FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Finanssektorens bruk av informasjons- og kommunikasjonsteknologi (IKT)

RISIKO- OG SÅRBARHETSANALYSE (ROS)

2017

Risiko- og sårbarhetsanalyse (ROS) 2017

Finanssektorens bruk av informasjons- og kommunikasjonsteknologi (IKT)

Finanstilsynet, 7. mai 2018

INNHOLD

1 Innledning

Finanstilsynet utarbeider hvert år en risiko- og sårbarhetsanalyse (ROS-analyse) av finanssektorens bruk av IKT. Gjennom tilsynsarbeidet har Finanstilsynet en bred kontaktflate med foretak, bransjeforeninger, leverandører, standardiseringsorganer og nasjonale og internasjonale myndigheter.

Formålet med rapporten er å beskrive risiko og sårbarhet, både med hensyn til finansiell stabilitet, det enkelte foretak og den enkelte forbruker.

I kapittel 2 oppsummeres risikoen ved finanssektorens bruk av IKT og betalingstjenester.

Kapittel 3 gir et bilde av Finanstilsynets funn, observasjoner og erfaringer fra tilsynsvirksomheten i 2017. Teknologiske utviklingstrekk som antas å kunne få betydning for foretakenes bruk av IKT, blir omtalt.

Kapittel 4 refererer foretakenes egne vurderinger. I tillegg er noen sentrale leverandører av tjenester og sikkerhetsløsninger intervjuet, og aktuelle vurderinger av trusselbildet med relevans for finansnæringen er referert.

I kapittel 5 framkommer Finanstilsynets overordnede vurdering av risikobildet i 2017 på bakgrunn av funn, observasjoner og utviklingstrekk. Vurderingene trekker fram 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 6 beskriver områder som Finanstilsynets vil ha særskilt oppmerksomhet på framover.

En ordliste som forklarer ord og akronymer er vedlagt.

2 Oppsummering

Den norske finansielle infrastrukturen er i hovedsak robust. Det var ingen IKT-hendelser med konsekvenser for finansiell stabilitet i 2017. Foretakenes kunder opplevde imidlertid flere alvorlige hendelser som medførte lavere tilgjengelighet og bortfall av tjenester.

Finanstilsynet har identifisert sårbarheter som utgjør risiko for at alvorlige hendelser kan inntreffe. På det grunnlaget mener Finanstilsynet at foretakene bør styrke arbeidet innen IKT-sikkerhetsområdet og arbeidet med å etablere tilstrekkelige robuste løsninger. Leverandørstyringen er utfordrende for foretakene, og det er behov for å bedre samhandlingen mellom foretakene og leverandørene.

Høy endringstakt og kompliserte verdikjeder med et stadig økende antall aktører utfordrer foretakene i deres arbeid med å opprettholde god styring og kontroll. Mangelfull tilgang til kvalifisert personell med kompetanse innen sikkerhetsområdet, arkitektur og ny teknologi er også en utfordring.

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

2.1.1 Tilsynsområder

Betalingssystemer

Finanstilsynet observerte flere alvorlige hendelser, både i omfang og varighet, for betalingssystemene i 2017. For noen av hendelsene var betalingstjenestene utilgjengelige opp til et helt døgn for mer enn 30 prosent av bankkundene. Hendelsene skapte usikkerhet i markedet knyttet til foretakenes evne til kontinuerlig å levere betalingstjenester og gjennomføre betalingsoppdrag, og viste at det for enkelte typer betalingskort ikke er etablert reserveløsninger.

Betalingsområdet var også i 2017 preget av store endringer, blant annet ved etablering av eget betalingsforetak for samarbeid om Vipps, og avvikling av MobilePay og mCASH.

Flere av foretakene og deres leverandører har i 2017 arbeidet med å tilpasse virksomheten til det nye betalingstjenestedirektivet (PSD 2), både organisatorisk og teknisk.

Finanstilsynet har for første gang siden registreringen startet i 2010, observert en nedgang i kortsvindel. Antall misbrukte kort gikk ned med 5 prosent, mens samlede tap var 30 prosent lavere i 2017 enn i 2016. Det antas at nedgangen er et resultat av strengere sikkerhetskrav fra blant annet kortutstedere, hvor sterk autentisering av kortholder ved bruk av betalingskort har vært et viktig virkemiddel. Det var også en nedgang i svindler mot nettbank sammenliknet med 2016.

Finanstilsynet mener foretakene bør få bedre styring og kontroll med risikoen og sårbarheten i betalingssystemene.

Bank

Kontinuerlige endringer i trusselbildet for digitale angrep er en risiko som i økende grad utfordrer bankene i arbeidet med å etablere risikoreduserende tiltak. Finanstilsynet ser behov for at bankene forbedrer sitt arbeid på IKT-sikkerhetsområdet. Dette gjelder blant annet organisering av arbeidet, gjennomføring av risikoanalyser både for egen infrastruktur og for utkontraktert IKT-infrastruktur, ajourføring av sikkerhetsrammeverket og proaktive tiltak for å styrke foretakets forsvarsverk. Styring og kontroll med utvidete tilgangsrettigheter må forbedres.

Finanstilsynet har registrert en forbedring i bankenes arbeid med å utarbeide forretningsmessige konsekvensanalyser som grunnlag for bankenes krav til kontinuitets- og katastrofeløsninger. Hendelser viser imidlertid at det fortsatt er behov ytterligere forbedringer.

Verdipapirområdet

Flere regelverksendringer medførte behov for endringer i foretakenes IKT-systemer. Systemendringene førte til hendelser og avdekket svakheter i foretakenes IKT-systemer, herunder testsystemer. I forbindelse med lanseringen av det nye produktet aksjesparekonto, var det enkelte foretak som etablerte løsninger uten nødvendig funksjonalitet.

Mange av foretakene har behov for å forbedre sin dokumentasjon av retningslinjer, rutiner og planer for gjennomføring av sikkerhetstester.

Forsikringsområdet

Finanstilsynet erfarer at de fleste forsikringsforetakene har god risikostyring, men at det også er foretak hvor situasjonen ikke er tilfredsstillende.

Når ny teknologi tas i bruk ved nye forsikringsprodukter, stiller det økte krav til både bruk av og kontroll med innsamlede data og krav til risikovurderinger som identifiserer relevant risiko. Dette gjelder for eksempel ved bruk av sensorteknologi og overvåking av kundeatferd.

2.1.2 Hendelser

Antall hendelser økte med rundt 25 prosent fra 2016 til 2017, og tilgjengeligheten til betalingstjenester og kunderettede løsninger ble redusert. Av de 190 rapporterte hendelsene gjaldt kun ti av rapportene tilsiktede sikkerhetshendelser (digital kriminalitet). De resterende 180 var meldinger knyttet til operasjonelle hendelser.

De meste alvorlige hendelsene var forårsaket av feil i styringssystemer som i sin tur medførte at dupliseringsløsninger for kontinuitet ved avbrudd ikke fungerte som forutsatt. Dette rammet både banker og betalingstjenester, og i noen tilfeller også forsikringsforetak. Hendelsene viste at svikt i sentrale styringsmekanismer, som skal sikre redundans og kontinuitet i foretakenes driftsløsninger, kan gi store konsekvenser.

Det var også flere hendelser knyttet til BankID, som i flere tilfeller rammet alle BankID-brukerne. Flere av hendelsene inntraff på dager med ekstra høy belastning og avdekket kapasitetsproblemer med tjenesten.

2.1.3 Utkontrakteringsmeldinger

Finanstilsynet mottok nærmere 50 meldinger om utkontraktering av IKT-virksomhet i 2017. De fleste meldingene gjaldt utkontraktering til store globale skyleverandører eller endringer av underleverandør. Finanstilsynet observerer et stadig økende antall underleverandør for utkontraktert IKT-virksomhet.

Risikovurderinger som skal danne grunnlag for styrebeslutninger om utkontraktering, er i noen tilfeller mangelfulle.

Ved gjennomgang av avtalene om utkontraktering erfarer Finanstilsynet at IKT-forskriftens krav om rett til revisjon og tilsynsmyndigheters rett til tilsyn bare unntaksvis ikke er oppfylt. Bestemmelser som skal gjelde ved overføring av tjenesten til annen leverandør (exit-bestemmelser), er etter Finanstilsynets vurdering ofte for lite spesifisert.

2.1.4 IKT- og informasjonssikkerhet

Digital kriminalitet utgjør en økende trussel. Digitale angrep kan ramme flere dimensjoner, og det kan være vanskelig å fastslå hva hensikten med angrepet er. Selv om omfanget av uønsket aktivitet mot foretakene øker vesentlig, er det kun et fåtall som resulterer i en sikkerhetshendelse.

Finanstilsynet har i 2017 registrert organisatoriske, operasjonelle og tekniske svakheter som medfører sårbarheter for tilsiktede angrep og utilsiktede feil. Arbeidet med IKT-sikkerhetsområdet må forbedres og gis en tydelig ansvarsplassering i organisasjonen. Ansvaret for henholdsvis styring av IKT-

sikkerheten, kontroll med IKT-sikkerheten og det operative IKT-sikkerhetsarbeid skal være klart adskilt.

Finanstilsynet anser sikkerhetstesting ved bruk av kvalifiserte eksterne ressurser som et viktig verktøy i arbeidet med å avdekke sårbarheter i foretakets infrastruktur og elektroniske forsvar.

Et annet viktig risikoreduserende tiltak er foretakenes forebyggende arbeid med å bevisstgjøre foretakets ansatte om de ulike metodene som kriminelle benytter. Slike metoder omfatter blant annet sosial manipulering[1] av ansatte for å tilegne seg informasjon som brukeridentiteter og passord, e-post med falsk avsender for å lure ansatte til å utføre uautoriserte handlinger, og lenker i e-post fra kriminelle med formål å plassere ondsinnet kode. Finanstilsynet konstaterer at foretakene er aktive i dette forebyggende arbeidet.

2.1.5 Utviklingstrekk innenfor finansiell teknologi

Utviklingen innen finansiell teknologi (FinTech) er knyttet både til nyetablerte og eksisterende foretaks tjenester. Teknologi for foretakets oppfølging og etterlevelse av regulatorisk regelverk (RegTech) er også tatt i bruk gjennom løsninger som skal bidra til mer effektive og automatiserte tilsynsprosesser både hos foretakene og hos tilsynsmyndighetene.

Kunstig intelligens og robotisering tas i bruk av foretakene for å effektivisere og forenkle virksomhetens prosesser. Også blokkjede-teknologiens potensiale vurderes av foretakene.

2.2 Foretakenes vurderinger

Foretakene vurderer følgende trusler som de viktigste:

- feil i systemer og svekket stabilitet som følge av økt omfang av og hyppighet på endringer i foretakets systemer
- dataangrep, herunder mer avanserte og lettere tilgjengelige angrepsmetoder og -verktøy
- manglende IKT-kompetanse og -kapasitet i foretaket
- mangelfull styring og kontroll av tilganger for beskyttelse av informasjon og systemer
- (sensitiv) informasjon på avveie
- BankID som ikke fungerer eller ikke fungerer tilfredsstillende
- redusert mulighet for å sikre tjenester fra ende-til-ende ved utkontraktering
- utkontrakterte tjenester som ikke tilfredsstiller foretakets krav til sikkerhet og krav som følger av lov og forskrift

[1] Sosial manipulering utnytter menneskelig kontakt og sosiale evner for å få tak i eller påvirke informasjon (nettvett.no)

Forventninger fra markedet om nye og enklere løsninger utgjør en risiko og kan medføre manglende kvalitet i løsningene ved at det ikke settes av nok tid til testing, spesielt av kapasitet og responstid. Andre trusler som nevnes av foretakene, er graden av kompleksitet i IT-systemer, nye regulatoriske krav som krever systemendringer, og tap ved uautorisert bruk av kortinformasjon i forbindelse med netthandel eller telefonhandel (Card Not Present – CNP). Noen foretak peker på risikoen for at deres systemer ikke har høy nok presisjon når det gjelder å flagge mistenkelige transaksjoner og god nok datakvalitet for ivaretakelse av kravet til "kjenn din kunde". Det blir også trukket fram som en risiko at informasjon foretaket har ikke blir tilstrekkelig utnyttet for å iverksette risikoreduserende tiltak.

2.3 Aktuelle risikoområder

Finansiell infrastruktur

Finanstilsynet mener den norske finansielle infrastrukturen i hovedsak er robust. Stabiliteten var noe dårligere i 2017 enn i 2016 og 2015, men bedre enn i 2014. Hendelser som rammer felles infrastruktur, leverandører til mange foretak eller større foretak alene, kan medføre store konsekvenser.

Foretakene

Finanstilsynet vurderer risiko knyttet til sårbarheter i foretakets driftsløsninger, tilgangsstyring, endringsstyring og forsvarsverk mot digital kriminalitet som de mest sentrale truslene. Sårbarheter knyttet til leverandørstyring, katastrofe- og beredskapsløsninger og kompetanse er også sentrale risikoer.

Forbrukere

Spor som legges igjen ved bruk av digitale tjenester kan misbrukes av tjenesteleverandører. Slike spor kan, dersom de kommer uvedkommende i hende, utgjøre en betydelig risiko for å bli brukt i kriminell vinning.

Økt digitalisering innebærer at bankkunder, som av forskjellige grunner ikke selv benytter bankenes digitale tjenester, ser seg nødt til å la familiemedlemmer eller andre betrodde få tilgang til sine digitale signaturer for bruk av digitale tjenester. Finanstilsynet vurderer at dette utgjør en risiko for at identiteter kan bli misbrukt, spesielt der kundens innlogging i nettbank opereres av den betrodde.

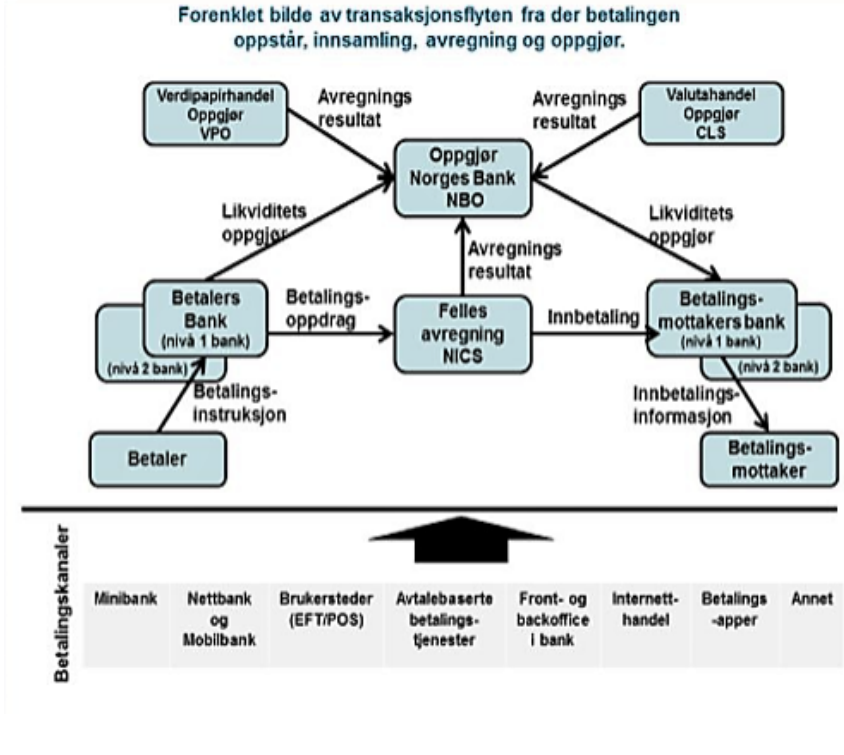
3 Finanstilsynets funn og vurderinger

Kapittelet omhandler vurderinger basert på Finanstilsynets arbeid med IKT og betalingstjenester i 2017 og omtaler observasjoner fra IKT-tilsyn, rapporterte hendelser, meldinger om endringer i utkontrakteringsavtaler, meldinger om nye eller endrede betalingstjenester og annen tilsynsvirksomhet.

Relevant regelverk og 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 2017 selv om enkelte hendelser skapte usikkerhet om foretakenes evne til kontinuerlig å levere robuste betalingstjenester og gjennomføre betalingsoppdrag.

Figur 1 Transaksjonsflyten i det norske betalingssystemet



Et betalingssystem defineres som et system basert på felles regler for avregning, oppgjør og overføring av betalinger mellom to parter som samhandler økonomisk. Juridisk skilles det mellom et interbanksystem, som behandler transaksjoner mellom banker, og en betalingstjeneste, som behandler transaksjoner mellom kunde og bank.

Figur 1 viser transaksjonsflyten i det norske betalingssystemet. Nederst i figuren illustreres de ulike betalingskanalene som kundene benytter.

Kilde: Finanstilsynet

3.1 Betalingssystemer

3.1.1 Generelt om betalingssystemer

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. Blant annet som følge av det reviderte betalingstjenestedirektivet (PSD 2), er det foreslått en rekke regelverksendringer som vil berøre betalingssystemene.

3.1.2 Styring og kontroll med risiko og sårbarhet i betalingssystemene

God styring og kontroll er avgjørende for å sikre robuste og stabile betalingssystemer.

Omfanget av og hyppigheten på endringer påvirker risikobildet. Finanstilsynet observerer en høy endringstakt som i seg selv utgjør en betydelig risiko. Endringstakten påvirkes i stor grad av økt konkurranse som følge av kunders forventninger, teknologiske framskritt og regulatoriske endringer. Nye aktører kommer inn i verdikjeden, og betalingstjenester integreres i andre tjenester. Flere foretak har allerede etablert grensesnitt (API-er) som gjør det mulig for tredjepartsaktører å tilby nye tjenester.

Foretakene må grundig vurdere risiko knyttet til betalingstjenestene[2], både med tanke på operasjonell risiko forbundet med drift og vedlikehold av tjenestene og sikkerhetsmessig risiko knyttet til blant annet uautorisert bruk av tjenestene. Finanstilsynet legger til grunn at omfattende risikovurderinger gjennomføres før nye betalingstjenester lanseres, særlig når ny teknologi tas i bruk i betalingsformidlingen.

Det reviderte betalingstjenestedirektivet (PSD 2) stiller flere krav når det gjelder styring og kontroll med betalingssystemene, herunder til styring og kontroll med operasjonell og sikkerhetsmessig risiko. Kravene vil gjelde både for eksisterende foretak som leverer betalingstjenester, og for nye betalingstjenesteforetak.

Foretakene må, i tillegg til å sikre at tjenester og informasjon er beskyttet gjennom logiske og fysiske sikringstiltak, sikre høy kvalitet i driftsløsningene og i tilknyttede prosesser som kan påvirke driften.

Det er Finanstilsynets erfaring at foretak, særlig de større, nedlegger et betydelig arbeid i sine drifts- og beredskapsløsninger for å redusere sårbarheten ved avvik i betalingsformidlingen, blant annet ved etablering av flere alternative driftssteder og redundante driftsløsninger. Finanstilsynet har imidlertid også i 2017 observert hendelser, jf. punkt 3.7.1, som viser at kvaliteten på enkelte foretaks arbeid på disse områdene ikke er tilfredsstillende. Hendelser i 2017 har vist at konsekvensen er stor dersom det

[2] Jf. forskrift om systemer for betalingstjenester

oppstår svikt i sentrale styringsmekanismer som skal sikre redundans og kontinuitet i foretakenes driftsløsninger. Løpende overvåking, kontroll og test av systemkomponenter som inngår i styringsmekanismer må være en viktig del av foretakets driftsoppgaver for å unngå denne type hendelser. Finanstilsynet har også observert at mangelfull kapasitetsstyring medførte at tjenestene ikke fungerte som forventet. Kapasitetsstyring er også en kritisk driftsoppgave for å opprettholde en kontinuerlig og stabil driftssituasjon.

De alvorligste hendelsene i 2017 skapte usikkerhet blant kundene om foretakenes evne til å gjennomføre betalingsoppdrag. Enkelte kunder, slik som ungdommer med betalingskort som ikke er omfattet av STIP[3], ble som følge av en hendelse helt forhindret fra å gjennomføre betalinger.

God informasjon til kundene ved hendelser er viktig. Erfaringen er at mange foretak har etablert gode prosesser når det gjelder å håndtere svikt i driftsløsningene, blant annet ved å informere kundene og iverksette avhjelpende tiltak.

Finanstilsynet mener det er behov for forbedringer på flere områder, som eksempelvis risikoreduserende tiltak knyttet til sentrale funksjoner i driftsløsninger og kapasitetsstyring. Hendelser kan få betydelige konsekvenser dersom alternative betalingsmåter ikke er tilgjengelig. Finanstilsynet understreker styrets og ledelsens ansvar for at foretaket har rutiner og systemer som sikrer stabile driftsløsninger og effektive beredskapsløsninger. Ansvaret gjelder også for de delene av tjenestene som er utkontraktert.

3.1.3 Melding 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 betalingstjenesten
- ny versjon med endret eller ny funksjonalitet som er vesentlig for systemet for betalingstjenesten

I 2017 mottok Finanstilsynet 17 meldinger om nye eller endrede betalingstjenesteløsninger. Meldingene er i hovedsak knyttet til mobile løsninger og betalingskortløsninger. Det er også mottatt meldinger om grensnitt mot tredjepartsleverandører.

Meldeplikten gjelder både eksisterende og nye foretak med konsesjon, og omfatter både banker, e-pengeforetak, betalingsforetak og andre aktører, der foretaket skal yte betalingstjenester. Finanstilsynet vil følge opp foretakenes etterlevelse av meldeplikten.

