FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

RAPPORT

RISIKO- OG SÅRBARHETSANALYSE (ROS)

2009

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Risiko- og sårbarhetsanalyse (ROS) 2009

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Finanstilsynet, 10. mars 2010

Innhold

1 Innledning

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

Formålet med ROS-analysen er å se hele finanssektoren under ett basert på informasjon Finanstilsynet har innhentet fra foretakene i løpet av 2009. Informasjonen kommer fra tilsyn, intervjuer og hendelsesrapportering fra foretakene. I tillegg er nasjonale og internasjonale kilder benyttet. Gjennom analysene og dataene Finanstilsynet har tilgang til, kan risikoutviklingen knyttet til finanssektorens IKT-systemer følges over tid. Dette gjør det mulig å identifisere problemområder og iverksette tiltak på tvers av finansnæringen.

Rapporten tar sikte på å gi et mest mulig korrekt bilde av risikosituasjonen og dermed være en nyttig informasjonskilde for enkeltforetak som arbeider med egen risikosituasjon. Et viktig mål i denne sammenheng er bruk og presentasjon av kvantitative data som informasjon for å kunne se omfang og utvikling av identifiserte problemområder.

ROS-analysen kan også gi indikasjoner på hvordan sektoren overholder regelverket og etterlever standarder og bransjemessige normer.

Hendelsesrapportering for foretak til Finanstilsynet ble etablert som en frivillig ordning fra november 2007 der finansforetakene varsler om uregelmessigheter eller feil i betalingssystemer til e-postadressen hendelse@finanstilsynet.no. Ordningen ble fra 1. desember 2009 iverksatt som en pliktig rapportering gjennom endring i IKT-forskriften.

I ROS-analysen for 2009 presenterer vi også resultater fra Finanstilsynets arbeid med IKT-infrastruktur og analyse av problemstillinger knyttet til flytting av IKT-oppgaver ut av Norge. Hensikten med dette arbeidet er å identifisere mulige mangler i styring og kontroll og å identifisere risikoområder og sårbarheter i teknisk infrastruktur som krever tiltak eller oppfølging fra myndighetene.

2 Teknologi og utviklingstrekk

Det er mange generelle utviklingstrekk i finanssektoren som påvirker foretakenes bruk av informasjonsteknologi. Finanstilsynet har identifisert følgende områder det er viktig å forstå effekten av for operasjonell risiko.

2.1 Cloud Computing – IKT-drift i nettskyen

Cloud Computing (CC)[1] er en ny måte å operere driften av internettbaserte tjenester på. CC leverer prosessorkraft, båndbredde og lagringskapasitet et sted i nettskyen, i motsetning til tradisjonelle datasentre som håndterer drift for ulike kunder atskilt i separate partisjoner. Tilbyderen av CC stiller til rådighet en maskinpark som kan utføre parallell prosessering, multipleksing og datalagring for mange ulike kunder i en størrelsesorden ordinære datasentre vanskelig kan konkurrere med. Summen av datakraft gjør det mulig å skalere bruk av dataressursene mer hensiktsmessig, og kunden betaler etter et såkalt *pay as you go*-prinsipp. Ved å betale for faktisk bruk, kan det bli billigere for kunden å bruke CC enn å skalere egen kapasitet etter maksimal belastning, eventuelt stå i fare for å underdimensjonere egen kapasitet og oppleve misfornøyde sluttbrukere/kunder. Likeledes kan den økonomiske risikoen bli redusert når en tilbyr nye tjenester man på forhånd ikke kjenner bruksmønsteret til.

Det er tre ulike modeller for CC med ulik grad av standardiserte tjenester. I den ene enden av skalaen tilbys CC som nærmest ren datakraft i form av prosessorkraft, lagringsplass og IP-nettverk (*Cloud Infrastructure as a Service*). Modellen setter ingen begrensinger på type applikasjon eller programvare som kan driftes i skyen da kunden tar hånd om dette selv. På den annen side kan ikke CC fullt ut tilby automatiske løsninger for skalerbarhet og reserveløsninger fordi replikering og konsistenskontroller av data er applikasjonsavhengige.

I den andre enden av skalaen finner man CC basert på web-applikasjoner bygd på en tradisjonell 3-lags modell med tydelig separering av laget for prosessering og laget for datalagring (*Cloud Service as a Service*). Kunden bruker applikasjonene gjennom en tynn klient, ofte en web-leser, og kunden har kontroll bare med dette laget. Modellen stiller altså strenge krav til applikasjonsstandardisering,

[1] National Institute of Standards and Technology (NIST):
http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

inkludert datalagring. Til gjengjeld medfører dette en forutsigbarhet som gjør det mulig for CC å tilby avanserte mekanismer for å sikre skalerbarhet og tilgjengelighet.

Midt på skalaen finner man en modell som er en mellomting mellom de to nevnt over. Brukeren kan til en viss grad velge programmeringsspråk og verktøy for applikasjonene, men kan ikke kontrollere underliggende operativsystem eller omgivelsene applikasjonene kjører i. CC kan tilby automatisk konfigurering og skalering i skyen, men brukeren må angi noen spesifikasjoner ved applikasjonene for at dette skal være mulig.

CC kan bidra til å overføre risiko fra den som er eier av tjenesten til den som er leverandør av tjenesten fordi brukerne av CC kan sikre seg forutsigbar drift ved å lene seg på den elastisiteten i ressurstilgang og kapasitetstilpasning som CC tilbyr. Videre kan CC gi stordriftsfordeler i form av spesialkompetanse på maskiner, maskinprogramvare, nettverk og sikkerhet som det kan være vanskelig for et mindre foretak å ha selv.

European Network and Information Security Agency (ENISA) har laget en rapport der de vurderer risikoen ved bruk av CC.[2] Den første risikoen de tar opp, er risikoen for tap av styring og kontroll. Dette er en risiko man til en viss grad må være villig til å ta om man ønsker å hente ut gevinster av CC.

Den neste risikoen ENISA tar opp, er risikoen for *data lock-in*. Dette omfatter hvilken garanti kunden har for å hente egne data tilbake dersom han/hun ønsker å bytte driftsleverandør, eller dersom driftsleverandøren skulle gå konkurs eller rammes av andre typer hendelser som setter driftsleverandør ut av spill. For å kompensere for risikoene, må kunden iverksette tiltak som sikrer eierskap og kontroll over egne data. Slik denne teknologien ser ut for øyeblikket, gjelder dette en rekke risikoområder som blir aktualisert dersom finansforetak begynner å bruke CC. Finanstilsynet er ikke kjent med at finansforetak i Norge har tatt denne teknologien i bruk.

CC blir vurdert som en av de store innovasjonene innen datateknologi de neste årene. Teknologien er fortsatt umoden, og mye utvikling gjenstår. Selv om konseptet er umodent som teknologi, er dette også et område som medfører utfordringer knyttet til foretakenes gjennomføring av ROS-analyser. Overholdelse av dagens regelverk i forhold til CC vil også kunne bli en utfordring for foretakene.

[2] ENISA: ”Cloud Computing: Benefits, risks and recommendations for information security” (nov. 2009)
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/

2.2 Infrastruktur

2.2.1 Innledning

Finansielle tjenester er i stadig større grad automatisert, og de er i realtid i et elektronisk samspill ende til ende mellom samhandlende parter i den tekniske infrastrukturen.

De elektroniske transaksjonskjedene kjennetegnes ved at de er automatiserte, og bestillinger skjer i realtid – kunden blir ferdigekspedert "der og da". Disse transaksjonskjedene blir stadig mer omfattende, og denne trenden fortsetter i 2010. Et eksempel er bruk av BankID for å signere elektroniske dokumenter, sammen med tilbud til kunden om å oppbevare dokumenter i elektronisk arkiv. Mange av transaksjonene blir behandlet i realtid med den følge at dersom systemer ikke er tilgjengelige, er dette godt synlig for brukerne.

2.2.2 Vedlikehold

Den globale finanskrisen kan føre til mangel på investeringer i kritisk infrastruktur i enkelte sektorer. Kritisk infrastruktur blir svekket som følge av alder og slitasje, mens krav til service og ytelse øker. Utdaterte systemer blir "klattet på", noe som kan føre til ytterligere svakheter. Erfaring indikerer at tilgang til strøm, vannforsyning, eldre generasjoner av datasystemer og transportinfrastruktur er sårbare områder.

2.2.3 Nye kanaler

I 2009 så vi fremvekst av nye kanaler for finansielle tjenester. Mobilbank og BankID på mobil er eksempler. Av flere grunner er dette positive tilskudd til distribusjon av slike tjenester.

For det første blir tjenestene mer robuste i og med at det nå finnes flere "veier" fra kunden inn til banken. Dersom fastlinjene svikter, kan kunden i visse tilfeller benytte mobilbanken.

For det andre gir dette en mulighet for sikrere autentisering av kunden. Risikoen for såkalt *phishing* kan reduseres. Et eksempel på phishing er at en svindler presenterer bankkunden for en falsk innloggingsside, for på den måten å tilrane seg kundens identitetskjennetegn. En slik fremgangsmåte er ikke mulig dersom identitetskjennetegn blir sendt over mobilnettet. Skal svindleren kunne tilegne seg kundens elektroniske identitetskjennetegn, må kunden da kunne avlytte både internettsesjonen og informasjonen som går over mobilnettet, noe som er et betydelig mer komplisert angrepsscenario.

Nye muligheter, som direkte mobilbank, SMS-bank, betalingskort med RFID-teknologi, generell autentisering og signering av dokumenter kan gi nye sårbarheter. Det blir økt kompleksitet ved at flere av tjenestene vil kunne benytte flere kanaler, for eksempel både SMS, blåtann og RFID-teknologi, flere operativsystemer og nye protokoller.

Det mangler standarder for mobile tjenester generelt og for mobilbank spesielt. Den internasjonale standardiseringsorganisasjonen ISO arbeider med å definere krav til mobilbank i forhold til andre standardiseringsorganisasjoners arbeid og i forhold til andre tjenester enn betaling, men dette viser seg å være utfordrende. Chip blir foreløpig oppfattet som sikker teknologi, men brikken skal kommunisere i usikre mobiltelefoner til nye lite testede kanaler og brukergrensesnitt. I tillegg kommer de avtalemessige utfordringene ved ansvar for ulike tjenester fra ulike leverandører på samme mobiltelefon.

2.2.4 Drift

På området IKT-utvikling (design, prototyping, koding, testing) er det introdusert effektive og sikre metoder og verktøy i senere år, for eksempel .Net og arbeidsmetoder som Scrum og Lean.

Det er produsert en rekke nye kundebetjente tjenester, og det forventes at disse skal være tilgjengelige til enhver tid. Denne strømmen av nyutviklede tjenester skal driftes med høye krav til tilgjengelighet og med mange avhengigheter, lange sammenhengende prosesskjeder og ditto avhengigheter. På driftsområdet har mulighetene for effektivisering vært mer begrenset enn innenfor utvikling. Av denne grunn er IKT-drift blitt en mye større utfordring relativt sett enn i tidligere år. Utfordringene er mangeartede.

De lange transaksjonskjedene er avhengige av at alle leddene fungerer. Ved at ett ledd i kjeden ikke fungerer som forutsatt, kan det medføre at hele tjenesten blir utilgjengelig.

