FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

RISIKO- OG SÅRBARHETSANALYSE (ROS)

2016

Risiko- og sårbarhetsanalyse (ROS) 2016

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Finanstilsynet, 26. april 2017

INNHOLD

1 INNLEDNING 3

2 OPPSUMMERING 4
2.1 Finanstilsynets funn og observasjoner 4
2.2 Foretakenes vurderinger 7
2.3 Endringer i reguleringer 7
2.4 Aktuelle risikoområder 7

3 FINANSTILSYNETS FUNN OG VURDERINGER 9
3.1 Betalingssystemer 9
3.2 Bank 18
3.3 Verdipapirområdet 19
3.4 Forsikring 22
3.5 Eiendomsmeglerforetak – oppgjør 23
3.6 Tilsyn med etterlevelse av hvitvaskingsregelverket 23
3.7 Fellestiltak innen finansnæringen 24
3.8 Endringer i utkontraktering 26
3.9 Rapporterte hendelser i 2016 27
3.10 Observasjoner av digital kriminalitet 30
3.11 Utviklingstrekk innenfor finansiell teknologi 32

4 AKTØRENES VURDERING AV RISIKO 34
4.1 Intervjuer 34
4.2 Spørreundersøkelse om sårbarhet 36
4.3 Nasjonale vurderinger av trusselbildet 39

5 ENDRINGER I REGULERINGER 41
5.1 Samordning innen EU og endringer i EUs regelverk 41
5.2 Endringer i norsk regelverk 44

6 RISIKOOMRÅDER 46
6.1 Finansiell infrastruktur 46
6.2 Foretakene 47
6.3 Brukere og forbrukere 52

7 FINANSTILSYNETS OPPFØLGING 53
7.1 Sentrale områder for Finanstilsynets IKT-tilsyn 53
7.2 Arbeid med betalingssystemer 53
7.3 Oppfølging av hendelser 53
7.4 Beredskapsarbeid 54
7.5 Oppfølging av trusselbildet knyttet til digital kriminalitet 54
7.6 Forbrukervern 54

8 ORDLISTE 55

1 Innledning

Finanstilsynet utarbeider hvert år en risiko- og sårbarhetsanalyse (ROS-analyse) av finanssektorens bruk av IKT. Formålet med rapporten er å beskrive risiko og sårbarhet, både med hensyn til finansiell stabilitet, det enkelte foretak og den enkelte forbruker.

Gjennom tilsynsarbeidet har Finanstilsynet en bred kontaktflate mot 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.

Rapporten gir et oppdatert bilde av risikoen ved finanssektorens bruk av IKT og betalingstjenester, oppsummert i rapportens kapittel 2.

Kapittel 3 gir et bilde av Finanstilsynets funn og observasjoner i 2016. Teknologiske utviklingstrekk som antas å kunne få betydning for foretakenes bruk av IKT, blir omtalt. Kapittel 4 refererer finansforetakenes egne vurderinger. I tillegg er noen sentrale leverandører av tjenester og sikkerhetsløsninger intervjuet, og nasjonale vurderinger av trusselbildet med relevans for finansnæringen er referert.

Regelverksendringer som kan medføre omfattende endringer i foretakets systemløsninger, er omtalt i kapittel 5.

I kapittel 6 fremkommer Finanstilsynets overordnede vurdering av risikobildet i 2016 på bakgrunn av funn, observasjoner og utviklingstrekk. Vurderingene trekker frem de mest sentrale truslene og sårbarhetene som kan skade foretakenes systemer i et omfang som negativt kan påvirke målsettingen om finansiell stabilitet og velfungerende markeder.

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

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

2 Oppsummering

I 2016 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 både enkeltforetak og forbrukere. Det var også nedgang i antall gjennomførte svindler. Imidlertid var det også i 2016 en økning i tap i kroner på betalingskort og svindel mot nettbank.

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

2.1 Finanstilsynets funn og observasjoner

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

Betalingssystemer

Finanstilsynet vurderer betalingssystemene generelt som solide og stabile i 2016. Det er likevel rom for forbedringer. I flere foretak er det blant annet observert mangler ved kapasitetsovervåkning, kapasitetsstyring og kriseløsninger. Styring av operasjonell risiko kan også bli bedre.

I takt med utviklingen av nye betalingsløsninger, øker også sårbarheten og konsekvensene ved mangler i driftsløsningene, manglende kvalitet på testing ved endringer og mangelfull kapasitetsovervåkning og -styring. Det gjelder både for nye løsninger og ved videreutvikling av eksisterende betalingsløsninger.

Endringene på betalingstjenesteområdet drives ved at nye aktører kommer til, at eksisterende aktører tilbyr nye tjenester gjennom allerede eksisterende kanaler, og ved at nye samarbeidskonstellasjoner oppstår mellom banker eller mellom banker og nye aktører.

På kortområdet økte tapene i kroner med 9,5 prosent. Tapene i 2016 var i stor grad knyttet til svindeltypen "Card Not Present", som isolert økte med 39 prosent. Antall involverte kort gikk opp med 52 prosent. Beregnede samlede kostnader knyttet til kortsvindel (direkte tap og behandlingskostnader) økte med 28 prosent, til 428 mill. kroner, hvorav direkte tap utgjorde 206 mill. kroner.

Det var høy aktivitet på svindel mot nettbank, hvor tapene økte med 48 prosent til 18,6 mill. kroner. Svindelaktiviteten var i hovedsak rettet mot bedriftsnettbankene. FinansCERT rapporterer at mange angrep ble stoppet.

Finanstilsynet er ikke kjent med svindel mot mobilbetalinger, til tross for at trusselnivået er økende.

Bank

Bankene hadde også i 2016 store endringsprosesser på IKT-området, men endringene ble generelt gjennomført uten vesentlige konsekvenser for driftsstabiliteten.Mot slutten av 2016 og inn i 2017 var det imidlertid en negativ utvikling i driftsstabiliteten.

Risikoen for digitale angrep er tiltakende, og arbeidet med IKT-sikkerhet bør intensiveres ytterligere. Finanstilsynet ser behov for å bedre kvaliteten på tilgangsstyringen til systemene. Vedrørende beredskapsløsninger er det observert at konsekvensen ved bortfall av en eller flere applikasjoner ikke er tilstrekkelig utredet.

Gjennomføringen av hvitvaskingsregelverkets krav om oppdatert kontroll av kundene ved endringer i sanksjonslistene[1] er utfordrende. Finanstilsynet har også observert at de elektroniske overvåkningsscenariene er lite treffsikre. Dette medfører mange falske treff, som krever store kontrollressurser i bankene for skille disse fra ekte treff.

Verdipapirområdet

Sektorens økende utkontraktering av IKT-systemer med sensitiv informasjon kombinert med at informasjonen konsentreres hos få driftsselskaper, skaper utfordringer når det gjelder å beskytte sensitiv informasjon. Økende trusselbilde fra omverdenen krever bedre beskyttelse av sensitiv informasjon.

Forsikringsområdet

Mange foretak har fremdeles behov for å bedre sitt arbeid med risikoanalyser for å skaffe seg et riktig bilde av den samlede risikoen ved foretakets bruk av IKT. Finanstilsynet erfarer at risikovurderingene ofte er fragmenterte, og slik sett ikke et godt hjelpemiddel for risiko-styringen. IT-risikoene knyttet til utkontraktert virksomhet, er ofte ikke i tilstrekkelig grad vurdert og inngår ikke alltid i de årlige risikogjennomgangene av den samlede IT-risikoen.

Utkontrakteringsmeldinger

Aktørene utkontrakterer IKT-tjenester til tjenesteleverandører som tradisjonelt ikke har hatt utvikling eller driftstjenester til finansnæringen i sin tjenesteportefølje. Finanstilsynet fant ved mottak av meldingene om utkontraktering i flere tilfeller at avtalene var ikke oppfylte kravene i IKT-forskriften. Etter påtrykk fra Finanstilsynet og finansnæringen, har disse nye tjenesteleverandørene tilpasset kontraktene, slik at de følger regelverket.

[1] Blant annet FNs konsoliderte sanksjonsliste og EUs konsoliderte liste over personer, grupper og enheter som er underlagt finansielle restriksjoner.

Hendelser

Det rapporteres et synkende antall hendelser, og betalingssystemene og kunderettede tjenester var mer tilgjengelige i 2016 enn i året før. Derimot var det et økt omfang av svindelangrep. Flere foretak ble i 2016 utsatt for angrep med krav om løsepenger (ransomware).

Parallelt med utvidelsen av tilbudet om betalingstjenester på mobil, ikke minst BankID, har teleleverandørene fått større betydning for tilgjengeligheten til betalingstjenestene.

Digital kriminalitet

Kriminelle benytter i økende grad phishing og sosial manipulering (social engineering) for å trenge inn i foretakenes systemer, både for uthenting av sensitiv informasjon og til manipulering av betalingsoppdrag. Det er nødvendig at foretakene sikrer seg mot cyberangrep. Antall DDoS-angrep holder seg på et høyt nivå, men foretakenes forsvarsverk er gode. Det har forekommet noen tilfeller av ransomware. Finanstilsynet er ikke kjent med at løsepenger er utbetalt.

Det er observert en ny svindeltype hvor virus plantes på steder det er naturlig at ansatte i finansforetak besøker (vannhull). Viruset følger med over til datasystemene på den ansattes arbeidsplass, hvor det åpner en inngang som kan benyttes av kriminelle.

Ny teknologi

FinTech er en samlebetegnelse som beskriver ulike måter å endre/påvirke tradisjonelle finansielle tjenester gjennom bruk av teknologi, gjerne løsninger utviklet av teknologiselskap. En rekke nye aktører har kommet til i finansmarkedet, enten som konkurrenter til, eller i samhandling med, eksisterende virksomhet. Norsk finansnæring har i praksis drevet med teknologisk utvikling siden næringen tok i bruk IT i sine driftsløsninger.

I enkelte land gjennomføres forsøk med en såkalt "regulatorisk sandkasse", som innebærer at nye løsninger (FinTech) får noe friere reguleringer i en oppstartsperiode, under forutsetning av at løsningene følges nøye av tilsynsmyndigheten. Etter oppstartperioden gjelder ordinære reguleringer. Slike sandkasser er etablert i blant annet Storbritannia og Singapore. Norsk regelverk åpner per i dag ikke for slike løsninger. Finanstilsynet tilbyr imidlertid veiledning både knyttet til regelverk og til de planlagte tjenesteløsningene.

DLT (Distributed Ledger Technology) er en av teknologiene som er forventet å bidra til videre digitalisering og effektivisering av prosesser i finanssektoren, se nærmere omtale i punkt 3.11.2. Selv om eksisterende DLT-løsninger ikke er mange og synlige, er teknologien høyaktuell som fundament for utvikling av nye løsninger, f.eks. valutaoverføring mellom banker.

Bruk av DLT utredes av Verdipapirsentralen, i et samarbeidsprosjekt med Deutsche Börse, med tanke på å utvikle et grensekryssende system for sikkerhetsstillelser. Det er også etablert forsknings- og utviklingsprosjekter i flere banker og IT-selskaper.

2.2 Foretakenes vurderinger

Foretakene vurderer følgende trusler som de viktigste:

- manglende sikkerhetstenkning ved design av løsninger
- sikkerhet og tilgangsstyring
- beskyttelse av foretaksinformasjon
- kompleksitet i IKT-systemer
- omfanget av endringer og implementering av regulatoriske krav i systemene
- digital kriminalitet og inntrenging i systemer
- forstyrrelser i tilgjengeligheten på BankID, særlig på mobil

Andre trusselområder som trekkes frem av foretakene, er tilgang til kvalifiserte ressurser, manglende kunnskap for styring og kontroll ved bruk av skyløsninger, tap ved uautorisert bruk av kort i forbindelse med netthandel eller telefonhandel (Card Not Present) og at IKT-systemene ikke gir tilfredsstillende støtte til beslutninger, kundebehandling eller saksbehandling.
Forventninger fra markedet om nye og enklere løsninger utgjør en risiko ved at det ikke settes av nok tid til testing, spesielt av kapasitet og responstid.

Flere foretak ser også en risiko for at de ikke klarer å utvikle systemer som har høy nok presisjon når det gjelder å flagge mistenkelige transaksjoner og god nok datakvalitet for ivaretakelse av kravet til "kjenn din kunde".

2.3 Endringer i reguleringer

I 2016 pågikk 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. Reguleringsendringene vil på flere områder medføre behov for endringer i foretakenes systemløsninger eller prosesser og rutiner på IKT-området.

Den viktigste reguleringsendringen er EUs nye betalingstjenestedirektivet (PSD 2) og de utfyllende bestemmelsene som allerede er eller vil bli fastsatt. 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, forslag til nytt nasjonalt regelverk om hvitvasking og forskrift om formidlingsgebyrer i kortordninger.

2.4 Aktuelle risikoområder

Finansiell infrastruktur

Finanstilsynet vurderer den norske finansielle infrastrukturen som solid. Stabiliteten var i 2016 god og på linje med 2015, selv om det inntraff hendelser som medførte utilgjengelige betalingsløsninger og at sensitiv informasjon kunne kommet på avveie.

Foretakene

Finanstilsynet vurderer urettmessig tilgang til systemer og data, datalekkasje og datakriminalitet som de mest sentrale truslene mot og sårbarhetene i foretakenes systemer. Også kompleks drift, konsentrasjonsrisiko og feil i nettverk er sentrale trusler og sårbarheter. Andre risikoområder er mangelfulle kontinuitetsløsninger, manglende kompetanse og kapasitet, komplekse systemporteføljer og feil som oppstår ved endringer i systemene.

Forbrukere

Forbrukere som handler aktivt gjennom e-handelssystemer for verdipapirhandel, er sårbare for bortfall av tilgang til systemet, mens profesjonelle aktører ofte har tilgang til alternative e-handelssystemer for gjennomføring av handler.

Enkelte grupper av forbrukere får problemer når digitaliseringen medfører bortfall av eller vanskeliggjør bruk av manuelle betalingstjenester.

Manglende etterlevelse av retningslinjer for sikkerhet i Internett-betalinger hos betalingstjenesteytere reduserer forbrukerens muligheter til å beskytte seg mot svindel.

3 Finanstilsynets funn og vurderinger

Dette kapittelet omhandler funn og vurderinger basert på Finanstilsynets arbeid med IT og betalingstjenester i 2016. Kapittelet omtaler observasjoner fra IT-tilsyn, rapporterte hendelser, meldinger om endringer i utkontrakteringsavtaler, meldinger om nye eller endrede betalingstjenester og annen tilsynsvirksomhet.

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 foretak og for forbrukere, omtales også.

Finanstilsynets overordnede vurdering er at finansiell stabilitet og velfungerende markeder ikke var truet i 2016.

3.1 Betalingssystemer

3.1.1 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.

Betalingssystemer og -tjenester reguleres gjennom lover og forskrifter, samt gjennom finansnæringens selvregulering forvaltet av Finans Norge / Bits. Finansavtaleloven har som formål å ivareta forbrukerhensyn og sikre forbrukernes sikkerhet og rettigheter. Aktuelle regelverksendringer som berører betalingssystemene er beskrevet i kapittel 5.

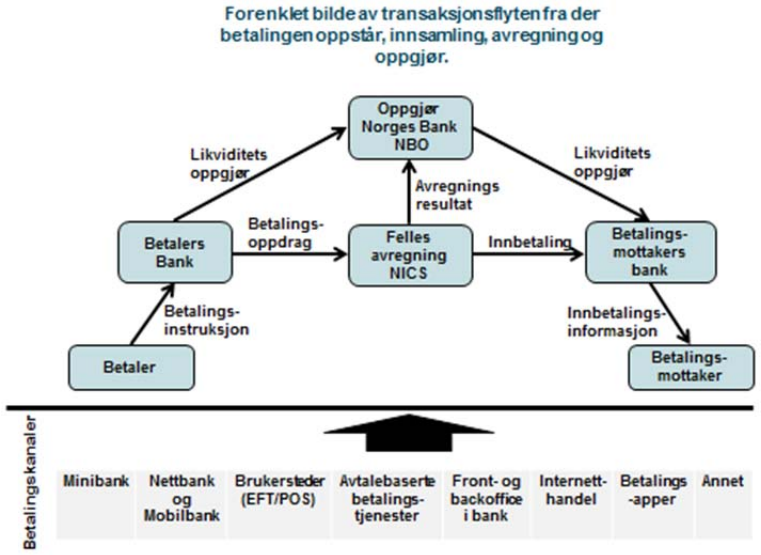
3.1.2 Styring og kontroll med risiko og sårbarhet i betalingssystemene

I takt med utviklingen av nye betalingsløsninger, både som alternativ til betaling med kontanter og for allerede etablerte elektroniske betalingsløsninger, øker også sårbarheten og konsekvensene ved mangler i driftsløsningene, manglende kvalitet på testing ved endringer og mangelfull kapasitetsovervåkning og -styring. Risikofaktorene gjelder også for eksisterende betalingsløsninger, der både betalingsformidlingen og teknologiene som brukes er under stadig forandring og medfører et løpende behov for endringer.

