FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

RISIKO- OG SÅRBARHETSANALYSE (ROS)

2015

Risiko- og sårbarhetsanalyse (ROS) 2015

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Finanstilsynet, 28. april 2016

INNHOLD

1 Innledning

Finanstilsynet utarbeider hvert år en risiko- og sårbarhetsanalyse (ROS-analyse) av finanssektorens bruk av IKT og betalingstjenester. Gjennom tilsynsarbeidet har Finanstilsynet en bred kontaktflate med finansforetak, bransjeforeninger, leverandører, standardiseringsorganer og nasjonale og internasjonale myndigheter. Basert på disse kildene gir rapporten en vurdering av hvordan identifiserte risikoer kan få innvirkning på finanssektoren i Norge.

Formålet med rapporten er å reflektere risikoen og sårbarheten både med hensyn til finansiell stabilitet og det enkelte foretak, og med hensyn til den enkelte forbruker. Den gir et oppdatert bilde av risikoen ved finanssektorens bruk av IKT og betalingstjenester, oppsummert i rapportens kapittel 2.

Noen risikoer og sårbarheter omtales årlig, andre ikke. I rapporten peker Finanstilsynet på de risikoene som er vurdert som de viktigste dette året. Risikoer pekt på i tidligere rapporter og som ikke er omtalt i årets rapport, er ikke vurdert som like aktuelle, men det betyr ikke at de ikke fortsatt er til stede.

Kjernen i rapporten er kapitlene 3 og 4. Kapittel 3 gir et bilde av funn og observasjoner gjennom Finanstilsynets aktiviteter i 2015. Kapittel 3 omtaler også digital kriminalitet og trekk ved utviklingen i denne. Teknologiske utviklingstrekk som antas å kunne få betydning for foretakenes bruk av IKT blir omtalt. Kapittel 4 refererer finansforetakenes egne vurderinger innhentet gjennom spørreskjema og intervjuer. I tillegg er noen sentrale tjenesteleverandører, herunder for sikkerhetsløsninger, intervjuet og årsrapporter fra internasjonale sikkerhetsselskaper med særlig fokus mot finansnæringen refereres.

Endringer i reguleringer som kan medføre omfattende endringer i foretakets systemløsninger er omtalt i kapittel 5.

I kapittel 6 fremkommer Finanstilsynets overordnede vurdering av risikobildet i 2015 på bakgrunn av funn, observasjoner og utviklingstrekk. Vurderingene trekker frem de mest sentrale trusler og sårbarheter som kan føre til at foretakenes systemer får skader av et omfang som negativt kan påvirke målsettingen om finansiell stabilitet og velfungerende markeder.

Kapittel 7 beskriver de hovedområdene som Finanstilsynets vil ha særskilt oppmerksomhet på fremover.

En ordliste som forklarer ord og akronymer brukt i rapporten er vedlagt.

2 Oppsummering

I 2015 var det ingen alvorlige IKT-hendelser med konsekvenser for finansiell stabilitet. Sammenliknet med året før, var det en nedgang i antall hendelser med konsekvens for hhv. enkeltforetak og forbrukerne. Det var imidlertid en tendens til et økende antall svindelangrep.

Den teknologiske utviklingen har stor innvirkning på tjenesteutviklingen i finansnæringen. Deregulering åpner for nye aktører og nye løsninger som utfordrer de etablerte forretningsmodellene.

2.1 Finanstilsynets funn og observasjoner

Gjennom oppfølging av rapporterte hendelser, funn fra tilsyn og annen oppfølging mot finansnæringen får tilsynet god innsikt i foretakenes bruk av IKT, betalingsløsninger og i aktuelle risikoområder.

Betalingssystemer

Finanstilsynet vurderer betalingssystemene generelt som solide og stabile i 2015, men på enkelte områder er det likevel rom for forbedringer. I flere foretak er det observert at blant annet kriseløsninger, styring av operasjonell risiko og styring av tilganger kan bli bedre.

Som et ledd i styringen og kontrollen av betalingstjenestene, bør tiltak for å sikre god samhandling om fellesløsninger og infrastruktur videreføres.

Til tross for en økning i angrep mot betalingstjenestene i 2015, er de direkte tapene fortsatt små. Mye av årsaken til lave tap skyldes forebyggende tiltak. Samlede tap ved bruk av nettbank endret seg lite fra 2014 til 2015. Tapene ved bruk av nettbank i 2015 var i stor grad knyttet til svindel via bedrifts-nettbanker.

Det er fortsatt økning i tap ved handel med betalingskort der det ikke er krav til ekstra sikkerhet, for eksempel PIN-kode ("Card-Not-Present"). Økningen i disse tapene er større enn økningen i volumet av kortbetalinger, og var på 37 prosent fra 2014 til 2015. Dette er nær en fordobling fra 2013. Samlede tapstall for kortbruk økte med 25 mill. kroner fra 2014 til 2015, en økning på 15 prosent.

Bank

Bankene har de senere år vært gjennom store endringsprosesser på IKT-området, men endringene er gjennomført uten vesentlige konsekvenser for driftsstabiliteten.

Finanstilsynet ser imidlertid at det på flere områder er behov for forbedringer. Risikoen for digitale angrep tiltar, og arbeidet med IKT-sikkerheten bør intensiveres ytterligere. Finanstilsynets erfaring fra tilsyn er at oppfølgingen av ISP[1]-leverandører kan være mangelfull. Det er Finanstilsynet vurdering at foretakene kan bedre kvaliteten på tilgangsstyringen. Finanstilsynet ser samtidig at det kan bli utfordrende for foretakene å skaffe tilstrekkelig kompetanse på sikkerhetsområdet.

Verdipapirområdet

Det er Finanstilsynet vurdering at IKT-systemene i den norske verdipapirsektoren gjennomgående har god kvalitet og høy stabilitet.

Foretakene må imidlertid bli bedre på å sikre at sensitiv informasjon fra verdipapirforetakenes corporate-avdelinger, ikke kommer på avveier. Finanstilsynet har registrert utkontraktering av IKT-systemer med kurssensitive data hvor foretaket har hatt manglende kontroll med leverandørenes driftsoperatører.

Avtaler knyttet til verdipapirforetaks IKT-utkontraktering viste mangler i foretakets rett til å kontrollere og revidere leverandørens aktiviteter knyttet til avtalene.

I 2015 ble det registrert flere hendelser med manglende lydopptak av samtaler med kunder mv. grunnet teknisk svikt i opptaksutstyret.

Forsikringsområdet

Forsikringsnæringen er for tiden gjenstand for mange regelverksendringer som medfører betydelige endringer i store og komplekse IKT-systemer. Foretakene må sikre kvaliteten i, og etterlevelse av, sine IKT-prosesser for å sikre kontroll med endringene, slik at kvaliteten på systemene ikke blir forringet.

Mange foretak har fremdeles behov for å bedre sitt arbeid med risikoanalyser for å skaffe seg et riktig bilde over den samlede risikoen ved selskapets bruk av IKT.

Regnskapsførerselskap

Finanstilsynet gjennomførte i 2015 et dokumentbasert tilsyn med regnskapsførerselskapenes bruk av IKT. Tilsynet viste at en del selskaper har behov for å iverksette tiltak som kan redusere risikoen knyttet til IKT-systemene i virksomheten.

Utkontrakteringsmeldinger

Foretakene er pålagt å sende melding til Finanstilsynet ved utkontraktering av IKT-tjenester. Ved behandling av meldinger om utkontraktering har Finanstilsynet erfart svakheter både når det gjelder gjennomførte risikoanalyser, foretakets selvstendige vurderinger av utkontrakteringsforholdet og etterlevelse av gjeldende lover og forskrifter. Dette gjelder blant annet IKT-forskriften og

[1] Internet Service Provider

internkontrollforskriftens krav om at foretaket under tilsyn skal gis rett til å kontrollere, herunder revidere, de av leverandørens aktiviteter som er knyttet til avtalen.

Bruk av skytjenester vil etter Finanstilsynets vurdering falle inn under reglene som gjelder tradisjonell utkontraktering.

Hendelser

Foretakene er pålagt å rapportere alvorlige og kritiske avvik i IKT-virksomheten. Det ble rapportert færre hendelser i 2015 enn i 2014, og betalingssystemene og kunderettede tjenester var mere tilgjengelige i 2015 enn i året før. Utviklingen er tilbake på den positivt synkende trenden fra 2011, etter at den i 2014 ble brutt. Derimot er det et økt omfang av svindelangrep, og flere foretak ble i 2015 utsatt for angrep med krav om løsepenger, dog slik at løsepenger ikke ble betalt.

Digital kriminalitet

Den digitale kriminaliteten vokser og endrer trusselbildet for finansnæringen. IKT-forskriften stiller tydelige krav til foretakets styring og kontroll med IKT-sikkerhet. Det er viktig at foretakenes ledelse og styre stiller tydelige krav til og følger opp foretakets arbeid med IKT-sikkerhet. Tilsiktede kriminelle hendelser kan få betydelige konsekvenser for det enkelte foretak. Eksempelvis medførte krypteringsvirus at foretak ble utestengt fra arbeidsverktøy og data gjennom hele arbeidsdager inntil dataene var gjenopprettet fra backup. Også finansiell stabilitet kan bli forstyrret hvis slike hendelser treffer samordnede løsninger, felles driftsleverandører eller andre sentrale aktører.

2.2 Foretakenes vurderinger

Foretakene vurderer forstyrrelser i infrastruktur, kompleksitet i IKT-systemer og leveransekjeder, digital kriminalitet og inntrenging i systemer samt brudd på konfidensialitet som de mest fremtredende truslene.

Andre trusselområder som trekkes frem av foretakene er knapphet på kompetanse, ukritisk bruk av fildelingstjenester og manglende styring og kontroll med bruk av skytjenester, manglende kvalitet eller mangel på penetrasjonstesting, omfanget av endringer og at IKT-systemene ikke gir tilfredsstillende støtte til beslutninger, kundebehandling eller saksbehandling.

Foretakene peker også på samfunnsendringene, hvor betalingssystemene i økende grad kan bli brukt til flytting av ulovlige midler, som en trussel. Foretakene ser også en risiko for at de ikke klarer å lage systemer som har høy nok presisjon når det gjelder å flagge mistenkelige transaksjoner.

2.3 Endringer i reguleringer

I 2015 var en rekke EU-prosesser knyttet til forslag til nye, eller endringer i eksisterende direktiver, forordninger, tekniske standarder og veiledninger. Disse vil få betydning for norske forhold etter hvert som de tas inn i norsk lovgiving. Også nasjonalt var det endringer i lover, forskrifter og retningslinjer. Reguleringsendringene vil på flere områder medføre behov for endringer i foretakenes systemløsninger.

Den mest sentrale regelendringen er EUs nye betalingstjenestedirektivet (PSD2). Det åpner for at nye aktører kan tilby betalingstjenester og gis rett til tilgang til betalingskonto. Andre større regelendringer er EUs forordning om behandling av personopplysninger, EUs direktiv for nettverks- og informasjonssikkerhet, ny avtale om overføring av data mellom EU/EØS og USA, norsk forskrift om systemer for betalingstjenester, retningslinjer for sikkerhet i Internett-betalinger og norsk forskrift om innføring av forordning om interbankgebyrer.

2.4 Aktuelle risikoområder

Finansiell infrastruktur

Finanstilsynet vurderer den norske finansielle infrastrukturen som solid. Den ble rammet av færre operasjonelle hendelser og stabiliteten var bedre i 2015 enn foregående år. På enkelte områder er det rom for forbedringer. Dette gjelder blant annet kriseløsninger og styring av operasjonell risiko.

Foretakene

Finanstilsynets vurderer feil i nettverk, informasjonslekkasjer, digitale angrep, komplekse systemporteføljer og feil ved endringer som de mest sentrale truslene mot og sårbarhetene i foretakenes systemer. Andre trusler mot og sårbarheter i foretakenes systemer er mangelfulle kontinuitetsløsninger, konsentrasjonsrisiko, manglende testmuligheter og manglende kompetanse og kapasitet.

Forbrukere

Graden av digitalisering i finansnæringen øker stadig. Det gjør forbrukeren mer sårbar for svikt i foretakenes elektroniske tjenester, og det stilles derfor større krav til robusthet i foretakenes løsninger.

Den økte digitaliseringen kan gjøre det vanskelig for forbrukerne å forstå alle konsekvenser av sine digitale handlinger. Hensynet til enkelhet og hurtighet på små digitale flater kan gå på bekostning av forbrukers sikkerhet og rettigheter. Forbruker er i økende grad eksponert for svindel ved bruk av digitale løsninger. Beskyttelse av informasjon og å forhindre ID-tyveri er stadig aktuelle utfordringer.

I arbeidet med regelverksendringer står hensynet til forbrukerne og forbrukernes sikkerhet og rettigheter sentralt.

3 Finanstilsynets funn og vurderinger

I dette kapitlet omtales i hovedsak funn og vurderinger basert på Finanstilsynets tilsynsvirksomhet, hendelsesrapporter, meldinger om nye og endrede betalingstjenester og nye og endrede utkontrakteringsavtaler for IKT.

Utviklingstrekk som på sikt antas å kunne få betydning for foretakenes bruk av IKT, og som kan medføre endringer i risiko- og sårbarhetsforhold både for foretakene og for forbrukerne, omtales også.

Det var i 2015 en rekke hendelser med konsekvens både for enkeltforetak og for forbrukerne. Finanstilsynets vurdering er at finansiell stabilitet ikke var truet i 2015.

3.1 Utviklingstrekk innenfor finansiell teknologi

Den teknologiske utviklingen har stor innvirkning på utviklingen i finansnæringen. Nytenking og utvikling innen betalingssystemer, utlån, forsikring og kapitalforvaltning utfordrer de etablerte forretningsmodellene, og gir nye aktører muligheter til å komme inn som deltagere eller bidragsytere.

Norsk finansnæring har vært tidlig ute med å ta i bruk teknologi i løsninger både for medarbeidere og publikum. For fortsatt å være i front med teknologiske verktøy, er det viktig å være oppmerksom på mulighetene nye finansteknologiske løsninger åpner for. Utviklingen er stimulert av stor økning i investert kapital i finansteknologi som muliggjør utvikling av nye løsninger. Økt bredbåndstilgang med større kapasitet og bruk av moderne datamaskiner, smarttelefoner og lesebrett har bidratt til økt bruk av digitale tjenester.

Bruken av teknologi sammen med nye og eller forbedrede tjenesteleveranser innen finansnæringen faller i to kategorier, hvor den ene er nye tjenester som levert av nye aktører, og den andre er nye tjenester levert av etablerte aktører i næringen. Nye aktører vil trolig føre til økt grad av utvikling og ideskaping.

3.2 Betalingssystemer

3.2.1 Generelt om betalingssystemer

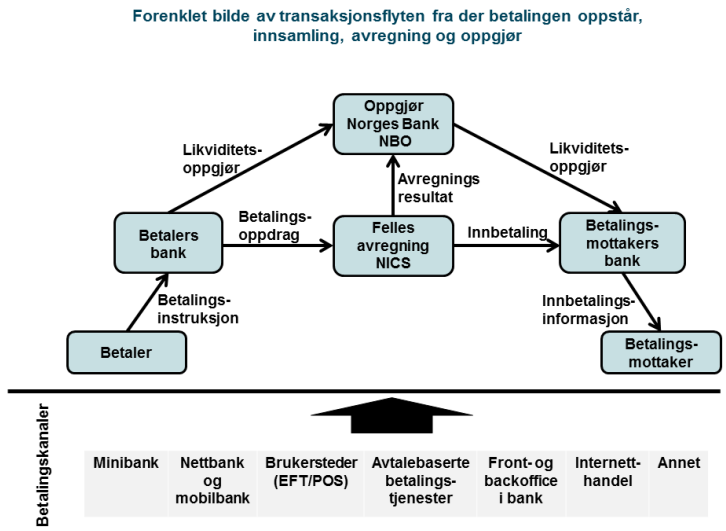
Finansiell stabilitet innebærer at det finansielle systemet er robust nok til å utføre betalinger, formidle finansiering og fordele risiko på en tilfredsstillende måte. Effektive, robuste og stabile betalingssystemer er grunnleggende for finansiell stabilitet og velfungerende markeder.

I Norge reguleres betalingssystemer og -tjenester gjennom lover og forskrifter, og gjennom Finans Norges forvaltning av finansnæringens selvregulering.

Finansavtaleloven og EUs betalingstjenestedirektiv, som nylig er revidert, har som formål å ivareta forbrukerhensyn og best mulig sikre forbrukernes sikkerhet og rettigheter.
Betalingstjenestedirektivet har også til formål å stimulere til økt konkurranse.

Aktuelle regelverksendringer for betalingssystemene er beskrevet i punkt 5.2.3.

Figur 1: Transaksjonsflyten i det norske betalingssystemet



Et betalingssystem defineres som et system basert på felles regler for avregning, oppgjør og overføring av betalinger mellom to parter som samhandler økonomisk. Juridisk skilles det mellom et interbanksystem, som behandler transaksjoner mellom banker, og en betalingstjeneste, som behandler transaksjoner mellom kunde og bank. Figur 1 viser transaksjonsflyten i det norske betalingssystemet. Nederst i figuren illustreres de ulike betalingskanalene som kundene benytter.

Kilde: Finanstilsynet

3.2.2 Styring med risiko og sårbarhet i betalingssystemene

Finanstilsynet har funnet endringer i utkontrakteringsforhold hvor foretaket ikke har gjort risikovurderinger av endringene i forkant. I tillegg har Finanstilsynet observert at betalingstjenester er lansert der risikoreduserende tiltak ikke var på plass ved oppstart, hendelser som viser mangelfull kvalitet på testing og avtaler som ikke har tilfredsstilt regulatoriske krav.

Det er et ledelsesansvar å sørge for at det enkelte foretak har styring og kontroll med hele betalingsformidlingen som samsvarer med den sentrale rollen den utgjør i en velfungerende økonomi. Foretaket har ansvar for tjenesten i sin helhet, også utkontrakterte deler.

Hendelser som oppstår i, eller innvirker på betalingsinfrastrukturen eller betalingstjenester, kan ramme bredt og raskt medføre store konsekvenser. Feil og avvik i betalingsformidlingen forårsakes hyppigst av systemendringer og -oppdateringer. Betalingsformidlingen og teknologiene som brukes, er under stadig forandring. Det medfører et løpende behov for endringer i eksisterende betalingsformidlingsløsninger, i tillegg til utvikling av nye løsninger. Dette medvirker til en høy endringstakt og risiko.

Styring av risiko, kvalitetssikring av utvikling, god ende-til-ende-testing og etablering av god sikkerhetskultur i alle ledd, er en sentral del av foretakenes utviklings- og endringsprosesser. Også gjennomføring av regelmessige verdikjedebaserte risiko- og sårbarhetsanalyser innenfor betalingsformidlingen er nødvendige for å redusere sårbarhet og risiko til definert og akseptabelt nivå.

Det er viktig at foretakene gjør grundige risikovurderinger gjennom sikkerhets- og sårbarhetsanalyser før lansering av nye betalingstjenester, og senere periodisk. Foretakene må sikre at tjenesten er beskyttet gjennom logiske og fysiske sikringstiltak, og at informasjon beskyttes tilstrekkelig. Betalingstjenesten må overvåkes for å sikre tilstrekkelig sikkerhetsnivå, og for å avdekke og hindre uautorisert bruk av tjenesten. Det vises i den sammenheng til forskrift om systemer for betalingstjenester, se punkt 5.2.3, som regulerer dette.

3.2.3 Meldinger om systemer for betalingstjenester

Lov om betalingssystemer stiller krav til at det uten unødig opphold skal gis melding til Finanstilsynet om etablering og drift av betalingstjenester. Følgende forhold utløser meldeplikt:

- Innføring av nytt system for betalingstjeneste
- Ny versjon som vesentlig påvirker andre berørte parter som inngår i løsningen
- Ny versjon med endret eller ny funksjonalitet som er vesentlig for systemet for betalingstjenesten.

I 2015 mottok Finanstilsynet ni meldinger om nye eller endrede betalingstjenesteløsninger.
Flere av meldingene er knyttet til mobile løsninger. De øvrige meldingene var knyttet til andre typer betalingsløsninger eller kortadministrasjonsløsninger.

Det er Finanstilsynets vurdering at etterlevelsen av meldeplikten ikke er tilfredsstillende i alle foretak. Enkelte foretak har med bakgrunn i innsendte meldinger blitt bedt om supplerende informasjon. Finanstilsynet erfarer at både nye løsninger lanseres, og endringer i eksisterende løsninger gjennomføres uten at disse blir meldt. Aktuelle foretak blir kontaktet og bedt om å sende inn melding.

3.2.4 Bruk av mobilens funksjoner og mobile betalingsløsninger

Teknologiutviklingen påvirker i vesentlig grad utviklingen av betalingstjenester og betalingssystemer ved at foretakene tar i bruk nye muligheter og ved at nye aktører, herunder utenlandske, etablerer seg.

Den raske utviklingen innen mobile løsninger fortsetter. Mobile enheter og -løsninger er i ferd med å få betydelig betydning både som betalingsinstrument, bærer av digitale lommebøker og som bærer av sikkerhetsløsninger.

Mobilbetalingsløsningene har i første rekke vært rettet mot person-til-person-betalinger, hvor potensialet for forenkling er størst. I 2015 lanserte DNB sin Vipps-applikasjon[2] og Danske Bank sin MobilePay-applikasjon[3] i det norske markedet. mCASH, hvor de norske rettighetene høsten 2015 ble kjøpt opp av Sparebank 1-bankene[4], lanserte sin løsning i 2014 for både person-til-person-betalinger og for person-til-bedrift-betalinger. Også andre aktører i finansnæringen utvikler løsninger for person-til-bedrift-betalinger, både til fysiske butikker, foreninger og lag og til Internett-butikker. Blant annet har Danske Bank utvidet sin MobilePay-applikasjon med løsninger som MobilePay Point of Sale[5], DNB har utvidet sin applikasjon Vipps[6] med løsninger mot foreninger og lag. Eika-bankene forventes å lansere sin Eika Safe[7]-løsning i 2016.

Hittil har de mobile løsningene i all vesentlighet bare kunne benyttes med bruk av internasjonale betalingskort. BankAxept, det nasjonale betalingskortet i Norge, har nye betalingsløsninger under utvikling og forventes å lansere BankAxept kontaktløs betaling (NCF-teknologi), med betalingskort, mobil og ved nettbetaling i 2016[8].

