FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Finanssektorens bruk av informasjons- og kommunikasjonsteknologi (IKT)

RISIKO- OG SÅRBARHETSANALYSE (ROS)

2020

Risiko- og sårbarhetsanalyse

Finanstilsynet utarbeider hvert år en risiko- og sårbarhetsanalyse (ROS-analyse) av finanssektorens bruk av IKT. Formålet med rapporten er å beskrive risiko og trekke frem de mest sentrale truslene mot, og sårbarheter i, foretakenes IKT-systemer og den finansielle infrastrukturen som kan ha betydning for foretak, finansiell stabilitet og velfungerende markeder. Sårbarheter og trusler rettet mot foretakets kunder beskrives også. Gjennom oppfølging av rapporterte hendelser, funn fra tilsyn og annen kontakt mot finanssektoren får Finanstilsynet god innsikt i foretakenes bruk av IKT, betalingsløsninger og aktuelle risikoområder.

INNHOLD

Redaksjon avsluttet 13. mai 2020

1. Oppsummering

Den norske finansielle infrastrukturen er robust. Det var ingen IKT-hendelser med konsekvenser for finansiell stabilitet i 2019. Det ble imidlertid rapportert noen flere IKT-hendelser i 2019 enn i 2018. Tilgjengeligheten til betalingstjenester og øvrige kunderettede tjenester var etter Finanstilsynets vurdering likevel bedre i 2019 enn i 2018. Selv om hendelsene medførte negative konsekvenser for berørte kunder, vurderes tilgjengeligheten til tjenestene samlet sett som tilfredsstillende.

Under koronakrisen har Finanstilsynet og Beredskapsutvalget for finansiell infrastruktur (BFI) rettet særlig oppmerksomhet mot virksomheter som støtter viktige funksjoner, herunder de kritiske samfunnsfunksjonene definert av Direktoratet for samfunnssikkerhet og beredskap. De sentrale foretakene i den norske finansielle infrastrukturen har gode beredskapsplaner. Aktørene har så langt hatt god kontroll på driftssituasjonen og har raskt iverksatt nødvendige tiltak.

Omfanget av digital kriminalitet øker fortsatt, men har så langt ikke ført til større hendelser hos foretak i den norske finanssektoren. Foretakenes forsvarsverk er styrket og angrep avverges hovedsakelig før det får alvorlige konsekvenser. Kun seks av de 206 rapporterte IKT-hendelsene i 2019 var sikkerhetshendelser.

Finanstilsynet har gjennom tilsyn og hendelsesrapportering observert sårbarheter som kan utgjøre risiko for alvorlige hendelser i finanssektoren. Finanstilsynet har blant annet påpekt forhold som bankers og betalingsforetaks utilstrekkelige oppfølging av leverandører, spesielt leverandørers etterlevelse av foretakets sikkerhetskrav, og at risikoanalysen av IKT-virksomheten ikke avdekker den reelle risikoen i tilstrekkelig grad. Det er også avdekket svakheter innen bankers kontinuitets- og kriseledelse. For både banker og verdipapirforetak er det påpekt mangelfulle rutiner for informasjonsklassifisering og -beskyttelse ved utveksling og håndtering av informasjon, samt mangler i rutiner for sikkerhetstesting.

For å sikre robustheten i den finansielle infrastrukturen mener Finanstilsynet at foretakene fortsatt bør styrke arbeidet på IKT-området, både for å redusere sannsynligheten for avvik og å bedre IKT-sikkerheten.

