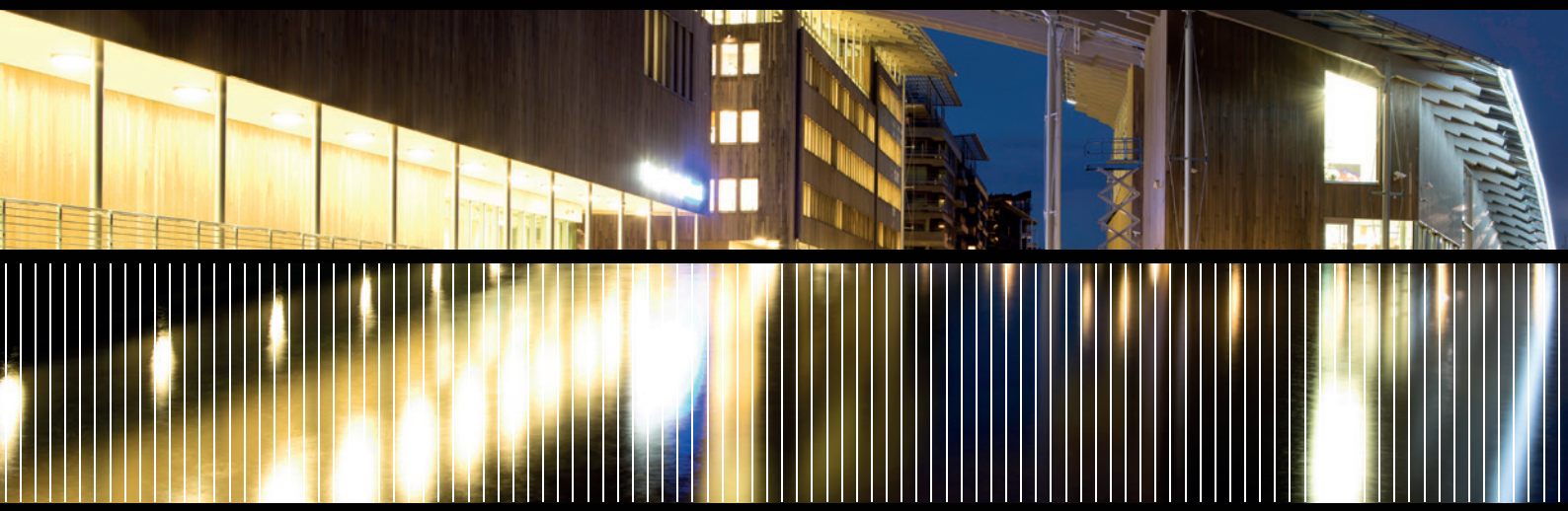
FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

RISIKO- OG SÅRBARHETSANALYSE (ROS)
2012



RAPPORT

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Risiko- og sårbarhetsanalyse (ROS) 2012

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Finanstilsynet, 5. april 2013

Innhold

1 Innledning

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

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

For å forstå hva som kan gi økt risiko i framtiden, er det viktig å ha fakta om risikosituasjonen og være i stand til å tolke hvilke faktorer som kan endre seg over tid og gi høyere risiko. Finanstilsynets årlige ROS-analyse har som mål å gi et bilde av risikoutviklingen i finanssektorens bruk av IKT og betalingstjenester.

1.1 Sammendrag

Det var registrert økende tap på betalingstjenestene i 2012. Særlig var det økte tap på nettbankløsningen i forhold til 2011, men tapene var relativt sett fortsatt lave.

Det var også økning i kriminelle angrep på betalingstjenestene, særlig knyttet til nettbankløsninger og internetthandel med betalingskort. Via Internett var det en sterk økning i såkalte DDOS-angrep ("Distributed Denial of Service Attack") i 2012.

I avregnings- og oppgjørssystemene var det høy stabilitet i 2012. Det var noen alvorlige hendelser knyttet til betalingstjenestene, men året sett under ett må likevel vurderes som stabilt. Det kan være viktig at bankene er tydeligere overfor kundene om hva som kan forventes av åpningstider på nettbanken. Det forventes at denne er tilgjengelig 24/7, men dette er ikke formelt forpliktet i avtalene med kundene. Det var en alvorlig hendelse på Verdipapirsentralen knyttet til feil sletting av aksjeregisterdata som senere ble gjenopprettet.

I kapittel 2 i rapporten beskrives generelle trender på IKT-området som har eller kan få betydning for risikohåndtering i Norge.

Kapittel 3 omtaler systemer for betalingstjenester som representerer en vesentlig del av virksomheten til bankene, men som også er en viktig forutsetning for øvrige deler av finanssektorens virksomhet. Det gis en vurdering av det generelle risikonivået, alvorlige hendelser knyttet til betalingstjenestene og utviklingen av kriminelle angrep mot betalingstjenestene. Det gis også en statistikk over tap i 2011 og 2012 knyttet til betalingstjenestene.

Kapittel 4 behandler funn og observasjoner som Finanstilsynet gjorde i 2012. De viktigste kildene for dette er gjennomførte tilsyn, innrapportering om hendelser, intervju med utvalgte tilsynsenheter og gjennomganger som er foretatt hos tilsynsenhetenes IKT-leverandører.

Kapittel 5 omtaler områdene som er vurdert å ha høyest risiko. Disse er:

- styring og kontroll
- angrep på nettbaserte løsninger
- kontinuitets- og katastrofeløsninger
- risiko ved gamle og komplekse system
- tilgang til betalingstjenester

I kapittel 6 gis det en beskrivelse av tiltak Finanstilsynet vil arbeide videre med knyttet til risikoområdene.

2 Utviklingstrekk

Det er en utfordring å følge med i utviklingen innen teknologi, tjenesteleverandører, datakriminalitet og nasjonale og internasjonale reguleringer og som kan påvirke risikobildet. Manglende forståelse og oppfølging kan føre til økt risiko. Det er derfor viktig at utviklingen følges for å sikre håndtering av en situasjon under endring.

2.1 Privat utstyr

Ansatte i offentlige og private virksomheter benytter i økende grad private mobile enheter (BYOD – "Bring Your Own Device") i jobbsammenheng. Finanstilsynets undersøkelser blant finansforetak i Norge indikerer imidlertid at disse er svært restriktive når det gjelder å tillate BYOD. Dersom det i foretaket er slik at sikkerhetsbestemmelsene som gjelder for foretakets arbeidsstasjoner, ikke gjelder for privat utstyr, må foretakets interne nettverk avvise privat utstyr som blir forsøkt tilkoblet foretakets nettverk. Foretaket bør da se på privat utstyr som en trussel, og anvende kjente mottiltak, som f.eks. antivirus, brannmur, IDS, IPS og trojanersignaturer.

Foretaket må kontrollere om privat utstyr er oppdatert sikkerhetsmessig, før utstyret eventuelt tillates å kommunisere i foretaket.

Privat utstyr har etter hvert stor lagrings- og behandlingskapasitet. Finansforetakets data og programmer kan praktisk overføres til privat utstyr. Det er viktig at foretaket har gode rutiner for å logge slik aktivitet. Dette er et generelt tiltak mot datatyveri, men introduksjon av privat utstyr aktualiserer problemet.

Finansforetak bør ha rutiner for plikt for ansatte til å melde om tapt utstyr, og at foretaket da har rett til å slette bedriftens data som måtte ligge lagret på den mobile enheten via nettet om dette er mulig.

Én usikret maskin i et nettverk er nok til at utenforstående kan skaffe seg "kontroll" over et nettverk. Automatiserte søkeprogrammer gjør det mulig å oppdage usikrede elementer. Det er derfor viktig å ha god oversikt over maskinene i nettverket. Også maskiner som sjelden blir benyttet og reserveutstyr må oppdateres etter de generelle sikkerhetsprosedyrene.

2.2 Identitetstyveri

Finanstilsynet bruker begrepet identitetstyveri der noen på uærlig vis har tilegnet seg personrelatert informasjon som misbrukes for å oppnå økonomiske gevinster eller andre fordeler uten den rettmessige eiers kjennskap. Identitetstyveri skjer blant annet ved at den som er på jakt etter identiteten:

- tar kontroll over brukeren ved hjelp av såkalt overlay services, phishing, trojaner eller tyveri av ID-papirer,
- utgir seg for å være banken ved hjelp av trojaner, falske sertifikater, falske nettsider, kopiere logo og annet,
- "tar over" nettverket ved hjelp av programmer som sender kunden til "angriperens" nettside i stedet for bankens, såkalt DNS-poisoning (Domain Name System).

Det er veldig enkelt i dag å kopiere bilder, tekst og internettsider. Angripere benytter kopiene og utgir seg for å være originalen. Angripere låner også logo og tekst fra banken og utgir seg for å ha bankfullmakter.

2.3 Utkontraktering

2.3.1 Offshoring

Utkontraktering til IKT-leverandører i land med større IKT-miljøer og lavere kostnadsnivå enn Norge, såkalt offshoring, skjer i større grad enn tidligere. I tillegg til kostnadsbesparelser, er det mange som vurderer at større, globale kompetansesentre gir sikrere tilgang til kompetanse og større fagmiljøer, noe som kan bidra til økt kvalitet i leveransen.

Kompetansen knyttet til eldre teknologi (Cobol, CICS, IMS, PL/1) kan være vanskelig å opprettholde i det enkelte finansforetaket. Det kan derfor være hensiktsmessig å samle kompetansen i internasjonale foretak som betjener flere foretak.

Det er viktig at foretakene sikrer at leverandøren av IKT-løsninger tilfredsstiller gjeldende norsk regelverk og beste praksis.

Besparelser og tilgang til kompetanse er viktige temaer når foretaket vurderer utkontraktering og offshoring. Foretaket vil normalt kun vurdere egen situasjon uavhengig av andre foretak i samme sektor. Hensynet til den samfunnsmessige risikoen ved at driftssystemene for finansielle tjenester flyttes ut av landet, er et forhold som det enkelte foretaket antakelig ikke vurderer som grunnlag for egne beslutninger, men som må vektlegges i en samfunnsmessig risikovurdering.

2.3.2 Cloud computing

Begrepet "cloud computing" (skytjenester) benyttes ofte om en leveranse av service fra Internett, for eksempel systemer for ekstern lagring av data. Slike tjenester er en variant av utkontraktering.

Skytjenester innebærer at datamaskiner og programmer (IT-ressurser) deles mellom aktuelle brukere. IT-ressursene representerer et nettverk som lagrer store mengder data for et stort antall dataservere.

Skytjenester har tidligere ikke vært godt tilpasset finanssektoren. I 2012 ble disse tjenestene lansert:

- NASDAQ OMX Financial cloud
- SAPs corporate bank-to-cloud

Dersom kunde- og kontoopplysninger er lagret i skyen og banktjenestene tilbys som skytjenester som nås ved hjelp av mobiltelefonen, vil det ikke lenger være behov for å distribuere løsninger på samme måte som i dag. Butikkterminaler og kort kan bli overflødig fordi mobiltelefonene benyttes for å nå kunde- og kontoinformasjon som ligger i skyen. Og brukeren kan klare seg med én ID, i motsetning til dagens situasjon der brukeren har mange ID-er å holde styr på, én eller flere nettbank-ID, flere kort og koder og flere sikkerhetskoder til VISA/MasterCard. Dette vil gi enkel administrasjon og minimum av utstyr er involvert, noe som reduserer behovet for vedlikehold og risiko for feil. Skyen er alltid tilgjengelig.