En rekke programmer og driftstjenester utgjør kjøreomgivelsen som tjenesten er avhengig av; operativsystem, web-server, applikasjonsserver, sertifikattjenester, nettverkstjenester osv. Programmene har en rekke parametre som skal settes riktig, vedlikeholdes, fornyes og tunes i lys av endring i belastning, kjøreomgivelse, nye versjoner og sikkerhetsoppdateringer. Dette puslespillet krever en nitid oppfølging og god oversikt. Det er derfor viktig at en så langt som mulig er grundig i utvikling, vedlikehold og drift for å sikre tilgjengelighet, konfidensialitet og integritet i løsningene.

2.2.5 Beskyttelse av kundedata

I stadig større grad får kunder tilgang til bankens støttesystemer. I denne sammenheng har bankene økt fokus på å beskytte og kontrollere data innenfor bankens domene. IPsec er et hjelpemiddel for å oppnå dette. IPsec er en protokoll som blant annet benyttes for å beskytte innsyn i maskin til maskin-kommunikasjon ved hjelp av kryptering. Enkelte banker har planer om å innføre adgangskontroll for maskiner i nettverket ved hjelp av IEEE 802.1X-protokollen.

2.3 Internettkriminalitet

Internettkriminalitet økte på flere områder i 2009. I løpet av de siste årene har antall sårbarheter i applikasjoner vært langt høyere enn for operativsystemer. Angrepene som søker å utnytte disse sårbarhetene, følger to spor – passordknekking og angrep på web-applikasjoner. SQL Injection, Cross-site Scripting og PHP File Include-angrep er fortsatt de tre mest vanlige når det gjelder å kompromittere web-steder og applikasjonene der. Automatiske programmer gjør at det er relativt enkelt å identifisere og utnytte sårbarheter i web-applikasjoner i stor skala.

Høsten 2009 publiserte den amerikanske organisasjonen Center for Strategic and International Studies (CSIS) en oppdatert versjon av Twenty Critical Controls for Effective Cyber Defense.[3] Her gir cyber-kriminelle og sikkerhetseksperter samlet uttrykk for viktige kontrolltiltak.

2.3.1 Klientprogrammer som ikke er sikkerhetsoppdatert

Såkalte ”drive by downloads” er en ondsinnet kode som lastes ned via nettsteder som brukeren besøker. Et eksempel på dette er reklame som ligger på nettsider og som inneholder ondsinnet kode.

Koden infiserer brukerens PC og utnytter svakheter i programmene som kjører der for å tilegne seg økte privilegier. Enkelte er slik at brukeren ikke engang behøver åpne dokumentet som er lastet ned. Brukerens infiserte PC-er benyttes til å spre infeksjon og kompromittere andre interne datamaskiner og sensitive servere som man tror er beskyttet mot uautorisert adgang utenfra. Angriperens mål er å stjele data. Angriperen installerer i den sammenheng bakdører som angriperen kan benytte for å komme inn i PC-en ved senere anledninger.

Angripere fortsetter å utnytte sårbarhetene ved å lure brukeren til å åpne dokumenter sendt via e-post eller ved å infisere web-sider med lenker til dokumenter som utnytter sårbarhetene. Ved å utnytte sårbarheter i nettstedets web-innholdssystem (Web Content Management System) kan angripere automatisere infiseringen og ramme svært mange i løpet av få timer. Angrep som utnytter sårbarheter i Adobe, økte i 2009 etter som det ble klart for angriperne hvor enkelt det er å utnytte sårbarhetene for å få kontroll over en maskin.

Java scorer ganske høyt på listen over sårbarheter. Java er mye benyttet i web-sider som applets eller som applikasjoner, og Java er tradisjonelt sett sent ute med sikkerhetsoppdateringer. Inntil nylig ble heller ikke gammel, sårbar kode fjernet, med den følge at ondsinnet programvare kunne benytte denne, selv etter at oppdatering var foretatt.

For en mer omfattende liste over aktuelle sårbarheter i mye benyttet programvare, viser vi til Qualys' liste over de 30 mest aktuelle sårbarheter, se http://www.sans.org/top-cyber-security-risks/.

[3] http://csis.org/files/publication/Twenty_Critical_Controls_for_Effective_Cyber_Defense_CAG.pdf

2.3.2 Nettsteder som er sårbare

Angrep mot web-applikasjoner utgjør mer enn 60 prosent av det totale antall angrep. Sårbarhetene utnyttes til å gjøre nettsteder som brukeren oppfatter som sikre, om til ondsinnede nettsteder. Web-sider fra disse nettstedene vil da inneholde en kode som utnytter sårbarheter i programmer som kjører på brukerens PC. Sårbarheter i web-applikasjoner som SQL-injection og Cross-site Scripting i åpen kildekode så vel som spesialutviklede applikasjoner, utgjør mer enn 80 prosent av sårbarhetene som avdekkes. Til tross for et stort antall angrep og mye pressedekning er det på langt nær alle nettsteder som skanner for vanlige svakheter. Dermed kan de lett bli redskaper i hendene på kriminelle, og skader indirekte nettstedet og kunder som i utgangspunktet har tiltro til nettstedet.

Media har rettet oppmerksomhet mot kredittkort og fødselsnummerlekkasjer, men også andre typer data lagres og kan lekke. Betydningen av å beskytte web-applikasjoner mot SQL-angrep er meget viktig.

Cross-site Scripting er en tilbakevendende feil i web-applikasjoner. Sidene til et nettsted som brukeren har definert som trygge, viser seg å inneholde ondsinnet Java Script fra eksterne nettsteder som det tiltrodde nettstedet samarbeider med. Sidene har funksjoner for å reflektere kode fra slike eksterne nettsteder, eller de har lenker som henter sider som i sin tur inneholder ondsinnet kode. Nettstedene bør i større grad ta et totalansvar for all kode som, direkte eller indirekte, kjører i brukerens nettleser som følge av at brukeren henter en side via et nettsted.

2.3.3 Sesjonssikring

Tilgang til nettbank forutsetter at brukeren identifiserer seg og blir autentisert før en handel/transaksjon kan finne sted. En av de store utfordringene når det gjelder kommunikasjon over Internett er å opprettholde forbindelsen mellom brukerstedet og den autentiserte brukeren under *hele sesjonen*, slik at transaksjoner som brukeren gjør i løpet av sesjonen, entydig kan knyttes til vedkommende. Det finnes avanserte trojanere som er i stand til å endre på opplysninger som brukeren registrerer på sin PC, og samtidig endre ”kvitteringer” som kommer fra banken på en slik måte at de falske transaksjonene ikke blir synlige.

Brukerstedet har ansvar for å programmere tjenesten slik at sesjonssikring blir ivaretatt. Flere teknikker benyttes i denne forbindelse. Mange banker krever reautentisering ved hver transaksjon. Flere banker benytter sekvensnumre, og dersom det kommer trafikk utenom en sekvens, reageres det.

2.4 Metoder for tyveri av personinformasjon

Identitetstyveri øker både nasjonalt og internasjonalt. Organiserte kriminelle står bak mange av tyveriene. Fra flere hold er det tatt fatt i problemstillingen. Finanstilsynet samarbeider med andre organisasjoner både i Norge og utlandet for å kartlegge hvordan den operasjonelle risikoen påvirkes av identitetstyveri.

2.4.1 Hvor finnes personinformasjon

Identitetstyveri er å stjele, kopiere eller på annen måte tilegne seg personinformasjon for senere utnyttelse. På Internett kan man ved hjelp av noen typer personinformasjon, skaffe seg mer betalingsrelevante opplysninger, som fødselsnummer. Tilgang til finansinstitusjonenes kundeinformasjon kan skje via sårbarheter knyttet til:

1. Informasjon som deles mellom kunde og bank, f.eks. PIN-kode eller fingeravtrykk.
2. Avlesningsutstyr som PIN-tastatur og betalingsterminaler
3. Protokoller for overføring av konfidensiell informasjon
4. Nettverk inn mot brukersteder og finansinstitusjoner
5. Servere og datamaskiner hos brukersteder og finansinstitusjoner
6. Rutiner knyttet til implementering, drifting og bruk av systemer og applikasjoner.
7. Måter å tilegne til seg sensitiv informasjon på, ved å manipulere folk til å gi deg den frivillig
8. Utro tjenere internt i foretakene

Bedragere som ikke har kompetanse til å utnytte en persons eller et firmas nettbank, har andre muligheter, for eksempel via tilgang til servere hos nettsteder der det lagres informasjon om kunder. Slike nettsteder, som hotellkjedenes nettsteder, har avtaler med kredittkortselskaper om at de kan legge inn reservasjon på kundenes kontoer etter at det er bestilt hotellovernatting. Finanstilsynet har sett eksempler på foretak som beholder betalingsinformasjon også etter at kjøpet er gjennomført. Det er ofte begrenset kontroll med sikkerheten i nettsteders servere, selv om disse skal være omfattet av relevante PCI-standarder. Bedragere har derfor ofte god tid til å utforske slike servere der de kan tilegne seg nødvendig informasjon for å gjennomføre handel på steder hvor kortnummer, utløpsdato og CVC-kode er tilstrekkelig informasjon for betaling.

Identifikatorer nært knyttet til betaler, som fødselsnummer eller fingeravtrykk, styrker sannsynligheten for at det er riktig person som initierer en betaling. Samtidig skaper det større problemer for offeret hvis disse identifikatorene misbrukes enn hvis en PIN-kode kommer på avveie.

Identitetstyveri var i 2009 særlig knyttet til ulike typer *skimming* (utstyr for å lese magnetstriper). I tillegg utgjør informasjonstapping fra nettverk og bankdatasentraler en reell risiko.

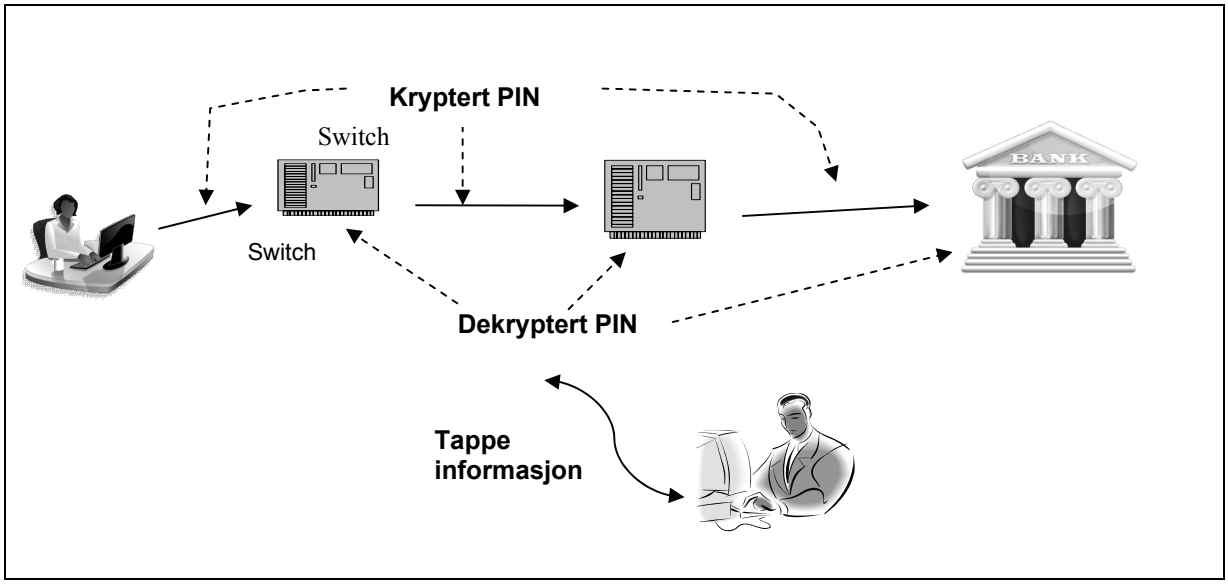
2.4.2 Angrep mot bankdatasentraler

Tidligere ble det ansett som meget vanskelig å stjele krypterte PIN-koder fra en *hardware security module* (HSM) og dekryptere kodene.[4] Nå kan slike angrep gjennomføres i praksis.