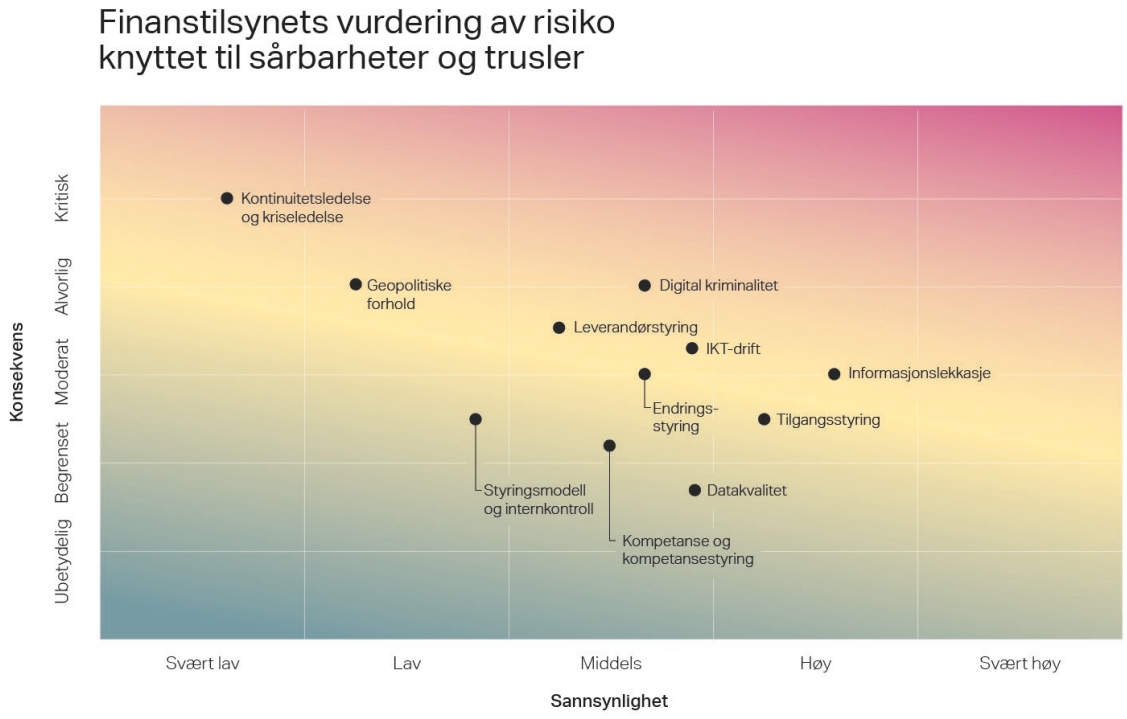
Finanstilsynets vurdering av risiko knyttet til sårbarheter og trusler i foretakenes IKT-virksomhet

Finanstilsynet vurderer sårbarheter knyttet til foretaks forsvarsverk mot digital kriminalitet og informasjonslekkasje, samt IKT-drift, som de mest sentrale truslene knyttet til foretakenes bruk av IKT. Risikoen vurderes til å være høy.

Risiko knyttet til sårbarheter i foretaks kontinuitets- og kriseledelse, geopolitiske forhold og tilgangstyring vurderes som middels til høy. Risiko knyttet til sårbarheter ved leverandørstyring, endringstyring, foretaks styringsmodell og internkontroll, kompetanse og kompetansestyring og datakvalitet vurderes til å være middels.

Figur 1.1 oppsummerer 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. Observasjoner og vurderinger som ligger til grunn for klassifiseringen fremgår av tabell 1.1, og er nærmere omtalt i kapitlene 3 til 6. Metodikken og detaljer som ligger til grunn for vurderingene er omtalt i vedlegg 2.