Betalingsapplikasjonen Valyou[9] basert på kontaktløs teknologi ble offisielt lansert høsten 2014. Allerede høsten 2015 ble tjenesten lagt ned grunnet blant annet manglende kundemasse og utbredelse av operative terminaler for kontaktløs betaling ute i butikkene.

Fingeravtrykk på mobilen er i 2015 tatt i bruk som autentisering for betalingstjenester i det norske markedet. Blant annet benyttes fingeravtrykk for å åpne Danske Banks MobilePay-applikasjon og for innlogging på DNBs mobil- og nettbank[10]. Kvaliteten på fingeravtrykkssensorene i mobilen er et nytt sårbarhetsområde for betalingstjenester, som må risikovurderes og følges opp av betalingstjenestetilbyder. Skandiabanken lanserte i 2015 bruk av QR-kode (Quick Response code) for innlogging i nettbanken[11].

[2] https://www.vipps.no
[3] http://danskebank.no/nb-no/mobilepay/Pages/mobilepay-privat.aspx
[4] https://www.bnbank.no/Omoss/Generell-informasjon/For-pressen/Pressemelding-03032014/
[5] https://www.danskebank.no/nb-no/mobilepay/Pages/tilmelding-til-pos.aspx
[6] https://www.vipps.no/bedrift/lag-forening.html
[7] https://eika.no/om-oss/nyheter/2015/eika-safe
[8] http://www.bankaxept.no/
[9] http://www.digi.no/931241/naa-er-valyou-lansert
[10] http://www.dinside.no/934551/logg-inn-i-nettbanken-med-fingeravtrykk
[11] https://skandiabanken.no/bruke/sikkerhet-og-innlogging2/logg-inn-med-qr-kode/

Nye autentiseringsløsninger er under utvikling, særlig ved bruk av biometri. Mastercard har lansert sin "selfie payments"[12] hvor autentiseringen skjer via bruk av billedgjenkjenning eller fingeravtrykk. Også løsninger for stemmegjenkjenning[13] er lansert.

Hensikten med mobile betalingsløsninger er å bidra til forenkling av elektronisk betaling, men også å erstatte bruken av kontanter. Betalingstjenestetilbyderne har imidlertid ikke samlet seg om felles bruk av utviklet infrastruktur for straksbetalinger[14]. I tillegg til utvikling av betalingsapplikasjonene, har tilbyderne også utviklet egen infrastruktur som gjør at betalingsmottaker ikke får tilgang til pengene uten å installere samme applikasjon som betaler. En manglende standardisering på terminalsiden i butikkene har medført at brukersteder (NorgesGruppen og Coop[15]) har gått sammen om etablering av én felles infrastruktur med én terminalløsning. Forenklingen sammenlignet med betalingsapplikasjonene synes så langt begrenset. Fordi de forskjellige applikasjonene kun fungerer for noen forretningskjeder, kan mobilbetaling virke både forvirrende og lite rasjonell for forbruker. I tillegg synes dagens kortbetalingsløsninger å være mer effektive innenfor mange bruksområder.

Manglende interoperabilitet vil kunne medføre redusert effektivitet og økte kostnader i betalingsformidlingen. Hvis kostnadene øker urimelig eller løsningene ikke er brukervennlige, må det vurderes om det er behov for regulatoriske tiltak.

Hittil har store internasjonale aktører innenfor mobile betalingsløsninger i liten grad gjort fremstøt i det norske markedet, men det antas at det fremover vil komme etableringer enten direkte eller via samarbeidskonstellasjoner. For andre betalingsløsninger har allerede en rekke aktører etablert seg og flere forventes å etablere seg når det nye betalingstjenestedirektivet PSD2 (se punkt 5.1.1) trer i kraft. Direktivet åpner for flere aktører som betalingstjenestetilbydere, og gir disse rett til tilgang til betalingskonto. Det forventes å medføre inntreden av en rekke nye aktører med nye løsninger innenfor alle typer betalingstjenester, i tillegg til at eksisterende aktører kan utvide sine nåværende løsninger med ny funksjonalitet. Disse endringene innenfor betalingsformidlingen vil kunne, spesielt i etableringsfasen, skape nye risikoer og sårbarheter som må håndteres.

Som en konsekvens av PSD2 er det stor aktivitet både innen nasjonal og europeisk finansnæring, og i tjenesteleverandørmarkedet for etablering av standarder og teknologi for tilgang til betalingskonto. EBA (se punkt 5.1.1) er tillagt et ansvar for å utarbeide forslag til regulatoriske tekniske standarder for sterk autentisering og sikker kommunikasjon for denne tilgangen.

Selv om den teknologiske utviklingen gir mulighet for å gjøre mobile betalingstjenester sikrere i bruk, øker samtidig trusselbildet i takt med utbredelsen av mobile løsninger. Mobiltelefoner er ett av de

[12] http://money.cnn.com/2016/02/22/technology/mastercard-selfie-pay-fingerprint-payments/
[13] http://www.pcquest.com/authshield-enhanced-online-payment-security-with-its-facial-and-voice-recognition-authentication-solution/
[14] https://www.fno.no/aktuelt/nyheter/2014/12/betal-fra-konto-til-konto-med-mobil/
[15] http://www.norgesgruppen.no/presse/nyhetsarkiv/aktuelt/onsker-a-gjore-mobilbetaling-tilgjengelig/

større vekstområdene for skadevare, og utviklingen antas å fortsette i takt med at mobiltelefonen i stadig større grad tas i bruk for daglige aktiviteter.

Finanstilsynet omtalte i Risiko- og sårbarhetsanalysen for 2014 vurderinger knyttet til mobilbaserte betalingsløsninger[16].

Finanstilsynet er kjent med at informasjon om kunders bruk av mobile bank- og betalingstjenester[17] brukes videre i kommersielle sammenhenger uten kundens viten. Dette kan bryte med personopplysningsloven. Det forventes at informasjon om kunder ikke deles med tredjepart uten at kunden både er innforstått med og har akseptert dette, og at kunden har adgang til å bruke tjenesten selv om aksept ikke gis. Dette blir fulgt opp av tilsynsmyndighetene.

3.2.5 Sperring av kort mot betalinger av handel på Internett

Retningslinjer for sikkerhet i Internett-betalinger trådte i kraft 1. august 2015. Retningslinjene sier blant annet at forbruker i større grad skal kunne sette effektive grenser for hva betalingskort kan benyttes til. Blant annet skal kunden kunne sperre kortet for bruk på Internett. Finanstilsynet har merket seg at ikke alle kortutstedere har implementert retningslinjene i sine løsninger. Finanstilsynet vil følge opp dette i 2016.

3.2.6 Angrep mot betalingstjenester

I 2015 rammet noen alvorlige hendelser tilgang til betalingsformidlingen. Finanstilsynet har likevel registrert økt grad av tilgjengelighet for betalingsløsninger i året som gikk, se punkt 3.9.2.

Flere av hendelsene rammet BankID, og medførte betalingsforstyrrelser for mange foretak samtidig. Hendelsene hadde ulike årsaker, men ingen var kritiske for tilgangen til betalingstjenestene. Flere foretak har etablert alternative løsninger for pålogging og signering, som reduserer konsekvensene ved avbrudd i BankID.

Selv om driftsstabiliteten økte, tiltok også de ondsinnede angrepene mot betalingsformidlingen. Det ble observert en rekke phishing-angrep rettet mot betalingskort og mot nettbank.

Svindelscenariene mot betalingstjenestene er i stor grad basert på phishing. Falske henvendelser og fisking av informasjon fremtrer i nye og mer troverdige varianter, og utfordrer sikkerheten i betalingstjenestene. De falske henvendelsene er kamuflert slik at de ser ut til å komme fra kjente kontakter. Det brukes både e-post og SMS. Phishing er ofte en del av scenariet både ved svindel mot betalingskort og nettbank, ransomware, APT- og CEO Fraud (se punkt 3.10.1). Ransomware, APT- og CEO Fraud rammer alle bransjer, men betalingstjenestene er spesielt utsatte fordi de er nært knyttet til penge-kildene.

[16] http://www.finanstilsynet.no/Global/Venstremeny/Rapport/2015/ROS_analyse_2014.pdf
[17] http://www.nrk.no/norge/dnb-sender-kundeinformasjon-til-facebook-1.12804837

I 2015 benyttet de kriminelle nye fremgangsmåter og bankene rapporterte ved flere anledninger om økt trusselnivå grunnet svindel mot bedriftsnettbank. Scenariet var basert på såkalt "sanntids-fisking". Den ansatte i bedriften mottok en falsk SMS eller e-post med en lenke til en falsk nettbank. Ved å trykke på lenka kom man inn på det som til forveksling lignet bankens bedriftsnettbank. Herfra var fremgangsmåten ganske lik som ved trojanerangrep på nettbank. Brukeren ble bedt om å oppgi brukernavn og to engangskoder som svindlerne fanget opp fortløpende og brukte i den ekte bedriftsnettbanken. Svindeltransaksjonene var til mottakere i utlandet. Til tross for betydelig svindelaktivitet av denne typen mot norske banker, er ikke tapene på nettbanksvindel i 2015 spesielt høye. Bankenes overvåking og samarbeidet i FinansCERT gjør at de fleste svindeltransaksjonene blir stoppet før de blir gjennomført, eller ved at pengene tilbakeføres fra mottakerbank.

Finanstilsynet er kjent med flere tilfeller av CEO Fraud[18] i 2015. Riktignok er ikke denne typen svindel rettet direkte mot betalingstjenestene, men tjenestene benyttes for pengeoverføring ved gjennomføring av svindel. Det er viktig at bankene gjennomgår sine rutiner, og der det er mulig iverksetter tiltak som kan bidra til å begrense skadeomfanget ved slik svindel.

Det er i 2015 observert svindel ved bruk av betalingsapplikasjoner (apper), hvor stjålen ID-informasjon og kort-informasjon er brukt til å etablere falske brukerkontoer. Finanstilsynets oppfatning er at foretakene har etablert en god oppfølging av den totale sikkerheten rundt tjenestene for å minimalisere risikoen, selv om det er svakheter knyttet til kontrolltiltak ved opprettelse av brukerkonto, særlig når det gjøres bruk av stjålen informasjon.

På tross av det økende omfanget av mobile betalingsløsninger og en global økning av infiserte mobiltelefoner[19], er Finanstilsynet ikke kjent med svindelforsøk i Norge basert på infiserte mobiltelefoner.

Erfaringene viser at kriminelle angrep mot betalingstjenester går i bølger. Aktiviteten flyttes fra land til land ut fra hvor de kriminelle antar at det finnes gevinstmuligheter.

Finanstilsynets vurdering er at foretakene har etablert en god beredskap og et godt forsvarsverk for å stoppe forsøk på svindel mot betalingstjenestene, og at effektive mottiltak reduserer skadeomfang og kunders tapsomfang ved svindel.

Det er Finanstilsynets vurdering at foretakenes informasjon til forbrukerne på hvordan de skal beskytte seg selv mot nett- og mobilbasert svindel stadig blir bedre.

[18] http://www.aftenposten.no/okonomi/Okokrim-advarer-mot-CEO-svindel---norske-bedrifter-rammet-av-millionbedrageri-8382868.html
[19] https://securityintelligence.com/mobile-malware-threats-in-2015-fraudsters-are-still-two-steps-ahead

3.2.7 Oversikt over årlige tap knyttet til betalingstjenester

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

3.2.7.1 Tapstall i Norge for kortbruk

Også i 2015 var det en kraftig økning i tap på svindel av typen CNP. Med en økning på nærmere 37 prosent, er tapene nesten fordoblet på to år og økt med 307 prosent på fem år. For de andre typene kortsvindel er samlet tap omtrent uendret.

Totalt er det 15 prosent økning i tap på kortbetalinger i 2015. På fem år har økningen vært 50 prosent.

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

Svindeltype betalingskort	**2011**	**2012**	**2013**	**2014**	**2015**
Misbruk av kortinformasjon, Card-Not-Present (CNP) (internetthandel m.m.)	24 190	35 701	51 954	72 056	98 410
Stjålet kortinformasjon (inkl. skimming), misbrukt med falske kort i Norge	468	2 308	762	524	2 670
Stjålet kortinformasjon (inkl. skimming), misbrukt med falske kort utenfor Norge	57 340	55 869	51 534	51 685	48 447
Originalkort tapt eller stjålet, misbrukt med PIN i Norge	32 224	28 128	21 274	21 266	18 875
Originalkort tapt eller stjålet, misbrukt med PIN utenfor Norge	7 008	8 544	9 570	13 071	14 224
Originalkort tapt eller stjålet, misbrukt uten PIN	4 488	4 603	4 949	5 510	6 033
TOTALT	**125 718**	**135 153**	**140 043**	**164 113**	**188 660**

Kilde: Finanstilsynet

Det totale volumet av korttransaksjoner i Norge økte med 7,6 prosent fra 2013 til 2014, mens volumet av kortbetalinger for varekjøp på Internett økte med 21 prosent (tall fra Norges Bank 2014[20]). Andelen svindel økte med 37 prosent fra 2014 til 2015 (fra ca. 72 millioner til ca. 98 millioner kroner). For handel på Internett utgjorde svindel vel 0,14 prosent (1,4 promille). Av den samlede verdien på kortbetalinger i Norge utgjorde svindel om lag 0,023 prosent[21].

[20] Norges Bank publiserer tall for 2015 først i mai 2016. Sammenligningene er derfor gjort mot tall fra Norges Bank for 2014.

[21] http://static.norges-bank.no/pages/103291/NB_memo_1_15.pdf?v=29062015145622&ft=.pdf
Tall fra Norges Bank viser at den samlede verdien på Internett-kjøp i 2014 var 69 milliarder kroner. Tap med CNP på 98 millioner utgjør 0,14 prosent, eller 1,4 promille av 69 milliarder kroner.
Totalt var verdien av kortbetalinger 807 milliarder i 2014. Tap med betalingskort på 188,660 millioner kroner utgjør 0,233 prosent av 807 milliarder kroner.

Tabell 2: Antall betalingskort rammet av misbruk

	2011	2012	2013	2014	2015
Antall kort rammet av misbruk	16 784	20 332	22 531	38 541	44 900

Kilde: Finanstilsynet

Sammenliknet med 2014 økte antall kort rammet av misbruk med 16,5 prosent i 2015. På fem år har økningen vært 168 prosent. Økningen i antall misbrukte kort i 2015 er lavere enn økningen i tapsbeløp i 2015, noe som innebærer større gjennomsnittlig tapsbeløp per kort som ble svindlet.

3.2.7.2 Kortsvindel og datatyveri

Tyveri av kortdata har i flere år vært omfattende og lønnsomt, og trenden er fortsatt økende. Driftsmiljøer som oppbevarer eller videreformidler store mengder kortrelatert informasjon[22] er mest sårbare.

Det er en fortsatt økning i tap ved CNP både nasjonalt og på europeisk nivå (se punkt 3.2.7.5[23]). Dette er hovedsakelig tap gjennom misbruk av stjålet kortinformasjon i nettbutikker som ikke stiller krav til 3-D Secure-autentisering. Manglende krav til 3-D Secure-autentisering fra netthandelsstedet, men kun krav til bruk av CVC-kode, utgjør en forbrukerrisiko i betalingsformidlingen. Ved tyveri av kortinformasjon er det lett å misbruke denne i netthandelsbutikker som ikke stiller krav til 3-D Secure-autentisering. Stjålet kortinformasjon er en lett omsettelig vare på "det mørke nettet"[24]. Misbruk av stjålet kortinformasjon skjer i all hovedsak utenfor Norge.

For blant annet å motvirke denne trenden, utarbeidet EBA retningslinjer for sikkerhet i Internett-betalinger. Finanstilsynet har kommunisert at disse vil legges til grunn for tilsynsvirksomheten. Retningslinjene trådte i kraft 1. august 2015, (se punkt 5.2.2), og er rettet både mot utstedere og innløsere av betalingskort, men også indirekte mot nettbutikkene. Det reviderte betalingstjenestedirektivet, PSD2 (se punkt 5.1.1), har også bestemmelser for å motvirke denne negative utviklingen.

Selv om finansnæringen i Norge gjennomfører mange tiltak og globalt ligger langt fremme i arbeidet med å redusere sårbarheten, er det fortsatt rom for forbedringer. Fortsatt er bruk av magnetstripe mulig, noe som kan gjøre det enkelt for kriminelle å utnytte stjålet kortinformasjon til svindel.

3.2.7.3 Kostnader forbundet med kortsvindel

Finanstilsynet har utarbeidet et anslag for samlede kostnader forbundet med stjålen kortinformasjon. Beregningen er basert på summen av årlige korttap og en vurdert gjennomsnittlig saksbehandlerkostnad for kortutsteder per misbrukt kort. I tillegg er det forutsatt et kostnadsbeløp per kort knyttet til at forbruker også har kostnader forbundet med stjålen kortinformasjon. (Saksbehandler- og forbrukerkostnader er holdt konstant for årene 2011–2015.)

[22] http://newsroom.hyatt.com/news-releases?item=123453
[23] https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf
[24] https://no.wikipedia.org/wiki/Dypnettet

I tillegg til kostnadene som fremkommer i tabell 3, kommer ytterligere kostnader forbundet med kortsvindel, som blant annet kostnader knyttet til saksbehandling hos kortinnløsere, brukersteder og hos Finansklagenemda samt kostnader knyttet til advokathonorarer og rettskostnader.

Tabell 3: Kostnader forbundet med kortsvindel (beløp i hele tusen kroner)

Kostnader svindel med betalingskort	**2011**	**2012**	**2013**	**2014**	**2015**
Antall kort rammet av misbruk, jf. tabell 2 (antall)	16 784	20 332	22 531	38 541	44 900
Samlede direkte tap, jf. tabell 1	125 718	135 153	140 043	164 113	188 660
Saksbehandlerkostnader kortutsteder (2 250 kroner per kort)	37 764	45 747	50 695	86 717	101 025
Forbrukerkostnader, 1 000 kroner per kort	16 784	20 332	22 531	38 541	44 900
Samlet beregnet kostnad	**180 266**	**201 232**	**213 269**	**289 371**	**334 585**

Kilde: Finanstilsynet

Samlede kostnader forbundet med kortmisbruk er derfor betydelige. Kostnadene ved kortmisbruk øker prosentvis mer enn det totale volumet i korttransaksjoner. I tillegg brukes det betydelige beløp knyttet til preventive tiltak og transaksjons- og svindelovervåkning for å forhindre at kortsvindel skjer.

3.2.7.4 Tapstall knyttet til bruk av nettbank

Som omtalt i punkt 3.9, økte svindel mot nettbank, og særlig mot bedriftsnettbank i 2015, men tapene er ikke store. Tapene kunne blitt langt større hvis ikke bankene hadde klart å stoppe de fleste transaksjonene før de ble gjennomført eller fått pengene tilbakeført fra mottakerbank. På den annen side kan det være rimelig også å inkludere bankenes investeringer i svindelpreventive tiltak (overvåking og etterretning) når totale kostnader vurderes.

Tabell 4: Tap ved bruk av nettbank (tall i hele tusen kroner)

Svindeltype nettbank	**2011**	**2012**	**2013**	**2014**	**2015**
Angrep ved bruk av ondartet programkode på kundens PC (trojaner)	664	5 064	1327	552	3055
Tapt/stjålet sikkerhetsmekanisme	3 321	3 367	1 285	6 655	963
Phishing og falske BankID-brukersteder		10		539	5815
Annet/ukjent		358	779	3474	2715
TOTALT	**3 985**	**8 799**	**3 391**	**11 220**	**12 548**

Kilde: Finanstilsynet

Metodene for svindel av nettbanker endrer seg stadig. Svindeltypene på nettbank er derfor vanskeligere å plassere i entydige kategorier enn svindeltypene på betalingskort.
Tapene grunnet sanntidsfisking, se punkt 3.2.6, fremkommer i raden "Phishing og falske BankID-brukersteder" i tabellen over.

3.2.7.5 Tapstall i andre europeiske land

Tapstall publiseres på ulike tidspunkt i ulike land, og få land publiserer tapstallene så tidlig som Norge. Sammenligningene nedenfor kan derfor være mellom ulike år, men de gir likevel en pekepinn på hvor Norge står.

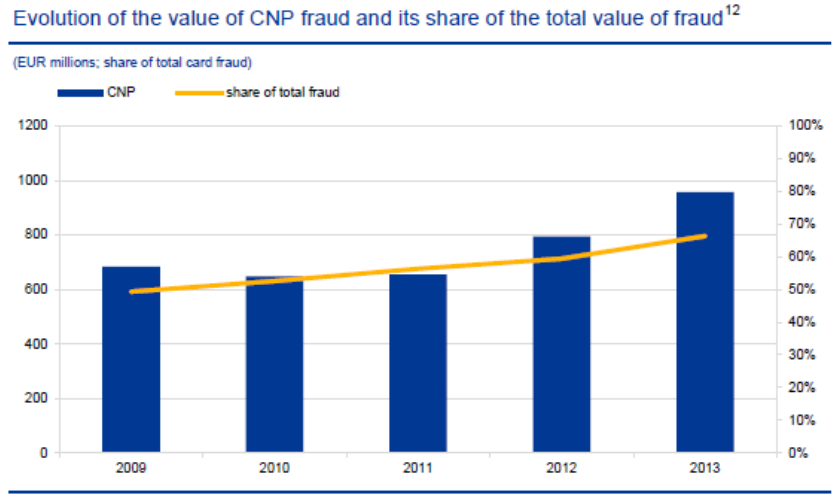
Tap på korttransaksjoner er økende i Norge, slik som ellers i Europa. Tap med CNP øker. Økningen ser likevel ut til å være spesielt stor for Norge, se avsnitt 3.2.7.1, men i Norge er det også stor økning i bruk av kort for handel på Internett. Tap på svindel mot nettbank varierer mer fra land til land. Mens det har vært en økning i Storbritannia og Norge, har man ikke sett det samme i Nederland og Belgia. Det er observert at angrep på nettbank gjerne flytter fra land til land sett over noe tid. Statistikk over tapstall som publisert fra andre land relevante for sammenligning med Norge, er gjengitt nedenfor.

Betalingskort

I den europeiske sentralbankens (ECB) rapport "Fourth report on card fraud"[25] fra juli 2015 framgår det at verdien av svindel med betalingskort i de europeiske landene økte med 8 prosent fra 2012 til 2013. CNP utgjorde 66 prosent av de svindlete verdiene, POS 20 prosent og ATM 14 prosent. CNP-svindel var den eneste typen svindel som økte, men handel på Internett utgjorde samtidig en stadig større del av den totale bruken av betalingskort.