På den annen side kan "kunden i skyen" bli et "single point of compromise", det vil si at dersom en angriper stjeler brukerens ID, kan tyven påføre brukeren stor skade.

Skylagring kan gi bedre driftsstabilitet og redundans. Som eksempel kan en vise til Google App-er, hvor data er replikert over mange systemer slik at ikke noe system utgjør et "single point of failure". Hver enkelt brukers data er replikert til minst to datasentre, der begge sentrene kan betjene brukeren.

Samtidig mangler det regelverk og likeverdig avtaleverk for bruk av grensekryssende skytjenester, slik at konfliktløsning mellom tilbyder og kunde kan bli en utfordring. Det mangler også metoder slik at kundene kan få hjelp til å velge leverandør ut fra de mer uttalte risikoene ved skybruk.

2.4 Tjenesteutvikling i betalingssystemer

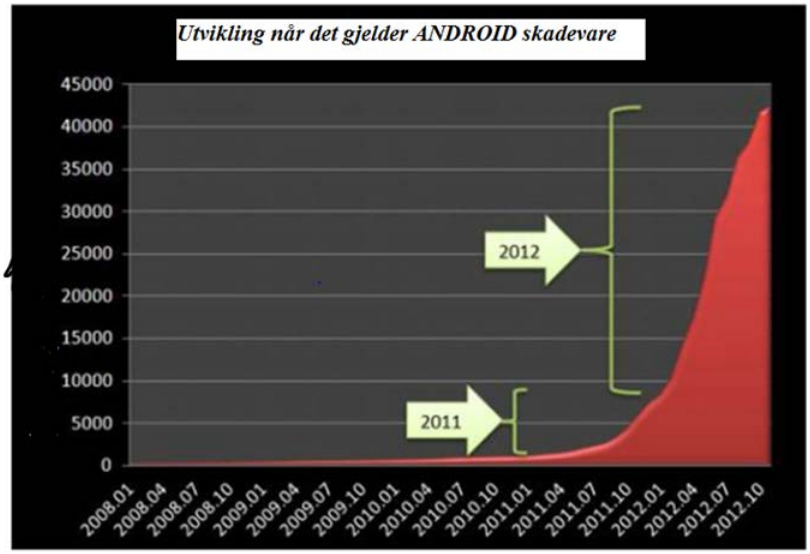
2.4.1 Nettbank på mobil

Flere og flere tjenester tilbys på mobil. I den senere tid har BankID-app, Nettbank-app og mobilbank-app ("mCash") blitt utviklet.

Risikoene ved disse mobiltjenestene er delvis de samme som for nettbank via PC. Mobiltjenestene har

imidlertid en risiko knyttet til "mobile skadevarer" som kan illustreres slik:

Figur 1: Android skadevare, antatt utvikling



Source: ZDNet

2.4.2 Bruk av BankID

BankID, som er bankenes felles system for bankkunders autentisering og elektronisk signatur, er nå godkjent som elektronisk ID av norske myndigheter. BankID skal kunne benyttes som innlogging til ca. 270 offentlige tjenester.

BankID på PC er basert på programproduktet Java fra Oracle. Java er en generell utviklingsplattform for et bredt spekter av utstyr og formål. Et betydelig sikkerhetshull i Java ble nylig avdekket. NorCERT og en rekke banker anbefalte kundene å avinstallere Java. Samtidig er det slik at et antall store banker i Norge krever at BankID benyttes. Disse nettbankene vil dermed være stengt for kunder som avinstallerer Java. Dette illustrerer hvor sårbart betalingssystemet kan være. Bankene arbeider aktivt med å gjøre BankID mer robust mot disse truslene.

I tillegg til banktjenester og offentlige tjenester, er det en rekke andre større og mindre brukersteder[1] som kan benyttes med BankID. Dersom brukeren etter hvert benytter BankID i meget stort omfang, kan det føre til at brukeren blir mindre kritisk når det gjelder å oppgi innloggingskoder (fødselsnummer, engangskode og fast kode) på nettet. Økt bruk av BankID kan øke risikoen for at brukere forledes til å oppgi koder til noen som urettmessig utgir seg for å være BankID-brukersted.

[1] https://www.bankid.no/Dette-er-BankID/Her-kan-du-benytte-BankID/

2.4.3 Mer avanserte og aggressive trojanere

Ondsinnet kode (trojaner) har blitt mer avansert. Koden analyserer kundens PC, finner svakheter, laster ned tilpasset ondsinnet programvare, overvåker kundens aktivitet og tilegner seg innloggingskoder eller introduserer falske transaksjoner mens den rette brukeren er pålogget. Det finnes databaser med oversikt over kunder som låner bort kontoen sin (såkalte mules) som mellomstasjon for stjålne midler. Disse kontoene hentes idet angrepet skjer.

2.4.4 DDoS

DDoS (Distributed Denial of Services) genererer transaksjoner (trafikkvolum) mot et nettsted for å "lamme" nettstedet for annen trafikk. I 2012 var det en markert økning i DDoS-angrep mot sentrale finansforetak. Dette er i samsvar med utviklingen internasjonalt.

Analyser av DDoS i Norge har ikke avklart om hensikten har vært "hærverk", eventuelt testing, kamuflering av et datainnbrudd eller nedstengning av en konkurrent. Foretakene som var utsatt for angrepene, har iverksatt effektive tiltak og samarbeidet med NorCERT og ISP-ene (Internet Service Provider).

2.4.5 Svakheter i infrastrukturen

Økte krav til tilgjengelighet og integrasjon av systemer fra ulike leverandører stiller høye krav til nettverk med hensyn til kvalitet og tilgjengelighet.

Nettverkene er inndelt i soner og atskilt ved hjelp av brannmur. Brannmuren er sentral. Dersom man ikke er knyttet til brannmuren på riktig måte, kan det få store negative konsekvenser for mange brukere. Samtidig øker antall tjenester og koblinger, noe som fører til at vedlikeholdet av brannmurene blir mer utfordrende.

2.4.6 Behov for modernisering av kjernesystemer

Mange av kjernesystemene i norsk finanssektor er 20–30 år gamle. I den tidlige perioden var det få tjenester og distribusjonskanaler. Nye tjenester er i stor grad programmert og lagt "utenpå" de opprinnelige kjernesystemene.

Ved hyppig etablering av nye tjenester og kanaler er det behov for å utvikle løsninger der likeartede funksjoner kan gjenbrukes. Et eksempel kan være en rapport, som typisk vil benytte funksjoner i et lag som inneholder ulike spørringer til databasen, i et lag som inneholder databaseskjemaer, i et lag med databasespørringer (SQL-spørringer), i et lag med rapportformatering og i et lag med rapportpresentasjon. Lagene "sys sammen" ved hjelp av standardiserte spørringer til laget over/under. Funksjonene i lagene kan kopieres og brukes som mal for en likeartet funksjon i samme laget. Testing kan begrenses til test mot laget over og under. Det motsatte er at det ikke er en planlagt arkitektur for løsningene, og det blir separate løsninger.

Mange banker har utfordringer knyttet til gammel arkitektur. Dette fører til økt kompleksitet med fare for feil og driftsavbrudd.

I tillegg til at den gamle arkitekturen er krevende å vedlikeholde, er kompetansen på de gamle systemene i ferd med å bli redusert betydelig.

2.4.7 Integrasjon

Finanstilsynet har de siste årene vært opptatt av risiko knyttet til funksjonsdelingen i nettjenester fra brukerens registrering av en transaksjon til endelig avregning i banken. I 2012 var det en økning i automatiserte tjenester som er blitt integrert med andre tjenester, og dette øker risikoen for feil.

Et nettverk inneholder et stort antall servere og funksjoner. Enkelt vedlikehold og stabil drift tilsier at alle brukere kaller på samme utgaven av funksjonen. Det finnes en rekke integrasjonsservere for dette formålet. Integrasjonsløsningen kan introdusere sikkerhetshull når kommandoer og data blir konvertert fra ett system til et annet. Et eksempel er kryptering. Ettersom en integrasjonsløsning konverterer og viderebefordrer informasjon og kommandoer, må en eventuell kryptering avsluttes i integrasjonsserveren for deretter å bli lagt til igjen i neste ledd av integrasjonen og kommunikasjonen. Et eksempel på dette er konvertering fra mobilnettet til banknettet når det gjelder mobilbank.

Selve integrasjonsserveren kan ha svakheter. I tillegg inneholder den som regel et stort antall krypteringsnøkler, innloggingskoder og passord som en inntrenger kan utnytte til å angripe alt fra interne systemer til integrerte skytjenester. Dersom en server ikke er beskyttet, kan angriperen injisere meldinger i integrasjonssystemet og ta kontroll over målsystemet innenfor. På denne måten ble tillitstjenesten (Certificate Authority) DigiNotar kompromittert.

Utfordringene med å få en integrasjonsserver til å fungere som tenkt, kan føre til at IT-teknikere og administratorer lar være å ta i bruk de innebygde sikkerhetsfunksjonene i produktene. Dessuten oppfattes integrasjonssystemer sjelden som virksomhetskritiske. De blir mer sett på som hjelpeverktøy, noe som kan føre til at sikkerhetshull ikke blir oppdaget.

2.4.8 Svakheter i betalingskort med chip

Forskeren Ross Anderson[2] m.fl. har oppdaget en gjennomgående svakhet ved generering av sikkerhetsverdier for betalinger med kort. Ved hjelp av skadevare fiskes transaksjonsinformasjon som gir grunnlag for beregning av en autentiseringskode. Denne informasjonen sammen med kortinformasjon og PIN-kode er tilstrekkelig for å kunne gjennomføre nye transaksjoner som ser autentiske ut, og ser også ut som om de kommer fra det originale betalingskortet med chip. Finanstilsynet er ikke kjent med at en slik svakhet foreløpig har vært utnyttet i det norske betalingskortmarkedet.

[2] http://www.cl.cam.ac.uk/~sjm217/papers/ches12preplay.pdf

2.5 Regulatoriske utviklingstrekk

Endringer i regelverk kan føre til behov for å gjøre endringer i eksisterende IT-systemer, IT-driftsopplegg, prosedyrer og kontrollopplegg. Slike endringer kan representere en operasjonell risiko. Følgende norske regelendringer er av betydning for arbeidet med risiko knyttet til automatiserte finansielle tjenester:

- Lov om næringsberedskap[3] trådte i kraft 1. januar 2012. Loven regulerer samarbeid om tiltak ved alvorlige avbrudd.
- Forbrukerombudet har ment at teleoperatørene må ta et større ansvar. Forbrukerombudet[4] krever to kontrakter for bruk av mobiltelefonen: Én for kommunikasjon, og én for betaling. Den siste forutsetter konsesjon fra Finanstilsynet.
- En sak som gjaldt lagring av e-post i skyen for en norsk kommune har gitt verdifull innsikt og verdifulle avklaringer når det gjelder vilkårene for lagring i skyen sett fra et personvernsynspunkt[5]. Datatilsynet peker på kravet om at det skal være foretatt risikovurdering, jf. personopplysningslovens § 13 og personopplysningsforskriftens § 2-4. Avtalte forhold knyttet til databehandlers innsyn, sikkerhetskopiering, sikkerhetsrevisjon, innsynsbeskyttelse (kryptering), jurisdiksjon, sletting av data og opphør omtales også.
- I juni 2012 publiserte Baselkomiteen reviderte retningslinjer til bruk for tilsynsmyndigheter når disse skal vurdere internrevisjonsfunksjoner i bank.[6] Retningslinjene beskriver prinsipper for internrevisjonen i bank.
- EU-kommisjonen har laget utkast til ny persondataforordning.[7] Forordningen gir privatpersoner utvidet rett til innsyn når det gjelder hvilke data som er lagret og behandlingen av dem.