En HSM er en fysisk enhet som ofte er kjernen i en virksomhets sikre infrastruktur. Den lagrer og prosesserer blant annet krypteringsnøkler med tilhørende sertifikater, PKI og passord. HSM-er er utviklet for å kunne brukes av mange slags kunder i mange land. Det gjør at de er laget med flere funksjoner som ikke alle trenger. En dårlig implementering av en HSM kan utnyttes av en inntrenger til å komme forbi sikkerhetssperrene.

HSM-er konfigureres og administreres forskjellig, ofte av leverandører som ikke er direkte relatert til en bank. I henhold til PCI-standarden skal PIN-koder være kryptert under overføring. Men en PIN må passere mange HSM-er over flere typer nettverk. Ved hver *switch* må PIN-koden dekrypteres og rekrypteres med riktig nøkkel for neste steg til bestemmelsesstedet. Ved manipulering og utnyttelse av svakheter i standardiserte programmer for brukergrensesnitt, Financial PIN Processing API, og svak implementering kan bedragere lure HSM-en til å finne masternøkler for systemet. Når sentrale komponenter er kompromittert, blir det trivielt å dekryptere PIN eller passord.

Figur 1: Kryptert og dekryptert PIN



[4] The unbearable lightness of PIN Cracking,
http://www.arx.com/files/Documents/The_Unbearable_Lightness_of_PIN_Cracking.pdf

Svakheter ved konfigurering av HSM-er er relevant også i Norge, og særlig der dette utføres av leverandører som drifter for mange foretak med ulike behov.

3 Finanstilsynets funn og observasjoner

3.1 Viktige funn fra IT-tilsyn

I 2009 ble det gjennomført 22 stedlige tilsyn og 21 dokumentbaserte IT-tilsyn. Det ble også rapportert om 165 IKT-hendelser, og det ble holdt egne oppfølgingsmøter om disse. Videre ble det gjennomført 16 intervjuer med aktører i finanssektoren. I tillegg har Finanstilsynet fortsatt arbeidet med å kartlegge IKT-infrastrukturen i finanssektoren. Utkontraktering til land utenfor Norge ble viet ekstra oppmerksomhet i 2009.

3.1.1 Finansforetakenes ROS-analyser

Finanstilsynet har påpekt mangler i foretakenes egne risikoanalyser av IKT-virksomheten. Risikoanalysene er ofte ikke dekkende for hele foretakets IKT-virksomhet. Dette skyldes ofte mangler i foretakenes tilnærmingsmåte i det å sikre at ROS-analysene er komplette. Analysen skal omfatte applikasjonsutvikling, drift, sikkerhet, organisasjon og rutiner, og i tillegg ha deltakere med kompetanse på disse områdene. Videre bør risikoanalyser omfatte vurdering av leverandører med avtaler og leveranser og leverandørenes egne ROS-analyser. Noen ROS-analyser mangler adekvat oppfølging. Det er viktig at ROS-analysen er et levende dokument der identifiserte risikoer regelmessig blir fulgt opp.

3.1.2 Utkontraktering

Som nevnt ovenfor, har mange foretak utkontraktert driften til en IKT-leverandør i Norge eller et annet land i Norden. Trenden er at IKT-leverandørene utkontrakterer visse tjenester videre til leverandører i lavkostland lenger unna, såkalt *offshoring*. Foretakene er i varierende grad og på ulike måter informert om slik utkontraktering til tredjepartsleverandører. Planer kan presenteres som bedriftsinterne endringer og i visse fall ikke vise de faktiske forhold, nemlig at data prosesseres i andre land med annet lovverk, noe som kan påvirke den norske operasjonen. Finansforetakene i Norge er ansvarlige for egen virksomhet, men blir ofte en passiv mottaker av informasjon fra driftsleverandøren når det gjelder planer om utkontraktering til tredjeparts leverandør. Det er finansforetaket som er ansvarlig når tjenestene er utkontraktert, jf. IKT-forskriften. Slike forhold krever oppmerksomhet fra foretakene, og

det er naturlig at forholdene blir reflektert i foretakenes egne ROS-analyser. Finanstilsynet har viet det samme forholdet oppmerksomhet i tilsyn med IKT-leverandørene.

3.1.3 Testing av katastrofeløsninger

Testing av katastrofeløsninger er et område der foretakets egne løsninger ikke kan vurderes isolert fra IKT-leverandørenes løsninger. Foretaket må sikre en samlet beredskap med reserveløsninger både for operasjoner som håndteres i eget hus og operasjoner basert på leveranser fra IKT-leverandørene. Katastrofeløsningene vil derfor kreve tester mange ulike steder i kjeden. Også i mindre foretak er det viktig å teste katastrofeplanen for å avdekke feil i opplegget og gi anledning til å utbedre feilene før en reell katastrofe inntrer.

3.1.4 Konfigurasjonsoversikt

I de store foretakene er det gjennom IT-tilsynene stilt spørsmål om foretakene har et tilfredsstillende opplegg for å sikre seg oppdatert oversikt over alle konfigurasjonselementer og deres innbyrdes sammenhenger. Ofte er slik informasjon samlet i det som kalles en Configuration Management Database (CMDB). En CMDB kan være arbeidskrevende å etablere, men gir stor gevinst når den først er etablert. Automatisert kobling mellom elementer som på en eller annen måte er avhengige av og kan påvirke hverandre, kan bidra til at endringshåndtering kan gjennomføres med færre feil. Imidlertid må slike oversikter oppdateres kontinuerlig for å ha sikker effekt. Fortsatt er mange hendelser forårsaket av uventede sideeffekter av endringer.

3.1.5 Styring og kontroll med IKT-virksomheten

Finanstilsynets merknader fra IT-tilsyn gjennomført i 2009 knytter seg til foretakenes styring og kontroll med IKT-virksomheten. Et foretaks IKT-strategi skal understøtte foretakets forretningsstrategi, samtidig som IKT-strategien operasjonaliseres gjennom IKT-prosessene og definerte tiltak. Ofte synes strategien å være løsrevet fra hvordan IKT-arbeidet faktisk blir utført. Det hjelper ikke å ha en lang liste med krav til sikkerhet når grunnleggende sikkerhetsarkitektur ikke er implementert i organisasjonen.

Finansforetakenes forretningsmessige drift hviler på utstrakt bruk av IKT-systemer både administrativt og i gjennomføringen av alle typer finansielle transaksjoner. Dette medfører mange faste kostnader hvor kostnadsreduksjoner i stor grad må skje ved å redusere transaksjonskostnader pr. enhet, noe som øker interessen for å delta i større driftsenheter. I denne utviklingen oppstår det økt organisatorisk og teknisk kompleksitet som kan føre til at nye risikoområder må utvikles.

Gjennom blant annet stedlige tilsyn har disse problemstillingene kommet frem ved at det er blitt avdekket noe manglende kompetanse og vektlegging på sentrale områder innenfor styring og kontroll innenfor IKT-virksomheten. Samtidig er det avdekket organisatoriske risikoområder i hvordan

forholdet mellom forretningsstrategi og IKT-strategi skal implementeres og fungere best mulig operasjonelt.

Slike risikoområder kan ha årsak i følgende:

- Finansforetakenes forretningsområder og IKT-områder har ulike drivere. Førstnevnte er inntekts- og kundeorientert, mens sistnevnte er produksjons- og kostnadsorientert. For å kunne dekke risikoområder, kan det være nødvendig å allokere ressurser for investeringer som ikke nødvendigvis vil vise seg inntektsmessig verken på kort eller lang sikt. Denne formen for egenforsikring for å unngå fremtidige driftsproblemer, vil ikke være synlig fordi alternative kostnader ikke vil oppstå i fremtiden. Følgelig er det nødvendig å ha en utviklet og synlig kompetanse innenfor operasjonell risiko på alle nivåer i foretakenes organisasjon.

- Finansforetak som har inngått strategiske samarbeidsavtaler med driftsenheter, som igjen har utkontraktert drift og administrasjon til spesialiserte IKT-foretak, har en potensiell operasjonell risiko. Ansvaret for å opprettholde nødvendig bestillerkompetanse ligger alltid hos det foretaket som har konsesjon. Likevel blir det avdekket at kritisk kompetanse ikke blir opprettholdt siden denne antas å bli dekket opp av den samarbeidende driftsenhet og på grunn av målsettingen om å redusere egne kostnader.

- For finansnæringen i Norge er det en klar konsentrasjonsrisiko knyttet til at næringen har få datasentraler å velge mellom når alternativer for IKT-relaterte spørsmål skal vurderes. Dette kan i seg selv bidra til valg av leverandører som benytter seg av utenlandske ressurser offshore i IKT-driftsleveranser. I tillegg er de ulike foretakene i stor grad bundet til etablerte eldre kjernesystemer med historie fra tidligere samarbeidsstrukturer, og som nå eies av datasentralene. Dette kan påvirke foretakenes muligheter for å skifte leverandør av denne type tjenester.

- I forbindelse med den dominerende bruken av betalingskort og betalingsterminalene vi har i Norge, samt økende trusler for kriminelle angrep på disse, er det formålstjenlig med et sentralt register for betalingsterminaler. Banknæringen etablerte i 2009 et slikt register som inneholder mest mulig informasjon slik at en skal kunne hindre fremtidige kriminelle angrep på dette området. Dersom det vil forekomme angrep på slike terminaler, vil det være vesentlig lettere å velge tiltak gjennom bruk av et slikt sentralt register.

3.2 Foretakenes egne vurderinger

I 2009 gjennomførte Finanstilsynet intervjuer med 16 foretak. Hensikten var å få foretakets vurdering av egen sikkerhetssituasjon.

Nedenfor følger spørsmålene som ble gjennomgått og et sammendrag av svarene.

1. Hva ser foretaket på som den/de største risiko/ene ved foretakets bruk av IKT?
Selv om innfallsvinkelen er litt forskjellig i de ulike foretakene, nevner mange at mangel på kompetanse er en av de største risikoene forbundet med bruk av IKT. Når flere tjenester og produkter blir automatisert som en følge av nye teknologiske muligheter, øker også kompetansekravet på stadig nye områder. Dette gjelder områder som systemutvikling, både i egen og i leverandørenes organisasjoner, bestillerkompetanse og kompetanse innen IKT-drift. Automatiseringen av produkter og prosesser gjør at den detaljerte forretningsforståelsen forvitrer. Man stoler helt og fullt på IKT-systemene.

2. Hva har vært de største problemer på IKT-området i 2009? Hva er grunnlaget for å kunne identifisere disse?
Mange foretak opplevde at kunder var blitt utsatt for en eller annen form for ID-tyveri i 2009. Det vanligste var tyveri av kortdata. Et stort tyveri av kortdata fra innsamling i Spania i 2009 medførte at mange kort ble kompromittert, deriblant også kort tilhørende norske kunder. Mange norske banker sendte i 2009 nye kort til et betydelig antall kunder som et risikoreduserende tiltak. Foretakene nevner i den forbindelse at det er et problem å få informasjon fra de internasjonale kortselskapene. Videre har kort med magnetstripe og PIN blitt *skimmet* i betalingsterminaler i norske dagligvarebutikker. Denne måten å kompromittere betalingsterminalene på er ny.