Innenlandske transaksjoner utgjorde 92 prosent av det totale antallet transaksjoner, men bare 49 prosent av svindelen. Grensekryssende transaksjoner innenfor SEPA utgjorde 6 prosent, men 29 prosent av svindelen. Grensekryssende transaksjoner utenfor SEPA utgjorde 2 prosent, men 22 prosent av svindelen.

Figur 2:



Kilde: ECB: Fourth report on card fraud

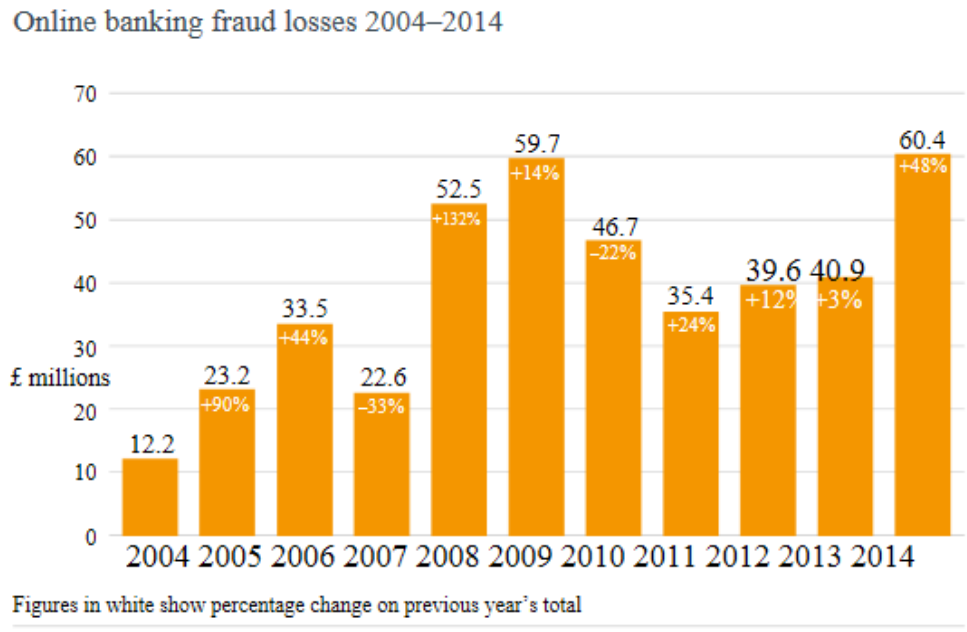
[25] https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf

I Storbritannia[26] økte tap på betalingskort med 6 prosent fra 2013 til 2014. Svindel av typen CNP (omtalt som "Remote purchase" i Storbritannia), økte med 10 prosent. CNP utgjør den desidert største typen svindel både i verdier som er svindlet og antall kort som er misbrukt. Størst er økningen (22 prosent) i CNP ved bruk i utenlandske nettbutikker.

Ved misbruk med falske kort kopieres detaljer fra magnetstripen i kortet. Disse brukes til å produsere falske kort som benyttes i land som ennå ikke har oppgradert til "Chip&PIN". USA er det landet der det benyttes fleste falske kort fra Storbritannia, og falske kort fra USA er hyppigst forekommende av falske kort brukt på nettsteder i Storbritannia.

Nettbank

Figur 3:



Kilde: Financial Fraud Action UK: Fraud The Facts 2015

Nettbanksvindel hadde en betydelig økning i Storbritannia i 2014. Økningen, som var på 48 prosent, forklares med en endring i angrepsmønstre, der den kriminelle gjennom ulike kanaler benytter sosial manipulering og phishing.

Tallene på nettbanksvindel er derimot lave i Belgia[27] og Nederland[28], både for 2014 og 2015.

[26] http://www.financialfraudaction.org.uk/Fraud-the-Facts-2015.asp
[27] https://www.febelfin.be/en/stable-level-internet-banking-fraud-2015-rising-number-bank-card-phishing-cases
[28] http://www.nvb.nl/publicaties-standpunten/publicaties/4522/veiligheid-en-fraude.html

3.3 Bank

Leveransene på IKT-siden blir spredt på flere aktører gjennom nye samarbeidsavtaler og ved endringer i inngåtte avtaler om utkontraktering. Det er økende bruk av eksterne utviklere, gjerne fra lavkostland. Kostnadsbesparelser er en hovedårsak til endringene, men også kjøp av kompetanse er brukt som begrunnelse. På sikkerhetssiden er det imidlertid mangel på kompetanse hos flere av foretakene, noe som på sikt er urovekkende på bakgrunn av forventet vekst i trussel fra nettangrep. På grunn av store endringer skulle en normalt forventet dårligere driftsstabilitet på tjenestene, men det er ikke tilfelle. Foretakene har lagt mye ressurser i disse endringene, og de har holdt kontroll på prosessene.

Finanstilsynet har overfor foretakene påpekt en del områder som bør forbedres. Hovedfunn er omtalt i etterfølgende kapitler.

3.3.1 Oppfølging av "Internet Service Provider" (ISP)

Med sin funksjon som transportvei for utveksling av informasjon, er Internett en kritisk komponent i bankenes produktporteføljе. Foretakenes oppfølging av leverandører av kritisk infrastruktur er viktig for å sikre at etablerte avtaler er relevante og at avtalt service-nivå leveres.

Finanstilsynets erfaring er at ikke alle foretak følger opp tjenesteleveransene fra ISP-leverandører på samme omfattende måte som leveranser fra andre tradisjonelle tjenesteleverandører.

3.3.2 Kontroll av tilganger

Gjennomgang av den enkelte ansattes tilganger til systemer, databaser og filområder er viktig for å verne mot uautorisert tilgang til foretakenes IKT-infrastruktur. Finanstilsynets erfaring fra IKT-tilsyn er at lister som benyttes ved gjennomgang av tilgangsrettigheter er omfattende og utformet i et format og med et innhold som kan gjøre det vanskelig å vurdere hvilke systemer, databaser og filområder den enkelte har tilgang til. Etter Finanstilsynets vurdering bør kvaliteten på tilgangslister forbedres slik at det er lettere for de forretningsansvarlige å gjennomføre gode kontroller. Dette gjelder også for tilganger til applikasjoner med egen tilgangsstyring.

3.3.3 Testmiljø

Finanstilsynet har igjennom IKT-tilsyn erfart at de færreste foretakene har testmiljøer som tilsvarer produksjonsmiljøene. Spesielt mangler det ende-til-ende-testmiljøer. Dette øker risikoen for at testingen ikke i tilstrekkelig grad avdekker svakheter i nye eller endrede løsninger. Videre er det en utfordring å sikre at testingen som utføres, er basert på fastsatte kriterier.

3.3.4 Nett-sikkerhet

Arbeidet med nett-sikkerhet intensiveres samtidig som risikoen for digitale angrep tiltar, men arbeidet er utfordrende siden tilgang på riktig kompetanse og tilstrekkelige ressurser er knapp. Finanstilsynet ser det som positivt at bankenes bruk av penetrasjonstesting synes å øke i omfang.

Gjennom IKT-tilsyn har Finanstilsynet erfart at overvåking av sikkerhetssystem, logg-overvåking, bearbeiding av rapporter fra nettverksutstyr og sikkerhetsnivå er mangelfullt utført. Dette kan medføre at uautorisert aktivitet både fra interne og eksterne kan være vanskelig å oppdage og følgelig også sette inn tiltak mot.

Utpressing er blitt en stadig vanligere trussel, også rettet mot banker. Finanstilsynet er kjent med at banker har mottatt e-poster med krav om løsepenger omtrent samtidig som de utsettes for mindre DDoS-angrep. I e-posten trues det med et sterkere DDoS-angrep dersom løsepengene ikke ble betalt innen fristen. Finanstilsynet er ikke kjent med at løsepenger er betalt i noen av tilfellene, og heller ikke med at angriperne gjennomførte truslene som ble fremsatt. Finanstilsynet mottok også rapporter fra banker som ble utsatt for kryptering (se punkt 3.10.2) av filområder med krav om løsepenger for dekryptering (ransomware). Heller ikke i disse tilfellene er Finanstilsynet kjent med at det ble utbetalt løsepenger. Denne typen angrep er ofte kostbare for bankene, særlig som følge av tapt arbeidstid ved manglende tilgang til systemer og data. Arbeidet med å gjenopprette IKT-systemer og data til normal drift er betydelig og kostbart.

3.3.5 Oppfølging av internrevisjonsrapporter for IKT-området

Internrevisjonen er en viktig del av foretakenes kontrollarbeid. Det er Finanstilsynets erfaring at foretakenes internrevisjonsrapporter på IKT-området i stor grad er grundige og har god kvalitet. Fra tilsynsarbeidet har Finanstilsynet imidlertid merket seg at oppfølging av tiltak som rapportene foreslår og tidspunkter for når tiltakene skal være utført, i flere tilfeller ikke er dokumentert, selv om aktiviteten kan være utført og avsluttet.

3.3.6 Datakvalitet – rapportering til Bankenes sikringsfond

Gjennom tilsynet med etterlevelse av forskrift 22. mars 2013 nr. 330 om krav til datasystemer og rapportering til Bankenes sikringsfond har Finanstilsynet notert seg at bankene i stor grad har etablert løsninger for rapportering i henhold til forskriftens krav. Som et vedlegg til rapporteringen utarbeides det ofte et følgeskriv basert på veiledningen til forskriften. Finanstilsynet har bedt bankene om å legge noe mer arbeid i følgeskrivet for bedre å kunne forberede eventuelle utbetalinger fra Bankenes sikringsfond.

Tilsynene viste noen kvalitetsmessige mangler i informasjonsleveransene som kunne fått konsekvenser ved en utbetaling fra Bankenes sikringsfond. Etterkontroll av listene til sikringsfondet er viktig for å sikre at leveransen til Bankenes sikringsfond er fullstendig, slik at alle kunder og korrekte data kommer med i uttrekket fra bankenes systemer.

3.4 Verdipapirområdet

Finanstilsynets generelle inntrykk av IKT-systemene i den norske verdipapirsektoren er at systemene har god kvalitet og høy stabilitet. Utfordringen fremover blir å sikre et fortsatt akseptabelt risikonivå

med de teknologiske endringene som Finanstilsynet ser komme i kombinasjon med sektorens stadig økende utkontraktering av IKT-systemer.

3.4.1 Informasjonslekkasjer

Å hindre informasjonslekkasjer fra verdipapirforetakenes corporate-avdelinger og bankenes markets-avdelinger er viktig for foretakene, foretakenes kunder, og for tilliten til norsk finanssektor. En sentral kilde til denne type informasjonslekkasjer ligger i bankenes og verdipapirforetakenes IKT-systemer og krever derfor effektiv sikring mot uautoriserte tilganger.

3.4.1.1 Sviktende kontroll ved utkontraktering

Også på verdipapirområdet har omfanget av utkontrakterte IKT-systemer økt de siste årene. Kravet til kostnadsreduksjon for drift og kostnadsdeling av spesialiserte løsninger kombinert med en stadig hurtigere systemutviklingstakt resulterer i at stadig flere verdipapirforetak utkontrakterer større deler av sin systemportefølje. Utviklingen stiller nye krav til foretakenes ledelse om høy kvalitet på risikoanalysene som gjennomføres forut for slike beslutninger. IKT-forskriften stiller krav om at foretakets mulighet for styring og kontroll med utkontrakterte løsninger ikke forringes sammenlignet med om løsninger forvaltes, utvikles og driftes av selskapet selv.

IKT-forskriftens utkontrakteringsparagraf peker også på at foretaket skal ha ubegrenset adgang til å kontrollere, revidere og føre tilsyn med alle elementer som er av betydning for den utkontrakterte systemleveransen. For verdipapirforetak har Finanstilsynet registrert utkontraktering av IKT-systemer med kurssensitive data hvor foretaket verken fører kontroll med driftsselskapenes brukere, eller har sikret i avtalen med leverandøren mulighet til å motta og kontrollere informasjon om hvilke driftspersoner som har hatt tilgang til dataene. Dette kunne for eksempel ha vært løst ved at systemer som kjøres på en utkontraktert plattform benytter kryptering styrt av foretaket selv, mens plattformen driftes av leverandøren.

3.4.1.2 Manglende klassifisering av sensitiv informasjon

Finanstilsynet har gjennom sine tilsyn merket seg at mange verdipapirforetak har manglende eller svake retningslinjer og rutiner for klassifisering av sensitiv informasjon. Dette kan resultere i redusert sikkerhet ved informasjonsutveksling og lagring av denne typen informasjon. Særlig er dette viktig for avdelinger som håndterer kurssensitiv informasjon, slik som verdipapirforetakenes corporate-avdelinger.

3.4.1.3 Mangelfull sikkerhet i epostutveksling

Gjennom sin tilsynsaktivitet har Finanstilsynet erfart at verdipapirforetak ofte mangler tilstrekkelig bevissthet på sikkerhet ved bruk av epost. For å oppnå et relevant sikkerhetsnivå for epost, vil det ikke være tilstrekkelig å etablere brukerrutiner og gjennomføre informasjonskampanjer. Foretaket må også ha kontroll med hvordan foretakenes epostservere er konfigurert.

Epostservere settes ofte opp med kryptering på en slik måte at serveren forhandler med motpartsserveren om hvilket krypteringsnivå som skal benyttes under en overføring. I de tilfeller

motpartsserveren ikke støtter kryptering, kan en kryptert epost likevel bli sendt ukryptert uten at avsenderen er klar over det eller gis mulighet til å stanse overføringen (opportunistisk kryptering). I foretak som regelmessig utveksler sensitiv informasjon med en motpart, kan kommunikasjonen sikres ved å inngå avtaler om et fastsatt graderingsnivå på krypteringen. Foretaket kan også konfigurere eposttjenerne slik at man kun kan sende og motta krypterte meldinger fra spesifikke motparter (tvungen kryptering). De fleste epostsystemer har mulighet for å verifisere identiteten til motpartens epostserver ved hjelp av tvungen bruk av sertifikater.

Finanstilsynet har også registrert lav bevissthet om risikoen forbundet med at en epost på veien fra sender til mottaker kan passere flere epostservere og nettverksknutepunkt (SMTP-servere), og at epost her kan leses i klartekst. Dette er mulig siden det er kommunikasjonen, ikke selve meldingen som krypteres. Slik kryptering beskytter bare mot "avlytting" av linjene.

Der det kreves høy grad av konfidensialitet i en epostforsendelse bør meldinger inklusive vedlegg krypteres før sending.

3.4.1.4 Bruk av tredjepartssystemer for informasjonsutveksling

Verdipapirforetakene mangler i stor utstrekning retningslinjer for bruk av tredjepartsløsninger som benyttes til utveksling av sensitiv informasjon. Tredjepartsløsningene kan være prosjektverktøy, skybaserte filsystemer eller andre tilsvarende løsninger som oppdragsgiver foretrekker og som ofte benyttes uten at verdipapirforetaket gjennomfører relevante risikoanalyser eller stiller sikkerhetskrav til løsningene. Et verdipapirforetak er en profesjonell part i et samarbeid og har ansvar for sikker kommunikasjon av sensitiv informasjon. Foretak bør ha rutiner for, og beskrivelser av, hvordan slik kommunikasjon skal utføres. Rutinene bør differensieres ut fra informasjonstyper og deres tilhørende sikkerhetskrav.

3.4.2 Overvåking av lydopptakssystemer

Verdipapirforskriften setter krav om gjennomføring av lydopptak i verdipapirforetak. I løpet av 2015 har Finanstilsynet registrert flere hendelser som har medført at lydopptakene ikke er gjennomført grunnet teknisk svikt i opptaksutstyret. Flere av disse hendelsene har vart over lengre tid uten at dette har blitt oppdaget av foretaket. Dette viser at foretakene har hatt svake rutiner for kontroll av opptaksoperasjonen og mangelfull elektronisk overvåking av opptakssystemene. Finanstilsynet vil nå se nærmere på foretakenes kontroll med systemer for lydopptak og deres rutiner for overvåking av disse.

3.4.3 Utkontrakterte ordresystemer

Flere større fonds- og kapitalforvaltningsselskaper samt en del meglerselskaper benytter seg i dag av løsninger fra tredjepartsselskaper for å håndtere ordreflyt mellom forvaltere og meglere. Markedet for denne type løsninger preges av få og store utenlandske aktører. Felles for disse løsningene er at de behandler kurssensitiv informasjon, og at oppgavene som utføres tidligere ble utført av verdipapirforetakene selv. Finanstilsynet anser derfor bruk av denne type tredjepartsløsninger som en utkontraktering av IKT-systemer.

Finanstilsynet har gjennom sitt tilsynsarbeid avdekket mangelfulle avtaler mellom verdipapirforetak og løsningsleverandører av utkontrakterte ordresystemer med tanke på krav om foretakets tilgang til å kontrollere og revidere leverandørens aktiviteter knyttet til avtalene.

3.4.4 Leverandørers leveringskapasitet i kritiske situasjoner

Tester av beredskapsløsninger og oppståtte hendelser har vist at beredskapsavtaler med infrastrukturleverandører om forhåndslagring av utstyr ikke er en garanti for at man får tilgang til utstyr som avtalt i en krisesituasjon. Mange verdipapirforetak har valgt samme produkt fra samme leverandør og har tegnet avtaler om beredskapslagring av ekstra komponenter hos den samme leverandøren. Finanstilsynet anser det som en risiko at leverandørene har et lavere antall av hver komponent på nærlager enn hva leverandøren totalt har avtalt med sine kunder, basert på en vurdering om at det er mindre sannsynlig at alle komponentene må skiftes for alle foretakene samtidig. Ved situasjoner der flere foretak får problem med sine komponenter samtidig (ved f.eks. feil i strømnettet), kan leverandørene få problemer med å oppfylle sine forpliktelser. Verdipapirforetaket vil i tilfelle ikke kunne levere forventet driftssikkerhet. Verdipapirforetakene må derfor ta dette inn som en faktor i risikovurderingen av egen IKT-infrastruktur.

3.4.5 Risikovurderinger og systemeierskap

Finanstilsynet har ved flere tilsyn notert seg at verdipapirforetakenes ledelse har vist manglende engasjement i foretakenes IKT-virksomhet. Finanstilsynet har observert tilfeller der IKT-avdelingen oppgis som formelle systemeiere til foretakets kjernesystemer uten at det eksisterer retningslinjer for, eller at det kan dokumenteres at beslutninger gjøres i samråd med selskapets øvrige ledelse. Dette kan resultere i at risikoanalyser som gjennomføres for foretakets IKT-systemer mangler en helhetlig og forretningsmessig dimensjon, samt at foretakets ledelse taper oversikt over foretakets IKT-risiko

Manglende involvering av verdipapirforetakenes ledelse i utkontrakteringen av foretakets IKT-virksomhet har resultert i kontrakter med manglende regulering av tilgang til foretakenes data. Det kan øke risikoen for informasjonslekkasjer. Et eksempel er et foretak som utkontrakterte drift av systemer med kurssensitiv informasjon. Informasjonen ble gjort tilgjengelig for driftspersonalet hos leverandøren i form av brukertilganger. Leverandøren ga administratorrettigheter med tilgang til foretakets sensitive data til mange av sine ansatte, mens verdipapirforetaket selv manglet muligheten til å overvåke hvilke personer som hadde tilgang til disse systemene. Loggføring av aksess til sensitive data var ikke implementert og leverandørens administratorer hadde i tillegg rettigheter til å slette digitale spor. Verdipapirforetaket har dermed ingen oversikt over hvem som eventuelt har aksessert de sensitive dataene og vet heller ingenting om hvordan denne informasjonen kan ha blitt brukt.

3.4.6 Ransomware-angrep

Finanstilsynet har registrert at verdipapirforetakene gjennom 2015 har opplevd tilfeller av phishing som resulterte i cryptolockerangrep, se punkt 3.10.2. Foretak har fått sine nettverksdisker kryptert og mottatt krav om løsepengebetaling i Bitcoin. Dette har medført driftsavbrudd med varighet på mer enn ett døgn på grunn av utilgjengelige nettverksdisker. Hendelsene viser at selv med godt proaktivt arbeid

for å unngå cryptolockerangrep, er en likevel avhengig av den reaktive sikkerheten i form av systemer for sikkerhetskopiering, fungerende rutiner og testet beredskap.

3.5 Forsikring

Noen forsikringsforetak er en del av større bank- eller forsikringskonsern, mens andre er frittstående foretak. Flere foretak har nært samarbeid med banker og benytter bankenes distribusjons- og salgsnett. Størrelsen på foretak ene og hva de tilbyr av produkter varierer. Forskjellene gjenspeiles i foretakenes bruk av IKT, organisering av IKT-virksomhet og IKT-risikobilde.

Foretakene utkontrakterer i stor grad IKT-virksomhet, noe som synes å være en økende trend. Foretakene er innovative når de gjelder å ta i bruk ny teknologi i sine løsninger. Som andre finansforetak, er forsikringsforetakene mål for eksterne dataangrep, et område som krever kontinuerlig oppmerksomhet og tilstrekkelig ressurser (jf. punkt 3.10).

Gjennom tilsyn er det avdekket risikoområder som bør vies økt oppmerksomhet, se omtale nedenfor.

3.5.1 Risiko ved komplekse forsikringssystemer

Som Finanstilsynet har beskrevet i tidligere risiko- og sårbarhetsanalyser, har forsikringsbransjen generelt mange, store og komplekse systemer med mye forretningslogikk, tunge forsikringstekniske beregninger og med grenseflater mot mange andre systemer. Feil og mangler i systemene kan få konsekvenser for selskapenes regnskap og kundenes premier og erstatninger.

Som det fremgår av punkt 5.2.4, er forsikringssektoren gjenstand for mange regelverksendringer. Disse medfører behov for betydelige endringer i IKT-systemene. Selskapenes kompetanse om de enkelte systemene, kvaliteten på IKT-prosessene som benyttes ved endringer, og etterlevelse av disse er av stor betydning for å sikre kontroll med endringene og at kvaliteten på systemene ikke blir forringet ved endringer.

Flere foretak kjøper fagsystemer fra eksterne leverandører, og hvor leverandøren utfører systemendringene. Finanstilsynet legger til grunn at foretakene, i tråd med risikostyringsforskriftens og IKT-forskriftens krav til utkontraktering, har tilstrekkelig kompetanse om systemene, tar aktivt del i, og tar ansvar for endringene som gjennomføres.