2.6 Internasjonale utviklingstrekk

2.6.1 Generelle initiativer

Det pågår et løpende arbeid i EU med sikte på å etablere prinsipper for beste praksis når det gjelder elektroniske finansielle tjenester. Følgende kan framheves for 2012:

EU-kommisjonen har gitt ut et "green paper" med tittelen "Towards an Integrated European Market for

[3] http://www.lovdata.no/all/hl-20111216-065.html#map001
[4] http://www.forbrukerombudet.no/2012/04/11042228.0
[5] http://www.datatilsynet.no/Global/05_vedtak_saker/2012/11-00593-18%20Avslutning%20av%20sak%20-%20Ny%20e-postl%C3%B8sning%20i%20Narvik%20Kommune%20-%20Google%20Apps.pdf
[6] http://www.bis.org/publ/bcbs223.pdf
[7] http://ec.europa.eu/justice/data-protection/index_en.htm.

Card, Internet and Mobile Payments".[8] Rapporten inneholder forslag til anbefalinger om integrering av europeisk kortinfrastruktur.

Denne rapporten gir anbefalinger om en framtidig integrert europeisk kortinfrastruktur. Forhold knyttet til gebyrer blir også omtalt. Gebyrer må gjenspeile kost og dermed påvirke til effektive løsninger. Kunden skal informeres om kostnader knyttet til lojalitetsprogrammer og eventuelle andre kundeprogrammer. Videre belastning til kunden av brukerstedets kostnader knyttet til betalingsinstrumentet, såkalt surcharging, skal dekke kostnader og ikke være en inntektskilde. Direktiv 2011/83/EU fra EU-parlamentet og EU-rådet om forbrukerrettigheter,[9] datert 25. oktober 2011, som skal være integrert i nasjonal lovgivning innen 13. juni 2014, vil sørge for at økt belastning på kundene vil opphøre.

European Payments Council (EPC) anbefaler å innføre en harmonisert sertifiseringsprosess for kort og terminaler. Videre anbefaler EPC å utvikle en godkjenningsordning for "Single Euro Payments Area (SEPA) Cards Standardisation Volume Book of Requirements".[10]

For transaksjonsbehandling anbefaler EPC standarden ISO 20022 XML, den samme som SEPA Credit / SEPA Direct Debits benytter. De anbefaler også at det defineres en felles protokoll for autorisasjon og avregning og at det bør utvikles en arkitektur for teknisk interoperabilitet.

Harmoniserte regler, vilkår og spesifikasjoner for betalinger på Internett og på mobil omtales også, og det vises til den pågående standardiseringsprosessen til EPC for betalinger over Internett. Like konkurransevilkår, regelverk og sikkerhetskrav er prioriterte oppgaver det arbeides med. Det er foreslått å benytte ISO 20022 XML for moderne betalingsløsninger (Internett og mobil) og andre løsninger (e-faktura) også. Når det gjelder eksisterende løsninger oppfordres det til interoperabilitet, dvs. utveksling av garanterte betalinger mellom løsningene, basert på åpne standarder som benyttes i SEPA, for eksempel ISO 20022 XML, IBAN og BIC.

For status i implementeringen av alle tre SEPA betalingstyper, se "Seventh SEPA Progress Report".[11]

2.6.2 Skytjenester

Databehandling i skyen skjer ved hjelp av delte IT-ressurser (nettverk, servere, lagring, applikasjoner og tjenester) som tildeles når behovet oppstår. Kunden betaler for bruk, og faste kostnader faller bort. Små foretak (SME) kan dermed få tilgang til IKT av høyere kvalitet enn mange ville klart alene. Skyen og mobile enheter utfyller hverandre. Begrenset lagringskapasitet og funksjonalitet i mobilen blir kompensert ved ubegrenset lagring og funksjonsrikdom i skyen. Mobilen på sin side sørger for et rikt brukergrensesnitt inn mot skytjenestene.

[8] http://www.ecb.int/paym/sepa/pdf/2012-03-23_Eurosystem_reaction_to_EC_Green_Paper.pdf
[9] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:304:0064:0088:EN:PDF
[10] http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=560
[11] http://www.ecb.int/pub/pdf/other/singleeuropaymentsarea201010en.pdf

EU-kommisjonen har utredet potensialet for skytjenester i Europa,[12] og EUs ombudsmann for personvern, European Data Protection Supervisor (EDPS), har uttalt seg om denne.[13] Det blir pekt på utfordringer knyttet til:

- sikring og beskyttelse av personopplysninger
- kontroll og drift i en infrastruktur som endrer seg hele tiden
- ansvar og kontroll i en sky som består av mange leverandører av tjenester
- data som flyttes rundt ofte og som derfor er eksponert

I 2012 ble "Opinion 05/2012 on Cloud Computing"[14] utgitt av det uavhengige EU- rådgivningsorganet Data Protection Working Party. Utfordringer knyttet til ressursdeling og ressursavgrensing, innsyn i skyen, datatransport og lagring utenfor EØS-området er av temaene som blir behandlet.

I 2011 kom standarden "PCI DSS Virtualization Guidelines Information Supplement"[15]. Butikker og tjenesteytere gis veiledning for etterlevelse av PCI/DSS i virtualiserte miljøer. Det pekes på den økte risikoen som hypervisoren[16] introduserer og risiko knyttet til virtuelle IKT-ressurser generelt. I et virtuelt miljø kommer det nye ressurser til fortløpende, og ressurser blir likeledes tatt ut. Kontroll-utfordringene som oppstår i denne forbindelse blir omtalt. I anbefalingen stilles det spørsmål ved om dagens overvåkingsløsninger er tilstrekkelig utviklet til å håndtere utfordringene i virtualiserte miljøer.

2.6.3 Sikkerhet i betalinger på Internett

Det europeiske forumet for sikkerhet i betalinger, Secure Pay, er et frivillig forum som består av tilsyn og overvåkingsorganer. Med utgangspunkt i Seventh SEPA Progress Report, avslutter Secure Pay nå sine anbefalinger og beste praksis når det gjelder sikkerhet i betalingstjenester på Internett der overføring med kredittkort er benyttet[17]. Noen av de viktigste anbefalingene er:

- Foretaket bør ha sentral overvåking og oppfølging av hendelser og sikkerhetsrelaterte kundeklager.
- Foretakene bør fjerne all unødvendig funksjonalitet fra serverne. Logganalyse er påkrevd. Løsninger som er i produksjon bør sikkerhetsvurderes på nytt når nye trusler oppstår. Løsningene bør testes på nytt i lys av nye trusler.
- Transaksjoner skal logges og tidsstemples. Parameterendringer og endringer i loggfiler skal være sporbare.
- Brukersteder bør støtte sterk autentisering hos kortutsteder. Alle betalingsløsninger bør motivere til sterk autentisering ved å overføre ansvaret fra brukerstedet til utsteder. Distribuert programvare (applikasjoner eller applets) bør være digitalt signert.

[12] http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf
[13] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf
[14] Det er i dag enkelt å kopiere bilder, tekst og internettsider. Angripere benytter kopiene og utgir seg for å være originalen.
[15] https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf
[16] Hypervisor er et program som styrer ressursene som inngår i det virtualiserte miljøet.
[17] http://www.ecb.int/pub/pdf/other/recommendationsforthesecurityofinternetpaymentsen.pdf

- Det oppfordres til realtidsovervåking og kontroll, som inkluderer sjekk mot svartelister og sperrelister, samt kontroll av unormal oppførsel. Den som tilbyr tjenesten, Payment Service Provider (PSP), skal oppfordre brukersteder til ikke å oppbevare kortdata, alternativt påse at de blir tilstrekkelig beskyttet. Kortselskapenes egne krav om å beskytte kortdata, de såkalte Payment Card Industry-kravene (PCI), vil også gjelde her. PSP skal tilby en sikker kommunikasjonskanal til kunden, som inkluderer å informere kunden om prosedyren for å rapportere mistenkelige hendelser eller belastninger som ikke er autorisert.
- PSP skal tilby kunden risikoreduserende tiltak og varslingstjeneste. Før oppstart skal PSP og kunden være enige om beløpsgrenser, enkelttransaksjoner og akkumulert, og sperretjenester. PSP bør innføre varsling, eksempelvis via oppringing eller SMS, for svindelutsatte betalinger. Kunden bør kunne sette geografiske begrensninger.

2.6.4 Maskinell verdipapirhandel

Den europeiske verdipapir- og markedstilsynsmyndigheten (ESMA) har publisert "Guidelines on systems and controls in an automated trading environment for trading platforms, investment firms and competent authorities"[18]. Kapasitet, kontinuitet, test, logging og overvåking, sikkerhet, bemanning, styring og kontroll og tilgangskontroll er omtalt i retningslinjene.

Funksjoner for å slette ordre, utestenge medlemmer, hindre at ordreboken "oversvømmes", kontrollere pågangen, stanse handel og rapportere til tilsynsmyndigheter er også omtalt. I tillegg er det eksempler på markedsatferd som indikerer manipulasjon av markedet, og som må overvåkes og rapporteres.

2.7 Felles tiltak fra finansnæringen

Bankene samarbeider løpende om sikkerhet, og arbeidet koordineres av Bankenes Standardiserings-kontor (BSK). Resultater fra hendelser, overvåking, analyser og statistikk utveksles og drøftes, og tiltak besluttes.

Det arbeides med å etablere et FinansCERT (CERT – Computer Emergency Response Team) i Norge, som vil supplere det frivillige samarbeidet som skjer i dag innenfor overvåking og reaksjon når det gjelder elektroniske angrep.

Nets Norway AS (Nets) drifter BankID i en infrastruktur som er felles for bankene. Gjennom Nets videreutviklet bankene i 2012 automatiske kontroller og analyser av BankID-trafikk med tanke på å avdekke angrep på systemet og angrep mot den enkelte bruker. Analysene skjer i realtid, dvs. mens brukeren er pålogget, og hensikten er at uautorisert bruk skal stoppes før pengeoverføringer finner sted.

[18] http://www.esma.europa.eu/system/files/2011-456_0.pdf

3 Systemer for betalingstjenester

3.1 Generelt om betalingssystemer

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

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

Elektroniske betalingstjenester har i praksis overtatt all betalingsformidling. Kun en helt marginal del benytter papirbaserte blanketter. Personkunders bruk av nettbank utgjør 66 prosent, mens bedriftskundenes bruk utgjør 34 prosent av antall transaksjoner i nettbanken. Bedriftskundene står likevel for over 80 prosent av verdiene (beløpet), mens personkundenes andel utgjør nærmere 20 prosent av verdiene.