[3] Reserveløsning som trer i kraft dersom det ikke oppnås kontakt med banken fra kortterminalen. Driftssentralen kan autorisere på vegne av banken etter gjeldende regler.

3.1.4 Utvikling innen betalingstjenester og mobile betalingsløsninger

3.1.4.1 Utviklingstrekk

I Norge skjer utviklingen blant annet gjennom 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.

DNB inngikk i 2017 et samarbeid med flere andre norske banker og etablerte betalingsforetaket Vipps AS[4]. Det ble også åpnet for andre bankers deltakelse i samarbeidet gjennom etablering av distribusjonsavtaler med Vipps.

Ved utgangen av 2017 deltok et flertall av de norske bankene i Vipps-samarbeidet. Den mobile betalingsløsningen MobilePay ble som følge av dette avviklet i det norske markedet, og mCASH ble i sin helhet avviklet.

Vipps har stor utbredelse i Norge for betaling mellom privatpersoner og som alternativ til kontantbetaling til blant annet lag og foreninger. I tillegg er tjenestene også utvidet til bruksområder som betaling ved netthandel, betaling i butikk og fakturabetaling. Vipps, som nå er den eneste mobilbetalingsaktøren i det norske markedet, benytter egen infrastruktur som betinger at betalingsmottaker må installere samme applikasjon som avsender for at transaksjonen kan gjennomføres. Opprinnelig var Vipps avhengig av kortløsningene til MasterCard og Visa for betaling, men det er nå i tillegg åpnet opp for konto-til-konto-betalinger ved bruk av infrastrukturen for straksbetalinger[5].

Vipps AS, BankAxept AS og BankID AS varslet i november 2017 at de har inngått intensjonsavtale om fusjon for å være bedre rustet mot internasjonal konkurranse.

BankAxept AS etablerte i 2017 støtte for kontaktløs betaling ved bruk av fysiske kort, særlig for betaling av mindre beløp. Mange brukersteder har tidligere valgt å ikke åpne for kontaktløse betalinger som følge av at denne teknologien kun var tilgjengelig gjennom de internasjonale betalingsordningene til Visa og MasterCard. BankAxepts løsning har vært viktig for å øke bruken av kontaktløse betalinger. BankAxept vil i løpet av 2018 lansere konto-til-konto-betalinger, som blant annet kan integreres som betalingsløsning for netthandel.

På grunn av finansnæringens manglende standardisering og interoperabilitet av betalingsløsninger for betaling i butikk, ble Retail Norge etablert i 2016 (omdannet til Area Payment & Identification AS

[4] DNB, Sparebank 1-alliansen, Eika-alliansen, Sparebanken Møre og femten selvstendige sparebanker etablerte i 2017 Vipps AS.
[5] https://www.bits.no/bank/straksbetalinger/

(Area) i 2017). Forretningsidéen er å tilby en åpen betalingsplattform som aksepterer alle betalingstyper[6] på tvers av kanaler (netthandel, mobilhandel og i butikk)[7].

Utviklingen med bruk av biometriske kjennetegn i forbindelse med autentisering og betaling fortsetter, og flere norske foretak benytter nå identifikasjon gjennom fingeravtrykk. I Vipps-appen er det også tilrettelagt for ansiktsgjenkjenning, som per i dag kun kan benyttes på en type smarttelefon. En løsning for fingerbetaling[8] blir testet ut i Danmark.

PSD 2 stiller krav til sterk kundeautentisering og sertifikatløsninger. Buypass[9] posisjonerer sine tillitstjenester for det kommende regelverket, blant annet med sertifikatløsninger. BankID AS har i 2017 lansert en ny tillitstjeneste med enkel pålogging kalt xID[10], som et supplement til BankID.

3.1.4.2 PSD 2 som katalysator for nye tjenester og aktører

Det nye betalingstjenestedirektivet som trådte i kraft 13. januar 2018 innenfor EU, legger til rette for økt konkurranse og etablering av nye betalingstjenester. Flere EU-land har allerede erfart dette ved mottak av konsesjonssøknader. Finanstilsynet forventer en tilsvarende utvikling når PSD 2 trer i kraft i Norge. Gjennom et åpent betalingsmarked, og etablering av offentlige API[11] mot foretakenes infrastruktur, vil nye og eksisterende aktører med konsesjon kunne tilby de nye betalingstjenestene betalingsfullmakt[12] og opplysningsfullmakt[13].

Forslag til endringer i finansavtaleloven, finansforetaksloven og betalingssystemloven som gjennomfører reglene i PSD 2 har vært på høring og er nå til behandling i Finansdepartementet og Justisdepartementet. Inntil PSD 2 trer i kraft i Norge, vil ikke aktører kunne tilby de nye betalingstjenestene i det norske markedet med mindre betalingskontotilbyderne, dvs. bankene, aksepterer dette. Det samme gjelder norske foretak som ønsker å tilby betalingstjenester i EU-land.

Tilbydere av de nye tjenestene kan både være nye foretak som etablerer seg som betalingstjenestetilbydere, og eksisterende foretak som ønsker å tilby de nye betalingstjenestene. Vipps har allerede inntatt en viktig posisjon gjennom avtaler med betalingskontotilbydere. Foretak som har fått konsesjon som betalingsforetak, har informert om at det kan bli aktuelt for dem å tilby nye betalingstjenester når PSD 2 trer i kraft.

---

[6] BankAxept, Visa/Visa, Electron, MasterCard/Maestro, Diners, American Express, JCB, China Union Pay, Apple Pay, Samsung Pay og Android Pay, Vipps, Alipay
[7] https://rpwp.blob.core.windows.net/wpdata1/2017/10/Aera_produktark_Betaling.pdf
[8] https://no.ehandel.com/artikler/tester-fingerbetaling-lover-hoy-sikkerhet/435358
[9] https://www.tu.no/filer/EVENT/Digital2017_presentasjoner/Mads_Henriksveen_Buypass.pdf
[10] https://www.bankid.no/bedrift/xid/
[11] Application programming interface. Grensesnitt i en programvare som gjør at spesifikke deler av denne kan kjøres fra en annen programvare
[12] Payment Initiation Service Providers (PISP). Aktører som kan initiere betalinger på vegne av kunde
[13] Account Information Service Providers (AISP). Aktører som kan hente informasjon fra bankkonto på vegne av kunde

Finanstilsynet forventer at PSD 2 vil medføre at flere internasjonale aktører etablerer betalingstjenester i det norske markedet. Alipay, som betegnes som verdens største betalingsløsning, tilbyr en betalingsløsning for kinesere som ferierer i Norge knyttet opp mot deres konto i Kina[14]. Alipay er gitt konsesjon som betalingsforetak i Storbritannia og meldte i oktober 2017 grensekryssende virksomhet til Norge. Andre store globale aktører, som Apple Pay og Google Pay, er etablert i flere europeiske land, men er foreløpig ikke lansert i Norge. Enkelte aktører, som svenske Tink[15], er i ferd med å etablere seg i det nordiske markedet for å tilby finansielle sammenstillinger av blant annet kontoinformasjon.

3.1.4.3 PSD 2 – krav til styring og oppfølging av operasjonell og sikkerhetsmessig risiko

Enkelte har uttrykt bekymring for at endringene, som følge av innføringen av PSD 2, vil introdusere nye risikoer og sårbarheter knyttet til betalingstjenester. Det er imidlertid viktig å poengtere, jf. punkt 3.1.2, at det ved innføringen av direktivet stilles strenge og likelydende krav til både nye og eksisterende aktører om oppfølging og håndtering av operasjonell og sikkerhetsmessig risiko knyttet til leveranser av betalingstjenester. Nye aktører må gjennomgå en omfattende kvalitetssikringsprosess før konsesjon gis, der det stilles strenge krav til rutiner og prosesser både når det gjelder foretakets virksomhet og betalingstjenestene som skal tilbys.

Den samlede operasjonelle risikoen innen betalingsområdet antas derfor ikke å øke, utover at flere aktører og lengre verdikjeder i seg selv medfører økt risiko. Nye løsninger basert på moderne teknologi og utviklingsmetoder, sammen med strenge konsesjonskrav, antas å begrense den operasjonelle risikoen.

3.1.4.4 PSD 2 – regelverk for tilgang til betalingskonto

Målet med PSD 2 er at kunden skal få tilgang til flere og bedre tjenester gjennom at regelverket definerer kravene (autentisering og sikker kommunikasjon) og at markedet utvikler flere og bedre løsninger innenfor kravene. Etter PSD 2 skal foretak med konsesjon få tilgang til kontoinformasjon og anledning til å utføre betalinger på vegne av kunder. Regler for tilgang til kontoinformasjon framgår av forordning 2018/389 "Regulatory technical standards for strong customer authentication and common and secure open standards of communication". Standarden skal gjelde fra 14. september 2019 innenfor EU. Dokumentasjon av tekniske spesifikasjoner og testfasiliteter (§§ 3 og 5 i artikkel 30) skal imidlertid være tilgjengelig fra kontotilbyder fra 14. mars 2019. Den europeiske banktilsynsmyndigheten (EBA) har tatt initiativ til en arbeidsgruppe som skal definere nærmere krav til kommunikasjonsgrensesnittet mellom tredjepartsaktører med konsesjon og kontotilbyder.

PSD 2 tillater at aktører med konsesjon autentiserer kunden med identitetskjennetegn som er utstedt av en aktør med konsesjon, eller med identitetskjennetegn kunden har fra før. Kravene til ID-ene og autentiseringen framgår av standarden.

[14] http://www.betal.no/nyheter/alipay-lansert-i-norge-for-kinesiske-turister_100219_100219
[15] https://www.nordea.com/no/presse-og-nyheter/nyheter-og-pressemeldinger/news-group/2017/nordea-partners-up-with-tink.html

Standarden forutsetter at aktører med konsesjon autentiserer seg overfor kontotilbyder. Dette kan skje ved hjelp av digitale sertifikater av type EIDAS Høy.

Finanstilsynet vurderer risikoen knyttet til den tekniske utviklingen av grensesnittene som begrenset. De tekniske protokollene og standardene som kreves for å realisere formålet, er vel kjente og mye benyttet.[16]

3.1.5 Sperring av kort for bruk på Internett

Etter EBAs retningslinjer for sikkerhet i Internett-betalinger, som trådte i kraft 1. august 2015, skal kortholder i større grad kunne sette grenser for hva eget betalingskort kan benyttes til. Kortholder skal blant annet kunne sperre kortet for bruk på Internett. Finanstilsynet anser en slik funksjonalitet som et viktig tiltak for å redusere Internettrelatert svindel.

Finanstilsynet konstaterer at noen av de store kortutstederne fremdeles ikke hadde implementert slik funksjonalitet i 2017. Finanstilsynet har påpekt mangelen og vil følge opp foretakene.

3.1.6 Svindel og angrep mot betalingstjenester

Norske nettbanker er i begrenset grad utsatt for svindelangrep. Dette indikerer at sikkerheten er på et nivå som gjør slike angrep mindre attraktive og/eller at potensielt utbytte anses som for lavt. Teknisk enklere scenarier med elementer av tradisjonelt bedrageri kan framstå mer attraktivt.

I flere tilfeller er det observert raffinerte former for sosial manipulering og informasjonsinnsamling om enkeltpersoner som gir kriminelle tilgang til offerets verdier, eller verdier som offeret råder over i en bedrift. Innsamlet informasjon blir sammenstilt og vinningspotensialet blir vurdert før svindelangrepet.

Falske e-poster og telefonsamtaler oppfattes av bankens medarbeidere, eller bankens kunder, som troverdige og medfører at de kriminelle lykkes i manipuleringen og gjennomføringen av svindelen. Kundene blir lurt til å registrere og autorisere transaksjoner som viser seg å ha en annen mottaker enn det kunden oppfatter. Både privatkunder og bedriftskunder er utsatt for svindel gjennom sosial manipulering, men på ulik måte.

Finanstilsynet er informert om at bankene ser en økning i denne typen svindel, både i form av faktiske tap og avvergede tap. Det er kunden som må dekke tap der kunden har vært uforsiktig og gitt svindlere tilgang til påloggingsinformasjon som følge av blant annet sosial manipulering. Bankene bistår kundene med å forsøke å stoppe betalingene og få tilbakeført pengene og kan til en viss grad advare kundene mot svindelmetoder som benyttes og der svindelforsøk er identifisert. Finanstilsynet konstaterer at enkelte foretak gjennomfører informasjonskampanjer og advarer både egne ansatte og kundene mot denne typen svindel. Finanstilsynet vil oppfordre foretakene til å intensivere dette arbeidet.

[16] Se for eksempel HelseID, https://www.nhn.no/helseid/

3.1.7 Oversikt over årlig tap knyttet til betalingstjenester

Nedenfor er det gjengitt tapstall i Norge for henholdsvis kort- og nettbanksvindel for de siste årene. Tallene viser samlede tap, uavhengig av om tapet dekkes av kunden selv, banken eller kortselskapet.

Tapstall i Norge for kortbruk

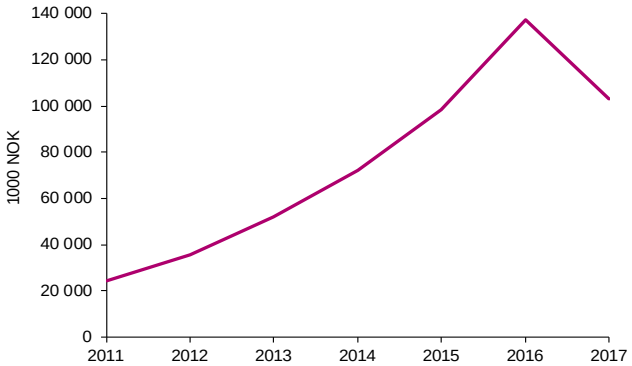
Tapstallene i 2017 viser en vesentlig nedgang i tap på kortbetalinger. Antallet misbrukte kort avtok med 5 prosent, mens samlede tap på kortbetalinger avtok med 30 prosent. Gjennomsnittlig svindlet beløp per misbrukte kort i 2017 var således vesentlig lavere enn i 2016.

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

Svindeltype betalingskort	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
Misbruk av kortinformasjon, Card-Not-Present (CNP) (Internett-handel m.m.)	35 701	51 954	72 056	98 410	137 015	102 908
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort i Norge	2 308	762	524	2 670	1 360	483
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort utenfor Norge	55 869	51 534	51 685	48 447	41 762	17 452
Originalkort tapt eller stjålet, misbrukt med PIN i Norge	28 128	21 274	21 266	18 875	12 857	10 194
Originalkort tapt eller stjålet, misbrukt med PIN utenfor Norge	8 544	9 570	13 071	14 224	10 223	9 663
Originalkort tapt eller stjålet, misbrukt uten PIN	4 603	4 949	5 510	6 033	3 286	4 891
TOTALT	**135 153**	**140 043**	**164 113**	**188 660**	**206 503**	**145 591**

Kilder: Finanstilsynet og Bits

Figur 2 Utvikling i svindel med misbruk av kortinformasjon der fysisk kort ikke brukes (CNP)



Kilder: Finanstilsynet og Bits

Kortsvindel og datatyveri

For første gang siden innhentingen av tapstall begynte i 2010, sank tapene på betalingskort i 2017. Dette inkluderer også nedgang i tap ved varekjøp på Internett (CNP[17]), hvor nedgangen var på 25 prosent. Finanstilsynet antar at økte krav fra kortutstedere, kortinnløsere og brukersteder til sterk autentisering av kortholder, med bruk av sikkerhetsverktøy som 3D Secure[18] eller lignende, er hovedårsaken til lavere tap ved Internetthandel.

Alle kort i Norge utstedes med chip. På noen automater, herunder for kjøp av kioskvarer og parkeringsautomater, kan betaling kun gjennomføres ved bruk av magnetstripe. Derfor er tapene knyttet til misbruk av falske kort i Norge lave. Tapstallene for misbruk av falske norske kort er derimot større i utlandet enn i Norge fordi kort eller kortinformasjon som stjeles i Norge brukes i land hvor det fortsatt er vanlig å bruke magnetstripen. Stadig færre land bruker kun magnetstripen, og tapstallene for 2017 viser en nedgang på nærmere 60 prosent i denne typen tap.

Kostnader forbundet med kortsvindel

Finanstilsynet har utarbeidet et anslag for samlede kostnader forbundet med stjålet kortinformasjon. Beregningen er basert på summen av årlige direkte tap ved bruk av betalingskort og en vurdert gjennomsnittlig saksbehandlerkostnad for kortutsteder per misbrukt kort. Samlede direkte tap er brutto tap, og der tapet enten tas av brukerstedet, kortinnløser, kortutsteder eller korteier. I tillegg er det forutsatt et kostnadsbeløp per kort knyttet til at forbruker også har kostnader forbundet med stjålet kortinformasjon.

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

Kostnader ved svindel med betalingskort	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
Antall kort rammet av misbruk (antall)	20 332	22 531	38 541	44 900	68 162	65 024
Samlede direkte tap, jf. tabell 1	135 153	140 043	164 113	188 660	206 503	145 591
Saksbehandlerkostnader hos kortutsteder (2.250 kroner per kort)	45 747	50 695	86 717	101 025	153 365	146 304
Forbrukerkostnader (1.000 kroner per kort)	20 332	22 531	38 541	44 900	68 162	65 024
Samlet beregnet kostnad	**201 232**	**213 269**	**289 371**	**334 585**	**428 030**	**356 919**

Kilde: Finanstilsynet

[17] Korttransaksjon hvor kortinnehaver ikke må presentere det fysiske kortet ved betaling, for eksempel ved netthandel.
[18] Kortselskapenes standard for å identifisere og beskytte kjøpere og selgere når kort benyttes for å betale via Internett.

I tillegg til kostnadene som framkommer i tabell 2, kommer ytterligere kostnader knyttet til saksbehandling hos kortinnløsere, brukersteder og hos Finansklagenemda. I tillegg brukes store ressurser på transaksjonsovervåking og oppfølging mot kortholdere for å avverge potensielle tap. Samlede kostnader forbundet med kortmisbruk er derfor betydelige.

Tapstall knyttet til bruk av nettbank

Tapstall knyttet til bruk av nettbank er lave og sank med nesten 60 prosent i 2017. De fleste forsøk på svindel i nettbanken blir avverget fordi transaksjonene avbrytes før gjennomføring. Bankene, i samarbeid med Nordic Financial CERT[19], 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**	**2017**
Angrep ved bruk av ondartet programkode på kundens PC eller sikkerhetsmekanisme (trojaner)	5 064	1 327	552	3 055	2	727
Tapt/stjålet sikkerhetsmekanisme	3 367	1 285	6 655	963	8 758	1 892
Phishing og falske BankID-brukersteder	10		539	5815	2 428	2 057
Annet/ukjent	358	779	3 474	2 715	7 444	2 911
TOTALT	**8 799**	**3 391**	**11 220**	**12 548**	**18 632**	**7 587**

Kilder: Finanstilsynet og Bits

Tap ved svindel gjennom sosial manipulering

Finanstilsynet har ikke innhentet tall over CEO-svindel (direktørsvindel) i 2017, men er kjent med at bankene har registrert en økning både i reelle tap og i avvergede tap. Økningen har kommet til tross for advarsler og opplysningskampanjer i 2017 om CEO-svindel basert på informasjon knyttet til svindelscenarioene i 2016.

I tillegg til direktørsvindel, forekommer også annen type svindel basert på sosial manipulering, som investeringssvindel og ulike former for dating-svindel.

Kundene som er svindlet kontakter ofte banken for å få hjelp til å stoppe transaksjonene og få tilbakeført beløpene.

[19] Tidligere FinansCERT

3.2 Bank

Finanstilsynet har påpekt områder som bør forbedres hos bankene. Særlig oppmerksomhet har vært rettet mot IKT-sikkerhet, utkontraktering og beredskap. En nærmere omtale av sentrale funn og vurderinger følger nedenfor.

3.2.1 Organisering av IKT-sikkerhet

Finanstilsynet har gjennom tilsyn avdekket behov for bedre organisering av arbeidet med IKT-sikkerhet i bankene. Uklarheter i roller og ansvar kan medføre at viktige sikkerhetstiltak ikke blir utført. Ansvar for henholdsvis styring av IKT-sikkerheten, kontroll med IKT-sikkerhetsarbeidet og operativt IKT-sikkerhetsarbeid skal være klart adskilt. Det vises til punkt 3.9.1.

3.2.2 Risikoanalyser knyttet til IKT-sikkerhet

Trusselbildet er i stadig endring og medfører en kontinuerlig utfordring for, og endring i, risikobildet for bankene. Situasjonen tilsier at bankene løpende må oppdatere risikobildet og at tiltak iverksettes i tide. Gode risikoanalyser er avgjørende. Risikoanalyser kan imidlertid også skape falsk trygghet dersom vesentlige risikoer ikke blir identifisert og rapportert, og fulgt opp med nødvendige tiltak.

Ved tilsyn konstaterer Finanstilsynet at bankene gjennomfører risikovurderinger, men ser at dette ikke i tilstrekkelig grad omfatter teknisk infrastruktur som er utkontraktert. Dette gjelder blant annet risikovurderinger av nettverksarkitektur, nettverkskvalitet, brannmurer, klassifisering og beskyttelse av informasjon, konfigurering av servere og oppdatering av programvare.