3.5.2 Manglende etterlevelse av IKT-forskriftens krav om å rapportere hendelser

Finansforetak skal etter IKT-forskriftens § 9 "Avviks- og endringshåndtering" rapportere til Finanstilsynet hendelser som medfører vesentlig reduksjon i funksjonalitet som følge av brudd på konfidensialitet, integritet eller tilgjengelighet til IKT-systemer og/eller data. Av 148 hendelser som ble rapportert i 2015 var 14 fra forsikringsforetak. Dette er en økning fra året før. Finanstilsynets

Hendelsesseminar 2014 var spesielt rettet mot forsikringsforetakene, og dette kan ha hatt en viss effekt.

Etter IKT-forskriften skal rapportering til Finanstilsynet normalt omfatte hendelser som foretakene selv kategoriserer som alvorlige eller kritiske. Det fremgår imidlertid av forskriften at rapporteringen også kan omfatte andre avvik dersom disse avdekker sårbarhet i applikasjon, arkitektur, infrastruktur eller forsvarsverk. Jevnt over er dette et punkt ikke alle foretak er klar over. Finanstilsynet ser ikke bort fra at det kan ha vært avvik som følge av sårbarheter i forsikringsforetakenes applikasjoner som burde vært rapportert til Finanstilsynet.

3.5.3 Mangelfulle Risikovurderinger

Mange forsikringsselskaper har fremdeles behov for å utarbeide bedre og mer helhetlige risikoanalyser, som viser den samlete risikoen ved selskapets bruk av IKT. Mangelfulle og fragmenterte risikovurderinger gjør det vanskelig å styre selskapets IKT-risikoer og sikre at disse er innenfor fastsatte rammer og at selskapet når sine mål og strategier.

3.6 Regnskapsførerselskaper

Finanstilsynet gjennomførte i 2015 et dokumentbasert tilsyn med regnskapsførerselskaper. Formålet med tematilsynet var å kartlegge IKT-risikoen i autoriserte regnskapsførerselskaper, øke bevisstheten rundt IKT-risiko i regnskapsførerbransjen og styrke etterlevelsen av risikostyringsforskriften og god regnskapsføringsskikk.

Regnskapsførerselskaper benytter i stor grad maskin- og programvareteknologi i virksomheten. Det kan få stor betydning for oppdragsgiverne dersom disse hjelpemidlene svikter. IKT-risikoen skal håndteres i samsvar med risikostyringsforskriften. Svarene i tematilsynet viser at ikke alle regnskapsførerselskaper etterlever forskriften.

Det er viktig at regnskapsførerselskapene ikke oppfatter risikostyringsforskriften som et "formalkrav", fordi forskriften da ikke virker etter sin hensikt. Det er bare dersom det gjøres reelle vurderinger, ut fra den faktiske situasjonen i det enkelte regnskapsførerselskapet, at forskriften vil være et hjelpemiddel for styret og daglig leder til å ivareta det ansvaret de har etter regnskapsførerloven, selskapslovgivningen og annen relevant lovgivning. Etterlevelse av forskriften vil bidra til en forsvarlig risikostyring og internkontroll med hele regnkapsførerselskapets virksomhet, herunder IKT-driften, enten den er utkontraktert eller ikke. Resultatene fra tematilsynet tilsier at en del regnskapsførerselskaper må gjøre grundigere vurderinger av behovet for å iverksette tiltak som kan redusere risikoen knyttet til de IKT-systemene som benyttes i virksomheten. Tiltak som skal iverksettes etter lovkravet om "god regnskapsføringsskikk" (GRFS-standarden), må gjennomføres.

Tematilsynet gir også grunn til å tro at foreliggende avtaler mellom regnkapsførerselskapene og leverandører av IKT-systemer som selskapene benytter i sin virksomhet, ikke i tilstrekkelig grad gir

regnskapsførerselskapene de rettighetene som er nødvendige for at de skal kunne oppfylle sine plikter etter lovgivningen, herunder ansvaret for risikostyring og internkontroll.

3.7 Fellestiltak innen finansnæringen

Banker, andre sentrale aktører i finanssektoren og Finans Norge samarbeider om sikkerhet, utvikling av felles infrastruktur, tjenester og felles standarder. Resultater fra hendelser, overvåking, analyser og statistikk utveksles og drøftes, og tiltak besluttes.

Finansnæringen vedtok i 2015 å samle arbeidet innen betalingsformidling i et nytt og styrket infrastrukturselskap – Bits[29]. Bankenes standardiseringskontor (BSK) og Finans Norges fagenhet for betalingsformidling inngår i det etablerte selskapet, som var operativt fra 1. april 2016.

Finansnæringens rom for selvregulering endres gjennom endringer i lover og forskrifter, ikke minst påvirket av endringene som skjer i regi av EU. Det vil medvirke til at finansnæringen i sin samhandling må åpne for nye aktører i betalingsformidlingen (se punkt 5.1.1).

BSK har arbeidet med å modernisere Baltus, noe som vil gi en fleksibel og sikker infrastruktur for ruting og transport av transaksjonsrelaterte finansielle forespørsler mellom bankene tilknyttet den felles norske infrastrukturen. Løsningen ble tatt i bruk i 2015. Etter planen skal alle banker ta i bruk den nye infrastrukturen i løpet av 1. halvår 2016.

Arbeidet med overgang til ISO 20022 fortsetter. Arbeidet vil medføre vesentlige endringer for norsk betalingsinfrastruktur de nærmeste årene. Det er viktig at dette arbeidet skjer på en koordinert og kontrollert måte for å ivareta både sikkerhet og stabilitet på en god måte.

Finansnæringen har arbeidet med å forbedre identitetskontrollen ved utlevering av kodebrikker som benyttes sammen med BankID, både gjennom bruk av Postens PUM-tjeneste og i bankenes egne rutiner. Tiltakene forventes iverksatt i løpet av 2016.

FinansCERT er etablert som en privat sektor-CERT og er et viktig instrument for finanssektoren i arbeidet med digitale trusler og hendelser. I tillegg til å være et operativt koordinerende ledd mellom finansforetakene i dette arbeidet, har FinansCERT arbeidet aktivt med relasjoner til og samarbeidsavtaler med andre sentrale aktører på sikkerhetsområdet både nasjonalt og internasjonalt. For at arbeidet med digitale trusler og hendelser innen finanssektoren skal bli mest mulig effektivt, er det av stor betydning at samarbeidet mellom offentlig og privat sektor blir så smidig og hensiktsmessig som mulig.

[29] https://www.fno.no/aktuelt/nyheter/2016/03/bits-i-drift-fra-1.-april/

Etter etableringen av BankAxept i 2014 har selskapet bygd opp organisasjonen, samtidig som det er arbeidet med å modernisere det norske kortsystemet for blant annet kontaktløs betaling og nye digitale tjenester.

3.8 Endringer og utkontraktering

3.8.1 Endringer i leverandørmarkedet

I forbindelse med salg/eierbytte hos tjenesteleverandørene er det viktig at etablerte prosedyrer og samarbeidsrutiner tilpasses og forankres hos nye partnere. Primært er det finansforetakene som må se til at dette blir fulgt opp. Det gjelder også om det er en leverandør som får ny underleverandør.

Salg av **Evry**[30] ble gjennomført i 2014, og Evry har i 2015 inngått outsourcingavtale for driften av sin stormaskin med IBM. Driftssenteret Greenfield Data Center er lagt til Fet, Akershus.

Nets filialiserte virksomheten i 2015, og Norge ble en filial av Nets-konsernet i Danmark. Driften forblir i Norge. Nets Norge Infrastruktur AS, som blant annet drifter bankenes avregningssystem NICS, er fortsatt et eget norsk selskap.

Sandnes Sparebank gikk i 2015 inn i Eika Alliansen og flyttet i oktober 2015 sin IKT-drift til Eikabankenes driftsmiljø hos Eika Alliansen og SDC.

DNB valgte i 2013 HCL som ny driftspartner for drift av desentral plattform. I 2015 har DNB gjennomført flytting av serverparken (ikke stormaskin) til Green Mountain DC1 på Rennesøy, Rogaland, og er i gang med å etablere backup-sted for stormaskin der, og backup-sted for serverparken i Green Mountain DC2 på Rjukan, Telemark.

For deler av systemporteføljen har DNB inngått utviklings-/ vedlikeholdsavtaler med Infosys og TCS (Tata Consultancy Services).

Nordea har tatt tilbake all drift som tidligere ble levert av Nordic Processor, unntatt kjerne-drift av stormaskin (HW/OS), som fremover vil bli levert til Nordea av henholdsvis IBM og HP. Dette innebærer at Nordic Processor avvikles.

Store deler av serverparken (mid-range) med tilhørende systemer, er allerede flyttet fra IBM/NP sine datahaller i Solna og Kista, og inn til egne datahaller i Danmark.

Nordea har også startet et prosjekt for fornying av kjernesystemene. Systemer fra Temenos er valgt, som implementeres i samarbeid med Accenture.

[30] Omtalt i ROS-rapporten for 2014.

3.8.2 Utkontrakteringsmeldinger

Finanstilsynet har i 2015 mottatt over 100 meldinger om utkontraktering etter finanstilsynsloven § 4c.

På bakgrunn av variasjoner mellom foretakene i vurderingen av hva som skal meldes og betydelige variasjoner i mottatte meldinger, ser Finanstilsynet at det kan være behov for å gi nærmere presisering av når meldeplikten inntrer og hvordan meldingen skal utformes.

Finanstilsynet har i tidligere års ROS-analyser påpekt at tilsynet anser at bruk av skytjenester faller inn under reglene som gjelder tradisjonell utkontraktering. Finanstilsynet mottok i 2015 meldinger fra foretak som ønsket å ta i bruk løsninger fra store globale leverandører av skytjenester. Norsk finansnæring, særlig banker, har i flere tiår utkontraktert sine IKT-løsninger, og i stor grad har løsningene vært delt mellom flere foretak. I prinsippet er dette samme type løsninger som i dag omtales som skyløsninger. Forbedret teknologi har gjort det enklere for tjenesteleverandørene å tilby denne type leveransemodeller og dermed tilby både infrastruktur, plattform og programvareløsninger samlet eller hver for seg, og om ønskelig kan dette leveres av en tjenesteleverandørs datasentre på ulike geografiske steder.

Ved vurdering av meldingene om utkontraktering legger Finanstilsynet vekt på om foretaket har utført risikoanalyse og selvstendig vurdering av utkontrakteringsforholdet. Gjennom behandling av utkontrakteringsmeldingene har tilsynet erfart svakheter både når det gjelder gjennomførte risikoanalyser, foretakets selvstendige vurderinger av utkontrakteringen og etterlevelse av gjeldende lover og forskrifter. Finanstilsynet har blant annet fulgt opp meldinger der avtalene ikke tar tilstrekkelig hensyn reguleringskrav som IKT-forskriftens eller internkontrollforskriftens krav om at foretak under tilsyn skal gis rett til å kontrollere, herunder revidere, de av leverandørens aktiviteter som er knyttet til avtalen.

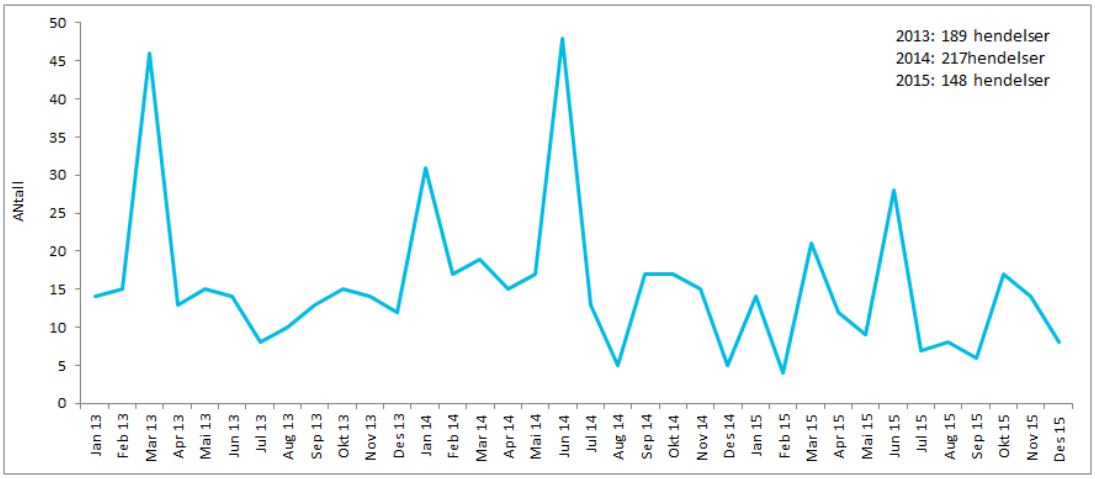
3.9 Rapporterte hendelser i 2015

Finansforetakene er i henhold til IKT-forskriften pålagt å rapportere alvorlige hendelser i IKT-systemene. Finanstilsynet følger opp at hendelsene analyseres av foretakene, og at rotårsak og mulige preventive tiltak klarlegges. Finanstilsynet krever også ved spesielt alvorlige hendelser en plan for gjennomføring av de preventive tiltakene. Generelt følges hendelser og preventive tiltak opp ved tilsyn.

3.9.1 Statistikk over hendelser

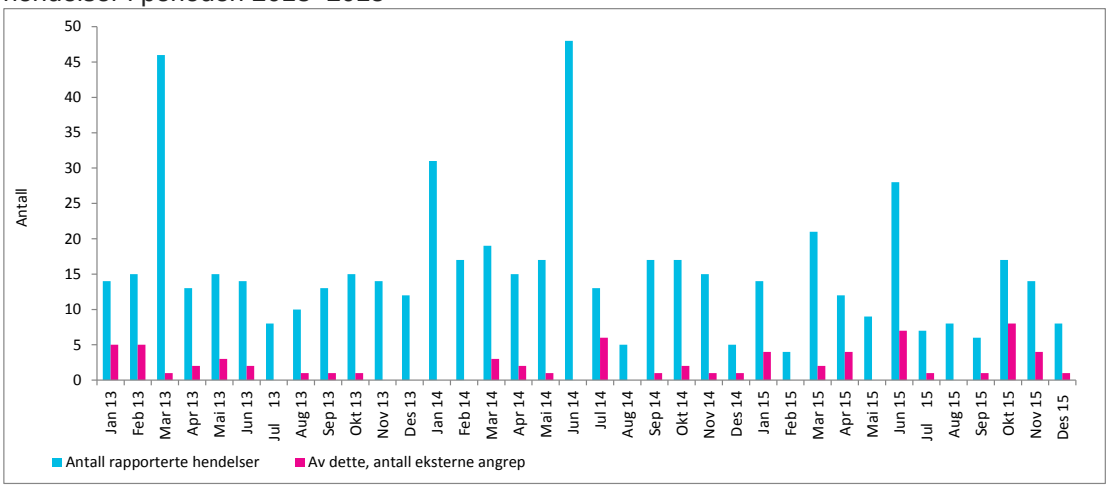
Statistikken nedenfor er basert på rapporter fra foretakene. Det var færre rapporterte driftshendelser og høyere tilgjengelighet til teknologiavhengige finanstjenester i 2015 enn i årene før. Derimot økte svindelangrepene mot finansforetakene. Selv om dette i liten grad påvirket den totale tilgjengeligheten, var angrepene til stor ulempe for kundene og foretakene som ble rammet.

Figur 4: Antall rapporterte hendelser i perioden 2013–2015



Kilde: Finanstilsynet

Figur 5: Antall rapporterte eksterne angrep (ondsinnede angrep) og totalt antall rapporterte hendelser i perioden 2013–2015



Kilde: Finanstilsynet

Årsakene til driftshendelsene kan grovt deles inn i hhv. feil etter endringer, mangelfull kapasitetsplanlegging eller svikt i overvåking av parametere som utløpsdatoer, fyllingsgrader og terskelverdier. Det er stadig et forbedringspotensial ved både selve prosedyrene og ved at prosedyrene brukes slik de skal.

Hendelser som rammet BankID i mai og juni, og dermed mange finansforetak samtidig, representerte de alvorligste driftshendelsene i 2015. Hendelsene rammet særlig bankene og betalingsformidlingen. Dette var flere hendelser med ulike årsaker, men ingen var etter Finanstilsynets vurdering kritiske for tilgangen til finanstjenestene.

Det ble registrert flere nettverkshendelser som påvirket mobile tjenester, inkludert BankID. Konsekvensen av feil i mobilnettet er økende, siden stadig flere tjenester baserer seg på at nettverksinfrastrukturen for mobile tjenester er tilgjengelig.

Globale endringer i Internett påvirket norske betalingstjenester og BankID i juni 2015. Nettverket for deler av den norske betalingsinfrastrukturen var ustabilt på grunn av en endring som ble utført av en teleleverandør i Malaysia. Årsaken var en feil i adressetabeller. Den aktuelle teleleverandøren hadde ikke god nok kontroll med hvilke adresser som tilhørte hvilke kunder.

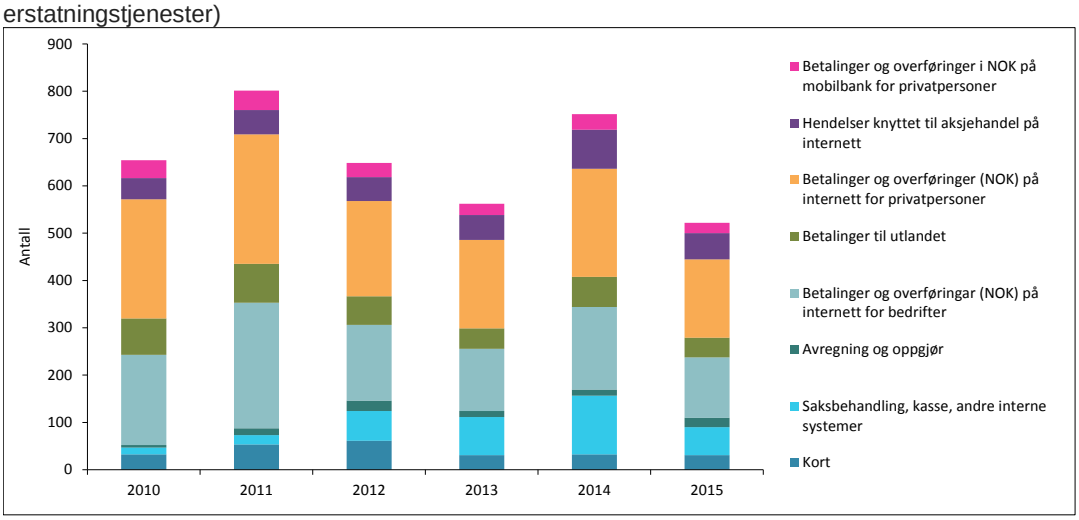
Svindel mot nettbanktjenestene økte i 2015, og særlig mot bedriftsnettbank der transaksjonsbeløpene er større, se punkt 3.2.6. Både banker, forsikringsforetak og verdipapirforetak rapporterte i 2015 om angrep med ransomware, se punkt 3.10.2.

For forsikringsforetakene gjaldt de fleste hendelsesrapportene applikasjonsfeil etter endringer. Nest-hyppigst var driftsproblemer. På verdipapirområdet var de fleste hendelsene knyttet til driftsproblemer, hvorav flere gjaldt tap av opptak av telefonsamtaler.

3.9.2 Analyse av hendelsene som mål på tilgjengelighet

For hver hendelse som har rammet tilgjengeligheten, har Finanstilsynet vurdert avbruddets lengde, antall foretak som er berørt, anslagsvis hvor mange kunder som er rammet og om det eksisterer erstatningstjenester som kunden kan benytte. På denne måten får Finanstilsynet en indeks for utilgjengelighet til betalingssystemet og kunderettede løsninger år for år, og kan dermed følge utviklingen over tid.

Figur 6: Hendelser vektet med konsekvens (vekter: berørte brukere, varighet, tidspunkt, erstatningstjenester)



Kilde: Finanstilsynet[31]

[31] I den grafiske fremstillingen er utilgjengeligheten for aksjehandel på Internett rekalibrert for alle år i figuren, fordi foretakene rapporterer at de har gode erstatningstjenester for tilfellet at aksjehandel på

Figur 6 viser at betalingssystemet og kunderettede løsninger var mer tilgjengelige for kundene i 2015 enn i 2014. Dette til tross for at flere foretak skiftet driftssted og leverandør i 2015, noe som innebærer en viss risiko for nedetid i overgangen. Foretakene er nå spredt på flere driftsleverandører enn tidligere. Alt annet likt, vil dette gi mindre risiko for at mange foretak er utilgjengelige samtidig.

3.10 Observasjoner av digital kriminalitet (Cybercrime)

Digital kriminalitet retter seg både mot foretak og mot kunder. Foretakene rammes av DDoS- og APT-angrep, kundene infiseres med ondsinnet kode i egen datamaskin. Et stadig mere sentralt element i den digitale kriminaliteten er fisking av informasjon. Fisking av informasjon rettes både mot foretak og sluttkunder. Å oppnå offerets tillit er et viktig element i svindlerens verdikjede. For å komme til de store beløpene, profesjonaliseres fiskingen med målrettede henvendelser fra noen som gir seg ut for å være navngitte bekjente/kollegaer av offeret. Kanaler for fiskingen kan være telefon, e-post, SMS eller telefon med forhåndsdefinerte svaralternativ (såkalt interactive voice response (IVR)). Metodene kan bli brukt alene eller i kombinasjon.

3.10.1 CEO Fraud

CEO Fraud er angrep der en ansatt, ofte med økonomiansvar, blir kontaktet via telefon og/eller e-post av det som tilsynelatende er øverste leder, men som i virkeligheten er en svindler. Den ansatte blir bedt om å gjennomføre spesifikke pengetransaksjoner. Av hensyn til markedet blir det bedt om at transaksjonene skal være konfidensielle. Dette gjør det lettere å lykkes med svindelen. Angrepene retter seg mot ulike typer foretak.

Ved CEO Fraud er det ofte svært store beløp som overføres. Som ved nettbanksvindel, er det behov for muldyrkontoer for mottak av svindeltransaksjonene. Transaksjonene går oftest til utlandet, og gjerne til land hvor det er vanskelig å spore dem. CEO Fraud rammer alle typer foretak, og banker rammes direkte når en ansatt i en bank er offeret. Bankene kommer også i nær befatning med svindelen når bedriftskunder av banken rammes, fordi de store svindel-transaksjonene overføres gjennom banken. CEO Fraud som har lyktes har medført store tap for bedriften som ble svindlet. Det er ingen grunn til å tro at CEO Fraud vil avta med det første og antagelig øke i omfang angrep, særlig rettet mot bankenes kunder i årene framover.