For kortbetalinger har BankAxept over 90 prosent av privatmarkedet målt i verdi. Norge er i verdenstoppen når det gjelder bruk av betalingskort.

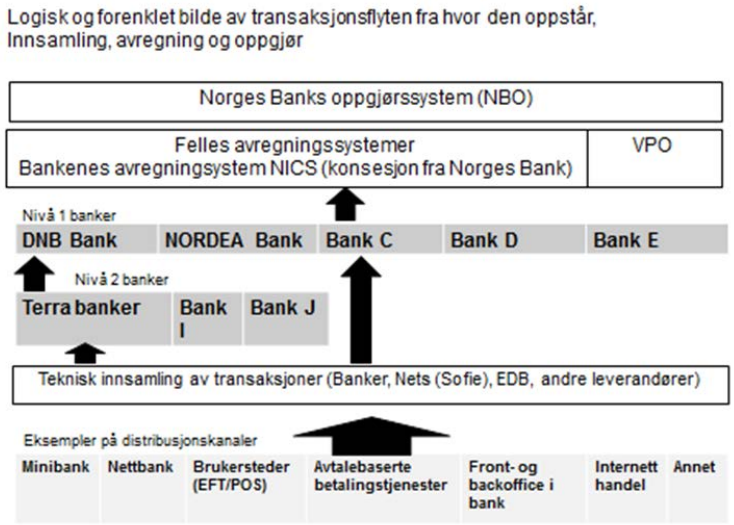
En stor del av den elektroniske infrastrukturen som betalingssystemene anvender er utkontraktert til IKT-leverandører, men foretakenes ansvar for operasjonen er den samme.

I Norges Banks *Årsrapport om betalingssystem 2012* er det mer informasjon og statistiske data om dette feltet.

Figuren nedenfor gir en oversikt over transaksjonsflyten i betalingssystemet. Nederst i figuren er det gitt en illustrasjon av ulike betalingstjenester initiert av kundene. Oppgjøret for handel med finansielle instrumenter skjer i verdipapiroppgjøret (VPO), angitt nest øverst i figuren. VPO omfatter overføring

av verdipapirer mellom kontoer i verdipapirregisteret og overføring av penger mellom kjøper og selger. VPO sørger for at finansielle instrumenter ikke overføres med mindre betalingen skjer, og omvendt.

Figur 2: Transaksjonsflyt



Kilde: Finanstilsynet

3.2 Styring og kontroll med betalingssystemene

Betalingssystemene utgjør et grunnleggende tjenesteområde i bankene, og er i dag nesten utelukkende basert på digitale løsninger. Bedriftskundene er knyttet opp til bankene elektronisk, og informasjon fra banken benyttes direkte i bedriftens egne systemer. Effektiv likviditetsstyring krever at betalings- og kontosystemene fungerer og er tilgjengelige. Et samordnet betalingssystem, slik det er i Norge, forutsetter bruk av felles infrastruktur som understøtter betalingstjenestene og gir "sømløse" tjenester overfor kundene. Bankene utvikler egne separate løsninger som bygger på infrastrukturen og fellesløsningene. Dette gjør det mulig å foreta betaling, avregning og oppgjør i en integrert handling mellom betaler i Bank A og mottaker i Bank B. Dette gjelder også om mottaker og Bank B er utenfor Norge.

Foretakene kan stå overfor vanskelige avveininger i den løpende virksomheten for betalingssystemene. Systemene må vedlikeholdes samtidig som nye tjenester blir utviklet på ny teknologi. De nye tjenestene skal integreres i det eksisterende tjenestetilbudet. Tjenestene skal samtidig være enkle å bruke, og de skal være sikre. Systemene må også være robuste mot stadig mer avanserte kriminelle angrep.

Avregning, oppgjør og løsninger som understøtter internasjonale betalinger har vært relativt stabile i drift og er foreløpig lite eksponert for kriminelle angrep. Det er først og fremst betalingstjenestene ut til kunden som er utsatt for kriminelle angrep og alvorlige hendelser.

Det er viktig å sikre at alle elementer og aktører i transaksjonskjeden mellom betaler og betalingsmottaker inngår i styringen av operasjonell risiko. Det er også viktig å sikre nødvendig kompetanse og tid til å kunne styre og kontrollere driften i egne operasjoner hos IT-leverandører og eventuelle underleverandører.

Det er en utfordring for enkelte finansinstitusjoner å ha tilstrekkelig kontroll med dette. Det er nødvendig å etablere et rammeverk for styring og kontroll med virksomheten og med fastlagte prosedyrer for viktige funksjoner. Det må etableres kontrollordninger som sikrer etterlevelse av regelverk og av fastlagt kvalitetsnivå. Gjennomføring av regelmessige risikoanalyser er nødvendig for å sikre tiltak mot kriminelle angrep og for å unngå alvorlige hendelser. Etablering og øving på beredskapsopplegget er også nødvendig for å være i stand til effektiv håndtering når hendelser likevel skjer. Det er et ledelsesansvar å sørge for at dette er på plass.

I lov om betalingssystemer stilles det krav til at det uten unødig opphold skal gis melding til Finanstilsynet om etablering og drift av betalingstjenester. I 2012 kom det fem meldinger til Finanstilsynet, to dreide seg om SWIFT, én om installasjon av BankID, én om BankID på mobil og én om kortløsning med RFID-teknologi.

Hovedhensikten med meldeplikten er å sikre at nødvendige risikovurderinger er gjort og at eventuelle avtaler mellom aktuelle parter er etablert før en ny betalingstjeneste tas i bruk. Det er grunn til å anta at det er en underrapportering om endringer av systemer for betalingstjenester, og tilsynet vil vurdere nærmere tiltak for å sikre at meldeplikten blir overholdt.

3.3 Risiko og sårbarhet i betalingssystemene

3.3.1 BankID

BankID blir i stadig større grad brukt av betalingstjenestene og har derfor blitt stadig viktigere. Bank ID benyttes til autentisering og elektronisk signering av transaksjoner, og er i hovedsak basert på utviklingsverktøyet Java. I 2012 var det tilfeller hvor nye Java-oppdateringer førte at det oppsto sikkerhetshull i Javakoden. Som følge av dette har BankID begynt å se etter mulige alternativer til den Java-baserte løsningen slik at hver enkelt bruker av den banklagrede BankID ikke trenger å laste ned Java for å benytte seg av BankID.

BankID har allerede i dag et alternativ til den Javabaserte løsningen: BankID på mobil. Brukerens BankID er lagret i mobilens SIM-kort. DNB, Skandiabanken, Terra-bankene og SpareBank 1 tilbyr

dette i samarbeid med Telenor, Djuice, Talkmore, Hello Norway eller Phonero. Det er lagt opp til at flere banker og mobilleverandører etter hvert vil tilby denne løsningen.

Direktoratet for forvaltning og IKT (Difi) inngikk i november 2012 kontrakt med BankID om levering av elektronisk ID på høyt sikkerhetsnivå til offentlige digitale tjenester. Det at BankID-løsningen også blir benyttet utenfor den finansielle infrastrukturen, både av offentlig forvaltning og av private foretak utenfor finanssektoren, kan innebære en risiko. De nye brukerstedene vil ikke nødvendigvis ha samme krav til sikkerhet og risikostyring som foretak innenfor finanssektoren har.

3.3.2 Ondsinnet kode

Bruk av phishing som metode for tyveri av data har blitt en svært vanlig angrepsform for ulovlig innsamling av data. Dataene blir benyttet til misbruk, f.eks. gjennom handel på nettet med bruk av betalingskort. Denne bruken av betalingskort blir betegnet som "card-not-present"-transaksjoner. Misbruket skjer ofte gjennom betaling ved kjøp av varer i nettbutikker, særlig i butikker som ikke stiller krav til sikkerhetsløsninger som BankID eller 3D-Secure. Trojanere blir stadig mer sofistikerte og dermed vanskeligere å oppdage av tradisjonell antivirus-programvare. Trojanerne kan spres på flere måter, men de to mest vanlige er ved at den ondsinnede koden ligger som et vedlegg til en e-post eller at den ondsinnede koden legges i en annonse eller lenke, f.eks. i en nettavis eller en søkemotor. Dersom leverandørene av søkemotorer ikke har gode løsninger for å avdekke lenker som inneholder ondsinnet kode, kan en infisert lenke legges på topp av resultatlisten ved søk på de mest populære søkebegrepene. Når PC-er blir infisert med trojanerkode, kan denne koden benyttes til svindelforsøk. Dette gjelder særlig svindel i nettbankløsninger når PC-eieren benytter den til nettbanktjenester.

3.3.3 Angrep på EFTPOS og minibanker

Både minibanker og EFTPOS-terminaler er sårbare for skimming. Minibankene er for det første mål for såkalt cash trapping, som vil si å avlure kunden pengesedlene. Nye kreative løsninger observeres. Både limlister på pengemateren og gaffellignende gjenstander som kiles inn i pengemateren blir benyttet til å ta pengene. Dernest er både EFTPOS-terminaler og minibanker mål for ekte skimming med avlesing av informasjon i magnetstripa.

Så langt er det ikke meldt om vellykket kompromittering av chip-en i bankkortene. Det er imidlertid observert aktivitet i form av såkalt chip-shimming der et elektronisk kretskort monteres inn i chip-leseren i forsøk på å avlese informasjonen som skjer mellom chip-en og mottakeren.

3.3.4 Mobile løsninger

Bruken av mobile løsninger økte betydelig i 2012, og den vil med stor sannsynlighet også øke i de neste årene. Løsningene er brukervennlige, og det introduseres stadig nye funksjoner. De mobile løsningene er ofte delt inn i to sikkerhetsnivåer. Eget passord er ofte tilstrekkelig for å kunne se saldo og overføre mellom egne kontoer. Dersom en skal gjennomføre regningsbetaling, må en også skrive inn engangskode i tillegg til passord.

Det er to typer operativsystemer som er markedsledere innenfor smarttelefoner: Googles Android og

Apples IOS. Det er kjent at operativsystemet fra Apple har en høyere grad av sikkerhet og at sikkerhetstiltakene som Apple har for at en utvikler skal kunne legge inn en app i Apples App Store er sikrere enn løsningene Google har for Google Play. Dette fører til at smarttelefoner med Android operativsystem som laster ned app-er fra Google Play har en langt svakere sikkerhet. Muligheten for at telefonen får ondsinnet kode ved nedlasting av app-er er derfor større enn ved Apples løsninger.

Norske banker har satt i gang pilotprosjekter hvor kredittkort har innebygget RFID-funksjonalitet.[19] RFID-funksjonaliteten er en relativt godt utprøvd teknologi som bl.a. benyttes i adgangskort. Når kortet holdes inntil terminalen, overføres betalingsinformasjon mellom kredittkort og terminal.
[Avsnittet er korrigert 10.4.2013, red.merkn.]

Parallelt med dette pågår det pilotprosjekter med Near Field Communication-teknologi (NFC). Den har tilsvarende funksjonalitet som RFID, men benyttes i smarttelefoner. I et samspill mellom NFC og SIM-kort med en betalingsapplikasjon kan en betalingsterminal som kan lese RFID også lese NFC-signaler og gjennomføre en betalingstransaksjon.