Figur 1.1



Kilde: Finanstilsynet

Tabell 1.1

Område	Sårbarheter og trusler som kan utgjøre en risiko for uønskede hendelser (Grad av risiko, sannsynlighet og konsekvens fremgår av figur 1.1)	Trend
Styringsmodell og internkontroll	Manglende oversikt over hvilke kontroller som inngår i foretaks internkontroll og hvordan kontrollene skal utføres, overvåkes og revideres, kan føre til at forhold som kan utgjøre en operasjonell risiko ikke avdekkes, og at risikoreduserende tiltak i tråd med foretakets risikotoleranse ikke iverksettes.	→
Kompetanse og kompetansestyring	Knapphet på ressurser i Norge innen drift, arkitektur, sikkerhet og ny teknologi, samt mangelfull kompetansestyring, kan føre til at foretak ikke får dekket dagens og fremtidens kompetansebehov. Problemer og feil som oppstår kan være utfordrende å løse. Avhengigheten til utlandet kan øke.	↗
Leverandørstyring	Komplekse leverandørkjeder, med flere leverandører og underleverandører i verdikjeden, krevende samhandlingsmodeller (strategisk, administrativt og operativt) og mangel på kompetanse kan føre til svakere oppfølging og kontroll med kritiske og utkontrakterte IKT-tjenester.	↗
Digital kriminalitet	Manglende sikkerhetstester, sikkerhetsoppdateringer, opplæring og bevisstgjøring av ansatte samt mangelfull overvåking av aktiviteter i egen tekniske infrastruktur, herunder nettverk og systemer, kan føre til at kriminelle påfører foretaket skade gjennom digitale angrep.	↗
Informasjonslekkasje	Manglende klassifisering av informasjon, herunder dokumentasjon, og kontroller for overvåking av informasjon som sendes ut på e-post, som kopieres til eksterne lagringsenheter eller kopieres til private skytjenester kan påføre foretaket eller dets kunder skade der uvedkommende får informasjonen i hende.	↗
IKT-drift	Kompleks integrasjon mellom systemer fra ulike leverandører, integrasjon mellom nye og gamle systemer, mange integrasjonspunkter mellom systemene, økt funksjonalitet i selvbetjente kanaler og økt bruk av skytjenester kan føre til utfordringer for sikker og stabil drift.	→
Kontinuitetsledelse og kriseledelse	Manglende analyser av konsekvenser ved en krise, mangelfull opplæring og øvelse i krisehåndtering, mangler i test av kriseløsninger/reserveløsninger og mangelfulle reserveløsninger, kan gi foretak utfordringer med å opprettholde kritiske IKT-tjenester ved alvorlige avbrudd på normalt driftssted.	→
Geopolitiske forhold	Geopolitiske forhold eller brudd i kommunikasjonen mot utlandet, hvor leverandører blir forhindret fra å opprettholde leveranser av kritiske IKT-tjenester fra utlandet, kan føre til utfordringer med å opprettholde sikker og stabil drift.	↗
Endringsstyring	Høy utviklingstakt, hvor kvalitet går på bekostning av tid, kan føre til funksjonelle feil i applikasjoner og systemer og at sikkerhetshull ikke avdekkes. Manglende kontroll av endringer i driftsoppsettet kan føre til brudd i kritiske forretningsprosesser og at foretaket eksponeres for digital kriminalitet.	→
Tilgangsstyring	Mangelfull kontroll med og overvåking av utvidede tilgangsrettigheter, for ansatte og personell hos leverandører, kan skade foretaket som følge av bevisste eller ubevisste operasjonelle feil. Det kan også føre til informasjonslekkasjer.	→
Datakvalitet	Mangler eller feil i data kan føre til at analyser og kontroller utføres på feil eller for svakt grunnlag. Dette kan blant annet omfatte feil i kredittvurderinger, feil i kontroller for å avdekke hvitvasking eller svindel, feil i risikovurderinger og feil i overvåking av driften.	→

Kilde: Finanstilsynet

Risikovurderingene i tabellen er basert på Finanstilsynets observasjoner og vurderinger omtalt i kapittel 3 til 6. Pilene angir Finanstilsynet vurdering av trenden (økende, uendret eller redusert risiko). Nærmere detaljer om grunnlaget for vurderingene fremgår av vedlegg 2.

Foretakenes vurdering av risiko

Dialog med foretak og foretakenes svar på den årlige undersøkelsen om digital sårbarhet, viser at den stadig økende kompleksiteten i systemporteføljen medfører risiko på en rekke områder, men risikoen vurderes likevel som minkende. Den økende kompleksiteten innebærer blant annet følgende utfordringer:

- Arbeidet med å utforme gode kriseløsninger kompliseres
- Logger fra ulike systemer kan være vanskelig å sammenholde og svekker muligheten for å utnytte informasjonen i loggene
- Utfordringer med å etablere et helhetlig forsvar mot elektroniske angrep
- Komplisert og tidkrevende feilsøking
- Komplisert, omfattende og krevende arbeid med risikoanalyser
- Manglende datakvalitet

Flere foretak ser digitale angrep som en alvorlig og aktuell risiko, og at manglende sikkerhetsbevissthet hos ansatte øker faren for at angrep lykkes. Videre utgjør leveransepresset en risiko, men foretakene antar denne risikoen vil dempes. Flere foretak påpeker også utfordringer med godt og samlet datagrunnlag og systemstøtte for analyser av mistenkelige transaksjoner.

Foretakene anser omfanget av regulatoriske krav, herunder nye krav med kort frist for gjennomføring, som en betydelig utfordring og risiko. Nye reguleringer kan innebære omfattende og krevende tilpasninger i systemene. Ofte er det behov for å fortolke og konkretisere nye reguleringer og krav, og foretakene mener avklaringer fra berørte myndigheter kommer for sent.