Ved gjennomgang av risikoanalyser utført av bankenes utkontrakteringspartnere (leverandørene), ser Finanstilsynet at enkelte funn er repeterende og/eller innen samme kategori. Dette indikerer at tiltak ikke iverksettes selv der risiko er identifisert.

Finanstilsynets vurdering er at bankene må styrke innsatsen og sørge for at risikoer i hele verdikjeden identifiseres, vurderes og håndteres. Dette krever nødvendig kompetanse og kapasitet for å kunne ivareta et sikkerhetsnivå som er nødvendig for å opprettholde en forsvarlig drift.

3.2.3 Sikkerhetsrammeverk og kompetanse

Bankenes IKT-infrastruktur og -systemer er under kontinuerlig endring. Nye sårbarheter avdekkes og nye etableres blant annet som følge av økt takt i utviklingen av nye tjenester, ny teknologi og nye aktører i verdikjeden. Sammen med endringer i risikobildet stiller dette krav til at bankene og dens leverandører må oppdatere sikkerhetsrammeverket, herunder rammeverket for cyber-sikkerhet. Kvaliteten og kapasiteten i bankenes kompetansemiljøer er viktige faktorer i dette arbeidet.

Finanstilsynet oppfatter at bankene er bevisst på den økende og endrede risikoen, og på behovet for kompetanse innen sikkerhetsområdet. Samtidig er situasjonen utfordrende fordi tilgangen på kompetente ressurser er begrenset. Finanstilsynet har observert manglende oppdatering i bankers sikkerhetsrammeverk, for eksempel ved at endringer i risiko- og sårbarhetsbildet ikke er ivaretatt.

3.2.4 Svakheter i bankenes forsvarsverk

Banker i Norge har hittil ikke vært utsatt for angrep som har resultert i alvorlige situasjoner. Imidlertid er det globalt en økning i cyber-angrep, og bankene registrerer økt uønsket aktivitet. Risikoen for angrep mot bankene forventes derfor å øke, herunder også alvorlighetsgraden i angrepene. Slike angrep kan i ytterste konsekvens påføre banken betydelige tap og/eller sette banken helt ut av spill.

Gjennom tilsyn på cyber-sikkerhetsområdet har Finanstilsynet identifisert og påpekt svakheter i bankenes forsvarsverk som i unødig grad eksponerer bankenes systemer og nettverk for angrep. Finanstilsynet har også observert uklar ansvarsfordeling og mangelfulle rutiner for programvareoppdateringer (patching) mot kjente sårbarheter.

Leverandør av IKT-tjenester er i mange tilfeller den utførende part i arbeidet med å etterleve sikkerhetskravene og å tette sikkerhetshull. Finanstilsynet registrerer imidlertid at bankene har utfordringer med å forankre sikkerhetskravene hos sine leverandører. Finanstilsynet understreker viktigheten av at sikkerhetskravene reguleres i avtalen mellom partene, og foretakets ansvar for å følge opp at leverandøren etterlever kravene.

3.2.5 Tilgangsstyring

Finanstilsynet har gjennom tilsyn med bankenes tilgangsstyring og -kontroll rettet særlig oppmerksomhet mot personell med utvidede tilgangsrettigheter (administrative rettigheter) hos foretakets leverandører. Også der ansatte i foretaket har slike utvidede rettigheter, er dette et viktig tema.

Personell med administrative rettigheter eller med utvidet tilgangsrett, kan utnytte sine rettigheter til ulovlig å hente ut informasjon eller plassere ondsinnet kode i bankens systemer. Personell kan også utføre ulovlige handlinger, bevisst eller ubevisst, som resulterer i ustabilitet i driften eller utføre handlinger som medfører at systemer og tjenester ikke er tilgjengelige. Logg over utførte handlinger kan slettes av den som utførte handlingene for å skjule spor.

Finanstilsynet har observert for svak styring og kontroll med utvidede tilgangsrettigheter. Manglende periodiske gjennomganger av tilganger og brukere med tilgangsrettigheter utover reelle behov, er noen av funnene. Finanstilsynet har overfor foretakene påpekt betydningen av kontroll med utvidede tilganger, også når det gjelder personell hos leverandører, og at utvidede tilganger ikke bør gis på permanent basis. Denne type tilganger skal underlegges god styring og kontroll og knyttes opp mot enkeltoppgaver som for eksempel en hendelse, et problem eller en endring.

Det er viktig at bankene er bevisst på risikoen og etablerer nødvendige proaktive kontroller for å fange opp mistenkelig aktivitet, for eksempel gjennom automatiserte kontroller.

Særlig oppmerksomhet bør rettes mot tilgang til konfidensiell informasjon og personopplysninger, og tilgang til områder som servere, databaser, systemprogrammer og nettverk.

3.2.6 Utkontrakteringsavtaler

Finanstilsynet har gjennomgått utkontrakteringsavtaler ved melding om utkontraktering, ved søknad om konsesjon eller ved mottatt dokumentasjon i forbindelse med IKT-tilsyn. Gjennomgangen viser at det legges ned mye arbeid i å etablere avtaler med bestemmelser som skal sikre at foretakene overholder lover og regler. Avtalene som er gjennomgått viser at det kun er unntaksvis at IKT-forskriftens § 12 om utkontraktering ikke er dekket av avtalens bestemmelser. Dette gjelder også for kontrakter som inngås med globale skyleverandører.

Imidlertid har Finanstilsynet erfart at foretakene har mangelfull innsikt i og forståelse av hva den utkontrakterte IKT-tjenesten omfatter, både hvilken teknisk infrastruktur som benyttes for tjenesten, og hvilke oppgaver som leverandøren er forpliktet til å utføre. Særlig gjelder dette for "Software as a Service" (programvare som tjeneste). Finanstilsynet understreker at foretakene har ansvar for egen IKT-virksomhet, inkludert tjenester som er utkontraktert, jf. IKT-forskriften, og det forventes at foretaket kan vurdere og følge opp utkontrakterte tjenester. Se også punkt 3.8.2.

3.2.7 Test av beredskapsløsninger og konsekvensanalyser

3.2.7.1 Test av beredskapsløsninger

IKT-forskriften krever årlig testing av beredskapsløsninger. I forbindelse med tilsyn er det blant annet avdekket at erfaring fra virkelige hendelser har blitt ansett som tilstrekkelig gjennomførte tester av beredskapsløsninger. Det framgår imidlertid ikke tydelig av bankens rapport at den planlagte testen ikke ble gjennomført. Finanstilsynet ser verdien av erfaringen som bankene tilegner seg ved virkelige hendelser, men forventer at bankene vurderer om en faktisk hendelse er tilstrekkelig grunnlag for å ikke gjennomføre planlagte tester, eventuelt om hendelsen tilsier tilpasning av den planlagte testen. Vurderingen bør legges fram for bankens styre.

3.2.7.2 Konsekvensanalyser

Analyser av forretningsmessige konsekvenser ved driftsavbrudd skal danne grunnlag for bankenes krav til kontinuitets- og katastrofeløsninger. Etablerte kontinuitets- og katastrofeplaner er viktige og styrende dokumenter når alvorlige hendelser inntreffer, og skal ivareta både tekniske og organisatoriske forhold. Iverksettelse av kontinuitets- og katastrofeplaner i en faktisk situasjon vil være krevende. Gjennomarbeidede konsekvensanalyser og planer samt gjennomføring av tester legger grunnlaget for hvordan bankens kriseledelse, i samarbeid med eventuelle leverandører, vil være i stand til å håndtere en kritisk situasjon.

Finanstilsynet har gjennom sine tilsyn registrert en forbedring i foretakenes arbeid med gode konsekvensanalyser. Det er likevel grunn til å minne om viktigheten av dette arbeidet og at beredskapstester gjennomføres. Finanstilsynet har gjennom sin oppfølging av hendelser observert at foretak har utfordringer med å håndtere alvorlige driftsavbrudd.

3.2.8 Test av bankenes krav til rapportering til Bankenes sikringsfond

Finanstilsynet gjennomførte i 2017 tilsyn som gjaldt etterlevelse av bankenes krav til datasystemer for rapportering til Bankenes sikringsfond. Dette er femte året Finanstilsynet sammen med Bankenes sikringsfond gjennomfører testingen. Erfaringen er at bankene synes å nærme seg en tilfredsstillende kvalitet på rapporteringen.

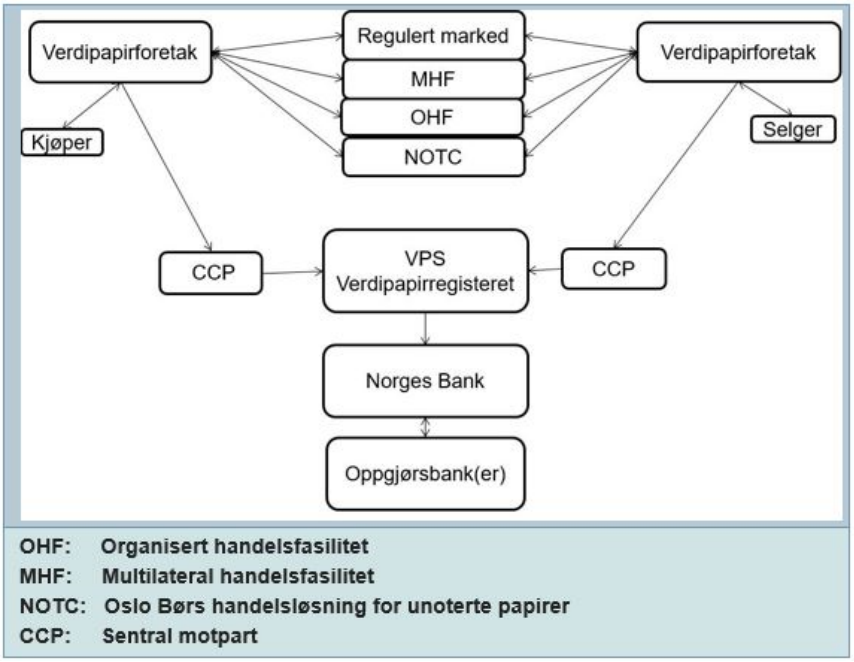
3.3 Verdipapirområdet

Betydelige endringer i rammevilkårene for verdipapirforetak og infrastrukturforetak, blant annet gjennomføringen av MiFID II og EMIR og MiFID, med utvidet TRS-Rapportering, gjeldende fra 2018, medførte i 2017 behov for endringer i foretakenes systemer. Nye produkter som aksjesparekonto og individuell pensjonssparing (IPS) ble lansert i 2017.

Sektoren har ikke hatt kritiske eller svært alvorlige IKT-hendelser i 2017, til tross for at foretakenes systemporteføljer generelt har vært preget av mange og til dels store endringer.

Finanstilsynet har gjennom sin tilsynsvirksomhet påpekt områder som bør forbedres hos foretakene. En nærmere omtale av de mest sentrale funn og vurderinger følger nedenfor.

Figur 3 Forenklet framstilling av sentrale roller og sammenhenger



Kilde: Finanstilsynet

3.3.1 Underrapportering av IKT-hendelser

Flere hendelser i verdipapirforetak ble ikke rapportert til Finanstilsynet slik IKT-forskriften krever. Finanstilsynet ser alvorlig på at verdipapirforetak ikke overholder krav om rapportering av vesentlige avvik til Finanstilsynet. Underrapportering hemmer Finanstilsynets mulighet til å følge opp foretakenes håndtering av kritiske situasjoner. Gjennom oppfølging av hendelser kan Finanstilsynet identifisere forhold som kan bidra til at viktige preventive og risikoreduserende tiltak etableres, også hos andre foretak.

3.3.2 Ustabile e-handelsløsninger

Ustabilitet i noen bankers og verdipapirforetaks e-handelsløsninger for aksjehandel har ført til at kunder ikke fikk gjort endringer i sine porteføljer. Tidspunktene for teknisk svikt har i noen grad sammenfalt med store markedsendringer og derav økte transaksjonsvolumer. Dette utfordret kapasiteten til systemløsningene hos enkelte foretak. Gjennom oppfølging av slike hendelser har Finanstilsynet overfor enkelte foretak stilt krav om evalueringer og iverksetting av nødvendige tiltak. Finanstilsynet ser alvorlig på slike hendelser og vil følge dette opp i 2018.

3.3.3 Problemer ved innføring av aksjesparekonto (ASK)

Ved innføringen av produktet aksjesparekonto, registrerte Finanstilsynet at enkelte banker og verdipapirforetak den første tiden etter innføringen ikke var i stand til å frigi/overføre kunders aktiva i henhold til ordre. Konsekvensen ble at enkelte kunder for en periode mistet muligheten til å endre i sine porteføljer. Årsaken til nevnte problemer var sviktende standardisering av utvekslingsformater mellom verdipapirforetak og mangelfull kompetanse innen verdipapirområdet i forbindelse med utvikling av enkelte foretaks IKT-løsninger.

3.3.4 Mangler ved utkontrakteringsavtaler

Finanstilsynet har ved gjennomgang av meldinger om utkontraktering av IKT-tjenester fra verdipapirforetak og ved stedlig tilsyn avdekket mangler i foretakenes risikovurderinger og mangler i utkontrakteringsavtalene. Avtalemotpartene besto både av mindre lokale leverandører og store multinasjonale selskaper som leverer skytjenester.

Finanstilsynet har overfor foretakene understreket kravet til styrebehandling av risikovurderinger i forbindelse med utkontrakteringsprosesser. Finanstilsynet understreker at foretakene ved utkontrakteringer skal sørge for å beholde uinnskrenkede rettigheter og muligheter til å drive kontroll med alle elementer hos leverandørene som kan påvirke den utkontrakterte leveransen. Se også punkt 3.8.2.

3.3.5 Manglende retningslinjer for bruk av tredjepart ved sikkerhetstesting

Finanstilsynet har registrert en økning i bruk av eksterne aktører/konsulenter for gjennomføring av sikkerhetstester for å avdekke sårbarheter i foretakets infrastruktur og elektroniske forsvar. Sikkerhetstester er nødvendig. Samtidig kan testing mot foretakets infrastruktur forårsake ustabilitet

eller utilgjengelighet for kritiske systemer, og/eller at sensitiv informasjon kommer på avveie. Styring og kontroll fra foretakets side er nødvendig for å gjennomføre tester på en betryggende måte. Ved tilsyn hos flere verdipapirforetak er det konstatert mangelfull eller fraværende dokumentasjon av retningslinjer, rutiner og planer for gjennomføring av sikkerhetstester. Se også punkt 3.9.4.

3.3.6 For lav kvalitet i testmiljøet og mangelfull testing

Det er viktig at testsystemer ajourholdes for å oppnå en nødvendig kvalitet i testarbeidet. Foretakene må sikre at testsystemer er tilstrekkelig adskilt fra produksjonssystemer for å hindre at testdata feilaktig blir benyttet i produksjonssystemene.

Risikoen for feil ved produksjonssetting av nye systemer eller systemkomponenter er stor dersom produksjonssettingen utføres uten tilstrekkelig kvalitet og kontroll, og testmiljøer ikke er tilstrekkelig ajourholdt.

Finanstilsynet registrerte i 2017 noen alvorlige feilsituasjoner som skyldtes mangler ved foretakenes testsystemer og testrutiner. Feilsituasjonene oppstod blant annet som følge av svakheter i testmiljøet og mangelfull testing i forkant av produksjonssetting. Resultatet var at ny funksjonalitet og nye systemer ble satt i produksjon uten tilstrekkelig kvalitet. Feilsituasjoner oppstod også som følge av at foretakets test- og produksjonssystemer ikke var tilstrekkelig adskilt, slik at testdata feilaktig ble lagt inn i produksjonssystemene.

3.4 Forsikring

Finanstilsynet har gjennom sin tilsynsvirksomhet funnet områder som bør forbedres hos forsikringsforetakene. En nærmere omtale av sentrale funn og vurderinger følger nedenfor.

3.4.1 Rapportering av hendelser

Finanstilsynet har tidligere påpekt underrapportering av IKT-hendelser. Gjennomgangen av innrapporteringen for 2017 viser at flere forsikringsforetak enn tidligere har innrapportert hendelser i 2017, noe som kan tyde på en viss bedring. Sammenlignet med innrapporteringen fra banker, er Finanstilsynets vurdering at det fortsatt synes å være en underrapportering. I tilsynsarbeidet i 2018 vil dette følges opp. Det vises også til punkt 3.7.

3.4.2 Mangelfull risikostyring på IKT-området

Teknologiske endringer påvirker også forsikringsnæringen. Endring i salgskanaler, bruk av ny teknologi og innsamling av data for bruk i prisingen og i utvikling av nye produkter er forhold som påvirker risikobildet. Foretakene må ha et bevisst forhold til dette. Se også punkt 3.4.5.

Gjennom tilsyn har Finanstilsynet observert at noen forsikringsforetak ikke har en tilfredsstillende risikostyring. Finanstilsynet understreker at ansvaret for å etablere tilstrekkelige prosesser for risikostyring og en forsvarlig håndtering av risiko er pålagt styret og daglig leder.

3.4.3 Risiko ved frittstående løsninger for avsetnings- og lønnsomhetsberegninger

Gjennom tilsyn i 2017 har Finanstilsynet vurdert utvikling, forvaltning og bruk av enkelte forsikringsforetaks risikomodeller. Modellene benyttes for vurdering av ulike typer markeds- og bransjerisiko, og for beregning av kapitalkrav. Modellene er viktige styringsverktøy for å følge opp risiko og lønnsomhet.

Resultatene fra modellberegningene inngår både i styrets vurdering av foretakets virksomhet, i rapporteringen til offentlige myndigheter og i informasjon som gis til markedet. Forsvarlig forvaltning og kvalitetssikring av beregningsmodellene er viktig.

Bruk av regneark og utvikling av frittstående systemer for denne type beregninger er vanlig. Finanstilsynet har tidligere påpekt svakheter i kontrollen av endringer i regneark og tilgangskontroll når det benyttes regneark, samt mangelfull integrasjonskontroll av data som legges inn i slike frittstående systemer. Dokumentasjon av prosesser er fraværende eller mangelfull. Nevnte forhold utgjør risiko for feil i beregningsformler og risiko for manuelle feil ved innleggelse av data.

Finanstilsynet observerer at løsningene for modellering ofte bærer preg av å være åpne analyseverktøy med dårlig eller manglende integrasjonskontroll. Eksempel er manglende funksjonalitet for å sikre konsistent parameterbruk fra periode til periode, samt fravær av funksjonalitet som sikrer at utgående verdier i foregående periode utgjør inngående verdier i påfølgende periode. Dette øker risikoen for feil i beregnede resultater.

Avhengigheten av nøkkelkompetanse som forvalter, utvikler og bruker beregningsmodellene er en kritisk faktor, spesielt hos mindre foretak. Forsikringsforetakene løper dermed en risiko for at analyser og rapportering har dårlig kvalitet, eller ikke kan gjennomføres.

3.4.4 Den nye personvernforordningen (GDPR)

Forsikringsforetak forvalter store mengder personsensitiv informasjon og mange av foretakene finner det krevende å tilpasse systemene til den nye personvernforordningen (GDPR). Den nye personvernforordningen stiller blant annet krav om at:

- alle foretak skal ha en forståelig personvernerklæring som forklarer hvordan foretaket behandler den registrertes personopplysninger
- foretaket må vite hvilke persondata det har og hvor disse lagres
- foretaket må kunne dokumentere behovet for de data som lagres, og hvem som bruker hvilke data til hvilket formål

- den registrerte kan be om å bli slettet. Implisitt i dette ligger krav om veldefinerte slette-prosesser
- den registrerte kan kreve å få utlevert sine data på et konsolidert og ryddig dataformat, og den registrerte skal dermed kunne ta med seg sine data til for eksempel et nytt forsikringsforetak

I GDPR ligger det et datakvalitetskrav der foretaket plikter å ha konsistente data. I mange tilfeller blir foretaket nødt til å foreta en manuell datakvalitetsgjennomgang for å kunne avdekke inkonsistente data.

Finanstilsynet har observert at enkelte forsikringsforetak har kommet sent i gang med sine tilpasninger til kravene i GDPR-regelverket.

3.4.5 Teknologisk utvikling

InsurTech er et samlebegrep innen forsikringsområdet for anvendelse av teknologi for blant annet å oppnå konkurransefordeler og økt lønnsomhet.

Den teknologiske utviklingen åpner for store endringer i forsikringsforetakenes tradisjonelle forretningsmodeller. Økt digitalisering av eksisterende forretningsprosesser for effektivisering og kostnadsreduksjon er en trend. Dette omfatter blant annet:

- automatisert rådgivning
- automatisering av skadebehandling
- mer detaljerte data om kunden, der forsikringsforetaket i større grad kan innhente data fra tredjeparter, og koble slike data til foretakets egne kundedata (beskrivelsen av kunden)
- bedre oversikt over verdien på forsikringsobjektet og eventuelt attributter ved forsikringsobjektet som vil kunne påvirke risikoen for at en forsikringshendelse kan inntreffe (beskrivelsen av forsikringsobjektet)
- hvor mye og hvordan forsikringsobjektet benyttes. Parameterne som påvirker risikoen for at en forsikringshendelse vil inntreffe (beskrivelse av risiko)

Ved å benytte nye måleinstrumenter og -metoder kan foretakene samle inn data knyttet til forsikringsrisiko som tidligere ikke var mulig. Selve datainnsamling foregår ved å benytte smarttelefoner, smartklokker og ulike typer sensorer som registrer relevante data. Med en mer presis datafangst vil datagrunnlaget for premiefastsettelsen bli forbedret. Dette vil kunne komme forsikringsforetak og kunde til gode.