Høy endringstakt utgjør i seg selv en betydelig risiko. Det er derfor viktig at foretakene gjør grundige risikovurderinger knyttet til betalingstjenestene[2], både når det gjelder operasjonell risiko knyttet til

[2] Jf. forskrift om systemer for betalingstjenester

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

drift og vedlikehold av tjenestene og sikkerhetsmessig risiko knyttet til blant annet uautorisert bruk av tjenestene. Foretakene må, i tillegg til å sikre at tjenestene er beskyttet gjennom logiske og fysiske sikringstiltak og at informasjonen er tilstrekkelig beskyttet, sikre høy kvalitet både i driftsløsningene og i tilknyttede prosesser som kan påvirke driften.

Finanstilsynet har merket seg at flere foretak, særlig de større, har nedlagt betydelig arbeid i sine drifts- og beredskapsløsninger. Både flere driftssteder og redundante driftsløsninger benyttes for å redusere sårbarheten ved avvik i betalingsformidlingen.

Imidlertid har Finanstilsynet i 2016 observert en rekke hendelser som viser at kvaliteten på enkelte foretaks arbeid på disse områdene ikke er tilfredsstillende. Særlig synes mangelfull kapasitetsstyring å være årsak til en rekke hendelser. Det er også observert flere hendelser der redundansen i driftsløsningene, som skal sikre kontinuitet i disse, ikke har fungert tilfredsstillende ved avvik.

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

3.1.3 Beredskap for kontantdistribusjon i krisesituasjoner

Finanstilsynet og Norges Bank har gjennom tidligere fellestilsyn vurdert at beredskapen i det elektroniske betalingssystemet ikke var god nok og at ingen av de undersøkte bankene hadde

tilfredsstillende beredskap for distribusjon av kontanter i en krisesituasjon. Ettersom rekkevidden av bankenes plikter etter finansforetaksloven § 16-4 kan oppfattes som uklar, har Finanstilsynet og Norges Bank på oppdrag fra Finansdepartementet vurdert behovet for å presisere bankenes plikt til å sikre beredskap for kontantdistribusjon i krisesituasjoner og foreslått at dette presiseres i forskrift. Finansdepartementet har sendt forslag til forskrift[3] om beredskap for kontantdistribusjon på høring.

3.1.4 Meldinger om systemer for betalingstjenester

Lov om betalingssystemer stiller krav om at det uten unødig opphold skal gis melding til Finanstilsynet om etablering og drift av betalingstjenester. Følgende forhold utløser meldeplikt (omtalt i Finanstilsynets rundskriv 17/2004):

- 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 2016 mottok Finanstilsynet 20 meldinger om nye eller endrede betalingstjenesteløsninger. De aller fleste meldingene er knyttet til mobile løsninger. De øvrige meldingene var knyttet til andre typer betalingsløsninger eller sikkerhetsløsninger knyttet til bruk av betalingstjenester.

Med bakgrunn i innsendt melding, er enkelte foretak blitt bedt om supplerende informasjon. Blant annet er foretakene forespurt om informasjon om risiko- og sårbarhetsanalyser og sikkerhetstiltak for tjenesten, jf. krav som følger av forskrift om systemer for betalingstjenester.

3.1.5 Utvikling innen betalingstjenester og mobile betalingsløsninger

Betalingstjenesteområdet er preget av store endringer, med bakgrunn i blant annet teknologiutviklingen, endring i kundeadferd, elektronisk handel og reguleringer. Området blir gjennom PSD 2 gjenstand for ny regulering, som åpner opp betalingsmarkedet og gir nye aktører adgang til eksisterende aktørers kundeforhold/-tjenester. "Open banking" eller "API[4] -banking" betegner denne endringen som skjer globalt og hvor banker åpner for at nye aktører kan utvikle nye og verdiøkende tjenester for kundene basert på tilgang til eksisterende virksomhet, eksempelvis konto- og kundeopplysninger. Spesielt i etableringsfasen vil disse endringene innenfor betalingsformidlingen kunne skape nye risikoer og sårbarheter som må håndteres.

I Norge observeres denne utviklingen gjennom blant annet nye aktørers inntreden, eksisterende aktørers tilbud av nye tjenester gjennom eksisterende løsninger, nye samarbeidskonstellasjoner mellom banker eller mellom banker og andre aktører, og samarbeid mellom brukere av betalingstjenester.

[3] https://www.regjeringen.no/no/dokumenter/horing---beredskap-for-kontantdistribusjon/id2537040/
[4] API: Application Program Interface = grensesnitt åpnes på bakgrunn av reguleringer eller frivillig samarbeid

Nye aktører som Facebook og Amazon har etablert e-pengeforetak innen EØS og meldt om grensekryssende virksomhet. Det er imidlertid ennå ikke etablert virksomhet i Norge. Andre aktører som Apple og Google forventes også å gjøre sin inntreden, samt nye norske aktører som Payr[5].

Nye betalingsapplikasjoner ble tatt i bruk i 2016, blant annet SPING[6] (en rekke sparebanker) og Eika Safe[7] (Eika-bankene). Det er utviklet nye tjenester og ny funksjonalitet i betalingsapplikasjoner som MobilePay og Vipps. Imidlertid er det fortsatt slik at de mobile betalingsapplikasjonene i stor grad benytter egen infrastruktur som betinger at betalingsmottaker må installere samme applikasjon som avsender for å få tilgang til det overførte beløpet.

Det har i løpet av 2016 og inn i 2017 vært en vesentlig konsolidering på betalingsapplikasjonsområdet, med formål å møte konkurransen fra globale aktører når PSD 2 trer i kraft. Nordea og Gjensidige Bank har inngått samarbeid med Danske Bank om MobilePay. DNB har sammen med Sparebank 1-alliansen, Eika Alliansen og en rekke andre sparebanker innledet et samarbeid om Vipps.

Hittil har internasjonale betalingskort vært en forutsetning for bruk av de mobile betalingsløsningene. BankAxept er nå tilrettelagt for bruk i mobile betalingsapplikasjoner. I praksis innebærer det at BankAxept også er tilrettelagt for kontaktløs betaling med mobil, dersom den mobile betalingsapplikasjonen er tilrettelagt for kontaktløs betaling. BankAxept lanserte i 2016 kontaktløs betaling ved bruk av fysiske kort, med tilsvarende funksjonalitet som de internasjonale betalingsordningene VISA og Mastercard allerede har. BankAxept vil i løpet av 2017 lansere løsninger for konto-til-konto-betaling, både for bruk ved Internett-handel og i mobile betalingsapplikasjoner.

Manglende standardisering av butikkterminaler førte til at store brukersteder i 2016 etablerte Retail Payment[8], som en motvekt til finansnæringens manglende standardisering av mobile betalingsløsninger. Formålet er etablering av én felles infrastruktur med én terminalløsning for felles oppgjør for butikkene. Det innebærer at løsningen både skal kunne håndtere fysiske kort og betaling via mobil, enten via QR-koder, blåtann-kommunikasjon, trådløs kommunikasjon (NFC) eller Internett. Også andre tjenesteleverandører, som Nets og Verifone, utvikler nye betalingsterminaler som tillater at mobilbetaling i stor grad kan erstatte betaling med fysiske kort i løpet av 2017.

Finanstilsynet har i tidligere risiko- og sårbarhetsanalyser påpekt at manglende interoperabilitet for betalingsløsninger vil kunne forårsake redusert effektivitet og økte kostnader i betalingsformidlingen, noe som kan medføre behov for regulatoriske tiltak. Det er derfor positivt at flere banker nå har åpnet for bruk av tjenesten "straksbetaling" og at det i næringen ble satt en frist for å åpne for mottak av slike

[5] https://www.payr.no/
[6] https://www.sbm.no/naringsliv/betalingstjenester/sping/sping---lag-og-organisasjoner/514/2284/
[7] https://esbank.no/betale/kredittkort/eikasafe
[8] http://www.dn.no/nyheter/2017/03/06/2127/Finans/mobilepay-har-fatt-nokkel-til-10000-butikker-i-norden

betalinger[9]. Det er også etablert et prosjekt i regi av Norges Bank, Finans Norge og Bits, med mandat å vurdere og anbefale løsninger for felles infrastruktur for betalinger der formålet er å oppnå raskere oppgjør[10].

Utviklingen innen bruk av biometri i forbindelse med autentisering og betaling gir opphav til nye måter betalinger kan gjennomføres på, som for eksempel bruk av fingeravtrykk i butikkenes betalingsterminaler[11]. Finanstilsynet legger til grunn at omfattende risikovurderinger gjennomføres før ny teknologi i betalingsformidlingen blir tatt i bruk.

I tråd med voksende bruk av mobile løsninger, ikke minst knyttet til betaling, øker samtidig trusselbildet[12], selv om den teknologiske utviklingen gir gode muligheter for sikre mobile betalingstjenester. Det er observert et økende volum av ny skadevare, som også er mer avanserte og komplekse.

3.1.6 Sperring av kort for bruk på Internett

Retningslinjer for sikkerhet i Internett-betalinger trådte i kraft 1. august 2015. Etter retningslinjene skal kortholder kunne sperre kortet for bruk på Internett. Finanstilsynet har merket seg at ikke alle kortutstedere har implementert funksjonalitet etter disse retningslinjene i sine løsninger.

Finanstilsynet har påpekt mangelen overfor de aktuelle kortutstederne, som er bedt om å redegjøre for sine planer for å implementere funksjonalitet iht. retningslinjene. Se også punkt 3.2.3.

3.1.7 Betalingsterminaler – betalingskort

Finanstilsynet er kjent med at det, i strid med kortselskapenes bestemmelser, tilbys betalingsløsninger der betalingsterminalen kan lese informasjon kun fra betalingskortets magnetstripe. Betalingsterminaler som tilbys i dag må kunne akseptere transaksjoner der informasjonen hentes fra kortets chip.

Terminaler utplassert før 1. mai 2014 og som kun leser fra kortets magnetstripe kan frem til 1. januar 2021, under visse vilkår, benyttes der de ble utplassert. Disse terminalene kan ikke flyttes og benyttes andre steder.

Dette er regler som er fastsatt av kortselskapene[13]. Hovedhensikten med reglene er å begrense kortsvindel. Såkalt "skimming", der kriminelle monterer avlesningsutstyr på terminalen og leser av informasjonen i magnetstripen, med påfølgende belastning av kortet i forbindelse med kjøp på

[9] http://www.bits.no/wp-content/uploads/2016/10/2016-Bits-rundskriv-02-Krav-om-mottak-av-Straksbetalinger.pdf
[10] http://www.bits.no/wp-content/uploads/2016/12/Mandat-Betalinger-med-raskere-oppgjør.pdf
[11] https://www.dn.no/nyheter/2017/03/01/2046/Teknologi/fingeren-kan-bli-bankkort
[12] https://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf
[13] Det vises her til Visa Member Letter 69-13.

Internett, er én svindelform som er i bruk. Det vil i praksis ikke være mulig for en angriper å lese ut informasjonen fra kortets chip.

3.1.8 Angrep mot betalingstjenester

Angrep på betalingstransaksjoner utgjør hovedtyngden av angrep rettet mot betalingstjenestene. Slike angrep er nærmere beskrevet nedenfor. Observasjoner av digital kriminalitet mot finanssektoren i et bredere perspektiv omtales under punkt 3.10.

Tre ulike metoder benyttes for svindel med betalingstransaksjoner:

a) Svindleren initierer en transaksjon, som ikke er autorisert av kunden
b) Svindleren endrer en transaksjon, som er autorisert av kunden
c) Svindleren manipulerer kunden til å initiere en transaksjon

Ifølge hendelsesrapportene Finanstilsynet mottok i 2016, var antall ondsinnede angrep mot betalingstjenestene noe lavere enn i 2015. Selv om banker og betalingsforetak skal rapportere hendelser til Finanstilsynet, blir ikke hendelser med svindel av enkeltkunder rapportert, med mindre svindelscenarioet er nytt og avdekker spesielle sårbarheter. For samlet oversikt over tapene, se punkt 3.1.9. Mange av bankene er medlemmer i FinansCERT, som overvåker angrep mot betalingstjenestene. Informasjon fra FinansCERT, sammen med tapsstatistikken, supplerer Finanstilsynets egen hendelsesrapportering.

Svindel mot nettbank

I en periode i 2016 var det høy aktivitet knyttet til svindel mot nettbank. Metodene var både angrep med trojanere som infiserte kundens PC og "sanntids-fisking" av engangskoder. Svindlerne initierte transaksjoner som ikke var autorisert av kunden. Svindelaktiviteten var større enn tapstallene tilsier. Tiltak i bankene og gjennom FinansCERT bidro til at svindelforsøk ble avdekket og stanset i tide, blant annet ved å stoppe transaksjoner i mottakers bank. Et viktig forebyggende tiltak er å identifisere muldyr[14]-kontoer, slik at en alarm utløses ved forsøk på å gjennomføre transaksjoner til slike kontoer.

Svindel mot mobilbetalinger

På tross av det økende omfanget av mobile betalingsløsninger og økende trusselbilde, er Finanstilsynet ikke kjent med svindelforsøk i Norge basert på infiserte mobiltelefoner.

Forbrukerinformasjon

Det er Finanstilsynets vurdering at foretakenes informasjon til forbrukerne om hvordan de kan beskytte seg mot kort-, nett- og mobilbasert svindel stadig blir bedre.

[14] Muldyr: Personer som stiller egen bankkonto til disposisjon for raskt å flytte penger ut av landet.

3.1.9 Oversikt over årlige tap knyttet til betalingstjenester

Nedenfor er det gjengitt tapstall i Norge for henholdsvis kort- og nettbanksvindel for de siste årene.

En arbeidsgruppe under SecuRe Pay er i gang med å definere regler for å harmonisere innrapporteringen av tapstall i Europa[15], se punkt 5.1.1.

Tapstall i Norge for kortbruk

I 2016 var det 39 prosent økning i svindel av typen CNP, mens svindel gjennom skimming avtok. Totalt var det 9,5 prosent økning i tap på kortbetalinger i 2016, mens antall misbrukte kort økte med over 50 prosent. Gjennomsnittlig svindlet beløp per misbrukte kort var lavere enn året før.

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

Svindeltype betalingskort	**2012**	**2013**	**2014**	**2015**	**2016**
Misbruk av kortinformasjon, Card-Not-Present (CNP) (Internett-handel m.m.)	35 701	51 954	72 056	98 410	137 015
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort i Norge	2 308	762	524	2 670	1 360
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort utenfor Norge	55 869	51 534	51 685	48 447	41 762
Originalkort tapt eller stjålet, misbrukt med PIN i Norge	28 128	21 274	21 266	18 875	12 857
Originalkort tapt eller stjålet, misbrukt med PIN utenfor Norge	8 544	9 570	13 071	14 224	10 223
Originalkort tapt eller stjålet, misbrukt uten PIN	4 603	4 949	5 510	6 033	3 286
TOTALT	**135 153**	**140 043**	**164 113**	**188 660**	**206 503**

Kilder: Finanstilsynet og Bits

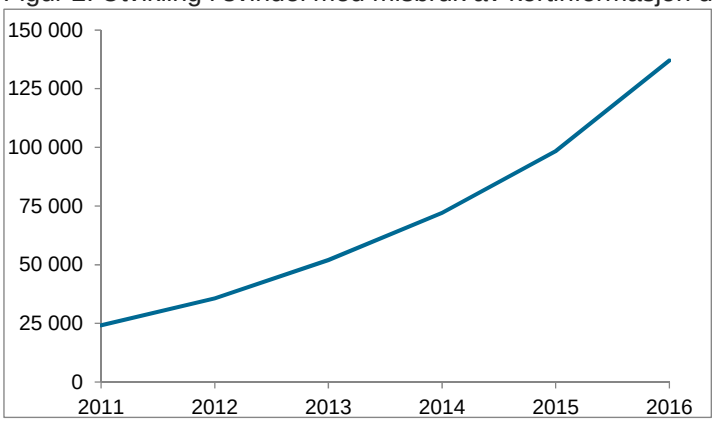
Verdien av korttransaksjoner med kort utstedt i Norge økte med 6 prosent fra 2014 til 2015, mens verdien av betalinger med kort utstedt i Norge for varekjøp på Internett økte med 16,8 prosent[16]. Andelen svindel ved varekjøp på Internett (CNP) økte med 39 prosent fra 2015 til 2016. Svindel utgjorde noe over 0,17 prosent av all handel på Internett. Av den samlede verdien på kortbetalinger i Norge utgjorde svindel om lag 0,02 prosent[17].

[15] Arbeidsgruppens mandat er å implementere PSD 2, artikkel 96(6) krav til årlig innrapportering av svindelstatistikk.

[16] http://www.norges-bank.no/Publisert/Publikasjoner/Norges-Bank-Memo-/2016/Norges-Bank-Memo-12016/

[17] Norges Bank publiserer først i mai 2017 tall for 2016. Sammenligningene er derfor gjort mot tall fra Norges Bank for 2015. Tall fra Norges Bank viser at den samlede verdien på Internett-kjøp i 2015 var 80 mrd. kroner. Tap gjennom CNP på 137 mill. kroner utgjør 0,17 prosent av 80 mrd. kroner. Totalt var verdien av kortbetalinger 855 mrd. kroner i 2015. Tap med betalingskort på 206 mill. kroner utgjør 0,024 prosent av 855 mrd. kroner.