Det var flere leveranser til IKT-prosjekter i finansforetakene som ikke hadde tilfredsstillende kvalitet. Ofte er det slik at den samme IKT-leverandøren brukes både til drift, applikasjonsutvikling og som bidragsyter til interne IKT-prosjekter. Til utviklingsprosjekter er leveransene ofte ikke presise på tid og ikke av tilstrekkelig kvalitet. Det er ikke bare leverandørene som er årsak til at prosjekter ikke leveres som avtalt. Det er også tilfeller hvor manglende bestillerkompetanse blir nevnt som en årsak.

3. Hva ser foretaket på som de største utfordringene i 2010 med hensyn til risiko ved bruk av IKT?
Foretakene prioriterer sikker og stabil drift først, samt beskyttelse av data og personinformasjon mot uautorisert tilgang. Det er viktig å sikre høy tilgjengelighet til tjenestene. Ved at det legges til flere tjenester i portalløsningene, for eksempel i nettbankportalen, øker kompleksiteten. Dermed øker også utfordringen med å sikre stabil drift av løsningene som forventes å være tilgjengelige 24 timer i døgnet 7 dager i uka.

Gjennomføring av sikkerhetstester og stadig forbedring av foretakenes sikkerhetsløsninger er viktig for å sikre egen infrastruktur mot inntrenging. Tilstrekkelig testing før produksjonssetting av nye og

endrede løsninger er en utfordring. Kvaliteten på testsystemer og testdata er helt avgjørende for at testene kan avdekke feil i løsninger før de blir satt i produksjon.

Regulatoriske krav er også en utfordring for finansforetakenes IKT-virksomhet. Som eksempel på dette er ny hvitvaskingslov, betalingsdirektivet som kan medføre flere lovendringer, implementering av Solvens II for forsikringsbransjen og den nye pensjonsreformen vil alle medføre endringer i foretakenes IKT-løsninger.

Konkurs eller andre vanskeligheter hos forretningskritiske IKT-leverandører er en aktuell trussel.

Motiverte medarbeidere er viktig. Både å ivareta nøkkelkompetanse og å følge opp egne medarbeideres utvikling vil vektlegges, samt tiltak for å øke strategiforståelsen hos medarbeiderne.

4. Hva ser foretaket på som viktige problemstillinger som må adresseres (gjennomføre tiltak) i 2010 med hensyn til IKT-sikkerhet?

Øke forståelsen og bevisstheten rundt IKT-sikkerhet hos medarbeiderne er et prioritert område. I forlengelsen av dette er det spesielt nevnt at tilgangskontroll til systemer og data på alle nivåer må gjennomgås slik at sikkerhetsmessige forhold blir kartlagt og tilrettelagt i forhold til dette.

Beskyttelse av kortdata er et område som blir nevnt av flere foretak. Foretakenes arbeid med PCI-standarden vil fortsette i 2010. Formålet med å legge inn PCI-standarden i egne løsninger øker sikkerheten ved bruk av kort, men er ingen garanti for at kortdata ikke kan komme på avveie. Banksektoren i Norge har gjennom Bankenes Standardiseringskontor (BSK) definert egne krav til sikkerhet ved bruk av kort, og disse kravene kan i enkelte tilfeller være strengere enn PCI-kravene. BSK har satt i gang arbeid med å sikre at sikkerhetskravene er tilstrekkelige og i samsvar med relevante standarder utarbeidet av PCI Security Standard Council.

Oppgradering av katastrofeløsninger står på planen for en del virksomheter. Noen foretak har manglet alternative løsninger med geografisk avstand, og de vil etablere dette i 2010.

På verdipapirområdet er det store IKT-prosjekter for utvikling av nytt handelssystem og oppgjørssystem. Dette påvirker alle medlemmene på Oslo Børs som må tilpasse sine løsninger til det nye handelssystemet. Å håndtere leveranser fra prosjektene parallelt med daglig drift nevnes av foretakene som spesielt krevende. For noen foretak med større IKT-prosjekter er det en ny erfaring å bruke mange innleide ressurser, og det er en utfordring å håndtere de eksterne konsulentene på riktig måte. Innen verdipapirområdet nevnes risiko knyttet til den dominansen én leverandør av IKT-løsninger utgjør for de norske verdipapirforetakene. Dette kan gi foretakene en ufordelaktig situasjon både når det gjelder pris, kvalitet og tidsmessig gjennomføring av leveransene.

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

Stikkord for hva foretakene ellers nevner som områder de vektlegger er standardisering, kvalitet på risikovurderinger og intern kontroll. Det blir lagt vekt på å implementere operasjonell risikostyring i flere prosesser for å sikre et objektivt og bevisst forhold til risiko, samt vekt på helhetlig risiko i prosesser og ikke bare IKT-risiko isolert sett.

Flere foretak har gjennomført oppkjøp og fusjoner for å hente ut synergieffekter. Foretakene opplever det slik at synergien som kan hentes ut på IKT-området, er vanskelig å realisere. Ofte tar det lang tid før det blir satt inn ressurser for å integrere løsningene til de fusjonerte partene. I mellomtiden lever parallelle systemer side om side, noe som innebærer dobbel drift, forvaltning og utvikling og spredt kompetanse.

3.3 Analyse av rapporterte hendelser

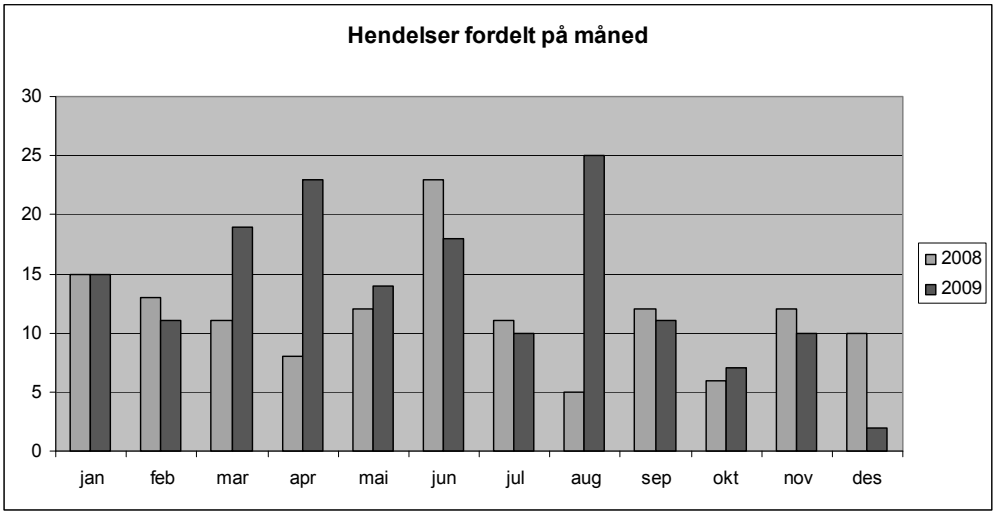
3.3.1 Rapportering av hendelser til Finanstilsynet

Hendelsesrapporteringen til Finanstilsynet ble fra 1. desember 2009 forskriftsregulert gjennom en utvidelse av IKT-forskriften. Samtidig ble virkeområdet utvidet til å omfatte alle finansforetak som er underlagt IKT-forskriften med unntak av eiendomsmeglingsforetak, inkassoforetak og pensjonskasser.

Siden filialer av utenlandske banker og forsikringsselskaper ikke er underlagt norske forskrifter, har tilsynet forespurt filialene om de på frivillig basis vil slutte seg til rapporteringen. Noen av filialene har valgt å følge det samme opplegget for hendelsesrapportering som de norske foretakene. Underrapportering av hendelser kan bli spesielt merkbar på områder der utenlandske filialer utgjør store deler av det norske markedet.

I bruk av betalingsterminaler er det avdekket svindelforsøk med stjålet kort og PIN-kode, og det har vært mulig å få ut store kontantbeløp i forbindelse med varekjøp. Det ser ikke ut til å være lagt inn sperrer på slike kontantuttak slik det er i minibanker. Finanstilsynet vil vurdere dette risikoområdet i 2010.

Figur 2: Hendelsesrapportering – måned



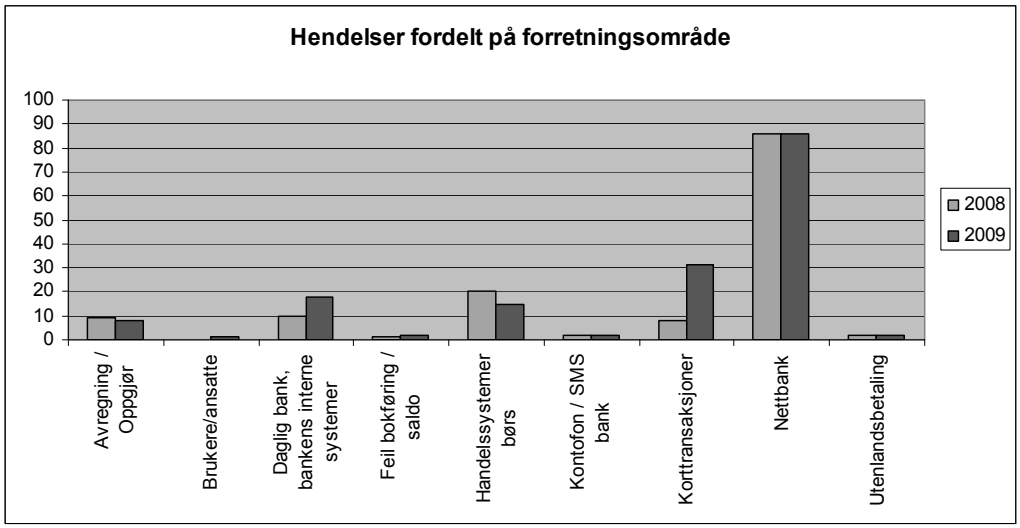
Kilde: Finanstilsynet

I 2009 ble det rapportert om flere hendelser knyttet til korttransaksjoner. For andre områder var antall hendelser omtrent det samme som i 2008.

Finanstilsynet strukturerte i 2009 oppfølgingen av rapporterte hendelser. Hvert kvartal blir det lagt ut en oppdatert oversikt over rapporterte hendelser fordelt på forretningsområde på tilsynets nettsted, se http://www.finanstilsynet.no/no/Bank-og-finans/Banker/Tema/IT-tilsyn/.

3.3.2 Hendelser i 2009

Figur 3: Hendelsesrapportering – forretningsområde



Kilde: Finanstilsynet

Hendelsene som fikk mest oppmerksomhet i 2009, var knyttet til skimming av butikkterminaler. Skimming-angrepene, som hadde størst omfang på sensommeren, medførte at det ble innført en rekke risikoreduserende tiltak, blant annet intensiverte utskiftingen av kort med magnetstripe til kort med chip og terminaler som kan lese chip.

For øvrig var det som i de foregående årene driftshendelsene som dominerte i 2009. Også på dette området var det hendelser knyttet til korttransaksjoner. Hendelser som fører til at kort blir avvist i varehandel, får raskt store konsekvenser. Lørdag 24. oktober 2009 var systemet for bruk av norske betalingskort med BankAxept ute av drift i 13 minutter. Dette rammet alle brukersteder og alle kort med BankAxept, og det skjedde på formiddagen i beste handletid. Bankenes BetalingsSentral (BBS) fikk et skred av henvendelser ved dette korte avbruddet.

