FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

RISIKO- OG SÅRBARHETSANALYSE (ROS)

2018

Risiko- og sårbarhetsanalyse (ROS) 2018

Finanssektorens bruk av informasjons- og kommunikasjonsteknologi (IKT)

Finanstilsynet, 8. mai 2019

INNHOLD

1 INNLEDNING 5

2 OPPSUMMERING 6

2.1 Overordnet vurdering 6

2.2 Finanstilsynets funn og observasjoner 6
2.2.1 Tilsynsområder 6
2.2.2 Hendelser 8
2.2.3 Utkontrakteringsmeldinger 8
2.2.4 IKT- og informasjonssikkerhet 8
2.2.5 Utviklingstrekk innenfor finansiell teknologi 9
2.2.6 Styring av IKT-virksomheten 9

2.3 Foretakenes vurderinger 10

2.4 Aktuelle risikoområder 10

3 FINANSTILSYNETS FUNN OG VURDERINGER 12

3.1 Betalingssystemer 12
3.1.1 Generelt om betalingssystemer 12
3.1.2 Styring og kontroll med risiko og sårbarhet i betalingssystemene 13
3.1.3 Melding om systemer for betalingstjenester 14
3.1.4 Utvikling innen betalingstjenester og mobile betalingsløsninger 14
3.1.5 Tap som følge av svindel med betalingstjenester 17

3.2 Betalingsforetak 20

3.3 Bank 20
3.3.1 Styring og kontroll 20
3.3.2 Informasjonssikkerhet 21
3.3.3 Kontinuitetsledelse, kriseledelse og kriseløsning 21
3.3.4 Tilgangsstyring 22
3.3.5 Systemer for å avdekke hvitvasking og terrorfinansiering 22
3.3.6 Transaksjonsovervåking 23
3.3.7 Bankenes etterlevelse av rapporteringskrav til Bankenes sikringsfond 23

3.4 Verdipapirområdet 23
3.4.1 Hendelser innen verdipapirområdet 23
3.4.2 Konfigurering av testsystemer 24
3.4.3 Havari i lagringsløsninger 24
3.4.4 Retningslinjer for bruk av tredjeparter til test av sikkerhet 24
3.4.5 Dimensjonering og testing av kriseløsning 24
3.4.6 Organisering av systemeierskap for viktige forretningsløsninger 25
3.4.7 Andre forhold 25

3.5 Forsikring 25
3.5.1 Underrapportering av IKT-hendelser 25
3.5.2 Konfidensialitetsbrudd 25
3.5.3 Oppfølging av utkontraktert virksomhet 26
3.5.4 Oppfølging av sikkerhetsområdet 26
3.5.5 IKT-strategi 26

3.6 Revisjonsselskaper 27

3.7 Rapporterte hendelser i 2018 27
3.7.1 Statistikk over hendelser 27
3.7.2 Analyse av hendelsene som mål på tilgjengelighet 30

3.8 Utkontraktering 30
3.8.1 Melding om utkontraktering 30
3.8.2 Exit-bestemmelser 31
3.8.3 Skytjenester 31
3.8.4 Leverandørstyring 31
3.8.5 Uavhengig vurdering og revidering av leverandørens risikostyring og internkontroll 32

3.9 IKT-sikkerhet og digital kriminalitet 33
3.9.1 Sikkerhetskultur gjennom opplæring og involvering 34
3.9.2 Trender innen digitale angrep 34
3.9.3 Handlinger når angriper er på innsiden av nettverket 35
3.9.4 Manipulering av betaleren 35
3.9.5 Manipulering og digitale angrep ved bruk av kunstig intelligens 36
3.9.6 Informasjonslekkasje 36
3.9.7 Innsidetrussel 37
3.9.8 Tap av forretningskritiske data 39
3.9.9 Sårbarheter i maskinvare og fastvare 40
3.9.10 ID-tyveri 41

3.10 Rammeverk innen IKT og sikkerhet 41
3.10.1 Tilsynspraksis og regulatoriske forbedringer 41
3.10.2 Rammeverk for sikkerhetstesting 41
3.10.3 Rammeverk for sikkerhet 42
3.10.4 Swifts sikkerhetsprogram 43

3.11 Foretakets styringsmodell og forsvarslinjer for IKT-området 43
3.11.1 Styringsmodell 43
3.11.2 Foretakets tre IKT-forsvarslinjer 44

3.12 Risikostyring innen IKT-området 45

3.13 Kompetansesituasjonen på IKT-området i Norge 46

3.14 Geopolitiske forhold 47

3.15 Utviklingstrekk innenfor finansiell teknologi 48
3.15.1 Utviklingsmål 48
3.15.2 Open banking 49
3.15.3 Blokkjede 49
3.15.4 Kunstig intelligens 50

3.16 Teknologisk gjeld 50

3.17 Beskyttelse av persondata 50

3.18 Bankenes tilbud av kontanttjenester 51

3.19 Fellestiltak innen finansnæringen 52

4 AKTØRENES VURDERING AV RISIKOFAKTORER 54

4.1 Intervjuer med foretak og leverandører 54
4.1.1 Sosial manipulering 54

4.1.2 Svindel ved bruk av nære relasjoners BankID ... 54
4.1.3 Leveransepress, sikkerhet og reguleringer ... 54
4.1.4 Kompleksitet i løsningsporteføljene ... 55
4.1.5 Komplekse leveringskjeder ... 55
4.1.6 Flytting av driftssted ... 55
4.1.7 Digitale angrep ... 56
4.1.8 Kompetanse ... 56

4.2 Spørreundersøkelse om sårbarhet ... 56
4.2.1 Støtte for strategiske beslutninger ... 57
4.2.2 Beskyttelse av data ... 57
4.2.3 Drift ... 58
4.2.4 ID-tyveri ... 59
4.2.5 Interne misligheter ... 59
4.2.6 Hvitvasking ... 59

4.3 Nasjonale vurderinger av trusselbildet ... 60

5 RISIKOOMRÅDER ... 61

5.1 Finansiell infrastruktur ... 61

5.2 Foretakene ... 63

5.3 Foretakenes kunder ... 72

6 FINANSTILSYNETS OPPFØLGING ... 74

6.1 Sentrale områder for Finanstilsynets IKT-tilsyn ... 74

6.2 Arbeid med betalingssystemer ... 74

6.3 Oppfølging av hendelser ... 75

6.4 Beredskapsarbeid ... 75

6.5 Oppfølging av trusselbildet knyttet til digital kriminalitet ... 75

6.6 Forbrukervern ... 76

1 Innledning

Finanstilsynet utarbeider hvert år en risiko- og sårbarhetsanalyse (ROS-analyse) av finanssektorens bruk av IKT.

Formålet med rapporten er å beskrive risiko og sårbarhet, både med hensyn til finansiell stabilitet, det enkelte foretak og foretakenes kunder. Gjennom oppfølging av rapporterte hendelser, funn fra tilsyn og annen kontakt mot finansnæringen får Finanstilsynet god innsikt i foretakenes bruk av IKT, betalingsløsninger og aktuelle risikoområder.

Kapittel 2 oppsummerer rapporten.

Kapittel 3 presenterer Finanstilsynets funn, observasjoner og erfaringer fra tilsynsvirksomheten i 2018, herunder mottatte hendelsesrapporter og meldinger om nye og endrede betalingstjenester. Kapitlet omtaler også IKT-sikkerhet, digitale trusler og utvikling i trusselbildet, samt hvordan foretakene bør ruste seg mot digitale trusler. Teknologiske utviklingstrekk som antas å kunne få betydning for foretakenes bruk av IKT, er omtalt. Oppfølgingen av utkontrakteringsavtaler omtales også. 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 foretakets kunder, er også omtalt.

Kapittel 4 refererer foretakenes egne vurderinger av de mest framtredende truslene, innhentet gjennom spørreskjema og intervjuer. I tillegg er noen sentrale tjenesteleverandører intervjuet, og trussel- og risikovurderinger fra nasjonale sikkerhetstjenester og -myndigheter med særlig fokus mot finansnæringen refereres.

I kapittel 5 framkommer Finanstilsynets overordnede vurdering av risikobildet i 2018 på bakgrunn av funn, observasjoner og utviklingstrekk. De mest sentrale truslene mot, og sårbarheter i, foretakenes IKT-systemer og den finansielle infrastrukturen som kan ha betydning for finansiell stabilitet og velfungerende markeder, omtales. Sårbarheter og trusler rettet mot foretakets kunder omtales også.

Kapittel 6 beskriver områder som Finanstilsynet vil ha særskilt oppmerksomhet på framover.

En ordliste som forklarer ord og akronymer er vedlagt.

2 Oppsummering

2.1 Overordnet vurdering

Den norske finansielle infrastrukturen er robust. Det var ingen IKT-hendelser med konsekvenser for finansiell stabilitet i 2018. Foretakenes kunder opplevde om lag like mange alvorlige hendelser som i 2017, men tilgjengeligheten til tjenestene var samlet sett bedre enn i 2017.

Finanstilsynet har også i 2018 identifisert sårbarheter som kan lede til alvorlige hendelser. På det grunnlaget mener Finanstilsynet fortsatt at foretakene bør styrke arbeidet med IKT-sikkerhet, samt etablere tiltak for å redusere risikoen for alvorlige avvik.

Kompleksiteten i den tekniske infrastrukturen øker som følge av flere aktører, ny teknologi og bruk av teknologi på nye områder. Det gir økt risiko for hendelser. En høy endringstakt og kompliserte verdikjeder, med et stadig økende antall aktører, utfordrer foretakene i deres arbeid med å opprettholde god styring og kontroll, og opprettholde tilstrekkelig sikkerhet.

2.2 Finanstilsynets funn og observasjoner

2.2.1 Tilsynsområder

Betalingssystemer

Finanstilsynet observerte få alvorlige hendelser i betalingssystemene i 2018, både i omfang og varighet.

Betalingsområdet var også i 2018 preget av store endringer, blant annet ved fusjon av Vipps AS, BankAxept AS og BankID AS. Flere banker etablerte avtaler med globale foretak om betalingsløsninger. Bankene har også forberedt seg til nye regler som følge av det reviderte betalingstjenestedirektivet (PSD 2), som trådte i kraft i Norge 1. april 2019.

Omfanget av kortsvindel avtok ytterligere i 2018. Antall misbrukte kort gikk ned med om lag 46 prosent sammenlignet med 2017, mens tapene målt i kroner gikk ned med 36 prosent. Siden 2016 er tapene redusert med 55 prosent, fra 207 millioner kroner til 97 millioner kroner. Iverksatte tiltak, som blant annet bankenes overvåking for å hindre at kort blir misbrukt og strengere sikkerhetskrav fra blant

annet kortutstedere, synes å ha gitt betydelig effekt. Tapene som følge av svindel mot nettbank er lave, selv om de økte noe i 2018, til 20 millioner kroner.
Med PSD 2 følger det utvidede krav til foretakene om styring og kontroll med risiko og sårbarheten i betalingssystemene. Tilsynsarbeidet i 2018 avdekket manglende funksjonalitet i betalingstjenester og behov for bedre informasjon om tjenestenes funksjonalitet.

Bank

Finanstilsynet har gjennom tilsyn funnet mangler knyttet til foretakenes virksomhetsstyring på IKT-området. Manglene er blant annet knyttet til organisering av styrings- og kontrollfunksjoner, kompetanse og ressurstilgang og tilgangsstyring hos underleverandører. Det er videre avdekket mangler innen området kontinuitetsledelse og kriseløsninger.

Leverandører har ofte adgang til å opprette brukere i bankens systemer, noe som kan gi åpning for tilgang til bankens data. Finanstilsynet mener foretakene må bedre sine rutiner når det gjelder oppfølging av leverandørenes forvaltning av tilgangsrettigheter.

Finanstilsynet har sett flere eksempler på at kunder og betalingstransaksjoner ikke har blitt kontrollert fordi data ikke har kommet med i uttrekkene fra kildesystemene til antihvitvaskingssystemet.

Verdipapirområdet

Finanstilsynet har gjennom tilsyn avdekket svakheter ved foretaks kriseløsninger, der systemer som skal brukes i en krisesituasjon ikke har hatt tilstrekkelig kapasitet til å kunne overta relevant driftsbelastning.

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

Forsikringsområdet

Innrapporterte hendelser viser at forsikringsforetak har svakheter i egne testrammeverk, som har medført konfidensialitetsbrudd ved driftssetting av løsninger.

Finanstilsynet har gjennom tilsyn avdekket at foretak ikke har en tilstrekkelig oppfølging av adgangs- og tilgangsrettigheter for egne, og i noen tilfeller også leverandørers personell.

Regnskap og revisjonsområdet

Finanstilsynets har avdekket at selskaper har utkontraktert IKT-virksomhet uten at det foreligger skriftlige avtaler som i tilstrekkelig grad sikrer selskapets innsyn i, og styring og kontroll med den utkontrakterte virksomheten.

Det er også avdekket manglende retningslinjer for testing av forsvar mot digital kriminalitet, herunder angrep rettet mot selskapets systemer.

2.2.2 Hendelser

I 2018 ble det rapportert 189 IKT-relaterte hendelser til Finanstilsynet, noe som er omtrent det samme som i 2017. Fem av hendelsene var tilsiktede sikkerhetshendelser, dvs. digital kriminalitet. De resterende 184 var meldinger knyttet til operasjonelle hendelser.

Betalingssystemet og kunderettede løsninger var mer tilgjengelige for kundene i 2018 enn i 2017. Alvorlighetsgraden på hendelsene var også lavere, målt mot antall kunder som ble rammet, og hvor lenge avbruddene varte.

Mest oppmerksomhet fikk en hendelse i et datasenter, som resulterte i platelager-havari grunnet akustikkpåvirkning eller trykkendringer i datasenteret.

Det ble rapportert om flere hendelser grunnet for dårlig styring og kontroll med kunders bruker-identiteter, noe som resulterte i alvorlige konfidensialitetsbrudd. Det ble også rapportert om en hendelse som skyldtes bruk av robot for utfylling av brev, hvor brevene ble sendt til feil kunder.

Enkelte foretak rapporterte om avdekkede sikkerhetshull, uten at disse nødvendigvis hadde blitt utnyttet i ondsinnet hensikt.

2.2.3 Utkontrakteringsmeldinger

Det ble i 2018 behandlet 161 meldinger om utkontraktering, mot 86 meldinger i 2017.

Meldingene viser en klar tendens til økt bruk av skytjenester. Finanstilsynets inntrykk er at foretak som tar i bruk skytjenester, i hovedsak foretar nødvendige risikovurderinger, at sikkerhetskrav søkes ivaretatt og at det er tilstrekkelig oppmerksomhet knyttet til oppfølging av drift og sikkerhet i den utkontrakterte virksomheten.

Foretakene må gjennom sin leverandørstyring sikre nødvendig styring og kontroll over utkontraktert virksomhet. Foretakene må derfor ha evne og kompetanse til å ivareta dette kravet.

2.2.4 IKT- og informasjonssikkerhet

Finansforetakene observerer at den uønskede aktiviteten (digital kriminalitet) mot deres tekniske infrastruktur og systemer øker betydelig fra år til år. Samtidig erfarer Finanstilsynet at foretakene i økende grad er oppmerksomme på et trusselbilde som er i kontinuerlig endring. Foretakenes digitale forsvar forbedres løpende, herunder overvåkingen av den tekniske infrastrukturen og systemene. Etablering av et tilstrekkelig digitalt forsvar er krevende.

Digitale angrep avverges som oftest før de får konsekvenser for foretaket. Det har til nå ikke vært sikkerhetshendelser innen finansnæringen med konsekvenser for finansiell stabilitet.

Ved målrettede angrep mot finansforetak i andre land, har motivet først og fremst vært økonomisk vinning. Manipulering av betaleren gjennom en kombinasjon av digital og sosial manipulering lykkes i størst grad, og øker derfor i omfang.

Foretakene har i hovedsak arbeidet med å sikre sine nettverk mot angrep utenfra. Foretakenes evne til å oppdage og fjerne uønskede aktører på innsiden må også vies oppmerksomhet.

Manglende klassifisering av informasjon medfører risiko for at informasjon ikke omfattes av beskyttende tiltak, og konfidensiell informasjon kan derfor komme på avveie.

Digitale angrep kan rokke ved tilliten til finansforetak og finansiell stabilitet, og er en stadig økende trussel. EU-kommisjonen og de europeiske tilsynsmyndighetene EBA, ESMA og EIOPA har som mål å harmonisere og etablere minimumskrav for IKT-sikkerhet for finansnæringen. Disse institusjonene peker også på behovet for en samordning av regelverk og testrammeverk for å teste robustheten i foretakenes digitale forsvarsverk. Dette er et område som det vil arbeides videre med fra tilsynsmyndighetenes side.

2.2.5 Utviklingstrekk innenfor finansiell teknologi

Utviklingen innenfor finansiell teknologi drives av både nye og eksisterende foretak. Foretakene søker kontinuerlig å forenkle og forbedre sine IKT-løsninger. Samtidig øker kompleksiteten og sårbarheten i den samlede tekniske infrastrukturen som følge flere aktører, ny teknologi, flere tjenester, samt en generelt høy endringstakt.

Foretak som tar i bruk kunstig intelligens (AI) bør etablere en styringsmodell som legger nødvendige føringer for bruk, og som forankres og godkjennes av foretakets ledelse og styre.

2.2.6 Styring av IKT-virksomheten

Foretakene må etablere en fungerende styringsmodell for IKT-virksomheten i tråd med prinsippet om tre forsvarslinjer; operativ ledelse, risikostyring og compliance, og internrevisjon. Videre må foretakene etablere god risikostyring innen IKT-virksomheten, med bred involvering i foretaket og en god risikoforståelse.

Tilstrekkelig IKT-kompetanse er en utfordring for foretakene. Det er risiko for at finansnæringen ikke vil få dekket sitt framtidige kompetansebehov innen kritiske områder. Det kan øke avhengigheten av utenlandske leverandører ytterligere i årene som kommer, og gi nye sårbarheter og økt risiko. Finanstilsynet legger vekt på at foretakene ved utkontraktering til utlandet må etablere beredskap som innebærer at kritiske IKT-tjenester kan overtas og utføres av personell i Norge eller i andre land, dersom leverandører i utlandet som følge av geopolitiske forhold, ikke vil være i stand til å utføre disse tjenestene.

2.3 Foretakenes vurderinger

Foretakene vurderer følgende trusler som de viktigste:

- sosial manipulering der angriperen kan få uautoriserte tilganger og misbruker disse
- svindel foretatt av familiemedlemmer, eksempelvis ved bruk av BankID
- leveransepress, både på grunn av mange nye reguleringer og kundekrav
- økt kompleksitet i systemporteføljene
- mange leverandører involvert i tjenesteleveranser
- bytte og flytting av driftssted
- digitale angrep
- mangel på kompetanse på viktige IKT-områder

Ifølge foretakene synker risikoen knyttet til dårlig datakvalitet og manglende beskyttelse av ustrukturerte data. Dette kan ha sammenheng med det arbeidet foretakene har gjort i forbindelse med implementeringen av datalagringsdirektivet (GDPR).

Foretakene mener et økende antall leverandører, og underleverandører, i verdikjedene utgjør en risiko som følge av mer kompleks infrastruktur og samhandling. Omfanget av endringer og nye regulatoriske krav kan redusere foretakenes evne til å levere på tid og med nødvendig kvalitet. Tendensen til avtakende risiko knyttet til mangler i organisering, stillingsbeskrivelser, rapportering og kontroll, har stoppet opp.

Foretakenes vurdering av risiko knyttet til beskyttelse av sensitive data viser omtrent det samme bildet som i 2017.

Det er Finanstilsynets vurdering at foretakene har fått bedre kontroll med utlevering av brukeridentitet og passord til kunder og medarbeidere. Risikoen for at en angriper tar over en brukeridentitet og misbruker denne, anses dermed noe mindre enn tidligere.

Risikoen for hvitvasking er redusert som følge av forbedringer i IT-systemenes evne til å samle relevant informasjon om kunder, kunderelasjoner og kundeadferd som grunnlag for kontroller.

Samlet sett synes foretakenes vurdering av risikoen å være svakt økende i 2018, slik den også var i 2017 og 2016.

2.4 Aktuelle risikoområder

Finansiell infrastruktur

Finanstilsynet mener den norske finansielle infrastrukturen er robust. Det var ingen IKT-hendelser med konsekvenser for finansiell stabilitet i 2018, selv om det var én kritisk hendelse i sentral infrastruktur i

betalingssystemet og hendelser som gjorde betalingsløsninger utilgjengelige i perioder. Samlet sett var stabiliteten i 2018 bedre enn i 2017, og på linje med 2016.

Foretakene

Finanstilsynet vurderer sårbarheter i foretaks operative drift, tilgangsstyring, kontinuitetsledelse og kriseløsninger, håndtering av konfidensiell informasjon og forsvarsverk mot digital kriminalitet, som de mest sentrale truslene knyttet til foretakenes bruk av IKT. Alle disse truslene vurderes å ha middels til høy risiko.

Sårbarheter knyttet til foretaks leverandørstyring, endringsstyring, styringsmodell og forsvarslinjer knyttet til IKT-virksomheten, samt sårbarheter knyttet til geopolitiske forhold og IKT-kompetanse i Norge, er også trusler knyttet til foretakenes bruk av IKT. Disse vurderes å ha middels risiko.

Foretakenes kunder

Den økte digitaliseringen har medført at foretakenes kunder har måttet ta i bruk digitale identifiserings- og autoriseringsløsninger som ofte består av blant annet et passord eller en kode som må huskes. Dette er en utfordring for mange, og ofte blir passord skrevet ned. Passord og koder som blir delt eller stjålet utgjør en betydelig risiko for misbruk, med i verste fall store økonomiske konsekvenser for den skadelidende.

Svindel rettet mot bankkunder, som kjærlighetssvindel, investeringssvindel, falske fakturaer og kunder som blir forledet til å gi fra seg sensitiv informasjon, utgjør en vesentlig større risiko for den enkelte kunde, enn digital kriminalitet rettet mot foretakene i finanssektoren eller bruken av foretakenes løsninger.

3 Finanstilsynets funn og vurderinger

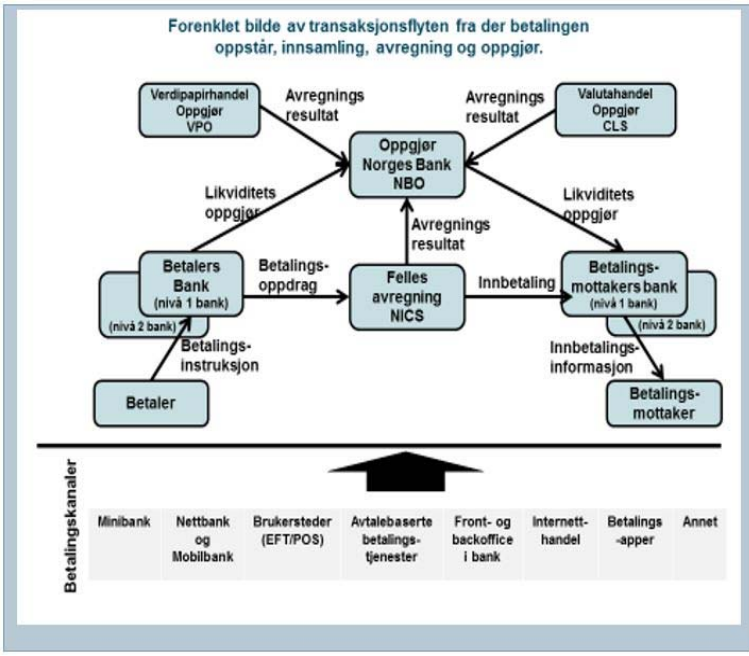
3.1 Betalingssystemer

3.1.1 Generelt om betalingssystemer

Effektive, robuste og stabile betalingssystemer er grunnleggende for finansiell stabilitet og velfungerende markeder. Norsk infrastruktur for betaling er blant verdens mest effektive og rimelige[1].

Betalingssystemer og -tjenester reguleres gjennom lover og forskrifter, samt gjennom finansnæringens selvregulering forvaltet av Finans Norge og Bits. Blant annet som følge av det reviderte betalingstjenestedirektivet (PSD 2), er det fastsatt en rekke regelverksendringer med virkning fra 1. april 2019 som vil berøre betalingssystemene. De mest sentrale endringene berører lov om betalingssystemer, forskrift om systemer for betalingstjenester og forskrift om betalingstjenester.