Figur 2: Utvikling i svindel med misbruk av kortinformasjon der kort ikke er til stede (CNP)



Kilder: Finanstilsynet og Bits

Kortsvindel og datatyveri

Alle kort utstedt i Norge har chip, og det er et fåtall betalingsterminaler (typisk knyttet til kjøp av kioskvarer fra automater og betaling av parkering) i Norge som bruker magnetstripen, ref. punkt 3.1.7. Derfor er tapene knyttet til misbruk av falske kort i Norge lave. Kort eller kortinformasjon som stjeles i Norge brukes derimot i land hvor det fortsatt er vanlig å bruke magnetstripen, som er årsaken til at tapstallene for misbruk av falske norske kort er større i utlandet enn i Norge.

Kostnader forbundet med kortsvindel

Finanstilsynet har utarbeidet et anslag for samlede kostnader forbundet med stjålet 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 stjålet kortinformasjon. (Saksbehandler- og forbrukerkostnader er holdt konstant for årene 2012–2016.)

Tabell 2: Kostnader forbundet med kortsvindel (beløp i hele tusen kroner)

Kostnader ved svindel med betalingskort	**2012**	**2013**	**2014**	**2015**	**2016**
Antall kort rammet av misbruk (antall)	20 332	22 531	38 541	44 900	68 162
Samlede direkte tap, jf. tabell 1	135 153	140 043	164 113	188 660	206 503
Saksbehandlerkostnader hos kortutsteder (2.250 kroner per kort)	45 747	50 695	86 717	101 025	153 365
Forbrukerkostnader (1.000 kroner per kort)	20 332	22 531	38 541	44 900	68 162
Samlet beregnet kostnad	**201 232**	**213 269**	**289 371**	**334 585**	**428 030**

Kilde: Finanstilsynet

I tillegg til kostnadene som fremkommer i tabell 2, kommer ytterligere kostnader knyttet til saksbehandling hos kortinnløsere, brukersteder og hos Finansklagenemda og, i noen tilfeller, til advokathonorarer og rettsbehandling. Samlede kostnader forbundet med kortmisbruk er derfor betydelige. Antall kort som ble misbrukt i 2016 var 68 162, over 50 prosent flere enn året før. De

samlede kostnadene ved kortmisbruk økte i 2016 derfor prosentvis langt mer enn det direkte kronetapet på kortbetalinger.

Tapstall knyttet til bruk av nettbank

Tapstall knyttet til bruk av nettbank økte noe i 2016. I tillegg til svindelen som reflekteres i beløpene i tabell 3 nedenfor, var det mange tap som ble avverget fordi transaksjonene ble stoppet før de ble gjennomført, eller fordi beløp ble tilbakeført fra mottakerbank. Bankene, i samarbeid med FinansCERT, arbeider kontinuerlig med å overvåke og stoppe nettbanksvindel.

Tabell 3: Tap ved bruk av nettbank (beløp i hele tusen kroner)

Svindeltype – nettbank	**2012**	**2013**	**2014**	**2015**	**2016**
Angrep ved bruk av ondartet programkode på kundens PC eller sikkerhetsmekanisme (trojaner)	5 064	1 327	552	3 055	2
Tapt/stjålet sikkerhetsmekanisme	3 367	1 285	6 655	963	8 758
Phishing og falske BankID-brukersteder	10		539	5815	2 428
Annet/ukjent	358	779	3 474	2 715	7 444
TOTALT	**8 799**	**3 391**	**11 220**	**12 548**	**18 632**

Kilder: Finanstilsynet og Bits

Tap ved CEO-fraud

CEO-fraud (direktørsvindel) økte i omfang i 2016. Ved CEO-fraud blir kundene manipulert til å autorisere transaksjoner. Svindelscenarioet er basert på sosial manipluering, og ikke på å utnytte tekniske sårbarheter eller svakheter i bankenes systemer. Bankene bidrar ofte til å stoppe transaksjonene hos mottakerbank og få tilbakeført beløpene. CEO-fraud førte til betydelige tap i 2016. Tallene er neppe fullstendige, da kundene ikke nødvendigvis kontakter banken hver gang de opplever denne typen svindel.

Tapene som ble rapportert til Bits viser et tap på CEO-fraud i 2016 på nesten 300 mill. kroner. Dette er mer enn tapene gjennom betalingskort og tapt beløp per sak[18] er høyt, i gjennomsnitt nær 1,4 mill. kroner per tilfelle.

Tabell 4: Tap ved CEO-fraud (beløp i hele tusen kroner)

Tap ved CEO-fraud	**2016**
Antall saker	214
Gjennomsnittlig tap per sak	1 374
TOTALT	**294 061**

Kilder: Finanstilsynet og Bits

[18] Én sak kan omfatte flere transaksjoner

3.2 Bank

Bankene har også i 2016 vært gjennom store endringsprosesser på IKT-området. Endringene er i store trekk gjennomført uten vesentlige konsekvenser for driftsstabiliteten. Stabiliteten hadde imidlertid en negativ utvikling mot slutten av 2016 og inn i 2017.

3.2.1 Bakdører inn i kjernesystem

Finanstilsynet har gjennom IKT-tilsyn observert ulik tilgangsstyring til hhv. saksbehandlingssystem og kjernesystem i foretak, og der samme type oppgaver kan utføres gjennom begge tilgangene. Funnene viser god tilgangsstyring for frontsystemene som begrenser hva en bruker av systemene kan gjøre, mens tilsvarende begrensninger ikke er etablert ved direkte innlogging mot kjernesystemet, f.eks. ved tilgang til lånesystemet. Dette medfører mulighet for omgåelse av hvordan systemene er ment brukt. Bankene må gjennom samordnet tilgangsstyring sikre konsistens for hva en bruker kan gjøre i et system uavhengig av hvilken tilgang som benyttes.

3.2.2 Tilgangsstyring

Finanstilsynet har i 2016 gjennomført flere IKT-tilsyn med særlig oppmerksomhet rettet mot foretakenes tilgangsstyring og -kontroll. Erfaringen fra tilsynene er at foretakene i stadig større grad legger ned betydelig innsats i arbeidet med tilgangsstyring og -kontroll. Likevel er det Finanstilsynets vurdering at dette området må ha stor prioritet i foretakene siden risikoen for misbruk eller utilsiktede hendelser kan være betydelig. Særlig bør brukere med særskilte privilegier, som f.eks. administrasjonsbrukere, kontrolleres nøye, men også kontroll med etterlevelse av prosessene for etablering, endring og avslutting av en brukerident må være en del av oppfølgingen.

3.2.3 Etterlevelse av retningslinjer for Internett-betalinger

I september 2015 publiserte Finanstilsynet retningslinjer for sikkerhet i Internett-betalinger. Retningslinjene definerer European Banking Authoritys syn på hva som er god tilsynspraksis innenfor det europeiske finanstilsynssystemet, og hva som er minimumskrav for sikker Internett-betaling. Retningslinjene bygger på direktiv 2007/64/EC Payment Services Directive (PSD).

Gjennom tilsyn har Finanstilsynet i noen tilfeller identifisert løsninger som ikke overholder retningslinjenes krav til sterk kundeautentisering. Finanstilsynets vurdering er at autentiseringsløsninger iht. retningslinjene vil være et godt bidrag til å redusere svindel knyttet til betalinger med "Card Not Present" (Internett-betalinger).

3.2.4 Utkontrakteringsavtaler

Finanstilsynet har ved tilsyn avdekket flere tilfeller hvor foretak har etablert avtaler om utkontraktering som ikke følger gjeldende regelverk. For finansforetak gir lov om finansforetak regler for utkontraktering, jf. § 13-4.

Etter loven har foretaket ansvaret for utkontraktert virksomhet. Loven krever videre at tilsynet ikke kan bli vanskeliggjort (innsyn i utkontraktert virksomhet) som følge av utkontrakteringen. Kompetanse i

foretaket til å håndtere utkontraktert virksomhet ligger implisitt i kravet om at virksomheten må være forsvarlig. IKT-forskriftens § 12 stiller krav om skriftlige avtaler, som er avgjørende for å kunne oppfylle generelle krav til virksomhetsstyring, herunder meldeplikten.

For foretak under tilsyn som ikke faller inn under finansforetaksloven, gjelder forskrift om internkontroll og risikostyring.

3.2.5 Beredskapsløsninger og konsekvensanalyser

Foretakene har stadig større oppmerksomhet rettet mot beredskapsløsninger som skal sikre en sikker og effektiv drift, også dersom normalt tilgjengelige tekniske løsninger bortfaller. Finanstilsynet har observert svakheter i foretakenes analyser av mulige konsekvenser ved bortfall av en eller flere applikasjoner (Business Impact Analysis). Svakhetene er knyttet til mangler i foretakenes dokumentasjon av hvilken teknisk infrastruktur som kreves for å etablere en velfungerende beredskapsløsning.

3.2.6 Distribusjon av sensitiv informasjon via e-åpen post

Finanstilsynet observerte i 2016 tilfeller av at bankkontoutskrifter og annen informasjon med sensitivt innhold ble distribuert gjennom åpen e-post til bankkunder. Åpen e-post passerer mange knutepunkter på veien fra bank til kunde og kan avleses underveis. Finanstilsynet vurderer derfor ikke e-post som en direkte eller sikker kommunikasjon mellom bank og kunde. Det vises i den sammenheng til Finanstilsynets rundskriv 10/2007, som omhandler taushetspliktsreglene for finansnæringen om kunders forhold mv.

3.2.7 Innføring av meldingsformatet ISO 20022 for filbaserte euro-betalinger

Finansavtaleloven § 9 (3)[19] stiller krav om at kredittoverføringer og direkte debiteringer i euro fra 31. oktober 2016 skal gjennomføres med meldingsformatet ISO 20022[20]. For å kartlegge om bankene følger opp kravet overfor sine bedriftskunder, gjennomførte Finanstilsynet en spørreundersøkelse i norske banker og filialer av utenlandske banker. Et ikke ubetydelig antall bedriftskunder hadde ikke konvertert til ISO 20022 for filbaserte euro-betalinger innen fristen, men de fleste vil være på plass i løpet av første kvartal i 2017. Flere banker tilbyr bedriftskundene en konverteringsløsning, som ligger på utsiden av nettbanken, inntil bedriften selv kan levere betalingene i riktig meldingsformat.

3.3 Verdipapirområdet

IKT-systemer i norsk verdipapirsektor har fortsatt god kvalitet og høy stabilitet. Sett i lys av trusselbildet og som følge av sektorens økende utkontraktering av IKT-systemer med sensitiv informasjon, er det imidlertid utfordrende å bevare et akseptabelt risikonivå fremover.
Flere omfattende regulatoriske endringer vil påvirke risikobildet for sektoren.

[19] I henhold til EØS-avtalens vedlegg XII nr. 3a (EU-forordning nr. 260/2012)
[20] Kravet gjelder når en betalingstjenestebruker som ikke er en forbruker eller svært liten bedrift, iverksetter eller mottar enkeltstående kredittoverføringer eller enkeltstående direkte debiteringer som ikke overføres enkeltvis, men samlet.

3.3.1 Aktørers motiv for digitale angrep mot norsk verdipapirsektor

Verdipapirområdets informasjonssystemer inneholder store mengder sensitiv informasjon om foretak i norsk næringsliv. Trusselvurderingene som i 2017 er kommet fra PST, den militære e-tjenesten og Norges sikkerhetsmyndigheter, indikerer at sensitiv informasjon å være det primære målet for informasjonsinnhenting for utenlandske aktører støttet av fremmede stater (statlig industrispionasje). For mer informasjon om nevnte trusselbilde, se punkt 4.3.

Utenlandske statlige aktører kan ha flere motiv for å kompromittere verdipapirsektorens IKT-systemer. Motivet kan være informasjonsinnhenting for å tilføre egne foretak informasjon om norske konkurrerende selskapers strategier, planer og teknologi for å styrke eget lands industri. Motivasjonen kan også være å skaffe til veie informasjon som letter oppkjøp av foretak der interessant kompetanse, løsninger og teknologi finnes.

Ved at uvedkommende aktører skaffer seg tilgang til og gjør bruk av kurssensitiv informasjon kan tilliten til norsk finansindustris integritet påvirkes, og dermed redusere investorers vilje til å investere i norsk næringsliv, som igjen påvirker norsk økonomi og arbeidsplasser negativt.

3.3.2 Funn på verdipapirområdet

Finanstilsynet registrerte i 2016 flere foretak med utilstrekkelig tilgangskontroll for systemer med sensitiv informasjon i tilfeller der foretakene har utkontrakterte sine løsninger. Dette er bekymringsfullt da stadig mer av forvaltningen av informasjonssystemene i verdipapirforetakene utkontrakteres.

Finanstilsynet har observert at mange foretak legger stor vekt på risikoanalyser som gjennomføres av datasentrene, uten at foretaket selv er involvert. Dette kan føre til at risikoanalysen ikke tilpasses risikonivået for foretakets særskilt sensitive data.

Gjennom IKT-tilsyn har Finanstilsynet funnet eksempler på utkontrakteringsavtaler der foretak har fraskrevet seg retten til å gjennomføre inspeksjoner og revisjoner av egne løsninger hos driftsselskapene. Det er i strid med IKT-forskriftens § 12 Utkontraktering. Det er også registrert foretak som ikke fører kontroll med tilgangsstyring av egne systemer overfor ansatte i driftsselskapene. Logging av aktivitetene som ansatte i driftsselskapene gjennomfører, og hvilke data de aksesserer, har også vist seg mangelfull, også for systemer som behandler og lagrer kurssensitiv informasjon.

Finanstilsynet har erfart at ansatte i IKT-driftssentre har handlet verdipapirer i foretak man forestår IKT-driften for i perioder med handelsbegrensing, noe som indikerer svake rutiner og lav bevissthet for risiko på dette området både hos foretak og driftssenter.

3.3.3 IKT-driftssentre

I Norge er det på verdipapirområdet et fåtall driftsselskaper som dominerer markedet for utkontrakterte IKT-driftstjenester. Disse selskapene har tradisjonelt vært benyttet til drift av IKT-løsninger for banker og bedrifter. Nye typer foretak ønsker også å nyttiggjøre seg driftssikkerheten, kostnadseffektiviteten og skalerbarheten til løsningene som leveres av de etablerte driftssentre. Eksempelvis kan børsnoterte selskaper, advokater og verdipapirforetak ønske å lagre og prosessere regnskapsinformasjon, strategidokumentasjon og korrespondanse vedrørende oppkjøp og finansiering i systemer som utkontrakteres til denne typen leverandører. Typiske løsninger som ønskes utkontraktert er e-postsystemer, filsystemer og regnskapssystemer.

Trusselbildet for driftssentre, som kan omfatte sterkt motiverte interessenter som disponerer tilstrekkelige ressurser, slik som ledende hackermiljøer understøttet av nasjonalstater, vil ikke alene kunne nøytraliseres ved hjelp av oppdaterte brannmurer, virusprogram, informasjonskampanjer, gode prosesser og mikrosegmentering. Metodene for å nå informasjon i datasentrene vil ikke være begrenset til bruk av elektroniske angrep. Angriperne vil også kunne benytte ulike former for sosial manipulering, som utpressing o.l. for å oppnå tilgang til data. Foretak under tilsyn må derfor regelmessig gjennomføre egne risikovurderinger for IKT-sikkerheten i sine driftssentre og se til at sikringstiltak blir tilpasset den type data/informasjon som lagres og prosesseres.

Når flere ulike aktører, både foretak under tilsyn og foretak som ikke er under tilsyn, benytter samme driftsleverandør, resulterer det i konsentrert lagring av store mengder sensitiv informasjon. Driftsleverandørens systemer og rutiner for skjerming av data kan i utgangspunktet ha høyere kvalitet enn foretakene enkeltvis. Konsentrasjonen av sensitiv informasjon vil gi sterk motivasjon for uvedkommende til å skaffe seg tilgang til systemene som lagrer informasjonen, noe som stiller høyere krav til sikring. Foretak under tilsyn må i risikoanalysen ved utkontraktering av systemer ta hensyn til konsentrasjonen av sensitiv informasjon i driftsselskapet.

Driftsselskapene har hverken ansvar eller tilstrekkelig forutsetning for å gjennomføre konsekvensanalyser av at kundenes sensitive informasjon kommer uvedkommende i hende. Risikoanalysen av data er eierforetakets eget ansvar, ref. IKT-forskriftens § 3.

Finanstilsynet forventer at foretak under tilsyn fører en sterkere kontroll med sine IKT-driftsselskaper og deres systemer og personell, slik at informasjonslekkasjer forebygges.

3.3.4 Svak styring og kontroll med IKT-sikkerhet hos Nasdaq

Med bakgrunn i funn etter Finansinspektionens (det svenske finanstilsynet) IKT-tilsyn hos Nasdaq Clearing AB og Nasdaq Stockholm AB, der foretakene i 2016 ble ilagt sanksjoner på SEK 55 mill. kroner, vil Finanstilsynet fortløpende vurdere Nasdaq Oslo ASAs oppfølging av foretakets cybersikkerhetsvirksomhet for å sikre at foretaket etablerer relevante prosesser og tiltak for å beskytte sine systemløsninger.