Risiko knyttet til kundenes tilgang til digitale tjenester

Digitaliseringen har medført at foretakenes kunder har måttet ta i bruk løsninger for identifikasjon og autorisering, der bl.a. BankID har blitt en form for "universalnøkkel" for tilgang til både privat og offentlig tjenesteyting. Det er effektivt, men den brede anvendelsen av BankID medfører risiko. BankID kan brukes på mange forskjellige tjenester og ofte uten at det er lagt inn ytterligere kontroller for å forhindre misbruk. Dette skaper en sårbarhet for både kundene og foretakene. Det bør vurderes risikoreduserende tiltak for ulike tjenester, tilpasset tjenestens egenart og potensialet for misbruk.

Utviklingen av digitale løsninger har også ført til at de fleste finansielle tjenestene er basert på selvbetjening. Dette stiller store krav til foretakenes IKT-drift og informasjonssikkerhet for å sikre tilgjengelighet, konfidensialitet og dataintegritet, slik at kundene skal føle trygghet knyttet til bruken. Det stiller også krav til god oppfølging av kunder som ved avvik i bruk av tjenestene er, eller oppfatter at de er, skadelidende. Digitaliseringen av finansielle tjenester har også gitt enkelte kundegrupper utfordringer. Det er viktig at foretakene etablerer gode løsninger også for disse kundene, enten ved å opprettholde manuelle løsninger, eller ved å tilby enkle digitale løsninger.

Tap knyttet til svindel

Svindelrapporteringen er etter innføringen av det reviderte betalingstjenestedirektivet (PSD 2) noe endret fra tidligere år, og rapporterte tall for andre halvår 2019 er dermed ikke direkte sammenlignbare med tidligere rapporteringer.

Samlet var tapene på kortsvindel ca. 190 millioner kroner i 2019. Det er en økning på 28 prosent fra 2018. Tapene var jevnt fordelt på første og andre halvår. Det er særlig misbruk av kortinformasjon ved internetthandel som har økt. Tallene for første halvår 2019 indikerer også en økning i antall betalingskort utsatt for misbruk. (Tilsvarende tall er ikke rapportert for andre halvår grunnet endringen som følger av PSD 2.)

Tapene på kortsvindel andre halvår viser at tapene tilsvarer 0,02 prosent av total transaksjonsverdi og at antall svindeltransaksjoner utgjorde 0,007 prosent av totalt antall transaksjoner.

Tap ved bruk av nettbank utgjorde 3,6 millioner kroner i første halvår 2019, som er lavt sammenlignet med tidligere år. For andre halvår er tap ved kontobetalinger, der svindleren utfører betalingen, på 46,5 millioner kroner. Tallene er ikke direkte sammenlignbare med tidligere rapporteringer.

Svindel gjennom sosial manipulering økte ytterligere i 2019 og er for kriminelle den mest lukrative metoden. Rapporterte tall indikerer tap på over 500 millioner kroner, mot i underkant av 300 millioner kroner i 2018.

Utkontraktering av IKT og melding om betalingstjenester

Finanstilsynet behandlet 135 meldinger om utkontraktering av IKT i 2019, som er lavere enn i 2018. Finanstilsynet ser at foretakene har blitt bedre til å håndtere utkontrakteringsavtaler, herunder risikoanalyser av utkontrakteringen, styrebehandling av utkontrakteringsforholdet og kvaliteten på avtalene med underleverandørene. Meldingene viser også i 2019 en klar tendens til økt bruk av skytjenester.

I 2019 mottok Finanstilsynet 21 meldinger om endrede eller nye betalingstjenester, særlig om samarbeid mellom banker om betalingsløsninger og nye løsninger for betaling med mobiltelefon. Finanstilsynet mottok også 30 søknader knyttet til reautorisering[1] og/eller konsesjon til å yte betalingstjenester. Av søknadene framgikk at flere foretak hadde manglende forståelse av regelverket og behov for vesentlig forbedring av sine rutiner.

[1] Godkjennelse under overgangsordningen ifm. det reviderte betalingstjenestedirektivet

Finanstilsynets oppfølging av foretakene

Hovedtema for tilsynsvirksomheten i 2020 er

- foretakenes styring og kontroll med IKT-virksomheten,
- organisering av IKT-/cyber-sikkerhetsarbeidet
- sikkerheten knyttet til foretakenes IKT-løsninger
- foretakenes beredskapsarbeid og testing av kontinuitets- og kriseløsninger
- foretakenes styring, kontroll og oppfølging av utkontraktert IKT-virksomhet
- foretakenes betalingstjenester, herunder etterlevelse av det reviderte betalingstjenestedirektivet
- Finanstilsynet vil også følge opp foretakenes IKT-løsninger for å avdekke hvitvasking og terrorfinansiering, og bankenes tilbud av kontanttjenester og kontantberedskap.