Flere land i Europa har vært utsatt for tilfeller av CEO Fraud[32], og slike angrep ser ut til å øke. Svindelscenarier som oppstår andre steder i Europa, kommer ofte etter en tid til Norge.

Internett er nede. Erstatningstjenestene består av at foretakene på kort tid bemanner opp, slik at de kan ta imot og utføre ordrer manuelt.

[32] http://www.investopedia.com/terms/c/corporate-fraud.asp

3.10.2 Ransomware

Ransomware er betegnelse på en type skadevare som infiserer systemene, og resulterer i krypterte harddisker. Deretter kreves løsepenger for å reetablere dem. Inngangsporten er oftest falske e-poster (phishing) med en lenke til skadevaren.

Både norske banker, forsikringsforetak og verdipapirforetak ble utsatt for angrep med ransomware i 2015, i tillegg til foretak i andre sektorer. Finanstilsynet har observert at angrepene fikk størst konsekvenser for mindre foretak, mens forsvarsmekanismer i større finansforetak var mer effektive til å avgrense skadene.

Cryptolocker er et eksempel på ransomware. Både selve skadevaren og den forutgående phishingen kan være vanskelige å oppdage og avvise med hjelp av antivirus og epostfiltrering, fordi avsender, tekster og lenker til stadighet endres. Tekstene som benyttes i eposten for å få brukere til å laste opp krypteringsmakroene har også blitt mer troverdige og slipper derfor lettere igjennom forsvarsverket foretakene kan bygge opp gjennom rutiner, opplæring og holdningskampanjer. Hendelsene viser at uansett hvor mye man legger ned i proaktivt arbeid for å unngå cryptolockerangrep, så vil man likevel være avhengig av den reaktive sikkerheten som bygges opp i form av systemer for sikkerhetskopiering, fungerende rutiner og testet beredskap.

3.10.3 Trojaneren Dyre

Dyre-viruset (også kalt Dyre/Dyreza), er en bank-trojaner designet for å stjele påloggingsinformasjon fra sine ofre ved å videresende all trafikk til og fra nettbanken til de kriminelles servere. Slik kan de endre hva brukeren ser i nettleseren, og samtidig stjele penger fra bankkontoen. Den kan også omdirigere brukeren til farlige og usikre nettsider hvor datamaskinen deres blir infisert med andre nett-trusler som kan brukes til kriminelle handlinger.

Denne type angrep kalles MITM (Man-in-the-middle) og hvor SSL-beskyttelsen mot nettbanken omgås. Dyre-trojanen er også i stand til å laste ned og starte tilleggsmoduler som gir den kriminelle økt kontroll på den infiserte PCen. Dyre-viruset spres stort sett via uønsket e-post (spam-kampanjer), og infiserer PCen enten via vedlagte filer eller via lenker en blir lurt til å klikke på.

Norske nettbankkunder ble i 2015 utsatt for angrep av Dyre, spesielt utformet for en bestemt bank.

3.10.4 Målrettede politiaksjoner lykkes

Dyre herjet i 2015 mange land i Europa. Bakmennene bak trojaneren ble arrestert i en koordinert politiaksjon i Moskva november[33] i 2015. Etter dette er det p.t. ikke registrert Dyre-angrep verken i Norge eller andre land. Den samme utviklingen så man i 2012, da den spesielle politienheten som jobber med cyberkriminalitet i Storbritannia slo til mot en organisert liga som sto bak et omfattende

[33] http://www.reuters.com/article/us-cybercrime-russia-dyre-exclusive-idUSKCN0VE2QS

botnet. Antall identifiserte falske nettsteder som kilde til phishing ble i løpet av en måned redusert til en tiendedel[34].

3.11 Blockchain

Blockchain er en digital logg av transaksjoner som inneholder eierrettigheter eller andre typer avtaler. Ved distribuerte Blockchain'er er loggen direkte styrt og kontrollert av deltakerne i transaksjonen eller rettighetshavere, uten at en sentral instans er involvert. Det er stor interesse for å ta i bruk Blockchain-teknologien innenfor finanssektoren.

Denne teknologien gjør det mulig å overføre eierskap til verdier i løpet av sekunder, uten sentral motpart og med minimale kostnader. Transaksjonene lagres i en distribuert logg av blokker som inneholder alle transaksjonene. Transaksjonene er digitalt signert, og deltakerne i nettverket må godkjenne transaksjonene. En har også sentraliserte Blockchain'er, der en sentral aktør står for godkjenning av transaksjoner.

I dag benyttes Blockchain i all vesentlighet i forbindelse med krypto-valuta. Fordelen er lave transaksjonskostnader og mulighet for å realisere straks-betalinger på en praktisk måte. Innvendingene har vært at krypto-valutaen er uregulert, noe som har ført til store og uforutsigbare kursbevegelser. I og med at en slik valuta ikke har noen sentral styringsinstans, vil den ikke kunne benyttes som et redskap i pengepolitikken.

Blockchain er egnet til å knytte eiere sammen med objekter, for eksempel eiendommer. Blockchain-transaksjoner vil fungere på tilsvarende måte som et digitalt signert dokument. Eieren av den private nøkkelen eier objektet som er beskrevet i dokumentet. Dokumentene er kjedet og utgjør et eierregister.

Det finnes flere initiativer for å definere plattformer som kan benyttes for å etablere løsninger for bruk i finansnæringen. Plattformene består regler, formater og protokoller for å inngå ulike bindende avtaler. Avtalene registreres i en Blockchain. Eksempel på initiativer: Ethereum (åpen), R3CEV[35] (flere finansforetak er med her).

Aktørene, f.eks. deltakerne i R3CEV, ser for seg digitale transaksjoner knyttes til fysiske eiendeler. Til forskjell fra et eierregister, vil dokumentet i dette tilfellet inkludere en definisjon av selve eiendelen. Dette vil kreve en tiltrodd tredjepart og en "market maker". Det vil også kreves faste formater. Et eksempel kan det være markedet for syndikerte lån. Dette er i dag et globalt marked med et volum i milliarder dollar, der transaksjonene i stor grad skjer ved hjelp av fax, e-post og regneark. Dette kan overføres til smarte kontrakter i faste formater der bestemmelser og vilkår er programmert inn, og som så blir delt mellom deltakerne i syndikatet via en distribuert logg. Tilsvarende løsninger kan tenkes

[34] http://www.finanstilsynet.no/Global/Venstremeny/Rapport/2014/ROS-analyse_2013.pdf, pkt. 7.5.2
[35] http://forklog.net/r3cev-tests-blockchain-for-banking-institutions/

innenfor Trade Finance og kapitalmarkedet. Dagens kompliserte prosesser blir sterkt forenklet, noe som kan senke risikoen for feil. Prosessene går raskere, noe som gir mindre operasjonell risiko og motpartsrisiko, og er følgelig rimeligere (redusert risikopåslag). Transaksjonsloggen er distribuert og mindre utsatt for "single point of failure" som følge av angrep eller driftsfeil.

Felles for alle ovenfor nevnte forretningsområder er at kontraktspartene i dag bruker mye ressurser på å synkronisere seg i løpet av transaksjonsforløpet, i stedet for at de har ett, samsvarende bilde til enhver tid. I dag sender de informasjon frem og tilbake for å forsøke å avstemme, og en går gjennom dyre etterbehandlinger for å rette feil og differanser. Distribuerte logger ville kunne avhjelpe disse problemene.

Internasjonale betalinger er i dag en komplisert samhandling mellom banker, sentrale motparter, likviditetsbanker og oppgjørssystemer på avsender- og mottakersiden. Disse betalingene mener aktørene er egnet for Blockchain-teknologi. Ripple, Stellar og Coinbase er eksempler på selskaper som arbeider med Blockchain-løsninger innen betalingsområdet.

Finanstilsynet mener at risiko og sikkerhet knyttet til Blockchain ikke er tilstrekkelig avklart.

4 Aktørenes vurdering av risikofaktorer

Dette kapitlet tar opp de mest fremtredende truslene foretakene selv tar opp i intervjuer og i besvarelser av spørreskjema fra Finanstilsynet. Videre omtales vesentlige trusler fremkommet gjennom intervjuer med sentrale aktører for sikkerhetsløsninger, og de mest alvorlige truslene ut fra enkelte internasjonale sikkerhetsselskapers vurderinger.

4.1 Intervjuer

Finanstilsynet intervjuet i 2015 ulike finansforetak som et ledd i kartleggingen av IKT-risikoer. Finanstilsynet hadde også samtaler med andre aktører, herunder noen sentrale aktører for sikkerhetsløsninger og overvåking i Norge. Nedenfor omtales de mest fremtredende trusselsområdene tilsynet har merket i disse samtalene. I enkelte tilfeller beskrives kontrolltiltak som ble trukket frem.

Visse typer trusler kan gjøre stor skade for foretaket dersom de inntreffer. Enkelte trusler kan påføre forbrukere betydelig skade og ulempe, og dermed også innvirke på foretakenes omdømme.

4.1.1 Samfunnsendringene påvirker sikkerheten

Hvitvaskingsregelverket krever at banker og betalingsforetak har sikker identifikasjon av kundene, og at transaksjoner overvåkes så de ikke inngår i terrorfinansiering, eller er del av slik virksomhet eller hvitvasking. Økende krav om hurtig betalingsformidling presser denne overvåkningen inn som en del av selve betalingskjeden, og medfører store utfordringer til endring hos aktørene.

Terrorfare og økt spenning i konfliktområder øker risikoen for at bankene blir brukt til terrorfinansiering. Foretakene framholder at den kraftige økningen i migrasjon over landegrensene gir sikkerhetsmessige utfordringer ved nye kundeetableringer. Spesielt flyktninger med manglende identitetsdokumenter skaper utfordringer i kundekontrollen i henhold til krav i hvitvaskingsregelverket og kan gi økt risiko for at ulovlige midler forsøkes overført gjennom betalingssystemene.

4.1.2 Forstyrrelser i infrastruktur

Bankene har i 2015 registrert økt ustabilitet i sin infrastruktur. Dette gjelder både tjenester fra telefonleverandørene og tjenester fra sentrale leverandører. For telefonoperatørene gjelder dette spesielt mobile tjenester og SMS-tjenesten som benyttes både for telefonbank og for enkelte

applikasjoner som bankene tilbyr på mobil. Det er registrert tilfeller av svikt i forsvaret mot digital kriminalitet hos individuelle leverandører av Internett-tjenester (ISP'er). Bankene opplever imidlertid at DDoS-sikringen hos ISP'ene er god.

Enkelte banker uttrykker bekymring for fallende driftskvalitet når det gjelder BankID-tjenesten.

Med økende avhengighet av elektroniske tjenester, gir ustabilitet og forstyrrelser redusert kvalitet på tjenesten til brukerne, og tilliten til tjenestene kan svekkes.

4.1.3 Knapphet på kompetanse

Flere foretak ser kompetanse på stormaskin-siden som utfordrende. En stor andel av arbeidstakerne med kompetanse på området nærmer seg pensjonsalder, og utdanning innen stormaskin er nærmest fraværende. Graden av utkontraktering øker hos finansforetakene, noe som resulterer i redusert kompetanse på egne systemer. Enkelte foretak kompenserer dette ved økt bruk av konsulenter, men også da forblir kompetansen utenfor foretakene. Dette kan medføre at foretakene ender opp med mangelfull fagstøtte til innkjøpere, og derav mangler vedrørende teknisk leveransekrav. Noen foretak uttrykker derfor behov for å bygge opp bestillerkompetanse på dette området. Det er de minste aktørene som taper mest i denne situasjonen.

Dersom utkontraktering ut av Norge blir for omfattende, kan dette true nasjonal kompetanse på de systemene som benyttes i finanssektoren. Det kan få følger for evnen til å håndtere kritiske situasjoner.

Når det gjelder sikkerhetsmiljøet, har de fleste finansforetakene forsøkt å bygge opp kompetanse. Her er det imidlertid mangel på utdanningsplasser eller søkere til disse. Kandidater trenger også praktisk erfaring innenfor området før de kan sies å være kvalifiserte sikkerhetseksperter. Flere av foretakene peker på knapphet på kompetanse innenfor sikkerhetsområdet som en utfordring.

Behov for kompetanse på IKT-sikkerhet er også påpekt flere steder i Lysne-utvalgets rapport.[36]

4.1.4 Risikoer knyttet til personell

Trusselen knyttet til skade forvoldt av egne ansatte ble i generelle vendinger omtalt av enkelte foretak. Utkontraktering generelt og off-shoring spesielt, medfører omplassering, oppsigelser og nytt personell. Omstrukturering, nedbemanning og salg kan medføre at lojaliteten til oppdragsgiver svekkes[37]. Bytte av personell fører til "friksjonskostnader" i form av opplæring, relasjonsbygging og samkjøring. Dette kan øke sannsynligheten for uønskede hendelser.

4.1.5 Kompleksitet i foretakenes leveransekjeder

Stadig nye tekniske muligheter tilbys av ulike leverandører. Når noen aktører tar slike muligheter i bruk, medfører dette oppmerksomhet i markedet, og foretakene føler et press for raskt å tilby

[36] Digitalt sårbarhetsutvalg – NOU 2015:13 Digital sårbarhet – sikkert samfunn
[37] http://e24.no/jobb/en-av-fire-norske-bedrifter-har-utro-ansatte/23592656

tilsvarende funksjonalitet. Samtidig kommer det nye regulatoriske krav, særlig fra EU-direktiver og -forordninger. Foretakene opplever dette som økende krav til endringer. Ny funksjonalitet for å møte dette presset løses gjerne ved en kombinasjon av utkontraktering og bruk av konsulenter. Løsningene fører til lange verdikjeder, særlig for nett- og mobilbank. Foretakene har utfordringer både med den høye endringstakten og den stadig mer krevende oppfølgingen.

Endringene får også følger utover selve programvaren. Både infrastruktur og interne forretningsprosesser berøres av disse endringene, og kapasitet på prosjektområdet for IKT-tilpasninger er også utfordrende.

På betalingsområdet uttrykker foretakene risiko for et lavere sikkerhetsnivå når flere aktører gis tilgang til å drive betalingstjenestevirksomhet som følge av nytt betalingstjenestedirektiv (PSD2), og krav til godkjennelse av flere autentiseringsmekanismer. Foretakene framhever at innenfor dette området kan leveransemønsteret blir uoversiktlig, selv om intensjonen er en forenkling for brukerne.

Endringene i produksjonsmiljøene gjør det stadig vanskeligere å vedlikeholde gode testmiljøer. Foretakene uttrykker behov for at test- og produksjonsmiljøene må samordnes bedre.

Den stadig økende kompleksiteten i transaksjonskjedene medfører økt risiko for feil, og det samme gjør et stort antall endringer. Dette kan resultere i et økende antall hendelser.

4.1.6 Foretakenes vurderinger knyttet til digital kriminalitet

Aktører melder at fra et globalt perspektiv er det liten malware-aktivitet i Norge (og Norden generelt) i forhold til enkelte andre land. Norge er fortsatt blant de minst infiserte landene.

Nasjonal Sikkerhetsmyndighet (NSM) overvåker målrettede angrep i Norge og melder om økende trussel. Mindre konsekvenser fra DDoS-angrep skyldes at foretakene har gode beskyttelsesmekanismer mot slike angrep.

Foretakene må være raskt ute med oppgraderinger for sikkerhetshull. Når kriminelle blir kjent med hvor svakhetene ligger, tar det kort tid før det er utviklet virus som kan angripe maskiner hvor svakheten ikke er reparert. Noen foretak har rutiner for å ivareta dette.

Foretakene melder at nettangrepene blir stadig mer sofistikerte og kombinerer flere av de tradisjonelle angrepsmetodene. Omgåelse av sikkerhet, og bruk av nettadresser som er tilnærmet like foretakenes nettadresser, brukes. For å kunne bruke sikker kommunikasjon (https) skaffer angriperne seg falske sertifikater. På dette området vokser det fram en "industri" som utsteder kriminelle sertifikater.

Flere aktører ønsker en bedre samhandling mellom CERT-aktørene og bedre samarbeid mellom de ulike sektorene på dette området.

Det har vært høy trussel fra digital kriminalitet i 2015, og det er viktig at foretakene jobber målrettet for å demme opp for denne trusselen. Det krever økende grad av overvåkning av tjeneste-leveransene og også fokus på sikkerhet på kundesiden. Foretakene som har kommet lengst, har ulike forsvarsnivåer, mot kunde, mot kanal og mot sentrale applikasjoner.
Det er ikke et spørsmål om et foretak blir angrepet, men om å være klar til å stå imot når angrepene kommer. Hittil har de største finansinstitusjonene vært mest utsatt.

Aktuelle angrepstyper:

- APT, for eksempel CARBANAK, som stjeler informasjon fra norske banker.
- Fremover er det ventet at små og mellomstore bedrifter (SMB-er) vil bli et viktig mål for APT-angrep, ut fra en antakelse om at de har mindre omfattende sikkerhetstiltak. Også mindre foretak må påse at de har god sikring på sine lokale nettverk, selv om hoveddelen av systemene er utkontraktert til eksterne leverandører og sikret av disse.
- Tyveri via mobile plattformer. I 2016 forventes flere angrep på mobile plattformer. For eksempel SMS der brukeren får lastet ned en falsk mobilbank.
- Tjenestenekt-angrep (DDoS).
- Tyveri via elektroniske selvbetjeningskanaler.
- Real-time phishing. I mer enn 95 prosent av tilfellene er det bedriftskunder som rammes. Én bank melder at 188 kunder ble forsøkt svindlet, men i kun fem tilfeller klarte de kriminelle å få tilgang til kundens konto.
- Trojaneren Dyre. Foretak har i 2015 hatt angrep av Dyre. Sikkerhetsmiljø har fulgt Dyre over lengre tid og fikk i midten av september indikasjoner på forberedelse av angrep mot utvalgte mål. Det er mye arbeid med gjenoppretting av data etter slike angrep. (Se også punkt 3.10.3.)

Angrepene i listen nedenfor synes å være de som i størst grad har truffet norske finansforetak. (Se forklaring i ordlisten i kapittel 8.)

- Dyre
- ReTeFe (DNS changer)
- Tinbal
- Vawtrak
- Gozi-ISFB
- MITM/MITB (inject mode)
- Dridex + ammyy
- RAT-basert "manuell" svindel

Bevisstgjøring av medarbeiderne

Mange foretak framhever at de satser mye på bevisstgjøring av ansatte, og gir opplæring i hva som kan skje dersom epostmottakeren er uvøren og åpner vedlegg eller følger oppfordringer eller anvisninger fra slike eposter. Foretakene peker på at slik bevisstgjøring og opplæring blir stadig viktigere for å motstå digitale angrep.

4.1.7 Brudd på konfidensialitet

Foretakene vurderer at det er en økende trussel for brudd på konfidensialitet. Det er samtidig økende grad av kunde-tilgang til egne data. Tilgjengelighet i nye kanaler forsterker trusselbildet ytterligere. Svindelforsøkene øker i antall, og gode systemer for beskyttelse må etableres.

Mange foretak prioriterer rask lansering av sine produkter i markedet, noe som kan gå på bekostning av sikkerhet. Gode lanseringsprosedyrer for nye tjenester og god utførelse av tilgangsstyring er vesentlig.

Beskyttelse av data

Mange foretak er opptatt av klassifisering av data og beskyttelse av data. Foretak har sett et behov for å gå gjennom såkalte ustrukturerte data, dvs. data som ikke er lagret i databaser, og som kan være mindre effektivt beskyttet mot uautorisert tilgang. Dette kan være presentasjoner, Microsoft Office-dokumenter, e-post-dokumenter mv. Det kan gjelde bedriftsintern informasjon så vel som informasjon som gjelder andre foretak som for eksempel kunder, leverandører og forretningsforbindelser.

Utlevering av BankID-kodebrikke

Enkelte banker opplyser at de har gått bort fra utlevering av BankID kodebrikker gjennom posten. Begrunnelsen er at BankID er et identitetsinstrument som på avveier kan brukes til svindel.

4.1.8 Bruk av sky- og fildelingstjenester

Foretakene har vist interesse for bruk av skytjenester på enkelte områder. Noen avventer avklaring av Safe Harbour-spørsmålet (se punkt 5.1.4), men planlegger for at "egnede tjenester" gradvis vil bli tilpasset og flyttet til skytjenester. Foretakene ønsker en avklaring av regelverket, slik at like konkurransevilkår opprettholdes.

Sett fra Finanstilsynets synsvinkel, er skytjenester utkontraktering, se punkt 3.8.2, som må være i tråd med foretakets utkontrakteringsstrategi, og med lover og regler. Skytjenester selges på mange måter. Det krever innkjøpskompetanse for å vite hva man kjøper, siden de fleste leverandørene utformer sine tjenestetilbud ulikt. Foretaket må sørge for kontroll med de enkelte enheters bruk av skytjenester slik at bruken er i tråd med foretakets utkontrakteringsstrategi.

Ulike former for fildelingstjenester er også i bruk. Enkelte foretak er bekymret for ukritisk bruk av fildelingstjenester som tilbys på Internett. Fildelingstjenestene er lett tilgjengelige, og dekker brukerens umiddelbare behov "der og da". Flere av tjenestene har hatt sikkerhets-svakheter. Data om ansatte, foretaket og forretningsforbindelser kan komme på avveier. Kunnskap om ansatte og foretak kan misbrukes av angripere til målrettede angrep ("spear phishing"). Styring med disse tjenestene synes mangelfull. Det sies at:

- IT-funksjonen i foretaket bare kjenner til en mindre del av skytjenestene som brukes
- det foregår mye opplasting til, og bruk av skytjenester med høy risikoprofil
- det er ikke uvanlig at et foretak bruker mange ulike fildelingstjenester

4.1.9 Penetrasjonstesting

Trussel om innbrudd i finansforetakenes systemer er økende. Foretakene og deres leverandører bygger opp forsvar mot slik inntrenging, men det et komplekst område som krever høy kompetanse. Inntrengingsforsvaret må testes for å sikre at det fungerer tilfredsstillende.

Noen foretak har gjennomført penetrasjonstester, gjerne ved hjelp av eksterne konsulenter. Andre foretak planlegger gjennomføring av slike tester i samarbeid med andre som har tilsvarende infrastruktur og benytter samme tjenesteleverandør for sine kjernesystemer.