Finansinspetionens tilsyn ble avholdt etter svensk regelverk, der EU-forordningen European Market Infrastructure Regulation (EMIR), som blant annet omfatter bestemmelser for IKT-området, er inntatt. Det ble under tilsynene lagt særlig vekt på kontroll med cybersikkerhet. Finansinspektionen anser at foretakene ikke oppfyller kravene til styring og kontroll av risikoen i egen virksomhet, særlig fordi styring og kontroll har vært utkontraktert til Nasdaqs morselskap. Ifølge rapporten er ikke de svenske foretakenes risiko håndtert særskilt. Grunnlaget for lokal kontroll med risikoen i de svenske foretakene ble dermed ansett mangelfull eller unødig vanskeliggjort. Det ble særlig påpekt at foretakenes kontinuitetsplan ikke omfattet noen form for tiltak mot cyberangrep. Foretakene manglet dermed alternative løsninger og planer for kritiske funksjoner og IKT-løsninger.

3.3.5 Reguleringsendringer som påvirker risikonivået

På verdipapirområdet medfører en rekke reguleringsendringer nye krav til foretakenes systemløsninger. Risikonivået påvirkes fordi systemene må endres, eller fordi foretaket risikerer støre bøter hvis foretaket ikke etterlever regelverket.

MiFID II og MiFIR stiller nye krav til verdipapirforetak og handelsplassers systemer for handel med finansielle instrumenter. Eksempler er nye krav om tidssynkronisering av handelssystemer, endrede krav til identifisering av deltakere i handel og utvidet TRS-rapportering. Varederivatposisjoner blir rapporteringspliktige og vil kreve nye IKT- løsninger. Etter innføring av EMIR, plikter alle foretak å rapportere inngåtte og endrede derivat-transaksjoner til et av EUs transaksjonsregistre.

General Data Protection Regulation (GDPR) erstatter personvernlovgivningen i Norge fra mai 2018. GDPR gir brukere høyere vern og foretak som behandler persondata større ansvar. Det stilles også høye krav til foretakenes IKT-systemer, og foretak som behandler persondata vil måtte gjøre endringer i sine løsninger. Brudd på reglene i GDPR kan medføre betydelige sanksjoner.

For ytterligere omtale av reguleringsendringer og systemkrav, se punkt 5.1.2.

3.4 Forsikring

3.4.1 Risiko ved mangelfulle risikovurderinger

Finanstilsynets erfaring er at gjennomføring av og forståelse for risikovurderinger fremdeles er et forbedringsområde for flere forsikringsforetak. Risikovurderinger som fremlegges for Finanstilsynet er ofte mangelfulle og fragmenterte, og synes ikke alltid å være et velegnet hjelpemiddel til å påse at virksomhetens IT-risiko er akseptabel.

Forsikringsforetakene har, som bankene, mye oppmerksomhet rettet mot Internett-sikkerhet (cyber security), primært knyttet til ondsinnete, kriminelle angrep. Finanstilsynet understreker at dette er en alvorlig risiko, men ikke den eneste. Selskapene må også være oppmerksomme på andre risikoer ved sin IT-virksomhet.

Selskapenes bruk av utkontraktering øker. Finanstilsynet har registrert at IT-risikoene ved den utkontrakterte virksomheten ofte ikke er vurdert i tilstrekkelig grad og ikke alltid inngår i den samlede, årlige risikogjennomgangen av IT-risiko etter IKT-forskriften.

3.4.2 Risiko ved bruk av regneark

Enkelte spesialister i foretakene benytter i utstrakt grad regneark i sitt arbeid, blant annet i aktuarmiljøer. Regnearkene danner grunnlag for forretningsmessig og regnskapsmessig rapportering og beslutning, og er derfor av vesentlig betydning.

Manglende systemløsninger og liten tilgang på IT-ressurser er i mange tilfeller bakgrunnen for utvikling og bruk av regneark, som har en lav brukerterskel. Utfordringen i den sammenheng er at mens systemutviklingsarbeidet som gjøres i en IT-organisasjon er basert på gjennomarbeidete prosesser og rutiner basert på anerkjente standarder og metoder, er normalt ikke regneark som utvikles lokalt i en fagenhet, basert på tilsvarende gjennomarbeidede prosesser. Brukerautorisasjoner og tilgangsstyring er ofte heller ikke tilstrekkelig ivaretatt. Bruk av regneark kan derfor representere risiko for blant annet feil, utilsiktede endringer og brudd på konfidensialitet. Foretak som bruker regneark av betydning for virksomheten, bør etablere felles prosesser og rutiner for utvikling og bruk av regneark, som blant annet ivaretar arbeidsdeling, kvalitetssikring, testing, endringshåndtering og tilgangsstyring.

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

Finanstilsynet har i tidligere ROS-analyser påpekt at få hendelser rapporteres fra forsikringsforetakene. Manglende rapportering av alvorlige IT-hendelser hindrer Finanstilsynet i å få nødvendig kjennskap til risikoen i selskapene. Der Finanstilsynet blir kjent med hendelser som burde vært rapportert, tas dette opp med foretaket.

3.4.4 Nytt personverndirektiv

Forsikringsforetakene står overfor omfattende systemutvikling i forbindelse med implementering av nytt personverndirektiv, jf. punkt 5.1.2.

3.5 Eiendomsmeglerforetak – oppgjør

Det ble i 2016 gjennomført tematilsyn om sikkerhet i oppgjørsfunksjonen i eiendomsmegler-foretak. Tematilsynet omfattet oppgjørsforetak med ulike systemløsninger som ivaretar oppgjøret ved om lag en fjerdedel av eiendomshandlene i Norge. Risikoen for feil eller tilsiktet manipulasjon er størst under klargjøringen av bilagene, før generering av bankfilene eller direkte på de ferdige utbetalingsfilene. Et viktig tiltak for foretakene er å etablere løsninger som sikrer at filene som genereres fra oppgjørssystemet, kontrolleres mot filene med betalings-data i nettbanken.

3.6 Tilsyn med etterlevelse av hvitvaskingsregelverket

Finanstilsynet gjennomførte i 2016 tilsyn hvor systemstøtte til anti-hvitvasking og anti-terrorfinansiering inngikk. Foretakene hadde utfordringer knyttet til å sikre oppdatert kontroll av kundene når sanksjonslistene endres. For finansforetak er det krav om elektroniske

overvåkingssystemer for å avdekke mistenkelige transaksjoner. En del av de elektroniske overvåkningsscenariene er lite treffsikre og gir så mange falske positive treff at det krever store kontrollressurser i bankene for skille falske treff fra ekte. Finanstilsynet har påpekt viktigheten av at scenariene evalueres kontinuerlig og at dette skjer i nært samarbeid mellom forretningssiden og IT-siden.

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. Finansnæringens nye infrastrukturselskap, Bits, har som oppgave å sikre og styrke effektiv betalingsformidling og betalingsinfrastruktur i Norge, og også på andre områder bidra til utvikling av infrastruktur.

I tråd med den teknologiske utviklingen og utnyttelse av de muligheter ny teknologi gir, er det behov for åpent samarbeid om etablering av effektiv og velfungerende infrastruktur. Dette medfører ofte omfattende endringer både i infrastruktur, hos det enkelte foretak og i teknologisk samhandling, både innenfor næringen og med andre aktører. Endringer er den hyppigste årsaken til uønskede hendelser. Hendelser i infrastrukturløsninger rammer ofte bredt, og det er derfor viktig med grundige vurderinger, både når det gjelder operasjonell risiko knyttet til drift og vedlikehold av tjenestene og sikkerhetsmessig risiko knyttet til blant annet uautorisert bruk av tjenestene.

Overgangen til et modernisert Baltus[21], fleksibel og sikker infrastruktur for ruting og transport av transaksjonsrelaterte finansielle forespørsler mellom bankene, ble fullført i 2016.

En arbeidsgruppe med representanter fra finansnæringen og Norges Bank ble etablert i 2016 for å skape en felles infrastruktur for betalinger med raskere oppgjør, inklusive tilpasninger i Norges Banks oppgjørssystem. Slik infrastruktur skal legge til rette for kontinuerlig gjennomføring av realtidsbetalinger. Betalinger mellom ulike bankers kunder kan da gjennomføres tilnærmet umiddelbart med kontrollert oppgjørsrisiko mellom banker. Arbeidsgruppens rapport ventes å foreligge i april 2017.

I samsvar med finansavtaleloven § 9 (3), har Bits gjennom 2016 fulgt opp bankenes og foretakenes overgang til ISO 20022-formater for filbaserte euro-betalinger, ref. punkt 3.2.7. I tillegg arbeides det med å etablere en felles formatstandard, basert på ISO 20022, for alle filbaserte betalingsinstruksjoner fra foretak til bank. Bankene har i dette arbeidet lagt til grunn at filbaserte betalingsinstruksjoner i andre valutaer enn euro også skal formidles ved bruk av ISO 20022-formater.

BankAxept har i 2016 modernisert sine tjenester, blant annet kontaktløs kortbetaling, og vil fortsette dette arbeidet i 2017, se ytterligere omtale i punkt 3.1.5.

[21] Bankenes on-line transaksjonsutvekslingssystem. Nettverk som bankene bruker for transaksjonsutveksling og dekningskontroll mot kontoer i hverandres kontosystemer.

PSD 2 krever at bankene må åpne for nye aktører i betalingsformidlingen. En arbeidsgruppe, ledet av Bits, skal vurdere hvordan bankene skal etablere tilgangen til betalingskontoer for aktører, både eksisterende og nye, som ønsker å tilby de nye betalingstjenestene; betalingsinitiering og kontoinformasjon. Også BankID ser nærmere på hvordan autentiseringsløsninger må tilpasses PSD 2s bestemmelser om bruk av sterk autentisering.

I kampen om det mobile betalingsmarkedet har det blitt etablert flere nye og teknologiske forskjellige terminalløsninger for betaling i fysiske butikker, i tillegg til de allerede eksisterende kortterminalene. Det resulterte i etableringen av Retail Payment, der målet er etablering av én felles infrastruktur med én terminalløsning[22]. Banknæringen har i regi av Bits igangsatt et prosjekt med formål å legge til rette for én teknisk installasjon per brukersted, som aksepterer de ulike betalingsløsningene som tilbys i markedet.

Finansnæringen og offentlig sektor vil gjennom digital samhandling utnytte mulighetene teknologien gir for effektivisering av en rekke prosesser på tvers av sektorene. Så langt er tre prosjekter etablert:

- **Samtykkebasert lånesøknad**
  Omfatter innhenting av informasjon fra offentlig sektor slik at kredittscore for lånsøkere kan utføres digitalt og direkte mellom dataeier og bank.
- **Kontrollinformasjon**
  Skatteetaten skal kunne spørre bankene, som ledd i en etterforskning, om utlevering av relevant kontrollinformasjon.
- **Konkursbehandling**
  Ved konkursåpning skal det umiddelbart gå en melding (digitalt) til bankene som fører til sperring av bankkontoer.

Finansnæringen ved Bits har utarbeidet krav til forbedret identitetskontroll og verifikasjon av identitet for BankID-kunder. Posten Norge vil første halvår 2017 lansere en ny PUM-tjeneste (Personlig Utlevering med Mottaksbevis), som gir bankene mulighet til å oppfylle de nye kontrollkravene. Det forventes at bankene etterlever disse kravene når de blir gjort gjeldende.

Banker i de andre nordiske landene har sett behov for å etablere et FinansCERT, tilsvarende det Norge har. Med det som utgangspunkt, ble etablering av et felles nordisk FinansCERT diskutert. Prosessen har resultert i at et nordisk FinansCERT (Nordic Financial CERT) er etablert, basert på den norske FinansCERT.[23]

[22] http://shifter.no/index.php/2016/10/25/norske-retail-payment-inngar-partnerskap-globale-teknologigiganter/
[23] https://www.finansnorge.no/aktuelt/nyheter/2017/04/nordisk-finansnaring-etablerer-digitalt-forsvarssenter-i-oslo/

3.8 Endringer i utkontraktering

Finanstilsynet har siden 1. juli 2014 mottatt meldinger om utkontrakteringer med bakgrunn i finanstilsynsloven § 4 c. Dette har gitt tilsynet en god oversikt over markedet for utkontraktering. Finanstilsynet følger opp at foretakene som utkontrakterer fortsatt har styring og kontroll. I tillegg følges det opp at avtaler og beredskapsplaner er i henhold til gjeldende regelverk.

3.8.1 Mottatte meldinger

Ut fra meldingene som ble mottatt i 2016, er det en trend at flere tjenester innen finansnæringen utføres utenfor Norges grenser. Store tjenesteleverandører som finansnæringen benytter, konsoliderer sine tjenester til færre senter. I stor grad gjelder dette oppgaver som drift og overvåkningstjenester.

Det er i hovedsak banker og forsikringsforetak som har sendt inn meldinger om utkontraktering. Meldingene kan inndeles i tre kategorier:

- Endringer som gjennomføres i selskaper som drifter deler av den teknologiske infrastrukturen, som EVRY og Nets.
- Nye avtaler eller større endringer av eksisterende avtaler som banker og forsikringsforetak har med sine leverandører av kjernesystem.
- Meldinger om utkontraktering av IKT-tjenester til tjenesteleverandører som tradisjonelt sett ikke har hatt utvikling eller driftstjenester til finansnæringen i sin tjenesteportefølje. Dette er tjenesteleverandører som f.eks. Microsoft, Google, Amazon, Salesforce og Facebook. Den største utfordringen Finanstilsynet fant ved mottak av disse meldingene, var at avtalene var mangelfulle i forhold til gjeldende regelverk. Etter påtrykk fra regulerende myndigheter og finansnæringen har tjenesteleverandørene tilpasset kontraktene som tilbys finansnæringen. Finanstilsynet vurderer i hvert enkelt tilfelle om kontrakten oppfyller bestemmelsene.

3.8.2 Meldeplikten som viktig verktøy

Markedet for utkontraktering utvikler seg i retning av mer globaliserte modeller og foretakenes adgang til utkontraktering utvides i nytt regelverk. Meldeplikt er nødvendig for at tilsynsmyndighetene skal kunne ha tilstrekkelig oversikt over den finansielle infrastrukturen.

Meldeplikten i henhold til finanstilsynsloven § 4 c gjelder også når leverandøren utkontrakterer til en underleverandør. Finanstilsynet følger opp at foretakene gjennom avtalen med leverandøren sikrer seg at de blir orientert når leverandøren planlegger å endre eller inngå avtaler om bruk av underleverandører.

Det kan være utfordrende for foretakene å ha tilstrekkelig kunnskap om nye leveransemodeller, f.eks. skytjenester. Foretakene skal ha tilstrekkelig IKT-faglig kompetanse til å bestille og kontrollere at IKT-tjenestene leveres i henhold til bestillingene. Dette gjelder også der det er flere lag med underleverandører. Vurderer Finanstilsynet at gjenværende kompetanse og ressurser hos foretaket ikke er tilstrekkelig, kan det være nødvendig å be foretaket iverksette og dokumentere tiltak.

Ved utkontraktering av IKT-tjenester ut av Norge vil Finanstilsynet påse at landrisikoen inngår i foretakets beslutningsunderlag, der internasjonale rankinglister og analyser bør hensyntas. Landrisikoen kan variere innen land, og området det utkontrakteres til må vurderes ved siden av landet som helhet. Dersom Finanstilsynet vurder at restrisiko etter eventuelle avhjelpende tiltak ikke er tilfredsstillende, kan foretaket bli pålagt å iverksette ytterligere tiltak i tråd med utkontrakteringens betydning for det finansielle systemet.

3.8.3 Revisjon av rundskriv om utflytting av IKT-oppgaver

Finanstilsynet ledet i 2016 en arbeidsgruppe som så på utkontraktering av oppgaver fra aktører innenfor betalingsformidling og annen finansiell infrastruktur, Finansdepartementet og Norges Bank deltok i arbeidet. Arbeidsgruppen la særlig vekt på utkontraktering til utlandet. Arbeidsgruppen la frem anbefalinger om hvordan gjeldende regelverk skal praktiseres samt hvilke forhold foretak bør vurdere ved en utkontraktering. I tillegg har gruppen gitt anbefalinger om risikoreduserende tiltak, herunder om noen oppgaver er av en slik betydning at de bør driftes fra Norge.

Finanstilsynet vil på bakgrunn av arbeidsgruppens anbefalinger revidere rundskriv 14/2010 Utflytting av bankenes IKT-oppgaver. Blant annet vil følgende punkter bli tatt inn i det reviderte rundskrivet:

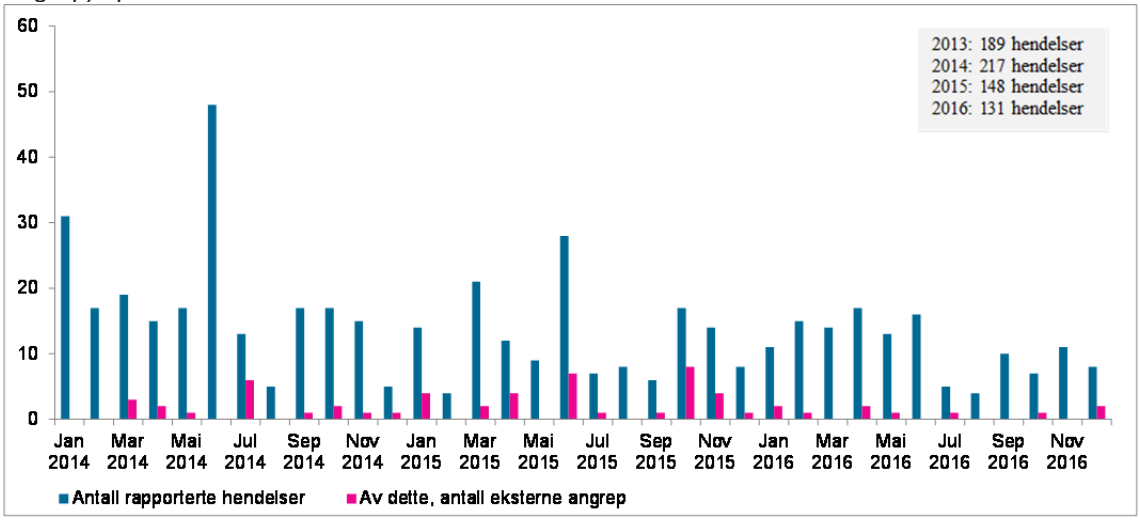
- Tydeliggjøre at plikten til å gi melding til Finanstilsynet ved utkontraktering også gjelder ved utkontraktering fra leverandøren til underleverandører.
- Angi hvilken informasjon melding om utkontraktering skal inneholde.
- Tydeliggjøre at landrisiko kan variere innenfor et land, og at området det utkontrakteres til må vurderes, i tillegg til landet som sådan.
- Henvisning til oppdaterte internasjonale rankinglister og analyser.