Figur 1 Transaksjonsflyten i det norske betalingssystemet



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

Kilde: Finanstilsynet

[1] Finansiell infrastruktur 2018. Rapport fra Norges Bank
Bits: Felles evaluering av mulig deltakelse i P27-initativet avsluttes i Norge

3.1.2 Styring og kontroll med risiko og sårbarhet i betalingssystemene

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

Regelverket stiller flere krav til styring og kontroll med betalingssystemene[2], herunder med operasjonell og sikkerhetsmessig risiko. Kravene vil gjelde både for eksisterende foretak som leverer betalingstjenester, og for nye betalingstjenesteforetak.

Tilbydere av betalingstjenester skal gjennomføre risiko- og sårbarhetsvurderinger før en ny betalingstjeneste lanseres og ved hendelser eller endringer av betydning for sikkerhetsnivået. På bakgrunn av risiko- og sårbarhetsvurderinger, skal det etableres tiltak for å sikre nødvendig konfidensialitet, integritet og tilgjengelighet. Foretakene skal sikre at deres systemer er i tråd med regelverk, avtaler og interne rutiner, og er ansvarlige for at tjenesten i sin helhet (ende-til-ende) er beskyttet gjennom logiske og fysiske sikringstiltak.

Datatrafikk i elektroniske betalingstjenester skal overvåkes for å sikre tilstrekkelig sikkerhetsnivå og kunne avdekke og hindre uautorisert bruk av tjenesten. Betalingstjenestetilbydere skal minst årlig rapportere statistikk om svindel knyttet til betalingstjenestene til Finanstilsynet.

Betalingstjenestetilbyderne skal ha systemer og kontrollmekanismer for operasjonell og sikkerhetsmessig risiko knyttet til tjenestens ytelse, samt effektive framgangsmåter for å håndtere hendelser, inkludert alvorlige operasjonelle hendelser og sikkerhetshendelser. Minst årlig skal betalingstjenestetilbydere gi Finanstilsynet en samlet vurdering av operasjonell risiko og sikkerhetsrisiko knyttet til tjenestene, samt en vurdering av egne tiltak.

Finanstilsynet observerer at endringstakten er høy, noe som i seg selv gir økt risiko. Endringene må ses i lys av økt konkurranse som følge av teknologiske framskritt, regulatoriske endringer og kunders forventninger. 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. Det forventes at tilbydere av betalingskontoer vil nedlegge et betydelig arbeid i å sikre en kvalitet på sine nye grensesnitt som fjerner behovet for at eksisterende kundegrensesnitt er tilgjengelig som fallback-løsning. Finanstilsynet er kjent med stor interesse fra fintech-foretak når det gjelder å utnytte de nye mulighetene som PSD 2 gir når det gjelder tilgang til betalingskonto.

Finanstilsynets erfarer at foretakene nedlegger et betydelig arbeid i sine kriseløsninger, også omtalt som reserveløsninger eller beredskapsløsninger, for å redusere sårbarheten ved avvik i betalingsformidlingen. Omfanget av hendelser i 2018 var på nivå med 2017, men tilgjengeligheten til foretakenes betalingstjenester var samlet sett bedre i 2018 enn året før. Imidlertid viser hendelsene at foretakene fortsatt kontinuerlig må forbedre kvaliteten i sine endringsprosesser og betalingstjenestenes

[2] Jf. forskrift om systemer for betalingstjenester

kriseløsninger, både for å redusere antall hendelser og redusere negative konsekvenser ved en hendelse.

God informasjon til kundene ved hendelser er viktig. Dersom en hendelse påvirker eller kan påvirke kundenes økonomiske interesser, skal tilbyderen uten ugrunnet opphold underrette kundene. Meldingen skal omtale tiltak som kundene selv kan iverksette.

Finanstilsynet understreker styrets og ledelsens ansvar for at foretaket har rutiner og systemer som sikrer stabile driftsløsninger og effektive kriseløsninger. 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. 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.

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 2018 mottok Finanstilsynet tolv meldinger om nye eller endrede systemer for betalingstjenester. Meldingene var knyttet til blant annet endringer i nettbanker, endringer i betalingskortløsninger, PSD 2-grensesnitt (API-er) og Vipps-tjenester.

3.1.4 Utvikling innen betalingstjenester og mobile betalingsløsninger

Utviklingstrekk

Nyutviklingen innen betalingstjenester kommer 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.

Ved inngangen til 2018 deltok et flertall av bankene som opererer i det norske markedet i Vipps-samarbeidet. Vipps er den dominerende mobile betalingsløsningen i Norge, men kan i liten grad benyttes for betaling i fysiske butikker. Gjennom Vipps kan det betales med konto-til-konto-betalinger

(foreløpig kun for person-til-person-betalinger), ved bruk av infrastruktur for straksbetalinger[3], eller kortløsningene til blant annet MasterCard og Visa. Vipps lanserte i 2018 mulighet for betaling av eFakturaer.

For å styrke konkurranseevnen overfor internasjonale aktører, fusjonerte Vipps AS, BankAxept AS og BankID AS i 2018. Det nye selskapet viderefører navnet Vipps AS.

Mange brukersteder har tidligere valgt å ikke åpne for kontaktløse betalinger som følge av at denne teknologien kun var tilgjengelig ved bruk av de internasjonale betalingsordningene til Visa og MasterCard. BankAxept AS etablerte i 2017 støtte for kontaktløs betaling ved bruk av fysiske kort og gjennom 2018 har bankene i stort omfang rullet ut betalingskort med støtte for kontaktløse betalinger, også for BankAxept. Antall brukersteder som aksepterer kontaktløse betalinger har økt betydelig og kundenes betalingsvaner endrer seg gradvis.

Aera Payment & Identification AS (Aera) fortsatte i 2018 sitt arbeid med å etablere en åpen betalingsplattform som skal kunne akseptere alle betalingstyper[4] på tvers av kanaler (netthandel, mobilhandel og i butikk)[5] og være integrert med dagligvarehandelens butikkløsninger og lojalitetsprogrammer.

Bruk av biometriske kjennetegn i forbindelse med autentisering og betaling øker, og flere foretak har tatt i bruk både fingeravtrykk ("touch") og ansiktsgjenkjenning for innlogging på mobile løsninger.

Flere norske banker har etablert bilaterale avtaler som muliggjør ytelse av tjenester tilsvarende PSD 2s betalingsfullmaktstjenester og kontoinformasjonstjenester for betalingskontoer i avtalebankene. Det er også banker som har etablert bilaterale avtaler som går utover de betalingstjenestene som følger av PSD 2, gjerne omtalt som "Open Banking". Se også punkt 3.15.2.

I 2018 inngikk en rekke banker samarbeid med Apple slik at deres betalingskort kunne benyttes i Apple Pay[6]. Det var også en del banker som inngikk avtale med Google slik at deres betalingskort kan benyttes ved bruk av Google Pay[7]. Flere banker har i 2018 også etablert avtaler som gjør det mulig å betale med klokker (Garmin Pay og Fitbit Pay).[8]

Høsten 2017 ble det mulig å betale med Alipay for kinesiske turister i Norge. I 2018 inngikk Alipay et samarbeid med Nets slik at norske butikker kan ta imot betalinger med Alipay, på lik linje som

[3] https://www.bits.no/bank/straksbetalinger/
[4] BankAxept, Visa/Visa, Electron, MasterCard/Maestro, Diners, American Express, JCB, China Union Pay, Apple Pay, Samsung Pay og Android Pay, Vipps, Alipay
[5] https://aera.id/betaling/
[6] https://www.tek.no/artikler/nordea-melder-om-ekstrem-interesse-for-apple-pay/440510
[7] https://www.dinside.no/mobil/na-kommer-google-pay-til-norge/70394529
[8] https://www.dinside.no/mobil/na-kan-dnb-kunder-betale-med-klokka---men-kanskje-ikke-den-du-onsker/70537330

betalinger med Visa og Mastercard. Teknologien er basert på QR-koder. Alipay har også inngått en avtale med Vipps for å gjøre Alipay-betalinger enklere.

PSD 2 stiller krav til sterk kundeautentisering og sertifikatløsninger. Buypass[9] vil tilby elektroniske sertifikatløsninger i tråd med regelverket.

Ved handel på Internett finnes det i dag flere forskjellige betalingsmåter, som betalingskort, fakturabetaling gjennom en rekke betalingstjenesteleverandører eller fakturainnkrevingsaktører, eller betaling via postoppkrav. Flere tjenesteleverandører tilbyr såkalt "checkout"-løsninger, dvs. er totalleverandør av alle typer betalinger. Med PSD 2 åpnes det opp for at betalingstjenestetilbydere også kan tilby konto-til-konto-betalinger.

Regler tilsvarende PSD 2 trådte i kraft 1. april 2019

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 betalingskonto for å yte betalingsfullmaktstjenester og kontoinformasjonstjenester framgår av forskrift for systemer for betalingstjenester, samt regler i samsvar med delegert forordning 2018/389 "Regulatory technical standards for strong customer authentication and common and secure open standards of communication", som skal gjelde fra 14. september 2019 også i Norge.

Betalingskontotilbydere arbeider med å etablere grensesnitt (API-er) som gjør det mulig for tredjepartsaktører å tilby nye tjenester basert på tilgang til betalingskonto. Det forventes at alle betalingskontotilbydere i Norge innen 14. september 2019 vil ha etablert dedikerte grensesnitt og søkt om godkjenning for unntak fra fallback-løsning.

Gjennom et åpent betalingsmarked, og etablering av offentlige API-er mot foretakenes infrastruktur, vil nye og eksisterende aktører med konsesjon kunne tilby de nye betalingstjenestene betalingsfullmakt[10] og opplysningsfullmakt[11]. Flere IKT-tjenesteleverandører har etablert konsentratorløsninger som etablerer tekniske løsninger for å koble seg opp mot kontotilbyderes API-er. Koblingspunktene selges til betalingsforetak som ønsker å tilby betalingsfullmaktstjenester og kontoinformasjonstjenester.

Når PSD 2 nå er trådt i kraft i Norge, forventer Finanstilsynet en moderat pågang av konsesjonssøknader fra nye aktører, tilsvarende den observerte utviklingen i EU-landene. PSD 2 stiller flere krav til betalingsforetak ved søknad om konsesjon enn PSD 1, men flere av kravene var allerede innarbeidet i Norge. Det gjelder blant annet krav til rapportering av hendelser, krav om risikoanalyser knyttet til betalingstjenestene, krav til sikkerhet og krav til sterk kundeautentisering. I tillegg har det vært krav om svindelrapportering for banker.

[9] https://www.tu.no/filer/EVENT/Digital2017_presentasjoner/Mads_Henriksveen_Buypass.pdf
[10] Payment Initiation Service Providers (PISP). Aktører som kan initiere betalinger på vegne av kunde
[11] Account Information Service Providers (AISP). Aktører som kan hente informasjon fra bankkonto på vegne av kunde

Som følge av gjennomføringen av PSD 2 i norsk rett, harmoniseres betalingstjenestetilbydernes forpliktelser knyttet til rapportering av hendelser og sikkerhetshendelser med EBAs retningslinjer om hendelsesrapportering. I tillegg skal betalingstjenestetilbyderne halvårlig rapportere svindel knyttet til betalingstjenestene og årlig rapportere samlet vurdering av operasjonell risiko og sikkerhetsrisiko, samt vurdere tilbydernes tiltak.

Etter at regelverket trådte i kraft, har utenlandske aktører som melder grensekryssende virksomhet for nye betalingstjenester rett til tilgang til betalingskonto hos banker som opererer i Norge. Finanstilsynet forventer at flere internasjonale aktører vil etablere seg med nye betalingstjenester i det norske markedet. En rekke globale aktører har allerede meldt grensekryssende virksomhet til Norge, mens andre foreløpig kun har etablert virksomhet i et eller flere EU-land.

3.1.5 Tap som følge av svindel med betalingstjenester

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

Tapstall i Norge for kortbruk

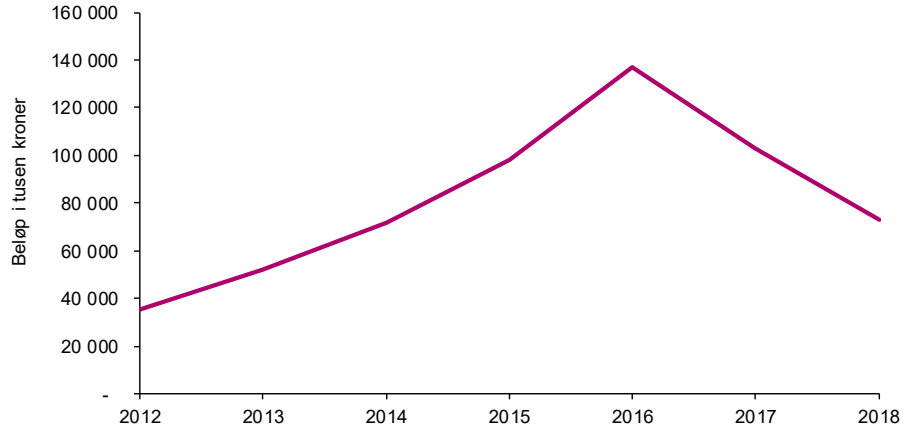
Samlet tap på kortbetalinger ble redusert med 36 prosent i 2018, og er mer enn halvert sammenlignet med 2016. Antallet misbrukte kort ble redusert med 46 prosent fra 2017 til 2018.

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

Svindeltype betalingskort	2012	2013	2014	2015	2016	2017	2018
Misbruk av kortinformasjon, Card-Not-Present (CNP) (Internett-handel m.m.)	35 701	51 954	72 056	98 410	137 015	102 908	72 909
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort i Norge	2 308	762	524	2 670	1 360	483	3 098
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort utenfor Norge	55 869	51 534	51 685	48 447	41 762	17 452	6 308
Originalkort tapt eller stjålet, misbrukt med PIN i Norge	28 128	21 274	21 266	18 875	12 857	10 194	4 972
Originalkort tapt eller stjålet, misbrukt med PIN utenfor Norge	8 544	9 570	13 071	14 224	10 223	9 663	4 699
Originalkort tapt eller stjålet, misbrukt uten PIN	4 603	4 949	5 510	6 033	3 286	4 891	618
Totalt	**135 153**	**140 043**	**164 113**	**188 660**	**206 503**	**145 591**	**92 604**

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

De to største tapskategoriene for betalingskort; tap ved Internetthandel og tap ved misbruk av falske kort utenfor Norge, har sunket mest. Finanstilsynet antar at den store nedgangen i tap på betalingskort ved Internetthandel kan forklares med strengere regelverk, økte krav fra kortutstedere, kortinnløsere og brukersteder til sterk autentisering av kortholder med bruk av sikkerhetsverktøy som 3D Secure[12], foretakenes preventive tiltak som overvåking av kortbruken og lignende. Reduksjonen i tap ved misbruk av falske kort utenfor Norge skyldes at stadig færre land bare bruker magnetstripen og ikke databrikke (chip). Alle norske kort utstedes med databrikke, som brukes ved betalingene. Svindlerne klarer ikke kopiere databrikken til falske kort.

Kostnader forbundet med kortsvindel

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

Kostnader ved svindel med betalingskort	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
Antall kort rammet av misbruk	20 332	22 531	38 541	44 900	68 162	65 024	34 999
Samlede direkte tap, jf. tabell 1	135 153	140 043	164 113	188 660	206 503	145 591	92604
Saksbehandlerkostnader hos kortutsteder (2 250 kroner per kort)	45 747	50 695	86 717	101 025	153 365	146 304	78 748
Forbrukerkostnader (1 000 kroner per kort)	20 332	22 531	38 541	44 900	68 162	65 024	34 999
Samlet beregnet kostnad	**201 232**	**213 269**	**289 371**	**334 585**	**428 030**	**356 919**	**206 351**

Kilde: Finanstilsynet

[12] Kortselskapenes standard for å identifisere og beskytte kjøpere og selgere når kort benyttes for å betale via Internett.

Finanstilsynet anslag for samlede kostnader forbundet med stjålet kortinformasjon er basert på summen av årlige direkte tap ved bruk av betalingskort og en vurdert gjennomsnittlig saksbehandlerkostnad for kortutsteder per misbrukt kort, og inkluderer eventuelle tap for brukerstedet, kortinnløser, kortutsteder og korteier. I tillegg er det forutsatt et kostnadsbeløp per kort knyttet til at kunden også har kostnader forbundet med stjålet kortinformasjon.

Tapstall knyttet til bruk av nettbank

Tapstall knyttet til bruk av nettbank økte i 2018. Kriminelle klarte ved bruk av trojaneren Retefe å gjennomføre noen falske transaksjoner. De fleste forsøkene på å gjennomføre falske transaksjoner lyktes bankene imidlertid å stoppe.

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

Svindeltype – nettbank	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
Angrep ved bruk av ondartet programkode på kundens PC eller sikkerhetsmekanisme (trojaner)	5 064	1 327	552	3 055	2	727	1 304
Tapt/stjålet sikkerhetsmekanisme	3 367	1 285	6 655	963	8 758	1 892	874
Phishing og falske BankID-brukersteder	10		539	5815	2 428	2 057	16 384
Annet/ukjent	358	779	3 474	2 715	7 444	2 911	1 624
Totalt	**8 799**	**3 391**	**11 220**	**12 548**	**18 632**	**7 587**	**20 186**

Kilder: Finanstilsynet og Bits

Tap ved svindel gjennom sosial manipulering

Det er innhentet tall for 2018 fra bankene over registrerte tap ved svindel gjennom sosial manipulering. Tapene er brutt ned på type sosial manipulering. Kategoriseringen er noe usikker, da mange banker i utgangspunktet ikke har inndelt tapene i spesifiserte typer, og at svindlene i noen tilfeller er en kombinasjon av svindeltyper. Tallene viser at det er ved sosial manipulering at de kriminelle har størst utbytte. I 2018 var tapene på i underkant av 300 millioner kroner, nesten tre ganger så høyt som tap ved svindel av betalingskort og nettbank til sammen. Ikke alle svindler som følge av sosial manipulering blir meldt til banken, og de faktisk tapene er antakelig vesentlig større.

Tap ved svindel gjennom sosial manipulering er tap for kundene, ikke for bankene. Kundene som er svindlet kontakter ofte banken for å stanse transaksjoner og for å få tilbakeført beløpet. Finanstilsynet er kjent med at banker varsler kunder der banken, basert på kunnskap om kunden, identifiserer gjentagende unormale transaksjoner for kunden.

Ofrene for sosial manipulering kan også forledes til å utføre tjenester for svindlerne. For eksempel kan kunden ledes til å stille sin konto til disposisjon for pengeoverføringer, og dermed bidra til å skjule overføringer av midler som stammer fra ulovlig virksomhet til mottakere i utlandet.

Tabell 4 Tap ved manipulering av betaleren (beløp i hele tusen kroner)

Type svindel i 2018	**Antall**
Betaling for å leie et objekt mottager av pengene ikke eier	948
Innskudd etter løfter om store utbetalinger senere	9 091
Kjærlighet	88 191
Investeringer i falske selskaper	92 073
Betaling for varer som ikke leveres	11 972
Endret mottakerkonto	8 606
Direktørsvindel	33 913
Falsk faktura	32 982
Andre/nye typer	19 593
TOTALT	**297 369**

Kilder: Finanstilsynet og Bits

3.2 Betalingsforetak

Finanstilsynet følger opp betalingsforetakene i henhold til krav i IKT-forskriften, forskrift om systemer for betalingstjenester, EBAs retningslinjer for sikkerhet i Internettbetalinger og hvitvaskingsregelverket. Gjennom tilsyn med betalingsforetak i 2018 påpekte Finanstilsynet mangelfull informasjon om funksjoner i betalingstjenesten og manglende valgmuligheter. Kunden kan få en følelse av å ikke ha kontroll med egne data og betalinger når kunden ikke blir tydelig informert om ny funksjonalitet og ikke selv kan velge å ta i bruk ny funksjonalitet i betalingstjenesten.

Tilsyn med betalingsforetak har også omfattet tilsyn med etterlevelsen av hvitvaskingsregelverket. Mange betalingsforetak har både brukersteder og sluttbrukere som kunder. Risikoen for hvitvasking og behov for forsterkede kundetiltak er ofte størst på brukerstedssiden. Finanstilsynet har avdekket svakheter i betalingsforetaks kundekontroll av brukersteder.

3.3 Bank

3.3.1 Styring og kontroll

Finanstilsynet har identifisert flere mangler når det gjelder bankenes etterlevelse av IKT-forskriften, blant annet med hensyn til virksomhetsstyring som omfatter IKT-området. Banknæringens styringsmodell baserer seg i stor grad på en anerkjent modell bestående av tre forsvarslinjer; operativ ledelse, risikostyring og compliance, og internrevisjon, jf. punkt 3.11.

Finanstilsynets funn kan i hovedsak knyttes til tre områder; mangler i hvordan styrings- og kontrollfunksjoner er etablert, mangelfull organisering og uklare rapporteringslinjer, og manglende sikring av tilstrekkelig kompetanse og ressurser.

Det er særlig utkontrakterte tjenester som peker seg ut med størst potensiale for forbedring. Det er viktig å understreke at det er bankenes egne vurderinger som skal ligge til grunn for rapportering av arbeid knyttet til styring og kontroll i egen virksomhet, jf. punkt 3.8.

I Risiko- og sårbarhetsanalysen for 2017 pekte Finanstilsynets på at foretakene må sikre at risikoer i hele verdikjeden identifiseres, vurderes og håndteres. I tillegg må bankene ha nødvendig kompetanse og kapasitet til å ivareta det sikkerhetsnivået som er nødvendig for å opprettholde forsvarlig drift. Vurderingen står fortsatt ved lag i 2018. Se også punkt 3.13.

3.3.2 Informasjonssikkerhet

Informasjonssikkerhet er et område som foretakene gir stor oppmerksomhet. For å ha en metodisk tilnærming til informasjonssikkerhet, er en etablert sikkerhetspolicy viktig. Foretakets ledelse har ansvaret for at sikkerhetspolicyen utarbeides i tråd med de forretningsmessige mål og regulatoriske krav som stilles.

Sikkerhetspolicyen skal gjenspeile foretakets krav til informasjonssikkerhet. Det vurderes som viktig at ansvaret for informasjonssikkerhet beskrives. Videre skal det beskrives hvordan oppfølgingen skal gjennomføres og hvilke krav som stilles til rapportering. Foretakets ledelse er ansvarlig for at innholdet i policyen samsvarer med foretakets krav.

3.3.3 Kontinuitetsledelse, kriseledelse og kriseløsning

Kontinuitetsledelse, også kalt "Business Continuity management" (BCM), i et foretak er en sentral og viktig funksjon for i størst mulig grad å sikre at foretaket er forberedt og i stand til å håndtere en alvorlig situasjon, ofte definert som en krise eller katastrofe (forhold som medfører at foretaket ikke er i stand til å opprettholde sin normale aktivitet, enten for hele eller deler av foretakets virksomhet).

Kriseledelse er en sentral og viktig funksjon når en krise eller katastrofe inntreffer. Skillet mellom kontinuitetsledelse og kriseledelse er ikke alltid tydelig, men kriseledelsen anses som den funksjonen som har det overordnede og operative ansvaret for å lede foretaket gjennom en krise eller katastrofe. Ofte vil kriseledelsen være den som håndterer mer alvorlige situasjoner der liv og helse står på spill. Krise er et begrep som kan benyttes ved alvorlige IKT-hendelser. Katastrofer er i stor grad situasjoner som truer ansattes liv og helse.

Finanstilsynet har nylig gjennomført en omfattende spørreundersøkelse om kontinuitetsledelse og kriseløsninger rettet mot norske banker og internasjonale banker med filial i Norge. Undersøkelsen gir et bilde av hvordan bankene vil være i stand til å håndtere en alvorlig IKT-hendelse. Finanstilsynet konstater at foretakene i stor grad har etablert kriseløsninger, også omtalte som beredskapsløsninger eller reserveløsninger, som skal iverksettes dersom normal driftsløsning ikke er tilgjengelig. Det er imidlertid avdekket en del mangler som utgjør risiko for at foretak vil få utfordringer med å håndtere

en alvorlige IKT-hendelse. Dette gjelder blant annet mangler i styrende dokumenter, opplæring, trening, øvelse og test av kriseløsning. Undersøkelsen viser at foretakene i større grad bør rette oppmerksomhet mot kontinuitetsledelse og kriseløsninger, og dermed redusere risikoen for omfattende skader ved alvorlige hendelser.

3.3.4 Tilgangsstyring

Finanstilsynet har gjennom tilsyn vurdert foretakenes rutiner for styring av og kontroll med personells tilgang til og bruk av foretakets systemer. Ved denne type tilsyn undersøkes særlig foretakenes styring og kontroll med utvidede tilgangsrettigheter for egne medarbeider, og for personell hos foretakets IKT-leverandører.