Manglende dekningskontroll er ofte årsak til problemer ved bruk av kort i betalingsterminalene og i minibankene. Oftest er slike hendelser begrenset til visse typer kort, visse typer minibanker eller visse typer brukersteder. Årsaken kan være nettverksproblemer eller ulike problemer knyttet til driften.

Antall hendelser knyttet til nettbank var omtrent det samme i 2009 som i 2008. Total nedetid for nettbank ser ut til å ha vært noe lavere i 2009 enn i 2008. Årsaksbildet er det samme som tidligere. Utilstrekkelig kapasitetsplanlegging enten det gjelder fulle disker eller andre grenseverdier som blir overskredet uten forutgående varsling, og komplikasjoner knyttet til en kompleks driftskonfigurasjon. I 2009 var det også programmeringsfeil knyttet til sesjonshåndtering som resulterte i at en kunde kan se

en annen kundes data. Når slike feil blir oppdaget, blir tjenesten stengt inntil feilen er identifisert og rettet.

3.4 Vurdering av andre aktuelle områder

3.4.1 IKT-infrastruktur

IKT-infrastruktur innebærer at blant annet finansielle tjenester i stadig større grad er automatisert, og de er i realtid i et elektronisk samspill ende til ende mellom samhandlende parter.

Brukere tilpasser seg den økte tilgjengeligheten til finansielle tjenester som IKT-infrastrukturen gir. En *day trader* i aksjer kjøper aksjer i tillit til at det elektroniske aksjehandelssystemet gir mulighet til å komme ut av posisjonen på rett tidspunkt. Dersom systemet er nede, kan det innebære et økonomisk tap. Samfunnet er avhengig av at IKT-infrastrukturen er velfungerende og tilgjengelig.

I og med at de automatiserte, elektroniske finansielle transaksjonskjedene blir lengre, øker kompleksiteten, og dermed øker risikoen for feil i et av leddene. Feil i ett ledd kan medføre at transaksjonen ikke kan gjennomføres og at den blir avvist. Kunden oppnår å ikke få levert fra seg betalingsoppdraget i tide, og er helt og holdent overlatt leverandøren av finansielle tjenester og dennes evne til å reetablere tjenesten.

Finanstilsynet har erfaring med at det er høyere risiko for feil i koblingen mellom aktørene i transaksjonskjeden enn hos den enkelte aktør. Dette har naturlig sammenheng med økt iboende risiko forbundet med det å skifte "sone" fra en aktør til den neste. I dette byttet skjer dekryptering/rekryptering, omformatering, protokollkonvertering, adresseoversettelse, versjonskontroller, sekvenskontroller osv. Slike koblingsoppgaver har vist seg å gi opphav til feil.

Det er derfor nyttig å analysere hele transaksjonskjeden under ett for viktige finansielle tjenester og da med oppmerksomhet rettet spesielt mot koblingene. Den finansielle tjenesten blir behandlet i ulike systemer i transaksjonskjeden. Systemene leveres ofte av ulike aktører innenfor den IKT-infrastrukturen. Arbeidet innebærer kartlegging av hele kjeden og alle finansinstitusjoner og andre infrastrukturleverandører og deres systemer som er en forutsetning for at tjenesten skal fungere.

På denne bakgrunnen forsøkte Finanstilsynet i 2009 å kartlegge den tekniske infrastrukturen som bærer viktige finansielle transaksjoner. Kort oppsummert er målet å kartlegge og vurdere følgende for hvert system:

- Hvor får systemet data fra og på hvilken måte blir dataene oversendt?
- Hva gjør systemet med dataene?
- Hvem avgir systemet data til og på hvilken måte skjer dette?
- Hvilke sikringstiltak er implementert?

Aktørene omfatter BBS, EDB Business Partner ASA, bankene, Verdipapirsentralen (VPS), Oslo Børs, Oslo Clearing, verdipapirforetak, tilbydere av nett for kredittkorttransaksjoner (VISA, MasterCard etc.), innløsere for kredittkorttransaksjoner (Teller, Nordea), Telenor og andre linjeleverandører, ISP-er.

Hovedkonklusjonene fra kartleggingen:

- På flere områder er bankvirksomhet avhengig av en eller noen få store leverandører av tjenester. Dette gjelder for eksempel innenfor IKT-drift, systemforvaltning, aksjehandelssystem, fondssystemer, systemer for validering av engangskoder, systemer for reservasjonsforespørsler på kort/konto. Er tjenesten nede, blir mange av kundene i Norge rammet.

- De lange transaksjonskjedene gjør at det er komplisert å teste ende til ende. Det viser seg vanskelig å vedlikeholde et produksjonslikt testmiljø. Dette gir opphav til feil i produksjon.

- Det viser seg å være en utfordring å få reserveløsninger, i særdeleshet reservelinjer, til å fungere etter forutsetningen.

- Driftsmiljøene er blitt svært kompliserte og vanskelige å kontrollere, noe som gir feil og nedetid. Bedre overvåking av prosesser og systemer er påkrevet.

- Nettbankene har vært programmert slik at alle tjenester i nettbanken deler sentrale ressurser. Dette fører til at heng i en av tjenestene går ut over tilgangen til andre tjenester.

3.4.2 Utkontraktering og offshoring

IKT-drift er i sin natur fabrikkproduksjon. Automatisering og integrert driftsovervåking sørger for det. Global konkurranse gjør at finansinstitusjoner ønsker å ekspandere og operere i flere land for å få større volumer og for å få tilgang til nye og flere markeder. De største finansinstitusjonene etablerer sentraliserte IKT-løsninger for sine globale operasjoner, og argumenterer med at sentralisert IKT-drift er en forutsetning for å drive rasjonelt.

I dag finnes ulike krav til finansforetak når det gjelder utkontraktering. For VPS og Oslo Børs er det sterke begrensninger, og det blir stilt krav om godkjenning fra Finanstilsynet, mens banker i Norge utkontrakterer tjenester uten at det foreligger tilsvarende krav. Sverige har innført krav til banker om å oversende utkontrakteringsavtalen til Finansinspektionen for gjennomgang når det foreligger planer og avtale om utkontraktering av IKT-tjenester.

For finansnæringen som for andre næringer er det å redusere kostnader innenfor IKT-virksomheten viktig for å kunne oppnå best mulig resultater. Dette er en utfordring for finansforetakenes egen IKT-virksomhet og ikke minst deres IKT-leverandører. Med kompleksiteten i foretakenes IKT-løsninger

innenfor både teknisk infrastruktur og applikasjoner kan det være vanskelig å sikre seg tilstrekkelig kompetanse på de ulike områdene. Dette gir drivkraft til en vedvarende prosess i utkontraktering og kostnadsreduksjoner. IKT representerer normalt mellom 15 og 25 prosent av en banks totale kostnader og utgjør derfor betydelige summer. Det er et sterkt press på IKT-leverandørene om å bidra med nødvendige kostnadsreduksjoner. En følge av dette vil naturlig være at leverandører vurderer offshoring som virkemiddel for å oppnå effektive kostnadsreduksjoner.

3.4.2.1 Prinsipper og regelverk

The Joint Forum ble etablert i 1996 av Basel Committee on Banking Supervision (BCBS), the International Organization of Securities Commissions (IOSCO) og the International Association of Insurance Supervisors (IAIS) for å ta seg av felles utfordringer innenfor bank-, verdipapir- og forsikringssektoren. The Joint Forum har utarbeidet ni prinsipper for utkontraktering. De første sju tar for seg det ansvarsområdet som foretaket under tilsyn har i forhold til utkontraktering og egen aktivitet. Disse prinsippene er innarbeidet i Finanstilsynets IKT-forskrift. De to siste tar for seg myndighetsrollen, og er innarbeidet i tilsynsmetodikken.

Den teknologiske utviklingen, utviklingen i finanssektoren og hendelser som har skjedd de siste årene reiser nye problemstillinger knyttet til risiko, lovtolkning og myndighetenes behov for virkemidler.

Aktuelt regelverk gir enkelte føringer når det gjelder enkeltforetak, men liten veiledning når det gjelder vurdering av risiko for hele finanssektoren samlet, og hvordan dette skal vurderes ut fra samfunnskritisk virksomhet.

I Norge ble det i forbindelse NOU 2006: 6 *Når sikkerheten er viktigst – Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner* gjort en vurdering av finanssektoren, og den ble definert som en samfunnskritisk virksomhet. Det er ikke kjent om det på grunnlag av NOU-en er laget ytterligere materiale eller regelverk annet enn utarbeidelsen av "Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007–2010". I kapittel 3.4 peker denne på behovet for å gjennomføre risiko- og sårbarhetsanalyser når en leverandør har leveranser til virksomheter som er definert som samfunnskritiske.

I forskningsprosjektet BAS5 (Beskyttelse av samfunnet) er det rettet oppmerksomhet mot risiko knyttet til samfunnskritisk virksomhet. Ansvarlige myndighetsinstanser for prosjektet var Forsvarets forskningsinstitutt (FFI), Direktoratet for samfunnssikkerhet og beredskap (DSB) og Nasjonal Sikkerhetsmyndighet (NSM), og Finanstilsynet var blant deltakerne. Det antas at flere leverandører og en rekke av de oppgavene som de ivaretar kan bli definert som samfunnskritisk virksomhet. Følgende risikoelementer har betydning ved vurdering av offshoring (jf. kap. 3.1.2 og 5.3):

- Finansforetakenes behov for egen styring og kontroll med egen IKT-virksomhet. Det må antas at denne vil bli svekket over tid om foretaket og/eller IKT-leverandøren ikke har tilstrekkelig nærhet til oppgavene som utføres.

- Behov for instruksjonsmuligheter og kontroll i katastrofesituasjoner, både av berørte foretak og myndigheter.

- Svekket nasjonal kontroll dersom store deler av IKT-virksomheten til finanssektoren, som er definert som samfunnskritisk, opereres fra utlandet.

- Manglende oversikt over lovverket i det landet som utfører IKT-oppgavene og som kan gi utilsiktede virkninger, særlig i en beredskapssituasjon.

- Håndtering av og sikker oppbevaring av personopplysninger der lokal lovgivning kan gi utilsiktede virkninger for etterlevelse av lovmessige krav. Særlig gjelder dette utenfor EØS-området.

- Forholdet til konsesjonsbelagt virksomhet og hva som kan defineres som kjernevirksomhet og som ikke uten videre kan utkontrakteres.

- Om regelverk for utkontraktering er tilstrekkelig sett i sammenheng for de ulike delene av finanssektoren.

- Svekket mulighet til å foreta tilsyn med foretakenes IKT-virksomhet.

3.5 Resultater fra gjennomførte spørreundersøkelser

I september 2009 foretok Finanstilsynet en spørreundersøkelse med spørsmål knyttet til utkontraktering av IKT og test av katastrofeløsning for IKT-virksomheten. Spørreundersøkelsen ble sendt til 144 banker (forretningsbanker, sparebanker og filialer av utenlandske banker i Norge). 126 foretak svarte på undersøkelsen.

Spørsmålene var differensiert på hvilke deler av IKT-virksomheten som var utkontraktert (support, drift, forvaltning, utvikling, annet) og om utkontrakteringen var til leverandører i Norge, i Norden eller i land utenfor Norden.

De fleste sparebankene i Norge tilhører en bankgruppering. Det er mer enn 80 sparebanker som tilhører Terra-Gruppen der IKT-virksomheten administreres av Terra-Gruppen sentralt og der driften er utkontraktert til Scandinavisk Data Center (SDC) i Danmark. Videre er det mellom 40 og 50 sparebanker som tilhører SpareBank 1 Gruppen der driften hovedsakelig er utkontraktert til EDB Business Partner ASA. EDB er også den mest sentrale driftsleverandøren til et større antall frittstående sparebanker. Svarene på spørsmålene om utkontraktering fra sparebanker i samme gruppe er i stor grad sammenfallende.