Samtidig vil det tas hensyn til EBAs kommende retningslinjer om utkontraktering og skytjenester, jf. punkt 5.1.5.

3.9 Rapporterte hendelser i 2016

Finansforetakene rapporterer til Finanstilsynet i henhold til krav i IKT-forskriftens § 9 Avviks- og endringshåndtering om alvorlige og kritiske IKT-relaterte hendelser. Rapporteringen omfatter både utilsiktede (operasjonelle) og tilsiktede (ondsinnede) hendelser. Finanstilsynet mottar flest rapporter om operasjonelle hendelser. En grunn til dette, er at hendelser som berører enkeltkunder som regel ikke faller inn under rapporteringsplikten. Et samlet bilde av nivået på tilsiktede hendelser kommer bedre fram gjennom statusrapporteringer fra FinansCERT og gjennom tapsstatistikken, se punkt 3.1.9.

Figur 3: Totalt antall rapporterte hendelser og antall rapporterte eksterne angrep (ondsinnede angrep) i perioden 2014–2016



Kilde: Finanstilsynet

3.9.1 Statistikk over hendelser

Basert på hendelsesrapporteringen til Finanstilsynet, var driftsstabiliteten totalt sett bedre i 2016 enn i 2015. Av 131 rapporterte hendelser var det ti rapporter om eksterne angrep (tilsiktede, ondsinnede hendelser). Dette var lavere både i faktisk antall og i prosent enn i 2015.

Parallelt med flere betalingstjenester på mobil, ikke minst BankID, har teleleverandørene fått større betydning for tilgjengeligheten til betalingstjenestene.

Det ble i 2016 også rapportert alvorlige hendelser som medførte lange tjenesteavbrudd for mobilbetalingstjenester.

Finanstilsynet mottok i 2016 flere rapporter om feil og driftsproblemer knyttet til bankenes elektroniske overvåkningssystemer mot hvitvasking og terrorfinansiering. Finanstilsynet vurderer hendelser som medfører tap av AML-kontroller som alvorlige og rapporteringspliktige.

Ved tre anledninger meldte banker om forsinkelser i levering av SWIFT-transaksjoner. Dette var operasjonelle hendelser. Hendelsene var uten tilknytning til angrepene (sikkerhetshendelser) som enkelte globale deltagere i SWIFT-nettverket ble rammet av.

Finanstilsynet har merket seg at en gjenganger blant årsakene til hendelser er svikt i kapasitetsovervåking og/eller -planlegging. Overskridelse av fyllingsgrader eller terskelverdier i tekniske komponenter som databaseservere, meldingskøer osv. medfører alvorlige avbrudd i tjenestene.

Finanstilsynet får hvert år rapportert hendelser fra foretakene om ufrivillig eksponering av kundedata eller andre konfidensielle data på grunn av feil i applikasjoner eller i driftsoperasjoner. Slik eksponering øker sårbarheten og kan utnyttes i ondsinnet hensikt.

For verdipapirselskapene var de fleste innmeldte hendelsene knyttet til manglende lydopptak av telefonsamtaler.

Inkassoforetak ble underlagt krav om hendelsesrapportering i desember 2015. Finanstilsynet mottok tre rapporter fra inkassoforetak i 2016, alle om driftsproblemer som medførte feil i brevutsendelser til skyldnere.

Finanstilsynet mottok to rapporter fra forsikringsforetak i 2016; en om utilgjengelig nettsted og en om feil i brevutsendelse til kundene.

Finanstilsynet mottok rapporter om DDoS-angrep, krypteringsvirus og phishing fra både banker og verdipapirforetak, men noen færre enn året før.

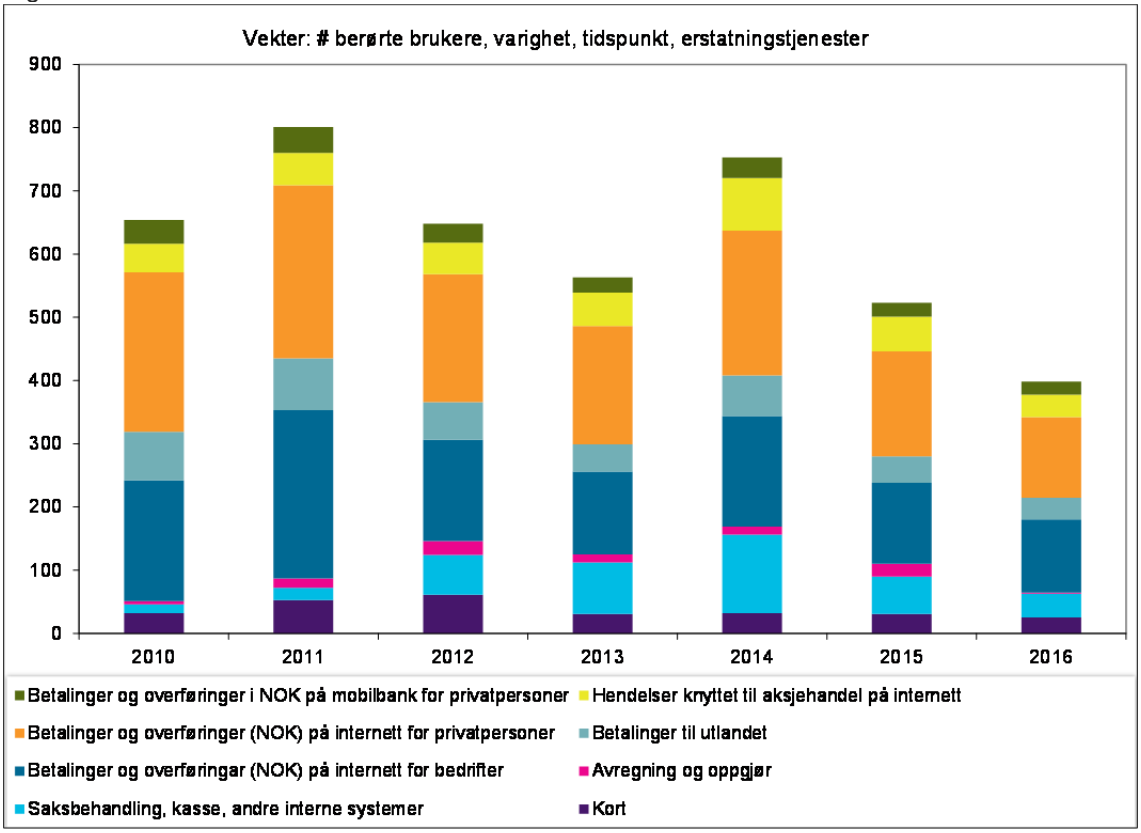
3.9.2 Analyse av hendelsene som mål på tilgjengelighet

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 alternative tjenester som kunder kan benytte. Dataene vektes og sammenstilles i tidsserier, slik at utviklingen kan følges over tid.

Figur 4 viser at betalingssystemet og kunderettede løsninger var mer tilgjengelige for kundene i 2016 enn i 2015, til tross for at flere foretak skiftet driftssted og leverandør i 2016, noe som innebærer en viss risiko for nedetid i overgangen.

Bankene er spredt på flere driftsleverandører enn for noen år tilbake og de fleste hendelser får derfor konsekvenser for en mindre kundemasse enn tidligere, da driften var konsentrert hos færre leverandører. Alt annet likt, reduserer dette risikoen for at mange foretak er utilgjengelige samtidig.

Figur 4: Hendelser veiet med konsekvens



Kilde: Finanstilsynet

3.10 Observasjoner av digital kriminalitet

Digital kriminalitet mot finansforetakene kan være angrep både på tilgjengelighet, konfidensialitet gjennom uautorisert uthenting av informasjon, og integritet gjennom uautoriserte betalingstransaksjoner. Digitale angrep kan ramme flere dimensjoner, og det kan være vanskelig å fastslå hva hensikten med angrepet er.

3.10.1 Phishing og sosial manipulering

De ansatte utgjør ofte det svakeste ledd i cyberforsvaret. Phishing og sosial manipulering er de mest brukte metodene for å utsette foretak for skadevare. Foretakene må forebygge uønskede hendelser gjennom intern opplæring og bevisstgjøring. Finanstilsynet har merket seg at noen banker har slike program for de ansatte.

3.10.2 DDoS-angrep og krypteringsvirus

Nivået på DDoS-angrep var det samme i 2016 som det har vært de siste årene. DDoS-angrep medfører sjelden lange avbrudd i tilgjengeligheten, sammenlignet med tidligere år, som følge av at foretakenes forsvar mot DDoS-angrep er forsterket. Spredning av krypteringsvirus gjennom ulike phishing-framstøt fortsatte i 2016 og det lyktes å infisere ulike typer finansforetak. Foretakene fikk filsystemer

kryptert og ble påført betydelig mer-arbeid med å hente fram backup av data og reetablere systemene. Både DDoS-angrep og angrep med krypteringsvirus ble i noen tilfeller i 2016 fulgt av krav om løsepenger (ransomware) for at angrepet skulle opphøre eller filsystemene dekrypteres. Finanstilsynet kjenner ikke til at finansforetak har betalt ut løsepenger.

3.10.3 Angrep i det internasjonale SWIFT-nettverket

Digitale angrep rettet mot SWIFT fikk mye oppmerksomhet i 2016. Selve SWIFT-nettverket ble ikke angrepet, og det er ikke avdekket sårbarheter i dette, men angrepene var kanalisert gjennom banker og rettet mot gjennomføringen av betalingstransaksjoner for overførsel gjennom SWIFT-nettverket. Land i Mellom-Europa og flere land utenfor Europa opplevde dette, bl.a. Bangladesh. Angrepene var en kombinasjon av sosial manipulering og teknisk svindel. Gjennom ulike former for manipulering, tilegnet angriperne seg informasjon om brukerne og brukergrensesnittet samt brukertilganger til foretakenes applikasjoner. Tilgangen kunne brukes til svindel ved å opprette betalingstransaksjoner for overførsel gjennom SWIFT-nettverket. Svindlerne la også inn kode som delvis slettet sporene etter angrepet. For norske brukere av SWIFT-nettverket og applikasjoner som skaper transaksjoner for overførsel gjennom SWIFT-nettverket, er sikkerhetstiltakene i tilgangsstyringen på et høyere nivå enn de landene som har opplevd slike angrep. I etterkant av hendelsen, har SWIFT iverksatt et omfattende sikkerhetsprogram med nye obligatoriske sikkerhetskrav. Disse omfatter bl.a. kjenn-din-kunde-aktiviteter og kontroller mot sanksjonerte kunder og land. Sikkerhetskravene vil gjelde for alle brukere av SWIFT-nettverket.

3.10.4 "Vannhull"-angrep

I 2016 ble det, antagelig gjennom former for phishing, spredd en type såkalt "vannhull"- skadevare til ulike typer finansforetak i ulike deler av verden. Skadevaren inneholdt lister over nettadresser til andre, ofte mer sentrale, finansforetak. Ansatte i finansforetak på de aktuelle listene fikk sin PC infisert når de besøkte det infiserte nettstedet. Også i Norge er det avdekket at finansforetak i 2016 var "vannhull" for denne typen målrettet distribusjon av ondsinnet kode. I den grad spredning av koden skjedde, lyktes det ikke viruset å komme på innsiden av finansforetakets systemer. Foretakenes overvåkning og anti-virus-programvare hindret dette. Det er uklart hvorvidt hensikten med angrepet har vært ren informasjonsinnhenting eller informasjonsinnhenting som grunnlag for å gjøre uautoriserte transaksjoner.

3.10.5 Andre observerte sårbarheter

Finanstilsynet observerer at det er sårbarheter i servere og tjenester som er tilgjengelige på Internett, herunder eldre versjoner av programvare som inneholder en rekke sikkerhetshull. Angripere kan forsøke å utnytte sårbarhetene for å ødelegge eller skade tjenesten, eller for andre kriminelle formål.

Finanstilsynet observerer også uheldig konfigurering av programvare, som gjør at kontrollmekanismene mot innbrudd ikke registrerer alle kommunikasjonsforbindelser, og dermed ikke kontrollerer dem.

Observerte forhold tas opp med aktuelle foretak, som blir bedt om å rette opp svakhetene.

3.11 Utviklingstrekk innenfor finansiell teknologi

Bruk av teknologi har medført at norsk finansnæring er blant den mest moderne, effektive og framtidsrettede i verden. Når ny teknologi har blitt tilgjengelig, har finansnæringen tidlig tatt teknologien i bruk og laget tjenester som sørger for økt effektivitet og bedret brukervennlighet.

FinTech er et nytt begrep som er tatt i bruk de siste årene. Finanstilsynets vurdering av begrepet, en samlebetegnelse som beskriver ulike måter å endre/påvirke tradisjonelle finansielle tjenester gjennom bruk av teknologi – derav begrepet FinTech, er at norsk finansnæring og finansielle tjenester over lang tid har absorbert teknologiske endringer. Finanstilsynet ser derfor ikke på FinTech som noe nytt og ukjent. Eksempelvis kan nevnes flere av de store initiativene innen betalingstjenester som opp gjennom årene er gjennomført i fellesskap av bankene.

Finanstilsynet ser at den teknologiske utviklingen sammen med endring av regelverk, særlig med innføring av PSD 2, vil kunne skape utfordringer. Et eksempel på dette kan være hvordan en skal sikre like konkurransevilkår for alle aktører for samme type betalingstjeneste.

3.11.1 Regulatorisk sandkasse

"Sandbox", eller på norsk "sandkasse", er et begrep som ofte dukker opp i forbindelse med FinTech. Blant annet tilbyr tilsynsmyndighetene FCA i Storbritannia og MAS i Singapore sandkasser for selskap med idéer for nye tjenester innen finansnæringen. Tilsynsmyndighetene har tatt på seg å hjelpe nye tjenesteleverandører inn i finansnæringen ved å lempe på noen regulatoriske krav i en tidsbegrenset periode. Eksempel på krav som lempes på kan være sammensetning av styre, kredittvurderingen av foretaket, kompetanse i foretakets ledelse og kapitalkrav. Regulatoriske krav som konfidensialitet for kundeinformasjon, behandling av midler som tilhører kunder eller krav til hvitvaskingsrutiner er krav det ikke lempes på. Etter prøveperioden, stilles det krav til oppfyllelse av alle relevante konsesjonsvilkår.

Finanstilsynet har dialog med IT-tilsynskollegaer i både FCA og MAS, med tanke på å følge utviklingen og trekke på deres erfaringer.

Selv om det ikke er etablert noen regulatorisk sandkasse i Norge, bistår Finanstilsynet FinTech-virksomheter med betydelig veiledning både når det gjelder regelverk og de planlagte tjenesteløsningene. Finansdepartementet har bedt Finanstilsynet vurdere hvordan et lavterskel-kontaktpunkt for veiledning av innovativ virksomhet kan etableres på en hensiktsmessig måte.[24]

3.11.2 "Distrubuted Ledger Technology" (DLT)

DLT[25] er en av teknologiene som er forventet å bidra mest til videre digitalisering og effektivisering av prosesser i finanssektoren. DLT er en distribuert database som deles på tvers av noder i et nettverk.

[24] https://www.regjeringen.no/no/dokumenter/etablering-av-kontaktpunkt-i-finanstilsynet-for-veiledning-av-fintech-virksomheter/id2548606/
[25] https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf

Teknologien får mye oppmerksomhet i forbindelse med at reguleringer og infrastruktur standardiseres og handelshindre fjernes i Europa.

Som følge av de nevnte endringene, ser aktører muligheter for utvikling av løsninger som er basert på strukturelle endringer fremfor å lage løsninger som forholder seg til bestående infrastruktur (disruptiv).

Som for annen teknologi, vil DLT også gjennomgå en utvikling og standardisering. Det kan forventes at teknologien vil tas i bruk på flere områder. Det vil etter hvert være applikasjonsområdene og deres behov som påvirker hastighet og retning for utviklingen, mer enn dagens situasjon, der nye bruksområder vurderes ut fra tilgjengelig teknologi. Et generelt kjennetegn for slik teknologisk endring er at det gjerne tar lengre tid enn forventet før den tas i bruk, men at konsekvensene av endringene ofte blir større enn forutsett.