Anvendelse av ny teknologi introduserer nye risikoer som foretakene må identifisere og håndtere. Finanstilsynet vil i sitt tilsynsarbeid rette oppmerksomhet mot hvordan foretakene gjennomfører, dokumenterer og kvalitetssikrer løsninger. Spesielt gjelder dette løsninger der bruk av teknologi påvirker premiefastsettelsen direkte.

3.5 Revisjonsselskaper

Finanstilsynet har gjennom tilsyn i 2017 konstatert at revisjonsselskaper har utkontraktert deler av sin virksomhet. Selv om arbeidsoppgaver settes ut til andre, forblir ansvaret i revisjonsselskapet. For å ivareta dette ansvaret på en forsvarlig måte, må det foreligge skriftlige avtaler som sikrer at revisjonsselskapet har tilstrekkelig innsyn i og kontroll med den utkontrakterte virksomheten. Dette gjelder også utkontraktering til andre selskaper i samme nettverk.

Finanstilsynets tilsyn har avdekket mangel på skriftlige avtaler om utkontraktering. Finanstilsynet vurderte nærmere et revisjonsselskap som var tilknyttet en utkontrakteringsavtale med skyleverandør gjennom en avtale inngått av nettverket. Den aktuelle skyleverandøren benytter et standard vedlegg til sine avtaler med kunder innen finanssektoren, som skal ivareta slike kunders behov for innsyn og kontroll. Etter Finanstilsynets tilsyn har skyleverandøren og revisjonsnettverket utarbeidet et vedlegg til den foreliggende utkontrakteringsavtalen som er tilpasset revisjonsvirksomhet og som gir revisjonsselskapene nødvendig innsyn og kontroll.

3.6 Tilsyn med etterlevelse av hvitvaskingsregelverket

Finanstilsynet fører tilsyn med foretakenes systemstøtte for avdekking av hvitvasking og terrorfinansiering. Finanstilsynet har observert mangelfull dokumentasjon av risikovurderingene som ligger til grunn for de elektroniske kunde- og transaksjonskontrollene. Dette kan føre til at foretaket mangler innsikt i om kontrollene er tilstrekkelige for å avdekke risiko for hvitvasking og terrorfinansiering. Finanstilsynet har videre påpekt at rutiner for å beslutte en ny elektronisk kontroll, og for å evaluere og følge opp nye/endrede kontroller, skal være formaliserte og dokumenterte for å sikre at kontrollene har rimelig grad av treffsikkerhet. For screening mot sanksjonslister har Finanstilsynet vurdert om kunder og transaksjoner til enhver tid er screenet mot sist oppdaterte liste. Ved avvik er dette påpekt overfor foretaket.

3.7 Rapporterte hendelser i 2017

Foretakene rapporterer avviks- og endringshåndtering av alvorlige og kritiske IKT-relaterte hendelser til Finanstilsynet i henhold til krav i IKT-forskriften. Rapporteringen omfatter både utilsiktede (operasjonelle feil) og tilsiktede (ondsinnede) hendelser. Finanstilsynet mottar flest rapporter om operasjonelle hendelser. En grunn til dette, er at hendelser som berører en enkelt eller et fåtall kunde(r), eksempelvis der betalingskort er stjålet, som regel ikke faller inn under rapporteringsplikten. Et samlet bilde av nivået på tilsiktede hendelser kommer av den grunn bedre fram gjennom Nordic Financial CERTs rapportering og gjennom tapsstatistikken, se punkt 3.7.1.

3.7.1 Statistikk over hendelser

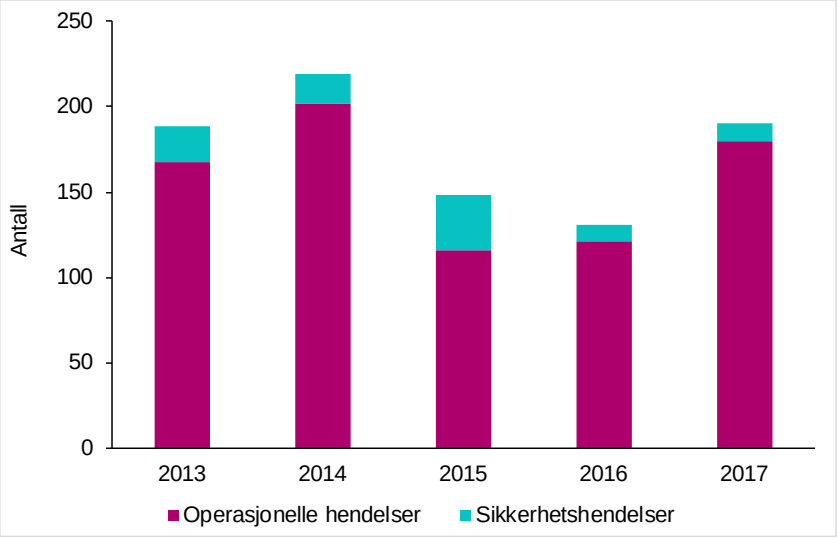
Flere alvorlige hendelser rammet tilgjengeligheten til betalingstjenestene og bankenes kunderettede løsninger i 2017. Etter en nedgang i antall rapporterte hendelser i 2015 og 2016, økte antallet i 2017 med ca. 25 prosent til 190 hendelser. 160 av de rapporterte hendelsene var fra banker. Ved flere av hendelsene i 2017 mistet mer enn 30 prosent av de norske bankkundene tilgang til betalingstjenestene en hel dag. Disse operasjonelle hendelsene rammet bankenes tekniske infrastruktur. Av de 190 rapporterte hendelsene, var det ti rapporter om sikkerhetshendelser (tilsiktede, ondsinnede hendelser), hvorav flere var knyttet til angrep med kryptovirus.

BankID, BankAxept og NICS er en del av felles operasjonell infrastruktur for bankene. For øvrig er bankenes IT-drift spredd på flere driftsmiljøer og/eller -steder. Dersom en hendelse ikke rammer felles operasjonell infrastruktur, er det lite sannsynlig at mer enn ca. 40 prosent av bankkundene samtidig kan rammes av en hendelse. Bankene som opererer i Norge har driftsmiljøer både i Norge, Sverige og Danmark. Flere foretak har også tatt i bruk skytjenester.

De mest alvorlige driftshendelsene i 2017 var knyttet til feil i styringssystemer på stormaskin som førte til at den etablerte dupliseringsløsningen ikke fungerte som forutsatt. En av hendelsene oppstod hos en felles leverandør og rammet av den grunn flere banker, i tillegg til flere forsikringsforetak og verdipapirforetak. Som følge av at løsningstiden ble underestimert og at det var usikkerhet knyttet til om kriseløsningen (Disaster Recovery) ville fungere som antatt, selv om denne var testet, ble kriseløsningen ikke iverksatt. Finanstilsynet vurderer disse forholdene som alvorlige. Se også punkt 3.7.2.

En del driftshendelser kan knyttes til problemer som har oppstått i etterkant av flytting av driften til nye datasentre.

Figur 4 Statistikk over hendelser



Kilde: Finanstilsynet

Tabell 4 Rapporterte hendelser

	Operasjonelle hendelser	Sikkerhetshendelser
2013	168	21
2014	202	17
2015	116	32
2016	121	10
2017	180	10

Kilde: Finanstilsynet

Vipps er den mest benyttede tjenesten for betalinger mellom privatpersoner. Med et stadig utvidet bruksområde både innen privat- og bedriftsmarkedet, er tilgang til tjenesten blitt kritisk da svært mange brukere vil bli berørt ved hendelser. I 2017 ble det rapportert flere hendelser, som blant annet oppstod i forbindelse med flytting av tjenesten til nytt driftsmiljø.

Også i 2017 har det vært flere hendelser med avvik knyttet til tjenesten fra BankID. Hendelsene har rammet banklagret BankID, BankID på mobil og/eller produksjon av engangspassord. BankID har en rekke underleverandører i telesektoren, og hendelser vil ramme ulikt avhengig av den enkelte kundens mobilabonnement. På dager med ekstra høy belastning, slik som når skattemeldingen legges ut, registrerte Finanstilsynet også i 2017 kapasitetsproblemer med BankID. Finanstilsynet vil følge utviklingen og vurdere behov for tiltak.

I 2017 ble driften av viktige betalingssystemer flyttet til globale skyleverandører. Det ble rapportert flere hendelser knyttet til denne driften, som medførte utilgjengelige betalingstjenester. Hendelsene oppstod oftest i forbindelse med endringer og hadde til dels lang re-etableringstid, noe som indikerer at prosessene for endringshåndtering ikke er modne nok. Hendelsene viste også at skyleverandører ikke hadde etablert en prosess for hendelseshåndtering som samsvarte med tjenestens kritikalitet og bankens forventning.

Til tross for stadig modnere driftsrutiner, er menneskelige faktorer fortsatt en avgjørende og medvirkende årsak til at en hendelse oppstår. Flere alvorlige hendelser var forårsaket av at endringshåndtering ikke ble gjennomført i henhold til etablerte rutiner.

Av de 190 rapportert hendelsene som Finanstilsynet mottok i 2017, kom 14 fra verdipapirforetak og infrastrukturforetak, inkludert VPS og Oslo Børs. Det var ulike driftshendelser som medførte at aksjehandel i en periode ikke var tilgjengelig, herunder også tilgangen til oppdatert informasjon. Blant annet skyldtes en alvorlig transaksjonsfeil endringer som ble implementert uten at feilen ble avdekket i testing. Én hendelse oppstod som følge av angrep med kryptovirus[20].

[20] Virusene blir også kalt løsepengevirus (ransomware) hvor angripere krypterer data for deretter å kreve løsepenger for at den som er angrepet skal å få tilgang til sine data.

Fra forsikringsforetakene mottok Finanstilsynet ti rapporter om hendelser. Det ble rapportert om mulig eksponering av kundedata og om ulike driftsproblemer som hindret tilgang til nettbaserte tjenester. Dette inkluderte to rapporter om angrep med kryptovirus.

Det ble rapportert om tre hendelser som rammet bankenes systemer for elektronisk kunde- og transaksjonsovervåkning mot hvitvasking og terrorfinansiering.

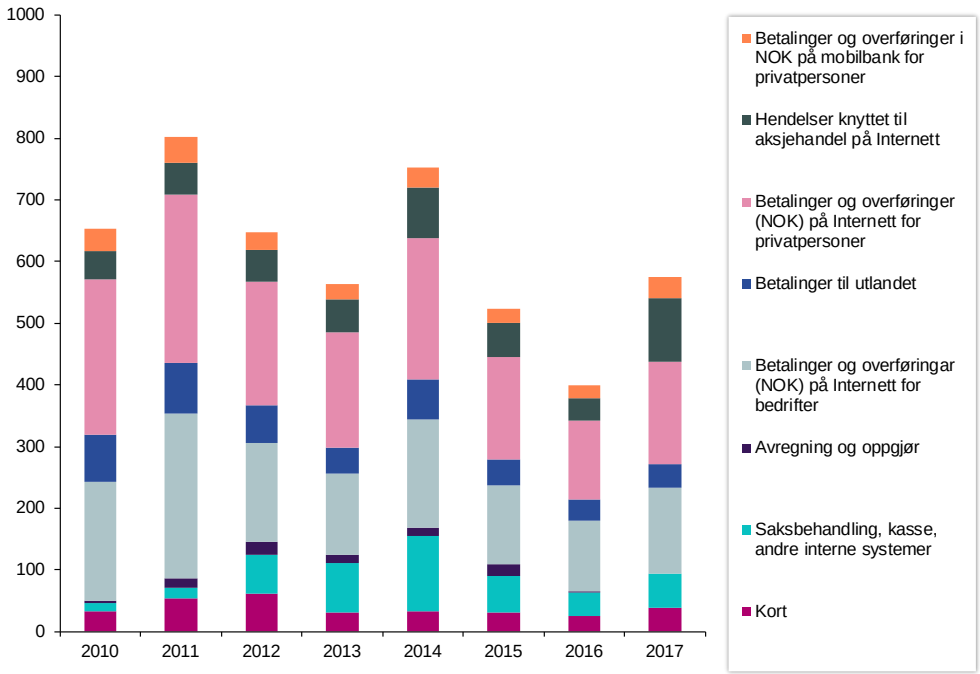
Det kan være krevende å vurdere alvorlighetsgraden av en tilsiktet hendelse, og om den skal rapporteres, men det forventes at melding sendes Finanstilsynet blant annet når:

- angrep/feil har rammet infrastruktur
- angrep/feil har rammet mange kunder
- mange mindre angrep/feil til sammen rammer mange kunder
- nye angrepsformer ("modus operandi")
- internt trusselnivå er hevet til rødt

3.7.2 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 dekker kundens behov (som for eksempel at mobilbanken er utilgjengelig

Figur 5: Hendelser veiet med konsekvens



Vekter: antall berørte brukere, varighet, tidspunkt, erstatningstjenester. Kilde: Finanstilsynet

men at nettbanken er tilgjengelig). Dataene vektes og sammenstilles i tidsserier, slik at utviklingen kan følges over tid. Figur 5 viser at betalingssystemet og kunderettede løsninger var mindre tilgjengelige for kundene i 2017 sammenliknet med de to foregående årene.

Hendelser knyttet til mobilbank dreier seg om at komponenter unike for mobilbanken er nede, for eksempel at mobilnettet er nede, at mobiltjenester (som Vipps) ikke er tilgjengelig, eller at programvarekomponenter knyttet til mobilbanken er nede.

3.7.3 Svikt i kontinuitets- og beredskapsløsningene

Finanstilsynet har fulgt opp alvorlige driftshendelser i 2017, blant annet gjennom å innhente bankenes vurderinger av hvordan kontinuitets- og kriseløsninger (Disaster Recovery) fungerte under hendelsene og om de fungerte som forventet. Det ble her avdekket mangler i dupliseringsløsningene. Videre registrerte Finanstilsynet en usikkerhet hos bankene/driftsleverandørene knyttet til hvor lang tid det vil ta å re-etablere produksjonen med kriseløsningen under en reell krise. Foretakene har iverksatt intensiv testing av kriseløsningene for å sikre at re-etableringen gjennomføres som forutsatt. Finanstilsynet vil følge opp resultatet av tiltakene.

3.8 Utkontraktering

Utkontraktering, eller tjenesteutsetting, er når foretaket velger å benytte en ekstern leverandør framfor selv å drifte, utvikle og forvalte egne IKT-tjenester. IKT-tjenester som understøtter foretakets virksomhet er underlagt IKT-forskriften. Foretakene har et selvstendig ansvar for å påse og kontrollere at foretaket og dets leverandører etterlever forskriftens krav. God forståelse av hva som ligger i dette ansvaret, både hos foretaket og hos leverandøren, er en forutsetning for etterlevelse av regelverket. Se også punkt 4.1.7.

3.8.1 Melding om utkontraktering fra foretakene

Finanstilsynet mottok i 2017 nærmere 50 meldinger om utkontraktering av IKT-virksomhet. De fleste meldingene omhandlet utkontraktering til store globale skyleverandører og endringer i underleverandørforhold.

Hvis driftstjenester av vesentlig betydning for betalingsformidling eller annen finansiell infrastruktur utkontrakteres til utenlandske aktører, kan Finanstilsynet stille særskilte krav til etablering av beredskapsløsninger.

Finanstilsynet konstaterer at foretakene benytter et stadig økende antall underleverandører. Dette skyldes både at løsningene er mer sammensatte ved at flere leverandører bidrar til løsningene, og at leverandøren foretaket utkontrakterer til, igjen utkontrakterer til underleverandører. Dette stiller økte krav til samhandling med underleverandørene og mellom underleverandørene, også ved håndtering av alvorlige hendelser.

3.8.2 Utkontrakteringsavtaler

Bestemmelsene i utkontrakteringsavtaler skal understøtte foretakets ansvar, herunder krav til rapportering og samhandling, samt bestemmelser som sikrer foretakets og myndigheters rett til å gjennomføre revisjon og tilsyn hos leverandøren og dens underleverandører. Videre må foretakene selv sørge for å etablere og dokumentere rutiner som er i tråd med IKT-forskriftens krav.

Avtaler som Finanstilsynet har gjennomgått, viser at det kun er unntaksvis at forskriftens krav ikke er oppfylt. Finanstilsynet ser imidlertid behov for sterkere bevissthet i enkelte foretak for at avtalene best mulig sikrer foretakets etterlevelse av lover og regler, herunder sikrer forsvarlig drift av foretaket og etablere nødvendig styring og kontroll med leveranse av utkontrakterte tjenester. Dette kan for eksempel være håndteringen av kritiske hendelser, akseptanse- og godkjenningsbestemmelser og termineringsbestemmelser.

3.8.2.1 Kritiske hendelser

Finanstilsynets gjennomgang har i noen tilfeller avdekket mangler i avtalebestemmelser som skal gjøres gjeldende ved kritiske hendelser. Konsekvenser en kritisk hendelse kan påføre foretaket og/eller foretakets kunder, er ikke tilstrekkelig vurdert, og krav til løsningstid samsvarer ikke alltid med konsekvensen. Det framgår heller ikke klart av avtalen når beredskapsløsninger skal iverksettes. Forhold som gir foretaket rett til å påberope vesentlig mislighold fra leverandøren, er ikke tydelig definert i avtalen. Dette utgjør en risiko for at foretaket kan påføres stor skade ved gjentakende og alvorlige avvik i leveransen. Finanstilsynet understreker viktigheten av at foretaket selv og leverandøren har etablert forsikringsavtaler med dekning som står i forhold til konsekvens og risiko ved leveransen.

3.8.2.2 Ressurssituasjon hos mindre leverandører

Mindre leverandører kan, som følge av begrensede ressurser og avhengighet av enkeltpersoner, utgjøre en risiko for ustabilitet i kritiske leveranser. Finanstilsynet mener det er viktig at foretakene gjennom avtalen sikrer tilgang til kildekode gjennom deponeringsordning. Videre bør avtalen sikre at programvaren kan overføres til videre forvalting og utvikling av annen leverandør og/eller til eget foretaket dersom leverandøren ikke kan overholde sine forpliktelser i leveranse av kritiske tjenester.

3.8.2.3 Bestemmelser ved terminering

Utkontraktering som ikke gir et forventet resultat vil som oftest resultere i opphør av leveransen og terminering av avtalen. I slike prosesser kan foretaket påføres store kostnader og en krevende driftssituasjon. Flytting av leveransen til en annen leverandør kan være utfordrende og medføre høy risiko for foretaket.

Finanstilsynet erfarer mangelfulle, og i noen tilfeller fraværende, strategier og bestemmelser som skal gjelde ved en terminering. Ved forhandling og inngåelse av avtale er bestemmelser (exit-bestemmelser) som forplikter leverandøren ved overføring av leveransen, særdeles viktig. For å sikre en kontrollert og sikker flytting, bør det fastsettes hvilke forpliktelser hhv. eksisterende leverandør og foretaket selv har ved overføring av leveransen til ny leverandør / foretaket selv.

3.8.3 Utkontraktering til skyen

Finanstilsynet har ikke observert avtaler med skyleverandører inngått i 2017 som ikke er i tråd med regelverket. Selv om foretakene har inkludert vurdering av utkontraktering til skytjenester i sitt rammeverk for risikostyring, er det Finanstilsynets vurdering at risikovurderinger som følger med utkontrakteringsmeldingen, og som er lagt til grunn for foretakenes og styrets beslutninger, bør forbedres.

3.8.4 Skyleverandørers hendelseshåndtering av kritiske tjenester

Finanstilsynet forutsetter at utkontraktering til skyleverandører gjennomføres med tilsvarende styring og kontroll fra foretakenes side som ved utkontraktering til andre leverandører.

Introduksjonen av skytjenester for drift av foretakenes kritiske tjenester medfører også nye utfordringer i samhandlingen når alvorlige driftsavbrudd oppstår. Velfungerende samhandlingsmodeller med tydelige roller og ansvar hos alle parter er en forutsetning for effektiv problemløsning når hendelser inntreffer.

Gjennom en alvorlig hendelse i 2017 ble det avdekket svakheter i hendelseshåndteringen hos en skytjenesteleverandør. Prosessen var ikke tilstrekkelig etablert for å håndtere hendelser som rammet tidskritiske tjenester, herunder rutiner for samhandling med det berørte foretaket og foretakets øvrige leverandører. Finanstilsynet konstaterer at denne erfaringen har bidratt til at foretaket har iverksatt tiltak ovenfor leverandøren.

3.8.5 Utkontrakteringsregelverk

Det europeiske banktilsynet (European Banking Authority – EBA) har utarbeidet anbefalinger for utkontraktering til skytjenesteleverandører[21] som vil gjelde fra 1. juli 2018. EBAs retningslinjer for utkontraktering er under revisjon og vil erstatte den nevnte anbefalingen etter revisjonen. Retningslinjene vil også omfatte utkontraktering av IKT og vil bli utvidet til å omfatte utkontraktering til skytjenesteleverandører.

3.9 IKT- og informasjonssikkerhet (IKT-sikkerhet)

IKT- og informasjonssikkerhet får stadig større oppmerksomhet. Det gjelder særlig cyber-sikkerhet, siden risikoen vurderes som høy og økende, blant annet som følge av internasjonale angrep og hendelser mot både nasjoner og store foretak innen finansnæringen, for eksempel Equifax[22].