Finanstilsynet er kjent med at leverandører ofte har adgang til å opprette brukere med utvidede rettigheter i foretakets systemer. Dette er rettigheter som utgjør en særskilt risiko ved at personell har tilgang til å endre på data, hente ut data eller påvirke driften av systemet. Uautoriserte handlinger kan skjules ved at den som utfører handlingene selv kan slette logginformasjon.

Personell som skal gis utvidede rettigheter bør underlegges særskilt bakgrunnssjekk før tildeling. Det er også viktig at det etablere nøye kontroll med hvem som er gitt tilgangene, og om behovet samsvarer med oppgavene som skal utføres. Det bør være et krav hos det enkelte foretak at utvidede rettigheter jevnlig revideres. Finanstilsynet er kjent med at foretak styrker kontrollen ved bruk av særskilte tilgangsstyringssystem for utvidede rettigheter, et tiltak som etter Finanstilsynets vurdering er nødvendig for å etablere god styring og kontroll.

For øvrige tilganger konstaterer Finanstilsynet at det er utfordrende for ledere å forstå og tolke detaljerte oversikter som viser medarbeideres tilganger og autorisasjonsnivå. Dette medfører at kvaliteten på gjennomgangen svekkes, og at medarbeidere har tilganger utover deres autorisasjonsnivå. Systemstøtte for rollebasert tilgangsstyring skal sørge for at medarbeider kun gis tilgang til systemer og informasjon som er nødvendig i utførelsen av arbeidet. Dette er et særdeles viktig risikoreduserende tiltak.

3.3.5 Systemer for å avdekke hvitvasking og terrorfinansiering

Gode systemer for elektronisk transaksjonsovervåking (antihvitvaskingssystemer) er helt nødvendig for at foretakene skal kunne etterleve hvitvaskingsloven § 25 'Undersøkelsesplikt' og § 26 'Rapporteringsplikt', samt for å etterleve kravene til slike systemer i § 38. Finanstilsynet har de siste årene gjennomført flere hvitvaskingstilsyn enn tidligere, og har observert en dreining mot mer gjennomarbeidede scenarier for å avdekke hvitvasking og terrorfinansiering. I transaksjonsovervåkingen er det imidlertid fortsatt en høy andel treff som ikke er reelle, såkalte falske positive treff, og det er ofte en del scenarier uten treff. Finanstilsynet mener at dette skyldes at arbeidet med å identifisere og utvikle scenarier, som igjen er grunnlaget for hvordan transaksjonene kontrolleres gjennom regler i antihvitvaskingssystemet, ikke er gitt nødvendig prioritet av foretakenes styre og ledelse. Det er fortsatt et stort potensiale for å videreutvikle scenarier som vurderer kundeforholdet under ett, og som kan avdekke avvik i forhold til kundens forventede adferd.

Finanstilsynet er gjennom hendelsesrapporteringen informert om at en del kunder og transaksjoner i perioder ikke har blitt kontrollert fordi de ikke har kommet med i uttrekk fra kildesystemet, der transaksjonen genereres, til antihvitvaskingssystemet. Endringer i kildesystemene, uttrekket til antihvitvaskingssystemet, antihvitvaskingssystemet eller driften har vist seg å kunne føre til mangelfulle uttrekk som ikke har blitt oppdaget i testene av endringen. Finanstilsynet vil i kommende hvitvaskingstilsyn legge vekt på at foretakene har gode rutiner for å kontrollere at uttrekkene av data til antihvitvaskingssystemet er komplette.

3.3.6 Transaksjonsovervåking

Analyse av transaksjonsmønstre for å avdekke uautoriserte transaksjoner er i stor grad basert på regler som er definert i overvåkingssystemene. Kriminelle vil kunne teste ut hvilke regler som gjelder og dermed omgå disse. I tillegg viser det seg at en stor andel av identifiserte avvik ikke er en følge av kriminelle handlinger. Transaksjonsovervåkingen vil kunne bli betydelig forbedret ved bruk av maskinlæring (ML). Ved bruk av ML vil hver kundetransaksjon kunne bidra til å utvikle algoritmen i systemet, slik at den blir "smartere" og gir mer nøyaktige resultater. Med omfanget av nye aktører som antas å følge av PSD 2, er Finanstilsynets vurdering at bruk av mer avanserte overvåkingsverktøy vil være et viktig risikoreduserende tiltak i arbeidet med å bekjempe kriminell aktivitet rettet mot bankens kunder, samt også hvitvasking og terrorfinansiering.

3.3.7 Bankenes etterlevelse av rapporteringskrav til Bankenes sikringsfond

Finanstilsynet, i samarbeid med Bankenes sikringsfond, gjennomførte også i 2018 tilsyn for å vurdere bankenes etterlevelse av krav til datasystemer for rapportering til Bankenes sikringsfond om banken blir satt under offentlig administrasjon. Datasystemene har vært testet gjennom flere år. Erfaringen er at bankenes kvalitet på rapporteringen stadig bedres og nærmer seg en tilfredsstillende kvalitet.

Dersom kundenes bankinnskudd blir utilgjengelige som følge av at banken er satt under offentlig administrasjon, vil Bankenes sikringsfond utbetale garanterte innskudd innen syv arbeidsdager. Detaljer om dette finnes på nettstedet til Bankenes sikringsfond[13].

3.4 Verdipapirområdet

3.4.1 Hendelser innen verdipapirområdet

Verdipapirområdet har vært rammet av enkelte alvorlige IT-hendelser de siste årene. Eksempelvis har det vært svikt i datahaller som påvirker markedsplasser, og svikt i IT-prosesser som har resultert i betydelige feilutbetalinger. Konsekvensene for finansmarkedet blir størst når infrastrukturforetak rammes.
Hendelsene på verdipapirområdet viser at foretakene utfører effektiv gjenoppretting, og at det arbeides aktivt både med å redusere antall feil som oppstår og konsekvensene av disse.

[13] https://www.bankenessikringsfond.no/krav-til-datafiler/category891.html

Finanstilsynet har gjennomført flere stedlige tilsyn med digital sikkerhet som tema. Dette har ført til økt kunnskap om foretakenes beredskap knyttet til digital kriminalitet. På bakgrunn av påpekte funn, har foretakene iverksatt tiltak for å bedre sin forsvarsevne.

3.4.2 Konfigurering av testsystemer

Ulike typer feil, som ikke ble avdekket grunnet feilkonfigurering av testsystemer, har ved produksjonssetting utfordret driftsstabilitet og kvalitet hos flere foretak. Testsystemer som ikke er likt konfigurert som produksjonssystemet og testsystemer som har mangler når det gjelder tilgangsstyring er blant de problemene som er avdekket.

3.4.3 Havari i lagringsløsninger

I løpet av 2018 oppsto hendelser i datahaller der platelager i lagringsenheter havarerte på grunn av akustikk eller økt lufttrykk. Akustikkpåvirkning kan komme fra alarmer eller lyd som oppstår når slukningsgass for brann utløses. Trykkendringer i datahaller kan oppstå på grunn av at slukningsgasser frigjøres hurtig ved utløsing av automatiske brannslukningssystemer, noe som kan påvirke et platelagers lesehode slik at det oppstår skade på magnetplatene. I ytterste konsekvens kan dette ramme alle foretakets platelagre. For å eliminere risikoen kan platelagre byttes ut med SSD-disker (Solid State Drives), som er et lagringsmedium uten mekaniske deler. Kostnadene forbundet med SSD-disker kan imidlertid være høy.

Finanstilsynet anbefaler at foretak vurderer om deres installasjoner er i risikogruppen for denne type hendelse.

3.4.4 Retningslinjer for bruk av tredjeparter til test av sikkerhet

Ved stedlige tilsyn har Finanstilsynet registrert at det ofte benyttes tredjepartsaktører for test av foretakets sikkerhetsoppsett. Risikoelementer som må adresseres ved slik testing innbefatter valg av foretak og personell for testing, hvordan testing utføres, og foretakets kontroll med gjennomføringen av testene. Foretaket bør også ha retningslinjer for frekvensen av testene.
Det vises også til punkt 3.10.2.

3.4.5 Dimensjonering og testing av kriseløsning

Finanstilsynet har gjennom tilsyn avdekket at foretaks kriseløsninger ikke var dimensjonert med tilstrekkelig kapasitet til å opprettholde kritiske tjenester ved iverksettelse av kriseløsningen.

Finanstilsynet har erfart at tester av kriseløsningen har vært gjennomført der foretakets systemer for normal drift har vært tilgjengelig, med det resultat at kriseløsningen ikke nødvendigvis har blitt tilstrekkelig testet. Det medfører en usikkerhet om kriseløsningen i en beredskapssituasjon vil fungere i henhold til de krav som er satt. Finanstilsynet understreker her viktigheten av at kriseløsninger testes under de forhold og forutsetninger som løsningene er ment å fungere.

3.4.6 Organisering av systemeierskap for viktige forretningsløsninger

Systemeierskap for viktige eller kritiske forretningsløsninger inkluderer totalansvar for systemets risiko, økonomi, funksjonalitet og sikkerhet. Finanstilsynet registrerer at foretakene har ulike tolkninger av systemeierrollen og at ansatte i IT-avdelinger i enkelte foretak er tillagt dette ansvaret. En slik organisering kan bidra til økt avstand mellom forretningssiden og tilhørende IT-systemer, samtidig som IT-avdelingens prioriteringer vil kunne være i konflikt med forretningsområdets behov. Finanstilsynet mener at oppdeling av ansvar for kritiske systemer bør unngås og at forretningsansvarlige bør ha totalansvaret for viktige løsninger på eget område.

3.4.7 Andre forhold

Avanserte former for digitale angrep er en økende trussel for foretakene og må prioriteres høyt i foretakenes risikovurderinger. Planlegging, øving og test av kriseløsninger er essensielt for at foretakene skal være i stand til å håndtere reelle situasjoner som følge av digitale angrep.

Sensitiv informasjon på avveie er en reell risiko og bør også prioriteres i foretakenes risikovurderinger. Finanstilsynet understreker foretakenes ansvar for å redusere risikoen til akseptable nivåer. Dette kan gjøres gjennom styrking av foretakets digitale forsvar, klassifisering av informasjon, tilgangsstyring og kontroll med dokumentasjon som sendes fra foretaket.

3.5 Forsikring

3.5.1 Underrapportering av IKT-hendelser

Finanstilsynet har tidligere påpekt underrapportering av IKT-hendelser innen forsikringsområdet, og observerer fortsatt at hendelser ikke rapporteres. I IKT-forskriften §9 framgår at:

> "Avvik som medfører vesentlig reduksjon i funksjonalitet som følge av brudd på konfidensialitet (beskyttelse av data), integritet (sikring mot uautoriserte endringer) eller tilgjengelighet til IKT-systemer og/eller data skal rapporteres til Finanstilsynet. Rapporteringen skal normalt omfatte hendelser som foretaket selv kategoriserer til alvorlighetsgrad svært alvorlig eller kritisk, men kan også omfatte andre avvik dersom disse avdekker spesielle sårbarheter i applikasjon, arkitektur, infrastruktur eller forsvarsverk."

Foretak som har innarbeidet rutiner for avvikshåndtering har som regel inkludert en vurdering av om avviket er av en slik art at det skal rapporteres til Finanstilsynet. I tilsynsarbeidet vil Finanstilsynet påse at foretakene rapporterer avvik i tråd med IKT-forskriften.

3.5.2 Konfidensialitetsbrudd

Basert på innrapporterte hendelser, er Finanstilsynets vurdering at forsikringsforetakene ikke har etablert tilstrekkelige testregimer for å ivareta sikkerheten ved endringer i egenutviklede systemer.

Flere typer feil er rapportert. Kunder har fått tilgang til andre kunders informasjon, både som følge av programfeil, og som følge av manglende uttesting ved tekniske endringer. Videre er det innrapportert tilfeller der kunder har mottatt andre kunders faktura, samt tilfeller der gjenbruk av brukeridentitet i bedriftsløsninger har gitt kunder tilgang til informasjon fra kundeforhold det ikke skulle vært innsyn i. Ved ett tilfelle var fødselsnummer lagret som kundeidentifikator, samtidig som fødselsnummer-informasjonen kunne knyttes til hvordan kunden hadde navigert på nettstedet, når dette skjedde og fra hvilken geografiske lokasjon.

For de rapporterte hendelsene utgjør tap av renommé den største risikoen for foretakene.

Finanstilsynet ser alvorlig på de innrapporterte hendelsene og har understreket styrets og ledelsens ansvar for å følge opp sikkerhetsproblematikken. Forsikringsforetakene bør ha retningslinjer for sikker utvikling, samt etablerte testrutiner som sørger for at sikkerhetsfunksjonalitet blir ivaretatt ved alle typer endringer i systemene.

3.5.3 Oppfølging av utkontraktert virksomhet

Tilsyn viser at forsikringsforetakene har forbedret sin oppfølging av utkontraktert virksomhet. Finanstilsynet ser imidlertid fortsatt at utkontrakterte leveranser ikke følges opp i samme grad som de interne IT-tjenestene. Samtidig konstaterer Finanstilsynet at det også er mangler innen foretakets oppfølging av egne IT-områder. En løpende overvåking og oppfølging av utkontrakterte tjenester skal sikre god styring og kontroll. Finanstilsynet mener at foretakene må styrke kontrollhandlingene som utføres i både foretakets første- og andrelinje for å oppfylle kravene til styring og kontroll.

3.5.4 Oppfølging av sikkerhetsområdet

Finanstilsynet har ved tilsyn observert at forsikringsforetakene ikke har etablert tilstrekkelig tilgangsstyring, herunder oppfølging av sikkerheten knyttet til medarbeideres tilgangsrettigheter. I enkelte tilfeller er det også manglende innsikt og oppfølging av leverandørers tilgangsstyring og kontroll. Finanstilsynet legger til grunn prinsippet om at medarbeidere i forretningskritiske systemer kun skal ha nødvendige tilganger for å kunne utføre sine oppgaver, og at det samme gjelder for personell med tilgang til infrastruktur og systemer hos leverandørene. Spesielt kan dette utgjøre en risiko der personell hos leverandørene har utvidede tilgangsrettigheter. I utgangspunktet er tilgangsstyringen enkel å definere og kontrollere. Finanstilsynet konstaterer imidlertid at det er utfordrende for foretakene å følge opp dette i praksis.

Finanstilsynet forventer at foretakenes ledelse er særlig oppmerksomme på hvilke risikoer som følger av en dårlig ivaretatt sikkerhetsadministrasjon, og bør sørge for at krav til oppfølging og kontroll av sikkerheten er nedfelt i styrende dokumenter. Dette kan omfatte konkrete lister over aktiviteter som skal gjennomføres periodisk, slik at foretaket internt og ved utkontraktering sikrer at sikkerhetskrav etterleves på en tilfredsstillende måte.

3.5.5 IKT-strategi

Finanstilsynet konstaterer at forsikringsforetakene gjennomgående har etablert en egen IKT-strategi, i tråd med IKT-forskriften §2. I enkelte tilfeller er imidlertid IKT-strategien etablert uten en klar

forankring til foretakets forretningsstrategi. Det er også tilfeller av forsikringsforetak i større konsern som ikke har hensyntatt konsernets overordnede strategier i egen IKT-strategi. Finanstilsynet har avdekket tilfeller med manglende oppdatering av IKT-strategien der foretaket har gjennomført endringer i forretningsstrategi eller andre forhold som naturlig påvirker IKT-strategien.

Finanstilsynet understreker foretakets ansvar for at alle relevante forhold som kan påvirke IKT-strategien tas opp til vurdering av foretakets styre. Med høy endringstakt og en rask teknologisk utvikling er det viktig at IKT-strategien jevnlig revideres.

3.6 Revisjonsselskaper

Finanstilsynet har avdekket at revisjonsselskaper har utkontraktert IKT-virksomhet uten at det foreligger skriftlige avtaler som i tilstrekkelig grad sikrer revisjonsselskapets styring, innsyn og kontroll med den utkontrakterte virksomheten. Forsvarlig utkontraktering omfatter blant annet at risikoen ved utkontrakteringen må identifiseres, vurderes og håndteres, og det må sikres at Finanstilsynet kan føre tilsyn med den utkontrakterte delen av virksomheten. Kravet til forsvarlig risikohåndtering, herunder skriftlige avtaler, gjelder også i tilfeller der virksomheten er utkontraktert til et selskap i samme konsern eller i samme nettverk. Finanstilsynet har avdekket de samme svakhetene i regnskapsførerselskaper.

Det er også avdekket manglende retningslinjer for testing av forsvaret mot digital kriminalitet, herunder angrep rettet mot revisjonsselskapets systemer. Retningslinjer og rutiner er et viktig tiltak for å redusere risikoen for at testing fører til driftsavbrudd eller at informasjon kommer på avveie. Retningslinjer og rutiner må beskrive krav til testere, når testing skal skje og hvordan testingen skal gjennomføres. Dersom slik testing utkontrakteres, må avtalen med leverandøren gjenspeile disse prinsippene.

Revisjonsselskaper besitter konfidensiell informasjon, herunder taushetsbelagt informasjon, personopplysninger og kurssensitiv informasjon. Det er viktig å ha retningslinjer og rutiner for tilgangen som reduserer risikoen for at informasjon kommer på avveie eller misbrukes. Det er avdekket vesentlige svakheter i revisjonsselskapers retningslinjer og rutiner for styring og kontroll med tilgangen til konfidensiell informasjon.

3.7 Rapporterte hendelser i 2018

3.7.1 Statistikk over hendelser

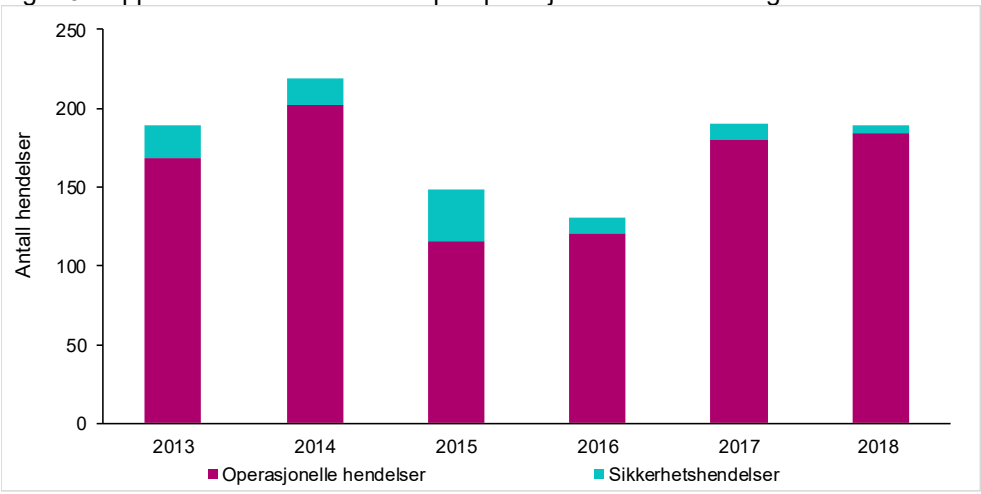
I 2018 ble det rapportert 189 IKT-relaterte hendelser fra foretak under tilsyn av Finanstilsynet. Til tross for at dette er omtrent samme antall hendelser som i 2017, har tilgjengeligheten til betalingstjenestene likevel vært bedre i 2018. Dette skyldes at alvorlighetsgraden var lavere enn foregående år, målt i antall kunder som ble rammet og avbruddenes varighet.

Tabell 5 Antall rapporterte hendelser

Årstall	Operasjonelle hendelser	Sikkerhetshendelser	Totalt antall hendelser
2013	168	21	189
2014	202	17	219
2015	116	32	148
2016	121	10	131
2017	180	10	190
2018	184	5	189

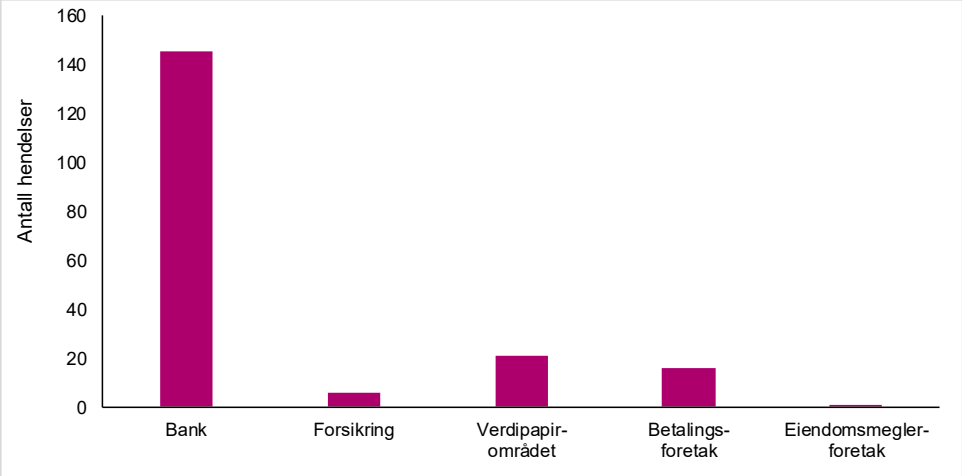
Kilde: Finanstilsynet

Figur 3 Rapporterte hendelser fordelt på operasjonelle hendelser og sikkerhetshendelser



Kilde: Finanstilsynet

Figur 4 Rapporterte hendelser i 2018 fordelt på type finansforetak



Kilde: Finanstilsynet

Figur 4 viser at bankene står for 74 prosent av de rapporterte hendelsene i 2018.

Mest oppmerksomhet fikk hendelsen med tilløp til brann i datasenteret til Nasdaq i Stockholm i april 2018, selv om norske kunder bare i begrenset grad ble rammet av denne hendelsen.

Flere hendelser rammet Vipps i første halvår av 2018. Vipps har en sammensatt infrastruktur og kan berøres av driftsproblemer hos mange ulike leverandører i verdikjeden. Som oftest er det bare deler av tjenesten som rammes ved hendelser. I takt med økt antall kunder og økt funksjonalitet, øker likevel konsekvensene ved hendelser som rammer en betalingstjeneste som Vipps.

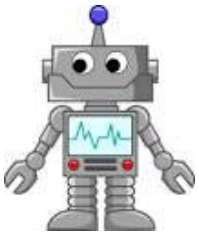
Det ble rapportert tre hendelser med DDoS-angrep mot banker i 2018. Til tross for angrep med relativ høy intensitet, begrenset konsekvensene seg til korte perioder med redusert tilgjengelighet til bankenes selvbetjente løsninger.

Enkelte foretak rapporterte om sikkerhetshull, uten at disse nødvendigvis ble utnyttet i ondsinnet hensikt. Sikkerhetshullene er oftest introdusert i forbindelse med endringer i systemet, og blir gjerne avdekket av kunder som urettmessig gis tilgang til andre kunders data, eller gjennom sikkerhetstester som foretakene utfører. Det var også tilfeller der foretakenes systemer for transaksjonsovervåking avdekket sikkerhetshull når svakhetene ble forsøkt utnyttet.

Årsakene til driftshendelsene kan grovt deles inn i hhv. feil etter endringer, mangelfull kapasitetsplanlegging eller svikt i overvåking av parametere som utløpsdatoer, fyllingsgrader og terskelverdier. Endringer som ikke gjennomføres i tråd med etablerte endringsrutiner og mangelfull kvalitet på testing, er som regel medvirkende årsaker til at endringer som settes i produksjon medfører feilsituasjoner.

I 2018 var det flere hendelser som skyldes for dårlig styring og kontroll med brukeridentiteter. Mangelfulle rutiner, eller manglende bruk av fastsatte rutiner, har ført til gjenbruk av brukeridentiteter og feilkoblinger, slik at foretakets kunde blir presentert for en annen kundes engasjementer. Dette er både et alvorlig brudd på konfidensialitet for kunden som får eksponert sine data, og brudd på tilgjengelighet for kunden som ikke får tilgang til sine egne data.

Finanstilsynet mottok for første gang i 2018 rapportering av en hendelse grunnet bruk av robot. Roboten utførte oppgavene den var programmert til å utføre, men de programmerte feilmarginene var ikke tilstrekkelige til å håndtere uforutsette hendelser med tilknyttet utstyr. Resultatet var at brev ble sendt til feil kunder.