DLT fungerer som et selvkontrollerende regnskapssystem og egner seg til å løse oppgaver som kan baseres på kontohold, eierskapsregistrering, transaksjoner og historikk. Selv om dagens løsninger ikke er mange og synlige, har DLT-løsninger fått oppmerksomhet som fundament for utvikling av nye løsninger, f.eks. valutaoverføring mellom banker. Flere internasjonale storbanker deltar i slik utvikling og noen systemer er også i pilotdrift.

Flere sentralbanker har etablert prosjekter for å undersøke muligheten for å utstede nasjonal digital valuta, blant annet utreder Norges Bank mulighet for å innføre elektroniske sentralbankpenger. Løsninger basert på DLT-teknologi kan være aktuelle.

Av prosjekter i Norge kan nevnes Verdipapirsentralens samarbeidsprosjekt med Deutsche Börse med formål å utvikle et grensekryssende system for sikkerhetsstillelser samt etablerte FOU-prosjekter for bruk av DLT i flere banker og IT-selskaper. Norske bankers samarbeidsorgan Bits har etablert et forum for utveksling av erfaringer om bruk av DLT-teknologi.

Selv om det foreløpig er få etablerte løsninger basert på DLT-teknologi, gjennomføres det betydelig forskning og utprøving på området. Forventningene til fremtidige bruksområder er store.

4 Aktørenes vurdering av risiko

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.

4.1 Intervjuer

4.1.1 BankID – særlig på mobil – forårsaket problemer

BankID er en sentral del av bankenes autentisering- og signeringsmekanisme og det er derfor viktig at denne funksjonen er operativ og tilgjengelig for forbrukerne. I intervjuene var det flere av foretakene som tilkjennega at løsningen med BankID på mobil i 2016 hadde hatt utfordringer når det gjelder tilgjengelighet. Flere av hendelsene var forårsaket av feil hos teleleverandører. Det er mange tjenesteleverandører som bidrar til den tekniske infrastrukturen i finansmarkedet. For å bidra til økt kvalitet i tjenesteleveransene, er det viktig at alle tjenesteleveranser kontrolleres og følges opp.

4.1.2 Manglende sikkerhetstenking ved design av løsninger

Et tema som ofte ble nevnt i intervjuene, var utfordringer knyttet til å integrere sikkerhetstenking i designfasen. Dette gjelder særlig nye utviklingsprosjekter, men også til en viss grad for endringer i eksisterende løsninger. Erfaringen var at dersom sikkerhetsarkitektur ikke var med i designfasen av nye utviklingsprosjekter, var det ofte både dyrt og vanskelig å legge sikkerhetsløsninger inn i en ferdig programmert løsning. Sikkerhetsløsninger som ble lagt til i ettertid medførte også dårligere sikring enn om sikkerhet var en integrert del av løsningen.

4.1.3 Ressurser – mangel på kvalifiserte ressurser for både stormaskin, tradisjonell programmering og sikkerhetskompetanse

Som nevnt i tidligere års ROS-analyser, er flere av løsningene som benyttes innenfor bank- og finansnæringen i Norge blitt utviklet med en annen IT-arkitektur (f.eks. operativsystem), og andre programmeringsspråk enn de som brukes til utvikling i dag. Foretakene er samstemte i at det er vanskelig å få tak i kompetanse som kan forvalte og drifte den eldre delen av applikasjonsporteføljen, siden nyutdannede innen IKT i svært liten grad søker seg til eldre teknologier. Det er en trend at stadig flere utkontrakterer disse tjenestene til land der tilgangen på denne type ressurser er bedre enn i Norge. Dette kan medføre risiko ved at foretaksintern kunnskap blir svekket. Imidlertid er foretakene avhengige av de gamle løsningene i flere år framover. Ved å utkontraktere utvikling, forvaltning og drift til foretak som har denne kompetansen tilgjengelig, reduseres risikoen noe, men det stiller samtidig store krav til avtaler og styring og kontroll av de utkontrakterte løsningene.

4.1.4 Kunnskap om bruk, arkitektur og oppfølging av skyløsninger

Finansnæringen ønsker i økende grad å benytte seg av tjenester som leveres som skyløsninger (utkontraktering). Tjenestene som ønskes benyttet er ofte løsninger som tilbys av store tjenesteleverandører som f.eks. Amazon, Google eller Microsoft. Flere av foretakene erkjenner manglende kunnskap om teknisk infrastruktur, driftsopplegg og hvordan styring og kontroll utføres av tjenesteleverandørene. Siden foretak under tilsyn har det hele og fulle ansvaret for egen infrastruktur, er det for foretaket en utfordring å ha tilstrekkelig kompetanse om de utkontrakterte tjenestene for å kunne utøve styring og kontroll på en god måte, jf. punkt 3.8.

4.1.5 Sikkerhet og tilgangsstyring – beskyttelse av foretaksinformasjon

Foretaksinformasjon ("Corporate information") er sensitive data og det må derfor være strenge krav til tilgangsstyring og informasjonssikkerhetsløsninger for infrastruktur hvor denne type informasjon er lagret. Foretak som ble intervjuet påpekte at særlig der informasjon er lagret på løsninger som er utkontrakterte, er oppfølging av tilgangsstyring avgjørende for å kunne vedlikeholde og kontrollere f.eks. innside-lister. Av de som ble intervjuet, ble sensitiv foretaksinformasjon sett på som lett omsettelig og dermed av særlig interesse for kriminelle organisasjoner. Det er derfor viktig at alle som oppbevarer foretaksinformasjon, både eier og driftsoperatør, legger stor vekt på styring og kontroll for å sikre at kvaliteten på sikkerhetsløsningene er hensiktsmessige og fungerer etter hensikten.

4.1.6 Time to market

Aktørene legger vekt på å få nye eller forbedrede løsninger raskt i drift. Konkurransen om kundene er stor og det er ofte de som er raskt ute med nye løsninger som vinner markedsandeler. Dette kan medføre at løsningene som settes i produksjon ikke er tilstrekkelig testet før de settes i produksjon. Sammen med manglende integrering av sikkerhetsarkitektur i løsningene, kan dette medføre en stor risiko ved at løsningene ikke har det sikkerhetshetsnivået som løsningen bør ha. Dette gjelder både autentiseringsløsninger og hvordan informasjon behandles og deles.

4.1.7 Kriminelle organisasjoner benytter kunstig intelligens

Som et av mange bevis på at Internett-kriminalitet har flyttet ut av "gutterommet" og inn i organisert kriminalitet, er bruken av stadig mer avanserte og kostbare metoder. Kunstig intelligens (AI) er en av flere tjenester som kriminelle benytter for å innhente informasjon om hvordan kunder utfører sine transaksjoner eller hvordan forsvarsverk på Internett agerer på angrep. Ved at de kriminelle bruker kunstig intelligens, tilegner de seg store mengder med informasjon som kan benyttes i målrettede angrep. Innhentingen av informasjon begrenser seg ikke til utstyr som brukes i nettbank- eller mobilbankløsninger, men også til det stadig økende antall forbrukerartikler eller kjøretøy som via Internett kan sende eller motta informasjon. Foretakene som ble intervjuet så det som avgjørende at løsningene for Cybersikkerhet tar i bruk tilsvarende avanserte løsninger som kunstig intelligens representerer.

4.1.8 Phishing

Det har de siste årene blitt lettere å gjennomføre større phishing-angrep siden tekniske løsninger for å utføre slike angrep er til salgs på Internett. Løsningene kan ofte kjøpes for mellom USD 2 og 10, og

bruken av løsningene krever ikke særlig teknisk kompetanse. I stadig større grad har angrepene blitt mer sofistikerte og phishingen retter seg ofte mot enkeltavdelinger i foretak og de ansatte i disse avdelingene framfor mot hele foretaket, slik at innbruddsforsøket vekker mindre oppmerksomhet. Potensialet for at kriminelle kan lykkes med svindel basert på phishing er til stede. Foretakene gir uttrykk for at de legger stor vekt på opplæring og informasjon til sine ansatte om phishing og bruk av e-post for å redusere denne risikoen.

4.2 Spørreundersøkelse om sårbarhet

I desember 2016 gjennomførte Finanstilsynet en spørreundersøkelse blant 23 foretak. I spørre-undersøkelsen ba Finanstilsynet foretakene vurdere i hvilken grad foretaket anser seg for å være 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).

Foretakenes størrelse er ikke reflektert i tabellen nedenfor.

4.2.1 Støtte for strategiske beslutninger

Tabell 5: Støtte for strategiske beslutninger

	Sårbarhet	Foretakenes svar	Trend 2016	Trend 2015
1	Systemenes evne til å hente informasjon fra eksterne og interne kilder og sammenstille og synkronisere informasjonen til et bilde av foretakets risiko til bruk i styringsøyemed og til myndighetsrapportering		→	→
2	Systemenes evne til automatisk å gi 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		→	→
3	Systemenes evne til å reflektere kundens evne til å betjene gjeld		→	→
4	Datakvaliteten i våre systemer og registre		→	→
5	Integrasjon og synkronisering mellom systemene		→	↘
6	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		→	→
7	Grad av kompleksitet i IT-systemene		↗	→
8	Omfanget av mangler og feil i systemene		→	→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert.			

Kilde: Finanstilsynet

Tabellen viser risikoen for at IKT ikke alltid 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.

Kompleksitet i IT-systemene anses å være en økende risiko. Nye tjenester kombinert med til dels gammel arkitektur gir kompleksitet og risiko.

4.2.2 Avvik i driften

Tabell 6: Avvik i driften

	Sårbarhet	Foretakenes svar	Trend 2016	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 antivirus 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, sertifikatdatoer, 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 svartider) 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, jf. IKT-forskiften § 11		↘	→
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	Omfanget av endringer		↗	→
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. Hvit: Ikke vurdert.			

Kilde: Finanstilsynet

Betydelige aktører har testet kontinuitetsløsninger med positivt utfall – risikoen har gått fra stabil til minkende.

Leveransepress, endringer som følge av nye reguleringer og knapphet på kompetanse utgjør en økende trussel.

Mangelfull logging og overvåking har gått fra minkende trussel i 2015 til stabil trussel i 2016, og har dermed økt fra 2015. Den økende trusselen knyttet til "Internet of Things" kan være en medvirkende årsak til dette.

4.2.3 Data er ikke tilstrekkelig beskyttet

Tabell 7: Data er ikke tilstrekkelig beskyttet

	Sårbarhet	Foretakenes svar	Trend 2016	Trend 2015
1	Våre retningslinjer for klassifisering av strukturert (databaser) og ustrukturert (word, e-post) informasjon og beskyttelse av informasjonen		→	→
2	Tilgangskontroller – ansatte, konsulenter, leverandører, applikasjoner, software		→	→
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		→	→
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. Hvit: Ikke vurdert.			

Kilde: Finanstilsynet

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

I 2016 var det en økning i såkalt ransomware, noe som fremgår av foretakenes kommentarer.

Sårbarheten knyttet til logging og evne til å reagere på loggenes innhold er avtakende.

4.2.4 ID-tyveri

Tabell 8: ID-tyveri

	Sårbarhet	Foretakenes svar	Trend 2016	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. Hvit: Ikke vurdert.			

Kilde: Finanstilsynet

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

4.2.5 Misbruk av tilgang til datasystemene

Tabell 9: Misbruk av tilgang til datasystemene

	Sårbarhet	Foretakenes svar	Trend 2016	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. Hvit: Ikke vurdert.			

Kilde: Finanstilsynet

Trusselbildet er uendret fra foregående år.

4.2.6 Hvitvasking

Tabell 10: Hvitvasking

	Sårbarhet	Foretakenes svar	Trend 2016	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 og transaksjonsmønstre - presisjon i flagging av mistenkelige transaksjoner		→	→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert.			

Kilde: Finanstilsynet

Flere foretak mener fortsatt 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.

4.3 Nasjonale vurderinger av trusselbildet

NSM har sin publikasjon "Helhetlig IKT-risikobilde 2016" en beskrivelse av trusselsaktører for digital spionasje, der det pekes på at utenlandske statlige aktører representerer en høy risiko fordi de rår over ressurser for å bedrive metodisk aktivitet over lengre tid. PST sier i sin trusselvurdering for 2017: "Datanettverksoperasjoner vil være en integrert del av de ulike etterretningsoperasjonene mot mål i Norge. I tillegg vil etterretningstjenestene arbeide aktivt for å få tilgang til personer i virksomheter som behandler sensitiv informasjon og teknologi."

Militære E-tjenestens analyse (Fokus 2017) peker på at de mest alvorlige truslene finnes i det digitale rom, og at statsstøttede utenlandske aktører har norske økonomiske og tekniske verdier som mål for sin aktivitet.

Den sensitive informasjonen det siktes til i rapportene, er informasjon om norske foretaks strategi, teknologi og finansielle situasjon. Finanstilsynet vurderer derfor at tyngden av informasjon som rammes av disse truslene vil finnes på verdipapirområdet og i verdipapirforetakene spesielt, men at slik informasjon også finnes andre steder som hos bankenes corporate-funksjoner og i foretakenes økonomienheter. Finanstilsynet mener at tiltak på området derfor bør få økt oppmerksomhet i foretakenes risikovurderinger.

5 Endringer i reguleringer

Også i 2016 var det en rekke EU-prosesser knyttet til forslag til nye eller endring i eksisterende direktiver, forordninger, utfyllende bestemmelser 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 eller IKT-relaterte prosesser. 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 – nytt betalingstjenestedirektiv

Det nye betalingstjenestedirektivet (PSD 2)[26] trer i kraft i EU 13. januar 2018 og skal fremme innovasjon gjennom å skape økt konkurranse mellom eksisterende og nye aktører. EBA har, i samarbeid med ECB, med hjemmel i PSD 2 fått myndighet til å gi ti anbefalinger eller utfyllende bestemmelser, blant annet utfyllende bestemmelser om sterk kundeautentisering og sikker kommunikasjon, anbefalinger om hendelsesrapportering og anbefalinger om styring av operasjonell risiko og sikkerhetsrisiko. I tillegg vil ECB og EBA utforme anbefalinger om rapportering av svindelstatistikk.

Forslag til utfyllende bestemmelser for sterk kundeautentisering og sikker kommunikasjon[27] er oversendt fra EBA til EU-kommisjonen og vil tre i kraft 18 måneder etter fastsettelse. Forslaget spesifiserer kravene til bruk av sterk autentisering. Det angis også en rekke unntaksbestemmelser basert på blant annet forhold som risikoprofil for betalingen, kanal for betalingen, type betaling, betalingsmottaker og beløp. Det stilles omfattende krav til ivaretakelse av konfidensialitet og integritet av betalers personlige sikkerhetsinformasjon, både når det gjelder bruk og utlevering. Videre spesifiseres også krav til autentisering og kommunikasjon mellom eksisterende aktører/tilbydere av betalingskonto og nye/eksisterende aktører, som ønsker å tilby de nye betalingstjenestene betalingsinitiering og kontoinformasjon. Forslaget er av den grunn sentralt i nå målene med PSD 2.

26 https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2013/okt/revidert-betalingstjenestedirektiv---psd-2.-/id2434721/

27 https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2

Det stilles krav til at betalingskontotilbydere må stille til rådighet minst ett grensesnitt som tilbyr samme tilgjengelighet, ytelse, support og beredskapstiltak som de grensesnitt som er gjort tilgjengelig for betalingstjenestebrukers direkte tilgang til sine betalingskontoer. Det stilles også datautvekslingskrav, der blant annet informasjonen som betalingskontotilbyder skal gjøre tilgjengelig gjennom grensesnittene, skal være minst den samme som ved betalingstjenestebrukerens direkte tilgang.

EBA har hatt på høring anbefalinger om hendelsesrapportering. Anbefalingene omfatter både operasjonelle hendelser og sikkerhetshendelser og inneholder krav til klassifisering av hendelser og krav til varslingsprosessen overfor tilsynsmyndigheten. Anbefalingene åpner opp for både delegert og konsolidert rapportering og stiller krav til tilsynsmyndighetenes oppfølging av innrapporterte hendelser og samhandling med andre lands myndigheter der det er relevant. Anbefalingene omfatter også forslag til skjema som skal benyttes ved rapportering. Endelige anbefalinger vil bli fastsatt i 2017. I hovedtrekk er anbefalingene i tråd med eksisterende bestemmelser i IKT-forskriften, men endringer må påregnes når anbefalingene gjøres gjeldende i Norge.

Anbefalinger om styring av operasjonell- og sikkerhetsrisiko for betalingsforetak sendes på høring første halvår 2017. Anbefalingene omfatter krav til risikostyring og en rekke krav til blant annet identifisering av risikoområder, policyer og tiltak, overvåkning, testing av robusthet og håndtering av sikkerhetshendelser. Endelige anbefalinger forventes fastsatt i 2017.

PSD 2 stiller krav til rapportering av tapstall knyttet til bruk av betalingstjenester. I Norge har slike tapstall vært rapportert siden 2011. For å sikre konsistent rapportering på tvers av landene og forenklet konsolidering på EØS-nivå, er det nedsatt et arbeid i regi av EBA og ECB. Kategoriene for svindel med betalingskort, nettbank (credit transfer) og automatiske betalinger (direct debet) vil bli spesifisert. Sammen med svindeltallene, skal også det totale antallet transaksjoner i samme kategori rapporteres. Svindel med betalingstransaksjoner er oftest grensekryssende. Harmoniserte tapstall vil gi et bilde av hvordan svindelen utvikler seg og beveger seg mellom land. Finanstilsynet har ikke slik statistikk i dag. Oppstart av rapportering etter de nye reglene er planlagt i 2018, med publisering første gang i 2019. Det antas at regelverket vil medføre behov for endringer i eksisterende regelverk for tapsrapportering i Norge.