IKT-hendelser hos foretakene følges opp. Det vil bli lagt vekt på at foretakene avdekker årsaker og iverksetter tiltak for å forebygge gjentakelser. Trusselbildet knyttet til digital kriminalitet overvåkes, og foretakenes beredskapsarbeid rettet mot digital sårbarhet og digital sikkerhet gjennomgås.

Finanstilsynet legger vekt på at foretakene ivaretar sikkerheten i sine tjenester på en god måte, slik at kundene ikke blir skadelidende. Det vil også bli fulgt opp at foretakene ikke deler kundenes data uten samtykke og at data ikke kommer uvedkommende i hende.

Finanstilsynet leder og er sekretariat for Beredskapsutvalget for finansiell infrastruktur (BFI). Utvalget følger opp beredskap og hendelser i den finansielle infrastrukturen. I spesielle situasjoner, som koronakrisen, vil BFI særlig følge opp IKT-virksomheten hos de viktigste aktørene.

Kort oppsummering av vedleggene

I egne vedlegg fremkommer foretakenes svar på spørreundersøkelsen om sårbarhet, grunnlaget for Finanstilsynet vurdering av risiko og Finanstilsynets oppfølging av foretakene. Videre omtales interkontrollfunksjonene og styrende rammeverk som strategi, policy og retningslinjer, samt forhold knyttet til utkontraktering og kontroll med leverandører. I vedlegg beskrives også relevante forhold knyttet til informasjonssikkerhet og hva det er viktig at foretakene er oppmerksomme på, de europeiske tilsynsmyndighetenes internasjonale rammeverk knyttet til IKT-sikkerhet, rammeverk for informasjonssikkerhet og sikkerhetstesting, risiko og sårbarhet ved å ta i bruk nye teknologier og viktige forhold knyttet til cyberforsikring.

2. Finansiell infrastruktur

Den finansielle infrastrukturen består av betalingssystemet og verdipapiroppgjørssystemet, samt verdipapirregisteret (VPS), markedsplasser og sentrale motparter.

Betalingssystemet består av interbanksystemer og systemer for betalingstjenester for overføring av midler, med formelle og standardiserte ordninger og felles regler for behandling, avregning eller oppgjør av betalingstransaksjoner.

Betalingssystemet, herunder betalingstjenester, reguleres gjennom lover og forskrifter, samt gjennom finansnæringens selvregulering forvaltet av Finans Norge og Bits. Som følge av det reviderte betalingstjenestedirektivet (PSD 2), ble det fastsatt en rekke regelverksendringer med virkning fra 1. april 2019. De mest sentrale endringene er knyttet til lov om betalingssystemer, forskrift om systemer for betalingstjenester og forskrift om betalingstjenester.

Den nye infrastrukturen for realtidsbetalinger, også kjent som straksbetalinger, der beløpet er tilgjengelig på konto hos mottaker umiddelbart, ble i 2019 tatt i bruk av bankene i Norge.

Verdipapirområdet reguleres gjennom flere sentrale lover og forskrifter, blant annet verdipapirhandelloven, verdipapirforskriften og verdipapirsentralloven. Verdipapirområdet består blant annet av aktører som er involvert i verdipapirtransaksjoner knyttet til egenkapitalinstrumenter som aksjer og egenkapitalbevis, herunder gjennomføring av handler og oppgjør av disse.

2.1. Betydningen av den finansielle infrastrukturen

Effektive, robuste og stabile betalingssystemer er grunnleggende for finansiell stabilitet og velfungerende markeder. Den finansielle infrastrukturen skal sørge for at pengebetalinger og transaksjoner i finansielle instrumenter blir registrert, avregnet og gjort opp.

Direktoratet for samfunnssikkerhet og beredskap[2] har utpekt finansielle tjenester som samfunnskritisk funksjon. Justis- og beredskapsdepartementet har i den nye sikkerhetsloven definert finansiell stabilitet og handlefrihet som en av flere nasjonale sikkerhetsinteresser[3].