[21] https://www.eba.europa.eu/-/eba-issues-guidance-for-the-use-of-cloud-service-providers-by-financial-institutions
[22] https://www.theguardian.com/technology/2017/oct/11/personal-details-of-almost-700000-britons-hacked-in-cyber-attack

3.9.1 Organisering av arbeidet med IKT-sikkerhet

Foretakets styre skal sørge for en forsvarlig organisering av virksomheten, og er ansvarlig for å påse at foretakets ledelse organiserer og utøver sikkerhetsarbeidet i tråd med krav til forsvarlig organisering og drift, gjeldende regelverk og god praksis. Dette forutsetter at både styre og ledelse har nødvendig kompetanse, og at foretakets sikkerhetsarbeid gis nødvendig oppmerksomhet og prioritet.

Det skal settes mål for foretakets organisering og arbeid med IKT-sikkerhet. Roller og ansvar i organisasjonen må defineres tydelig. Ansvaret for henholdsvis styring av IKT-sikkerheten, kontroll med IKT-sikkerheten og det operative IKT-sikkerhetsarbeid skal være klart adskilt.

Finanstilsynet anser det som viktig at forretningssiden er involvert i og har eierskap til IKT-sikkerheten innen eget forretningsområde.

3.9.2 Observasjoner av digital kriminalitet

Digital kriminalitet rettet mot foretakene 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.

Fra oppfølgingsmøter med foretak om hendelsesrapporteringen, er Finanstilsynet kjent med at foretakene har observert en vesentlig økning i uønsket aktivitet. En liten andel av den uønskede aktiviteten resulterer i sikkerhetshendelser som rapporteres Finanstilsynet, jf. punkt 3.7.1.

Informasjonssikkerhet: omfatter sikring av informasjon, uavhengig av om den er lagret digitalt eller ikke. Informasjonssikkerhet er å sikre at informasjonen ikke blir kjent for uvedkommende (konfidensialitet), ikke blir endret utilsiktet eller av uvedkommende (integritet) og er tilgjengelig ved behov (tilgjengelighet)

IKT-sikkerhet: omfatter sikring av informasjons- og kommunikasjonsteknologi (IKT), dvs. maskinvare og programvare.

I rapporten brukes IKT-sikkerhet som fellesbetegnelse for informasjonssikkerhet og sikkerhet i IKT-systemer.

3.9.2.1 Phishing og sosial manipulering

Fra oppfølgingsmøter om hendelsesrapporteringen og intervjuer med foretakene er Finanstilsynet kjent med at foretakene observerer en stadig økning i "phishing" og sosial manipulering av kunder hvor hensikten til angriperne både er økonomisk svindel og å tilegne seg informasjon. Dette er metoder som anses som enklere for å trenge inn i et foretaks IT-systemer enn gjennom krevende tekniske angrep. Metodene utvikles og blir mer og mer utspekulerte og avanserte. Informasjon om personer fra sosiale

medier, e-postadresser, brukernavn og passord, kjøpes og selges mellom kriminelle hvoretter informasjonen benyttes for målrettede angrep.

Kriminelle som lykkes med å få tilgang til e-postservere vil kunne overvåke trafikken og gjennom dette tilegne seg kunnskap om mønstre og atferd. Videre kan kriminelle tre inn i en pågående e-postutveksling og endre innholdet, for eksempel kontonummer og -informasjon, eller tilegne seg informasjon som kan benyttes til annen kriminell sammenheng.

Finanstilsynet er kjent med at CEO-svindel og tilsvarende svindel fortsatt er en stor utfordring, og at den har blitt mer sofistikert. Samtidig ser Finanstilsynet en bedring i foretakenes forebygging av denne type hendelser gjennom opplæring og bevisstgjøring av de ansatte.

3.9.2.2 Tekniske tiltak for å avdekke uautorisert e-post

Utfordringene med falske e-poster er som nevnt fortsatt stor. For mottaker av en falsk e-post kan det være vanskelig, om ikke umulig, å avdekke at e-posten er falsk. Phishing-e-poster blokkeres gjennom spesifikke tiltak.

Domain-based Message Authentication, Reporting & Conformance (DMARC)[23] er en metode for å beskytte foretakets egne domener mot falsk e-post, blokkere falsk e-post fra domener fra utsiden og rapportere tilfeller der falsk e-post avdekkes. Gjennom denne metoden utarbeides det en beskrivelse (policy) med IP-adresser og signeringsinformasjon som det skal kontrolleres mot i oversendelsen. Denne informasjonen lagres i det sentrale domenesystemet på Internett, Domain Name System (DNS), og foretak kan på den måten kontrollere innkommende e-post som et ledd i sin vurdering av avsender av e-posten.

3.9.2.3 Alvorlige globale cyber-angrep i 2017

I 2017 inntraff cyber-angrep som rammet på tvers av land og sektorer, hhv. skadevaren WannaCry i mai og NotPetya i juni. Begge hadde elementer av kryptovirus. Angrepene forårsaket stor skade der viruset klarte å komme på innsiden av bedrifters nettverk, og illustrerte hvilken kraft det kan være i massive cyber-angrep. Svakheter i forsvarsverket, som usikrede innganger til nettverket og mangelfull sonedeling av nettverket, ble utnyttet.

Finanssektoren i Norge ble ikke rammet, noe som trolig skyldes at finanssektoren er bedre beskyttet og har lengre erfaring i å sikre seg mot angrep.

3.9.3 SWIFTs sikkerhetsprogram

SWIFT er et internasjonalt kommunikasjonsnettverk for blant annet overføring av grensekryssende betalinger og større betalinger innenlands. De største bankene i Norge, Norges Bank og VPS bruker SWIFT og er SWIFT-medlemmer.

[23] Se https://dmarc.org

Sikkerhetshendelsene i 2016 som rammet banker og sentralbanker, fikk stor oppmerksomhet. I følge SWIFT var hendelsene knyttet til berørte bankers interne systemer for gjennomføring av betalinger og ikke til SWIFTs løsninger. Som en følge av hendelsene, etablerte SWIFT i 2017, sikkerhetsprogrammet Swift Customer Security Program[24] for sine kunder.

Hvert SWIFT-medlem har ansvar for sikkerheten i systemet, men SWIFT har forpliktet seg til å hjelpe kundene med ekspertise og kompetanse for å bekjempe cyber-angrep. Sikkerhetsprogrammet består av 16 obligatoriske sikkerhetskontroller som alle SWIFT-brukere, uansett om de er tilknyttet SWIFT direkte eller indirekte, må implementere. SWIFT-brukerne må levere en egenerklæring hver tolvte måned om at de etterlever kravene. Finanstilsynet vil følge med på foretakenes arbeid med egenerklæringen.

3.9.4 Sikkerhetstesting ved bruk av tredjeparts aktører

Sikkerhetstesting er et viktig virkemiddel for å verifisere robusthet og for å avdekke sårbarheter i foretakenes tekniske infrastruktur og organisasjon. Gjennomføring av tester krever nøye planlegging og skal utføres etter definerte krav i foretakets sikkerhetsrammeverk. Foretakets styre og ledelse har et overordnet ansvar både for at sikkerhetsrammeverk etableres etter god praksis og at sikkerhetstester gjennomføres i henhold til dette.

Gjennomføring av sikkerhetstester vil eksponere teknisk infrastruktur for ustabilitet eller utilgjengelighet av kritiske systemer, og denne type tester utgjør også en risiko for at sensitiv informasjon kommer på avveie om testene ikke gjennomføres med nødvendig styring og kontroll. Risikovurderinger bør foretas for å identifisere forhold som kan utløse uønskede hendelser som følge av sikkerhetstester.

Finanstilsynet registrerer at sikkerhetstester ofte begrenses til penetrasjonstester av foretakets tekniske infrastruktur, herunder test av brannmurer. Metoder som sosial manipulering, DDoS-angrep og andre alternative angrepsformer benyttes i mindre grad. Bruk av tredjepartsaktører til overvåking, test og forbedring av sikkerhetsnivået i foretakenes tekniske infrastruktur, er økende, blant annet som følge av at foretakene selv ikke har nødvendig kompetanse. Det er viktig å benytte aktører som er kvalifisert for slike oppgaver, spesielt når aktører som engasjeres, får tilgang til detaljer om foretakets tekniske infrastruktur, informasjon og organisering.

Nasjonal sikkerhetsmyndighet (NSM) har opprettet et pilotprosjekt for kvalitetssikring av aktører som leverer tjenester innen sikkerhetsområdet. En oversikt over aktører som er kvalitetssikret framgår av NSMs nettsted. Det er viktig at foretakene har grundige prosesser ved valg av leverandører av sikkerhetstjenester.

[24] https://www.swift.com/myswift/customer-security-programme-csp

3.9.5 Sårbarhetsrapportering

Finanstilsynet er kjent med at enkelte foretak, som et av flere tiltak knyttet til å avhjelpe kompetanseutfordringen innenfor IKT-sikkerhet, belønner personer som oppdager sikkerhetshull og sårbarheter i foretakets forsvarsverk. En forutsetning er at oppdageren gir tilbake nødvendig informasjon om sårbarheten, og at oppdageren forplikter konfidensialitet om avdekkede svakheter til dette er reparert.

Tiltaket kan redusere svakheter og bidra til bedret IKT-sikkerhet for foretak. Erfaringsgrunnlaget er foreløpig begrenset. Finanstilsynet vil følge med på om en slik praksis medfører negative konsekvenser for foretaket, for eksempel redusert driftsstabilitet på grunn av økt antall digitale angrep.

3.9.6 Brukeridentitet og passord på avveie

Bruk av digitale tjenester, både privat og i arbeidssammenheng, blant annet på smarttelefon, nettbrett og TV har blitt en viktig del av den digitale hverdagen. Det er mange leverandører av disse tjenestene, og bruk av tjenestene krever i økende grad autentisering av brukere med krav om e-post og passord.

I de senere år er det registrert flere hendelser hvor hackere har lykkes med å hente ut registre med e-postadresser og passord som følge av sårbarheter i aktørers infrastruktur. Denne informasjon tilbys nå gjennom digitale markedsplasser som kriminelle igjen benytter i sin aktivitet. Ansatte som benytter samme påloggingsinformasjon for flere digitale tjenester, medfører økt risiko for at informasjonen kan komme kriminelle i hende. Kriminelle vil enklere kunne identifisere ansattes roller og ansvar, for eksempel gjennom sosiale medier. Identifiserte ansatte løper en høy risiko for sosial manipulering og trusler, og at kriminelle kan lykkes med å få tilgang til foretakets systemer. Risikoen for at ansatte kan tvinges til å gjennomføre uautoriserte handlinger, øker også.

Bevisstgjøring av foretakets ansatte bør være en kontinuerlig prosess. Bruk av to-faktor-autentifisering samt etablering av en normal og god praksis for sikkerhetsoppsett i foretaket, herunder tvungent passordbytte og krav til utforming av passord, er viktige risikoreduserende tiltak. Det finnes tjenester som kan angi om en e-postadresse er kompromittert[25]. For ansatte som kan være utsatt for sosial manipulering, vil det være nyttig å foreta en undersøkelse.

3.9.7 Kommende sikkerhetsregelverk

EUs direktiv om tiltak for et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer (NIS-direktivet) vil bli innført i norsk rett. Direktivet stiller blant annet krav til at tilbydere av samfunnsviktige tjenester skal gjennomføre risikovurderinger av nettverk og informasjonssystemer, iverksette nødvendige tiltak for å forebygge, avdekke og redusere konsekvensene av hendelser og varsle om hendelser. Det framgår av direktivet at der det finnes regelverk som minimum stiller krav tilsvarende direktivets krav, skal annen lov benyttes. Finanstilsynets vurdering er at dagens regelverk for finanssektoren i hovedsak dekker kravene i direktivet.

[25] https://haveibeenpwned.com/

Ny lov om nasjonal sikkerhet (sikkerhetsloven) trer i kraft 1. januar 2019. Høsten 2017 ble det etablert et prosjekt for å utarbeide forslag til forskriftsbestemmelser til loven. Forskriftsforslaget vil bli sendt på høring i løpet av 2018, og det tas sikte på at bestemmelsene skal tre i kraft samtidig med loven.

Det pågår også et arbeid i regi av IKT-sikkerhetsutvalget[26], som er et tverssektorielt norsk utvalg, med mandat å vurdere om dagens regulering og organisering av IKT-sikkerhet i Norge er hensiktsmessig.

3.10 Kompetansestyring ved omstilling

"Run the Bank vs Change the Bank"[27] benyttes som begrep for å illustrere utfordringene forbundet med å balansere ressursdelingen mellom sikker og stabil drift opp mot å omstille foretaket til for eksempel nye produkter/tjenester og anvendelse av nye systemer og ny teknologi. I dette ligger også vurderinger av hvilken kompetanse foretaket må ha på kort og lang sikt, slik at det i tillegg til å håndtere de planlagte oppgavene, også er i stand til å håndtere uforutsette oppgaver.

Det er Finanstilsynets inntrykk at foretakene i en nedbemanningssituasjon lar hensynet til framtidige behov veie tyngst. Finanstilsynet er opptatt av at foretakene også vektlegger og opprettholder kompetanse for å ivareta den daglige driften og at foretakene må legge større vekt på evnen til å opprettholde stabil og sikker drift av eksisterende tjenester.

Finanstilsynet har registrert at foretak gjennom utkontrakteringsprosesser har nedbemannet for siden å bygge opp igjen kompetansen som gikk tapt. Dette kan indikere at kompetansebehovet for den daglige operative driften ikke ble tilstrekkelig vurdert. Det er også indikasjoner på at utkontrakteringspart ikke har vært i stand til å utføre alle forventede oppgaver.

3.11 Fellestiltak innen finansnæringen

På en rekke områder samarbeides det på tvers i finanssektoren. Særlig gjelder dette innen områdene sikkerhet og felles infrastruktur, tjenester og standarder.

En arbeidsgruppe med representanter fra finansnæringen og Norges Bank leverte i april 2017, gjennom det såkalte BRO-prosjektet, en rapport om etablering av en ny felles infrastruktur for betalinger med raskere oppgjør[28], inkludert tilpasninger i Norges Banks oppgjørssystem. Den foreslåtte infrastrukturen skal legge til rette for en kontinuerlig prosessering av realtidsbetalinger, som benevnes BRO-betal-

[26] https://www.regjeringen.no/no/dep/jd/org/styre-rad-og-utval/tidsbegrensede-styrer-rad-og-utvalg/IKT-sikkerhetsutvalget/id2570775/
[27] "Run the Bank" beskriver aktiviteter som skal gi sikker og stabil drift. "Change the Bank" beskriver det å skulle tilpasse foretaket til nye produkter/tjenester og å omstille foretaket ved anvendelse av nye systemer og ny teknologi.
[28] https://www.bits.no/wp-content/uploads/2017/04/Sluttrapport-BRO.pdf

inger. Det er foreslått at alle banker må forplikte seg til å integrere sine løsninger for betalingstjenester mot den nye felles infrastrukturen og derigjennom tilby sine kunder realtidsbetalinger, og at dette gjennomføres i tråd med tidsplanen fastsatt av etableringsprosjektet for BRO-løsningen. Bankenes planlegger å starte gjennomføringen i 2018 med mål om en etablert løsning i løpet av 2019.

De største nordiske bankene[29] har informert om at muligheten for en nordisk betalingsinfrastruktur med felles produkter er under utredning. Målet er å etablere løsninger for nasjonale og grensekryssende betalinger i flere valutaer (SEK, DKK, NOK og EUR) i Norden for å lette betalinger på tvers av landegrenser og fremme handel mellom de nordiske landene. Det framgår av informasjon fra initiativtakerne at målet sammenfaller med eksisterende nasjonale infrastrukturprosjekter i Sverige og Norge, jf. BRO-prosjektet. Framfor å etablere landspesifikke løsninger, er målet å skape løsninger som dekker behovene både innenfor og på tvers av de nordiske landene.

Offentlig sektor og finansnæringen samarbeider om digitalisering og effektivisering av viktige prosesser i samfunnet gjennom DSPO[30]. Det omfatter samarbeid med både med Skatteetaten, NAV, Brønnøysundregistrene og politiet innenfor blant annet områdene:

- **samtykkebasert lånesøknad** – innhenting av informasjon fra offentlig sektor
- **kontrollinformasjon** – utveksling av relevant kontrollinformasjon mellom bank og skatteetaten knyttet til etterforskning[31]
- **konkursbehandling** – umiddelbart digital melding til bank for sperring av kontoer
- **selskapsetablering** – forenkle prosessen ved selskapsetablering
- **syke- og uføreopplysninger fra NAV** – forenkle og effektivisere prosessen mellom forsikringsforetak og NAV

Det er også betydelig samhandling internt i finansnæringen i regi av Bits gjennom arbeidet i PSD 2- og XS2A-prosjektet[32], etablert for blant annet å vurdere mulige felles løsninger og etablering av felles standarder i tråd med PSD 2.

De nordiske bankene etablerte i 2017 Nordic Financial CERT, som bygger på og erstatter den norske finansnæringens FinansCert. Formålet med Nordic Finans CERT er å bidra til bedre sikkerhet for foretakene og deres kunder gjennom deling av informasjon, kompetanse og erfaringer på cyber-sikkerhetsområdet.

[29] http://www.hegnar.no/Nyheter/Naeringsliv/2018/02/Nordiske-banker-utreder-muligheten-for-felles-betalingsinfrastruktur
[30] Digitaliseringssamarbeidet mellom offentlig og privat sektor, https://www.bits.no/project/dsop/
[31] https://www.bits.no/project/kontrollinformasjon/
[32] https://www.bits.no/project/psd2-xs2a/

3.12 Utviklingstrekk innenfor finansiell teknologi

Utviklingen innenfor finansiell teknologi er knyttet til både nye og eksisterende foretaks tjenester, men teknologien tas også i bruk for foretakets oppfølging av etterlevelse av regulatorisk regelverk.

3.12.1 FinTech

Finansnæringen er i konstant endring, og flere nye aktører vil etablere seg med tjenester i finanssektoren. Selv om finansnæringen har ligget langt framme i bruken av IKT, ser en nå stadig oppblomstring av nye initiativ som utfordrer de etablerte foretakene.

FinTech omfatter teknologisk utvikling innen alle deler av finansnæringen, men ofte brukes mer tjenesteorienterte begreper som BankTech, PayTech og InsureTech mv. i omtalen av bruk av ny teknologi innenfor de ulike bransjene.

Den teknologiske innovasjonen endrer næringen gjennom nye løsninger, økt konkurranse og nye aktører i verdikjedene. Progresjonen i utviklingen innen kunstig intelligens, maskinlæring, robotisering, økt bruk av stordata samt ny teknologi som blokkjede og bruk av skytjenester, bidrar til en digitaliseringsbølge som påvirker og utfordrer foretakenes forretningsmodeller.

Finanstilsynet følger utviklingen, og ser blant annet på hvordan foretakene og nye aktører innretter seg etter lover og regler. Finanstilsynet legger vekt på at hensynet til finansiell stabilitet, trygge tjenester og god kundebeskyttelse blir ivaretatt. For å oppnå dette, bør lik risiko behandles likt, uavhengig av forretningsmodell.

Finanstilsynet har etablert en informasjonsside[33] for FinTech-foretak. Her kan foretakene finne relevant informasjon og kontaktinformasjon for å kunne henvende seg til Finanstilsynet for veiledning, både i forkant av og underveis i prosessen med å etablere forretningsmodell og utarbeide konsesjonssøknad.

Det europeiske banktilsynet (European Banking Authority) har utarbeidet et veikart (The EBA's FinTech Roadmap[34]) som, basert på en kartlegging av FinTech innenfor EU/EØS, redegjør for det arbeidet som er iverksatt og som skal gjennomføres i 2018/2019. I tillegg har EU-kommisjonen utarbeidet en handlingsplan for FinTech.[35]

Ved innføring av ny teknologi og alternativ anvendelse av eksisterende teknologi forutsetter Finanstilsynet at det gjennomføres risikovurderinger som identifiserer relevant risiko. Relevant risiko i denne sammenheng er fare for misbruk/svik, fare for feilrapportering og ansvaret som foretaket har tatt på seg ved at de nye teknologiske løsningene tas i bruk.

[33] https://www.finanstilsynet.no/tema/fintech/
[34] http://www.eba.europa.eu/documents/10180/1919160/EBA+FinTech+Roadmap.pdf
[35] https://ec.europa.eu/info/publications/180308-action-plan-fintech_en

3.12.2 Kunstig intelligens (AI) og maskinlæring

Teknologien innen kunstig intelligens har nådd et nivå som medfører at foretakene de siste årene har rettet oppmerksomhet mot mulighetene som ligger i avanserte former for blant annet databehandling og systemenes selvlæring.

Finanstilsynet understreker nødvendigheten av å etablere kontroller som skal sikre at systemer som er basert på kunstig intelligens, ikke agerer utover de forventninger og krav som settes. Dersom det ikke gjennomføres tilstrekkelig kvalitetssikring ved utvikling, test og kontroll av resultater etter produksjonssetting av selvlærende systemer, kan bruk av teknologien i foretakenes forretningsprosesser og støttefunksjoner resultere i alvorlige hendelser.

Kunstig intelligens vil kunne misbrukes av kriminelle for å gjennomføre avanserte angrep mot den finansielle sektoren. Den økte trusselen dette medfører, krever at foretakene sammen arbeider for å etablere ressurser og kompetanse for å sikre en løpende oppgradering av forsvarsverket.