Begge teknologier kan innebære følgende risikoer:

- Informasjon mellom kort/telefon og leser kan fanges opp, og sensitiv informasjon om kortet kan lagres og misbrukes ved f.eks. kloning av kort.
- Informasjon mellom kort/telefon og leser kan fanges opp, endres og sendes videre for prosessering.

Denne siste risikoen gjelder særlig for smarttelefoner som benytter seg av operativsystemet Android. Selv om det så langt har vært få hendelser med virus på mobiltelefoner, er det antatt at dette vil øke i omfang. NFC-teknologien gir brukerne muligheter til å lagre bankinformasjon om konto og kort på smarttelefonene.

Med tanke på økningen i bruken av mobiltelefonen som betalingskanal, er det viktig at bankene stiller samme krav til sikkerhet for mobile løsninger som det er for tradisjonelle nettbankløsninger. De mobile løsningene er i stadig større utstrekning utsatt for de samme farene som tradisjonelle nettbanker er. Det er derfor viktig at løsningene, som f.eks. bruken av SSL-sertifikater, har den samme sterke krypteringen på mobile løsninger som på arbeidsstasjoner.

3.3.5 Konsentrasjonsrisiko

Flere finansielle tjenester er koblet sammen og deler tekniske ressurser. Feil på en av tjenestene kan føre til at en eller flere av de andre tjenestene også svikter.

Nets utfører tjenester for bankene som kan betegnes som navet i infrastrukturen for betalingstjenester. Betalingstjenester som BankAxept, BankID og avregningssystemet NICS[20] er løsninger som alle blir

[19] RFID – Radio Frequency Identification
[20] NICS – Norwegian Interbank Clearing System

forvaltet og driftet av Nets. BankAxept-kortet er det mest brukte kortet i Norge, og hver måned i 2012 ble dette kortet benyttet til betaling av varer og tjenester for gjennomsnittlig over 40 milliarder kroner. I overkant av 8 av 10 kortbetalinger i Norge er med BankAxept, i følge www.bankaxept.no. I Norges Banks årsrapport for betalingssystemer 2011 står det at kontantandelen av betalingsmiddel disponert av publikum utgjorde ca. seks prosent, noe som er en halvering på de siste ti årene.

De fleste bankene har større eller mindre oppgaver som IT-leverandøren Evry ASA (Evry) utfører. Dette innebærer at om en tjeneste blir utilgjengelig, så rammes ofte flere enn én bank. En av tjenestene hvor flere banker benytter seg av samme løsning, er motoren i regningsbetalingen RBS (RegningsBetalingsSystem). Det er en forutsetning at denne funksjonen fungerer for at bankkunder skal kunne utføre regningsbetalinger. Et annet eksempel er verifisering av PIN. Denne typen konsentrasjonsrisiko gjør at Evry legger stor vekt på kontinuitets- og katastrofeplaner. Også i 2012 hadde noen av IT-tjenestene som Evry leverer til finanssektoren alvorlige feil og/eller mangler som førte til utilgjengelige tjenester for banker og bankkunder.

3.4 Oversikt over tap knyttet til betalingstjenester

3.4.1 Tapstall i Norge

Nedenfor er det gjengitt tapstall i Norge for henholdsvis kort- og nettbanksvindel for de to siste årene. Tallene er innhentet av FNO og Bankenes Standardiseringskontor (BSK) i samarbeid med Finanstilsynet.

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

Svindeltype betalingskort	**2011**	**2012**
Misbruk av kortinformasjon, kort ikke til stede (internetthandel)	24 190	35 701
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort i Norge	468	2 308
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort utenfor Norge	57 340	55 869
Originalkort tapt eller stjålet, misbrukt med PIN i Norge	32 224	28 128
Originalkort tapt eller stjålet, misbrukt med PIN utenfor Norge	7 008	8 544
Originalkort tapt eller stjålet, misbrukt uten PIN	4 488	4 603
TOTALT	**125 718**	**135 153**

Kilde: Finanstilsynet

Tapene på kortområdet økte i 2012. Dette skyldes først og fremst økning i svindel av typen card-not-present (CNP). Dette er handel med bruk av kortdata på Internett (hovedsakelig), telefon eller e-post. Av det totale transaksjonsbeløpet for korttransaksjoner i Norge i 2012 utgjorde svindel omkring 0,017 prosent. Dette er relativt sett noe lavere enn ellers i Europa. Tendensen med økning i svindel av typen

CNP er på linje med resten av Europa.

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

Svindeltype nettbank	2011	2012
Angrep ved bruk av ondartet programkode på kundens PC (trojaner)	664	5 064
Angrep som utnytter sårbarheter i nettbankapplikasjon (hacking)	0	0
Tapt/stålet sikkerhetsmekanisme	3 321	3 367
TOTALT	**3 985**	**8 431**

Kilde: Finanstilsynet

Tapstallene for nettbank økte i 2012 grunnet økning i angrep fra internasjonal kriminalitet med bruk av trojanere. Tallene er likevel beløpsmessig fortsatt lave. For å få et reelt bilde av svindelnivået, rapporterte bankene fra andre halvår i 2012, i tillegg til tap, også på to andre parametere:

- Antall kunder der banken har oppdaget at kundens datamaskin er infisert med en aktiv nettbanktrojaner.
- Svindeltransaksjoner som er registrert i nettbanken med et gyldig kontonummer og et beløp, men avverget før de ble gjennomført.

Tallene som bankene rapporterte på disse to parameterne indikerer at de potensielle tapene er vesentlig høyere.

Mens Norge hadde en betydelig økning i antall angrep i 2012 på linje med land som Belgia og Nederland, er det andre land, blant annet Storbritannia, som opplever en reduksjon i antall angrep.

3.4.2 Tapstall i andre europeiske land

Her knyttes noen kommentarer til tapstallene ellers i Europa. Informasjonen er hentet fra rapporter fra European ATM Security Team (EAST)[21], Financial Fraud Action UK[22], Observatorie de la Securite des Cartes de Paiement[23] i Frankrike og den europeiske sentralbanken (ECB)[24].

Tap på kortområdet har sunket i de fleste europeiske landene etter innføring av chip. Storbritannia er typisk for denne utviklingen. Der har det vært en jevn nedgang i tapene siden 2008. Av totalt transaksjonsbeløp utgjorde svindel 0,061 prosent av beløpet i 2011. Tap med falske kort synker mest. Tap av typen CNP har økt for hvert år i prosent i forhold til totaltapet.

[21] https://www.european-atm-security.eu/Press%20and%20Media/
[22] Financial Fraud Action UK – Fraud The Facts 2012: http://www.financialfraudaction.org.uk/downloads.asp?genre=consumer
[23] Rapport for 2011: http://www.banque-france.fr/observatoire/rap_act_fr_11.htm
[24] European Central Bank (ECB) – Report on card fraud July 2012: http://www.ecb.int/pub/pdf/other/cardfraudreport201207en.pdf

Innføring av chip og pin har ført til at svindel med bruk av falske kort har avtatt i hele Europa. Færre og færre land tillater bruk av magnetstripe. Når det i tillegg brukes regionsperre på kort slik at disse eksempelvis ikke kan brukes i USA eller Mellom-Amerika, reduseres tapene ytterligere. Enkelte land har innført streng regulering av regionsperre. Et eksempel er Belgia, som har innført pliktig bruk av regionsperre. Dette har redusert tap med bruk av falske kort med over 95 prosent.

Sammen med oppdatert anti-skimming-utstyr, har regionsperre også ført til stor nedgang i skimming av minibanker.

Tap av type CNP avtar minst. Det er betalinger gjennom e-post, telefon og Internett. Verken kort eller kortbruker er til stede i det svindelen skjer, og det kan være vanskelig å kartlegge. Tiltak er passordbeskyttelse som "Verified by VISA", overvåking og verifisering av fakturaadresse.

Det har vært en økning i antall tyveri av originalkort og misbruk av disse. Dette kan ha sammenheng med at det har blitt dårligere fortjeneste i å lage falske kort.

Tap på nettbank varierer mye fra land til land. I 2012 var det en stor økning i Belgia[25] og i Nederland[26]. I Storbritannia har det vært nedgang de siste årene. Størrelsen på tapene er ikke uten videre et bilde på intensiteten i angrepene. Innsats på tiltakssiden kompenserer for størrelsen på tapstallene, jf. tapstallene for Norge i 2012.

[25] http://www.febelfin.be/nl/veilig-internetbankieren-enkele-tips
[26] http://www.nvb.nl/veelgestelde-vragen/1351/hoe-hoog-is-de-schade-door-fraude-met-internetbankieren.html

4 Funn og observasjoner

Finanstilsynets observasjoner er basert på gjennomføring av IT-tilsyn, rapportering av hendelser, ROS-intervju i slutten av året (se 4.2, side 26), møter med foretak og leverandører og spesielle prosjekter. I tillegg har en viktig informasjonskilde vært bankenes svar på Finanstilsynets rundskriv 20/2011 etter driftsavbruddet i påsken i 2011.

4.1 Noen funn fra IT-tilsyn i 2012

I 2012 valgte Finanstilsynet å gjøre tematilsyn på utvalgte områder av IKT-virksomheten i finansforetakene, noe som førte til færre, men mer omfattende tilsyn. De utvalgte temaene var katastrofe- og beredskapsopplegg, elektroniske betalingstjenester, samt styring og kontroll med IKT-infrastruktur.

4.1.1 Kontinuitets- og katastrofeløsninger

Kontinuitets- og katastrofeløsninger krever et nært samarbeid mellom foretaket og tjenesteytere som forvalter og/eller drifter systemene. Løsningene skal dekke ulike scenarier hvor flere ledd kan være rammet samtidig. Grundige risikovurderinger og planlegging av tiltak er nødvendig.

For å gjennomføre ende-til-ende-tester av kontinuitets- og katastrofeløsninger kreves det felles tester/øvelser mellom foretak og leverandører. Disse forholdene må reguleres i utkontrakteringsavtalene. Det kan bli kostbart å få dette på plass i ettertid, og det kan gi insentiv til utsettelse/nedprioritering.

Foretakene viser ofte til test av kontinuitetsløsninger på enkeltsystemer og katastrofescenarier som rammer lokalt på foretakenes hovedkontor. Det ser ut til at når utkontrakteringsveien blir lang, overlates katastrofescenariene stilltiende til tjenesteyterne. Foretakene viser manglende engasjement i denne sammenheng. Testingen blir gjort enkeltvis av hvert enkelt ledd i kjeden, og da for scenarier som rammer lokalt, uten en tilfredsstillende test som rommer samhandlingsaspektet.

Stedlige tilsyn har også avdekket manglende dokumentasjon av forutsetninger og avhengigheter mellom systemene. Dette gjør det vanskelig å prioritere i en kritisk situasjon.

Det er finansforetakenes ansvar å sikre at løsninger og tester er tilfredsstillende, og at også opplæring blir ivaretatt. Enkelte foretak har ikke opplæringsaktiviteter utenom den tekniske testen.

4.1.2 Økende risiko ved gamle og komplekse kjerneløsninger

De fleste bankene benytter kjernesystemer som er gamle, og de benytter ofte teknologi som ikke så enkelt kan tilpasses dagens krav til kommunikasjon og drift/vedlikehold. Nye funksjonsområder og systemer er kommet til, og er koblet til kjernesystemene på ulike måter. Nye brukergrensesnitt er utviklet med ny teknologi og lagt på utsiden. Banksystemene er derfor blitt meget komplekse og til dels uoversiktlige. Det kan lett oppstå feil når akutte problemer skal løses under stort tidspress.