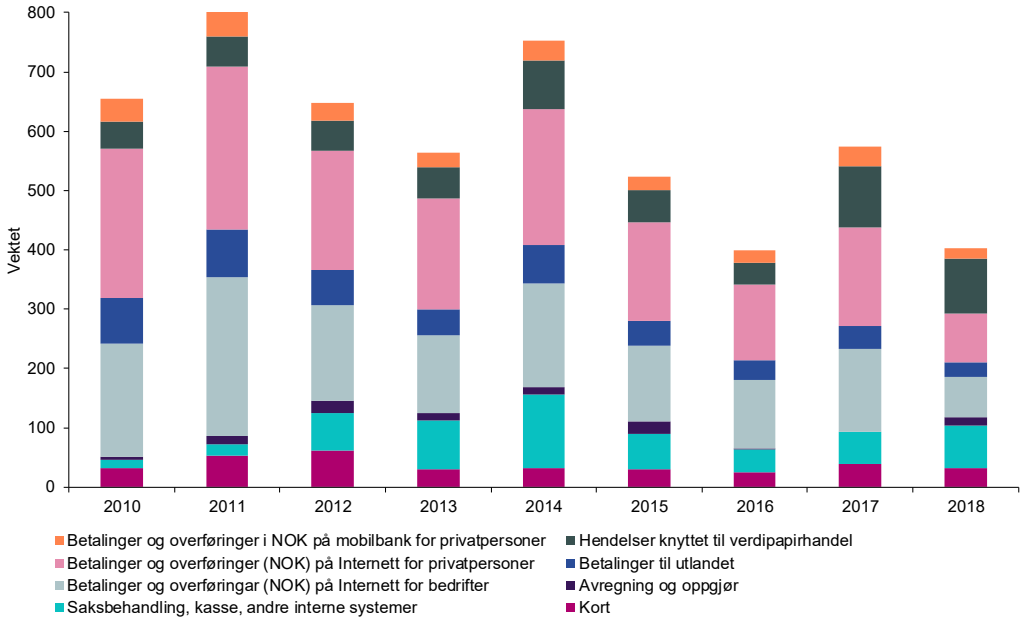


"Roboten fylte i finansieringsbevis og lagret dem som pdf-filer slik at de ikke kunne editeres. Roboten var satt opp til å vente en god stund på at lagring skjedde, men denne tiden var ved noen tilfeller ikke lang nok. Hvis filen ikke ble lagret innen oppsatt tid, satte roboten finansieringsbeviset til «feilet» og gikk videre til neste sak mens lagring av pdf-filen fortsatt pågikk. Når roboten skulle fylle i finansieringsbeviset for neste kunde, lå det allerede en pdf-fil klar, nemlig den fra forrige kunde, som roboten brukte og sendte til neste kunde."

3.7.2 Analyse av hendelsene som mål på tilgjengelighet

For hver hendelse som har medført redusert tilgjengelighet, 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, men at nettbanken er tilgjengelig). Dataene vektes (antall berørte brukere, varighet, tidspunkt, erstatningstjenester) og sammenstilles i tidsserier, slik at utviklingen kan følges over tid. Figur 5 viser at betalingssystemet og kunderettede løsninger var mer tilgjengelige for kundene i 2018 enn i 2017 og på samme nivå som i 2016. Skalaen på y-aksen er en indeks som framkommer basert på vektingen av hver enkelt hendelse.

Figur 5 Hendelser veiet med konsekvens



Kilde: Finanstilsynet

3.8 Utkontraktering

3.8.1 Melding om utkontraktering

Finanstilsynet vurderer avtaler ved melding om utkontraktering med utgangspunkt i finansforetaksloven § 4 c ved søknad om konsesjon og ved mottatt dokumentasjon i forbindelse med IKT-tilsyn. Det understrekes at det er foretaket selv som har ansvaret for egen IKT-virksomhet, inkludert tjenester som er utkontraktert, jf. §12 i IKT-forskriften. I tillegg kan også sektorlovgivning inneholde detaljerte regler om utkontraktering. Foretakene må etablere leverandøravtaler som tilfredsstiller lover og regler, og påse at leverandøren og dens underleverandører leverer IKT-tjenester i tråd med disse kravene.

Det ble i 2018 behandlet 161 meldinger om utkontraktering fra foretak som er omfattet av meldeplikten. Meldingene viser økt bruk av skytjenester.

3.8.2 Exit-bestemmelser

European Banking Authority (EBA) "Recommendations on outsourcing to cloud service providers"[14] var gjeldende fra 1. juli 2018.

Den gjeldende norske reguleringen for utkontraktering av IKT-tjenester gitt ved IKT-forskriften er etter Finanstilsynets vurdering i svært stor grad på linje med anbefalingene fra EBA. Et område som ikke er omfattet i dagens norske regelverk, er krav til såkalte exit-bestemmelser. I EBAs anbefaling legges det opp til at utkontrakteringsavtaler skal inneholde bestemmelser som gjør seg gjeldende, herunder hvilke forpliktelser leverandøren er pålagt i avtalen, ved flytting til ny leverandør, ved innkontraktering eller der behovet for tjenestene ikke lenger er tilstede. Finanstilsynet legger til grunn EBAs anbefalinger i sitt tilsynsarbeid.

3.8.3 Skytjenester

Finanstilsynets vurdering er at foretak, i prosessen med å beslutte bruk av skytjenester, gjennomfører nødvendige risikovurderinger og påser at krav til sikkerhet ivaretas. Foretakene synes videre å ha nødvendige oppmerksomhet knyttet til oppfølging av driften og sikkerheten i den utkontrakterte virksomheten. Finanstilsynet konstaterer at flere velger å etablere administrative systemer som skytjeneste, noe som krever sikring av data gjennom kryptering og flerfaktorautentisering av brukere.

3.8.4 Leverandørstyring

Det enkelte foretak skal sikre nødvendig styring og kontroll med sine leverandører, herunder at leverandøren leverer IKT-tjenestene i henhold til de krav som er satt, inkludert gjeldende lover. Effektiv leverandørstyring stiller strenge krav til foretakets kompetanse og organisering.

Utfordringen for mindre foretak er hovedsakelig å etablere en tilstrekkelig bestiller-kompetanse for å sikre at alle relevante krav inntas i avtalen med leverandøren ved etablering av tjenesten, og at foretaket har medarbeidere som har kompetanse til å følge opp leverandøren.

Store foretak og allianser har gjennom sitt avtaleverk og samhandlingsmodeller som regel etablert krav som legger føringer for leverandørstyringen. Utfordringen er kompleksitet og omfanget av tjenestene, og omfanget av leverandører, med underleverandører.

Foretakene skal ivareta styring og kontroll av de operative, strategiske og administrative aktivitetene i samhandlingen med hver enkelt leverandør, og i grensesnittet mellom leverandørene. Finanstilsynet mener kompleksiteten i samhandlingen mellom flere aktører utgjør en risiko, spesielt dersom alvorlige hendelser inntreffer.

14 https://eba.europa.eu/documents/10180/2170125/Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29_EN.pdf

3.8.5 Uavhengig vurdering og revidering av leverandørens risikostyring og internkontroll

Av forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT) §12 'Utkontraktering' heter det blant annet "Avtalen må sikre at foretak under tilsyn også gis rett til å kontrollere, herunder revidere de av leverandørens aktiviteter som er knyttet til avtalen."

Et foretaks internrevisjon er den funksjonen som foretakets styre og ledelse benytter blant annet for å vurdere om foretakets IKT-leverandører ivaretar risikostyring og internkontroll på en forsvarlig måte innen de tjenester som er underlagt IKT-forskriften. Finanstilsynet ser det som viktig at leverandørene ovenfor foretakene dokumenterer sin egen vurdering av internkontrollen, i tillegg til at foretakene får innsyn i uavhengige vurderinger, for eksempel av leverandørenes internrevisjon.

Uavhengige revisjonserklæringer og bekreftelse på etterlevelse

De største IKT-leverandørene imøtekommer til en viss grad foretakenes behov, blant annet ved utsendelse av revisjonserklæring, som ISAE 3402 Type II, hvor leverandørens eksterne revisor, eller andre som leverandøren velger, gjennom revisjonshandlinger vurderer internkontrollen av leverandørens prosesser. Slike gjennomganger er ofte begrenset til systemer som håndterer finansielle data, som igjen inngår som grunnlag for bekreftelse og revisorgodkjenning av foretakets regnskap. Gjennomgangen gir gode indikasjoner på kvaliteten i leverandørens kontroller innen prosesser som blant annet endringsstyring, tilgangsstyring, tilgjengelighet og sikkerhet, men på et overordnet nivå. Finanstilsynet er kjent med at enkelte leverandører i tillegg utsteder en uttalelse til foretakene om deres etterlevelse av IKT-forskriften, hvor grunnlaget for uttalelsen er basert på vurderinger fra leverandørens andre- og tredjelinjeforsvar.

Finanstilsynet observerer at enkelte leverandører ikke utsteder uavhengige erklæringer eller bekreftelse på etterlevelse av f.eks. IKT-forskriften.

Foretaket bør sørge for uavhengige vurderinger av leverandørenes etterlevelse av de krav som er satt gjennom lover og avtaler. Der foretaket selv mener uavhengige vurderinger fra leverandøren ikke er tilstrekkelig, bør dette legges fram for leverandøren for videre avklaring. Dette kan eksempelvis være at foretaket spesifiserer hvilke type kontroller som ønskes gjennomført.

Bekreftelse på etterlevelse fra skyleverandører

De største skytjenesteleverandørene, herunder Microsoft[15], Google[16] og Amazon[17], har etablert tjenestene sine med integrerte kontrollsystemer, der kundene kan hente ut informasjon og dokumentasjon knyttet leverandørens internkontroll for tjenesteleveransene. Foretakene som benytter skytjenester må etablere nødvendig kompetanse og innsikt i kontrollsystemene, og velge tjenenester

[15] https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings
[16] https://cloud.google.com/security/compliance/#/
[17] https://aws.amazon.com/compliance/programs/

som samsvarer med kontrollkravet. Dette kan være utfordrende, men er etter Finanstilsynets vurdering helt nødvendig.

Revisjon av leverandøren

Finanstilsynet har observert at foretakenes internrevisjon i varierende grad vurderer den operasjonelle risikoen og internkontrollen knyttet til IKT-virksomhet i eget foretak, og spesielt til de utkontrakterte IKT-tjenestene. Revisjon er en viktig og nødvendig kontrollfunksjon for å avdekke eventuelle forhold som kan utgjøre en høy risiko for foretaket. Leverandører som ikke blir revidert innebærer høy iboende risiko. Etter Finanstilsynets syn bør foretakene sørge for at det gjennomføres revisjoner av de mest kritiske områdene, herunder sikkerhet, risikostyring, hendelseshåndtering, tilgangsstyring, endringsstyring og tilgjengelighet. Dette kan utføres av foretakets egen internrevisjon, eller av eksterne spesialister. For mindre foretak som benytter samme leverandør, kan foretakene samarbeide om en felles revisjon av leverandøren.

3.9 IKT-sikkerhet og digital kriminalitet

Finanstilsynet mottar jevnlig statusoppdateringer om angreps- og trusselbildet fra foretakene selv og fra Nordic Financial CERT (NFCERT). Finansforetakene opplever at den digitale kriminaliteten øker i form av flere angrep enn tidligere, og forsøk på målrettede angrep skjer kontinuerlig. Finanstilsynet konstaterer imidlertid at det til nå ikke har vært sikkerhetshendelser innen finansnæringen som kan kategoriseres som alvorlige.

Foretakenes systemer for overvåking blir stadig bedre, og angrepene avverges som oftest før konsekvenser oppstår. Dette skyldes i hovedsak at finansnæringen generelt har en høy modenhet i sitt sikkerhetsarbeid. Samtidig viser hendelser som har rammet norske selskap de senere år hvor viktig det er at sikkerhetsarbeidet også rettes mot innsiden av foretakets nettverk for å avdekke kriminelle som har lykkes å komme på innsiden og etablert et digitalt fotfeste i de ulike sonene i nettverket.

Fra andre land, hvor finansforetak er blitt rammet av hendelser, konstateres det at motivet for de målrettede angrepene først og fremst er økonomisk vinning. Finanstilsynet viser her til en hendelse i februar 2019 hvor en bank i Malta valgte å stenge ned sine systemer som følge av at angripere lyktes å komme på innsiden av bankens nettverk. Uautoriserte grensekryssende transaksjoner til en samlet verdi av rundt EUR 13 millioner[18] ble sendt ut av banken.

I 2018 var det aktivitet mot norske banker fra trojaneren Retefe. Denne trojaneren har vært aktiv i enkelte andre land tilbake til 2013, men var aktiv mot norske banker først i 2018. De fleste angrepene ble stoppet før transaksjoner gikk ut av kundens konto, men ved hjelp av trojaneren lyktes det kriminelle å gjennomføre enkelte svindeltransaksjoner.

[18] https://www.timesofmalta.com/articles/view/20190215/local/not-all-money-stolen-in-cyberattack-may-be-found.702048

Det er også avdekket tilfeller av falske domener rettet mot finansnæringen hvor formålet er at ansatte, gjennom klikking på lenker, uforvarende installerer ondsinnet kode i foretakets nettverk. Denne type kriminell aktivitet er det vanskelig å sikre seg mot.

3.9.1 Sikkerhetskultur gjennom opplæring og involvering

Finanstilsynet konstaterer at foretakene har etablert opplæringsprogrammer innen området informasjonssikkerhet og cyber-sikkerhet. Gjennom opplæring av foretakets medarbeidere etableres det en sikkerhetskultur ved å bevisstgjøre medarbeidere om trusler og sårbarheter. Hovedsakelig omfatter opplæringen grunnleggende holdninger, som skal begrense risikoen for at foretakets medarbeidere utfører uaktsomme handlinger som følge av blant annet sosial manipulering. Finanstilsynet ser det som viktig at alle foretak sørger for at foretakets medarbeidere gjennomfører denne type opplæring, og at denne repeteres.

Finanstilsynet observerer at forretningssiden ofte ikke er involvert i sikkerhetsarbeidet. Det er av stor betydning at forretningssiden er innforstått med trusselbildet, og hvordan dette kan påvirke systemer som understøtter egne forretningsprosesser. Finanstilsynets mener forretningssiden i større grad bør involveres, og at forretningssidens ansvar som kravstiller tydeliggjøres.

3.9.2 Trender innen digitale angrep

Det er en trend at angrepene i større grad er rettet mot grunnleggende infrastruktur og manipulering av data som styrer infrastrukturen. Angrep mot nettverkskomponenter er avanserte, og både maskinvare og programvare angripes. Sosial manipulering er kraftig økende, herunder phishing gjennom ondsinnet e-post. Finanstilsynet antar at de største truslene kommer fra velorganiserte angripere med høy kompetanse og betydelige ressurser.

Et profesjonelt angrep starter ofte med en rekognoseringsfase i ytterste sone av nettverket, hvor angriperen identifiserer svakheter i systemer og komponenter som er eksponert mot Internett. Ved en vellykket infisering blir det foretatt ytterligere rekognoseringer for å avdekke svakheter i interne soner av nettverket som kan utnyttes. Lykkes dette, vil angriperen over tid, og uten å bli oppdaget, kunne identifisere muligheter for å få tilgang til større deler av foretakets infrastruktur og systemer. Ved en etablering på innsiden kan angriperen bruke tid til å tilegne seg nødvendig kunnskap for deretter å utføre sine handlinger.

Foretakene har i hovedsak arbeidet med å sikre sine nettverk mot angrep utenifra. Men faktum er at flere selskaper nasjonalt og internasjonalt har opplevd at angripere over lengre tid har operert på innsiden av nettverkene. Ettersom angrepsmetodene utvikles, vil foretakets evne til å oppdage og fjerne uønskede aktører på innsiden være avgjørende for å redusere risiko og skadeomfang.

Finanstilsynet mener det er viktig at foretakene sikrer at overvåking og kontroll ikke bare etableres gjennom de tradisjonelle perimeterbeskyttelsene, men også styrker overvåking og analysering for å identifisere om kriminelle har etablert ett eller flere digitale fotfester på innsiden av nettverket.

Finanstilsynet erfarer at foretakene i økende grad er oppmerksom på at angrepsform og -metodikk er i kontinuerlig endring. Finanstilsynet understreker at sårbarheter og trusler knyttet til endringer i trusselbildet bør ha særskilt oppmerksomhet fra styret og ledelsen i alle foretak.

3.9.3 Handlinger når angriper er på innsiden av nettverket

Reaksjonstiden og tiltakene som iverksettes er avgjørende for å begrense skadeomfanget når en angriper er i ferd med å etablere eller har etablert et fotfeste på innsiden av et foretaks nettverk. Identifisering og isolering av infiserte systemer for å begrense spredningen krever forhåndsbestemte rutiner som bør inngå i foretakets kontinuitets-/ kriseplan, hvor det framgår hvilke aktiviteter som skal iverksettes, og hvem som er bemyndiget til å beslutte iverksettelse. Foretakene bør på forhånd i størst mulig grad identifisere hvilke konsekvenser det vil kunne får dersom nettverket helt eller delvis må tas ned, noe som kan være nødvendig for å begrense skadeomfanget. Forhåndsbestemte og veloverveide tiltak vil også bidra til at raske beslutninger kan tas, og at de tas i riktig rekkefølge.

Finanstilsynet er kjent med at selskap som har opplevd denne type alvorlige hendelser har manglet gode nok kontinuitetsplaner, herunder krise- og beredskapsplaner, og heller ikke var tilstrekkelig forberedt gjennom trening og øvelser. Kontinuerlig tilgang til nøkkelpersonell over lengre tid kan være nødvendig, men vil være utfordrende om foretakene ikke på forhånd har planlagt beredskap gjennom bemanning.

Finansnæringen i Norge har vært forskånet for alvorlige cyber-hendelser, og det er derfor en usikkerhet knyttet til hvordan et foretak vil takle og håndtere en alvorlig situasjon der angripere har etablert fotfeste på innsiden og iverksatt sine handlinger. Finanstilsynet mener generelt at foretakene ikke er tilstrekkelig forberedt på slike situasjoner og kan derfor ha store utfordringer med å håndtere alvorlige cyber-hendelser. Det er imidlertid det enkelte foretaks ansvar å vurdere om det er behov for å styrke egen organisasjon og samhandlingen med leverandører for å være best mulig forberedt dersom en virkelig situasjon oppstår.

Aktører som har erfart alvorlige hendelser besitter etter Finanstilsynets syn en uvurderlig kunnskap og erfaring som andre foretak kan ha nytte av. Dette gjelder blant annet Helse Sør-Øst[19] og Hydro[20], som begge har vært rammet av alvorlige hendelser.

3.9.4 Manipulering av betaleren

Angrep som er en kombinasjon av digital og sosial manipulering er den typen angrep som i størst grad lykkes. Angrepene øker i antall og varianter, og medførte større tap i 2018 enn året før. Bankene gjør en stor innsats for å redusere kundenes tap på kjærlighetssvindel, investeringssvindel, fakturasvindel, direktørsvindel m.m. Finansforetakenes overvåkning, svindeldeteksjon og -etterretning klarer å hindre omtrent halvparten av de potensielle tapene. Likevel er de største tapstallene på dette svindelområdet.

[19] https://www.helse-sorost.no/nyheter/innbrudd-i-datasystemene-til-sykehuspartner-i-helse-sor-ost
[20] https://www.hydro.com/Document/Index?name=General%20cyber-attack%20presentation%20April%2012.pdf&id=28255

3.9.5 Manipulering og digitale angrep ved bruk av kunstig intelligens

Finanstilsynet tror "falske nyheter" på sikt også vil kunne ramme finansnæringen. Ved bruk av kunstig intelligens og dyplæring er det nå mulig å generere troverdige, men falske bilder, videoer og lyd. Ikke-eksisterende personer, eller personer som framstår som en annen, kan fremme budskap og ytringer som av mottakeren oppfattes som ekte, men som er manipulert og styrt for å påvirke mottakeren i en ønsket retning. Dette kan være i form av falske framstillinger rettet mot ansatte og ledelse, eller foretakets kunder. Det kan også være falske nyheter med formål om å skade et foretak eller å påvirke kursen for børsnoterte foretak.

Kunstig intelligens kan benyttes både til angrep og forsvar, og finansnæringen må i sitt forsvarsarbeid også rette oppmerksomheten mot nye trusler gjennom stadig mer avanserte angrepsformer.

3.9.6 Informasjonslekkasje

Informasjonslekkasje via e-post og USB-lagringsmedia

Foretakene håndterer store mengder konfidensiell informasjon om kunder og om foretaket selv. Tilliten til egne ansatte er stor, og det forventes høy grad av integritet og konfidensialitet fra medarbeidere som er gitt tilgang til informasjonen. Finanstilsynet har gjennom flere tilsyn observert en manglende klassifisering av informasjon. I tillegg kommer at dokumentasjon som sendes ut som vedlegg til e-post ikke kontrolleres. Det er også manglende kontroll med bruk av USB-lagringsenheter. Foretakene har således ingen kjennskap til om konfidensiell informasjon, gjennom bevisste eller ubevisste handlinger fra medarbeidere er kommet på avveie. Finanstilsynet mener at dette er en uforsvarlig praksis, og at det utgjør en høy risiko for at foretaket eller dets kunder kan påføres skade, både gjennom økonomiske tap og tap av omdømme. Det utgjør også en risiko for at medarbeidere gjennom sosial manipulering sender fra seg dokumentasjon med informasjon som kan utnyttes av kriminelle. Finanstilsynet mener foretakene bør arbeide for å etablere tiltak som reduserer denne risikoen.

Personopplysninger som diagnosedata

Nederlandske Ministry of Justice and Security publiserte 5. november 2018 informasjon om en konsekvensanalyse for databeskyttelse, "DPIA Diagnostic Data In Microsoft Office 365 ProPlus"[21]. Resultatet omtales som alarmerende da det ifølge analysen viser seg at Microsoft blant annet samler og lagrer personopplysninger. Microsoft har som følge av de avdekkede forholdene forpliktet seg til å iverksette tiltak[22]. Foretak som benytter produktene fra Microsoft bør vurdere denne risikoen og konsekvensene dette kan medføre, samt påse at nødvendige tiltak blir gjennomført.

[21] https://www.privacycompany.eu/en/impact-assessment-shows-privacy-risks-microsoft-office-proplus-enterprise/
[22] https://docs.microsoft.com/en-us/deployoffice/privacy/overview-privacy-controls

3.9.7 Innsidetrussel

Tillit og forventninger om lojalitet fra betrodde medarbeidere står sterkt innen finansnæringen. Samtidig kan et foretak ikke neglisjere risiko for at en medarbeider misbruker denne tilliten. Utro medarbeidere utgjør en risiko, og kan undergrave sikringen av foretakets og kundens verdier, om ikke internkontrollen også rettes mot medarbeideres aktiviteter, spesielt i forretningskritiske systemer.

Finanstilsynet har gjennom sitt arbeid i 2018 ikke blitt kjent med alvorlig svindel eller skadeverk ved bruk av IKT-systemene, hvor medarbeidere eller personell hos leverandører har vært involvert. Samtidig kan mangelfulle eller manglende kontroller være årsak til at ulovlige handlinger ikke oppdages. Denne type handlinger innebærer en svært høy risiko for den som utfører handlingen, og det er mindre sannsynlig at medarbeidere utfører denne type handlinger innen områder hvor oppdagelsesrisikoen er høy. Kompetente medarbeider, som er kjent med sårbarheter og manglende kontroller, kan velge å utføre ulovlige handlinger uten at dette oppdages, og uten å legge igjen spor.

Finanstilsynet mener det i for liten grad er rettet oppmerksomhet mot denne type trusler, og at medarbeideres aktiviteter i systemene i for begrenset grad overvåkes og analyseres. Logger blir som regel gjennomgått og analysert reaktivt når det oppstår mistanke mot en medarbeider.

Finanstilsynet er kjent med at enkelte foretak har etablert en proaktiv kontroll gjennom verktøystøtte som skal fange opp unormale aktiviteter, herunder overvåking av aktiviteter og analyse av logger. Dette kan ses på som et viktig tiltak for å redusere innsidetrusselen. Samtidig vil det medføre en forebyggende effekt ved at oppdagelsesrisikoen økes betydelig.

For foretakene er dette en vanskelig problemstilling. Balansen mellom kontroll, medarbeideres følelse av mistenkeliggjøring og frykten for å gjøre noe galt kan være krevende. Finanstilsynet vil peke på at personvernet skal ivaretas og at foretakets etiske retningslinjer må legges til grunn for å sikre at denne type kontroll etableres og utføres innen fastsatte regler.

Medarbeidere som middel for digitale angrep

Medarbeidere hos foretaket eller personell hos leverandører kan frivillig eller ufrivillig bli utnyttet i kriminelles planlegging og gjennomføring av digitale angrep.

