temaer i 2009 er blant annet IKT-styring og -kontroll og beredskapsplaner og katastrofeløsninger.

Kredittilsynet
Østensjøveien 43
Postboks 100 Bryn
0611 Oslo

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

Milamaster as

Foto: Jarle Nyttingnes

02.2009/700