Denne utviklingen har flere årsaker. Bankene er ofte organisert etter kundesegmenter, og utvikling av systemer er delt tilsvarende. Helhetsløsningene blir ikke prioritert i tilstrekkelig grad. For mange banker, særlig de mindre, er det lang vei gjennom utkontrakteringer til tjenesteyter. Avstanden mellom systemene og de ansvarlige i bankene er stor, og oppmerksomheten blir konsentrert om drift og kostnader, samt nye funksjoner. Modernisering av systemer og teknologi får dermed liten oppmerksomhet i styrende og bevilgende organer og kommer ofte ikke opp i prioritering.

Flere banker vurderer nå risikoen ved de gamle og komplekse kjernesystemene som økende, samtidig som det for noen er vanskelig å rekruttere personell med kompetanse på den anvendte teknologien. Det er en økende erkjennelse av at man nå står foran store investeringer for å fornye og rasjonalisere kjernesystemene.

4.1.3 Oppfølging av identifiserte risikoer

Ved stedlige tilsyn er det avdekket at oppfølgingen av allerede identifiserte risikoer og sårbarheter ikke er god nok. Foretaket gjør i første omgang en tilfredsstillende jobb med risikovurderinger, analyse av hendelser for å avdekke årsaker og hindre gjentakelse og test av kontinuitets- og katastrofeløsninger. Dette resulterer i definerte tiltak og tiltaksplaner.

Ofte blir definerte aktiviteter for å avhjelpe identifiserte risikoer utsatt. Utsettelsen kan skyldes tekniske vanskeligheter, kostnadsmessige vurderinger, problemer med leverandører, tidspress, frysperioder m.m. Det viser seg at slik utsettelse kan bety pulverisering og uklarhet rundt hvem som har ansvar for å iverksette tiltakene. Tiltak kan bli strøket eller glemt. En del alvorlige hendelser de siste årene er forårsaket av svikt i komponenter det allerede er identifisert en sårbarhet ved. Rapportering og oppfølging av slike forhold må derfor forbedres.

4.1.4 Endringer hos leverandør

Ved utkontraktering vurderer ofte tjenesteyter enkelte endringer som "sine", fordi de er nødvendige å gjennomføre teknisk. Endringer innenfor slike områder blir derfor ikke alltid varslet til foretakene, slik at de kan vurdere påvirkning på egne kritiske systemer. Foretakene er derfor ikke forberedt på at problemer kan oppstå, og eventuell konflikt med andre aktiviteter lokalt. Finanstilsynet konstaterer at dette likevel bedret seg i 2012.

4.2 Foretakenes egne vurderinger

For å få informasjon om hvordan finansforetakene vurderer sin IKT-risiko hadde Finanstilsynet i 2012 samtaler med 13 utvalgte foretak av ulik type og størrelse. Temaene var foretakenes erfarte problemer og utfordringer i 2012 og hva de vurderer å være de største risikoene i 2013. I tillegg ba Finanstilsynet om oversikt over foretakenes bruk av skytjenester (cloud computing).

Foretakene mener dette var de største problemområdene i 2012:

- *Eksterne angrep*
  Tilnærmet alle foretak rapporterer at eksterne angrep, som trojanerangrep, hacker-angrep og DDoS. Dette var en stor utfordring i 2012. For bankene har slike angrep i stor grad vært svindelforsøk mot nettbanken. Angrep eller angrepsforsøk økte betraktelig i 2012. Angrepene endrer seg raskt, og krever stor oppmerksomhet og beredskap fra foretakenes side.

- *Driftsavbrudd eller ustabil drift*
  Mange av foretakene har erfart at driftsavbrudd og ustabil eller treg drift, som skyldes feilhåndtering eller feil grunnet kompleksitet i infrastruktur og nettverk, har vært et problem. Foretakene synes i stor grad å mene at dette skyldes forhold hos leverandøren.

- *Utkontraktert virksomhet*
  Mange foretak har gitt uttrykk for at det er utfordringer med utkontraktert virksomhet, også utover driftsproblemene nevnt over. Foretak har opplevd mangelfull overholdelse av tjenestenivåavtaler (SLA-avtaler), svak leveranseevne og samarbeid med leverandøren som et problem. Noen foretak som har satt ut systemutvikling til India (offshoring), har blant annet erfart mangelfull kompetanse hos leverandøren og mangelfull leveransekvalitet.

- *Endringshåndtering*
  Generelt gis det inntrykk av at endringshåndtering er et gjennomgående forbedringsområde. Dette gjelder både driftsendringer og applikasjonsendringer utført av foretaket selv og av leverandøren. De fleste feil skjer i forbindelse med en endring.

Risikoområder i 2013:
Foretakene vurderer at områdene som forårsaket flest problemer i 2012, også utgjør de største risikoene i 2013, på tross av iverksatte tiltak:

- *eksterne angrep*
- *driftsavbrudd og ustabil drift*
- *utkontraktert virksomhet*
- *endringshåndtering*

Flere foretak nevner også følgende risikoer:

- *Nye plattformer og ny teknologi*
  I denne sammenheng er det spesielt nevnt at risikobildet ved bruk av mobiltelefoner/ smarttelefoner antas ikke å være tilstrekkelig kjent.

- *Kompetanse- og ressurssituasjonen*
  Dette gjelder spesielt kompetanse- og ressurssituasjonen på eldre systemer og teknologi, som etter hvert få personer har kompetanse på, og som ikke er attraktive for nyutdannede.

- *Mangelfulle katastrofeplaner og verifisering gjennom testing*
  Noen foretak påpeker risikoen for at krisesituasjoner ikke blir håndtert tilfredsstillende fordi katastrofeplaner og/eller testing av disse er utilstrekkelig.

Bruk av skytjenester (cloud computing)
Noen foretak har tatt i bruk skytjenester på et begrenset område, som for eksempel i forbindelse med rekruttering og medarbeidersamtaler, men har ingen planer om å ta det i bruk utover dette. Øvrige foretak har ikke tatt i bruk slike tjenester, og har heller ikke noen planer om det. Flere av foretakene vurderer risikoen i forbindelse med skytjenester som uavklart og/eller for stor.

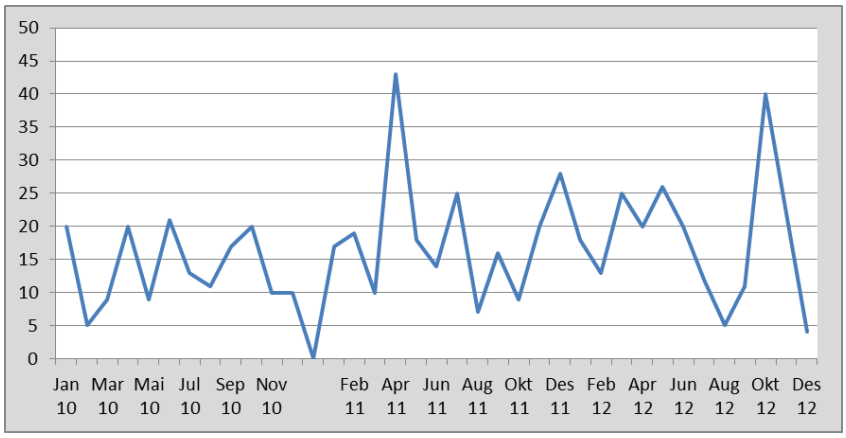
4.3 Rapporterte hendelser i 2012

Antall rapporterte hendelser i 2012 var omtrent på samme nivå som i 2011. Det var en økning i ondsinnede angrep. Dette gjelder både trojanerangrep og DDoS-angrep. Det var også en økning i angrep mot minibanker.

Det var også enkelte alvorlige driftshendelser i 2012.

I september var det en alvorlig hendelse i VPS knyttet til en feilregistrering som førte til utilsiktet sletting av data.

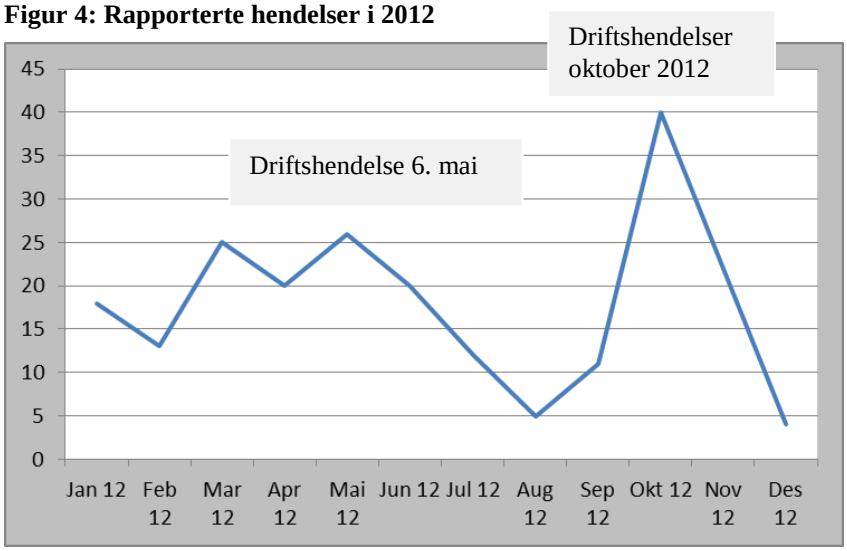
Figur 3: Antall rapporterte hendelser i perioden 2010–2012



2010: 156 hendelser
2011: 221 hendelser
2012: 216 hendelser

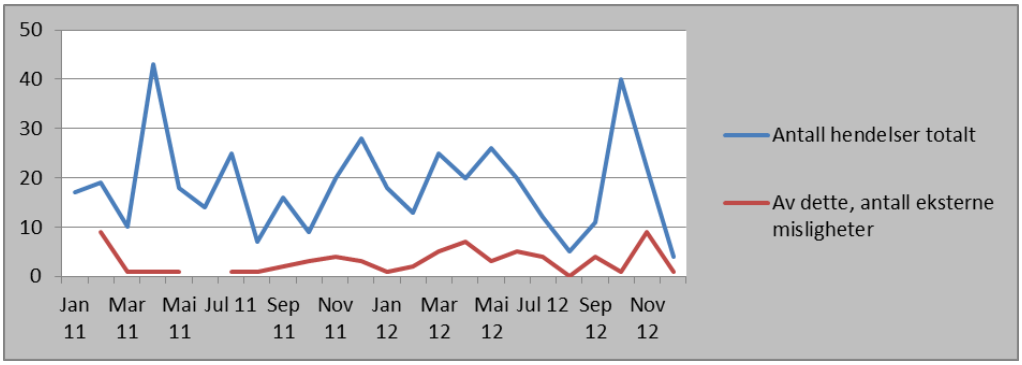
Kilde: Finanstilsynet

Figur 4: Rapporterte hendelser i 2012



Kilde: Finanstilsynet

Figur 5: Antall rapporterte ondsinnede angrep i perioden 2011–2012



Kilde: Finanstilsynet

4.3.1 Trojanerangrep

Bankene rapporterte om trojanerangrep gjennom hele 2012, med angrep fra ulike typer trojanere. Det startet med varianter av Zeus og SpyEye, fortsatte med Ice IX og Torpig. Sistnevnte har vært spesielt utfordrende å håndtere. Den er uforutsigbar, kartlegger før den angriper, er vanskelig å oppdage og gjenskape, framtrer for kunden på ulike måter og endrer seg i takt med mottiltakene som iverksettes. Mange kunder har fått sine PC-er infisert. Blant annet var en stor bølge med phishing-e-post som utga seg for å være sendt fra DNB en kilde til infeksjon. Tapene er likevel lave som følge av stor innsats fra bankene og felles samarbeidspartnere som BSK og NorCERT.