Medarbeidere som samarbeider med kriminelle

Finanstilsynets vurdering at det trolig er en økende sannsynlighet og risiko for at kriminelle samarbeider med, og lykkes med, å plassere personer på innsiden av et foretak, eller hos dets leverandører. For å redusere denne risikoen, anbefaler Finanstilsynet at foretakene følger rådene i veilederen "Sikkerhet ved ansettelsesforhold – før, under og ved avvikling[23]" utgitt av Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet, Politiet og Næringslivets Sikkerhetsråd.

[23] https://www.nsr-org.no/getfile.php/139531-1505211147/Dokumenter/NSR%20publikasjoner/Veiledninger%20og%20orienteringer/sikkerhet_ved_ansettelsesforhold_2017_utskrift.pdf

Trusselsituasjoner

Ansatte med utvidete fullmakter, administrasjonsrettigheter til systemer, utviklere, ledere og andre som kriminelle kan utnytte for å utføre sine handlinger er også eksponert for å bli truet til å gjennomføre uautoriserte handlinger. Dette kan være å utføre transaksjoner, overlevere sensitiv informasjon, plassere ondsinnet kode eller andre aktiviteter som kan skade foretaket eller dens kunder. Ansatte som utsettes for en trussel har begrenset handlingsrom og vil oppleve en svært krevende situasjon.

Finanstilsynet har ved ett tilsyn i 2018 fått informasjon om at rutiner for håndtering av trusselsituasjoner er dokumentert og at øvelse var gjennomført. Andre foretak har ikke etablert rutiner og har heller ikke vurdert risikoen. Finanstilsynet mener foretakene bør etablere rutiner hvor medarbeidere gis tydelige instrukser for opptreden om en slik situasjon oppstår og hvilke tiltak som skal iverksettes basert på ulike scenarioer. Dette bør spesielt rettes mot personer som har posisjoner som vil være av interesse for kriminelle.

Uaktsomme medarbeidere og personell hos leverandører

Det vil alltid være enkelte medarbeidere som er mer uaktsomme enn andre, som for eksempel klikker på lenker i e-post, og åpner vedlegg uten å ta nødvendige forholdsregler. Dette er en gruppe medarbeidere som lett kan bli offer for sosial manipulering, og dermed være den kriminelles ufrivillige hjelpende hånd.

Foretakene bør identifisere slike medarbeidere og rette særlig oppmerksomhet mot disse i sitt opplæringsprogram. Medarbeidere som viser stor uaktsomhet bør vurderes i forhold til hvilke arbeidsoppgaver medarbeiderne utfører, og om det er grunnlag for å iverksette tiltak. Tilsvarende tiltak bør iverksettes ovenfor leverandørene og deres personell, spesielt ovenfor ansatte som har utvidede tilgangsrettigheter.

Skjerming av medarbeidere og personell hos leverandører

En skjerming av ansattes rettigheter og fullmakter for omgivelsene, internt og eksternt, gjennom bevisstgjøring hos den ansatte selv og gjennom egne rutiner i foretaket vil være et viktig tiltak for å redusere risikoen for at alvorlige situasjoner oppstår. Foretakene bør spesielt rette oppmerksomhet mot eksponerte medarbeidere, samt eksponert personell hos leverandører.

Uautorisert kode i applikasjoner

Applikasjonsporteføljen til et foretak er ofte svært omfattende med et høyt antall applikasjoner og med en betydelig kodemengde. I tillegg er det mange aktører, interne og eksterne, som utvikler og forvalter applikasjonene. Det er også høy grad av endringer som gjerne gjennomføres fortløpende. Smidige utviklingsmetoder medfører også at nye produkter og tjenester lanseres i et raskere tempo enn før. Tredjepartsaktører, som gjennom "Open Banking" kobler sine systemer til bankenes infrastruktur, vil bidra til at omfanget av applikasjoner økes ytterligere.

Foretakene og deres leverandører har i stor grad etablert en endringsstyring som sikrer at endringer behandles, kontrolleres, testes og godkjennes før de settes i produksjon. Finanstilsynet har imidlertid i

enkelte tilfeller påpekt at foretak ikke har tilstrekkelige kontroller for å identifisere endringer som er satt i produksjon uten at endringsprosedyren er fulgt, såkalte uautoriserte endringer.

Mangler i kravspesifikasjonen, eller at test ikke gjennomføres i tråd med det krav som er satt, kan gjøre at endringer resulterer i feil. Mangelfull sårbarhetstest kan også medføre at sikkerhetshull i koden ikke oppdages, og dermed eksponerer foretaket for digitale angrep. Finanstilsynets er kjent med at foretak bruker ulike verktøy for å avdekke sårbarheter i koden, men konstaterer at det er lite fokus på å avdekke uautorisert kode plassert av utviklere. Manglende gjennomgang og kontroll av kodeendringer utgjør en vesentlig risiko ved at uautorisert kode neppe vil oppdages dersom rutiner og verktøystøtte ikke er etablert. Uautorisert kode kan være en tikkende bombe som kan utløses på de mest ugunstige tidspunktene, eller det kan være kode som løpende generer uautoriserte transaksjoner uten at dette oppdages.

Selv om sannsynligheten for at denne type kriminalitet anses som liten, mener Finanstilsynet at det bør rettes større oppmerksomhet mot denne risikoen. Foretakene bør forsikre seg om at testmiljøene, internt eller eksternt, etablerer og gjennomfører uavhengig kodegjennomgang i nye systemer og i endringer i eksisterende systemer, med det formål å avdekke ondsinnet kode, plassert av egne utviklere eller av utviklere hos leverandører.

3.9.8 Tap av forretningskritiske data

Angrepsformen løsepengevirus (ransomware), hvor hackere lykkes med å kryptere data i et foretaks datasystemer, kan medføre uopprettelig skade dersom data ikke kan regenereres fra backup. Selv tilfeller der foretaket taper data kun over kortere perioder vil kunne få alvorlige konsekvenser. Løsepengevirus som forplanter seg selv i systemene ("self-propagating ransomware") kan påføre foretaket driftsstans. Ved en slik alvorlig hendelse vil utfordringene først og fremst være å identifisere hvilke data som er rammet og hvilke konsekvenser dette har medført, og vil gi. Foretak med høy kompleksitet i plattformer, nettverk og systemer vil møte spesielt store utfordringer dersom et angrep rammer flere steder. Denne type hendelse vil være svært arbeids- og tidkrevende og legge beslag på store ressurser i foretaket og dets samarbeidspartnere over lang tid.

Finanstilsynet har gjennom en nylig spørreundersøkelse (Kontinuitetsledelse og kriseløsninger), som nevnt i punkt 3.3.3, blant annet kartlagt andelen av banker i Norge som har etablert kontroller for å redusere risikoen for at korrumperte data blir lagt til backup. Det er en liten andel som svarer at slike kontroller ikke er etablert. Basert på dette, antar Finanstilsynet at risikoen for at en bank mister alle sine data som liten, men det vil alltid være usikkerhet rundt teknologiske løsninger, for eksempel at disse svikter eller at data tapes som følge av menneskelig feil. Finanstilsynet understreker at foretakene bør sikre og verifisere at backup-løsningene er satt opp slik at uautorisert krypterte data ikke legges til backup. Utfordringen med denne type angrep er at det er stor sannsynlighet for at siste inkrementelle backup også rammes. Spesielt kritisk vil dette være dersom full backup tas før tiltak om stans blir iverksatt. Finanstilsynet påpeker her viktigheten at foretakene verifiserer at nødvendige sikringstiltak er etablert for å begrense skadeomfanget ved et angrep. Dette kan blant annet være segmentering mellom systemer og backup-løsningen, eller sikring av filsystemer ved at filer ikke kan overskrives før

backup er tatt. Finanstilsynet mener at et viktig tiltak er en backup-strategi som tar høyde for å sikre data ved angrep, men også for å verifisere korrekte backup-data gjennom grundig og periodisk test.

Det er viktig at foretak er forberedt på denne type angrep, og at det etableres egne kontinuitetsplaner ved cyber-angrep som skal iverksettes dersom en hendelse oppstår. Det bør utarbeides en oversikt over kritiske systemer, avhengigheten mellom systemer og oversikt over kritiske data, samt i hvilken rekkefølge systemer og data skal reetableres. Det bør også etableres rutiner for beredskap som sikrer at personell er tilgjengelig over lengre tid, og at de er tildelt tydelige roller og ansvar.

Finanstilsynet mener at foretakene bør vurdere ekstraordinære tiltak som tar høyde for et "worst case"-scenario der kritiske data i databaser og i ordinær backup er tapt. Selv om sannsynligheten for en hendelse hvor alle data går tapt, eller som følge av andre teknologiske hendelser som medfører at systemene ikke kan gjenopprettes, anses som liten, vil konsekvensene være fatale. Det vil også medføre store samfunnsmessige problemer om større foretak rammes av en slik ekstraordinær hendelse. En manuell eller maskinell gjenoppretting av data fra lister på papir kan i ytterste konsekvens være eneste utvei.

3.9.9 Sårbarheter i maskinvare og fastvare

Sårbarheter knyttet til maskinvarens mikroprosessor

Det ble i 2018 avdekket sårbarheter knyttet til mikroprosessorer (CPU) og gjennom året ble det avdekket flere sårbarheter knyttet til ulike prosessorer. Sårbarhetene ble gitt betegnelsen "Meltdown"[24] og "Specter"[25]. Utnyttelse av sårbarhetene gjør det mulig for en angriper å få tilgang til minnet i maskinvaren, og dermed tilgang til programmer og operativsystemet. Angripere kan hente ut data og påloggingsinformasjon fra blant annet personlige datamaskiner, mobile enheter og fra servere som benyttes for skytjenester.

Sårbarheter knyttet til maskinvaren (fastvare, UEFI)

Datakoden for UEFI er fastkodet i en databrikke, kalt firmware, og prosesseres ved oppstart av datamaskinen. UEFI har styringen over datamaskinens operativsystem. Sårbarheter knyttet til UEFI gjør det mulig for en hacker å få tilgang til operativsystemet under oppstartsfasen. Sikkerheten kan kompromitteres slik at en hacker kan oppnå full tilgang til maskinen med de muligheter dette gir.

Utnyttelse av sårbarheter i maskinvare og fastvare

Det krevende for angripere å utnytte sårbarheter i CPU og UEFI, men så lenge sårbarhetene eksisterer og det faktum at det er vanskelig å etablere kontrolltiltak med dagens teknologi, er det viktig at foretakets ledelse tar sine forholdsregler ved å følger opp IKT-leverandørenes arbeid med nødvendig tiltak.

[24] Bryter isolasjonen mellom brukerapplikasjonen og operativsystemet, og gjør det mulig for en angriper å få tilgang til minnet, og gjennom det tilgang til andre programmer og operativsystemet. Dette kan være påloggingsinformasjon og sensitive data.
[25] Bryter isolasjonen mellom forskjellige applikasjoner.

3.9.10 ID-tyveri

I en undersøkelse utført av YouGov på oppdrag fra sikkerhetsselskapet NTT Security framkommer det at nesten halvparten (49 prosent) som deltok i undersøkelsen er bekymret for at bank- og kreditt-opplysninger skal misbrukes av uvedkommende ved netthandel, og at sju av ti er bekymret for ID-tyveri. Det framgår også at bruk av få eller korte passord gjør det enklere for uvedkommende å stjele en digital identitet. Finanstilsynet viser her til passordanbefalinger fra Nasjonal sikkerhetsmyndighet[26], som finansnæringen med fordel kan gjøre sine kunder oppmerksomme på for å redusere risikoen for svindel og ID-tyveri.

3.10 Rammeverk innen IKT og sikkerhet

3.10.1 Tilsynspraksis og regulatoriske forbedringer

EU-kommisjonen publiserte 8. mars 2018 FinTech Action Plan[27], hvor det framgår at cyber-risiko kan rokke ved tilliten til finansiell stabilitet og at cyber-angrep er en stadig økende trussel. De europeiske tilsynsmyndighetene EBA, ESMA og EIOPA ble bedt om å kartlegge tilsynspraksis i finansnæringen for områdene IKT-sikkerhet, -styring og -kontroll.

Rapporten[28]fra tilsynsmyndighetene ble oversendt Kommisjonen i april 2019 og inneholder forslag om å etablere et felles regulatorisk rammeverk for tilsynspraksis for EU/EØS-land for å sikre god og ens risikostyring, samt å stille minimumskrav for IKT-sikkerhet for finansnæringen i EU/EØS.

3.10.2 Rammeverk for sikkerhetstesting

Rammeverk for test av digitalt forsvarsverk

I FinTech Action Plan ba Kommisjonen også om en vurdering av kostnader og gevinster ved etablering av et helhetlig rammeverk for å teste robustheten i digitalt forsvarsverk for signifikante foretak og infrastrukturer innen finanssektoren.

Rapporten[29] viser til at foretakenes testing av sin digitale forsvarsevne er utviklet til å bli "best praksis". Foretak i finanssektoren opererer på kryss av landegrenser og det er i rapporten pekt på at ulikhetene i rammeverk innenfor testing av cyber-sikkerhet kan føre til unødvendige kostnader og økt risiko. Det er i rapporten også pekt på behovet for en samordning på europeisk nivå av regulatorisk rammeverk og behovet for bedre tilrettelegging for samarbeid mellom ulike jurisdiksjoner.

Rapport med forslag til tiltak er oversendt Kommisjonen i april 2019.

---

[26] https://www.nsm.stat.no/aktuelt/passordanbefalinger-fra-nasjonal-sikkerhetsmyndighet/
[27] https://ec.europa.eu/info/publications/180308-action-plan-fintech_en
[28] https://www.esma.europa.eu/press-news/esma-news/esas-publish-joint-advice-information-and-communication-technology-risk
[29] https://eba.europa.eu/-/esas-publish-joint-advice-on-information-and-communication-technology-risk-management-and-cybersecurity

Et eksempel på et slik rammeverk er den europeiske sentralbankens (ECB) rammeverk TIBER-EU[30] (Threat Intelligence Based Ethical Red Teaming). Rammeverket skal hjelpe nasjonale myndigheter med å legge til rette for at foretak i finanssektoren skal kunne etablere program for å teste og forbedre forsvarsevnen mot avanserte cyber-angrep gjennom kontrollert og kunnskapsbasert testing av produksjonssystem som vurderes som kritiske. Testingen skal i størst mulig grad simulere aktuelle angrepsteknikker og -scenarier. Formålet er å gjøre foretakene bedre rustet til å vurdere egen evne til å oppdage, beskytte seg mot og å håndtere cyber-angrep.

Det å oppnå cyber-robusthet krever en helhetlig tenkning som omfatter opplæring og informasjonsaktiviteter både for ansatte i finansnæringen og deres kunder. For å øke kunnskapen rundt bruken av digitale løsninger har kommisjonen etablert Digital Education Plan[31].

Threat Led Penetration Test

TLPT (Threat Led Penetration Test) er et kontrollert forsøk på å kompromittere foretaks elektroniske forsvar ved simulering av taktikk, teknikk og prosedyrer som benyttes av reelle trusselaktører. Metodikken er utarbeidet av en ekspertgruppe opprettet av G7-landene og publisert i et metodeverk som heter G7FE. Finansiell sektor er spesielt adressert. Bank of England har utarbeidet to beskrivelser, STAR og CBEST. Disse er i utgangspunktet samme metode, men koordineringen som myndighetene gjennomfører i CBEST er utelatt i STAR slik at metodikken er like anvendelig for foretak i alle sektorer.

TLPT utføres som regel av eksterne spesialister. Hensikten er å forberede eget elektronisk forsvarsverk ved hjelp av kunnskap tilført gjennom penetrasjonstester og fordrer bruk av gode metodeverk for å minimere foretakets risiko under gjennomføring. Metodeverkene skal sørge for beste praksis ved innkjøp av tjenester som ligger til grunn for slike tester, hvordan roller og ansvar fordeles mellom foretak og leverandør av TLPT-tjenester, kriterier for valg av leverandører og målekriterier for kvalitet på leveransene.

Den europeiske sentralbankens variant av dette rammeverket er TIBER-EU, omtalt i punkt 3.10.2.1.

Rammeverk for sikkerhetstesting i finanssektoren

Finanstilsynet vil sammen med Norges Bank og andre relevante myndighetsinstanser se på hvordan et slikt rammeverk bør etableres og tas i bruk i Norge.

3.10.3 Rammeverk for sikkerhet

Bestillerkompetanse er spesielt viktig når det kommer til valg av utkontrakteringspart. Særlig gjelder dette krav til sikkerhet og hvordan leverandøren kan bekrefte etterlevelse av fastsatte krav.

For mindre foretak som ikke har detaljkunnskap om hvilke krav som er i tråd med god praksis, finnes det flere rammeverk og veiledninger som vil være til god hjelp. Center for Internet Security (CIS),

[30] https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
[31] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en

Cloud Security Alliance (CSA) med rammeverk for sikkerhet ved skytjenester, NISTs rammeverk for cyber-sikkerhet, og ISACA med sitt COBIT-rammeverk er noen eksempler.

Finanstilsynet påpeker at selv der utkontraktering skjer gjennom et samarbeid mellom flere aktører, for eksempel en bankallianse, eller at utkontrakteringsprosessen settes ut til tredjepart, er det det enkelte foretaks ansvar å påse at alle nødvendige sikkerhetskrav er ivaretatt, og at disse etterleves.

3.10.4 Swifts sikkerhetsprogram

Som en følge av en alvorlig hendelse i 2016,[32] som rammet internasjonale bankers og sentralbankers interne systemer for gjennomføring av Swift-transaksjoner, etablerte Swift i 2017 sikkerhetsprogrammet Swift Customer Security Program. Swift-brukere har i 2018 blitt pålagt å implementert 16 obligatoriske sikkerhetskontroller. I tillegg er det 11 ikke-obligatoriske kontroller, hvor enkelte av disse antagelig blir obligatoriske i 2019. Swift-brukere må gjennomføre en årlig selvevaluering og attestasjon, hvor det blant annet angis om de obligatoriske kravene er oppfylt. Swift har utviklet et kjenn-din-kunde-verktøy til vurdering av brukere av Swift. Swift har utvidet rammeverket[33], som vil gjøres gjeldende i slutten av 2019. Finanstilsynet vil ved tilsyn be om framleggelse av selvevalueringen.

3.11 Foretakets styringsmodell og forsvarslinjer for IKT-området

3.11.1 Styringsmodell

Et foretaks dokumenterte styringsmodell, herunder policyer, strategier, standarder, retningslinjer og instrukser, skal blant annet understøtte regulatoriske krav og foretakets egne definerte krav. Dette rammeverket gir foretakets førstelinje nødvendige føringer som skal sikre at prosesser som implementeres etableres med nødvendig styring og kontroll. Rammeverket legges også til grunn for andre- og tredjelinjevurderinger av foretakets risikostyring og internkontroll, herunder vurdering av foretakets etterlevelse av eget rammeverk.

Finanstilsynet konstaterer at foretakene i stor grad etablerer og forvalter sine rammeverk på en god måte, men enkelte foretak har manglende rutiner for ledelsens godkjenning av dokumenter som inngår i rammeverket. De ansattes tilgang til dokumentasjonen kan også være en utfordring, og det er tilfeller der styrende dokumentasjon ikke er tilstrekkelig kjent og heller ikke operasjonalisert.

Finanstilsynet mener at styre og ledelse i større grad må påse at foretakets rammeverket er underlagt gode rutiner for utvikling, implementering, operasjonalisering og forvaltning. Videre må ledelsen påse at det etableres kontroller som gir styret og ledelsen bekreftelse på at rammeverkets krav etterleves. Mangelfulle kontroller for bekreftelse utgjør en risiko for at forutsetninger om etterlevelse ikke er til stede.

[32] https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery
[33] https://www.swift.com/myswift/customer-security-programme-csp/security-controls

3.11.2 Foretakets tre IKT-forsvarslinjer

God kvalitet på foretakets tre forsvarslinjer – operasjonell ledelse, risikostyring og compliance, og internrevisjon – er avgjørende for effektiv styring og kontroll. Svakheter i forsvarslinjene øker risikoen for at alvorlige sårbarheter ikke avdekkes. For å sikre at de tre forsvarslinjene fungerer etter hensikten, må alle funksjoner i forsvarslinjene være uavhengige av områdene og enhetene de kontrollerer. Forsvarslinjene skal rapportere direkte til ledelsen og/eller styret. Innenfor alle tre forsvarslinjer bør hensiktsmessige interne kontrollprosedyrer, mekanismer og prosesser utformes, utvikles, vedlikeholdes og evalueres.

Første forsvarslinje (operasjonell ledelse)

Første forsvarslinje utføres av den operasjonelle ledelsen som eier og håndterer identifiserte risikoer, og som har ansvar for å gjennomføre korrigerende tiltak. Den operasjonelle ledelsen skal også etablere effektive og hensiktsmessige prosesser og kontroller som skal sikre at risiko identifiseres, analyseres, overvåkes og forvaltes. Videre skal førstelinjen rapportere risiko, sørge for at risiko holdes innenfor de rammene foretaket aksepterer, og påse at IKT-virksomheten samsvarer med eksterne og interne krav.

Andre forsvarslinje (risikostyring og compliance)

Andre forsvarslinje består av risikostyrings- og compliance-funksjoner som overvåker og følger opp den operative ledelsens styring og kontroll.

Risikostyringsfunksjonens oppgave er å fasilitere implementeringen av rammeverket for foretakets risikostyring. Videre skal risikostyringsfunksjonen assistere førstelinjen i implementeringen av risikostyringen, samt sikre at prosesser og kontroller som er etablert i førstelinjen er effektive og riktig utformet. Videre er oppgaven å identifisere, overvåke, analysere og rapportere risikoer basert på førstelinjens risikorapportering, og ut fra det gi et helhetlig bilde av foretakets risikosituasjon.

Compliance-funksjonens oppgave er å overvåke etterlevelsen av juridiske og regulatoriske krav, og foretakets interne krav. Funksjonen skal være rådgivende ovenfor ledelsen og andre interessenter hva gjelder etterlevelse av nevnte krav, samt etablere retningslinjer og prosesser for å håndtere etterlevelsesrisiko og for å sikre etterlevelse.

Andre forsvarslinje kan også bestå av andre ikke-operative funksjoner, for eksempel innen informasjonssikkerhet.

Tredje forsvarslinje (internrevisjon)

Foretakets tredje forsvarslinje består av en uavhengige internrevisjon, som gjennomfører risikobaserte og generelle revisjoner og gjennomganger av foretakets styring og kontroll. Internrevisjonen er også ansvarlig for en uavhengig gjennomgang av de to første forsvarslinjene. En uavhengig internrevisjon er et viktig redskap for foretakets styre i arbeidet med å vurdere og innhente bekreftelse på etterlevelse av styrende rammeverk, lover og regler, samt å avdekke forhold som innebærer høy risiko.

Med økt endringstakt, både teknologisk og av trusselbildet, er det spesielt viktig at styret og ledelsen løpende vurderer om forsvarslinjene er riktig organisert, med riktige roller, ansvar og kompetanse, og har tilstrekkelige ressurser.

For mindre foretak er det ikke vanlig med egne og dedikerte ressurser i de tre forsvarslinjene innen IKT-området. Compliance-rollen i andrelinjen har som regel ikke nødvendig IKT-kompetanse til å overvåke foretakets etterlevelse av IKT-forskriften, og tredjelinjeforsvaret ved internrevisjonen er som regel utkontraktert. Finanstilsynet vil oppfordre foretak som ikke besitter tilstrekkelig kompetanse selv, om å benytte seg av eksterne ressurser. Det vil også bidra til å avdekke eventuelle alvorlige og ukjente sårbarheter.

Finanstilsynet konstaterer gjennom tilsyn at rollene og ansvaret mellom første- og andrelinjeforsvaret ikke alltid er tydelig definert. Spesielt gjelder dette innen risikostyring og informasjonssikkerhet. Uklare roller svekker foretakets kontrollfunksjoner, og øker risikoen for at foretakets styring og kontroll ikke blir hensiktsmessig vurdert. Finanstilsynet understreker viktigheten av at foretakene er tydelig på å definere roller og ansvar mellom første- og andrelinjeforsvaret.

Kunnskap om foretakets risikobilde og trusselsituasjon står sentralt i arbeidet med å identifisere områder som skal prioriteres for internrevisjon. De raske endringene gjennom innovasjon, bruk av ny teknologi, nye regulatoriske krav, samt endringer i trusselbildet, stiller også krav til internrevisjonens evne til omstilling og kompetansebygging. De siste årene har den teknologiske utviklingen i vesentlig større grad enn tidligere vært knyttet til foretakenes forretningsprosesser, noe som krever at revisorene innehar en viss forretningsforståelse i tillegg til IKT-kompetanse.