4.1.10 Internettfeil rammer globalt

Foretakene rapporterer om en økt bevissthet rundt at sårbarheter langt utenfor Norges grenser kan ramme Norge. Et eksempel, som nevnt i punkt 3.9.1, er en svakhet i Border Gateway Protocol[38] (BGP definerer hvem som eier IP-adresseområder og benyttes av ISP'ene for å rute trafikk).

4.1.11 Andre risikoer påpekt av foretakene.

Reservedeler

Noen foretak erfarte i 2015 at leverandørene ikke hadde tilstrekkelig med reservedeler til å dekke behovet, se også punkt 3.4.4. I ett tilfelle medførte strømutfall og etterfølgende strøminnkopling at flere nettverkskomponenter ble ødelagt. I denne situasjonen viste det seg vanskelig å få levert tilstrekkelig med erstatningskomponenter innenfor rimelig tid. Dersom flere viktige foretak innenfor finanssektoren opplever dette på samme tid, kan det få alvorlige konsekvensene for leveransen av finansielle tjenester i Norge

Fysisk tilgang

Flere foretak rapporterer om at uvedkommende har hatt fysisk tilgang til teknisk infrastruktur. Dette gjelder helst i bygg med flere leietakere. Ikke alle leietakere har samme krav til adgangskontroll, og uvedkommende kan trenge langt inn i lokalene før det reageres.

Logiske tilgangskontroller

Sviktende kontroll når det gjelder logiske tilgangskontroller oppfattes stadig som en risiko. Drift og utvikling av løsningene er et komplekst samspill mellom egne ansatte og leverandører ute og hjemme. Godkjenning og oppfølging av personer, roller og tilganger er et omfattende arbeid. Enkelte foretak erfarer at det er behov for forbedringstiltak på dette området.

4.2 Spørreundersøkelse

I desember 2015 gjennomførte Finanstilsynet en spørreundersøkelse blant 22 foretak. I spørre-undersøkelsen ber Finanstilsynet foretakene vurdere i hvilken grad foretaket anser seg for å være

[38] http://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/

sårbare for aktuelle trusler. Resultatene fremgår av tabellene 5–10 nedenfor. Grønt gir uttrykk for lav sårbarhet for foretaket, gult innebærer middels sårbarhet og rødt uttrykker høy sårbarhet. Ingen farge innebærer at foretaket ikke har svart.

Videre ble foretakene bedt om å vurdere sårbarhetene fremover, dvs. om sårbarhetene anses å være økende, stabile eller minkende. Trenden som kommer til uttrykk i kolonnen lengst til høyre i tabellene nedenfor, er uttrykk for gjennomsnittet av de vurderingene som ble gitt, der intervallet -0,2 til +0,2 angis av en horisontal pil og innebærer en stabil trend. Piler som peker opp, indikerer at sårbarheten anses å være økende (intervallet +0,2 til +1), og piler som peker nedover, indikerer at sårbarheten anses å være minkende (intervallet -0,2 til -1).

4.2.1 Støtte for strategiske beslutninger

Tabell 5: Støtte for strategiske beslutninger

	Sårbarhet	Foretakenes svar	Trend 2014	Trend 2015
1	Systemenes evne til å innhente og sammenstiller relevant informasjon fra interne og eksterne kilder for beslutningsformål		↘	→
2	Systemer for beslutningsstøtte og rapportering henter relevant informasjon fra våre produksjonssystemer og sammenstiller og synkroniserer informasjonen til et bilde av foretakets risiko til bruk i styringsøyemed og til myndighetsrapportering.		↘	→
3	Systemene gir automatisk et totalbilde av risikoen, for eksempel slik at hvis en hjørnestensbedrift går konkurs, så varsler systemet automatisk om lån til ansatte i bedriften og lån til leverandører til bedriften, slik at vi kan vurdere å tapsavskrive på disse.		↘	→
4	Systemene våre gir et godt bilde av kundens behov og evne til å betjene gjeld.		↘	→
5	Datakvaliteten i våre systemer og registre		↘	↘
6	Integrasjon og synkronisering mellom systemene		↘	→
7	Når nye IT-løsninger skal utvikles, tar vi i betraktning behovene og løsningene til alle relevante avdelinger. Dette for å unngå utfordringer forbundet med "silo-løsninger" slik som omfattende vedlikehold av programmer, komplisert drift og utfordringer med synkronisering av data.		↘	→
8	Grad av kompleksitet i IT-systemene		→	→
9	Omfanget av mangler og feil i systemene		→	→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet.			

Kilde: Finanstilsynet

Tabellen viser risikoen for at IKT ikke fungerer tilfredsstillende som støtte for strategiske beslutninger, kundebehandling eller saksbehandling. Et eksempel er at IKT-systemene ikke i tilstrekkelig grad varsler om f.eks. økonomiske problemer som rammer en hjørnestensbedrift eller en hel bransje. Foretakene får da ikke informasjon fra IKT-systemene som setter de i stand til å iverksette nødvendige tiltak.

På dette området har seks av truslene gått fra å være minkende i 2014 til å være stabile i 2015.

4.2.2 Avvik i driften

Tabell 6: Avvik i driften

	Sårbarhet	Foretakenes svar	Trend 2014	Trend 2015
1	Organisering, rutiner, stillingsbeskrivelse, rapportering og kontroll		↘	↘
2	Avtalene med leverandørene sikrer oss rett til innsyn i alle forhold som gjelder leveransen		→	→
3	Test-systemene er "produksjonslike", dvs. at testdata, applikasjoner, programvare, styresystemer (SW) og maskinvare er det samme for test som i produksjon		↘	→
4	Vi gjør endringer i infrastrukturen ("ikke- funksjonelle" endringer) i trafikkstille perioder, og kan reversere endringen og rulle tilbake på kort tid hvis nødvendig		→	→
5	Vår evne til å avdekke alle svakheter		↘	→
6	Kontroller som skal sikre at alle maskiner og programmer er inkludert i IDS/IDP, brannmur og virus og andre tiltak for å sikre stabil drift		→	→
7	Logger og vår evne til å reagere på innholdet i loggene		→	↘
8	"Tikkende miner", dvs. komponenter som gradvis slites eller verdier som gradvis når nivåer som krever inngrep uten at vi oppdager det, for eksempel minnelekkasje, elektroniske komponenter som slites, energiforsyning som "slites" (batterier eller annet)		↘	↘
9	Vår evne til å avdekke avvik i datatrafikken (unormal belastning, unormale porter/ protokoller, avvikende svarstider) i driftsmønsteret og ta aksjon før skade		↘	→
10	Vår beskyttelse mot dataangrep (Advanced persistence threat, trojaner, ransomware, DDoS)		→	→
11	Kvaliteten på kontinuitet- og katastrofeløsningene våre		↘	→
12	Samarbeidsrutiner med leverandører		→	→
13	Leveransepresset vi er utsatt for i markedet		→	↗
14	Tilgang på kompetanse, herunder kompetanse til å stille krav til leverandører og følge opp leveransene		↘	→
15	Mengden av endringer (ny leverandør, nye grunnsystemer)		→	→
16	Nye regulatoriske krav som gjør at vi må endre systemene våre		→	↗
17	Vår kunnskap om hvor datalinjene går og redundans når det gjelder datalinjer		→	→
18	Tilgangskontroll, adgangskontroll og tjenestedeling ("segregation of duty")		→	→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet.			

Kilde: Finanstilsynet

Dataangrep er en vedvarende trussel. Omfanget av endringer i systemer og leverandører likeså. Flere foretak enn i fjor anser at testsystemene kunne vært bedre. Dette kan henge sammen med økt leveransepress (tema 13) og omfanget av endringer (tema 15) og endringer fra nye regulatoriske krav (tema 16).

4.2.3 Data er ikke tilstrekkelig beskyttet

Tabell 7: Data er ikke tilstrekkelig beskyttet

	Sårbarhet	Foretakenes svar	Trend 2014	Trend 2015
1	Våre retningslinjer for klassifisering av informasjon og beskyttelse av informasjonen		→	→
2	Kvaliteten på våre tilgangskontroller		→	→
3	Våre systemer for logging og evne til å reagere på innholdet i loggene		→	→
4	Mulig inntrenging i våre systemer		→	→
5	Sikring av data på bærbart utstyr (fjernsletting av mobildata osv.)		→	→
6	Ved terminering av avtaler om datalagring må leverandøren dokumentere at data er fullstendig slettet.		→	→
7	Ustrukturerte data (dvs. data der brukeren selv vurderer behovet for å beskytte dataene) som epost, presentasjoner, tekst-dokumenter blir gjennomgått regelmessig med tanke på beskyttelse, eventuelt sletting.		→	→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet.			

Kilde: Finanstilsynet

Tilgangskontroller er stadig en utfordring. Utkontraktering, off-shoring og midlertidig, innleid kompetanse skaper utfordringer.

Inntrenging i systemene anses som en trussel. I 2015 var det en økning i såkalt ransomware, jf. omtale i punkt 3.10.2.

4.2.4 ID-tyveri

Tabell 8: ID-tyveri

	Sårbarhet	Foretakenes svar	Trend 2014	Trend 2015
1	Vår beskyttelse mot skadevare som infiserer en bruker i foretaket og misbruker den infiserte brukeren sine rettigheter		→	→
2	Kontroll når det gjelder utlevering og bruk av logon-id og passord til kunder og medarbeidere (BankID, ansatte-id, systembrukere, admin-brukere)		→	→
3	Kontroller som forhindrer "skimming" og "Card not present"-svindel		→	↗
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet.			

Kilde: Finanstilsynet

Skadevare og misbruk av rettigheter i forbindelse med ID-tyveri anses fortsatt som en betydelig trussel.

I 2015 ble trusselen fra CNP-svindel ansett å være økende.

4.2.5 Misbruk av tilgang til datasystemene

Tabell 9: Misbruk av tilgang til datasystemene

	Sårbarhet	Foretakenes svar	Trend 2014	Trend 2015
1	Tilgangskontroll		→	→
2	Vår policy når det gjelder tjenestedeling		→	→
3	Logging		→	→
4	Analyse av "mistenkelige" transaksjoner som tilbakevalutering, bevegelser på interne kontoer, overføring fra kunde til ansatt og tilbake		→	→
5	Overvåking av ansattes egenhandel		→	→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet.			

Kilde: Finanstilsynet

Trusselbildet er uendret fra foregående år.

4.2.6 Hvitvasking

Tabell 10: Hvitvasking

	Sårbarhet	Foretakenes svar	Trend 2014	Trend 2015
1	Markedsovervåking		→	→
2	IT-systemenes evne til å samle informasjon om kunde, kunderelasjoner og kundeadferd (KYC– Know Your Customer)		→	→
3	Elektronisk overvåkning av transaksjoner – presisjon i flagging av mistenkelige transaksjoner		→	→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet.			

Kilde: Finanstilsynet

Flere foretak mener det er utfordrende å lage systemer som har høy presisjon når det gjelder å flagge mistenkelig transaksjoner. Et betydelig antall foretak rapporterer at det arbeides aktivt med å forbedre innsamling, "flagging", analyse og rapportering innenfor dette området.

Samlet viser tabellene 5–10 at elleve av sårbarhetene har gått fra å være minkende i 2014 til stabil i 2015. Dette kan være uttrykk for at truslene enten har flatet ut eller at de er blitt mer aktuelle eller akutte i 2015 i forhold til 2014, eller at foretaket ikke anser at de har tilstrekkelige beskyttelsestiltak mot truslene. Det er også verdt å merke seg at tre av sårbarhetene har gått fra å være stabile til ansett å være økende. Alt i alt vurderer foretakene at risikoen har økt fra 2014 til 2015.

4.3 Rapporten fra EUs sikkerhetsorganisasjon ENISA

ENISA (The European Union Network and Information Security Agency) er EU-landenes ressurssenter for nettverk og IKT-sikkerhet. I forbindelse med IKT-sikkerhet blir ENISA benyttet og referert til av EUs tilsynsorganer på finansområdet (EBA, ESMA og EIOPA). ENISA gir årlig ut en

rapport[39] med oppsummering av siste års hendelser og endringer i trusselbildet for IKT-sikkerhet for finansområdet i Europa.

I rapporten for 2015 påpeker ENISA at kampen mot digital sårbarhet fortsetter, og at offentlige myndigheter og deres leverandører har blitt mer effektive ved:

- Mere samstemte/organiserte tiltak for å stanse cyberangrep.
- Økt kompetanse og kjennskap til cyberkriminalitet, økte budsjetter og mer samarbeid over landegrenser.
- Øvelser, økt etterretning og informasjonsdeling mellom nasjoner.
- Økt fokus på forskning og utvikling for å utvikle løsninger som beskytter mot cyberkriminalitet.

På den andre siden fortsetter også en utvikling der kriminelle krefter demonstrerer at de rår over betydelige ressurser ved:

- Stadig forbedrede applikasjoner for kriminelle handlinger, og som tilbys som tjenester over Internett.
- Forbedrede løsninger for avdekking og utnytting av svakheter i eksisterende systemer.
- Å i stor grad å lykkes med å utvikle ulike innbringende ransomware-tjenester.
- Å utvide fokusområdet for kriminalitet til å omfatte alle Internett-tilkoblede enheter.
- Å gjennomføre angrep som ikke registreres av vanlige forsvarsløsninger.

ENISA mener at 2015 kan karakteriseres som "ransomware-året", med tanke på den store utbredelse ransomware nå har fått, se punkt 3.10.2. Det pekes spesielt på en variant som kalles CTB-locker (Curve-Tor-Bitcoin).

En del av ENISAs rapport viser utviklingen av ulike IKT-risikoområder basert på innrapporteringer fra ulike kilder. Kort sammenfattet har følgende risikoområder:

- økt i omfang:
  - Malware
  - Nettbaserte angrep
  - Web application/onjection attacks
  - Denial of service(DDoS)
  - Innside-trusler
  - Informasjonslekkasjer
  - Ransomware
  - Cyber-spionasje

- minket i omfang:
  - Spam
  - Phishing
  - Bruk av botnets

[39] ENISA Threat Landscape 2015 (ETL). Publisert på ENISAs nettsted.

5 Endringer i reguleringer

Også i 2015 var det en rekke EU-prosesser knyttet til forslag til nye eller endring i eksisterende direktiver, forordninger, tekniske standarder og veiledninger som vil få betydning for norske forhold etter hvert som de blir tatt inn i norsk lovgiving. Også nasjonalt var det endringer i lover, forskrifter og retningslinjer.

Endringene kan på enkelte områder medføre behov for omfattende endringer i foretakenes systemløsninger. Endringer i systemporteføljen er generelt en betydelig kilde til feilsituasjoner som oppstår.

5.1 Samordning innen EU og endringer i EUs regelverk

5.1.1 Betalingsformidling

Retningslinjer for sikkerhet i Internett-betalinger (Guidelines on the security of internet payments) ble vedtatt med virkning fra 1. august 2015. Finanstilsynet har sluttet seg til retningslinjene (se punkt 5.2.3).

Arbeidet med revidering av det nye betalingstjenestedirektivet (PSD2)[40] ble sluttført i 2015. Direktivet trer i kraft 13. januar 2018 og skal fremme innovasjon gjennom å skape økt konkurranse mellom eksisterende og nye aktører. Det har fått et bredere anvendelsesområde ved at alle valutaer og såkalte one-leg transaksjoner innen EU omfattes. Direktivet åpner for flere aktører som betalingstjenestetilbydere og gir rett til tilgang til betalingskonto, både for eksisterende og nye aktører. Det stilles krav til autorisering for betalingstjenesteinitiatorer (PIS) og at kontoinformasjonstilbydere (AIS) skal registrere seg. For de nye betalingstjenesteaktørene stilles det krav til forsikring. Direktivet stiller høye sikkerhetskrav for alle elektroniske betalinger og alle betalingstjenestetilbydere, blant annet ved krav til sterk autentisering og sikker kommunikasjon. Det stilles krav til foretakene om hendelsesrapportering, gjennomføring av risikoanalyser og styring av risiko for betalingstjenesten. Bestemmelser i direktivet skal styrke tilsynssamarbeidet ved grensekryssende virksomhet og gi forbedret forbrukerbeskyttelse. Direktivet regulerer i tillegg også adgangen til å belaste gebyrer på

[40] http://ec.europa.eu/finance/payments/framework/index_en.htm

forbruker. Finansdepartementet har varslet at Justisdepartementet og Finanstilsynet vil få i oppdrag å utarbeide forslag til innarbeiding av PSD2 i norsk rett[41].

EBA er tillagt et ansvar for å utarbeide forslag til nærmere retningslinjer på flere av direktivets områder. Disse ble overordnet omtalt i risiko- og sårbarhetsanalysen for 2014. Det mest krevende arbeidet er knyttet til utarbeidelse av regulatoriske tekniske standarder for sterk autentisering, herunder unntaksbestemmelser, og sikker kommunikasjon. Bestemmelsene skal sikre trygge og sikre betalingstjenester, selv når flere aktører er involvert i verdikjeden for gjennomføring av en betaling.

EU utarbeidet i 2015 en såkalt grønnbok vedrørende finansielle tjenester i detaljhandelen[42], der formålet var bedre produkter, mer valgfrihet og større muligheter for forbrukere og bedrifter. EU-kommisjonen sendte dokumentet på høring i desember 2015.

EU har igangsatt en prosess for revisjon av e-penge-direktivet. Det forventes at de første delutredningene vil foreligge vinteren/våren 2016. Ett av formålene med revisjonen er å oppnå konsistens med det vedtatte PSD2.

5.1.2 "Personvernpakken"

EU har vedtatt ny forordning[43] om behandling av personopplysninger. Formell ikrafttredelse forventes å være første kvartal 2018. Forslaget styrker rettighetene til den opplysningene gjelder gjennom:

- krav om at vedkommende klart skal samtykke til behandling av personopplysninger
- enklere adgang til å kontrollere egne personopplysninger
- rett til å få opplysningene korrigert, slettet og "retten til å bli glemt"
- rett til å reise innvendinger, herunder innvendinger mot at opplysningene blir benyttet til profilering
- rett til å flytte egne personopplysninger fra en tjenestetilbyder til en annen

Personvernforordningen inneholder regler om innebygd personvern ("Privacy by design, privacy by default"), personvernombud og internkontroll.

5.1.3 Nettverk og informasjonssikkerhet

I arbeidet med det foreslåtte direktivet for nettverks- og informasjonssikkerhet (NIS-direktivet), der det har pågått omfattende og krevende diskusjoner i EU knyttet til flere av områdene, ble det i desember i 2015 oppnådd politisk enighet om direktivutkastet[44]. Finanssektoren er en av flere sektorer som vil bli omfattet og påvirket, selv om flere av direktivets bestemmelser er innarbeidet i PSD2. Temaet har tidligere blitt omtalt i Finanstilsynets ROS-rapporter for hhv. 2013 og 2014.

[41] https://www.regjeringen.no/contentassets/034971cd8bc54244b025fab9af15c45e/betalingstjenestedirektiv.pdf
[42] http://ec.europa.eu/finance/consultations/2015/retail-financial-services/index_en.htm
[43] http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/en/pdf
[44] Direktivutkast

5.1.4 Overføring av data mellom EU/EØS og USA – Privacy Shield

EU-domstolen har tidligere kjent en avtale mellom EU og USA om dataoverføring (Safe Harbour) ugyldig. Det har siden vært forhandlet om en ny avtale. Avtalen, som vil bli kalt Privacy Shield, vil gjelde for alle virksomheter som yter tjenester i EU.

Hovedpunktene i det nye avtaleverket er:

- Nye krav til virksomheters håndtering av personopplysninger
- Regler for amerikanske myndigheters innsyn
- Ombudsmannsordning
- Ny klagemekanisme
- Regler for ordinær klagebehandling

Alle foretak som ønsker å delta i ordningen må vise hvordan de har tenkt å etterleve prinsippene i avtalen. Det vil bli innført årlige kontroller av virksomheter som tar del i Privacy Shield-ordningen.

Den nye avtalen inneholder regler for amerikanske myndigheters muligheter for innsyn i europeiske borgeres personopplysninger. Det amerikanske handelsdepartementet skal levere årlige rapporter som viser hvordan avtalen etterleves. Det skal opprettes en ombudsmann som er knyttet til USAs utenriksdepartement. Ombudsmannsrollen skal ivareta klagers rettigheter.

En uavhengig voldgiftsordning opprettes, med medlemmer fra Europa og USA. Foretak som håndterer personopplysninger på basis av den nye avtalen blir pliktige til å behandle klager innen en gitt frist, og oppfølging av klager garanteres av det amerikanske handelsdepartementet. Klageordningen skal evalueres årlig.

Før det tas en endelig beslutning om innhold og iverksettelse, skal en komité bestående av representanter fra medlemslandene bli konsultert, og Artikkel 29-gruppen (EUs arbeidsgruppe for personvern) skal uttale seg. Artikkel 29-gruppen tar mål av seg til å ha en uttalelse klar 2. kvartal 2016. Samtidig gjennomfører amerikanske myndigheter de nødvendige forberedelsene for innføring av det nye rammeverket, inkludert opprettelse av den nye ombudsmannsordningen.

5.1.5 Forsikring

Det nye europeiske soliditetsregelverket for forsikringsforetak, Solvens II[45], trådte i kraft 1. januar 2016. Blant annet stilles det økte krav til intern og ekstern rapportering og store krav til data og datakvalitet, noe som krever vesentlige endringer i IKT-løsningene.

[45] http://www.finanstilsynet.no/no/Artikkelarkiv/Aktuelt/2014/4_kvartal/Finanstilsynets-forskriftsforslag-for-gjennomforing-av-Solvens-II/

5.1.6 Tiltak mot hvitvasking

EU vedtok i 2015 fjerde hvitvaskingsdirektiv basert på Financial Action Task Force (FATF)s anbefalinger fra 2012[46]. Det nye direktivet og merknadene i FATFs evalueringsrapport for Norge fra 2014[47] er grunnlaget for arbeidet som er igangsatt med ny lovgiving om tiltak mot hvitvasking og terrorfinansiering i Norge. Lovutvalget skal ferdigstille sin utredning i 2016.

Det norske hvitvaskingsregelverket stiller krav til at bankene skal ha systemer for elektronisk overvåkning av transaksjoner og at gitte typer mistenkelige transaksjoner ikke skal gjennomføres før de er nærmere undersøkt. Kompleksiteten i kontrollene øker stadig, og det kan ikke utelukkes at dette kan utfordre driftsstabiliteten.