5.1.2 Ny personvernlov[28]

I mai 2018 trer EUs nye personvernforordning i kraft. Reglene gjelder for alle virksomheter som samler inn eller bruker personopplysninger om EU/EØS-borgere. Reglene innebærer blant annet at virksomheter skal ha en personvernerklæring, og vurdere risiko og personvernkonsekvenser. Mange foretak må etablere eget personvernombud. Forordningen vil kreve at personvern integreres i IKT-løsninger som omfatter persondata. Systemalternativet som minst mulig griper inn i personvernet skal være systemets standard (default). Eksempler på elementer som det vil kreves standardinnstillinger for, kan være:

28 https://www.datatilsynet.no/Regelverk/EUs-personvernforordning/

- mengden av informasjon som skal samles inn
- behandlingsomfang
- lagringstid for dataene
- hvem som skal ha tilgang på dataene

Foretak som ikke etterlever reglene risikerer betydelig økonomiske sanksjoner.

Det er Finanstilsynets vurdering at endringene innebærer at foretakene må gjøre til dels betydelige tilpasninger i sine IT-systemer. Finanstilsynet legger videre til grunn at foretakene arbeider aktivt med å få på plass rutiner og systemer.

5.1.3 Nettverkssikkerhet

Europaparlamentets og Rådets direktiv (EU) 2016/1148 av 6. juli 2016[29] (NIS-direktivet) definerer tiltak som skal sikre et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU.

Direktivet pålegger medlemsstatene å sørge for at operatører av viktige tjenester, herunder banker, finansmarkedsinfrastruktur og digital infrastruktur, iverksetter sikkerhetstiltak og rapporterer hendelser. For finansektoren er dette allerede regulert gjennom IKT-forskriften og medfører derfor ikke vesentlige endringer i foretakenes plikter.

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

EU-kommisjonen vedtok 12. juli 2016 det nye rammeverket om overføring av personopplysninger fra Europa til USA, det såkalte EU-US Privacy Shield. Vedtaket gjelder også for Norge gjennom EØS-avtalen.

EU-kommisjonen har vurdert at det nye avtaleverket, som erstatter Safe Harbour-rammeverket som ble kjent ugyldig i oktober 2015, sikrer et tilstrekkelig beskyttelsesnivå ved overføring av personopplysninger fra Europa til USA.

Overføring av personopplysninger kan nå skje til amerikanske selskaper som er sertifisert av Handelsdepartementet i USA i henhold til Privacy Shield-avtaleverket, og som dermed har forpliktet seg til å følge særlige regler for beskyttelse av personopplysninger.

5.1.5 Taskforce on IT Risk Supervision

Finanstilsynet har i 2016 deltatt i EBAs Task Force on IT risk supervision (TFIT) og er med i to arbeidsgrupper på dette området. Den ene arbeidsgruppen har utarbeidet utkast til retningslinjer for vurdering av IT-risko i tilknytning til SREP[30]-prosessen. Den andre arbeidsgruppen arbeider med en anbefaling for tilsynspraksis i forbindelse med bankenes bruk av skytjenester. Resultatet fra disse arbeidsgruppene er planlagt ferdigstilt i løpet av 1. halvår 2017.

[29] https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/sep/nis-direktivet/id2483374/
[30] Supervisory Review and Evaluation Process (SREP) er Finanstilsynet evaluering av bankenes egen risiko, kapitalbehov (ICAAP) og likviditetsbehov (ILAAP).

5.2 Endringer i norsk regelverk

5.2.1 MiFID II / MiFIR

Markets in Financial Instruments Directive (MiFID I) er gjennomført i verdipapirhandelloven og børsloven. MiFID I erstattes i EU av MiFID II og MiFIR (Markets in Financial Instruments Regulation), med virkning fra 3. januar 2018. MiFID I regulerer virksomheten til handelsplasser og verdipapirforetak, herunder hvilke krav som stilles til transparens i markedet. Formålet med revideringen av MiFID I er mer transparente og velfungerende markeder og økt investorbeskyttelse. MiFID II og MiFIR suppleres av utfyllende rettsakter i form av rundt 40 kommisjonsforordninger og ett kommisjonsdirektiv.

Verdipapirlovutvalgets forslag til gjennomføring av MiFID II og MiFIR i norsk rett er lagt frem i NOU 2017:1. Finansdepartementet har sendt forslaget på høring, med frist 15. mai 2017.

Flere av de nye kravene i MiFID II og MiFIR knytter seg til verdipapirforetakenes og handelsplassenes systemer for handel med finansielle instrumenter. Det stilles blant annet nye systemkrav til verdipapirforetak og handelsplasser som benytter algoritmer og krav til tidsregistrering og synkronisering av hendelser, eksempelvis handler og prisendringer, på handelsplassene. Når det gjelder transaksjonsrapportering (TRS-rapportering), skal det benyttes nye formater for rapporteringen og det kreves at Legal Entity Identifier (LEI) benyttes for identifisering av utstedere, handelsplasser og investorer, der disse er juridiske enheter. Det stilles videre krav om rapportering av posisjoner i varederivater for både handelsplassene, deres medlemmer og verdipapirforetak som handler med varederivater. Dette vil også innebære krav til foretakenes systemløsninger.

5.2.2 The European Market Infrastructure Regulation

EMIR innfører en plikt for partene i en derivattransaksjon til å rapportere en del standardiserte opplysninger om enhver inngått derivatkontrakt og endringer i denne, til et transaksjonsregister (Trade Repository – TR). Denne rapporteringsplikten vil påhvile alle foretak som er involvert slike transaksjoner, i motsetning til TRS-rapportering som er en plikt kun pålagt verdipapirforetakene. Rapporteringsplikten ifølge EMIR trådte i kraft i EU 12. februar 2014. EMIR er (per medio april 2017) ikke gjennomført i norsk rett, og norske foretak er derfor ikke forpliktet til å rapportere inngåtte derivattransaksjoner til transaksjonsregistre. Det er forventet at EMIR vil gjennomføres i Norge i løpet av annet kvartal 2017, og at norske foretak fra det tidspunktet får et rapporteringskrav. Det er imidlertid ikke fastsatt når selve rapporteringsplikten inntrer, da dette vil avhenge av gjennomføringen av utfyllende rettsakter til EMIR i norsk regelverk.

De utfyllende bestemmelsene som inneholder nærmere krav til rapportering (herunder rapporteringsskjemaet) vil i EU endres med virkning fra 1. november 2017. Det bør tas høyde for dette under utviklingen av rapporteringsskjemaet.

For å tilby tjenester i EØS-området må transaksjonsregistre være registrert hos ESMA. Oversikt over registrerte transaksjonsregistre foretakene kan velge å benytte for rapporteringen, finnes på ESMAs nettsted.

5.2.3 Tiltak mot hvitvasking

Lovutvalget som har utredet ny lov og forskrift om tiltak mot hvitvasking og terrorfinansiering overleverte i desember 2016 sin andre delutredning til Finansdepartementet. Lovforslaget ble sendt på høring med frist 1. april 2017. Utvalgets mandat var å lage utkast til lov og forskrift som gjennomfører EUs fjerde hvitvaskingsdirektiv, samt ta hensyn til anbefalingene fra FATF. Hvitvaskingsdirektivet er et fullharmoniseringsdirektiv som begrenser muligheten for nasjonale valg. Store deler av innholdet i gjeldende hvitvaskingsforskrift er foreslått tatt inn i loven. I sin første delutredning, som ble avgitt i november 2015, foreslo utvalget blant annet enkelte justeringer i lovens virkeområde. Delutredningen omfattet også en vurdering av om det bør innføres øvre beløpsgrenser for kontantkjøp.

I desember 2016 publiserte Finanstilsynet i rundskriv 24/2016 en veiledning til hvitvaskingsregler. Veiledningen vil tilpasses nye regler etter at disse er satt i kraft.

5.2.4 Forskrift om formidlingsgebyr i kortordninger

Forskrift om formidlingsgebyrer ved kortbaserte betalingstransaksjoner trådte i kraft 1. september 2016. Forskriften setter tak på formidlingsgebyrer for kortbaserte forbrukerbetalinger. Den regulerer blant annet brukerstedets rett til å påvirke en forbruker til å betale med de kortene brukerstedet foretrekker, men forbruker står fritt til selv å velge hvilket som ønskes benyttet. Det innebærer at brukerstedene må etablere tekniske løsninger som understøtter forbrukers rett til å velge kort for betalingen.

Forskriften stiller også krav til separasjon mellom eier av kortordning og selskap som forestår kortprosesseringen. Anbefalinger om utfyllende bestemmelser når det gjelder krav til separasjon er oversendt fra EBA til EU-kommisjonen.

5.2.5 Forslag til ny sikkerhetslov

Det ble i 2016 fremmet forslag til ny lov om forebyggende nasjonal sikkerhet. Loven vil gjelde for alle virksomheter som er av kritisk betydning for grunnleggende nasjonale funksjoner. I rapporten vises det til at bank- og pengevesen er en grunnleggende nasjonal funksjon.

Virkeområdet for sikkerhetsloven foreslås utvidet slik at enhver virksomhet som er av kritisk betydning for grunnleggende nasjonale funksjoner, omfattes av loven. Banker og infrastrukturforetak kan bli omfattet. Begrepet skjermingsverdige objekt og skjermingsverdig infrastruktur foreslås benyttet for objekter og infrastruktur utpekt av sektormyndigheten til å være av kritisk betydning for grunnleggende nasjonale funksjoner.

I lovforslaget foreslås det bestemmelser om generelle krav til forebyggende sikkerhet. På dette området er det allerede for finanssektoren etablert et sektorregelverk som i hovedtrekk dekker den nye sikkerhetslovens bestemmelser. Tilsvarende er det for utkontraktering etablert et omfattende sektorregeleverk som i hovedtrekk dekker mye av den nye sikkerhetslovens foreslåtte bestemmelser om sikkerhetsgraderte anskaffelser.

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.

6.1 Finansiell infrastruktur

Dersom det ikke er mulig å foreta betalinger, vil viktige samfunnsfunksjoner etter kort tid ikke lenger fungere tilfredsstillende.

Finanstilsynet har i 2016 registrert at den dominerende løsningen for innlogging til betalingstjenester (BankID og BankID på mobil, som begge er avhengige av FOI) har vært utilgjengelig ved flere anledninger. Flere store finansforetak har denne løsningen som eneste mulige innlogging til foretakets tjenester. Da må det stilles særskilt høye krav til kvalitet i innloggingsløsningen.

I senere år er det kommet nye og alternative måter å foreta overføringer og betalinger på. I 2016 kom flere løsninger for betalinger der kunden benytter mobiltelefonen for å godkjenne betalinger. Fra tidligere år nevnes e-faktura, avtalegiro og faste oppdrag, foruten betalinger i nettbanken. Tjenestene kan nås via nettbank eller mobilbank. De mange alternativene gjør betalingssystemet mindre sårbart; mobilbanken kan være tilgjengelig selv om nettbanken ikke virker og avtalegirobetalingen blir gjennomført selv om nettbanken ikke virker.

I 2016 ble flere foretak utsatt for en type angrep der angriper lyktes i å gjøre foretakets data uleselige for foretaket. Skulle angriperne lykkes i å få tilgang til store mengder kunde- og kontodata, og gjøre disse utilgjengelige, kan dette skape betydelige utfordringer for foretaket. Foretak som opererer på vegne av alle eller flere finansforetak er spesielt sårbare. Foretakene bør øve på å rekonstruere og tilbakeføre data.

Regler for behandling av innsideinformasjon skal bidra til velfungerende markeder for verdipapirhandel. Brudd på reglene vil kunne føre til svekket tillit til markedsplassene og at investorer trekker seg ut av markedet. Finanstilsynet har i 2016 observert betydelige svakheter når det gjelder styring og kontroll med tilganger til systemer som kan inneholde markedssensitiv informasjon.

Finanstilsynet får gjennom tilsynsvirksomheten og arbeidet i BFI, med blant annet gjennomgang av hendelser i foretakene og FMI-foretakene, et bredt og godt bilde av tilstanden i den norske finansielle infrastrukturen.

Stabiliteten i den finansielle infrastrukturen var i 2016 god og på linje med 2015. Det var ellers en god regularitet på avregnings- og oppgjørssystemene og kommunikasjonen mot det internasjonale betalingssystemet SWIFT og det internasjonale oppgjørssystemet CLS.

Selv om det var hendelser som gjorde betalingsløsninger utilgjengelige i kortere perioder, vurderer Finanstilsynet den norske finansielle infrastrukturen som solid og stabil.

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.

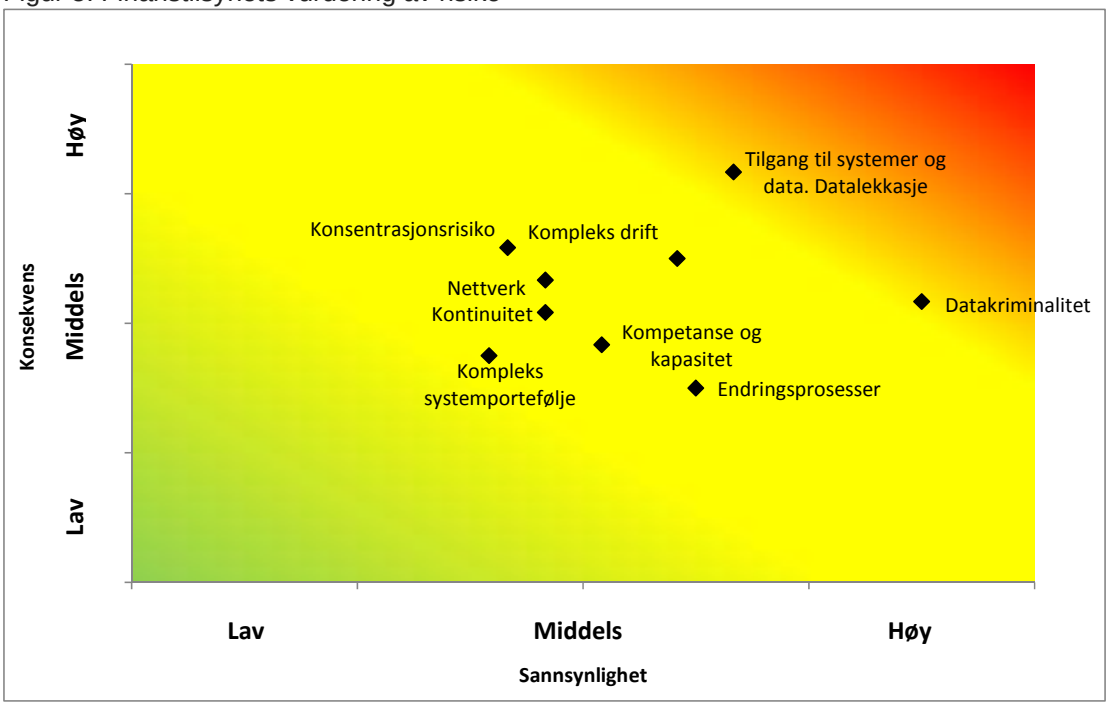
Finanstilsynet kan delta som observatør på tilsyns- og overvåkingsmøtene som Norges Bank har med FMI[31]-foretakene, og Norges Bank kan delta som observatør på Finanstilsynets tilsyn med banker og datasentraler av betydning for finansiell infrastruktur.

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).

[31] Financial Market Infrastructures

Figur 5: Finanstilsynets vurdering av risiko



Kilde: Finanstilsynet

Finanstilsynet vurderer tilganger til systemer og data, datalekkasje og datakriminalitet som de mest sentrale truslene mot og sårbarhetene i foretakenes systemer. Tilsyn i 2016 viser at det er betydelige mangler når det gjelder kontroll med tilgang til systemer og data, og Finanstilsynet vurderer at risikoen er høyere enn i 2015. Datakriminalitet øker i omfang og kompleksitet og gjør at risikoen er høyere enn i 2015.

Kompleks drift, konsentrasjonsrisiko og feil i nettverk utgjør også sentrale trusler og sårbarheter. Andre risikoområder er mangelfulle kontinuitetsløsninger, manglende kompetanse og kapasitet, komplekse systemporteføljer og feil som oppstår ved endringer i systemene.

Nettverk

Finansielle tjenester bygger på tjenester fra en rekke leverandører og er avhengig av kvaliteten og sikkerheten i nettverkene til leverandørene. Samspillet er meget komplisert, med høy risiko for feil og mangler i tjenesten. Et aktuelt eksempel er at den dominerende løsning for innlogging er avhengig av en SMS-tjeneste, som er en såkalt "best effort"-tjeneste, det vil si at det ikke gis garantier med hensyn til tjenestens tilgjengelighet.

I 2016 økte omfanget av det som kalles Internet of Things (IOT). IOT betyr at stadig flere enheter kobles opp i foretakenes nettverk. Eksempler kan være systemer for overvåking, adgangskontroll, prosesstyring og videosystemer. Disse enhetene er ikke godt sikret mot hacking og andre angrep. De

har typisk firmware og software som ikke har vært endret på lang tid, og som har sårbarheter. I tillegg er ofte leverandørens standard brukerident for pålogging fremdeles aktiv.