Finanstilsynet påpeker viktigheten av at foretakets internrevisjon har tilstrekkelig kompetanse og risikoforståelse, samt styrets ansvar for at internrevisjonen har nødvendig kompetanse og ressurser til å utøve sin rolle i tråd med endringer i risikobildet.

Finanstilsynet vil i sitt tilsynsarbeid vurdere foretakets styring og kontroll innen IKT-området, og gjennom dette kunne avdekke sårbarheter som kan utgjøre en risiko for foretaket. Finanstilsynet vil også kunne påpeke forbedringsområder som kan redusere foretakets risiko. Åpenhet og god samhandling er viktig for at Finanstilsynet skal kunne danne seg et riktig bilde av risiko- og kontrollsituasjonen hos foretakene.

3.12 Risikostyring innen IKT-området

Finanstilsynet har observert at flere av foretakene har utfordringer med å etablere en tilfredsstillende risikostyring. Mangelfull verktøystøtte, som skal bidra til enkel registrering av risikoer med støtte for effektiv behandling og oppfølging, er en av utfordringene. Samtidig konstaterer Finanstilsynet at foretakene arbeider med å forbedre sine prosesser, også ved bruk av bedre verktøy.

Selve prosessen med å identifisere risikoer bør stå sentralt i et foretaks risikostyring. Finanstilsynet konstaterer at prosessen for risikoidentifisering, herunder rutiner, regler og metodikk, ofte er mangelfull eller fraværende. Det mangler også klare regler for hvem som er gitt fullmakt til å akseptere en risiko eller beslutte at tiltak skal gjennomføres for å redusere en risiko. Finanstilsynets inntrykk er at risikoidentifiseringen i mange tilfeller kun involverer IT-ledelsen. Dette er en praksis som kan medføre at viktige risikoer ikke blir identifisert og rapportert, f.eks. fra IT-operativt personell, eller personell fra forretningssiden. Samhandlingen mellom IT-avdelingen og forretningssiden er viktig for å etablere en helhetlig risikoforståelse i foretaket. Finanstilsynet mener at forretningssiden i større grad bør inkludere sårbarheter knyttet til bruk, drift og forvaltning av forretningskritiske systemer i sin risikovurdering, og at dette må gjøres i samarbeid med IT-avdelingen.

Risikoidentifisering, og det å forstå hva en IKT-risiko er, eller fange opp at et forhold utgjør en risiko, krever bevisstgjøring gjennom informasjon og trening av alle relevante medarbeidere. Svakheter i prosessen med risikoidentifisering vil i seg selv utgjøre en risiko.

3.13 Kompetansesituasjonen på IKT-området i Norge

Finanstilsynet konstaterer at det er utfordrende for finansforetakene og deres norske IKT-leverandører å dekke sitt behov for IKT-kompetanse. Det er trolig én viktig årsak til at foretakene utkontrakter sine interne IKT-tjenester i større grad enn tidligere, og at IKT-leverandører velger å utkontraktere hele eller deler av sine oppgaver til aktører utenfor Norge, eller etablerer egen virksomhet utenfor Norge. Det er også eksempler på at foretak velger å flytte utkontrakterte IKT-tjenester tilbake til egen virksomhet, men at foretaket samtidig etablerer egne IT-avdelinger i utlandet. Den raske digitale transformasjonen tilsier at kampen om ressursene vil kunne strammes ytterligere til. Finanstilsynet tror dette kan medføre at avhengigheten av utenlandske aktører vil øke i årene framover.

Tiltak fra myndighetene

I 2014 gjennomførte Kommunal- og moderniseringsdepartementet en undersøkelse hvor det framgikk at behovet for avansert IKT-kompetanse vil øke og at det trolig vil være et betydelig økt behov fram mot 2030. I perioden fra 2010 til 2020 ble det anslått at behovet ville øke fra 31 000 til 42 500 personer, og i 2030 vil behovet være vel 55 000. Resultatet fra undersøkelsen framgår av rapporten fra DAMWAD[34], hvor også de negative konsekvensene dette kan føre til i Norge påpekes. I en artikkel fra mars 2018 skriver Digi.no at Norge i dag mangler 2 000 personer med kompetanse innenfor IKT og datasikkerhet. Kompetanseutvalget peker på tilsvarende utfordringer i sin rapport[35] (NOU 2019: 2), som ble lagt frem i februar 2019.

[34] https://www.regjeringen.no/globalassets/upload/kmd/aif/dokumenter/dimensjonering_avansert_ikt_kompetanse.pdf?id=2260119

[35] https://www.regjeringen.no/no/dokumenter/nou-2019-2/id2627309/

Justis- og beredskapsdepartementet har i samarbeid med Kunnskapsdepartementet utarbeidet en nasjonal strategi for digital sikkerhetskompetanse[36], datert 30. januar 2019. Formålet med strategien er; "å utvikle kompetanse i tråd med samfunnets, arbeidslivets og den enkeltes behov". I tillegg har regjeringen i sin langtidsplan for forskning og høyere utdanning 2019–2028[37] definert konkrete mål; "Styrke konkurransekraft og innovasjonsevne, møte store samfunnsordninger og utvikle fagmiljøer av fremragende kvalitet".

Samarbeid mellom finansnæringen, utdanningsinstitusjoner og teknologinæringen

DNB, Norges største bank, inngikk en intensjonsavtale med NTNU i 2017, hvor hensikten er å samarbeide innenfor områder som cyber-sikkerhet og digitale forretningsmodeller i internasjonal bank- og finansvirksomhet. I 2018 finansierte DNB, i samarbeid med NTNU, tre nye doktorgrader og en postdoktorgrad innen områdene stordata og kunstig intelligens, herunder maskinlæring.

Gjennom sertifiseringsprogrammer fra teknologinæringen vil også medarbeidere, eller andre som ikke har nødvendig formell kompetanse, kunne læres opp til viktige oppgaver innen drift og sikkerhet, eller andre relevante områder. Utdanningsprogram kan rettes mot ansatte eller andre som har utviklet gode grunnleggende ferdigheter i bruk av teknologi, som generasjon Z[38], og som ikke har den nødvendige formelle kompetansen. Et eksempel på dette er DNB som har etablert et eget program for å utdanne datascientister[39].

Kortsiktig og langsiktig konsekvensvurdering

Finansnæringen bør vurdere hvilke konsekvenser mangel på kompetanse kan medføre, både på kort og lang sikt, særlig med tanke på avhengighet av utenlandske aktører. Dette bør også ses i lys av endrede geopolitiske forhold, som er omtalt i punktet nedenfor.

3.14 Geopolitiske forhold

De geopolitiske forholdene er mer spent enn på mange år og kan forårsake situasjoner som finansnæringen må forholde seg til. NSM har gjennom temarapporten "Sikkerhetsfaglige anbefalinger ved tjenesteutsetting"[40] utarbeidet sikkerhetsanbefalinger ved tjenesteutsetting til utlandet.

Avhengighet til kritiske IKT-tjenester fra utlandet

Med dagens komplekse infrastruktur, både teknologisk og operasjonelt, samt avhengighetsforholdet til flere globale aktører, vil alvorlige kriser eller katastrofer, herunder krig, sabotasje, terrorhandlinger og

[36] https://www.regjeringen.no/contentassets/8ed748d37e504a469874ce936551b4f8/nasjonal-strategi-for-digital-sikkerhetskompetanse.pdf
[37] https://www.regjeringen.no/no/dokumenter/meld.-st.-4-20182019/id2614131/sec1
[38] https://en.wikipedia.org/wiki/Generation_Z
[39] https://en.wikipedia.org/wiki/Data_science
[40] https://www.nsm.stat.no/globalassets/dokumenter/temahefter/tjenesteutsetting2018v1.1_enkelstsider.pdf

cyber-angrep som rammer globale aktører som leverer kritiske IKT-tjenester til finansnæringen, kunne medføre vesentlige utfordringer med å opprettholde samfunnskritiske tjenester. Spesielt mener Finanstilsynet dette vil gjøre seg gjeldende dersom operativt personell fra utlandet er avskåret fra å utføre sine oppgaver.

Personellberedskap i Norge

Finanstilsynet konstaterer at flere av foretakene som benytter aktører i utlandet for utførelse av kritiske IKT-tjenester mener personell i beredskap i Norge, eller i andre land, vil kunne overta og utføre sentrale IKT-oppgaver om en kritisk situasjon oppstår. Det er imidlertid knyttet usikkerhet til i hvilken grad foretakene vil være i stand til å opprettholde driften av kritiske tjenester over lengre tid dersom personell fra utenlandske aktører ikke vil være i stand til å utføre sine oppgaver. Tilsvarende usikkerhet er knyttet til forvalting, herunder håndtering av alvorlige feilsituasjoner som kan medføre behov for et tett samarbeid med flere involverte leverandører. Finanstilsynet vil om nødvendig stille krav om at en slik beredskap etableres.

Konsekvenser ved avhengighet til utenlandske aktører

Finanstilsynet mener at IKT-kompetanse som ikke lenger forvaltes og utvikles i Norge, og en økende avhengighet av utenlandske aktører og kompetanse, kan utgjøre en vesentlig risiko. Det er i dag vanskelig å se de fulle konsekvensene av denne utviklingen, ikke minst i lys av den geopolitiske situasjonen.

Foretakene, og deres leverandører, bør gjennomføre periodiske konsekvensanalyser som omfatter konsekvenser som følge av at IKT-tjenester levert fra aktører i utlandet ikke vil være tilgjengelig over lang tid. Dette omfatter også å verifisere at personellberedskap, teknisk infrastruktur og kriseplaner til enhver tid er på et nivå som er nødvendig for å håndtere denne type situasjoner.

Det er viktig at foretakenes styrer tar hensyn til geopolitisk usikkerhet i sine risikovurderinger og beslutningsprosesser.

3.15 Utviklingstrekk innenfor finansiell teknologi

Utviklingen innenfor finansiell teknologi er knyttet til både nye og eksisterende foretaks tjenester. Foretakene har kontinuerlig fokus på å forenkle sine IKT-løsninger. Samtidig øker kompleksiteten i den samlede tekniske infrastrukturen og gir en økende risiko som følge av at det blir flere aktører, bruk av ny teknologi og teknologi på nye områder samt en fortsatt høy endringstakt.

3.15.1 Utviklingsmål

Finanstilsynet mener det er viktig at foretakets styre og ledelse også retter et kritisk blikk på hvilke interessenter som skaper forventinger og behov for en raskere og økt digital transformasjon, både internt i foretaket og av eksterne aktører. Dersom beslutninger tas på feil grunnlag, kan dette medføre at foretakene etablerer strategier og endringsprosesser som fører foretaket inn i kostbare og mislykkede organisatoriske og teknologiske endringsprosjekter.

For foretakene er det en krevende balanse mellom å oppmuntre til nytenking og innovasjon, og samtidig ha tilstrekkelig innsikt og forståelse i arbeidet med å identifisere og definere nye og realistiske forretningsmodeller gjennom en digital transformasjon. Finanstilsynet ser det som viktig at det gjennomføres grundige analyser i en tidlig fase av endrings- og utviklingsprosjekter, som kan avdekke forhold som utgjør en risiko for at prosjekter ikke kan gjennomføres som planlagt, eller at det avdekkes forhold som medfører at prosjekter ikke kan realiseres.

3.15.2 Open banking

Det er nå en utvikling hvor tredjeparter etablerer tjenester mellom banker og bankers kunder. Integrasjonen skjer gjennom bankenes API-er, hvor tredjepart gis tilgang til bankdata og -tjenester. Banker vil gjennom Open Banking blant annet kunne tilby sine kunder tilgang til tjenester hos andre banker, mens kundene på sin side vil kunne velge å etablere kundeforhold med flere banker. Alle banktjenestene kan nås fra ett og samme brukergrensesnitt, enten fra en bank eller fra en tredjepart. Gjennom Open banking forventes det at bankens kunder vil få tilgang til et bredt spekter av produkter og tjenester på tvers av bankene, nasjonalt og internasjonalt innen EØS.

Der det er regulert tilgang til bankenes infrastruktur, som innen PSD 2, er de regulatoriske kravene strenge, og bankene står ansvarlig for å bygge tilstrekkelig sikkerhet både i forhold til tredjepart og i forhold til bankens kunder som benytter tredjepartsløsninger som en del av sine banktjenester. Kravet til aktører som tilbyr tjenester mellom banker og bankers kunder er regulert blant annet gjennom konsesjonskrav. Det er også høy oppmerksomhet fra myndighetenes side, herunder Finanstilsynet, når det gjelder risiko for hvitvasking og terrorfinansiering gjennom nye kanaler.

Det antas at angrepsflaten vil endres ved at kriminelle også vil rette sin aktivitet mot tredjepartsaktører. Angrep kan skje gjennom utnyttelse av sårbarheter i applikasjonene fra tredjepart, og bankkunder kan i større grad bli utsatt for sosial manipulering. Bankenes utfordring er først og fremst å sikre en forståelse av sikkerhetskravene i dette nye økosystemet, både hos den enkelte tredjepart og i forhold til kunders bruk av tredjepartsløsninger.

Finanstilsynet understreker viktigheten av å oppfylle pålagte sikkerhetskrav, herunder kravene i PSD 2 og GDPR, for å redusere risikoen for alvorlige hendelser. Mangelfull etterlevelse og kontroll vil medføre økt risiko for økonomiske tap og tap av omdømme. Det er også viktig at bankene etablerer gode kontrollrutiner, herunder gjennomfører løpende penetrasjonstesting, for å avdekke sårbarheter i bankens egne API-er. Transaksjonsovervåking, som nevnt under punkt 3.3.6, vil være et viktig middel for å avdekke unormale transaksjonsmønstre for transaksjoner som mottas fra en tredjepart. Dette vil også kunne avdekke digitale angrep som rammer en tredjepartsaktør. Finanstilsynet understreker viktigheten av at foretakene etablerer rutiner for å stanse transaksjoner som er av mistenkelig karakter, og etablerer rutiner for å sperre transaksjoner fra tredjepartsaktører som er rammet av et angrep.

3.15.3 Blokkjede

Finanstilsynet skrev i ROS-rapporten for 2017 at et generelt kjennetegn ved teknologiske endringer, som blokkjede-teknologien, er at det gjerne tar lengre tid enn forventet før den tas i bruk og at konsekvensene ofte blir større enn forutsett. Aktiviteten for å utrede potensialet og muligheten i denne

teknologien synes noe avtagende innen finansnæringen, men det er fortsatt viktig at foretakene følger med på utviklingen og hvordan teknologien kan komme til anvendelse.

3.15.4 Kunstig intelligens

Den raske teknologiske utviklingen og muligheter for innsamling og prosessering av store mengder data, både strukturerte og ustrukturerte, åpner opp for nye muligheter. Bruk av kunstig intelligens har potensiale til å endre dagens forretningsmodeller i finansnæringen. Det er derfor viktig at foretakene etabler en forståelse av teknologien, hvordan den kan anvendes og hvilke risikoer den innebærer.

Foretak som tar i bruk kunstig intelligens (AI) bør etablere en styringsmodell som legger nødvendige føringer for bruken. Denne bør omfatte strategiske valg, roller og ansvar, kompetansekrav, anvendelse av datakilder m.m. En styringsmodell bør forankres og godkjennes av foretakets styre og ledelse. Bruk av teknologi uten at dette understøttes av en tydelig styringsmodell vil kunne medføre risiko for blant annet feilslåtte investeringer og alvorlige feil i forretningsprosesser, og kan bryte med personvernreglementet som skal beskytte foretakets kunder.

3.16 Teknologisk gjeld

Den tradisjonelle bankmodellen, hvor bankene i hovedsak konkurrerer seg imellom med det samme tjenestespekteret, har gjennom de senere år vært i endring. En rask teknologisk utvikling har åpnet opp for nye forretningsmodeller og økt automatisering.

Utfordringen til mange foretak, og deres leverandører, er den teknologiske gjelden som har bygget seg opp gjennom flere tiår. Bygging av funksjonalitet, i tråd med forretningssidens behov, har gått på bekostning av forvaltningen av blant annet teknologisk arkitektur. Skreddersøm foran hyllevare har også resultert i stor leverandøravhengighet eller avhengighet av enkeltpersoner i arbeidet med å forvalte eldre systemer. Finanstilsynet konstaterer at situasjonen legger begrensninger i foretakenes ambisjoner om en rask og effektiv utvikling av nye tjenester.

Finanstilsynet er informert om at både foretak og leverandører bruker vesentlige ressurser i arbeidet med å fornye sin infrastruktur, og i arbeidet med å etablere tjenester på nye teknologiske plattformer. Dette er et arbeid som er svært krevende, omfattende og kostbart. Det er også her utfordringer når det gjelder å opprettholde kompetanse innen forvaltning og utvikling av gamle systemer. Finanstilsynet mener det er viktig at foretakenes styre og ledelse er bevisst de utfordringene og risikoene dette medfører.

3.17 Beskyttelse av persondata

Nytt personvernregelverk trådte i kraft i Norge 1. juli 2018.

Personopplysninger skal behandles slik at integritet, konfidensialitet og tilgjengelighet blir ivaretatt. Ansvaret for å opptre i samsvar med personopplysningsregelverket ligger på alle foretak som

behandler personopplysninger. Foretaket er ansvarlig for å etablere tiltak mot utilsiktet og ulovlig ødeleggelse, tap og endringer av personopplysninger. Det er viktig å understreke at foretakene både har ansvar for selve behandlingen av personopplysningene, og i tillegg skal kunne vise til og dokumentere at denne behandlingen ikke er lovstridig.

Personopplysningsregelverket stiller krav til beskyttelse av personopplysninger. Foretak bør i den forbindelse innarbeide sletterutiner i alle fag- og støttesystemer. Videre må det gjennomføres manuell sletting av persondata som er lagret lokalt eller på fellesområder ("ustrukturerte data"). Systemløsninger for logging av uautorisert bruk av informasjonssystemer og et godt system for tilgangskontroller når det gjelder ansatte og leverandører bør være på plass.

Når det gjelder kommunikasjon med kunder, er det viktig at foretakene har spesiell oppmerksomhet rettet mot feilforsendelser av personopplysninger gjennom utgående post, både digital og fysisk.

3.18 Bankenes tilbud av kontanttjenester

Etter oppdrag fra Finansdepartementet, gjennomførte Finanstilsynet i 2018 to undersøkelser om hhv. kontanttilbudet i Norge, herunder innskudds- og uttakstjenester, og om hvordan bankene etterlever kravet i finansforetaksloven §16.4, hvor det heter at "Banker skal i samsvar med kundenes forventninger og behov, motta kontanter fra kundene og gjøre innskudd tilgjengelig for kundene i form av kontanter. Departementet kan gi forskrift om bankers plikt til å ta imot og til å gjøre kontanter tilgjengelig for kundene".

Gjennom undersøkelsene konkluderte Finanstilsynet med at summen av minibanker, innskuddsautomater, kontantuttak i butikk, "Post i butikk" og de ulike systemene for regningsbetaling vil dekke de fleste kunders daglige behov, men peker på at det er en fare for at kontanttjenestetilbudet kan bli svekket framover. Det er behov for å tydeliggjøre bankenes ansvar for et hensiktsmessig tilbud av kontanttjenester i hele landet, tilsvarende ansvaret de har for å møte etterspørselen etter kontanter i en situasjon med svikt i det elektroniske betalingssystemet. Finansdepartementet presiserte 17. april 2018 i finansforetaksforskriften §16-7 at: "bankene skal ha løsninger for å kunne møte en eventuell økt etterspørsel etter kontanter ved svikt i de elektroniske betalingssystemene". Bankene ble pålagt å oppfylle kravene innen 1. januar 2019.
Finanstilsynet mener det er behov for nærmere forskriftsregler om grunnleggende banktjenester, både om geografisk distribusjon og om hvilke tjenester som må tilbys, og det pekes på at hensynet til effektive og rasjonelle løsninger tilsier at kontanttjenestene i stor grad bør baseres på fellesløsninger, jf. Finansmarkedsmeldingen 2019[41].

Blant annet på bakgrunn av Finanstilsynets undersøkelser og anbefalinger, har Bits iverksatt et prosjekt for å utrede mulighetsrom og framtidige løsninger for kontanttjenester i Norge.

[41] https://www.regjeringen.no/no/dokumenter/meld.-st.-24-20182019/id2642702/sec1

Vipps planlegger etablering av en Bank i butikk-løsning for innskudd og uttak av kontanter basert på BankAxepts kortordning[42]. Banker som deltar i kortordningen kan inngå avtale om løsningen. DNB har meddelt at de vil legge ned sine banktjenester gjennom "Post i butikk" og erstatte denne med Vipps nye løsning. Vipps planlegger oppstart av tjenesten i 2020 i Kiwi og Meny-butikker over hele landet, samt i enkelte Spar- og Joker-butikker.

3.19 Fellestiltak innen finansnæringen

Finanssektoren samarbeider på tvers om teknologiske løsninger på en rekke områder. Særlig gjelder dette innenfor områdene sikkerhet og felles infrastruktur, tjenester og standarder.

For å bedre beredskapen i de elektroniske betalingssystemene for kortbetalinger, har Bits blant annet tatt initiativ til å øke kapasiteten i reserveløsningen i kortterminalene.

Det ble i 2017 foreslått etablering av en ny felles infrastruktur for betalinger med raskere oppgjør[43], der infrastrukturen skulle legge til rette for en kontinuerlig prosessering av realtidsbetalinger, såkalte BRO-betalinger. BRO-betalingsløsningen var ment å erstatte eksisterende straks-betalingsløsning i løpet av 2019.

Syv nordiske banker, deriblant DNB, nedsatte i 2018 et prosjekt (P27)[44] for å etablere en nordisk betalingsinfrastruktur med løsninger for nasjonale og grensekryssende betalinger i flere valutaer (SEK, DKK, NOK og EUR) for å lette betalinger på tvers av landegrenser og fremme handel mellom de nordiske landene. Finans Norge og Bits samt også øvrige norske banker ble involvert. Utvikling av BRO-betalingsløsningen ble satt på vent som følge av P27-prosjektet i P27.

Høsten 2018 ble det besluttet, uavhengig av planene til P27, å iverksette et prosjekt for raskt å etablere en bedre realtidsløsning (Straks 2.0) enn den eksisterende straks-betalingsløsningen, og med realtidsoppgjør. I mars 2019 ble det kjent at DNB trakk seg fra videre deltakelse i P27. Finans Norge og Bits avsluttet også videre deltakelse i P27-prosjektet og hovedstyret i Finans Norge vedtok at finansnæringen vil videreutvikle den norske betalingsinfrastrukturen.

[42] https://www.dnbnyheter.no/nyheter/dnb-gar-for-ny-losning-for-kontanttjenester-i-2020/
[43] https://www.bits.no/wp-content/uploads/2017/04/Sluttrapport-BRO.pdf
[44] https://www.project27.info/

Offentlig sektor og finansnæringen har fortsatt sitt samarbeid om digitalisering og effektivisering av viktige prosesser i samfunnet gjennom DSOP[45]. Samarbeidet omfatter Skatteetaten, NAV, Brønnøysundregistrene og politiet innenfor blant annet områdene:

- **samtykkebasert lånesøknad** – innhenting av informasjon fra offentlig sektor
- **kontrollinformasjon** – utveksling av kontrollinformasjon mellom bank og skatteetaten, politiet og NAV knyttet til etterforskning
- **konkursbehandling** – umiddelbart digital melding til bank for sperring av kontoer
- **oppgjør etter dødsfall** – forenklet prosess etter dødsfall
- **selskapsetablering** – forenklet prosess ved selskapsetablering
- **syke- og uføreopplysninger fra NAV** – forenklet og effektivisert prosess mellom forsikringsforetak og NAV
- **maskinell kontroll av signaturrett og prokura** – oversikt hvem som har signaturrett eller prokura for en bestemt enhet
- **ajourhold av pensjonsberegninger** – forenklet rapportering av lønn til pensjonsforetak og Skatteetaten

Løsningen for samtykkebasert lånesøknad er tatt i bruk i mer enn 100 banker. I november 2018 ble løsningen for kontrollinformasjon satt produksjon. Løsningen for konkursbehandling ble satt i pilot i februar 2019, og løsning for syke- og uføreopplysninger fra NAV ble satt i pilot i april 2019.

Det har vært og vil fremdeles være betydelig samhandling internt i finansnæringen i regi av Bits knyttet til foretakenes arbeid med å tilpasse seg PSD 2[46], som trådte i kraft i Norge 1. april 2019. Arbeidet har etter hvert kun hatt fokus på å etablere felles standarder og formater på kontotilbyderes grensesnitt, der Bits har valgt å følge Berlin Groups[47] initiativer.