3.12.3 Robotisering

Robotisering bidrar til å automatisere foretakenes manuelle oppgaver som i dag utføres av blant annet foretakets kunde- og saksbehandlere. Avanserte former for robotisering benytter teknologi som kunstig intelligens og maskinlæring, og i kundegrensesnittet benyttes også "chatbot[36]". Dette er en naturlig utvikling som i økende grad vil medføre at interaksjon mellom foretakene og kundene foregår uten menneskelig kontakt fra foretaket sin side.

Finanstilsynet vil følge denne utviklingen og gjennom tilsyn vurdere hvordan foretakene styrer og kontrollerer bruken av teknologien.

3.12.4 Blokkjede

Blokkjede-teknologien (Blockchain) hevdes av mange å kunne revolusjonere finansnæringen i årene framover. Finanstilsynet observerer høy aktivitet både i Norge og internasjonalt for å utrede potensialet som ligger i denne teknologien. DNB har blant inngått i et samarbeid mellom flere storbanker for bruk av teknologien innen Trade Finance[37]. Bank of England vil se på bruken av teknologien ved fornying av oppgjørssystemet[38].

Et generelt kjennetegn ved slik teknologisk endring er at det gjerne tar lengre tid enn forventet før den tas i bruk, og at konsekvensene ofte blir større enn forutsett. Fortsatt er det etablert få løsninger innen finansnæringen basert på teknologien.

[36] Dataprogram som håndterer kundehenvendelser gjennom talekommandoer eller tekst. Avanserte chatbots er basert på bruk av kunstig intelligens.
[37] https://e24.no/boers-og-finans/dnb/dnb-inngaar-globalt-blokkjedesamarbeid-med-flere-storbanker/24267065
[38] https://www.bankofengland.co.uk/-/media/boe/files/payments/rtgs-renewal-proof-of-concept.pdf?la=en&hash=2367D4475E64266B1C1F0399851C19DA05749543

Finanstilsynet mener det er viktig at foretakenes styre og ledelse er forberedt på hvordan ny teknologi, som blokkjede, kan påvirke finansnæringen, herunder hvordan og innen hvilke forretningsområder ny teknologi kan komme til anvendelse. Bruk av teknologien vil kunne medføre behov for endringer i foretakets organisering og arbeidsmetoder.

Teknologien kan medføre betydelige endringer for foretak og for samhandling mellom foretak. Finanstilsynet vil følge med på den videre utviklingen.

3.12.5 Initial Coin Offerings (ICO)

ICO er kapitalinnhenting[39] ved utstedelse av egen virtuell valuta. Formålet er rask og rimelig innhenting av kapital til oppstartselskaper og til selskaper med nye ideer og behov for finansiering. ICO har også vært benyttet av etablerte selskaper for kapitalinnhenting. Investorer betaler hovedsakelig med virtuell valuta som f.eks. Etherum eller Bitcoin og tildeles "tokens" som vil være oppstartselskapets egen virtuelle valuta. Etter en gjennomført ICO, etablerer utsteder en handelsplass (børs) der man omsetter/veksler foretakets token til Bitcoin eller Etherum.

Risiko for investorer

ICO-er faller i dag utenfor eksisterende regelverk på verdipapirområdet, med mindre investor gis medbestemmelsesrett i selskapet, rettigheter til overskuddsdeling mv. Dersom en ICO faller utenfor regelverket, kan investorer ikke forvente investorbeskyttelse.

Ved tegning av en ICO utstedes et "Whitepaper" som beskriver prosjektet eller selskapet som kan sammenlignes med prospekter ved IPO[40]. Det foreligger ingen regulering eller kvalitetskontroll av innholdet i et "Whitepaper".

Finanstilsynet er kjent med at det internasjonalt har vært etablert falske ICO-er, kun med det formål å svindle investorer. Internasjonalt har det også skjedd at ICO-er har "forsvunnet", blant annet der aktørene har sett at forretningsidéen ikke var så levedyktig som antatt, og aktørene bak ikke overholdt sine forpliktelser overfor investorene. Det har også forekommet at svindlere har etablert falske kopier av ICO-usteders tegningssider, slik at innbetalinger er blitt gjort til svindlerens konto.

Investorer løper også en risiko for at en ICO lar midlene gå til andre formål enn tiltenkt, for eksempel dersom beløpet som innbetales ved ICO-en blir høyere enn verdien på produktet eller verdien på selskapet som ICO-en skulle finansiere. Det er også en risiko for at investorer kan bli involvert i hvitvasking av penger.

[39] https://www.finanstilsynet.no/nyhetsarkiv/rundskriv/2017/lanebasert-folkefinansiering-crowdfunding--en-veiledning-om-laneformidling/
[40] IPO (Initial Public Offering) – det første offentlige tilbudet på aksjer i et selskap.

Finanstilsynet har publisert en advarsel mot deltakelse i ICO-er[41]. Advarselen bygger på de europeiske finanstilsynsmyndighetenes advarsel. En stor andel ICO-er er ment for å finansiere realisering av en idé eller utvikling av et produkt som ikke eksisterer i dag. Dette vil derfor ofte være ensbetydende med høyrisikoinvesteringer.

Utviklingen i Europa

EU-kommisjonen har i sin FinTech-plan[42] opplyst at de ønsker å utvikle og harmonisere regelverket for bruk av ICO-er som et bidrag til effektivisering av kapitalinnhenting på tvers av landegrenser. Dette vil bli gjort i samarbeid med de europeiske finanstilsynsmyndighetene, og risikoer, muligheter og hensiktsmessigheten ved eksisterende regelverk bli vurdert.

3.12.6 Virtuelle valutaer

Prisutviklingen på virtuell valuta har siden sommeren 2017 vært svært volatil, og de europeiske finanstilsynsmyndighetene (EBA, EIOPA og ESMA) er bekymret for at et økende antall forbrukere kjøper virtuell valuta uvitende om risikoen dette innebærer.

Finanstilsynet har publisert en advarsel mot å kjøpe og eie kryptovaluta[43]. Advarselen bygger på ESAenes advarsel. Virtuelle valutaer er svært risikable og spekulative produkter, og investeringer innebærer stor risiko for tap. Det samme gjelder finansielle instrumenter som gir eksponering mot virtuelle valutaer. Virtuelle valutaer er ikke regulert, men blir omsatt på uregulerte markedsplasser med manglende pristransparens. Virtuelle valutaer vurderes som uegnet for kort- og langsiktig sparing for de fleste forbrukere.

3.13 Utvikling av teknologiske løsninger for etterlevelse av nytt regelverk

Finansforetakene bruker betydelige ressurser på å etterleve gjeldende regelverk og holde seg oppdatert på og implementere nye krav. Manuelle prosesser ved utarbeidelse av interne rapporter og rapporter til myndigheter er tidkrevende. Finanstilsynet registrerer at det er en økt aktivitet for å utvikle teknologiske løsninger som skal støtte både foretak og myndigheter i deres arbeide.

RegTech (Regulatory Technology) er en samlebetegnelse for teknologibaserte løsninger som skal støtte foretakene med å identifisere og oppfylle eksisterende og nye nasjonale og internasjonale regulatoriske krav, herunder reguleringer innen EU/EØS. Risiko for menneskelig feil kan reduseres, og

[41] https://www.finanstilsynet.no/markedsadvarsler/2017/initial-coin-offerings-icoer---advarsel-til-investorer-og-foretak/
[42] http://europa.eu/rapid/press-release_IP-18-1403_da.htm?utm_campaign=unspecified&utm_content=unspecified&utm_medium=email&utm_source=apsis-anp-3
[43] https://www.finanstilsynet.no/markedsadvarsler/2018/finanstilsynet-advarer-forbrukere-om-kryptovaluta/

intern og ekstern rapportering effektiviseres. RegTech-løsninger anvendes blant annet for å avdekke hvitvasking og terrorfinansiering.

Finanstilsynet ser positivt på at foretakene tar i bruk slik teknologi som bidrag til å sikre og følge opp etterlevelse av lover og regler, samt som et risikoreduserende tiltak. Samtidig stiller dette krav til foretakenes kunnskap om og styring og kontroll med løsningene.

4 Aktørenes vurdering av risikofaktorer

Dette kapitlet tar opp de mest framtredende truslene foretakene selv trekker fram i intervjuer og i besvarelser av spørreskjema fra Finanstilsynet.

4.1 Intervjuer

4.1.1 Endringer

Foretakene gir uttrykk for at det er mange og hyppige endringer i systemene og stor konkurranse om tjenester og funksjoner. Det er usikkerhet knyttet til foretakenes etterlevelse av nye regulatoriske krav. Spesielt gjelder dette PSD 2 og EUs nye personvernforordning hvor foretakene mener at de må gjennomføre betydelige endringer i rutiner og prosesser.

4.1.2 Dataangrep

Foretakene er bekymret for at dataangrep blir mer avanserte, og viser til at metoder og verktøy for å utøve angrep har blitt lettere tilgjengelig. NotPetya-angrepet i 2017 nevnes som et eksempel. Angriperne forsøker ikke nødvendigvis å bryte seg direkte gjennom foretakets forsvarsverk, men "smugler" inn skadevare i programvare som foretaket benytter.

Foretakene uttaler at det brukes store ressurser i arbeidet med å sikre egen virksomhet. Tiltak som sikkerhetsoppgraderinger (patching), DMARC (beskyttelse av e-post) og Response Policy Zone (filtrering av web-trafikk) følges tett opp, og må stadig justeres og tilpasses for at tiltakene skal virke som forutsatt. I motsatt fall vil tiltakene kunne gå ut over driftsstabiliteten og føre til mangler i leveransen. Nedetid, lange svartider og feil i tjenesten kan bli resultatet.

4.1.3 Kompetanse og kapasitet

En rekke foretak melder om utfordringer knyttet til kompetanse og kapasitet innenfor IKT-området. Utfordringene er størst innenfor områdene utvikling og sikkerhet, spesielt innenfor området kryptering. Når det gjelder drift av servere og nettverk, er utfordringene ikke like store.

4.1.4 Tilgangsstyring

Tilgangsstyring til data og systemer innebærer å kontrollere:

- tilganger som ansatte har
- tilganger som applikasjoner og programvare har
- tilganger som eksterne brukere har
- tilganger som angripere kan tilegne seg
- tilganger som leverandører og underleverandører har og eventuelt uberettiget kan tilegne seg
- forsøk på å eskalere privilegier
- uautorisert kartlegging av svakheter ("lateral movements")

En rekke foretak anser tilgangsstyring som en betydelig utfordring og enkelte foretak avdekket i 2017 svakheter i sin tilgangsstyring. God tilgangsstyring forutsetter kontroll innenfor en rekke områder og fagfelt, og tilgangskontrollen er ikke sterkere enn det svakeste leddet. Store investeringer i god kontroll er bortkastet hvis det er én svakhet som angriperen kan utnytte.

En slik svakhet kan være at kontinuitetsløsninger ikke er sikkerhetsoppdatert, slik at usikre utgaver av programvare settes i produksjon etter overgang til kontinuitetsløsningen, eller det kan være installert programvare som foretaket ikke benytter eller benytter svært sjelden, og som ikke blir sikkerhetsoppdatert. Angriperen kan utnytte en slik sårbarhet som brohode for å trenge videre inn i foretaket.

4.1.5 Datalekkasje

En følge av utfordringen knyttet til tilgangskontroller, er at data lekker ut av foretaket. Foretakene viste til tilfeller der programmeringsfeil i nettbanken førte til at informasjon kom uvedkommende i hende og til tilfeller der det ble sendt konto- og kundeinformasjon i klartekst i e-post, til tross for at e-post er en usikker forsendelsesform. Også tilfeller med feil knyttet til bruk av den såkalte "mail-merge"-funksjonen, som medførte at e-post ble sendt til feil mottaker, ble nevnt.

Foretakene er bekymret for datalekkasje. En leverandør av sikkerhetstjenester mener dette utgjør en trussel da foretakene risikerer betydelige bøter ved brudd på det nye personverndirektivet (GDPR). Utfordringen rettes mot en mulig økt angrepsaktivitet der det trues med å offentliggjøre stjålne personopplysningene dersom foretaket ikke utbetaler krav om løsepenger.

4.1.6 BankID

En del foretak rapporterer om utfordringer knyttet til økende antall tilfeller der BankID ikke fungerer eller ikke fungerer tilfredsstillende. Det har gjentatte ganger vært ustabilitet i forbindelse med oversending av melding til mobiltelefon som brukeren skal godkjenne (push-meldinger).

4.1.7 Utkontraktering og sikkerhet

Et økende antall foretak rapporter utkontraktering til skytjenester. Foretaket får tilgang på et stort kompetansemiljø og løsninger som er velprøvde og redundante. Samtidig medfører samhandling og

samtrafikk i stadig mer distribuerte tjenesteleveranser at det blir mer krevende å sikre tjenesten fra ende-til-ende.

En stadig større andel av Internett-trafikken er kryptert (HTTPS). Dekryptering, rekryptering og endelig dekryptering hos mottaker fører til en komplisert drift (sertifikatadministrasjon) og feil.

Flere foretak nevner at for å unngå spoofing[44], kan foretakene beskytte trafikken over Internett ved bruk av en teknikk som heter Certificate pinning (der en eller flere offentlige nøkler bindes til Internett-domenet som tjenesten leveres fra). Denne vil imidlertid feile dersom Internett-trafikken dekrypteres og kontrolleres i en server satt opp mellom avsender og mottaker.

Flere foretak gir uttrykk for at det er utfordrende å etablere tilstrekkelig sikkerhet for at leverandøren og dennes underleverandører leverer tjenester som tilfredsstiller foretakets krav til sikkerhet og krav som følger av lov og forskrift.

En rekke alvorlige mangler knyttet til leveransene ble avdekket i 2017. I en del tilfeller har foretakene endret sin oppfølging. I noen tilfeller har foretakene gått sammen i kundegrupper, som samarbeider om oppfølging av leverandør.

4.2 Spørreundersøkelse om sårbarhet

I likhet med tidligere år, har Finanstilsynet i 2017 gjennomført en spørreundersøkelse om vurdering av sårbarhet på IKT-området. 21 foretak var med i undersøkelsen. Finanstilsynet ba foretakene vurdere i hvilken grad foretaket anser seg for å være sårbar for aktuelle trusler. Resultatene framgår av tabellene 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 framover, dvs. om sårbarhetene anses å være økende, stabile eller minkende. Trenden som kommer til uttrykk i kolonnen lengst til høyre i tabellene, 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 tabellene.

[44] Spoofing: forfalske hvem som er avsender

Tabell 5 Støtte for strategiske beslutninger

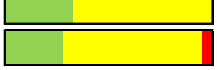
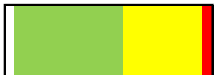
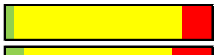
	Sårbarhet	Foretakenes svar	Trend 2017	Trend 2016
1	Systemes evne til å hente informasjon fra eksterne og interne kilder og sammenstille og synkronisere informasjonen til et bilde av foretakets risiko til bruk i styringsøyemed og til myndighetsrapportering		→	→
2	Systemenes evne til automatisk å gi et 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 feil og mangler i systemene		↘	→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert.			

Kilde: Finanstilsynet

Enkelte forhold går igjen, blant annet:

- risikorapporteringen er avhengig av manuelle operasjoner, både når det gjelder intern oppfølging og styring og myndighetsrapportering
- nye og mer integrerte løsninger eksponerer i økende grad svakheter i integrasjoner mot eksisterende kjernesystemer
- flere integrasjonspunkter på grunn av økt funksjonalitet i selvbetjente kanaler
- økte krav til kommunikasjon mellom systemene forklarer høy og økende risiko
- økningen i systemporteføljen og komplekse systemer gir økt risiko for mangler når det gjelder datakvalitet

Tabell 6 Avvik i driften

	Sårbarhet	Foretakenes svar	Trend 2017	Trend 2016
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	Intrusion Detection og Intrusion Prevention, brannmur, antivirus, kontroll av web-trafikk, sikring av e-post, 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, og vi oppdager det ikke, for eksempel minnelekkasje, sertifikater som går ut på dato, elektroniske komponenter som slites, energiforsyning som "slites" (batterier, brennstoff til nødstrømsaggregat)		→	→
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 kontinuitets- og katastrofeløsningene våre, jf. IKT-forskiften § 11		→	↘
12	Samarbeidsrutiner med leverandører		→	→
13	Leveransepresset vi er utsatt for i markedet gjør kvaliteten i løsningene ikke alltid er god nok		↗	↗
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 dual kontroll		→	→
19	Medarbeidernes årvåkenhet når det gjelder trusler og angrep		→	I/A
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert.			

Kilde: Finanstilsynet

Følgende forhold synes å dominere:

- det er utfordrende å balansere implementering av store regulatoriske endringer, teknologiskifte, forretningsutvikling og digitalisering
- kompleksitet i forvaltning og drift øker, blant annet som følge av økt endringstakt
- kompleksitet og arbeid forbundet med vedlikehold av Intrusion Detection og Intrusion Prevention, brannmur, antivirus, kontroll av web-trafikk, sikring av e-post, og andre tiltak for å sikre stabil drift

- økt teknisk kompleksitet og økt tjenesteomfang øker risikoen for at sikkerhetstiltakene ikke fanger opp angrep
- økt sikkerhetsrisiko pga. økt eksponering av tjenester – integrasjon og åpenhet, deling av data
- utfordringer når det gjelder avhengigheter mellom tjenester / leverandører i økosystemet (tele, bank, ID)
- store mengder ustrukturerte data (e-post, Office-dokumenter, private filer). Rydding i forbindelse med GDPR
- risiko for å bli utkonkurrert på teknologi – nye brukeropplevelser / nye aktører / nye løsninger
- forvaltning av komplekse verdikjeder og systemportefølje opp mot krav om hyppige endringer
- migrering / flytting av porteføljer fra gammel til ny teknologi
- Open Banking og PSD 2; hvordan vil markedet endre seg? Stor usikkerhet rundt PSD 2
- det er vanskelig å rekruttere adekvat kompetanse på flere områder, herunder knapp tilgang på kritisk kompetanse; sikkerhet, utvikling, arkitektur knyttet til ny teknologi
- kompetanseskifte, overgang til partnerskap med ekspertise. Verdikjedene endres mot partnere ved tettere samarbeid
- overgang til skyløsninger og standardiserte løsninger som vil redusere kompleksiteten i betjente løsninger
- utkontraktering hos leverandørene gjør det vanskeligere å følge opp
- leverandørene har utfordringer med sine underleverandører
- kontinuitetsløsningene (failover-løsningene) fungerer ikke

Tabell 7 Data er ikke tilstrekkelig beskyttet

	Sårbarhet	Foretakenes svar	Trend 2017	Trend 2016
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	Nettverkssegmentering, perimetersikring, kryptering		→	→
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 e-post, presentasjoner, tekstdokumenter blir gjennomgått regelmessig med tanke på beskyttelse, eventuelt sletting?		→	→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert.			

Kilde: Finanstilsynet

Disse forholdene synes å være dominerende:

- økt teknisk kompleksitet og økt tjenesteomfang øker risikoen for at sikkerhetstiltakene ikke fanger opp angrep
- profesjonelle angripere og flere angrep krever økt ressursbruk og strengere kontroll

- intern kompetanse: korrekt bruk av IT-systemer og informasjon/datakvalitet

Tabell 8 ID-tyveri

	Sårbarhet	Foretakenes svar	Trend 2017	Trend 2016
1	En angriper tar over en brukerid og misbruker denne		→	→
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

Arbeidet mot ID-tyveri er kjennetegnet av at:

- det er et prioritert område for majoriteten av foretakene
- flere foretak rapporterer at de arbeider med ny sonestruktur og nytt tilgangsregime
- økt bruk av DMARC for å hindre mottak av uautorisert e-post, jf. omtale i punkt 3.9.2.2

Tabell 9 Misbruk av tilgang til systemene

	Sårbarhet	Foretakenes svar	Trend 2017	Trend 2016
1	Tilgangskontroll		→	→
2	Våre rutiner når det gjelder tjenestedeling		→	→
3	Logging og varsling		→	→
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

Ansatte misbruker tilgangen til informasjon, enten indirekte ved å se seg ut potensielle målgrupper som kan svindles, eller direkte ved å tilegne seg penger fra kontoer som ikke følges opp i tilstrekkelig grad.

Risikoen synes å ha gått litt ned i 2017 sammenlignet med 2016.

Tabell 10 Hvitvasking

	Sårbarhet	Foretakenes svar	Trend 2017	Trend 2016
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

Det meldes fortsatt om usikkerhet knyttet til presisjon i flagging av mistenkelige transaksjoner. Svarene tyder på at foretakene kontinuerlig arbeider med å forbedre systemenes evne til å fange opp mistenkelige transaksjoner.

4.3 Nasjonale, samt ENISAs, vurderinger av trusselbildet

Publiserte rapporter[45] som vurderer trusselbildet for Norge, peker på at IKT-ressurssentre med statsstøtte fra i hovedsak Russland og Kina utgjør en økende trussel. Aktørene søker å kompromittere og infiltrere norske myndigheter og virksomheter for å innhente informasjon om tradisjonelle politiske og militære mål, samt utføre industrispionasje. For finanssektoren innebærer industrispionasje en risiko for kompromittering, blant annet av informasjon om norske virksomheter som lagres hos banker og finansforetak.