Fortsatt er de fleste kontonumre som transaksjonene skal overføres til utenfor Norge, men det er også aktiv rekruttering av norske kontoholdere ("mules") til å stille sin konto til disposisjon. Rekrutteringen er fordekt som en ordinær ansettelse i et mindre finansforetak som utfører betalinger og hvor den ansatte honoreres med en viss prosent av omsetningen. På denne måten rekrutteres personer i Norge, kanskje mer eller mindre intetanende, til det man kaller "money mules", og dermed reell helerivirksomhet ved å stille sin konto til rådighet for kriminalitet.

Figur 6: Utdrag av rekrutteringsbrev til "Betaling instituttagent"("money mule")

BETALING INSTITUTT AGENT

Vi søker etter folk til å behandle betalinger som kommer fra våre kunder. Selskapet vil gi agenten detaljerte instruksjoner som er relevante for betalingsprosessen, inkludert fullt navn på avsender og summen i hvert enkelt tilfelle.

Når midlene er mottatt på ansattes bankkonto er det finansagentens plikt å ta ut penger og overføre midlene via internasjonal bankoverføring eller ved å bruke internasjonal WesternUnion/Money Gram pengeoverføringssystem.

LØNN

I prøvetiden tilbyr vi 2000 EUR i månedslønn pluss 5% provisjon for hver betalingsbehandling.

Figur 7:
Figuren viser del av "ansettelseskontrakt" som "Betaling instituttagent". Dette tilsvarer "money mule" der personen blir bedt om å fylle ut informasjon om sin bankkonto. Språket er relativt godt, men "ansettelseskontrakten" har skrivefeil og framstår som uprofesjonell ved nøyere gjennomlesing.

4. SKJEMA FOR ANSATTINFORMASJON
Fyll ut skjemaet under

For- og etternavn:_____

Fasttelefon:_____

Mobiltelefon:_____

Adresse:_____

Betaling

For å kunne motta innbetalinger fra kunder, og lønnen din, oppgi følgende kontoinformasjon:

Kontoinnehaver:_____

Bankens navn:_____

Avdeling:_____

Avdelingens adresse:_____

Bankens daglige uttaksgrense _____

Kontonummer:_____

IBAN:_____

BIC/SWIFT:_____

*Du er ansvarlig for reliabiliteten i denne informasjonen. Hvis det skulle oppstå problemer, kontakt banken din.

Selskapet vil ikke røpe dine opplysninger og vil kun betale avtalte beløpt til kontoen på de klokkeslett og datoer som spesifiseres før hver transaksjon. Den ansatte vil ikke forsøke å bruke noen av selskapets midler - andre enn dem som sette inn i forbindelse med ansettelsen som avtalt godtgjørelse, og provisjoner.

Avtale om prøveperiode Side 7 av 8

4.3.2 DDoS-angrep

Fra å være et tilnærmet ikke-eksisterende fenomen i Norge, økte DDoS-angrep mot finansforetak betydelig i 2012. De største bankene, Oslo Børs og IKT-leverandører ble angrepet. Mest alvorlig var DDoS-angrepet mot Oslo Børs i juni 2012. Tilgangen til Oslo Børs' internettsider var redusert i en uke som følge av et angrep med varierende styrke. De siste årene har det blitt utviklet effektive tiltak mot DDoS-angrep. Falsk pakke-trafikk kan gjenkjennes og filtreres både i nettverket hos ISP-ene og hos foretakenes egne tiltak. DDoS-angrepene har derfor i liten grad påvirket kundetjenestene eller driften.

4.3.3 Driftshendelser

Antall driftshendelser var på samme nivå i 2012 som i 2011. Etter en del hendelser i mars og en større hendelse i mai 2012, var det få alvorlige hendelser før oktober og ut året da det var flere hendelser. Det var ingen enkelthendelse som i alvorlighet kan måle seg med "påskehendelsen 2011", men det var en rekke hendelser som rammet mange banker samtidig. Årsaken til disse var flere ulike feil i komponenter i felles sentral infrastruktur hos Evry.

Etter påskehendelsen i 2011, iverksatte Evry "snu-hver-stein"-programmet, som kartla sårbarheter i betalingskanalene. I løpet av 2012 utvidet Evry programmet til å omfatte felles sentral infrastruktur i form av nettverk, server- og "mainframe"-miljø.

4.3.4 Angrep på minibanker

Til tross for at det har blitt vanskeligere å bruke kort med magnetstripe, er det fortsatt betydelige tap knyttet til bruk av falske kort i Norge. I 2012 var det en økning i angrep på minibankene i Norge. Det brukes flere metoder:

- Sosial manipulering, ofte av eldre personer. Mens korteieren benytter minibanken, blir han/hun avledet, og den kriminelle napper ut kortet uten at korteieren oppdager det.
- "Cash trap": Pengene limer seg fast på en innretning som er påmontert pengemateren.
- Ekte skimming der det ikke er oppgradert anti-skimming-løsning på minibanken.

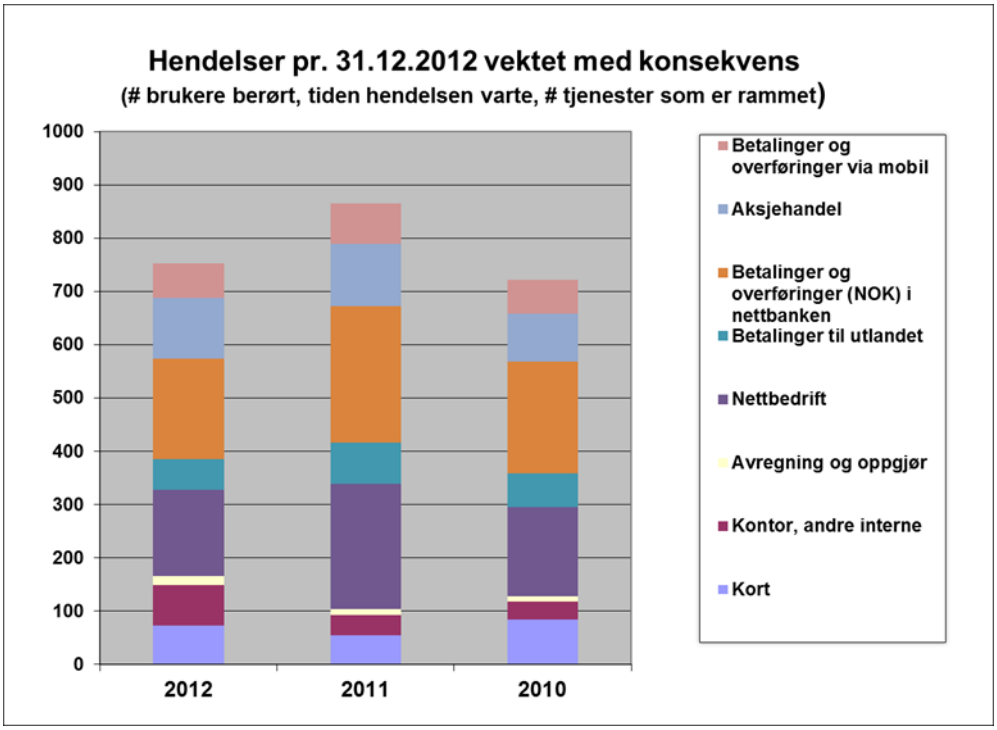
Bankene oppdaterer fortløpende anti-skimming-utstyr på minibankene.

4.3.5 Analyse av hendelsene

Finanstilsynet mottar ofte rapporter fra flere banker om samme hendelse når hendelsen har skjedd hos felles leverandør. Likevel er det ikke slik at alle banker rammes på samme måte, verken når det gjelder type tjenester eller varigheten av avbruddet.

Med dette som utgangspunkt har Finanstilsynet analysert hendelsene i 2012. Omfanget av hendelsene er vurdert ut fra antall brukere som er rammet og hvor lenge avbruddet varte. Skaden er vurdert for hver hendelse etter identiske kriterier. Hendelsene kan derfor summeres for hvert år og for hver tjeneste og sammenlignes over tid. Verdien på den vertikale aksen i figur 9 under er uttrykk for en veiet og summert vurdering av hendelsenes skadeomfang. Indeksen gir uttrykk for utilgjengeligheten av banktjenester.

Figur 8: Hendelser vektet med konsekvens



4.4 Resultater fra gjennomførte prosjekter

4.4.1 Kritiske komponenter på IKT-området

Etter problemene i kortsystemene påsken 2011, ba Finanstilsynet bankene dokumentere kritiske komponenter i IKT-infrastrukturen, og beskrive oppfølging av leverandørenes endringshåndtering og beredskap. Se Finanstilsynets rundskriv 20/2011 "Økte krav til bankene i lys av driftsproblemene i påsken 2011".

Bankene og leverandørene har utarbeidet relativt detaljerte beskrivelser av de kritiske komponentene, og i større eller mindre grad gjort en sårbarhetsanalyse av dem. Tiltak er iverksatt der sårbarheten er funnet for høy. Evry har iverksatt det såkalte "snu-hver-stein"-programmet som blant annet har til hensikt å bedre kvaliteten.

Tradisjonelt har vedlikehold, feilretting og oppgraderinger av systemene i noen grad vært overlatt til leverandørene. Flere banker har nå fått installert eget endringshåndteringssystem som formaliserer samhandlingen med leverandør når det gjelder endringer.

Samordnet beredskap er konkret styrket ved at det etter initiativ fra Finans Norge er opprettet en samhandlingsrutine ved feil og hendelser i BankAxepts verdikjede. Samhandlingsrutinen omfatter alle leverandørene og bankene. I tillegg har Nets og Evry inngått en ny bilateral avtale om samhandling. Flere banker varsler at de nå vil ha felles øvelser med sine leverandører.

De fleste bankene bekrefter eksplisitt sitt ansvar for systemporteføljen og at de heretter vil følge leverandørens arbeid tettere.

4.5 Risikoområder identifisert av andre

4.5.1 Mobilnettets betydning

Fra å være den sekundære telekommunikasjonskanalen har mobiltelefonen blitt den primære, og mobilnettet benyttes stadig mer også når det gjelder finansielle tjenester.

Orkanen "Dagmar" i desember 2011 avdekket hvor sårbart samfunnet har blitt dersom mobilnettet faller ut. Ekstremværet avdekket at store områder kan miste de fleste muligheter til elektronisk kommunikasjon der aksessnettene for mobiltelefon får omfattende skader.