Et annet viktig fellestiltak er Bits' arbeid med å etablere én internasjonal standard for filbasert finansiell meldingsutveksling, ISO 20022, som dekker hele verdikjeden fra kunde til bank, bank til bank og bank til kunde.

[45] Digitaliseringssamarbeidet mellom offentlig og privat sektor, https://www.bits.no/project/dsop/
[46] https://www.bits.no/project/psd2-xs2a/
[47] https://www.berlin-group.org/psd2-access-to-bank-accounts

4 Aktørenes vurdering av risikofaktorer

4.1 Intervjuer med foretak og leverandører

4.1.1 Sosial manipulering

Aktørene er tydelige på at sosial manipulasjon utgjør en stor risiko. Framveksten av sosiale medier gjør at personlig informasjon deles i større grad enn før. Aktørene mener angripere kan benytte denne informasjonen til å etablere angrep som er tilpasset den enkeltes profil. For eksempel kan en (falsk) e-post se ut som den kommer fra en god venn. I e-posten finnes gjerne informasjon som bekrefter dette ytterligere. I dette tilfellet er det kundene selv som blir det svake leddet idet de åpner og svarer på e-posten. Angriperen kan da få uautoriserte tilganger og misbruke dette ved å for eksempel distribuere sensitive data til uvedkommende.

4.1.2 Svindel ved bruk av nære relasjoners BankID

Misbruk av avtaleinngåelse gjennom digital signering (BankID) er ifølge foretakene økende, og skjer i særlig grad i nære relasjoner. Personer med nære relasjoner kan ha tilgang til hverandres BankID, og personer som ikke er datakyndige, blir hjulpet til å signere. Dette er utfordrende for foretakene å håndtere. Et foretak opplyser at krav om erstatning som følge av familiesvindel er blitt rettet mot foretaket. Finanstilsynet understreker kundens ansvar for at informasjon som benyttes for identifikasjon ved signering og pålogging ved bruk av BankID, ikke kommer på avveie.

4.1.3 Leveransepress, sikkerhet og reguleringer

Leveransepress ble av mange av foretakene angitt som en betydelig sikkerhetsrisiko. Kravet fra markedet i forhold til nyskaping og hyppige publiseringer kan utfordre kodekvaliteten. Marginpress og nye konkurrenter utfordrer forholdet mellom fart og omstilling på den ene siden, og sikkerhet på den andre siden. I tillegg vil kundevennlighet kunne utfordre sikkerheten på grunn av kravet om brukervennlige løsninger i et sammensatt konkurransebilde.

Foretakene opplyser at tilpasning til reguleringer, som GDPR og retningslinjer fra Finanstilsynet, resulterer i økte IT-kostnader som ellers kunne bli brukt på blant annet økt sikkerhet, tilgjengelighet og nyskapning. Det nevnes også at ulike reguleringer som gjennomføres samtidig, herunder eIDAS, PSD 2, GDPR og ISO20022, er utfordrende.

Aktører innen forsikring nevner at GDPR-krav er utfordrende å implementere, da det ikke er koordinering av testdatabruk i det offentlige, og at foretakene har integrasjoner mot mange eksterne registre.

4.1.4 Kompleksitet i løsningsporteføljene

Foretakene opplyser at det generelt er en økt kompleksitet i løsningsporteføljene. Dette handler både om endringer i betalingsformidlingen som kommer som følge av PSD 2, som blant annet inkluderer flere aktører enn tidligere, og at foretakenes egne fornyelsesprogrammer gjør det spesielt utfordrende i overgangsfasen når nytt og gammelt løsningssett skal være operative side om side. Dette gir økt eksponeringsflate, lengre leveransekjeder og potensiell ansvarsfragmentering. Eierskap til applikasjoner, oversikt over applikasjoner og detaljkunnskap er også mangelfull. Enkelte foretak opplyser at de har hatt utviklingsprosjekter som har feilet, og som utgjør en stor risiko for foretaket, ved at regulatoriske krav ikke vil kunne etterleves innen de frister som er satt.

Foretakene opplyser at de gjennom årene har akkumulert store mengder ustrukturerte data, det vil si data som ikke er lagret og indeksert i databaser, men som er lagret i form av e-poster, private dokumenter og i sosiale medier. Det er stor risiko knyttet til mengden og innholdet når det gjelder ustrukturerte data fordi det kan bli svært utfordrende for foretakene å etterleve kravene i GDPR.

4.1.5 Komplekse leveringskjeder

Foretak opplyser at mange leverandører er involvert i produksjonen av en finansiell tjeneste. Dette skaper sårbarhet fordi tjenesten er avhengig av mange ledd for å fungere optimalt. Foretak opplyser om blant annet utfordringer når det gjelder tilgang til tjenester fra BankID og fra teleoperatørene knyttet til identifisering av personer og signering av kontrakter.

Stor grad av utkontraktering samtidig som bruken av skytjenester øker, skaper en driftskompleksitet med økt sårbarhet. Sikker utveksling av informasjon mellom systemer, tjenester og driftsleverandører blir dermed essensiell. Kommunikasjonslinjer og infrastruktur internt og mot leverandørene er en stor utfordring og forbundet med høy risiko. Det er stor risiko for feil eller mangler i konfigurasjoner og kontroll og styring med denne. Nye løsninger gir nye innganger og teknisk ulike måter å aksessere systemer på. Dette mener foretak i verste fall kan resultere i feil og nedetid.

4.1.6 Flytting av driftssted

En rekke foretak melder om flytting av driftssted og bytte av leverandører og tekniske utfordringer knyttet til dette. Foretak opplyser at omfattende og vanskelig tilgjengelige lovkrav, compliance-krav og sikkerhetskrav kompliserer arbeidet med strategiske beslutninger for utkontraktering. Nye lovkrav kan være uklare og det er lite tolkningspraksis. Dette gjør at det er stor risiko forbundet med langsiktige strategiske beslutninger.

En sentral premissgiver i bransjen mener at finansielle tjenester ikke bør flyttes til sky, men (fortsatt) bør driftes i fjellhaller i Norge. Driftsstedene for skydrift består av "overflateanlegg" og er sårbare for et organisert angrep.

4.1.7 Digitale angrep

Det synes å være bred enighet hos foretakene om at det i dag eksisterer potensielle angripere som har ressurser til å sette betalingstjenestene i Norge ut av spill, og som også vil kunne hindre ethvert forsøk på å reetablere tjenesten. Norge vil i så tilfelle være uten betalingstjenester over lengre tid. Foretakene har begrenset med planer og muligheter for å yte betalingstjenester dersom en slik situasjon skulle oppstå. Foretakene som er spurt, viser til at det er et myndighetsansvar å utarbeide planer for en slik situasjon.

De mindre, daglige angrepene håndteres tilfredsstillende og gjør i det store og hele mindre og mindre skade.

4.1.8 Kompetanse

Foretakene melder om utfordringer med tilgang på relevant og ny kompetanse og vanskeligheter med å rekruttere utviklere, arkitekter, prosjekt-/test-ledelse samt kompetanse innenfor sikkerhet, compliance, og risiko. Enkelte foretak antar at det kan bli mangel på kompetanse innen programmeringsspråket Cobol. Dette kan gå ut over nyutvikling, feilretting og driftsstøtte. I tillegg er erfaren skykompetanse også en mangelvare.

Ny nasjonal strategi for IKT-sikkerhet fokuserer på mangelen på kryptologer. Enkelte foretak mente at det er like viktig med tverrfaglig forretningsmessig kompetanse til å håndtere krypteringsløsningene.

4.2 Spørreundersøkelse om sårbarhet

I likhet med tidligere år, gjennomførte Finanstilsynet i desember 2018 en spørreundersøkelse. 17 foretak besvarte undersøkelsen. Finanstilsynet ba foretakene vurdere i hvilken grad foretaket anser seg for å være sårbare for aktuelle trusler. Resultatene framgår av tabellene nedenfor. Samlet sett synes foretakenes vurdering av risikoen å være svakt økende også i 2018, slik den også var i 2017 og i 2016.

Grønt gir uttrykk for lav sårbarhet, 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, representerer gjennomsnittet av foretakenes vurderinger. En horisontal pil (der intervallet er -0,2 til +0,2) indikerer 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.

4.2.1 Støtte for strategiske beslutninger

Tabell 6 Støtte for strategiske beslutninger

	Sårbarhet	Foretakenes svar	Trend 2018	Trend 2017
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	Omfanget av mangler og feil i systemene		→	↘

Kilde: Finanstilsynet

Det er liten endring fra 2017 til 2018. Det er verdt å merke seg at foretakene mener at risikoen knyttet til dårlig datakvalitet er synkende. Dette kan ha sammenheng med at foretakene har arbeidet mye med klassifisering og sletting av data i forbindelse med datalagringsdirektivet (GDPR).

4.2.2 Beskyttelse av data

Tabell 7 Data er ikke tilstrekkelig beskyttet

	Sårbarhet	Foretakenes svar	Trend 2018	Trend 2017
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 epost, presentasjoner, tekst-dokumenter blir gjennomgått regelmessig med tanke på beskyttelse, eventuelt sletting?		↘	→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert.			

Kilde: Finanstilsynet

Foretakenes risiko knyttet til beskyttelse av data viser omtrent det samme bildet som i 2017. Finanstilsynet merker seg at risikoen knyttet til beskyttelse av ustrukturerte data er synkende, og antar at dette henger sammen med at det har vært ryddet og slettet i ustrukturerte data i forbindelse med datalagringsdirektivet (GDPR).

4.2.3 Drift

Tabell 8 Drift

	Sårbarhet	Foretakenes svar	Trend 2018	Trend 2017
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	Grad av kompleksitet i IT-systemene		↗	↗
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 nødstrømagregat))		→	→
9	Vår evne til å avdekke avvik i datatrafikken (unormal belastning, unormale porter/ protokoller, avvikende svartider) i driftsmønsteret og ta aksjon før skade		→	→
10	Vår beskyttelse mot dataangrep (Advanced persistence threat, trojaner, ransomware, DDoS)		→	→
11	Kvaliteten på kontinuitet- og katastrofeløsningene våre, jf. IKT-forskiften § 11		→	→
12	Samarbeidsrutiner med leverandører		→	→
13	Leveransepresset vi er utsatt for i markedet 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		→	→
	Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert.			

Kilde: Finanstilsynet

Finanstilsynet merker seg at risikoen knyttet til mangler i organisering, stillingsbeskrivelser, rapportering og kontroll har gått fra en synkende til en stabil trend. Dette kan skyldes at foretakene rapporterer at de har et mer komplisert leverandørbilde, med mange leverandører inne i verdikjeden. Dette henger sannsynligvis også sammen med at kompleksiteten i IT-systemene i 2018, som i 2017, anses å være økende.

Finanstilsynet noterer også at risikoen knyttet til press på leveranseapparatene fremdeles er økende, som følge av stort omfang av endringer og nye regulatoriske krav.

4.2.4 ID-tyveri

Tabell 9 ID-tyveri

	Sårbarhet	Foretakenes svar	Trend 2018	Trend 2017
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

Risikoen for at en angriper tar over en bruker-id og misbruker denne anses av foretakene noe mindre i 2018 enn i 2017. Dette kan henge sammen med at foretakene synes å ha innført bedre kontroller når det gjelder utlevering av bruker-id og passord til kunder og medarbeidere.

4.2.5 Interne misligheter

Tabell 10 Misbruk av tilgang til datasystemene

	Sårbarhet	Foretakenes svar	Trend 2018	Trend 2017
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

Når det gjelder risikoen knyttet til interne misligheter, er vurderingene lite endret fra 2017 til 2018.

4.2.6 Hvitvasking

Tabell 11 Hvitvasking

	Sårbarhet	Foretakenes svar	Trend 2018	Trend 2017
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

Hvitvaskingsrisikoen anses å være redusert som følge av forbedringer i IT-systemenes evne til å samle relevant informasjon om kunde, kunderelasjoner og kundeadferd. Dette kan henge sammen med at risikoen knyttet til mangelfull markedsovervåking viser en nedadgående trend.

4.3 Nasjonale vurderinger av trusselbildet

PSTs Trusselvurdering 2019, E-tjenestens Fokus 2019 og NSMs Risikobilde 2018 viser de siste par årene en økning i forsøk på industrispionasje mot foretak i finanssektoren for å innhente teknologisk og finansiell informasjon om norske virksomheter.

Den stadig økende trusselen fra utenlandske etterretningstjenester som innehar store kunnskaper og ressurser er bekymringsfull. Truslene består blant annet av forsøk på å rekruttere og styre hemmelige kilder i norske virksomheter. Det gjennomføres også operasjoner der formålet er innhenting av sensitiv informasjon og påvirkning av beslutningsprosesser. Dette gjelder både innenfor norsk politikk og forvaltning, forsvars- og beredskapssektoren, kritisk infrastruktur og forskning og utvikling.

Gjennom datanettverksoperasjoner fra fremmede stater, som både er billige, effektive og i konstant utvikling, kan det gjennomføres kartlegging av både infrastruktur og sårbarheter i nettverkene. De digitale verdiene i norske virksomheter er i stor grad bygget på skyteknologi og all kommunikasjon og arkivering foregår elektronisk. Verdifulle prosesser og forretningshemmeligheter eksisterer ofte kun digitalt og er derfor sårbare og må beskyttes.

I forkant av slike datanettverksoperasjoner har det gjerne foregått kartlegging av enkeltpersoner, for eksempel e-postadresser, brukerprofiler på sosiale medier eller i skytjenester, samt deres rolle innenfor en organisasjon.

Det er den russiske etterretningstjenesten som i dag anses som den største utfordringen, men også land som Kina vil kunne utføre etterretningsoperasjoner mot norske mål og virksomheter. Vellykkede operasjoner vil kunne påføre Norge stor skade. Russiske påvirkningsoperasjoner har som mål å undergrave politiske prosesser og øke polariseringen i Europa og NATO.

Foretakene må være bevisst på det globale trusselbilde når de vurderer tjenesteutsetting. Virksomheten kan få redusert kontroll over stadig mer komplekse verdikjeder, miste intern kompetanse og bli avhengig av eksterne tjenesteleverandører for å kunne levere sine tjenester.

5 Risikoområder

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.

Digital sårbarhet har så langt ikke ført til systemkriser, men alvorlig svikt har forekommet og sårbarheter har blitt avdekket. Et digitalt sammenbrudd kan komme brått og vil kunne få vidtrekkende samfunnsmessige konsekvenser. Finanssektoren er, i tillegg til finansnæringens egen infrastruktur, avhengig av felles infrastruktur som el-forsyning og telekommunikasjon, herunder nettverk.

Svikt hos sentrale aktører i finansnæringen eller i felles infrastruktur kan få betydelige samfunnsmessige konsekvenser. Dersom det ikke er mulig å 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 svekke tilliten til markedsplassene og det finansielle systemet. Dersom kriminelle får tilgang til store mengder kunde- og kontodata og kompromitterer disse eller gjøre data utilgjengelige, kan det skape betydelige utfordringer for kunder og foretak, og også kunne påvirke den finansielle stabiliteten. De samfunnsmessige virkningene vil kunne være særlig store hvis foretak som opererer på vegne av alle eller flere foretak rammes. Foretakenes arbeid med robuste driftsløsninger, inkludert kontinuitetsløsninger, kriseløsninger og beredskap, gjenopprettingsplaner og IKT-sikkerhetsarbeid, er vesentlige tiltak i arbeidet med å sikre finansiell stabilitet.

Det finnes i dag flere alternative betalingsmåter for forbrukere og foretak, noe som gjør deler av betalingssystemet mindre sårbart. Det ble i 2018 også stilt krav til løsninger for kontantberedskap[48].

[48] 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/

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) et bredt og godt bilde av tilstanden i den norske finansielle infrastrukturen. Det var i 2018 en hendelse i betalingssystemet som ble vurdert som kritisk, da det ble sendt doble posteringer fra avregningssystemet NICS til oppgjøret i Norges Bank.

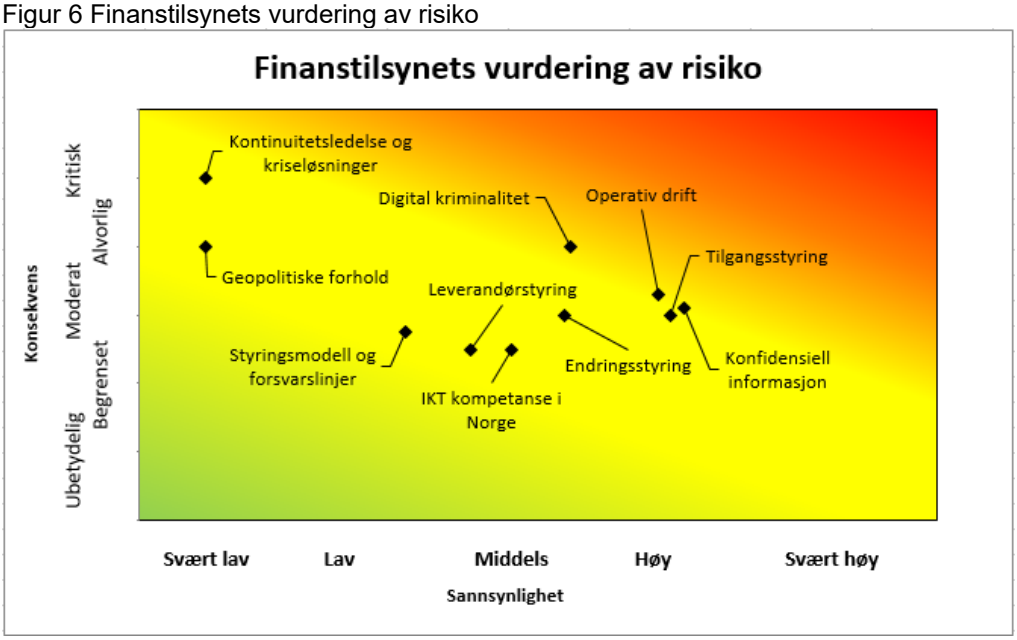
Det var i 2018 god regularitet på avregnings- og oppgjørssystemene og kommunikasjonen mot det internasjonale betalingssystemet Swift og det internasjonale oppgjørssystemet CLS.

Finanstilsynet vurderer den norske finansielle infrastrukturen som robust, selv om det var en kritisk hendelse som medførte feil i betalingssystemet og hendelser som gjorde betalingsløsninger utilgjengelige i perioder.

5.2 Foretakene

Figur 6 viser Finanstilsynets vurdering av områder med de mest sentrale truslene og sårbarhetene i finanssektoren. I figuren er de ulike risikoområdene klassifisert etter sannsynlighet for at en alvorlig negativ hendelse oppstår, og graden av konsekvens for det enkelte foretak. Grunnlaget for plasseringen i matrisen av de enkelte områdene, herunder sårbarheter med sannsynlighet og konsekvens, er omtalt nedenfor.

Figur 6 Finanstilsynets vurdering av risiko



Kilde: Finanstilsynet

Finanstilsynet vurderer risiko knyttet til sårbarheter i foretaks operative drift, tilgangsstyring, kontinuitetsledelse og kriseløsninger, beskyttelse av konfidensiell informasjon og forsvarsverk mot digital kriminalitet, som de mest sentrale truslene knyttet til foretakenes bruk av IKT. Alle disse vurderes å ha middels til høy risiko. Sårbarheter knyttet til foretaks leverandørstyring, endringsstyring, styringsmodell og forsvarslinjer knyttet til IKT-virksomheten, samt sårbarheter knyttet til geopolitiske forhold og IKT-kompetanse i Norge, er også trusler knyttet til foretakenes bruk av IKT. Disse vurderes å ha middels risiko.

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.

Operativ drift

Foretakenes tjenester er basert på digitale løsninger. 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.

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 flere 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. Stor grad av utkontraktering og bruk av skytjenester skaper også en driftskompleksitet med økt sårbarhet. Press på foretakenes og leverandørenes leveranseapparat, med stort omfang av endringer, øker risikoen for at feil oppstår.

Den teknologiske gjelden i foretakenes systemer medfører krevende integrasjoner og tilpasninger mellom nye og gamle systemer, og med svakheter i arkitekturen utgjør også dette en risiko for driftsproblemer. Mangelfull tilgang på kompetanse innen forvaltning og drift av stormaskinløsninger medfører utfordringer innen driftsstøtte. Ved bruk av skyteknologi utgjør foretaks mangel på kompetanse risiko for feil i oppsett og sikring av data.

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

- Sannsynligheten 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.
- Sannsynligheten for driftsproblemer som rammer felles operasjonell infrastruktur, vurderes som *middels* og med *alvorlig* konsekvens.
- Sannsynligheten for utilgjengelige tjenester som følge av mangelfull kapasitetsstyring, vurderes som *middels* og med *alvorlig* konsekvens.
- Sannsynligheten for at systemkomponenter i redundante løsninger feiler, som følge av mangelfull overvåking og test, vurderes som *lav* og med *alvorlig* konsekvens.
- Sannsynligheten for driftsproblemer (nettverk og tjenester) som følge av ugyldige digitale sertifikater eller ugyldige lisenser, vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for driftsproblemer, som følge av mangelfull kompetanse innen driftstøtte for stormaskin, vurderes som *middels* og med *moderat* konsekvens.

Digital kriminalitet

Sårbarheter knyttet til foretakenes styring, forsvarsverk og reaksjonsevne, herunder organisering av 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.

Finanstilsynet konstaterer at metodene som kriminelle benytter er endret fra tidligere år, hvor angrepene hovedsakelig dreide seg om å plassere ondsinnet kode eller gjennomføre tjenesteangrep gjennom DDoS-angrep. Metodene som nå benyttes er mer sammensatte, med kombinasjoner av ulike former for sosial manipulering for å etablere et digitalt fotfeste på innsiden av foretakets nettverk, avanserte teknikker for å skjule sin tilstedeværelse i nettverket og med grundig kartlegging fra innsiden før selve angrepet iverksettes.

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

- Sannsynligheten for at ansatte benyttes ufrivillig, gjennom sosial manipulering som middel for digitalt angrep, vurderes som *høy* og med *alvorlig* konsekvens.
- Sannsynligheten for at ansatte benyttes ufrivillig, gjennom trusler som middel for digitalt angrep, vurderes som *lav* og med *alvorlig* konsekvens.

- Sannsynligheten for at ansatte hos leverandører benyttes ufrivillig, gjennom trusler som middel for digitalt angrep, vurderes som *lav* og med *moderat* konsekvens.
- Sannsynligheten for at utro medarbeidere i foretakets eller leverandørers utviklingsmiljø plasserer ondsinnet kode i forretningskritiske applikasjoner, vurderes som *lav* og med *moderat* konsekvens.
- Sannsynligheten for at foretak rammes av løsepengevirus med tap av forretningskritiske data, som følge av skadevare (kryptering), vurderes som *lav* til *middels* og med *kritisk* konsekvens.
- Sannsynligheten for at kriminelle lykkes med å utnytte sårbarheter i maskinvare (CPU) eller fastvare (UEFI), som rammer et finansforetak, vurderes som *lav* og med *moderat* konsekvens.
- Sannsynligheten for at foretaket ikke avdekker kriminelle som har etablert et digitalt fotfeste på innsiden av nettverket før skade avverges, vurderes som *middels* med *kritisk* konsekvens.
- Sannsynligheten for at alvorlige sikkerhetshull ikke blir tettet som følg av mangelfull sikkerhetsoppdateringer (patch-management), vurderes som *middels* med *alvorlig* konsekvens.
- Sannsynligheten for at nye applikasjoner eller endringer i eksisterende applikasjoner settes i produksjon med alvorlige sikkerhetshull, vurderes som *middels* med *alvorlig* konsekvens.

Konfidensiell informasjon

Betrodde medarbeidere hos foretakene og betrodd personell hos foretakenes leverandører har tilgang til konfidensiell informasjon om foretakenes kunder og om foretakenes interne forhold. Tilgangen til denne informasjonen er basert på bakgrunnssjekk, arbeidsoppgaver og tillit som den enkelte er gitt. Finanstilsynet har gjennom tilsyn konstatert at foretak mangler kontrollsystemer for å avdekke om konfidensielt innhold forsøkes kopiert til mobilt lagringsmedium eller sendes som vedlegg til e-post. Slike mangler ser ut til å være en generell utfordring i finansnæringen.