Det største spennet i svarene er fra filialer av utenlandske banker i Norge. Disse har ofte basert IKT-virksomheten på utkontraktering til morselskapets IKT-leverandør.

Majoriteten av banker er kjent med at leverandører som foretaket har avtale med, selv har utkontraktert deler av leveransen til tredjepartsleverandør. Utkontraktering til tredjepartsleverandør i land utenfor Norden blir besvart med "Ja" i noen banker og med "Nei" i andre banker basert på at sistnevnte ikke anser det som en tredjepartsleverandør når den norske leverandøren har eierskap i aktuelle selskap i disse landene.

Det er relativt beskjedne planer for å endre på det utkontrakteringsopplegget den enkelte bank har etablert. Det er få banker som planlegger å utkontraktere flere deler av IKT-virksomheten eller å bytte utkontrakteringsleverandør, og svært få som planlegger å ta IKT-virksomhet tilbake.

De fleste foretakene svarer bekreftende på at risikoanalyser blir utført og at det blir sendt melding til Finanstilsynet når det skjer endringer i utkontrakteringsforhold som påvirker betalingssystemer. Imidlertid var det en rekke kommentarer til disse spørsmålene. Typiske og gjennomgående kommentarer var at Terra-Gruppen og SpareBank 1 Gruppen gjennomfører risikoanalyser på vegne av banken i spørsmål om utkontraktering eller at leverandør gjør dette. Det samme gjaldt utkontraktering som kan utløse meldeplikten for nye eller endrede betalingssystemer.

Spørsmålene om test av katastrofeplanen var direkte rettet til den enkelte bank med spørsmål om banken hadde gjennomført test av katastrofeplanen og om banken vurderte at den oppfyller § 11 i IKT-forskriften. Som svar på spørsmålet om banken hadde gjennomført test av katastrofeplanen, svarte mange ja og med tilleggskommentar om at det var en skrivebordstest. Mange av bankene som svarte "Nei" på det samme spørsmålet, kommenterte at test vil bli utført senere i 2009, eventuelt i første kvartal av 2010.

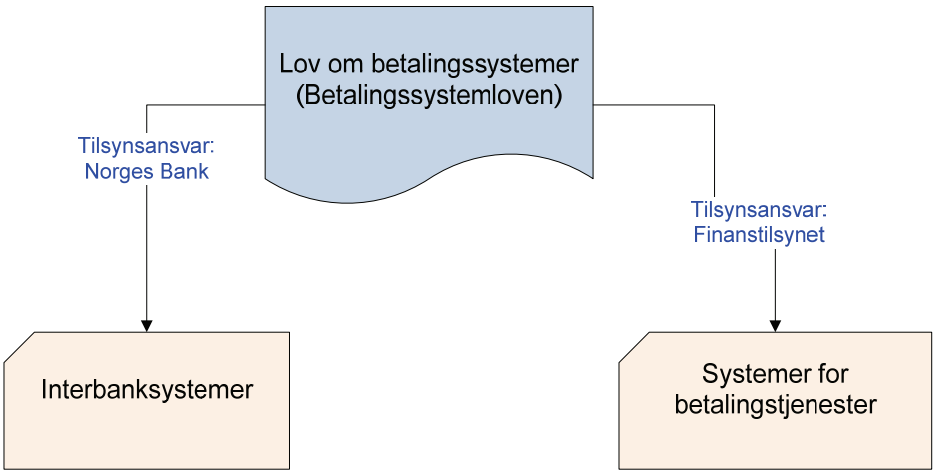
De mange ulike svarene viser at det er et stykke igjen før veldefinerte og velprøvde rutiner for test av katastrofeplanen er på plass i alle bankene. Videre at det er ulikt hvor bokstavelig bankene tolker kravene i IKT-forskriften. Noe av hensikten med spørreundersøkelsen var å sette søkelyset på operasjonalisering av test av katastrofeplanen. Katastrofeplanen er en kombinasjon av reserveløsninger i banken og hos driftsleverandørene. For å sikre at alle deler virker i en krisesituasjon enten denne oppstår i banken, hos leverandøren eller i kombinasjon begge steder, må den samlede katastrofeberedskapen dekke alle deler, og katastrofeplanen må reflektere dette.

4 Systemer for betalingstjenester

4.1 Generelt om betalingssystemer

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. 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.



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. Styring og kontroll av betalingssystemer inngår som et viktig element i vurderingen av operasjonell risiko basert på reglene i kapitaldekningsregelverket (Basel II) og som er innarbeidet i norsk finanslovgivning. Av konkurransehensyn blir alle betalingssystemer og alle lovlige tilbydere av betalingstjenester pålagt å sikre tilgang til hverandres betalingssystemer på visse vilkår.

4.2 Risiko og sårbarhet

Finanssektoren og løsningene som tilbys er i økende grad utsatt for angrep fra ulike kriminelle grupperinger. Dette er ingen ny situasjon, men det er bekymringsfullt at det ser ut til å være en gradvis økning i angrep fra internasjonal organisert kriminalitet. Denne formen for kriminalitet blir i stor grad utført via Internett, og det er en utfordring for det enkelte land å stoppe denne typen utvikling. Mottiltak vil derfor kreve flere tiltak som blant annet risikoanalyser og internasjonalt samarbeid for å identifisere sårbarheter og for å iverksette risikoreduserende tiltak.

Om vi ser på utviklingen i Norge kan vi konstatere at det er intensiv bruk av elektroniske løsninger i betalingsformidlingen som dekker behovet for betalingsløsninger nærmest fullt ut. Volumutvikling og innovasjon viser at Norge ligger i øverste sjikt på dette området i internasjonal sammenheng. Volumtall målt mot befolkningsstørrelse som beskrevet i Norges Banks *Årsrapport om betalingssystem 2008*, viser dette.

Erfaringen hittil har vist at det er de digitale kanalene i det ytterste leddet ut mot den enkelte bruker, eller enkeltledd i håndteringen av betalingstransaksjoner, som er mest utsatt.

Basert på den erfaringen Finanstilsynet har, er det følgende bruk som har blitt utsatt for angrep:

- **Bruk av betalingskort i minibanker**
  I Norge har det vært et problem at det har blitt montert utstyr på bankenes minibanker som kunne kopiere innholdet i magnetstripen uten at kortinnehaver oppdaget dette. Bankene har iverksatt effektive tiltak slik at restproblemet i dag er filming av inntasting av PIN-kode kombinert med tyveri av kortet og påfølgende misbruk.

- **Bruk av betalingskort i bensinstasjonsautomater**
  En konsekvens av risikoreduksjon på minibanker har vært at noe av kriminaliteten har flyttet seg over til bensinautomater med bruk av lignende type utstyr for ulovlig kopiering av innholdet i magnetstripen på betalingskortet. Foreløpig ser dette ut til å være en håndterbar situasjon, og ulike tiltak er og vil bli iverksatt.

- **Bruk av betalingskort i butikkterminaler**
  Det er betalingsterminalene, der kortinnehaver taster inn PIN-koden, som har vært utsatt for modifisering og ulovlig kopiering av innholdet i kortinnehavers magnetstripe. Dette var en helt ny trusselsituasjon i Norge i 2009. Det ser ut til at angrepene var godt forberedt og organisert for å få størst mulig utbytte. Det er mange butikker som har vært utsatt for dette, særlig i østlandsområdet. Antall kort som potensielt kan ha vært utsatt for *skimming* antas å være mer enn 10 000. Forsøk på misbruk av kort har i all hovedsak skjedd i betalingsautomater utenfor Norge. Informasjonen er mest sannsynlig sendt ut av Norge via Internett til en mottaker det samarbeides med. Vi antar at det reelt sett er flere kort som er kopiert, men av ulike grunner enten blitt stoppet ved misbruksforsøk eller ikke brukt.

- **Ulovlig kopiering av kortinformasjon på innsamlings- og kortprosesseringssentraler utenfor Norge**
  Et annet økende problem er at kriminelle gjennom ulike teknikker har skaffet seg ulovlig tilgang til informasjon fra betalingskort hos innsamlingssentraler i land utenfor Norge. På den måten har de skaffet seg ulovlig tilgang til norske kortinnehaveres kortinformasjon i forbindelse med at betalingskortet til den norske kunden har blitt benyttet utenfor Norge. Norske banker har som generelt tiltak, da dette ble kjent, sørget for å sperre kortet, kontaktet kunden og utstedt nytt betalingskort. Denne typen ulovlig tilgang til betalingskortinformasjon har økt kraftig utenfor Norge. Det er særlig i USA, Storbritannia og Spania vi er kjent med at dette har skjedd. I praksis har det i Norge vært begrensede tap, men det har vært til stor ulempe for kundene og mye arbeid for bankene. I Norge er vi ikke kjent med at dette har skjedd i større skala. Siste gang Finanstilsynet registrerte en slik lekkasje var i 2004, og da i svært begrenset omfang. Det er imidlertid all grunn til å arbeide videre med tiltak på dette området for best mulig å sikre at informasjon om betalingskort ikke kommer på avveie.

Når det gjelder oversikt over samlet tap i Norge på de ulike tjenesteområdene, har Finanstilsynet i forbindelse med hendelsesrapporteringen og oppfølgingen av den, begynt å innhente mer presise tall fra enkeltorganisasjoner over tap. Dette er viktig informasjon for at tilsynet kan følge utviklingen over tid. For 2009 innhentet Finanstilsynet estimater som gir et relevant tapsbilde. Arbeidet med dette vil fortsette i 2010 slik at ROS-analysen for 2010 kan gi mer verifiserte data om samlede tap på aktuelle tjenesteområder.

4.3 Meldeplikten – systemer for betalingstjenester

Finanstilsynet har tilsynsansvar for systemer for betalingstjenester. Formålet er å bidra til at systemer for betalingstjenester blir innrettet og drevet slik at hensynet til sikker og effektiv betaling og til rasjonell og samordnet utførelse av betalingstjenester blir ivaretatt.

Institusjonene som er omfattet av betalingssystemloven skal uten opphold gi melding til Finanstilsynet om etablering av drift og system for betalingstjenester. Meldingen skal inneholde opplysninger om:

- avtalene mellom deltakende institusjoner om overføring eller uttak av betalingsmidler
- avtalene om tilknytning til brukersteder
- avtalene mellom systemer for betalingstjenester
- bruk av betalingskort, tallkoder eller annen form for selvstendig brukerlegitimasjon som skal benyttes ved betaling

Meldeplikten gir Finanstilsynet informasjon som kan fungere som grunnlag for risikovurdering og kontroll av etterlevelse av loven. Med bakgrunn i det relativt lave antallet meldinger som er mottatt, er det sannsynligvis noe underrapportering. I mange tilfeller viser det seg at kravene som blir stilt i innrapporteringen ikke har blitt fulgt i tilstrekkelig grad. Dette gjelder blant annet gjennomføring av tester før produksjonssetting, og at det også tar lang tid å innhente tilleggsinformasjon om nye eller endrede systemer for betalingstjenester.