Aktørenes interesse for energiselskaper og industrielle styringssystemer kan tyde på at de nevnte aktørene har ambisjoner om å sette seg i stand til å kunne sabotere infrastrukturen for kraftleveranser. Risikoen om bortfall av elektrisitet må tas alvorlig og derfor inngå i norske foretak og myndigheters risikovurderinger og tiltaksplaner for infrastruktur og IKT.

I 2017 ble det avdekket flere angrep på vestlige demokratiske valgprosesser som viste hvilken effekt og konsekvens digital kriminalitet kan medføre. Det ble også avdekket innbrudd i nettverket til Helse Sør-Østs datasystemer, som viste at aktører fra fremmede stater retter nettverksoperasjoner mot norske virksomheter og systemer, som tradisjonelt ikke forvalter skjermingsverdig informasjon og som tidligere ikke har vært regnet som aktuelle etterretningsmål.

I 2018 forventer etterretningstjenestene at det fortsatt vil gjøres forsøk på rekrutteringer, med den hensikten å skaffe informasjonskilder og agenter for å utsette norske virksomheter for kartlegging og nettverksangrep. Det forventes også at norske virksomheter vil bli utsatt for forsøk på ulovlig anskaffelse av informasjon og teknologi av fremmede makters aktører.

Det etablerte samarbeidet mellom myndigheter, politi og IKT-leverandører har ført til at flere cyber-kriminelle har blitt stanset, arrestert og stilt for retten.

Internasjonalt samarbeid har resultert i avsløring av flere kriminelle nettverk og statsstøttede kriminelle virksomheter, og deres metoder og verktøy for angrep.

ENISAs[46] rapport omtaler at tiltak på tvers av landegrenser og sektorer er et hensiktsmessig middel for å øke kvaliteten og effektiviteten i arbeidet mot digital kriminalitet. For finansiell sektor i Europa har

[45] PST Trusselvurdering 2018, E-tjenestens Fokus 2018, NSMs Risiko 2018
[46] ENISA Threat Landscape Report 2017

det blitt etablert team spesialisert i sikkerhetstesting for å sette aktuelle foretak og institusjoner i stand til å forbygge angrepsaktivitet.

Rapportene viser også at investeringene i IKT-sikkerhet, for både proaktive og reaktive tiltak og løsninger, var rekordstore i 2017. De viser også at cyber-angrepene har vokst i antall og kompleksitet. Kompleksiteten består i at angrepene i stadig større grad skjuler sitt nærvær og sine spor, og blir mer tilpasningsdyktig til nye oppgaver og endrede forutsetninger i ofrenes systemer.

Motivasjonen for de fleste digitale kriminelle er penger. Bruken av virtuell valuta for anonymisering av betalinger for utpressing og annen kriminell virksomhet har vist seg som et effektivt middel for å skjule handlinger.

5 Risikoområder

Finanstilsynets hovedmål er å bidra til finansiell stabilitet og velfungerende markeder. Finansielle tjenester kan ikke leveres uten velfungerende IKT-systemer. Bruk av ny teknologi og nye digitale løsninger øker effektiviteten og medvirker til lavere kostnader, men gir også økt sårbarhet. Også utviklingen innenfor digital kriminalitet øker sårbarheten.

5.1 Finansiell infrastruktur

Den finansielle infrastrukturen består av betalingssystemet og verdipapiroppgjørssystemet samt verdipapirregisteret (VPS), markedsplasser og sentrale motparter. Infrastrukturen skal sørge for at pengebetalinger og transaksjoner i finansielle instrumenter blir registrert, avregnet og gjort opp.

Dersom det ikke er mulig å foreta, gjennomføre eller gjøre opp betalinger, vil viktige samfunnsfunksjoner etter kort tid ikke lenger fungere tilfredsstillende. Sensitiv informasjon på avveie eller brudd på regler for behandling av innsideinformasjon kan medføre svekket tillit til markedsplassene og det finansielle systemet. Lykkes kriminelle i å få tilgang til store mengder kunde- og kontodata og kompromittere disse eller gjøre disse utilgjengelige, kan dette skape betydelige utfordringer for foretaket og også kunne påvirke den finansielle stabiliteten. Foretak som opererer på vegne av alle eller flere foretak, er spesielt sårbare. Foretakenes arbeid med robuste driftsløsninger, inkludert kontinuitetsløsninger, katastrofe- og beredskapsløsninger, gjenopprettingsplaner og IKT-sikkerhetsarbeid, er vesentlige tiltak i arbeidet med å sikre finansiell stabilitet.

Det finnes i dag flere alternative betalingsmåter som gjør deler av betalingssystemet mindre sårbart. Det er også stilt krav til løsninger for kontantberedskap[47]. Hendelser i 2017 viste imidlertid at svikt i styringssystemer, som skal sikre redundans og kontinuitet i foretakenes driftsløsninger, fikk store konsekvenser. Enkelte hendelser førte til at betalingstjenester var utilgjengelige over en hel dag for mer enn 30 prosent av bankkundene. Det skapte stor usikkerhet, både hos kunder og i markedet, til foretakenes evne til kontinuerlig å levere robuste betalingstjenester og gjennomføre betalingsoppdrag.

[47] Finansdepartementet har i forskrift presisert bankenes plikt til løsninger for kontantberedskap for å møte en eventuell økt etterspørsel etter kontanter ved svikt i de elektroniske betalingssystemene. https://www.regjeringen.no/no/aktuelt/nye-krav-til-bankenes-kontantberedskap/id2598131/

BankID er en viktig komponent i den finansielle infrastrukturen. BankID er den eneste tillatte løsning for PKI-basert digital signatur i bank, og er også mye benyttet utenfor banknæringen. Kunden tillates ikke å benytte alternativ PKI-basert digital signatur som kunne vært benyttet når BankID er nede. BankID hadde også i 2017 mange hendelser.

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 sårbarheter 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 delvis 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 sentrale infrastrukturforetak (FMI-foretakene), og Norges Bank kan delta som observatør på Finanstilsynets tilsyn med banker og datasentraler av betydning for finansiell infrastruktur.

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

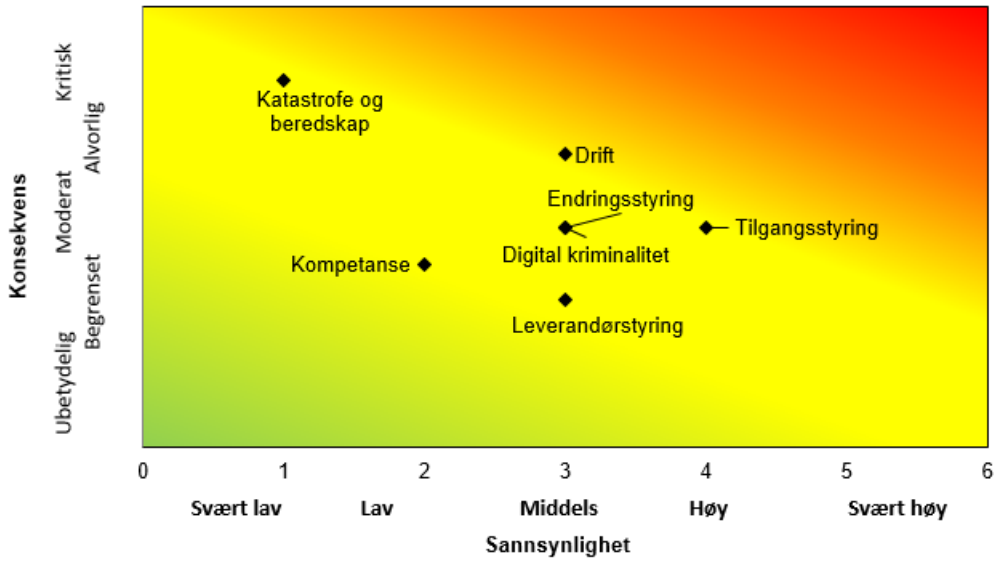
Det var i 2017 god regularitet på avregnings- og oppgjørssystemene og kommunikasjonen mot det internasjonale betalingssystemet SWIFT og det internasjonale oppgjørssystemet CLS.

Selv om det var hendelser som gjorde betalingsløsninger utilgjengelige i lengre perioder og tilgjengeligheten til betalingssystemer var noe svakere enn i 2016, vurderer Finanstilsynet likevel den norske finansielle infrastrukturen som hovedsakelig robust.

5.2 Foretakene

Figur 6 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 og konsekvensene dersom hendelsen oppstår.

Figur 6 Finanstilsynets vurdering av risiko



Kilde: Finanstilsynet

Finanstilsynet vurderer sårbarheter i driftsløsninger, mangelfull tilgangsstyring, mangelfull endringsstyring og svakheter i forsvarsverk som de dominerende risikoene i foretakene. Hendelser i 2017 viser at foretakenes driftssystemer ikke er tilstrekkelig robuste. Tilsyn viser mangler når det gjelder kontroll med tilgang til systemer og data. Finanstilsynet observerer også organisatoriske, operasjonelle og tekniske svakheter knyttet til foretakenes IKT-sikkerhetsarbeid.

Sårbarheter knyttet til leverandørstyring, katastrofe- og beredskapsløsninger og manglende kompetanse utgjør også sentrale risikoer.

Sårbarhet – svakhet i teknisk infrastruktur, funksjoner og prosesser som kan resultere i at uønskede hendelser inntreffer.

Trussel – forhold med potensiale til å forårsake en uønsket hendelse.

Risiko – risikoen for at en uønsket hendelse inntreffer som følge av utilstrekkelige eller sviktende interne prosesser eller systemer, menneskelige feil eller eksterne hendelser.

Konsekvens – mulig følge av en uønsket hendelse.

Risikovurdering – omfatter identifikasjon, analyse og evaluering av risiko. En risikovurdering legger grunnlag for foretakets risikoreduserende tiltak og prioritering av disse.

Flere av foretakene har utfordringer med å etablere en tilfredsstillende risikostyring på området, herunder et godt rammeverk for risikovurderinger. Finanstilsynet mener dette kan være en medvirkende årsak til noen av svakhetene som er avdekket gjennom tilsynsvirksomheten. Kritisk gjennomgang av risikovurderingene er viktig for å sikre at vesentlige risikoer for foretaket er identifisert, analysert og evaluert.

Nedenfor følger en nærmere gjennomgang av de sårbarheter som Finanstilsynet vurderer som de mest sentrale innen foretakenes IKT-tjenester. Dette er sårbarheter som alle kan true en sikker og stabil drift.

Drift

Foretakenes tjenester er basert på digitale løsninger, og sårbarheter som følge av at foretakets driftsløsninger ikke er tilstrekkelig robuste, utgjør risiko for utilgjengelige tjenester og/eller ustabile tjenester.

En kritisk tjeneste er ikke robust når avvik på en komponent gjør at tjenesten ikke er tilgjengelig fordi komponenter i økosystemet for tjenesten (nettverk, servere, programvare, strøm, lokaler m.m.) ikke er duplisert gjennom redundante løsninger, eller at kontinuitetsløsningen har avvik som medfører at denne ikke virker som forutsatt.

Graden av integrasjon mellom ulike tjenesteleverandører øker risikoen for driftsproblemer, dels fordi det er flere systemer som inngår i tjenesten som kan gå ned og dermed medføre at tjenesten ikke er tilgjengelig, og dels fordi integrasjonen av mange tjenesteleverandører gjør det mer komplisert å holde oversikt over sårbare komponenter. Nye og mer integrerte løsninger eksponerer i økende grad svakheter i integrasjoner mot eksisterende kjernesystemer. Omfanget av integrasjonspunkter mellom ulike systemer øker, blant annet på grunn av økt funksjonalitet i selvbetjente kanaler.

Økningen i systemporteføljen i kombinasjon med komplekse systemer gir også økt risiko for dårligere datakvalitet. Datastrukturene kjennetegnes av at samme data lagres flere steder. Det er ingen "master"-versjon av dataene, men det finnes flere utgaver som er "master" for sitt applikasjonsdomene. Det er utfordrende å synkronisere alle versjonene.

Mangler i dupliseringen av driftsløsningen, feil i styringssystem for overgang til duplisert løsning og menneskelig svikt var flere av årsakene til alvorlige driftsproblemer og utilgjengelige tjenester i 2017. Mangel på kompetente ressurser og utfordringer med hendelseshåndtering i samarbeid med leverandører, og mellom leverandører, medvirket til lang reetableringstid. Enkelte hendelser inntraff som følge av mangler i kapasitetsstyringen.

Finanstilsynet vurderer den samlede risikoen knyttet til sårbarheter ved **driftsløsninger** som **middels**. Sannsynligheten for uønskede hendelser vurderes som *middels* og konsekvensen som *alvorlig*. Dette er basert på følgende vurderinger:

- Sannsynlighet for redusert datakvalitet som følge av kompleks integrasjon mellom tjenesteleverandører vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for ustabile og /eller utilgjengelige tjenester som følge av økt grad av integrasjon mellom ulike tjenesteleverandører vurderes som *middels* og med *alvorlig* konsekvens.
- Sannsynlighet for driftsproblemer som rammer felles operasjonell infrastruktur vurderes som *middels* og med *alvorlig* konsekvens.
- Sannsynlighet for utilgjengelige tjenester som følge av mangelfull kapasitetsstyring som *middels* og med *alvorlig* konsekvens.
- Sannsynligheten for at systemkomponenter i redundante løsninger feiler, som følge av mangelfull overvåking og test, som *lav* og med *alvorlig* konsekvens.
- Sannsynlighet for driftsproblemer (nettverk og tjenester) som følge av ugyldige digitale sertifikater eller ugyldige lisenser som *middels* og med *moderat* konsekvens.

Katastrofe- og beredskapsløsning

Sårbarheter i katastrofe- og beredskapsløsninger utgjør en risiko dersom en alvorlig hendelse inntreffer i foretakets driftsløsning, herunder kontinuitets- og høytilgjengelighetsløsninger, som medfører at det kan bli behov for å ta i bruk katastrofe-/beredskapsløsningen.

Mangelfulle eller manglende testing av foretakets katastrofe- og beredskapsløsning og beredskapsledelse og mangelfulle evalueringer av tester utgjør risiko for at foretaket og dens leverandører ikke er tilstrekkelig forberedt, og dermed ikke vil være i stand til å håndtere en krise, eller en katastrofe.

Mangelfulle analyser av forretningsmessige konsekvenser, om en krise inntreffer, utgjør en risiko for at katastrofe- og beredskapsløsningen ikke etableres med nødvendig teknisk infrastruktur og med nødvendig kapasitet. Manglende krav til reetablering av driften (RTO) og manglende krav til hvor mye

data som kan gå tapt (RPO) er også forhold som utgjør risiko for at løsningen ikke blir dimensjonert riktig. Manglende sikkerhetsoppdateringer av katastrofeløsninger øker risikoen for digitale angrep i en spesielt sårbar situasjon for foretaket.

Finanstilsynets erfaring er at foretakene ikke er tilstrekkelig forberedt dersom en alvorlig krise eller katastrofe inntreffer. Manglende eller mangelfulle beredskaps- og katastrofeløsninger er en utfordring for flere foretak, og Finanstilsynet erfarer også at foretak generelt har utfordringer med å håndtere alvorlige driftsavbrudd. Dette er en bekymring som forsterkes dersom en krise eller katastrofe inntreffer.

Finanstilsynet anser sannsynligheten for at alvorlige hendelser inntreffer, som krever iverksettelse av katastrofe- og beredskapsløsninger, som *svært lav*. Konsekvensen anses allikevel som *kritisk* dersom løsningen ikke fungerer som forutsatt.

Finanstilsynet vurderer den samlede risikoen knyttet til sårbarheter ved **katastrofe- og beredskapsløsninger** som **høy**. Dette er basert på følgende vurderinger:

- Sannsynligheten for at foretakets løsning ikke er etablert i henhold til foretakets behov, som følge av mangelfulle konsekvensanalyser og krav, vurderes som *middels* og med *kritisk* konsekvens dersom løsningen iverksettes.
- Sannsynligheten for at foretak ikke er tilstrekkelig forberedt på en alvorlig situasjon, som følge av mangelfulle og realistiske øvelser, vurderes som *høy* og med *alvorlig* konsekvens.
- Sannsynligheten for at løsningen ikke fungerer som forventet, som følge av mangelfulle tekniske tester og evaluering av disse, vurderes som middels og med kritisk konsekvens.
- Sannsynlighet for mangelfull sikkerhetsoppdateringer på løsningene vurderes som *middels* og med *alvorlig* konsekvens.

Kompetanse

Sårbarheter som følge av mangel på tilgang til ekspertise innen driftsoperasjoner, arkitektur, IKT-sikkerhet og mangelfull kompetansestyring utgjør risiko for den operative driften. Mangelfull kompetanse kan også medføre at foretaket tar i bruk feil teknologi og/eller ikke ser mulighetene ved ny teknologi.

Finanstilsynet har registrert at foretakene har utfordringer med å få tak i nødvendig og kritisk kompetanse innen teknologi, herunder sikkerhet, arkitektur og utvikling, og i forståelsen av ny teknologi og anvendelsen av denne. Det er utfordringer i balansen mellom å opprettholde kompetanse for den daglige driften og kompetanse som kreves for å utvikle nye løsninger.

Finanstilsynet vurderer den samlede risikoen knyttet til sårbarheter ved **kompetanse** som **lav** til **middels**. Sannsynligheten for uønskede hendelser oppstår eller at uønskede hendelser ikke blir håndtert tilstrekkelig som en konsekvens av manglende kompetanse vurderes som *lav til middels* og konsekvensen som *begrenset til moderat*. Dette er basert på følgende vurderinger:

- Sannsynligheten for at mangelfull kompetansestyring medfører tap av og/eller manglende kompetanse for å ivareta en forsvarlig drift, vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for driftsavbrudd og utilgjengelige tjenester, som følge av mangelfull kompetanse, vurderes som *lav* og med *moderat* konsekvens.
- Sannsynligheten for at informasjonssikkerhetsbrudd inntreffer, som følge av mangelfull tilgang på sikkerhetskompetanse, vurderes som *lav* og med *moderat* konsekvens.
- Sannsynligheten for at mangelfull kompetanse i foretaket, vedrørende de tjenester som leverandører drifter og utvikler, medfører brudd på lover og regler, vurderes som *middels* og med *moderat* konsekvens.

Leverandørstyring

Sårbarheter som følge av manglende eller mangelfull leverandøroppfølging, administrativt og operativt, utgjør risiko for brudd på etterlevelse av avtalte krav og brudd på IKT-forskriftens bestemmelser. Det utgjør også en risiko for at leverandøren ikke har etablert tilstrekkelig internkontroll, som igjen eksponerer utkontrakterte tjenester for blant annet informasjonssikkerhets-brudd. Videre utgjør dette en risiko for at alvorlige økonomiske problemer eller manglende ressurser hos leverandøren, som kan true leverandørens leveranseevne, ikke oppdages. Uklare roller og ansvar mellom foretaket og leverandøren, og mellom leverandører i verdikjeden, utgjør en risiko for at alvorlige hendelser ikke blir løst i tide.

Uønsket leverandøravhengighet kan oppstå ved svakheter i leverandørstyringen, der avtalens bestemmelser ved overføring av tjenesten til annen leverandør ikke er tilstrekkelig forpliktende. Dette utgjør en risiko for langvarig ustabilitet i tjenesten i prosessen med å overføre tjenesten til annen leverandør, spesielt der overføringen er som følge av at leverandøren ikke oppfyller leveransekravene.

Finanstilsynet har gjennom sin tilsynsvirksomhet i 2017 registrert flere forhold som utgjør en risiko for at foretak ikke vil fange opp avvik i leverandørens internkontroll.

Foretakene har utfordringer med å etablere tilstrekkelig sikkerhet for at leverandøren, og dens underleverandører, leverer tjenester som tilfredsstiller foretakets krav til sikkerhet og krav som følge av lov og forskrift. Videre er det utfordrende for foretakene å forankre sikkerhetskravene hos sine leverandører.

Samhandlingen mellom foretak og leverandører knyttet til hendelser og endringer er utfordrende, og det er i noen tilfeller mangelfull kunnskap hos foretak når det gjelder forståelse av hva den utkontrakterte tjenesten omfatter.

Finanstilsynet vurderer den samlede risikoen knyttet til sårbarheter ved **leverandørstyring** som **middels**. Sannsynligheten for uønskede hendelser vurderes som *middels* og konsekvensen som

begrenset. Dette er basert på følgende vurderinger:

- Sannsynligheten for at vesentlige avvik i leverandørens internkontroll ikke oppdages av foretaket vurderes som *middels* og med *moderat* konsekvens.
- Sannsynlighet for at sikkerhetsbrudd inntreffer, som følge av mangelfull oppfølging og forankring av sikkerhetskravene hos leverandøren, vurderes som *middels* og med *moderat* konsekvens.
- Sannsynlighet for uforsvarlig lang reetableringstid ved alvorlige driftsavbrudd, som følge av uklare roller og ansvar i samhandlingen med leverandøren, vurderes som *middels* og med *moderat* konsekvens.
- Sannsynlighet for utilgjengelige tjenester, som følge av manglende overvåking av kvalitet på tjenesten, vurderes som *lav* og med *moderat* konsekvens.
- Sannsynlighet for uønsket leverandøravhengighet som følge av mangelfulle reguleringer (eksempelvis exit-bestemmelser) i avtalen vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for uønsket leverandøravhengighet som følge av mangelfull kompetanse om foretakets utkontrakterte tjenester vurderes som *middels* og med *begrenset* konsekvens.
- Sannsynligheten for at manglende risikovurdering (periodisk) ikke avdekker svak bærekraft hos leverandøren, som følge av en krevende likviditetssituasjon (konkursrisiko), utfordrende ressurssituasjon, eller andre forhold som kan true leverandørens leveranseevne, vurderes som *lav* og med *moderat* konsekvens.