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

- Sannsynligheten for at konfidensiell informasjon kommer på avveie som følge av mangelfull kontroll ved utsendelse av e-post, vurderes som *svært høy* og med *moderat* konsekvens.
- Sannsynligheten for at konfidensiell informasjon kommer på avveie som følge av mangelfull kontroll ved bruk av USB-lagringsmedier, vurderes som *svært høy* og med *moderat* konsekvens.
- Sannsynligheten for at konfidensiell informasjon kommer på avveie som følge av mangelfull kontroll av personell hos leverandører, vurderes som *middels* og med *alvorlig* konsekvens
- Sannsynligheten for at konfidensiell informasjon kommer på avveie som følge av mangelfull tilgangsstyring og -kontroll, vurderes som *høy* 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 2018 registrert at tilgangsstyring, som en proaktiv kontroll av tilganger til systemer og teknisk infrastruktur, er en gjentakende utfordring for flere av foretakene. Spesielt utgjør svakheter innen tilgangsstyring av medarbeidere og personell hos leverandører med utvidede rettigheter en risiko. Detaljerte og kompliserte lister, med oversikter over medarbeideres tilganger og autorisasjonsnivå, utgjør en risiko for at ledere feiltolker disse.

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

- Sannsynligheten for at medarbeidere med utvidede tilgangsrettigheter utfører ulovlige handlinger, vurderes som *lav* og med *moderat* konsekvens.
- Sannsynligheten for at personell hos en leverandør med utvidede tilgangsrettigheter utfører ulovlige handlinger, vurderes som *lav* og med *alvorlig* konsekvens.
- Sannsynligheten for at medarbeidere eller personell hos leverandører har administrasjonsrettigheter uten at ledelsen er klar over dette, vurderes som *middels* 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 *moderat* konsekvens.
- Sannsynligheten for at personell hos leverandøren, eller dens underleverandør, bryter regler i utførelsen av driftsoppgaver, vurderes som *middels* og med *alvorlig* konsekvens.

Kontinuitetsledelse og kriseløsninger

Sårbarheter innen kontinuitetsledelse, herunder krise- og beredskapsplaner, utgjør en risiko dersom en alvorlig hendelse inntreffer. Dette kan dreie seg om mangelfull trening og øvelse, eller manglende testing av foretakets kriseløsning. 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.

Mangelfulle analyser av forretningsmessige konsekvenser som følge av en krise, utgjør en risiko for at kriseløsningen 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 kriseløsninger, øker risikoen for digitale angrep i en spesielt sårbar situasjon for foretaket.

Finanstilsynet konstaterer at foretakene i stor grad har etablert kriseløsninger, også omtalt som beredskapsløsninger eller reserveløsninger, som skal iverksettes dersom normal driftsløsning ikke er tilgjengelig. Det er imidlertid avdekket en del mangler som kan gi foretak utfordringer med å håndtere en alvorlige IKT-hendelse. Dette gjelder blant annet mangler i styrende dokumenter, opplæring, trening, øvelse og test av kriseløsning. Foretakene bør i større grad rette oppmerksomhet mot

kontinuitetsledelse og kriseløsninger, for å redusere risikoen for omfattende skader ved alvorlige hendelser.

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

Finanstilsynet vurderer den samlede risikoen knyttet til sårbarheter ved **kontinuitetsledelse og kriseløsning som middels** til **høy**. Dette er basert på følgende vurderinger:

- Sannsynligheten for at foretakets kriseløsning ikke er etablert i henhold til foretakets behov, som følge av manglende eller mangelfulle forretningsmessige konsekvensanalyser og krav, vurderes som *middels* og med *kritisk* konsekvens dersom kriseløsningen må iverksettes.
- Sannsynligheten for at foretak og dets medarbeidere ikke er tilstrekkelig forberedt på å håndtere en alvorlig situasjon, som følge av mangelfull trening og øvelser, vurderes som *høy* og med *alvorlig* konsekvens.
- Sannsynligheten for at et foretaks kriseledelse og dets leverandørs kriseledelse ikke er tilstrekkelig samordnet og koordinert ved en alvorlig hendelse, vurderes som *middels* og med *kritisk* konsekvens.
- Sannsynligheten for at foretak ikke klarer å håndtere en alvorlig hendelse på en god måte som følge av uklare roller og ansvar internt og mellom foretaket og leverandører, vurderes som *middels* og med *alvorlig* konsekvens.
- Sannsynligheten for at kriseløsningen ikke fungerer som forventet, som følge av mangelfulle tekniske tester og evaluering av disse, vurderes som *middels* og med *kritisk* konsekvens.
- Sannsynligheten for mangelfull sikkerhetsoppdateringer av kriseløsningen, vurderes som *middels* og med *alvorlig* konsekvens.
- Sannsynligheten for at et foretaket som blir rammet av et alvorlig digitalt angrep ikke vil være i stand til å håndtere situasjonen på en god måte som følge av manglende kontinuitetsplan for cyber-angrep og mangel på trening og øvelse, vurderes som *svært høy* og med *kritisk* 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 kan dette medføre 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 prosessen med å overføre tjenesten til annen leverandør, spesielt der overføringen skjer som følge av at leverandøren ikke oppfyller leveransekravene.

Utfordringen for mindre foretak er hovedsakelig å etablere en tilstrekkelig bestiller-kompetanse for å sikre at alle relevante krav inntas i avtalen med leverandøren ved etablering av tjenesten, og at foretaket har medarbeidere som har kompetanse til å følge opp leverandøren. Store foretak og allianser har gjennom avtaleverk og samhandlingsmodeller som regel etablert krav som legger føringer for leverandørstyringen. Utfordringen er kompleksitet og omfanget av tjenestene, og omfanget av leverandører, med underleverandører.

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.
- Sannsynligheten for at sikkerhetsbrudd inntreffer, som følge av mangelfull oppfølging og forankring av sikkerhetskravene hos leverandøren, vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for uforsvarlig lang reetableringstid ved alvorlige driftsavbrudd som følge av uklare roller og ansvar i samhandlingen med leverandøren og mellom leverandørene, vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for utilgjengelige tjenester, som følge av manglende overvåking av kvaliteten på tjenesten, vurderes som *lav* og med *moderat* konsekvens.
- Sannsynligheten 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 foretakets mangelfulle kompetanse om foretakets utkontrakterte tjenester, vurderes som *middels* og med *begrenset* konsekvens.
- Sannsynligheten for at manglende risikovurdering (periodisk) ikke avdekker svak bærekraft hos leverandøren, for eksempel som følge av en krevende likviditetssituasjon (konkursrisiko), utfordrende ressurssituasjon, eller andre forhold som kan true leverandørens leveranseevne, vurderes som *lav* og med *moderat* konsekvens.
- Sannsynligheten for at alvorlige svakheter i en leverandørs internkontroll ikke avdekkes, gjennom en leverandørs valgte revisors arbeid med uavhengig revisjonserklæring, vurderes som *middels* og med *moderat* 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 forhold som øker risikoen for at sårbarheter introduseres ved endringer i IT-systemene som følge av for svak styring og kontroll.

Finanstilsynet registrerte i 2018 utfordringer i foretaks endringsstyring. Gjennom hendelsesrapporteringen til Finanstilsynet framgår det at alvorlige hendelser oppstod i forbindelse med 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 til høy* og konsekvensen som *moderat*. Dette er basert på følgende vurderinger:

- Sannsynligheten 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 det ikke er etablert tilstrekkelige kontroller for å identifisere endringer som er satt i produksjon uten at endringsprosessen er fulgt, såkalte uautoriserte endringer, vurderes som *høy* og med *alvorlig* konsekvens.
- Sannsynligheten for at den høy endringstakt medfører at nye tjenenester settes i produksjon uten nødvendig kvalitet, vurderes som *høy* og med *moderat* konsekvens.

Styringsmodell og forsvarslinjer

Sårbarheter knyttet til foretakets styringsmodell, som består blant annet av policyer, strategier, standarder og retningslinjer, utgjør en risiko for at foretakets risikostyring og internkontroll ikke etableres i samsvar med foretakets risikoprofil.

Sårbarheter knyttet til foretakets tre forsvarslinjer utgjør en risiko for at avvik i implementering av styringsmodellens krav, og at overvåking og kontroll ikke avdekker alvorlige svakheter innen foretakets styring og kontroll.

Finanstilsynet konstaterer at det er mangelfull forvaltning av styrende dokumenter ved at enkelte dokumenter ikke er formelt godkjent eller oppdatert. I noen tilfeller er ikke kravene i styrende dokumenter implementert og operasjonalisert. Det er også tilfeller der rolle og ansvar mellom første- og andrelinjeforsvar ikke er tydelig definert.

Finanstilsynet vurderer den samlede risikoen knyttet til sårbarheter ved **foretakets styringsmodell og forsvarslinjer** som **lav** til **middels**. Sannsynligheten for at de tre forsvarslinjene gjennom sin aktivitet

ikke avdekker alvorlige svakheter i foretakets internkontroll vurderes som *lav* til *middels* og konsekvensen som *moderat*. Dette er basert på følgende vurderinger:

- Sannsynligheten for at mangler i etterlevelse av lover og regler ikke oppdages, som følge av mangelfull kontroll av foretakets operative ledelse, vurderes som *lav* og med *alvorlig* konsekvens.
- Sannsynligheten for at viktige krav i styrende dokumenter ikke implementeres og operasjonaliseres, vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for uklare roller mellom foretakets første- og andrelinjeforsvar, som fører til alvorlige svakheter i overvåkingen av foretakets styring og kontroll, vurderes som *lav* og med *begrenset* konsekvens.
- Sannsynligheten for at alvorlige sårbarheter ikke avdekkes, som følge av mangelfull eller fraværende prosess for risikoidentifisering, vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for at alvorlige svakheter i internkontrollen ikke avdekkes av internrevisjonen, som følge av mangelfull kompetanse og risikoforståelse hos foretakets internrevisjon, vurderes som *lav* og med *moderat* konsekvens.

IKT-Kompetanse i Norge

Sårbarheter som følge av mangel på tilgang til ekspertise innen driftsoperasjoner, arkitektur, teknologi, utvikling og utviklingsmetodikk, 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.

Sårbarheter knyttet til mangel på tilgang til IKT-kompetanse i Norge, og det faktum at det utdannes for få innen IKT-området, utgjør en risiko for økt avhengighet av utenlandske aktører. Dette kan medføre alvorlige konsekvenser for finansnæringen om aktører blir avskåret fra å utføre nødvendige oppgaver for å opprettholde sikker og stabil drift.

Finanstilsynet konstaterer at tilgang til kompetanse og ressurser innen IKT-området i Norge er en utfordring for finansnæringen og dens leverandører. Dagens kompetansesituasjon i Norge anses ikke å være kritisk, men sårbarheten vil kunne forsterkes i årene framover som følge av begrenset utdanningskapasitet og økende etterspørsel. Utkontraktering av IKT-tjenester til utlandet kan over tid resultere i tap av kompetanse i Norge innen nevnte områder.

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

- Sannsynligheten for at mangelfull kompetansestyring i foretak 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 om tjenester som utvikles og driftes av leverandører medfører brudd på lover og regler, vurderes som *middels* og med *moderat* konsekvens.

Geopolitiske forhold

Avhengigheten av IKT-kompetanse og IKT-tjenester fra utlandet er økende for finansnæringen. Dette er en avhengighet som kan skape betydelige utfordringer for deler av finansnæringen dersom det oppstår alvorlige situasjoner som forhindrer aktører i utlandet fra å opprettholde sine leveranser av kritiske IKT-tjenester. Geopolitiske utviklingstrekk med økt uro og usikkerhet er forhold som utgjør en risiko for at utenlandske aktører kan rammes.

Basert på nasjonale og internasjonale trusselvurderinger, mener Finanstilsynet at dette er forhold som foretakene må ta hensyn til for å sikre at kritiske IKT-tjenester, som leveres fra aktører i utlandet som rammes, kan overtas av andre aktører i Norge eller utlandet innen den tid som er nødvendig for å opprettholde sikker og stabil drift.

Finanstilsynet vurderer den samlede risikoen knyttet til sårbarheter overfor utenlandske aktører som leverer kritiske IKT-tjenester til Finansnæringen i Norge, som **middels** i dag. Sannsynligheten for uønskede hendelser, der utenlandske leverandører blir avskåret fra å levere sine tjenester, vurderes som svært *lav* og konsekvensen som *alvorlig*.

5.3 Foretakenes kunder

Påloggingsinformasjon på avveie og misbruk av BankID

Den økte digitaliseringen har medført at foretakenes kunder har måtte ta i bruk digitale identifiserings- og autoriseringsløsninger. Dette gjør kunden sårbar og utgjør en betydelig risiko for misbruk, med i verste fall store økonomiske konsekvenser for den skadelidende.

Passord og PIN-koder kan for enkelte være vanskelig å huske og kunden velger å skrive ned denne informasjonen. Dette utgjør en risiko for at informasjonen kommer uvedkommende i hende og at kunden blir svindlet. Nære relasjoner kan ha tilgang til hverandres digitale identifiserings- og autoriseringsløsninger, og personer som ikke er datakyndige overlater sin digitale signatur til andre for å utføre sine finansielle tjenester.

BankID har et svært bredt bruksområde. Det er derfor knyttet en konsentrasjonsrisiko til misbruk av BankID, ved at misbruket kan oppstå innen mange områder, slik som inngåelse av kjøpekontrakter, tegning av forsikring, skatteopplysninger, låneavtaler m.m. Det har vært en økning i antall låneavtaler som inngås gjennom misbruk av andres digitale signatur (BankID), i særlig grad utført av personer i nær relasjon til den som blir svindlet. Politiet peker på tre hovedområder der BankID brukes til svindel, blant annet misbruk av nære relasjoner.[49]

Identitetstyveri

Ifølge en nylig undersøkelse (2019) fra Norsk senter for informasjonssikring (NorSIS) har mer enn 150 000 nordmenn over 18 år opplevd misbruk av egen identitet de to siste årene. Vanlig misbruk skjer ved kjøp av varer og tjenester over nett (28 prosent), eller ved at svindlere tar opp lån eller gis kreditt (17 prosent). Selve tyveriet kan skje ved at svindlere stjeler pass eller bankkort som sendes i posten. Ifølge NorSIS er det kun 38 prosent av ofrene for ID-tyveri som anmelder dette til politiet. Se også punkt 3.9.10.

Sosial manipulering

Kjærlighetssvindel, hvor kriminelle etablerer en relasjon med sitt offer over lengre tid før selve svindelen iverksettes, er et psykologisk spill som fanger offeret i en følelsesmessig relasjon som det kan være vanskelig å komme ut av. Kundene utsettes også for fakturasvindel, investeringsvindel og annen form for økonomisk svindel.

Situasjonen vil ofte oppleves som svært krevende for den som rammes, og dens nærstående. Finanstilsynet er kjent med at bankene tar initiativ ovenfor kunden der banken fatter mistanke om at en kunde er utsatt for sosial manipulering. Samtidig er dette krevende for bankene ettersom kunden i en del tilfeller ikke innser, eller vil akseptere, at pengeoverføringen forårsakes av manipulasjon og svindel. Ettersom denne type svindel er et økende problem, oppfordrer Finanstilsynet foretakene til å fortsette arbeidet med å finne effektive tiltak ovenfor de ulike kundegruppene.

Kundegrensesnitt gjennom nye aktører

Gjennom Open Banking, herunder PSD 2, vil brukerne oppleve at nye aktører som ikke er banker, vil tilby løsninger hvor kunden får tilgang til sine kontoer. Finanstilsynet mener bankene og de nye aktører bør ta et felles ansvar for at kunder opplyses og informeres om de nye regulatoriske kravene, og hva dette vil innebære.

Foretakenes integritet som følge av digital kriminalitet

Digital kriminalitet skaper usikkerhet hos brukerne av foretakets tjenester. Ved alvorlige hendelser vil usikkerheten blant foretakets kunder forsterkes. Finanstilsynet har vært kontaktet av kunder som er redde for at deres midler skal gå tap som følge av digital kriminalitet. Dette er en bekymring som foretakene må ta på alvor.

[49] https://www.nettavisen.no/økonomi/politiet-dette-er-de-vanligste-bankid-svindlene/3423676674.html

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-risiko vil bli gjennomgått. Tilsyn med organisering av IKT-/cyber-sikkerhetsarbeidet, sikkerheten knyttet til foretakenes IKT-løsninger og organiseringen av overvåkingen vil bli vektlagt. Det omfatter blant annet foretakenes kontroll med tilganger til systemer, særlig der det er systemer som inneholder sensitiv informasjon, og foretakenes testing mht. inntrenging i foretakenes systemer.

Andre prioriterte tema for tilsyn vil være overordnet styring og kontroll med IKT-virksomheten, foretakenes beredskapsarbeid knyttet til kontinuitet og kriseløsninger og testing av disse, utkontraktering, foretakenes betalingstjenester og IKT-løsninger for å avdekke hvitvasking og terrorfinansiering. Finanstilsynet vil blant annet legge vekt på å kontrollere at foretakene har rutiner for å påse at uttrekkene til antihvitvaskingssystemene er komplette.

Bruk av ny teknologi eller større endringer på IKT-området er også aktuelle tema.

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

6.2 Arbeid med betalingssystemer

Det reviderte betalingstjenestedirektivet (PSD 2) fra EU er tatt inn i norsk lovgivning, og vil ligge til grunn for Finanstilsynets oppfølging av foretakenes betalingstjenester. Foretakene vil blant annet bli fulgt opp mht. etterlevelse av ny forskrift om systemer for betalingstjenester[50], risiko knyttet til betalingstjenestene og etterlevelse av meldeplikten.

Samarbeidet med Norges Bank vil videreføres.

[50] Forskrift om systemer for betalingstjenester

6.3 Oppfølging av hendelser

Oppfølging av hendelser er et prioritert område. Finanstilsynet vil i 2019 følge nøye med på utviklingen og 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 hendelsesforløpet, og ved behov vil det bli gjennomført oppfølgingsmøter. Særlige tiltak vil bli vurdert.

6.4 Beredskapsarbeid

Arbeidet i Beredskapsutvalget for finansiell infrastruktur (BFI) videreføres. BFI gjennomgår blant annet hendelsesscenarier, og det vurderes om ansvarsforhold ved krisesituasjoner er tilstrekkelig klare. Det er planlagt gjennomføring av beredskapsøvelser også i 2019, 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[51]. Finansdepartementet har oppnevnt Finanstilsynet som sektorvis responsmiljø (SRM) på finansmarkedsområdet, og vil utøve rollen i samarbeid med Nordic Financial CERT etter avtalte regler for informasjonsutveksling. Med bakgrunn i NSMs rammeverk, arbeides det med en formalisering av samhandlingen mellom Finanstilsynet og Nordic Financial CERT for å etablere et sektorvis responsmiljø (SRM) for den delen av finansmarkedsområdet som Finanstilsynet har tilsyn med.

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),
- grensekryssende virksomhet

[51] 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, og at løsninger som lanseres har en funksjonalitet i tråd med forbrukernes forventninger. Det vil blant annet bli fulgt opp at løsninger for betalingstjenester ikke krever at forbrukerne må akseptere tilleggsfunksjonalitet for å kunne benytte seg av betalingstjenesten og at forbrukerne gis mulighet til å beskytte seg mot uønskede hendelser, som for eksempel adgang til sperring av kort for bruk på Internett.

Ved hendelser vil Finanstilsynet følge opp at foretakene gir kundene informasjon om hvordan de blir rammet og hvordan foretaket eller kunden selv kan avhjelpe situasjonen.

Finanstilsynet vil følge opp at bankene ivaretar sine plikter når det gjelder etterlevelse av finansforetakslovens[52] bestemmelser om tilbud av kontanter. Finanstilsynet vil også følge opp at bankene har etablert løsninger i tråd med finansforetaksforskriftens bestemmelser om løsninger for å møte økt etterspørsel etter kontanter i en krisesituasjon[53].

[52] https://lovdata.no/dokument/NL/lov/2015-04-10-17/KAPITTEL_16#KAPITTEL_16
[53] https://lovdata.no/dokument/SF/forskrift/2016-12-09-1502/KAPITTEL_16#KAPITTEL_16

Ordliste

Term/forkortelse	Betydning
3D Secure	3D 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".
AISP	Account Information Service Providers. Se også 'Opplysningsfullmakt'.
API	Application Programming Interface. Grensesnitt i en programvare som gjør at spesifikke deler av denne kan kjøres fra en annen programvare.
AML	Tiltak mot hvitvasking (Anti Money Laundering)
BFI	Beredskapsutvalget for finansiell infrastruktur Koordineringsutvalg ved kriser i finanssektoren. Ledes av Finanstilsynet.
Betalingsfullmakt	Adgang for aktører til å initiere betalinger på vegne av kunder.
Blokkjede	Liste med data/transaksjoner, kalt blokker, som er koblet sammen i en kjede og sikret ved hjelp av kryptografi
Checkout-løsning	Løsning med flere integrerte betalingsmuligheter, f. eks. kort, faktura og delbetaling
CLS	Continuous Linked Settlement. Internasjonalt oppgjørssystem for valutahandler
COBIT	Styringsrammeverk for å utvikle, organisere og implementere gode og sikre strategier for informasjonsforvaltning
Cobol	COBOL er et programmeringsspråk designet for forretningsbruk. Mainframe er datamaskiner som hovedsakelig brukes av store organisasjoner til deres kritiske applikasjoner for behandling av store mengder data.
CRM	Customer-relationship management. System for håndtering av relasjoner til eksisterende og potensielle kunder
Datasenter	Et dedikert område, evt. én eller flere bygninger, som inneholder datasystemer og tilhørende komponenter som f. eks. telekommunikasjon- og lagringssystemer
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting and Conformance
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.
ESMA	European Securities and Markets Authority. Den europeiske verdipapir- og markedstilsynsmyndigheten.
Falske nyheter	Nyhetsliknende opplysninger med uriktig, mangelfullt eller villedende innhold eller med falsk avsender som noen med vilje lager og sprer gjennom ulike nyhetskanaler og sosiale medier

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
IKT	Informasjons- og kommunikasjonsteknologi
ISACA	Information Systems Audit and Control Association
ISAE 3402 Type II	Forsikringsstandard. Assurance Reports on Controls at a Service Organization
ISO 20022	Financial Services - Universal financial industry message scheme
Kontantberedskap	Bankers plikt til å ta imot og gjøre kontanter tilgjengelige for kundene. Denne plikten er ikke begrenset til normalsituasjon, men kan bli enda viktigere i en eventuell krisesituasjon
Kontinuitetsplan	En plan som skal beskrive de alternative rutinene som en virksomhet må følge når en kritisk situasjon har oppstått
Løsepengevirus	Skadevare som begrenser tilgangen til infiserte IKT-løsninger og krever en løsesum for å fjerne begrensningene.
Maskinlæring (ML)	Utvikling av algoritmer som gjør datamaskiner i stand å lære fra og utvikle atferd basert på empiriske data
Nedetid	Den tid en maskin, tjeneste, applikasjon ol. er ute av funksjon
NICS	Norwegian Interbank Clearing System
Nordic Financial CERT	Nordic Financial CERT (NFCERT) er en samarbeidsorganisasjon etablert av nordiske finansforetak som skal identifisere og bekjempe cyber-angrep rettet mot finansnæringen i Norden, se www.nfcert.org.
Open Banking	Open banking er et foretaks åpne API-er (grensesnitt) som gjør det mulig for tredjepart å bygge løsninger som utveksler informasjon mellom tredjeparts løsninger og foretakets løsninger.
Opplysningsfullmakt	Aktører som kan hente informasjon fra bankkonto på vegne av kunde.
Overflateanlegg	Datasenter som er ikke er etablert i fjellhall eller under bakken.
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.
PISP	Payment Initiation Service Providers. Se også "Betalingsfullmakt".
PSD 2	Revidert betalingstjenestedirektiv 2015/36/EU
Revisjonserklæring	Egenerklæring om at revisjonsarbeidet med styringssystemet er ivaretatt både internt og eksternt hvis man har en ekstern leverandør.
RPO	Recovery Point Objective
RTO	Recovery Time Objective
Skytjenester	Skybasert plattform, infrastruktur, program eller lagringstjenester. 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.
SRM	Sektorvist responsmiljø. Skal ha oversikt over egen sektor, være informasjonsknutepunkt for alle relevante virksomheter og være sektorens bindeledd mot NSM NorCERT.

Sterk kundeautentisering	Transaksjoner som er autentisert ved hjelp av tofaktorautentisering eller mer, f.eks. pinkode + passord.
SSD-disker	Solid State Drives. Elektronisk, flashminnebasert lagringsenhet.
Swift	The Society for Worldwide Interbank Financial Telecommunication.
Trojaner	Et dataprogram som utgir seg for å være nyttig, men som i virkeligheten er skadelig

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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

04.2019