5 Identifiserte risikoområder

5.1 Skimming

I 2009 ble det stjålet flere betalingsterminaler fra butikker i Norge. Terminalene blir så utstyrt med det nødvendige utstyr for å kunne kopiere innholdet i et betalingskorts magnetstripe (*skimming*), og sammen med PIN-koden til samme kort. Ut fra den informasjonen Finanstilsynet har mottatt, har disse tyveriene sammenheng med skimming av mer enn 10 000 kort, men bare for et mindre antall av disse har det oppstått tap. Denne type svindelmetode har ikke vært sett i Norge før, men lignende forsøk har tidligere skjedd i blant annet Storbritannia.

I Norge er det etablert standarder og krav til sikkerhet som tilsvarer de kravene til sikkerhet som kortselskapene stiller til løsninger for bruk av selskapenes kort. Standarden det vises til, er PCI-standarden. Denne standarden oppdateres jevnlig, men det gis ofte flere års utsettelse for at gamle produkter skal overholde de nye standardene. Det er Bankenes Standardiseringskontor, etablert av Finansnæringens Fellesorganisasjon (FNO), som har ansvar for å fastsette standarder og krav til sikkerhet i norske betalingssystemer.

Omfanget av skimming er så langt begrenset. Bakgrunnen for det er trolig at det er en relativt vanskelig måte å svindle på siden man trenger komponenter fra flere terminaler for å kunne lage en som fungerer. Videre må man ha detaljert teknisk kompetanse på teknologien i betalingsterminalene.

Så langt har risikoen i betalingskort vært knyttet til den relativt enkle oppgaven det er å kopiere informasjon fra et betalingskorts magnetstripe, for så å kopiere det over på et nytt falskt kort.

Ved overgang til bruk av chip vil denne risikoen bli redusert. Finansnæringen og Finanstilsynet anbefaler derfor alle brukere av betalingskort å benytte chipen og ikke magnetstripen ved betalinger i betalingsterminaler.

5.2 Identitetstyveri

I følge Datatilsynet defineres identitetstyveri som alle situasjoner hvor en person, uten samtykke fra rette vedkommende, enten:

- helt eller delvis er i stand til å utføre en eller annen form for uønsket transaksjon i en annen persons navn,
- skaffer seg tilgang til ressurser tilhørende andre, eller
- urettmessig tilegner seg rettigheter som tilhører andre

I følge the Federal Trade Commission er identitetstyveri et av de raskest voksende lovbruddene i USA. De mest vanlige metodene kriminelle benytter for å tilegne seg informasjon til bruk ved identitetstyveri, er:

Phishing og falske web-områder: Gir seg ut for å være velkjente organisasjoner gjennom svindel-e-postmeldinger (phishing) og falske web-områder.

Personlig oppmøte: Tyvlytter eller spionerer på mennesker under økonomiske transaksjoner.

Hacking: Bryter seg inn i databaser hvor persondata ligger, for så å hente ut nødvendig informasjon. Eksempel på dette er datainnbrudd i betalingskortbehandlere som Heartland Payment Services og RBS Worldpay.

5.3 Offshoring

Basert på informasjon Finanstilsynet har mottatt fra enkeltforetak, gjennom tilsynets interne prosjekt for kartlegging og vurdering av risiko knyttet til utkontraktering generelt og flytting av IKT-oppgaver ut av Norge spesielt (offshoring), har Finanstilsynet identifisert dette som et område med økt operasjonell risiko. Dette har både bakgrunn i dagens omfang når det gjelder utkontraktering og flytting av IKT-oppgaver ut av Norge, men også med basis i de pågående prosesser og planer hos enkeltforetak og IKT-leverandører på dette området som kan gi økt risiko.

En tilnærmingsmåte er å vurdere risikoen som gjelder for det enkelte finansforetak, både med hensyn til sannsynlighet og konsekvens av det enkelte risikoelement og på dette grunnlaget vurdere om risikoen er akseptabel. En annen tilnærmingsmåte er å se hele finanssektoren samlet, både med hensyn til sannsynlighet og konsekvens. Det kan da tenkes at konsekvensene samlet sett gir for høy operasjonell risiko veid opp mot en samfunnskritisk virksomhet.

Det vil derfor være nødvendig for Finanstilsynet å følge denne utviklingen nøye, særlig når det gjelder operasjonell risiko vurdert mot samfunnskritisk virksomhet. Det foreligger noen føringer på dette

området gjennom NOU 2006: 6, hvor deler av finanssektoren er definert som kritisk samfunnsfunksjon. Likeledes gjennom "Nasjonale retningslinjer for informasjonssikkerheten 2007–2010". Hovedgrunnlaget for en risikovurdering av dette området i Finanstilsynet vil likevel være en vurdering av etterlevelse av finanstilsynsloven og andre relevante lover og forskrifter som gjelder for de ulike delene av finanssektoren.

5.4 Stor endringstakt

Innenfor verdipapirområdet er det iverksatt store prosjekter som vil endre infrastrukturen. Oslo Børs inngikk i 2009 avtale med London Stock Exchange om kjøp av handelsplattformer for derivater og verdipapirer. Plattformen for derivater ble satt i produksjon første helgen i desember 2009. Handelsløsningen for aksjer er planlagt satt i produksjon i april 2010, men den største delen av arbeidet ble gjennomført i 2009. Endringene som gjennomføres innenfor verdipapirområdet er store og omfattende der oppfølgingen av risikoen som prosjektene løper, er svært viktig.

Som en konsekvens av at nye handelsløsninger settes i drift, vil medlemmene på Oslo Børs måtte gjennomføre endringer i sine interne systemer. I stor grad benytter medlemmene på Oslo Børs leveranser fra én og samme leverandør. I utgangspunktet kan dette ses på som en fordel hvor det å gjennomføre endringer én gang vil kunne implementeres av alle medlemmene. På den annen side benytter medlemmene løsningen ulikt, så noe skreddersøm må likevel påregnes. Dette vil kunne medføre økt leveringstid. Våre naboland gjennomfører tilsvarende prosjekter hvor også de er avhengige av leveranser fra samme leverandør. Med stort press på leveranser fra alle involverte i verdidpapirinfrastrukturen vil dette kunne øke den totale operasjonelle risikoen for verdipapirvirksomhet og føre til forsinkelser.

5.5 Katastrofe

IKT-forskriftens § 11 Driftsavbrudd og katastrofeberedskap stiller krav til at det minst én gang årlig skal gjennomføres opplæring, øvelse og test i et omfang som gir tilstrekkelig trygghet for at katastrofeløsningen virker som forutsatt. Resultatet av testen skal dokumenteres slik at det er mulig å kontrollere.

Finanstilsynets erfaringer fra mottatt dokumentasjon viser at det å gjennomføre og dokumentere katastrofetester er et område som det må legges vekt på fremover. Erfaringer viser flere foretak som baserer egen katastrofetest på at løsningen kun testes hos driftsleverandørene og ikke som en integrert del av foretakets katastrofeløsning. Fungerende katastrofeløsninger er ofte en forutsetning for at foretak skal kunne drive forsvarlig dersom en katastrofesituasjon oppstår.

5.6 Kompleks infrastruktur

Den økende kompleksiteten i IKT-infrastruktur er utfordrende. Tradisjonelt er datasentralene delt i tre hovedgrupper som har ansvar både for utvikling og vedlikehold av datautstyr, systemer, applikasjoner og leveranser. Gruppene dekker serverfarmer, lagring og nettverk. De ulike miljøene som har slikt ansvar, bygger opp egne miljø for å verne om eget kompetanseområde. Dette går på bekostning av den nødvendige kommunikasjonen som bør være åpen og uhindret mellom alle disse tre hovedgruppene. Manglende koordinering med de andre gruppene og vern om egne områder øker kompleksiteten, gir dårligere styring og kontroll av operasjonell risiko samt medfører unødvendige koordineringskostnader.

Dette bildet blir enda mer komplisert når det også tas hensyn til alle mindre underleverandører av for eksempel applikasjoner som bare er opptatt av å levere mindre deler av hele IKT-infrastrukturen til et allerede fragmentert IKT-miljø.

Ved at operasjonell risiko i større grad er knyttet til avsetninger til egenkapital innen Basel II (ICAAP), er det tidsbegrenset hvor lenge en uoversiktlig IKT-infrastruktur skal kunne aksepteres. Det vil derfor bli satt et ytterligere søkelys på at foretakene selv kan dokumentere alle elementene i IKT-infrastrukturen og at de samtidig forstår hvordan de enkelte elementene fungerer sammen. Dette må igjen bygges inn i foretakenes strategiske og operasjonelle planer og ledelsesmessige kontrollsystemer.

5.7 Transaksjonskjede

Flere leverandører av IKT-tjenester er involvert i de finansielle tjenestene. På sin vei kan transaksjonen bli transportert i nett som har ulike protokoller. I punktene der transaksjonen overleveres fra en leverandør til neste, må transaksjonen åpnes og omformes slik at den passer til transportprotokollen i neste etappe. Et tenkt eksempel kan være en tjeneste som leveres via mobiltelefonen. Transaksjonen transporteres da ved hjelp av mobilnettet og tilhørende protokoll (GSM) og sikring (GSM-kryptering) til teleleverandørens server der den pakkes opp, omformateres (for eksempel til IP), rekrypteres og transporteres videre til tjenesteleverandøren. I omformateringspunktet er transaksjonen sårbar, for eksempel for uautorisert innsyn. For å kompensere for usikkerheten anbefales det å gjøre ende til ende-kryptering på applikasjonsnivå. Slik kryptering innebærer utfordringer både teknisk og logistikkmessig knyttet til sikring av nøkler og administrasjon av nøkler (nøkkelbytte). Risikoen øker i takt med at transaksjonskjedene blir lengre og ytterligere automatisert.

6 Finanstilsynets videre oppfølging

6.1 Aktuelle tiltak

Det er først når en risiko er kjent at det er mulig å iverksette hensiktsmessige tiltak. Når egen risikoforståelse er liten, blir det ofte hendelsene som styrer sikkerhetsarbeidet. Det er ikke alltid slik at det er mulig å oppdage alle sårbarheter på forhånd, men det bør være et mål at alle sårbarheter som kan avdekkes gjennom målrettet risikoarbeid og andre planmessige tiltak blir det som samlet ligger til grunn for risikoreduserende tiltak. Vi vet også at det ofte er slik at reparasjon koster vesentlig mer enn om aktuelle problemer er tatt høyde for på en planlagt måte. I sitt tilsynsarbeid legger Finanstilsynet vekt på foretakenes preventive sikkerhetsarbeid.

Tiltak som Finanstilsynet kan ivareta på risikoområdet er i hovedsak:

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

- å forvalte hendelsesrapporteringssystemet og sikre at informasjon fra rapportering om IKT-hendelser til Finanstilsynet via e-post til: hendelse@finanstilsynet.no benyttes til preventive tiltak, og samtidig bidra til å sikre at feilsituasjoner som oppstår blir håndtert hensiktsmessig og at det raskest mulig blir gjenopprettet normal drift

- å innhente nødvendig informasjon, blant annet gjennom arbeidet med ROS-analysen, for å ha en mest mulig riktig risikoforståelse av finanssektoren som helhet

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

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

Å overvåke prosesser og ressurser er en forutsetning for å kunne forutse flaskehalser og trender i tide og å reagere og avverge en uønsket situasjon. Finanstilsynets hendelsesstatistikk for 2009 indikerer at foretakene bør legge mer vekt på overvåking. God overvåking er ikke bare et spørsmål om gode verktøy. Det å sette inn overvåking på rett sted, sette riktige terskelverdier og lage og innarbeide gode rutiner for å reagere og rapportere, krever personell med høy kompetanse. Finanstilsynet anbefaler foretakene å prioritere dette viktige området i 2010.