5.1.7 Taskforce on IT Risk Supervision

EBAs enhet for IKT-tilsyn (Taskforce on IT Risk Supervision – TFIT[48]) ble etablert i 2015. Oppgaver og mål for TFIT er å bistå med rådgiving og støtte til nasjonale tilsynsmyndigheter og EBAs ansatte, og bidra til at EBAs arbeidsprogram knyttet til tilsynspraksis for IKT-risikotilsyn, samt å utvikle en enhetlig og effektiv ramme for vurdering av IKT-risiko. Dette gjøres gjennom utveksling av informasjon om tilsynstilnærminger og -praksis, identifikasjon av aktuelt tilsynssamarbeid og utforming av retningslinjer. TFIT vil også ta stilling til problemstillinger rundt implementering av internasjonale standarder, beste praksis og andre anbefalinger.

5.2 Endringer i norsk regelverk

5.2.1 Finansforetaksloven

Ny lov om finansforetak og finanskonsern (finansforetaksloven) trådte i kraft 1. januar 2016. Finansforetaksloven har erstattet sparebankloven, forretningsbankloven, finansieringsvirksomhetsloven og banksikringsloven samt deler av forsikringsvirksomhetsloven. Loven inneholder blant annet regler om konsesjon, organisatoriske regler, generelle virksomhetsregler, regler om sikringsordninger og soliditetssvikt og sanksjonsbestemmelser for banker, forsikringsforetak og andre finansforetak.

Finansforetak som allerede drev virksomhet når loven trådte i kraft, har fått ett års frist på å oppfylle en del av kravene, mens resterende deler av loven skal være oppfylt fra 1. januar 2016.

Finansdepartementet har sendt utkast til forskrifter til finansforetaksloven på høring med frist 1. april 2016.

[46] http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf
[47] http://www.fatf-gafi.org/countries/n-r/norway/documents/mer-norway-2014.html
[48] https://www.eba.europa.eu/documents/10180/758113/EBA+BS+2015+180rev1+(Final+Minutes+BoS+28-29+April+2015).pdf

5.2.2 Endringer i IKT-forskriften

IKT-forskriften[49] ble endret på to vesentlige punkter 17. desember 2015. Det stilles i § 2, 4. ledd krav om at avtaler om utkontraktering og endringer i slike avtaler skal behandles av foretakets styre. § 10 Krav til kontinuitet er opphevet og det materielle innholdet er inntatt i § 8 Drift, da kontinuitetsløsninger mer og mer blir etablert som del av foretakenes ordinære driftsløsninger. Det er også gjort endringer i § 9, 3. ledd, som innebærer at inkassoselskaper og pensjonskasser ikke lenger er unntatt fra krav om hendelsesrapportering. I tillegg er det foretatt noen mindre justeringer i forskriften.

5.2.3 Nye forskrifter og retningslinjer for betalingstjenester

Forskrift om systemer for betalingstjenester trådte i kraft 1. januar 2016[50]. I forskriften stilles det krav til foretaket om å gjennomføre risiko- og sårbarhetsanalyser, som en del av beslutningsgrunnlaget, før en ny betalingstjeneste lanseres, og ved hendelser eller endringer av betydning for sikkerhetsnivået. Videre stilles det i forskriften en rekke sikkerhetskrav.

Retningslinjer for sikkerhet i Internett-betalinger[51], utarbeidet av det europeiske banktilsynet (EBA)[52] i samarbeid med SecuRe Pay, ble gjort gjeldende fra 1. august 2015. Finanstilsynet vil legge disse til grunn under tilsyn. Retningslinjene, som er utarbeidet med basis i det eksisterende betalingstjenestedirektivet (PSD1), er i Norge knyttet mot forskriften om systemer for betalingstjenester.

Hensikten med retningslinjene er å definere felles minimumskrav for sikkerhet når det gjelder Internett-betalingene som er listet nedenfor, uansett hvilken teknologisk løsning som benyttes for tilgang til tjenesten:

- utførelse av kortbetalinger på Internett, inkludert betalinger med virtuelle kort og registrering av kortbetalingsdata for bruk i "lommebokløsninger"
- gjennomføring av kredittoverføringer på Internett
- registrere og endre elektroniske oppdrag for direkte debitering
- overføring av elektroniske penger mellom to e-pengekontoer via Internett

Retningslinjene definerer sterk kundeautentisering og slår fast at sterk kundeautentisering er hovedregelen når det gjelder betalinger på Internett. Retningslinjene stiller krav om ende-til-ende-sikring.

Finanstilsynet har i 2015 holdt informasjonsmøter for finansnæringen for å informere om innholdet i retningslinjene.

[49] https://lovdata.no/dokument/SF/forskrift/2003-05-21-630
[50] https://lovdata.no/dokument/SF/forskrift/2015-12-17-1731
[51] http://www.finanstilsynet.no/Global/Temasider/IT-tilsyn/Retningslinjer%20for%20sikkerhet%20i%20internettbetalinger_korr-AEJ-21-09.pdf
[52] https://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments

Forslag til innføring av forordning om interbankgebyrer[53] i norsk rett ble sendt på høring i desember 2015. Det stilles krav til blant annet tak på formidlingsgebyrer for forbrukerkort, at kortordninger skal separeres fra behandlingen av kortbetalingene, til co-branding (felles markedsføring) av kort og forbrukers rett til å bestemme valg av kort-merkevare. Det gis forbud mot å styre bruken av et kort med flere merkevarer slik at dagens prioriteringsregel, der BankAxept-merkevaren prioriteres foran ved kombinerte kort, ikke lenger vil være lovlig.
Forskriften om formidlingsgebyrer i kortordning foreslås å tre i kraft 1. juli 2016.

5.2.4 Regelverksendringer på forsikringsområdet

På forsikringsområdet har det gjennom flere år vært store regelverksendringer, som blant annet tjenestepensjonsloven og Solvens II-regelverket. Regelverksendringer for pensjonsinnretningene pågår fortsatt og medfører betydelig IKT-arbeid for å tilpasse seg disse. Solvens II-regelverket gjelder både skade- og livsforsikring. Blant annet medfører regelverkets krav til modellberegninger og økte krav til rapportering omfattende IKT-arbeid, og god datakvalitet er en forutsetning. Solvens II-rapporteringen er ikke i overensstemmelse med gjeldende standard for finansregnskap, IRFS, og innebærer en utfordring for selskapene. Grensesnitt og avstemming mellom de ulike systemene er vesentlig.

5.2.5 Elektronisk signatur

Nærings- og fiskeridepartementet har frem til 1. mars 2016 hatt på høring forslag[54] til gjennomføring av Europaparlaments- og rådsforordning (EU) 910/2014 om elektronisk identifisering og tillitstjenester for elektroniske transaksjoner på det indre marked og om opphevelse av direktiv 1999/93/EF. I høringsnotatet foreslås det en ny lov som gjennomfører forordningen, samtidig som lov 15. juni 2001 nr. 81 om elektronisk signatur oppheves. Forordningen styrker og utvider reglene om elektronisk signatur, regulerer eID og omfatter også andre typer elektroniske tillitstjenester. Forordningen er todelt, og inneholder regler som skal legge til rette for:

- Gjensidig aksept av løsninger for elektronisk identifisering (eID). Dette innebærer at privatpersoner og bedrifter skal kunne bruke sin eID, utstedt enten av offentlig sektor eller under ansvar av en offentlig myndighet, for å få tilgang til elektroniske tjenester fra offentlig sektor i andre land som tilbyr pålogging med eID.
- Gjensidig aksept av elektronisk signatur og andre tillitstjenester – kapittel III og IV. Forordningen styrker dagens regler om elektronisk signatur og innfører regler om flere typer elektroniske tillitstjenester, deriblant om elektroniske segl, tidsstemplingstjenester, elektronisk registrerte leveringstjenester og sertifikattjenester for autentisering av nettsteder.

53 https://www.regjeringen.no/contentassets/fbc25cd42f8d44c781924e597fed3da0/horingsnotat_des2015.pdf

54 https://www.regjeringen.no/no/dokumenter/gjennomforing-av-eus-forordning-om-elektronisk-identifisering-eid-og-tillitstjenester-for-elektroniske-transaksjoner-i-det-indre-marked---horing/id2464892/

6 Risikoområder

Finanstilsynets hovedmål er å bidra til finansiell stabilitet og velfungerende markeder.
Finansielle tjenester kan ikke leveres uten velfungerende IKT-systemer. Nye digitale løsninger øker effektiviteten og medvirker til lavere kostnader. Utviklingen innebærer imidlertid også økt sårbarhet.

Dersom betalinger og enkelte andre finansielle tjenester er utilgjengelige, vil viktige samfunnsfunksjoner etter kort tid ikke lenger fungere tilfredsstillende. Etter lengre tid vil viktige samfunnsfunksjoner kunne stoppe opp. Markedene fungerer ikke lenger som forutsatt.

6.1 Finansiell infrastruktur

Det norske finansielle systemet er samordnet, og felles løsninger og felles driftsleverandører benyttes i stor grad innen finansnæringen. Det medvirker til et effektivt og vel fungerende system. Imidlertid gjør det at både tilsiktede, ved IKT-rettede angrep, og utilsiktede hendelser som treffer samordnede løsninger eller driftsleverandører brukt av mange foretak kan få store konsekvenser. I tillegg kan hendelser som rammer enkeltforetak få uheldige følgekonsekvenser for andre aktører i det finansielle systemet. I tillegg til systemmessige ødeleggelser og økonomiske belastninger, kan slike hendelser få samfunnsmessige konsekvenser og påvirke finansiell stabilitet.

Flere foretak byttet fra felles leverandør til individuell leverandør i 2015. Dette kan gi mindre sårbarhet, fordi det er mindre sannsynlig at flere av driftssentrene blir slått ut samtidig.

Finansielle tjenester blir tilgjengelig i stadig flere betjeningskanaler. Dersom én kanal er utilgjengelig, vil kunden i en del tilfeller kunne benytte annen kanal.

Gjennom tilsynsvirksomheten og arbeidet i Beredskapsutvalget for finansiell infrastruktur (BFI), med blant annet gjennomgang av hendelser i foretakene og FMI-foretakene, får Finanstilsynet et bredt og godt bilde av tilstanden i den norske finansielle infrastrukturen.

Stabiliteten i den finansielle infrastrukturen var bedre i 2015 enn i 2014 og den ble rammet av færre operasjonelle hendelser. Det var ellers en god regularitet på avregnings- og oppgjørssystemene og kommunikasjonen mot det internasjonale betalingssystemet SWIFT (Society for Worldwide Interbank Financial Telecommunication) og det internasjonale oppgjørssystemet CLS (Continuous Linked Settlement).

Finanstilsynet vurderer på den bakgrunn den norske finansielle infrastrukturen som solid og stabil, men at det på enkelte områder er rom for forbedringer. Det gjelder både hos enkelte infrastrukturforetak i finanssektoren og hos enkelte øvrige foretak på blant annet beredskapsløsninger, styring av operasjonell risiko og bedre styring av tilganger.

IMFs vurdering av finansiell infrastruktur i Norge

Det internasjonale pengefondet (IMF) gjennomførte i 2014/2015 Financial Sector Assessment Program (FSAP) for Norge. Hensikten med programmet er å vurdere svakheter og styrker i systemviktige medlemslands finansielle system og foreslå tiltak som kan bidra til økt stabilitet og sikkerhet. Den finansielle infrastrukturen i Norge ble omtalt i hovedrapporten (Financial System Stability Assessment) og i en teknisk rapport (Technical note – Oversight and Supervision of Financial Market Infrastructure, and Selected Issues in the Payment Systems).

I hovedrapporten omtales Norges finansielle infrastruktur (FMI) som moderne og stabil og det gis uttrykk for at tilsyns- og overvåkingsfunksjonene med FMI-foretakene virker å være effektive. IMF gir imidlertid også uttrykk for at det finnes et potensiale for å styrke samarbeidet på myndighetsnivå for å adressere risikoene som enkelte av FMI-foretakene har når det gjelder avhengighet av kritiske leverandører. Etter IMFs vurdering, kan et risikoreduserende tiltak være at Norges Bank får bistand fra den tekniske og operative kompetansen i Finanstilsynet til å utarbeide krav til leverandører av kritisk infrastruktur.

Utkontraktering av systemkritiske betalingssystemer har forbedret effektiviteten i disse, men også økt den potensielle risikoen. IMF peker på at forbedringer kan gjøres ved å styrke risikostyring og administrasjonen av NICS. Et annet tiltak vil være å forbedre beredskapsplanene for NBO og NICS. Det vises til figur 1 for en oversikt over transaksjonsflyten i det norske betalingssystemet.

IMFs "Technical Notes" peker på mer konkrete tiltak for blant annet å minske den operasjonelle risikoen for FMI-foretakene som utgjør kjernekomponentene i landets finansielle infrastruktur. Sammenfattet er dette IMFs anbefalte tiltak på området:

- Styrke styring og kontroll med Norges Banks driftsutkontraktering av NBO og NICS.
- Utvide dagens samarbeidsavtaler mellom Norges Bank og Finanstilsynet til å omfatte krisehåndtering av FMI-foretak, samt utvide Beredskapsutvalget for finansiell infrastruktur (BFI) sin rolle ved kriser i finansiell infrastruktur.
- Bidra til økt synlighet ved å publisere egenvurderingene av CPMI/IOSCO-analyser.
- Etablere klare målsettinger for FMI-foretaks gjenopprettelsestid av IKT-løsninger.
- Analysere risiko i forbindelse med FMI-foretakenes bruk av multiple driftssteder.
- Analysere mulighetene for å redusere FMI-foretakenes avhengighet av sentrale leverandører(CSP).
- Utvikle samarbeidet med regulerende myndigheter i hjemland for CCPer (sentrale motparter) som opererer i Norge.
- Økt transparens rundt Finanstilsynets tilsynspraksis, for eksempel i ROS-analysen og på Finanstilsynets nettsted.

Samarbeid om tilsyn og overvåking av finansiell infrastruktur i Norge

En robust finansiell infrastruktur er avgjørende for finansiell stabilitet. Finanstilsynet vil i sitt IKT-tilsynsarbeid ha særlig oppmerksomhet mot sårbarhetsområder som kan medføre alvorlig svikt eller store forstyrrelser i den finansielle infrastrukturen og utgjøre en trussel for finansiell stabilitet.

Områder som vektlegges ved tilsyn er foretakets styring og kontroll av IKT-virksomheten og IKT-sikkerhetsarbeidet, inklusive arbeidet mot digital kriminalitet, robustheten i foretakets drifts- og beredskapsløsninger og foretakets håndtering av endringer og styring av tilgangsrettigheter.

Finanstilsynet og Norges Bank har gjennom flere år utviklet sitt samarbeid om tilsyn og overvåking av Norges finansielle infrastruktur, blant annet gjennom regulære samarbeidsmøter og samarbeid om risikovurderinger og felles tilsyn.

Finanstilsynets og Norges Banks tilsyns- og overvåkingsoppgaver av Norges finansielle infrastruktur er overlappende. Finanstilsynet har tilsynsansvar for registerfunksjonen i VPS samt verdipapiroppgjøret, mens Norges Bank har overvåkingsansvaret for de samme funksjonene. Finanstilsynet har tilsynsansvar for norske banker og bankenes betalingssystemer. Norges Bank har tilsynsansvar for interbanksystemene i Norge. Der interbank-/oppgjørssystemer tilbys av banker, vil dette operasjonelt sett i store trekk være en del av bankenes ordinære systemer. Observasjoner og tilbakemeldinger fra Finanstilsynets IKT-tilsyn med slike banker vil således være viktig informasjon som Norges Bank kan dra nytte av i sitt tilsyn med interbanksystemene.

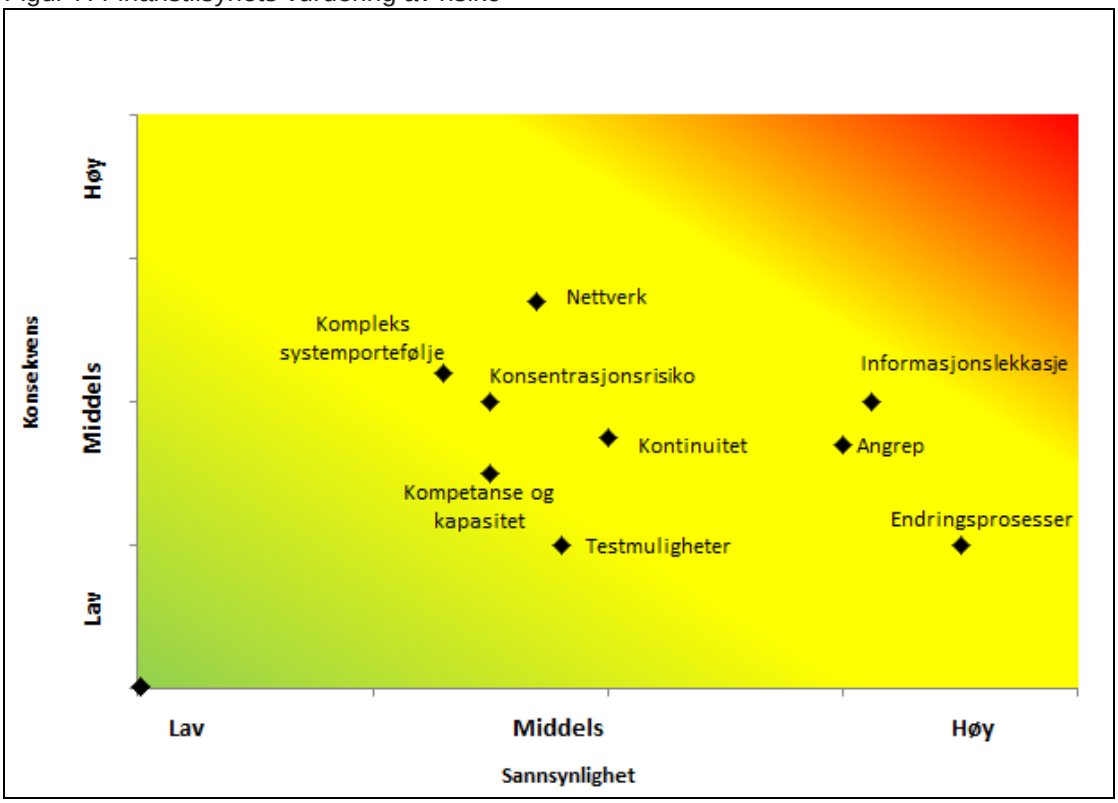
Finanstilsynet kan delta som observatør på tilsyns- og overvåkingsmøtene som Norges Bank har med FMI-foretakene, og Norges Bank kan delta som observatør på Finanstilsynets tilsyn med banker og datasentraler av betydning for finansiell infrastruktur.

6.2 Foretakene

Figuren under viser Finanstilsynets vurdering av de mest sentrale truslene mot og sårbarhetene i foretakenes systemer. I figuren er de ulike risikoområdene klassifisert etter sannsynlighet for at en negativ hendelse oppstår (lav, middels, høy) og konsekvensene dersom hendelsen oppstår (lav, middels, høy).

Finanstilsynets vurderer feil i nettverk, informasjonslekkasjer, digitale angrep, komplekse systemporteføljer og feil ved endringer som de mest sentrale truslene mot og sårbarhetene i foretakenes systemer. Andre trusler mot og sårbarheter i foretakenes systemer er mangelfulle kontinuitetsløsninger, konsentrasjonsrisiko, manglende testmuligheter og manglende kompetanse og kapasitet.

Figur 7: Finanstilsynets vurdering av risiko



Kilde: Finanstilsynet

Nettverk

Nettverk omfatter nettverk lokalt i foretakene, mellom foretakenes kontorer og datterselskaper, og koblinger til Internett (via ISPene). Det omfatter også nettverket mellom de ulike samarbeidspartene i bransjen. Nettverkene er komplekse og krever spesialkompetanse, ikke minst på brannmurer og forsvarsverket mot internett. Feil er i mange tilfeller forårsaket av fysiske hendelser som kabelbrudd, strømbrudd, anleggsarbeid eller naturhendelser.

Nettverksfeil kan være vanskelig å lokalisere hvis det er tekniske komponenter eller programvare som svikter, og reparasjoner kan også ta lang tid ved fysiske hendelser. Noen nettverk er kritiske for infrastrukturen.

Informasjonslekkasjer

Finanstilsynet mottar hvert år rapporter om uønsket eksponering av informasjon. Finanstilsynet har ved inspeksjoner konstatert mangelfull tilgangskontroll. Det er konstatert mangelfull klassifisering av systemer slik at informasjon ikke beskyttes tilstrekkelig. Foretakene har også mangelfulle logger over hvem som har hatt tilgang slik at graden av lekkasjer er vanskelig å bedømme. Nye aktører, som forventes å komme til med et mer deregulert marked, kan også ønske å bruke informasjonen som blir tilgjengelig for dem på en annen måte enn tidligere.

Konsekvensene av lekkasjer av persondata kan være høy for den det gjelder. For foretakene innebærer slike lekkasjer omdømmerisiko, og spesielt ved lekkasje av sensitiv informasjon kan de økonomiske konsekvensene være store.

Angrep

Angrepsfrekvens og -mangfold i nettangrepene øker. Foretakene har imidlertid bygget opp gode forsvar som reduserer sannsynligheten for at angrepene forårsaker stor skade.

I 2015 var det flere tilfeller av at angripere gjorde data utilgjengelige for foretaket og krevde løsepenger. Finanstilsynet er ikke kjent med at det har vært utbetalt løsepenger. Finanstilsynet er kjent med at forholdet har medført til dels betydelige kostnader knyttet til å reetablere dataene fra kopier og tapt arbeidstid ved manglende tilgang til systemer og data.

Kompleks systemportefølje

Drift av flerlagsarkitektur med systemer og applikasjoner på ulike tekniske plattformer som skal samspille er utfordrende. De ulike lagene i arkitekturen driftes ofte av ulike aktører. Dagskjøresyklusen for større finansforetak omfatter et stort antall enkeltoppgaver som er avhengige av hverandre og som må synkroniseres med eksterne leveranser fra andre foretak og samarbeidsparter. Ved endringer, også rent tekniske, kan noen avhengigheter bli utelatt. Avhengigheten mellom systemene er ikke alltid tilstrekkelig dokumentert. Avtaler og prosedyrer for samhandling ved feil mellom de ulike aktørene er ikke alltid gode nok.

Driftsfeil av denne typen kan være vanskelig å lokalisere. Det kan være behov for omkjøringer og opprettinger, og det kan medføre utilgjengelighet på tjenester som kan få konsekvenser både for foretaket og kundene.