I teorien bør alle data klassifiseres med henblikk på dataenes betydning og sårbarhet, og tilegnes en unik sikkerhetspolicy etter dette. Imidlertid setter kostnader til utstyr og administrasjon en grense her. Såkalt mikrosegmentering av nettverk, som var mye omtalt i sikkerhetsmiljøene i 2016, er et forsøk på komme nærmere dette målet. Mikrosegmentering er en slags virtualisering av nettversstakken – en parallell til virtualisering av minne, disk og CPU. Det vil si at foretaket for hvert lag i stakken har definert flere nivåer av sikkerhet. Etter en forutgående analyse av data med tanke på betydning og sårbarhet, tilegnes dataene riktig sikkerhet i hvert lag av stakken. Et praktisk eksempel er høysensitive data, som får høyeste nivå av sikkerhet. På transportlaget betyr det kryptering – dataene transporteres gjennom en kryptert kanal (Virtual Private Network). På applikasjonslaget betyr det sterk autentisering – brukerne kobles mot en prosedyre for sterk autentisering. I praksis holder foretakene seg til tre eller fire sikkerhetssoner (admin og krypto, internt, DMZ, Internett). Data må i et visst omfang tilpasses policy, og ikke omvendt. Dette stiller store krav til overvåking og at data puttes i rett sone.

Flere foretak anser at dette blir så komplisert at de lar andre styre det hele, inklusiv å administrere brannmurer. Fremmed administrasjon av brannmur og nettverkssegmenter og soner medfører muligheter for uønsket og ulovlig innsyn i data og systemer.

Tilganger til systemer og data. Datalekkasje.

I 2016 ble det avdekket at enkelte foretak knyttet til verdipapirmarkedet bør forbedre kontrollene når det gjelder tilgang til innsideinformasjon. Dersom innsideinformasjon blir benyttet til å oppnå økonomisk fordel, kan dette føre til at investorer unngår det norske verdipapirmarkedet.

Finanstilsynet har observert at et foretaks e-postserver driftes sammen med andre e-post-servere. Kryptering av e-post på transaksjonsnivå skjer mellom servere, dvs. at e-posten som regel ligger i klartekst på serverne. Dersom flere foretak deler infrastruktur, er det en risiko for at informasjon kan bli tilgjengelig for uvedkommende.

Finanstilsynet observerer at foretakene mangler rutiner som sikrer at e-post-konfigurasjonen er satt opp slik at den støtter kryptering, og at konfigurasjonen er slik satt opp, at sendinger ikke skjer dersom konfigurasjonen på mottakersiden ikke støtter kryptering eller ikke støtter kryptering som anses som tilstrekkelig sikker i dag.

Administrasjon (innmelding og fjerning av brukere og rettigheter) skjer i dag gjerne ved hjelp av et dertil egnet brukergrensesnitt i form av en eller flere applikasjoner som er bygget på tilgangskontrollsystemet. Tidligere var det mer vanlig å administrere brukere direkte i tilgangskontrollsystemet, det vil si ved hjelp av registreringsfunksjoner som er en integrert del av tilgangskontrollsystemet. Systemene kan fremdeles være slik at det er mulig å administrere brukere ved å registrere rett i tilgangskontrollsystemet. Dette utgjør en risiko.

Fra mai 2018 må foretakene tilfredsstille kravene i den nye personvernloven. Loven vil stille store krav til foretakene, med store negative konsekvenser ved mangelfull etterlevelse av kravene.

Datakriminalitet

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

I 2016 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 slike hendelser har medført til dels betydelige kostnader knyttet til å reetablere dataene fra kopier og tapt arbeidstid ved manglende tilgang til systemer og data.

Det vil være svært alvorlig dersom angripere klarer å gjøre store mengder kunde- og kortdata utilgjengelig.

Kompleks systemportefølje

Systemene er over lang tid bygd på teknologi og plattform som gjaldt på det aktuelle tidspunktet de ble utviklet. Dette har gitt komplekse systemer preget av flere produksjonskopier av dataene og egenutviklede koblinger mellom systemer. Mye ressurser går med til å holde oversikt, synkronisere data og vedlikeholde programmer. Dette gir kompleksitet og risiko.

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 ikke nødvendigvis kan gi full sikkerhet for at endringer vil fungere helt etter planen når de settes i produksjon.

Kompleks drift

Drift av flerlagsarkitekturer 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.

En rekke innrapporterte hendelser i 2016 var forårsaket av ressursmangel som diskplass, for få tråder i en prosess, minne eller nettverkskapasitet. Det kan synes som overvåking og trafikkanalyse er mangelfull. Disse manglene bør kunne rettes med en rimelig ressursinnsats.

Det er utfordrende å teste endringer i driftsoppsettet, blant annet fordi det økonomisk og praktisk ikke lar seg gjøre å opprette og vedlikeholde et komplett driftsmiljø for test, med applikasjoner, systemer, data og trafikk som svarer til et fullt produksjonsoppsett.

Endringsprosesser

Endringer innebærer stor iboende risiko for feil.

I 2016 er det en nedgang i omfanget av hendelser som kan henføres til mangler i endringsprosessene, selv om året var preget av betydelige endringer i systemene.

Nye metoder for gjennomføring av finansielle tjenester vil kunne medføre en større omforming av markedet. Banker og betalingsforetak kan måtte endre seg betydelig som følge av ytterligere automatisering innenfor kreditt og betaling. Nytt betalingstjenestedirektiv (PSD 2) åpner for inntreden av nye type aktører i markedet for betalingstjenester og kontoinformasjon.

Nye regulatoriske krav gjør at foretakene må foreta omfattende systemendringer og nyutvikling i 2016 og 2017.

Konsentrasjonsrisiko

Bankenes kjernesystemer driftes ulike steder. Nordea og DNB drifter egne kjernesystemer, Eika-bankene og en del mindre banker drifter hos SDC, og øvrige sparebanker har sin drift hos Evry. Filialer av utenlandske banker i Norge har også ulike løsninger, de fleste hos sin morbank. Tidligere var konsentrasjonen større, og en hendelse ville da sette større deler av finansnæringen ut av spill. Det er nå mindre sannsynlig at samme hendelse rammer flere av foretakene samtidig.

Infrastruktur for betalingsformidling er imidlertid i stor grad konsentrert hos Nets, noe som medfører høy sårbarhet.

Forsikringsnæringen og verdipapirnæringen har i stor grad drift ulike driftssteder.

Kontinuitet

Innrapporterte hendelser i 2016 viser at i mange tilfelle fungerer ikke kontinuitetsløsningene slik de skal. Det kan skyldes komplikasjoner i oppsett, at reserveløsningen ikke oppdateres i takt med endringer i omgivelsene, eller at reserveløsningene ikke testes etter endringer i omgivelsene.

Enkelte store aktører testet i 2016 sine kontinuitetsløsninger. Finanstilsynet er etter dette tryggere på at disse løsningene vil fungere som forutsatt i en avvikssituasjon.

For betalingskortinfrastrukturen er det etablert velfungerende kontinuitetsløsninger.

Kompetanse og kapasitet

Det er stor etterspørsel etter IT-kompetanse generelt, ikke minst i offentlig sektor. Det er for tiden stor konkurranse når det gjelder å komme først til markedet med nye finansielle tjenester. Iboende risiko for feil og mangler øker. Disiplin når det gjelder kvalitet og kontroll settes på prøve.

6.3 Brukere og forbrukere

Risiko ved bruk av e-handelssystemer for verdipapirhandel

Tilgang til korrekt informasjon og muligheten til å utføre handler på bakgrunn av denne informasjonen er kritisk suksessfaktor for alle brukere av elektroniske handelssystemer for verdipapirer.

E-handel med verdipapirer består av ulike typer eller kategorier brukere med ulike behov og ulik grad av risikoappetitt. Brukere som handler aksjer en sjelden gang (ukentlig, månedlig eller årlig), benytter sin e-handelsløsning mest for å følge utviklingen i porteføljen. Handel gjøres gjerne med sikkerhet i kundens bankkonto og oppgjøret blir et internt bytte mellom penger på bankkonto og verdipapirer på depotkonto. Denne kategorien brukere vil sjelden være eksponert for så høy grad av risiko at de har behov for akutte endringer av sine posisjoner.

Mer aktive brukere, som ønsker høy eksponering, benytter seg av kreditter og derivater, og vil helst bruke systemer med innebygd kredittgivning uten bankkobling. Dette medfører at brukere av slike systemer ikke er avhengig av banksystemer for å gjennomføre handel, og har således betydelig lavere risiko for avbrudd i systemtilgangen. Samme verdipapirforetak tilbyr ofte flere typer løsninger som er tilpasset de ulike brukergruppene.

Brukergrupper blir stengt ute

Fra næringen er det uttalt at Norge har et effektivt betalingssystem fordi betalingsforetakene er innovative, og at foretakene er raske med å sanere gamle løsninger. En velkjent saneringsmekanisme er å prise tjenestene opp, og å fjerne manuelle løsninger, det være seg blankettbaserte betalinger, minibanker eller kontorer. Dette går ut over brukere som ikke har samme forutsetninger for å ta i bruk digitale løsninger, blant annet mange eldre forbrukere.

Brukerne påføres risiko

Betalingssystemene bør ikke påføre kunden større risiko enn nødvendig. Store kundegrupper, for eksempel eldre forbrukere, benytter kort kun i fysiske butikker og minibanker. Samtidig vet vi at omfanget av svindel knyttet til uautorisert[32] bruk av kort på Internett er betydelig og økende. Retningslinjer for sikkerhet i internettbetalinger fastsatt av EBA stiller krav om at forbruker skal kunne sperre kortet for bruk på Internett. Flere betalingsforetak har enda ikke innført dette for sine kort.

[32] Uautorisert vil si at kunden ikke har godkjent bruken.

7 Finanstilsynets oppfølging

7.1 Sentrale områder for Finanstilsynets IKT-tilsyn

Tilsynsvirksomheten er risikobasert.

Finanstilsynet vil ha stor oppmerksomhet på de tilsynsenhetene og deres leverandører som har størst innvirkning på finansiell stabilitet og velfungerende markeder. Finansforetak som gjennomfører større endringer på IKT-området, og dermed kan øke risikoen innenfor operasjonell risiko, vil vektlegges. Andre aktuelle tema for tilsyn er blant annet foretakenes kontroll med alle former for tilganger til systemer som inneholder sensitiv informasjon, beredskap knyttet til kontinuitet og kriseløsninger, risikovurderinger, lydopptak av telefonsamtaler og utvikling av nye løsninger som omfatter å ta i bruk ny teknologi. Cybersikkerheten i foretakenes IKT-løsninger og organiseringen av overvåkning vil prioriteres.

Tilsynsvirksomheten vil også omfatte foretakenes risikovurderinger i forhold til utkontraktering av IKT og kvalitet på avtaleverk og oppfølging av avtaler mellom foretak og leverandør. Hvitvasking og terrorfinansieringsløsninger vil følges opp.

7.2 Arbeid med betalingssystemer

Finanstilsynet vil følge opp foretakenes betalingstjenester mht. ny forskrift[33] til betalingssystemloven og etterlevelse av meldeplikten.

Retningslinjer for sikkerhet for internettbetalinger vil følges opp gjennom stikkprøver og penetrasjonstesting mot Internett-baserte løsninger.

Samarbeidet med Norges Bank vil videreføres.

7.3 Oppfølging av hendelser

Finanstilsynet vil følge nøye med på utviklingen av alvorlige hendelser, og legge vekt på at årsak(er) avdekkes og tiltak iverksettes for å hindre gjentakelser.

Ved alvorlige avvik vil det ved behov bli gjennomført oppfølgingsmøter.

[33] Forskrift om systemer for betalingstjenester

7.4 Beredskapsarbeid

Arbeidet i Beredskapsutvalget for finansiell infrastruktur (BFI) vil videreføres. Blant annet gjennomgås hendelsesscenarioer og det vurderes om ansvarsforhold ved krisesituasjoner er tilstrekkelig klare. Det er planlagt gjennomføring av øvelser også i 2017.

Finanstilsynet vil også ta del i relevant beredskapsarbeid initiert fra andre sektorer og samhandling innenfor nasjonal rammeverk for digital hendelseshåndtering.

7.5 Oppfølging av trusselbildet knyttet til digital kriminalitet

Finanstilsynet vil holde seg orientert om foretakenes bruk av IKT og utvikling innen betalingstjenester, herunder særskilte utviklingstrekk innenfor:

- beredskapsarbeid rettet mot digital sårbarhet og digital sikkerhet
- endringene i betalingsformidlingen både ved utnyttelse av ny teknologi (FinTech), og ved høy grad av grensekryssende virksomhet

7.6 Forbrukervern

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

For svindel på Internett, er kopiering av magnetstripen den vanligste måten å tilegne seg informasjon, se punkt 3.1.7. Finanstilsynet vil fremover følge opp korttilbydernes etterlevelse av reglene om bruk av "magnetstripeterminaler".

8 Ordliste

Begrep/forkortelse	Betydning
AML	Tiltak mot hvitvasking (Anti Money Laundering)
Baltus	Bankenes on-line transaksjonsutvekslingssystem. Nettverk som bankene bruker for transaksjonsutveksling og dekningskontroll mot kontoer i hverandres kontosystemer.
BFI	Beredskapsutvalget for finansiell infrastruktur Koordineringsutvalg ved kriser i finanssektoren. Ledes av Finanstilsynet.
Bits	Bits AS er bank- og finansnæringens infrastrukturselskap.
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.
CEO-fraud	Svindler gir seg ut for å være øverste leder i en bedrift. Kalles også "Fake president fraud" eller "Business Email Compromise".
CERT	Computer Emergency Response Team. Ekspertgruppe som håndterer sikkerhetsbrudd på Internett.
CLS	Continuous Linked Settlement
DLT	Distributed Ledger Technology. En distribuert hovedbok kan anses som en type database som deles på tvers av noder i et nettverk
CNP	Card Not Present. Svindel med hjelp av stjålne kortopplysninger, vesentlig ved netthandel.
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.
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 forsikring og tjenestepensjon
EMIR	The European Market Infrastructure Regulation
ESMA	European Securities and Markets Authority. Den europeiske verdipapir- og markedstilsynsmyndigheten
FATF	Financial Action Task Force, medlemsorganisasjon for land hvor Norge er medlem, etablert for å sette standarder for AML/Hvitvasking og antiterrorfinansiering.
FCA	Financial Conduct Authority, Storbritannia
FinansCERT	Finanssektorens felles CERT
Fintech	Financial technology, brukes for teknologisk innovasjon i finanssektoren og også om foretak som tar i bruk moderne teknologi innenfor sektoren.

FOI	Felles Operativ Infrastruktur (for BankID)
Internet of Things (IoT)	Teknologiske enheter knyttet til Internett. Eksempler kan være systemer for overvåking, adgangskontroll, prosesstyring og videosystemer. Begrepet omfatter også utplasserte sensorer for innhenting av data. Mange av enhetene har innebygde datamaskiner og kan kommunisere med andre enheter og servicesentre. Teknologien legger til rette for å få utført tjenester fra hvor som helst, når som helst.
ISO 20022	ISO-standard for finansielle meldinger.
ISP	Internet Service Provider – Leverandøren av internettforbindelse og domenenavn
MAS	Monetary Authority of Singapore
NBO	Norges Banks Oppgjørssystem
NICS	Norwegian Interbank Clearing System
NFC	Near Field Communication. Benyttes i betalingskort og mobiltelefoner for kontaktløs betaling.
NSM	Nasjonal sikkerhetsmyndighet
Off-shoring	Kjøp av tjenester utenfor landets grenser. I noen sammenhenger brukt om kjøp av tjenester utenfor Norden/Baltikum.
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.
Privacy Shield	Avtale mellom EU og USA. Sikkerhet ved overføring av informasjon mellom partene. Trådte i kraft 12. juni 2017.
PSD 2	Nytt betalingstjenestedirektiv fra EU
PUM-tjeneste	Personlig utlevering med mottaksbevis. Sikker utleveringstjeneste for små forsendelser som leveres av Bring.
QR-kode	Quick Response Code er en mosaikkode for kommersiell og personlig bruk. Koden kan lagre et stort antall alfanumeriske tegn og kan leses hurtig. Den er derfor godt egnet til optisk lesing av data som eksempelvis en adresse.
Ransomware	Skadevare som begrenser eller hindrer tilgang til IKT-løsninger, med etterfølgende krav om løsepenger.
SecuRe Pay	European Forum on the Security of Retail Payments – forum under ECB
Sterk autentisering	Autentisering ved bruk av flere elementer, f.eks. pinkode + passord.
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TFIT	Taskforce on IT Risk Supervision – arbeidsgruppe under EBA
TFPS	Taskforce on Payment Services – arbeidsgruppe under EBA
Trojaner	Virus som utgir seg for å være et vanlig program, men som inneholder ondsinnet kode.
TR	Transaksjonsregister for verdipapirer (Trade Repository)
TRS	Transaksjonsrapportering (verdipapirområdet)
Vannhull	Betegner en digital angrepsstrategi der offeret er en gruppe organisasjoner eller type industri (i dette tilfelle finans). Angriperne infiserer nettsteder den valgte gruppen antas å besøke ofte med skadevare, som overføres til gjester.

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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

04.2017