Nedenfor vil vi redegjøre noe mer i detalj for hvordan bruk av aktuelle virkemidler innrettes og benyttes som bidrag til forsvarlig håndtering av operasjonell risiko.

6.2 Økt vektlegging av brukerstedene

Mangelfull sikkerhetsforståelse hos brukersteder kan føre til implementeringer som er beheftet med sikkerhetsmangler som åpner for misbruk og svindel. Hendelser i 2009 indikerer at det er behov for at den tjenesteansvarlige forbedrer kontroll på brukerstedene. Kontrollen kan tenkes å ta flere former.

Når PKI-tjenester nå etter hvert tas mer i bruk, kan det være ønskelig at den ansvarlige for PKI-tjenesten tar ansvar for at brukerstedet som godtar ID-en har implementert denne i sin tjeneste på en måte som gir brukeren tilstrekkelig sikkerhet for at ikke uvedkommende kan gjøre transaksjoner i rette brukers navn etter at sistnevnte er autentisert. For eksempel bør brukeren kunne forvente at brukerstedet har implementert ID-tjenesten i sin infrastruktur på en slik måte at en ID ikke lett kan misbrukes. Slikt misbruk kan for eksempel skje ved at uvedkommende ”henger seg på” en pålogget sesjon, ”plukker opp” en sesjon som rette bruker tror er avsluttet, men som ”henger” og fremdeles er åpen på brukerstedssiden og lignende. ID-tjenesten har liten verdi hvis den er implementert i brukerstedets tjeneste på en måte som åpner for slikt misbruk.

ID-leverandøren bør kreve at brukerstedet kvalitetssikrer integrasjonen av ID-tjenesten i brukerstedets tjeneste etter nærmere regler definert av ID-leverandøren.

6.3 IT-tilsyn

Gjennomføring av IT-tilsyn i tilstrekkelig omfang er et grunnleggende virkemiddel for å foreta ”temperaturmåling” av hvordan finanssektoren håndterer bruk av IKT og risiko knyttet til dette. Det er derfor viktig og fortsatt gi prioritet til økt IT-tilsyn, samtidig som det er en utfordring å videreutvikle tilsynsopplegget slik at relevante problemer og sårbarheter kan identifiseres.

Det pågår fortsatt en videreutvikling av tilsynsopplegget med forbedring av eksisterende opplegg og etablering av nye tilsynsmoduler. Likeledes pågår en videreføring av arbeidet med å ta i bruk en

metodisk gradering av modenhetsnivået til foretakets IKT-organisasjon. Det konseptuelle arbeidet med etablering av egen modul for såkalt transaksjonstest pågår også, og denne vil være siste hovedmodul i den totale IT-tilsynsarkitekturen. Finanstilsynet regner med gradvis å ta metodene i bruk og høste noe praktisk erfaring i løpet av 2010.

6.4 Videreutvikling av opplegget for meldeplikt for systemer for betalingstjenester

Finanstilsynet vil fortsette arbeidet med egenmelding som grunnlag for å ivareta ansvaret for meldeplikten for betalingstjenester, som er regulert gjennom betalingssystemloven § 3-3. Også i dette arbeidet er risikobetraktninger lagt til grunn. Finanstilsynet vil prioritere preventive tiltak for å bedre sikkerheten i betalingstjenestene som har elektroniske kanaler direkte til kunder. Elektroniske betalingstjenestene representerer en viktig samfunnsfunksjon. Samtidig er denne type tjenester under angrep fra organisert kriminalitet. Arbeidet på dette området vil foregå i nært samarbeid med bransjeorganisasjoner og fellesinstitusjoner som bankene har etablert på dette området. Det er laget en ny tilsynsmodul for systemer for betalingstjenester som benyttes i forbindelse med IT-tilsyn.

Standardskjemaet på 19 spørsmål (rundskriv 17/2004) som meldeplikten nå er basert på, vil bli gjennomgått i løpet av 2010. Målsettingen er å få en mer detaljert beskrivelse fra alle aktører om hva nye eller endrede systemer for betalingstjenester inneholder, samt hvilke ledd som er kritiske i produksjonen.

6.5 Gjennomføring av ROS-analyser

Gjennomføring av ROS-analyser som dekker hele finanssektoren er viktig, både for å sikre tilstrekkelig løpende forståelse av den operasjonelle risikoen når det gjelder bruk av IKT, og å sikre at det blir mulig å sammenligne resultater over år og mellom ulike deler av finanssektoren. Kunnskapen som Finanstilsynet får gjennom ROS-analysene representerer et viktig grunnlag for å prioritere fremtidige tilsyn, og for å beslutte risikoreduserende tiltak og/eller kvalitetsforbedringer.

6.6 Hendelsesregistrering og -rapportering

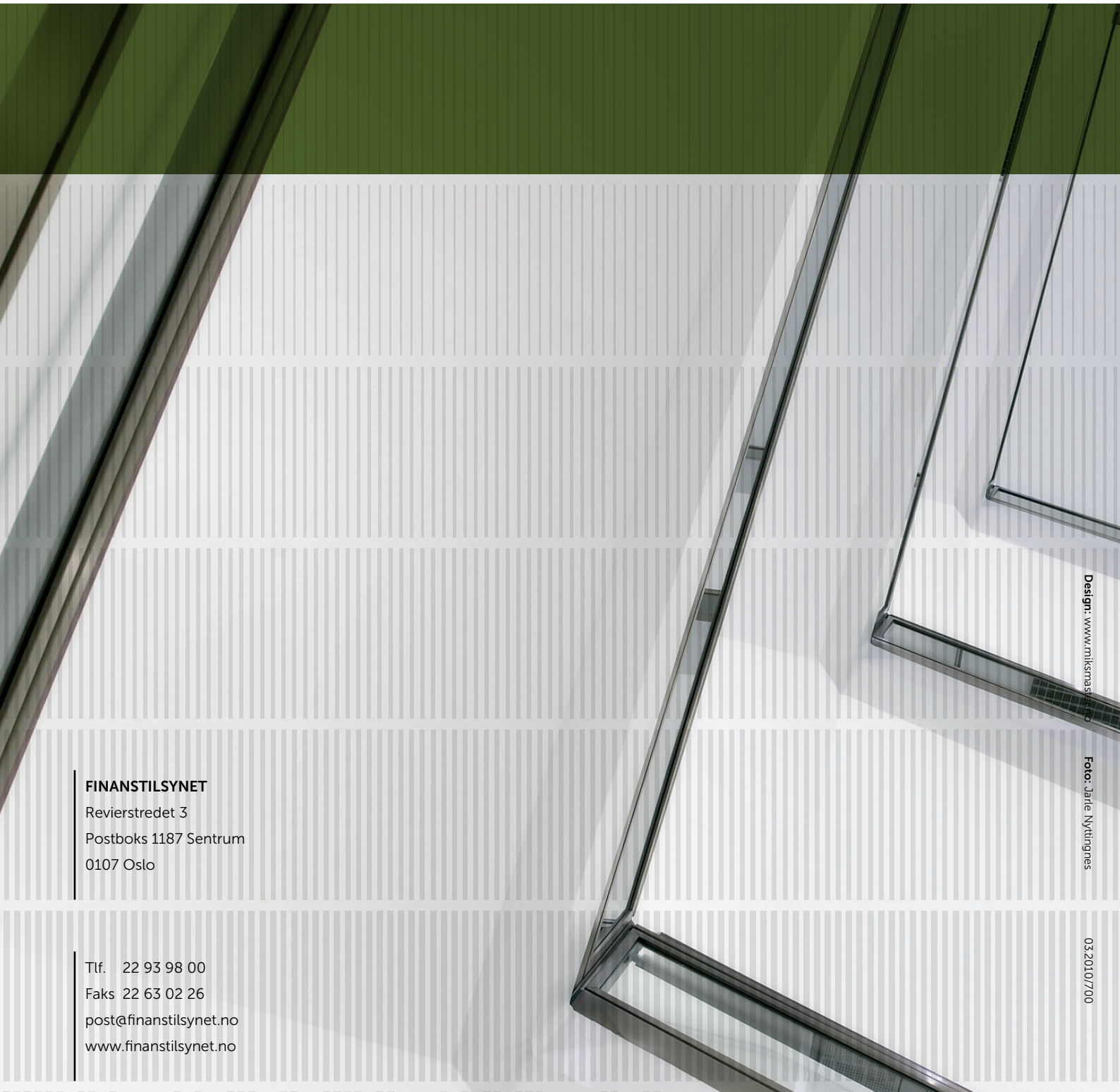
I 2007 ble det etablert et opplegg for hendelsesrapportering til Finanstilsynet. Dette var en prøveordning for banker, Oslo Børs, Verdipapirsentralen og Bankenes BetalingsSentral. På bakgrunn av resultatene fra prøveordningen, konkluderte Finanstilsynet med at dette var hensiktsmessig for å

sikre tidsriktig og korrekt informasjon om alvorlige IKT-hendelser i finanssektoren. Datagrunnlaget fra hendelsesrapporteringen benyttes som kilde til ROS-analysen, og er et bidrag til kvantitative data i rapporten. Rapportene brukes også som grunnlag for å ta opp aktuelle problemstillinger direkte med berørte foretak. I 2009 besluttet Finanstilsynet derfor å regulere hendelsesrapportering i form av en forskrift som gjelder fra 1. desember 2009. Finanstilsynet vil legge betydelige ressurser i oppfølgingen av opplegget og bruk av dataene i sitt arbeid. Det planlegges å etablere et brukerforum for deltakerne i hendelsesrapporteringen.

6.7 Informasjon og kommunikasjon

Som et ledd i arbeidet med IKT-sikkerhet i finanssektoren deltar Finanstilsynet i en rekke ulike fora. Blant de sentrale er Koordineringsorganet for forebyggende informasjonssikkerhet (KIS) og Beredskapsutvalget for finansiell infrastruktur (BFI). Det samarbeides også direkte med Norges Bank, Nasjonal sikkerhetsmyndighet (NSM), Post- og teletilsynet, Datatilsynet og bransjeorganisasjoner. Finanstilsynet samarbeider også nært med de øvrige nordiske IT-tilsynsenhetene, og er med i et internasjonalt IT-tilsynssamarbeid (Information Technology Supervisors Group) med en europeisk undergruppe. Likeledes deltar tilsynet i arbeidet med internasjonal standardisering i gruppene for bank- og sikkerhetsstandarder, standardisering for elektroniske signaturer (ETSI ESI) og i den internasjonale dataforeningen IFIPs gruppe for sikkerhet.

Finanstilsynet deltar i et EU-prosjekt knyttet til internettsikkerhet og varsling (Communication Middleware for Monitoring Financial Infrastructures). Prosjektet er støttet av EUs sjuende rammeprogram for forskning og utvikling og har en varighet på to og et halvt år (til 2011). Hensikten med prosjektet er å komme frem til tiltak som kan gjøre finanssektorens bruk av Internett mer sikker (europeiske tiltak). I prosjektet er Finanstilsynet med på å definere krav som tilsynsmyndigheter ønsker å stille til et overvåkings-/varslingssystem. Det er etablert en referansegruppe med representanter fra banker. I slutten av 2009 deltok Finanstilsynet i en ny prosjektsøknad til EUs sjuende rammeprogram på området, overvåkingssystem som tiltak mot hvitvasking betegnet OMAS (Online Money Laundering Report and Analysis System).



FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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

Design: www.miksmaster.no

Foto: Jarle Nyttingnes

03.2010/700