Tilgangsstyring

Sårbarheter knyttet til mangelfull tilgangsstyring utgjør en risiko for informasjonssikkerhetsbrudd, herunder brudd på konfidensialitet, integritet og tilgjengelighet.

Finanstilsynet har gjennom sin aktivitet i 2017 registrert flere forhold som har resultert i denne type brudd, eller avdekket og observert forhold som utgjør en risiko for at brudd vil oppstå.

Tilgangsstyring, som en proaktiv kontroll av tilganger til systemer og teknisk infrastruktur, både for egne ansatte og ansatte hos leverandørene, er en utfordring for foretakene. Finanstilsynet har også avdekket svak kontroll med personell som har utvidede rettigheter hos foretaks leverandører. Foretak har begrenset kontroll på informasjon som sendes ut av foretaket på e-post eller kopieres til minnepinner.

Konsekvenser ved identifiserte sårbarheter er mange og kan være; konfidensiell eller gradert informasjon kommer uvedkommende i hende, det foretas autoriserte endringer av kundeinformasjon eller uautoriserte endringer i betalingstransaksjoner. Det kan også føre til at systemene som følge av uautoriserte handlinger ikke er tilgjengelige eller medfører alvorlige driftsproblemer. Sårbarhetene kan medføre at foretaket og dens kunder påføres skade og/eller idømmes betydelige bøter som følge av regelverksbrudd.

Finanstilsynet vurderer den samlede risikoen knyttet til sårbarheter ved **tilgangsstyring** som **middels**. Sannsynligheten for uønskede hendelser vurderes som *middels* og konsekvensen som *moderat*. Dette er basert på følgende vurderinger:

- Sannsynligheten for at konfidensiell og/eller gradert informasjon kommer på avveie, som følge av ansattes utsendelse på e-post eller kopiering til minnebrikke, vurderes som *høy* og med *moderat* konsekvens.
- Sannsynligheten for at konfidensiell og/eller gradert informasjon kommer på avveie, som følge av sikkerhetsbrudd hos leverandøren, vurderes som *middels* og med *høy* konsekvens.
- Sannsynligheten for at ansatte eller ansatte hos leverandøren foretar uautoriserte transaksjoner eller endrer en transaksjon vurderes som *lav* og med *moderat* konsekvens.
- Sannsynligheten for at foretakets ansatte ulovlig endrer på informasjon vurderes som *lav* og med *begrenset* konsekvens.
- Sannsynligheten for at ansatte hos leverandøren, eller dens underleverandør, foretar regelbrudd i utførelsen av driftsoppgaver vurderes som *middels* og med *alvorlig* konsekvens.

Endringsstyring

Sårbarheter knyttet til mangelfull endringsstyring utgjør en risiko for uautoriserte endringer og at endringer med sårbarheter eller feil settes i produksjon. Nye regulatoriske krav, økt endringstakt og raskere utvikling av nye løsninger er alle forhold som øker risikoen for at sårbarheter introduseres ved endringer som følge av for svak styring og kontroll.

Finanstilsynet har gjennom sin aktivitet i 2017 registrert utfordringer i foretaks endringsstyring. Gjennom hendelsesrapporteringen til Finanstilsynet framgår det at alvorlige hendelser oppstod som følge av endringer. Dette gjelder både funksjonelle og ikke funksjonelle endringer.

Finanstilsynet vurderer den samlede risikoen knyttet til sårbarheter ved **endringsstyring** som **middels**. Sannsynligheten for uønskede hendelser vurderes som *middels* og konsekvensen som *moderat*. Dette er basert på følgende vurderinger:

- Sannsynlighet for utilgjengelige tjenester som følge av ikke-funksjonelle endringer (endring i konfigurasjon av driftskomponenter) vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for at funksjonelle endringer (programvare) introduserer sårbarheter i foretakets forsvarsverk vurderes som *lav* og med *moderat* konsekvens.
- Sannsynligheten for at den økte endringstakten medfører at nye tjenenester settes i produksjon uten nødvendig kvalitet vurderes som *høy* og med *moderat* konsekvens.
- Sannsynlighet for at foretaks usikkerhet knyttet til PSD 2-kravene medfører at nødvendige endringer ikke blir gjennomført, vurderes som *middels* og med *moderat* konsekvens.

Digital kriminalitet

Sårbarheter knyttet til foretakenes styring, forsvarsverk og reaksjonsevne, herunder organisering med roller og ansvar, sikkerhetsrammeverk, opplæring, avtalereguleringer og samhandling med

leverandører, testing, overvåking eller tekniske sikringer, utgjør en risiko for at foretaket og dens kunder skades gjennom digital kriminalitet.

Foretakenes sikkerhetsrammeverk, opplæring av ansatte, sikkerhetskrav i avtaler med leverandørene og organisering av sikkerhetsområdet danner grunnlaget for en god sikkerhetskultur i arbeidet med å forebygge digitale angrep.

Det er mange typer angrepsformer. Eksempler er ID-tyveri, sosial manipulering (jf. punkt 3.9.2.1) og tjenestenektangrep, som DDoS-angrep.

Finanstilsynet har i 2017 registrert både organisatoriske, operasjonelle og tekniske svakheter som medfører sårbarhet for tilsiktede og utilsiktede angrep og feil. Spesielt nevnes uklare ansvarsforhold, mangelfulle sikkerhetsoppdateringer, mangelfull sikkerhetstesting og manglende systemer for å avdekke falske e-poster.

Gjennom eksterne vurderinger av foretaks nettverksinfrastruktur ble det avdekket vesentlige svakheter relatert til sikkerhet som følge av manglende segmentering, herunder mangelfull soneinndeling av foretaks interne og eksterne nettverk. Det ble avdekket sårbarheter hvor det var mulighet for ansatte hos en leverandør å tilegne seg brukernavn og passord for ansatte i flere foretak.

Innen kortområdet har Finanstilsynet merket seg at noen av de største kortutstederne ikke har implementert funksjonalitet iht. retningslinjer for sikkerhet i Internett-betalinger.

Finanstilsynet vurderer den samlede risikoen knyttet til sårbarheter i foretakets forsvarsverk, som kan føre til skade som følge av **digital kriminalitet,** som **middels**. Sannsynligheten for uønskede hendelser vurderes som *middels* og konsekvensen som *moderat*. Dette er basert på følgende vurderinger:

- Sannsynligheten for at foretak rammes av skadevare vurderes som *middels* og med *alvorlig* konsekvens.
- Sannsynligheten for at gradert eller konfidensiell informasjon kommer på avveie vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten at sårbarheter ikke oppdages i foretakets forsvarsverk, som følge av mangelfull kompetanse og sikkerhetstesting, vurderes som *middels* og med *alvorlig* konsekvens.
- Sannsynligheten for at lite benyttede systemer i foretakets nettverk ikke blir sikkerhetsoppdatert vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for at ansatte med fullmakter blir identifisert av kriminelle og presset til å utføre uautoriserte handlinger vurderes som *middels* og med *begrenset* konsekvens for foretaket.

- Sannsynligheten for at en eller flere av foretakets kunder gir fra seg påloggingsinformasjon til betalingstjenenester som følge av sosial manipulering vurderes som *høy* og med *begrenset* konsekvens.

5.3 Brukere

Bruk av digitale løsninger innebærer at det legges igjen spor. Dette utfordrer personvernet. Sporene kan brukes til såkalt profilering, til utpressing, kartlegging, ID-tyveri og manipulering. Bruk av kontanter sikrer at kundens kjøpsadferd forblir en privatsak. På stadig flere brukersteder er det imidlertid ikke lenger mulig å betale med kontanter, og antall minibanker reduseres.

Digitale løsninger dominerer. Løsninger som ikke er digitale prises stadig høyere, for å gi kundene insentiver til å ta i bruk digitale tjenester. En rekke kunder har ikke kompetanse og forutsetninger som skal til for å benytte de digitale tjenestene. I følge Statistisk Sentralbyrås publikasjon om IKT i husholdningene[48] er det over 400.000 mennesker som føler seg utenfor grunnet teknologiutviklingen.

Det anslås at det er vel 220.000 bankkunder i Norge som ikke benytter bankens digitale tjenester, herunder betaling av regninger og kontooverføringer ved bruk av nettbank eller mobiltelefon. Disse kundene benevnes som "analoge kunder" og benytter tradisjonelle betalingstjenester som brevgiro og betaling over skranke.

Prisingen av tradisjonelle tjenester og/eller det at mange vegrer seg eller ikke er i stand til å ta i bruk digitale tjenester, har blant annet ført til at flere har valgt å overlate regningsbetalingen, ved å gi fra seg sin digitale ID, til familiemedlemmer eller andre betrodde som er brukere av de digitale tjenestene. Finanstilsynet mener dette i seg selv utgjør en risiko ved at denne tilliten kan misbrukes, spesielt der nettbank for kunden blir etablert og kundens påloggingsinformasjon blir benyttet av den betrodde.

Bankene har på sin side fokusert på å hjelpe denne kundegruppen over fra analoge til digitale løsninger gjennom informasjon og kurs. Finanstilsynet har inntrykk av dette er initiativ som har bidratt til at flere tar steget over i den digitale verden.

Samtidig er det fortsatt kunder som vil forbli analoge fordi de digitale løsningene er for kompliserte, de ønsker anonymitet eller fordi de rett og slett ikke vil være digitale.

[48] https://www.aftenposten.no/norge/i/gPp38L/Norge-er-i-digitaliseringstoppen-400000-mennesker-star-utenfor?spid_rel=2

6 Finanstilsynets oppfølging

6.1 Sentrale områder for Finanstilsynets IKT-tilsyn

Tilsynsvirksomheten er risikobasert. Finanstilsynet vil ha stor oppmerksomhet på de tilsynsenhetene som har størst innvirkning på finansiell stabilitet og velfungerende markeder. Foretakenes IKT-risiko vil bli vurdert, og foretakenes egne årlige vurderinger av IKT-risikoen vil bli gjennomgått. Prioriterte tema for tilsyn vil være styring og kontroll med IKT-virksomheten, foretakenes beredskapsarbeid knyttet til kontinuitet og kriseløsninger og testing av disse samt utkontraktering og IKT-løsninger for å avdekke hvitvasking og terrorfinansiering. Tilsyn med organisering av IKT-/cyber-sikkerhetsarbeidet, sikkerheten knyttet til foretakenes IKT-løsninger og organiseringen av overvåkningen vil også vektlegges.

Andre aktuelle tema for tilsyn er blant annet foretakenes kontroll med tilganger til systemer, særlig der det er systemer som inneholder sensitiv informasjon, og utvikling av nye løsninger som omfatter ny teknologi. Foretak som gjennomfører større endringer på IKT-området, og dermed kan øke risikoen innenfor operasjonell risiko, vil vektlegges.

Tilsynsvirksomheten vil også omfatte foretakenes risikovurderinger ved utkontraktering av IKT og kvalitet på avtaleverk og oppfølging av avtaler mellom foretak og leverandør.

6.2 Arbeid med betalingssystemer

Finanstilsynet vil følge opp foretakenes betalingstjenester mht. forskrift[49] til betalingssystemloven og etterlevelse av meldeplikten. Det vil også gjennomføres oppfølging mht. forskrift om formidlingsgebyrer i kortordninger. Når det reviderte betalingstjenestedirektivet (PSD 2) fra EU tas inn i norsk lovgivning, vil Finanstilsynet legge dette til grunn i oppfølgingen av foretakenes betalingstjenester.

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

Samarbeidet med Norges Bank vil videreføres.

[49] Forskrift om systemer for betalingstjenester

6.3 Oppfølging av hendelser

Det var en negativ utvikling når det gjelder alvorlige hendelser i 2017 i forhold til tidligere år. Finanstilsynet vil i 2018 følge nøye med på utviklingen og vurdere behov for tiltak. Det vil bli lagt vekt på at årsaker avdekkes og tiltak iverksettes for å hindre gjentakelser.

Ved alvorlige avvik vil hendelsen følges opp gjennom hele hendelsens livsløp, og ved behov vil det bli gjennomført oppfølgingsmøter. Særlige tiltak vil bli vurdert.

6.4 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 beredskapsøvelser også i 2018, og tiltak knyttet til funn fra tidligere øvelser vil bli fulgt opp.

Finanstilsynet vil også ta del i relevant beredskapsarbeid initiert av andre sektorer og samhandling innenfor nasjonalt rammeverk for håndtering av IKT-sikkerhetshendelser.

Finanstilsynet vil innrette sitt beredskapsarbeid og håndtering av IKT-sikkerhetshendelser i tråd med Nasjonal sikkerhetsmyndighets (NSM) rammeverk for håndtering av IKT-sikkerhetshendelser[50]. Med bakgrunn i rammeverket er det planlagt en formalisering av samarbeidet mellom Finanstilsynet og Nordic Financial CERT for å etablere et sektorvis responsmiljø (SRM) for den delen av finanssektoren som Finanstilsynet har tilsyn med. Finanstilsynet har den formelle rollen som SRM og vil utøve denne rollen i samarbeid med Nordic Financial CERT etter avtalte regler for informasjonsutveksling.

6.5 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:

- det digitale trusselbildet
- beredskapsarbeid rettet mot digital sårbarhet og digital sikkerhet
- hvordan foretakene organiserer og følger opp arbeidet med sikkerhet
- endringene i betalingsformidlingen ved utnyttelse av ny teknologi (FinTech), og for grensekryssende virksomhet

[50] https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/rammeverk-hendelseshandtering/

6.6 Forbrukervern

Finanstilsynet vil legge vekt på at foretakene ivaretar kundenes sikkerhet på en god måte. Det vil også bli fulgt opp at foretakene ikke deler kundenes data uten samtykke og at data ikke kommer tredjepart urettmessig i hende.

Finanstilsynet vil følge opp at foretakene etablerer løsninger, i tråd med regelverket, som gir forbrukerne mulighet til å beskytte seg, som for eksempel sperring av kort for bruk på Internett, se punkt 3.1.5.

Ved hendelser vil Finanstilsynet følge opp at foretakene gir forbrukerne informasjon i tråd med hvordan de blir rammet og hvordan foretaket eller forbrukeren selv kan avhjelpe situasjonen.

Ordliste

Begrep/forkortelse	Betydning
3-D Secure	3-D Secure er en XML-basert protokoll som benyttes ved nettbetaling. Den gir et ekstra sikkerhetslag ved bruk av kort, ved at bruker autentiserer seg overfor kortutsteder, uavhengig av betalingsmottaker. Hos Visa, som utviklet protokollen, heter den "Verified by Visa".
AIS	Account Information Supplier – Kontoinformasjonstilbyder
AISP	Account Information Service Providers. Se også Opplysningsfullmakt.
API	Application Programming Interface
App	Applikasjon – på nettbrett eller mobiltelefon
AML	Tiltak mot hvitvasking (Anti Money Laundering)
BFI	Beredskapsutvalget for finansiell infrastruktur Koordineringsutvalg ved kriser i finanssektoren. Ledes av Finanstilsynet.
Betalingsfullmakt	Aktører som kan initiere betalinger på vegne av kunder. Benevnes PISP under PSD 2.
Blokkjede	Liste med data/transaksjoner, kalt blokker, som er koblet sammen i en kjede og sikret ved hjelp av kryptografi.
CEO-svindel	Svindler gir seg ut for å være øverste leder i en bedrift. Kalles også 'Fake president fraud' eller 'Business Email Compromise'.
CEO-angrep	Nettangrep som bruker CEO-svindel.
CERT	Computer Emergency Response Team Ekspertgruppe som håndterer sikkerhetsbrudd på Internett.
Cloud Computing	Skytjeneste. Distribuert databehandling via et nettverk. Mulighet for å kjøre program på mange sammenknyttede servere. Skytjenester kan være både private og offentlige, eller en blanding av disse.
CLS	Continuous Linked Settlement. Internasjonalt oppgjørssystem for valutahandler.
CNP	Card Not Present. Svindel med hjelp av stjålne kortopplysninger, vesentlig ved netthandel.
CPMI/IOSCO	The Committee on Payments and Market Infrastructures / International Organization of Securities Commissions
CVC-kode	Card Verification Code. Verifiseringskode; de tre siste sifrene på baksiden av de fleste kredittkortene.
DMARC	Domain-based Message Authentication, Reporting and Conformance
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.
DSPO	Digitaliseringssamarbeidet mellom offentlig og privat sektor
EBA	European Banking Authority. Den europeiske banktilsynsmyndigheten.
ECB	European Central Bank. Den europeiske sentralbanken.
EIDAS	Electronic IDentification, Authentication and trust Services. Et sett med standarder for elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det europeiske fellesmarkedet
EIOPA	European Insurance and Occupational Pensions Authority. Den europeiske tilsynsmyndigheten for forsikrings- og tjenestepensjon.
EMIR	European Market Infrastructure regulation
ENISA	European Union Agency for Network and Information Security. Den europeiske etaten for nettverks- og informasjonssikkerhet.
ESMA	European Securities and Markets Authority. Den europeiske verdipapir- og markedstilsynsmyndigheten.
Fintech	Financial technology
FMI	Financial Market Infrastructure. FMI er en samlebetegnelse på institusjoner innen finansmarkedsinfrastrukturen som interbanksystemer, verdipapiroppgjørssystemer, sentrale motparter, verdipapirregistre, datavarehus mv.
GDPR	General Data Protection Regulation
IaaS	Infrastructure as a service (skytjeneste)
ICO	Initial Coin Offerings
Informasjons-sikkerhetsbrudd	Brudd på integritet, konfidensialitet og tilgjengelighet.
ISP	Internet Service Provider – Leverandøren av internettforbindelse og domenenavn
Malware	Fellesbetegnelse for software med "fiendtlige hensikter". som virus, trojanere, ransomware mv.
MIF-forordningen	Multilateral Interchange Fees. Forordning om formidlingsgebyr for kortbaserte betalingstransaksjoner
MIFID II	Forskrift om verdipapirforetak, regulerte markeder, datarapporteringstjenester og handel i varederivater og utslippskvoter.
NBO	Norges Banks oppgjørssystem
NICS	Norwegian Interbank Clearing System
NIS-direktivet	Network and information systems. EU-direktiv som skal sikre høyt felles nivå på nettverks- og informasjonssikkerhet i EU.
Nordic Financial CERT	Nordic Financial CERT er en samarbeidsorganisasjon etablert av nordiske finansforetak som skal identifisere og bekjempe cyber-angrep rettet mot finansnæringen i Norden, se www.nfcert.org.
Opplysningsfullmakt	Aktører som kan hente informasjon fra bankkonto på vegne av kunde. Benevnes AISP under PSD 2.

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.
PIS	Payment Initiation Services – Betalingstjenesteinitiatorer
PISP	Payment Initiation Service Providers. Se også "Betalingsfullmakt".
PKI	Public-key infrastructure. Består av maskinvare, programvare, prosedyrer, retningslinjer og personell som er nødvendig for å lage, forvalte, distribuere, bruke, lagre og kunne tilbakekalle digitale sertifikater.
PaaS	Platform as a Service (skytjeneste)
PSD 2	Revidert betalingstjenestedirektiv 2015/36/EU
Ransomware	Er en type skadevare som begrenser tilgang til IKT-løsninger som er infisert og krever en løsesum.
RegTech	Teknologiske løsninger som skal avhjelpe finansinstitusjoner gjennom bedre risikostyring og med større sikkerhet overholde regulatoriske krav.
SaaS	Software as a Service (skytjeneste)
SMTP-servere	Simple Mail Transfer Protocol-servere. Brukes for å sende og motta ekstern mail.
SSL	Secure Sockets Layer. Eldre krypteringsmetode, nå erstattet av TLS.
Skytjenester	Skybasert plattform, infrastruktur, program eller lagringstjenester.
Spoofing	Forfalske en avsenderadresse, for eksempel avsender av en e-post.
Sterk autentisering	Autentisering ved bruk av flere metoder, f.eks. pinkode + passord.
STIP	Stand-in processing. Dersom driftssentralen for transaksjonshåndtering ikke oppnår kontakt med kortutstedende bank/kredittkortselskap, kan driftssentralen, for eksempel Nets, autorisere på vegne av banken. Det samme gjelder Visa og MasterCard International. Ved slike situasjoner gjelder egne beløpsgrenser som kan variere fra et kort til et annet.
SWIFT	The Society for Worldwide Interbank Financial Telecommunication.
TFIT	Taskforce on IT Risk Supervision – arbeidsgruppe under EBA
TFPS	Taskforce on Payment Services – arbeidsgruppe under EBA
TLS	Transport Layer Security. En protokoll som brukes mellom e-postservere til å kryptere meldinger og levere dem trygt. Forhindrer tyvlytting og forfalsking mellom e-postservere.
TPP	Third Party Providers Begrep fra PSD 2-direktivet. Dette er tjenesteleverandører som yter betalingsformidlingstjenester og som normalt ikke kontofører betalers eller betalingsmottakers kontoer.
TRS-rapportering	Verdipapirforetakenes transaksjonsrapportering.
xID	xID er et supplement til BankID for nettsteder og tjenester som trenger en enkel innlogging, et tryggere og bedre alternativ til brukernavn og passord.
XML	Extensible Markup Language. Teknologi for utveksling av data.

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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

05.2018