Endringsprosesser

Endringer er en av de hyppigste feilårsakene på systemsiden, og endringstakten er høy.

De fleste feil etter endringer kommer raskt til syne, og foretakene har mulighet til å reversere disse før de får alvorlige konsekvenser. Finanstilsynet har imidlertid gjennom årene sett eksempler på endringer i nettverk og på datalagringssiden som har gitt lengre utfall av tjenestene.

Nærmere om endringsprosesser

Flere store finansforetak byttet IKT-leverandører i 2015. Det har vært enkelte uønskede hendelser knyttet til overgangene. God planlegging og testing hos foretakene har medvirket til at overgangene til nye leverandører totalt sett har vært vellykket.

Nye metoder for gjennomføring av finansielle tjenester ble tatt i bruk i 2015. Fingeravtrykk og QR-kode benyttes av enkelte til å autentisere kunden. App-er benyttes til betaling. Foretakene rapporterer om sterk konkurranse i markedet for nye betalingsmetoder.

Nye metoder for gjennomføring av finansielle tjenester kan være starten på en større omforming av dette markedet. Banker og betalingsforetak kan måtte endre seg betydelig som følge av ytterligere automatisering innenfor kreditt og betaling. Nytt betalingstjenestedirektiv (PSD2) legger premisser for inntreden av nye type aktører i markedet for betalingstjenester og kontoinformasjon.

Konsentrasjonsrisiko

Bankenes kjernesystemer driftes ulike steder. Nordea og DNB drifter hver for seg, Eika-bankene og en del mindre banker drifter hos SDC, og de andre sparebankene har sin drift hos Evry. Filialer av utenlandske banker i Norge har også ulike løsninger, de fleste hos sin morbank. Infrastruktur for betalingsformidling er i stor grad konsentrert hos Nets, men internasjonale kort og noen andre systemer håndteres også av Evry.
Forsikringssektoren og verdipapirnæringen har også i stor grad drift på ulike steder.

Kontinuitet

Finansforetak har kontinuitetsløsninger som vesentlig bygger på tidligere katastrofeløsninger. Overgang til kontinuitetsløsninger er hos mange foretak ikke automatisert. Det kreves manuelle inngrep og til dels koordinering mellom flere aktører før kontinuitetsløsninger kan iverksettes. Ved tilsyn har Finanstilsynet avdekket manglende krav til hva som er kritisk tilgjengelighet til systemene.

For betalingskortinfrastrukturen er det etablert velfungerende kontinuitetsløsninger.

Kompetanse og kapasitet

Antall ansatte i foretakene som har innsikt i systemene er få, blant annet som følge av utkontraktering. Kompetanse på en aldrende systemportefølje kan også være vanskelig å opprettholde fordi ansatte med slik kompetanse nærmer seg pensjonsalder, og det er lite nyrekruttering på tradisjonell stormaskinteknologi.

Det er knapphet på kompetanse på nettverksteknologi og forsvar mot digital kriminalitet.

Testmuligheter

Det er vanskelig å etablere produksjonslike testmiljøer. Ende-til-ende-test i en komplisert infrastruktur er vanskelig å få til. Ved tilsyn har Finanstilsynet også avdekket at testopplegg og testprosedyrer kan være mangelfulle.

Feil forårsaket av manglende test er erfaringsmessig relativt enkle å avdekke og kan raskt rettes eller reverseres uten alvorlige konsekvenser.

6.3 Forbrukere

BankID er den dominerende løsning for publikums tilgang til viktige tjenester innenfor og utenfor finanssektoren. BankID driftes på et felles driftssted for alle tjenestetilbydere som benytter BankID. I 2015 var det flere avbruddssituasjoner. Innenfor finanssektoren ble konsekvensene avdempet som følge av nye, alternative løsninger for tilgang til tjenestene. Det bør vurderes å etablere flere alternative løsninger og driftssteder.

Fra 1. august 2015 gjelder retningslinjene fra Det europeiske tilsynsorganet (EBA) om sikkerhet i Internett-betalinger. Retningslinjene fastslår at sterk autentisering er regelen. Det er økte krav til varsling og kommunikasjon med kunden. Kunden skal kunne sette bruksbegrensninger på kort, for eksempel slik at kortet ikke kan brukes til Internetthandel.

ID-tyveri er stadig en aktuell utfordring. Det er til enhver tid et stort antall pass på avveier. Pass kan være inngangen til å overta en identitet og å eskalere privilegiene. Nasjonale, signerte sperreregistre vil kunne avhjelpe dette.

Stadig flere kjøpsavtaler inngås på Internett. Oftest presenteres kunden for en omfattende avtaletekst i betalingsøyeblikket. I denne situasjonen kan avtaleteksten være vanskelig tilgjengelig. Det er grunn til å anta at i en rekke tilfeller er betingelser mv. ikke oppfattet av kunden i tilstrekkelig grad før kjøpet finner sted.

Informasjon som kunden legger igjen direkte (personinformasjon) og indirekte (kjøp, samt søk som gjøres på nettet) blir solgt og gjenbrukt i målrettet reklame. Kunden skal kunne styre bruken av persondata. Bevisstheten rundt dette synes å være lav, både blant innsamler og avgiver av data.

Kundens tilgang til konto og transaksjoner blir stadig enklere. Kunden kan følge med på kontoer og bevegelser og reagere ved mistanke. Risikoen er dermed redusert.

Foretakene varsler kunden på SMS om transaksjoner, sperringer, antatt misbruk og annet i større grad enn før. Videre kan kunden kan avgrense bruksområdet for kort. Dette gir kunden bedre kontroll og bedre forutsetninger for å kontrollere risikoen.

Måten finansielle tjenester utføres på endres svært raskt. Det er en fare for at eldre kunder ikke "henger med", og at disse må betale høye gebyrer for å få utført finansielle tjenester.

Forbrukerombudet mottar jevnlig henvendelser fra foreldre som har fått høye spill-regninger etter at barna har brukt telefonen deres. Spillene kan være gratis, men man må ofte betale for å oppnå fordeler. Via både App Store og Google Play kan man risikere å bruke mange tusen kroner med noen få tastetrykk.

Enkelte betalingsløsninger er utformet slik at når du kommer til kassen får du tilbud om blant annet å "delbetale i egen takt". I de senere årene har det vært en økning i antallet tilbud om avbetaling når kunder handler på nett.

Avbetalingsavtaler kan bli dyre for den enkelte forbruker, og det er viktig at regelverket følges slik at kunden får den informasjonen som trengs for å vurdere tilbudet. Avtaler som er fremstilt på en liten flate (mobil) og i en "presset" kjøpssituasjon, er mindre egnet i denne forbindelse.
Kredittavtaler skal signeres, enten ved hjelp av godkjent elektronisk signatur som Bank ID, eller med penn på papir. Det finnes eksempler der finansforetaket har inngått avtaler med forbrukere uten at forbrukeren har skrevet under på gyldig måte.

Falske PC-hjelpere var aktive i 2015. De falske hjelperne ringer og utgir seg for å være Microsoft-ansatte som skal hjelpe forbrukeren med et problem. Ofte påstår de at det er et virus eller en feil på maskinen, og at løsningen er å installere programvare som svindlerne anbefaler. Denne må forbrukeren betale for ved å oppgi kortnummer og kode. Gir forbrukeren ut betalingsinformasjon til svindlerne, kan forbrukeren i verste fall ende opp med å måtte dekke tap opp til 12.000 kroner fra egen lomme, etter en avgjørelse i Finansklagenemnda i en sak om Microsoft-telefonsvindel, da nemnda mente at forbruker hadde vært grovt uaktsom.

Andre oppringere ber forbrukeren om å gi dem fjerntilgang til PCen. Uten at forbrukeren vet det, gis svindleren full tilgang til datamaskinen. Det er kjent at forbrukere som har gitt svindlerne fjerntilgang, har fått tømt både kredittkort og bankkontoer.

7 Finanstilsynets oppfølging

7.1 IKT-tilsyn og annen kontakt med foretakene

Oppfølging av foretakenes IKT-risikoer skjer primært gjennom stedlige tilsyn. Finanstilsynet vil i 2016, som i 2015, ha stor oppmerksomhet på de tilsynsenhetene og deres leverandører som har størst innvirkning på finansiell stabilitet og velfungerende markeder.

Særlig oppmerksomhet vil være rettet mot utkontraktering av sentrale og beredskapskritiske IKT-systemer. Finanstilsynet vil spesielt følge opp finansforetak som gjennomfører større endringer på IKT-området, inkludert utkontrakteringer, og som derved øker den operasjonelle risikoen i endringsperiodene.

Finanstilsynet vil fortsette sin oppfølging av foretakenes beredskaps- og kriseløsninger. Via foretakstilsyn vil en også følge driftsstabilitet og strukturelle endringer hos tilsynsenhetenes leverandører. Etterlevelse av regelverk, som blant annet melding om ny eller endret utkontraktering av IKT og etterlevelse av IKT-forskriftens bestemmelser om utkontraktering, vil bli fulgt tett opp. Tilgangskontroller, telefonlogging og hvitvasking vil også være områder som vises oppmerksomhet.

Risikovurderinger vil bli fulgt nøye, spesielt ved innføring av ny teknologi hvor dette også kan skape mulighet for nye sikkerhetsrisikoer.

7.2 Arbeid med betalingssystemer

Kontroll med etterlevelse av regelverket er en viktig oppgave, samtidig som nødvendig utvikling av regelverket er viktig på et område hvor det er stor grad av dynamikk.

Der det gjennomføres større endringer på betalingssystemer, enten ved utvikling av nye løsninger eller ved utkontraktering, vil Finanstilsynet følge opp dette ettersom det kan medføre økt operasjonell risiko.

Retningslinjer for sikkerhet for Internett-betalinger vil følges opp mot finansnæringen gjennom selvevaluering, stikkprøver og penetrasjonstesting mot Internett-baserte løsninger.

Samarbeidet med Norges Bank vil videreføres.

7.3 Oppfølging av hendelser

Omfanget av alvorlige hendelser utviklet seg positivt i 2015. Finanstilsynet vil i 2016 fortsatt følge nøye med på utviklingen av alvorlige hendelser, og legge vekt på at årsak(er) blir funnet og tiltak iverksettes for å hindre gjentakelser.

7.4 Beredskapsarbeid

Arbeidet i Beredskapsutvalget for finansiell infrastruktur (BFI) vil videreføres, blant annet med oppfølging av stabiliteten i betalingsinfrastrukturen, hendelsesscenarioer og vurdering av om ansvarsforhold ved krisesituasjoner er tilstrekkelig klare. Det er planlagt gjennomføring av to øvelser i 2016.

Finanstilsynet vil også ta del i relevant beredskapsarbeid initiert fra andre sektorer vedrørende betalingsinfrastrukturen og betalingstjenester og foretakenes bruk av IKT.

7.5 Videreutvikling av tilsynsverktøy

Internasjonal beste praksis som COBIT, ITIL og ISO er lagt til grunn for egenevalueringsmetodene som Finanstilsynet benytter i sine IKT-tilsyn og tilsyn med betalingsformidlingen. Det er vesentlig at tilsynsverktøyet er à jour med beste praksis og tilsynsmodulene vil etter hvert bli oppdatert i henhold til COBIT 5.

I arbeidet med å utvikle tilsynsverktøy og -metodikk samarbeider Finanstilsynet tett med andre lands og EUs tilsynsorganer, blant annet med EBAs enhet for IKT-tilsyn TFIT (Taskforce on IT Risk Supervision).

7.6 Oppfølging av trusselbildet knyttet til digital kriminalitet

Finanstilsynet vil fortsette sin tette oppfølging knyttet til utviklingen innen digital kriminalitet og ha særskilt oppmerksomhet rettet mot foretakenes tiltak og beredskap mot det økende trusselbildet og håndtering av hendelser. Økt trusselnivå krever mer innsats og økt samarbeid mellom aktørene, og Finanstilsynet vil søke å bidra til dette.

7.7 Forbrukervern

Finanstilsynet vil legge vekt på at foretakene tar sikkerhet for kundene alvorlig og sikrer kundenes data mot deling uten samtykke eller kommer tredjepart urettmessig i hende.

Stabile betalingstjenester og tilgang til egne penger er også viktig for kundene. Foretakene må ha tjenester også for forbrukere som har utfordringer knyttet til å bruke ny teknologi.

Sikkerheten knyttet til nye betalingstjenester vil bli fulgt opp slik at risikoen for at det opprettes kundeforhold eller tjenester i andres navn, eller ved stjålet identitet blir minimalisert. Foretakets rutiner for å håndtere og være behjelpelig med å rette opp i slike forhold, om de skulle oppstå, vil også bli fulgt opp.

8 Ordliste

Begrep/forkortelse	Betydning
3-D Secure	3-D Secure er en XML-basert protokoll som benyttes ved nettbetaling. Den gir et ekstra sikkerhetslag ved bruk av kort, ved at bruker autentiserer seg overfor kortutsteder, uavhengig av betalingsmottaker. Hos Visa, som utviklet protokollen, heter den "Verified by Visa".
AIS	Account Information Supplier – Kontoinformasjonstilbyder
APT	Advanced Persistent Threat. Vedvarende angrep på systemer med formål å hente ut fortrolig informasjon. Normalt en kartleggingsfase hvor mange metoder benyttes, en gjennomføringsfase som foregår mest mulig skjult, ofte med lav intensitet, og gjerne en avslutningsfase for å skjule spor.
App	Applikasjon – på nettbrett eller mobiltelefon
AML	Tiltak mot hvitvasking (Anti Money Laundering)
Baltus	BAnkenes on-Line TransaksjonsUtvekslingsSystem. Nettverk som bankene bruker for blant annet dekningskontroll mot kontoer i hverandres kontosystemer.
BASH	Standard kommandotolk på mange GNU/Linux-systemer (gratis programvare)
BFI	Beredskapsutvalget for finansiell infrastruktur. Koordineringsutvalg ved kriser i finanssektoren. Ledes av Finanstilsynet.
Botnet	Botnet – laget ord fra robot og network. Et nettverk av programmer på ulike servere knyttet sammen via Internett. Programmene samarbeider om en gitt oppgave.
CARBANK	Et APT-virus som stjeler informasjon fra norske banker
CTB-locker	CTB-locker (Curve-Tor-Bitcoin). En ransomware som krever løsepenger i Bitcoin
CEO Fraud	Svindler gir seg ut for å være øverste leder i en bedrift. Kalles også 'Fake president fraud' eller 'Business Email Compromise'.
CEO-angrep	Nettangrep som bruker CEO Fraud
CERT	Computer Emergency Response Team. Ekspertgruppe som håndterer sikkerhetsbrudd på Internett.

Cloud Computing	Skytjeneste. Distribuert databehandling via et nettverk. Mulighet for å kjøre program på mange sammenknyttede servere. Skytjenester kan være både private og offentlige, eller en blanding av disse. Brukes ulikt av ulike leverandører, leveres over Internett.
CNP	Card Not Present. Svindel med hjelp av stjålne kortopplysninger, vesentlig ved netthandel.
CPMI/IOSCO	The Committee on Payments and Market Infrastructures/ International Organization of Securities Commissions
CVC-kode	Card Verification Code. Verifiseringskode; de tre siste sifrene bak på de fleste kredittkortene.
DNS	Domain Name System
DDoS-angrep	Et Internett-angrep som overbelaster en server ved at stor trafikk rettes mot serveren, gjerne ved bruk av et botnet. Hensikten er å hindre normal tilgang fra ordinære brukere.
Dyre	Skadevare, se http://www.symantec.com/connect/blogs/dyre-emerges-main-financial-trojan-threat
Dridex + ammyy	Malware i form av makroer i Microsoft Office-programmer. Ser "uskyldig" ut, men er farlig. http://blog.trendmicro.com/trendlabs-security-intelligence/banking-trojan-dridex-uses-macros-for-infection/
EBA	European Banking Authority. Den europeiske banktilsynsmyndigheten
ECB	European Central Bank. Den europeiske sentralbanken
EIOPA	European Insurance and Occupational Pensions Authority. Den europeiske tilsynsmyndigheten for forsikrings- og tjenestepensjon
ENISA	The European Union Network and Information Security Agency
ENISA	European Union Agency for Network and Information Security. Den europeiske etaten for nettverks- og informasjonssikkerhet
ESMA	European Securities and Markets Authority. Den europeiske verdipapir- og markedstilsynsmyndigheten
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FinansCERT	Finanssektorens felles CERT
FMI	Financial Market Infrastructure – betegner sentrale markedsaktører
FS-ISAC	Financial Services – Information Sharing and Analysis Center (FS-ISAC) er et europeisk tiltak primært med deltakere fra CERT-er, bankorganisasjoner og politimyndighet. I Norge er det samarbeid mellom NSM, BSK og Finanstilsynet. Foreløpig er det et uformelt samarbeid mellom enkeltland og definerte myndigheter, blant annet støttet av ENISA. I USA er det etablert en myndighetsenhet på samme område. Utveksler til dels konfidensiell informasjon om sårbarheter, angrep og tiltak knyttet til bruk av de elektroniske betalingsløsningene.

Gozi-ISFB	Skadevare, se: https://storify.com/bbddst/instructions-to-completely-remove-gozi-trojan-hors
GRFS-standarden	Standard for god regnskapsføringsskikk.
ISACA	En uavhengig, non-profit-organisasjon. Arbeider med å utvikle og fremme bruk av globalt aksepterte og industriledende kunnskap og praksis for informasjonssystemer. ISACA står for Information Systems Audit and Control Association, men har nå endret profil til en IT Governance-organisasjon.
ISO 20022	ISO 20022 er ISO-standarden for finansielle meldinger. Den inneholder beskrivelser av meldingene og forretningsprosessen og dets vedlikehold.
IRFS	Gjeldende standard for finansregnskap
ISP	Internet Service Provider – Leverandøren av internettforbindelse og domenenavn
Malware	Fellesbetegnelse for software med "fiendtlige hensikter". som virus, trojanere, ransomware mv.
Man-in-the-middle- angrep	Et angrep hvor angriperen i hemmelighet videresender kommunikasjon mellom to parter som tror de kommuniserer direkte med hverandre.
MIF-forordningen	Forordning om formidlingsgebyr for kortbaserte betalingstransaksjoner
MITM/MITB (inject mode)	Skadevare, se: https://en.wikipedia.org/wiki/Man-in-the-middle_attack
NBO	Norges Banks Oppgjørssystem
NICS	Norwegian Interbank Clearing System
NIS-direktivet	EU-direktiv som skal sikre høyt felles nivå på nettverks- og informasjonssikkerhet i EU.
NFC	Near Field Communication. Benyttes i enkelte betalingskort og mobiltelefoner (holde kort eller mobil nær betalingsterminalen).
NTP	Network Time Protocol. Brukes for å synkronisere klokkene i datamaskinene i et nettverk.
Off-shoring	Kjøp av tjenester utenfor landets grenser. Noen bruker det som begrep på kjøp utenfor Norden/ Baltikum
One-leg transaksjon	Transaksjon hvor den ene betalingstjenestetilbyderen har sete i et EU-/EØS-land, mens den andre betalingstjenestetilbyderen har sete utenfor EU-/EØS-området.
Outsourcing	Kjøp av tjenester utenfor eget foretak.
Passporting guidelines	Et betalingsforetak eller e-pengefortak i et EØS-land kan fritt etablere seg i annet EØS-land forutsatt at verken hjemlandets eller vertslandets myndigheter har vesentlige innvendinger. Prosessen når et slikt foretak, med lisens i et EØS-land ønsker å etablere seg i et annet EØS-land, kalles passporting. Passporting betyr i korthet meddelelse fra hjemlandet til vertslandet om at et foretak ønsker å drive virksomhet i vertslandet i form av filial eller agent. "Passporting guidelines" er veiledninger til hvordan dette skal gjøres.
PIS	Payment Initiation Suplier - Betalingstjenesteinitiatorer
Phishing	Å gi seg ut for å være en annen og be en person om opplysninger. Personens tillit til den originale avsenderen blir forsøkt utnyttet.

PKI	Public-key infrastructure. Består av maskinvare, programvare, prosedyrer, retningslinjer og personell som er nødvendig for å lage, forvalte, distribuere, bruke, lagre og kunne tilbakekalle digitale sertifikater.
Privacy Shield	Avtale mellom EU og USA. For sikring ved overføring av informasjon mellom partene. Ikke trådt i kraft p.t.
PSD2	Nytt betalingstjenestedirektiv fra EU (foreløpig et forslag).
Public cloud	Skytjeneste som tilbys til "alle" brukere"
QR-kode	Quick Response code er en mosaikkode for kommersiell og personlig bruk. Den kan lagre et svært stort antall alfanumeriske tegn og gjør at den kan leses svært hurtig. Den er derfor svært godt egnet til optisk lesing av data som eksempelvis en adresse.
Ransomware	Er en type skadevare som begrenser tilgang til IKT-løsninger som er infisert og krever en løsesum.
RAT-based "manuell" svindel	http://www.trusteer.com/glossary/remote-access-trojan-rat
Recovery-punkter	Gjenopprettelsespunkter
ReTeFe	Skadevare (DNS changer) Se: https://www.symantec.com/security_response/writeup.jsp?docid=2014-072516-1220-99
SMTP-servere	Simple Mail Transfer Protocol servere. Brukes for å sende og motta ekstern mail.
SSM	Single Supervision Mechanism. ECBs tilsyn for (system)viktige banker.
SSL	Secure Sockets Layer. Eldre krypteringsmetode, nå erstattet av TLS.
SecuRe Pay	European Forum on the Security of Retail Payments – forum under ECB
Skytjenester	Norsk for engelsk Cloud Computing, se dette.
Sterk autentisering	Autentisering ved bruk av flere faktorer, f.eks. pinkode + passord.
TFIT	Taskforce on IT Risk Supervision – arbeidsgruppe under EBA
TFPS	Taskforce on Payment Services – arbeidsgruppe under EBA
TLS	Transport Layer Security. En protokoll som brukes mellom e-postservere til å kryptere meldinger og levere dem trygt, og forhindrer tyvlytting og forfalsking mellom e-postservere.
TPP / Third Party Providers	Begrep fra PSD2-direktivet. Dette er tjenesteleverandører som yter betalingsformidlingstjenester og som normalt ikke kontofører betalers eller betalingsmottakers kontoer.
Trojaner	Virus som utgir seg for å være et vanlig program, men som inneholder ondsinnet kode.

Vawtrak	Skadevare, se: http://now.avg.com/wp-content/uploads/2015/03/avg_technologies_vawtrak_banking_trojan_report.pdf

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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

04.2016