Post- og teletilsynet (PT) publiserte i januar 2012 rapporten "Foreløpige erfaringer og forslag til tiltak etter ekstremværet Dagmar"[27], der flere forslag til forbedringer ble fremmet. PT vil pålegge tilbyderne å ha reservestrøm for minst seks timers drift på de aller fleste basestasjoner, og vil ta initiativ til et program for å styrke basestasjonslokasjoner som dekker særlig viktige områder. Målet er å sikre 1000 basestasjonslokasjoner på landsbasis og pålegge tilbyderne å sikre disse med batteri og aggregat for tre døgns drift.

PT foreslår videre å innføre prioritet i mobilnettene. Mange samfunnsfunksjoner er i dag avhengige av mobilkommunikasjon. Ved knapphet på nettkapasitet i en krise- eller beredskapssituasjon, er det viktig med ordninger som klart prioriterer funksjoner som er kritiske for samfunnet.

4.5.2 Test av sikkerhetsnivået på skytjenester

En britisk undersøkelse i regi av British Aerospace (BAE) resulterte i et sett med anbefalinger til dem som vurderer å sette ut tjenester til en skyleverandør:

- Sjekk at skyleverandøren har høykvalitets brannmur og IDS.
- Sjekk om skyleverandøren gjør regelmessige, uavhengige sikkerhetstester av kjøremiljøet. Undersøk grundig hvordan skyleverandørens sikkerhetsmodell passer med egen sikkerhetsarkitektur.

[27] Post- og teletilsynet, rapport nr. 2 2012: "Foreløpige erfaringer og forslag til tiltak etter ekstremværet Dagmar"

- Vær klar over et mulig botCloud-angrep[*]. Trafikken fra kjente skyleverandører kan ikke uten videre anses som sikker.

  [[*] http://baesystemsdetica.blogspot.no/2012/10/botcloud-emerging-platform-for-cyber_785.html, note satt inn 10.4.2013, red.merkn.]

4.5.3 Funn i trusselrapport fra ENISA

ENISA (The European Network and Information Security Agency) er et nettverk av informasjonssikkerhetseksperter i EU som lager veiledninger og anbefalinger til god praksis i informasjonssikkerhet. ENISA publiserte høsten 2012 rapporten "ENISA Threat Landscape".[28] Rapporten omhandler trusler mot cyber-sikkerhet, og den er basert på analyser av over 120 rapporter og funn fra IT-sikkerhetsindustrien, standardiseringsorganer, IT-sikkerhetsnettverk og andre uavhengige organisasjoner. I tillegg til å rangere truslene, konkluderer rapporten med et sett med anbefalinger.

Viktige elementer er bedre ende-til-ende-dokumentasjon av angrepsscenariet, bedre dokumentasjon av hvilke konsekvenser et vellykket angrep kan få, og felles terminologi. Øverst på ENISAs trusselliste kom såkalte Drive-by Exploits[29] og trojanere.

[28] http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISAThreatLandscape
[29] "Drive-by Exploits" vil si den trusselen som brukeren utsettes for i "forbifarten" ved åpning/klikking på lenker i web-sider/e-post som setter i gang nedlasting av ondsinnet kode til brukerens datamaskin uten at brukeren vet om det.

5 Identifiserte risikoområder

5.1 Styring og kontroll

Finansforetakene er ansvarlige for all informasjons- og kommunikasjonsteknologi som de benytter i sin virksomhet. Finanstilsynet erfarer ofte at foretakene anser leverandørene som ansvarlige. Dette kan føre til mangler når det gjelder styring og kontroll.

Finanstilsynet mener at den enkelte banks rettigheter og plikter knyttet til de samordnede fellesløsningene (BAX, NICS, BankID og andre) ikke er definert godt nok. Dette gjelder eierrettigheter, bruksretter, utvikling og forvaltning.

Leverandørene av løsningene er i stadig endring ved at de omorganiserer, selger, fusjonerer eller flytter. Foretakene utkontrakterer stadig mer. I denne situasjonen er det viktig at foretakene har frihet til å velge en annen retning enn den som leverandøren velger. Da er det viktig med klare eier- eller bruksrettigheter til programmer, dokumentasjon og annen IPR ("intellectual property rights") som inngår i løsningen.

5.2 Angrep på nettbaserte løsninger

Foretakene rapporterer at de anser kriminelle angrep som en stor utfordring, og øker innsatsen for å holde angrepene under kontroll. Trojanerkoden er avansert, ofte sammensatt av flere moduler slik at en og samme trojaner kan etablere kontakt med et kommandosenter, sende og samle informasjon, oppdatere seg selv og gjennomføre "mann-i-midten"-angrep.

I 2012 ble kundene oppfordret av bankene til å skru av bankenes innloggingsløsning (BankID) som følge av en svakhet i Java som kunne utnyttes.

Finanstilsynet anser angrep på nettbasert løsninger som en økende risiko.

5.3 Kontinuitets- og katastrofeløsninger

Stadig flere tjenester anses som tidskritiske. Nye tjenester kommer som krever umiddelbar behandling, som for eksempel straksbetaling ("fast payment") og tilsagn om lån "på stedet".

Når det gjelder kontinuitets- og katastrofeløsninger, erfarer Finanstilsynet at:

- løsningene ofte ikke fungerer som forventet
- løsningene er utfordrende å teste i sin helhet
- løsningene ikke blir oppdatert i takt med primærløsningen
- opplæring blir forsømt
- leverandørene samarbeider nå bedre enn før ved hendelser

Finansnæringen har sammen utviklet en rekke fellesløsninger som driftes ett sted. Dette fører til en konsentrasjonsrisiko som kan ha betydning når det gjelder kontinuitet og katastrofe.

Finanstilsynet anser kontinuitets- og katastrofeberedskapen som et risikoområde.

5.4 Risiko ved gamle og komplekse systemer

Det er utfordringer knyttet til:

- omfanget av vedlikehold på gamle systemer
- kompetanse og kapasitet på gamle systemer
- integrasjon mellom gamle systemer og nye tjenester
- stadig økende kompleksitet i integrasjonslaget, noe som gir opphav til feil og stopp
- sikkerhetshull som følge av kompleksitet

Finanstilsynet anser risikoen på dette området for å være økende.

5.5 Tilgang til betalingstjenester

Hendelsen i betalingstjenestene i påsken 2011 resulterte i en omfattende risikoanalyse av den finansielle IKT-infrastrukturen og tiltak for å redusere risikoen for hendelser. Det har likevel vært alvorlige hendelser som ligger innenfor området som har vært kartlagt. Det var ingen nedgang i antall hendelser i 2012 sammenlignet med 2011.

Risikoen for at det vil skje hendelser som går ut over tilgjengeligheten til tjenestene anses å være på samme nivå som i 2011, og må fortsatt følges opp.

6 Finanstilsynets videre oppfølging

6.1 IT-tilsyn og annen kontakt med foretakene

Finanstilsynets oppfølging av foretakenes IT-risikoer skjer primært gjennom tilsyn. Tilsynenes formål og omfang varierer, og er basert på en risikovurdering av det aktuelle foretaket. Det viktigste grunnlaget for tilsyn er IKT-forskriften og ulike tilsynsmoduler (egenevalueringsskjemaer). De mest vanlige tilsynsmodulene er tilgjengelige på Finanstilsynets nettsted. Ut fra Finanstilsynets risikovurderinger vil tematilsyn bli integrert i den generelle tilsynsvirksomheten.

Finanstilsynet har ellers løpende kontakt med foretakene, knyttet til den generelle IT-risikosituasjon, prosjekter eller hendelser.

6.2 Hendelsesrapportering

Foretakene skal rapportere vesentlige hendelser til Finanstilsynet, jf. IKT-forskriften § 9. Slike innrapporterte hendelser gir innblikk i foretakenes risikoer, som Finanstilsynet eventuelt også vil ha behov for å følge opp. Ikke minst representerer hendelsesdatabasen en verdifull kilde for analyse av trender og sammenhenger.[30]

6.3 Arbeid med betalingssystemer

Finanstilsynets ansvar for betalingssystemer er hjemlet i finanstilsynsloven og gjennom forskriftene om risikostyring og internkontroll og bruk av IKT. Oppgaver knyttet til systemer for betalingstjenester er i tillegg regulert gjennom lov om betalingssystemer m.v., kapittel 3. Det er også en omfattende

[30] Hendelsesrapportering til Finanstilsynet:
http://www.finanstilsynet.no/no/Bank-og-finans/Banker/Tema/IT-tilsyn/

selvregulering av dette området gjennom banksamarbeidet og oppgaver tillagt Finans Norge for fellestjenester. Regelverket er inntatt i den såkalte Blåboken. Norges Bank ivaretar også viktige oppgaver på betalingssystemområdet med hjemmel i sentralbankloven og betalingssystemloven. For å sikre et best mulig samspill på dette viktige området er samarbeidet mellom Norges Bank og Finanstilsynet beskrevet i egen avtale.[31] Norges Bank og Finanstilsynet samarbeider også om dokumentasjon som ligger til grunn for Norges Banks årsrapport om betalingssystemer og Finanstilsynet ROS-analyse. Rapportene gir til sammen et helhetlig bilde av risiko i betalingssystemene og finanssektorens IKT-bruk.

6.4 Meldeplikt om etablering og drift av systemer for betalingstjenester

Foretakene skal uten unødig opphold gi melding til Finanstilsynet om etablering og drift av systemer for betalingstjenester, jf. lov om betalingssystemer § 3-2. Meldeplikten er utdypet i tilsynets rundskriv 17/2004 med tilhørende egenmeldingsskjema. Meldingene er viktige for at Finanstilsynet skal kunne følge med på endringer som skjer i betalingstjenester og de operasjonelle risikoene relatert til slike tjenester.

Finanstilsynet mottar generelt få meldinger, og det er grunn til å tro at foretakene ikke i tilstrekkelig grad etterlever lovens krav. For å sikre at loven etterleves, vil Finanstilsynet vurdere om det er grunnlag for å benytte forskriftshjemmelen i betalingssystemloven, og om rundskriv 17/2004 skal erstattes av en forskrift.

6.5 Beredskapsarbeid

Gjennom samarbeid med finansnæringen, Norges Bank og andre myndigheter arbeides det med å sikre nødvendig prioritering av strøm og teletjenester for institusjoner som er viktige for å opprettholde virksomhet i nøkkelinstitusjoner i en beredskapssituasjon. Det blir også arbeidet med å sikre nødvendige betalingsmidler for befolkningen i en lengre beredskapssituasjon. Dette skjer i sammenheng med gjennomgang av viktige finansinstitusjoners etablerte beredskapsorganisasjon, beredskapsløsninger og verifisering av at løsningene er virksomme gjennom dokumenterte resultater fra katastrofetesting.

[31] Samarbeidsavtale mellom Norges Bank og Finanstilsynet om betalingssystemer: http://www.norges-bank.no/pages/88601/betalingssystemloven_samarbeid_ansvarsdeling_NB_FT_2012.pdf

6.3.1 Beredskapsutvalget for finansiell infrastruktur (BFI)

I regi av BFI planlegges og gjennomføres det årlige beredskapsøvelser med myndigheter, finansinstitusjoner og leverandører som deltakere.

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

Foto omslag: Cornelius Poppe/NTB scanpix
Design omslag: Miksmaster Creative
Trykkeri: Rolf Ottesen AS
04.2013/500

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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