Svikt hos sentrale aktører i finansnæringen eller i infrastrukturen kan få betydelige samfunnsmessige konsekvenser. Dersom det ikke er mulig å gjennomføre eller gjøre opp betalinger eller handel med verdipapirer, 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 gjør data utilgjengelige, påføres kunder og foretak

[2] DSB: Samfunnets kritiske funksjoner
[3] Sikkerhetsloven §1-5 Definisjoner

betydelige utfordringer. Slike hendelser vil også kunne påvirke den finansielle stabiliteten. De samfunnsmessige konsekvensene vil særlig kunne bli store om foretak som opererer på vegne av mange eller alle foretak rammes. Finanssektoren er også avhengig av felles infrastruktur som el-forsyning og telekommunikasjon, herunder nettverk.

Finanstilsynet og Norges Bank samarbeider om tilsyn og overvåking av den finansielle infrastrukturen i Norge, blant annet gjennom utredninger, risikovurderinger og felles tilsyn.

2.2. Den finansielle infrastrukturen er robust

Finanstilsynet vurderer den norske finansielle infrastrukturen som robust. Det var i 2019 ingen større IKT-hendelser som hadde konsekvenser for finansiell stabilitet. Tjenestenes driftsstabilitet var tilfredsstillende. I 2019 var det færre av de rapporterte IKT-hendelsene som påvirket tilgjengeligheten til betalingstjenestene og de øvrige kunderettede tjenestene enn i 2018. Selv om det også i 2019 var en rekke hendelser som medførte negative konsekvenser for berørte kunder, vurderes tilgjengeligheten til tjenestene samlet sett som tilfredsstillende, og bedre i 2019 enn i 2018.

Det var i 2019 i hovedsak god regularitet på avregnings- og oppgjørssystemene og ingen kritiske hendelser. Det var også god regularitet på kommunikasjonen mot det internasjonale betalingssystemet Swift og det internasjonale oppgjørssystemet CLS.

Omfanget av digital kriminalitet øker år for år, men har så langt ikke ført til større hendelser hos foretak i finanssektoren. Selv om sårbarheter har blitt avdekket og alvorlig operasjonell svikt med store konsekvenser har forekommet, har systemkriser foreløpig ikke forekommet.

En digital hendelse kan komme brått, medføre sammenbrudd og forårsake vidtrekkende samfunnsmessige konsekvenser. For å sikre robustheten i den finansielle infrastrukturen er foretakenes arbeid innen IKT-området, både for å redusere sannsynligheten for avvik og for generelt å forbedre IKT-sikkerheten, viktig for å sikre stabile og robuste driftsløsninger. Dette omfatter kontinuitetsløsninger, kriseløsninger og -beredskap, gjenopprettingsplaner og IKT-sikkerhetsarbeid.

2.3. Beredskapsutvalget for finansiell infrastruktur (BFI)

Beredskapsutvalget for finansiell infrastruktur (BFI)[4] er etablert for å

- komme frem til og koordinere tiltak for å forebygge og å løse krisesituasjoner og andre situasjoner som kan resultere i store forstyrrelser i den finansielle infrastrukturen. I en krisesituasjon skal utvalget varsle og informere berørte aktører og myndigheter om hvilke problemer som har oppstått, hvilke konsekvenser problemene kan medføre og hvilke tiltak som settes i verk for å løse problemene.

[4] Beredskapsutvalget for finansiell infrastruktur (BFI)

- forestå nødvendig koordinering av beredskapssaker innenfor finansiell sektor, herunder, på grunnlag av sivilt beredskapssystem, samordne utarbeidelse og iverksettelse av varslingsplaner og beredskapstiltak ved sikkerhetspolitiske kriser og krig.

Finanstilsynet får gjennom tilsynsvirksomheten og arbeidet i BFI, der blant annet alvorlige og kritiske hendelser som treffer de ulike delene av den finansielle infrastrukturen gjennomgås, et bredt og godt bilde av tilstanden.

2.4. Koronapandemien

Finanstilsynet har hatt stor oppmerksomhet på utviklingen i den finansielle infrastrukturen siden koronapandemien eskalerte i Norge. BFI har hatt hyppige møter for å følge opp hvordan de sentrale foretakene i den norske finansielle infrastrukturen ivaretar god, sikker og stabil drift, jf. utvalgets mandat. Møtene har bidratt til informasjonsutveksling om forhold som kan resultere i forstyrrelser i den finansielle infrastrukturen eller ha betydning for finansiell stabilitet, samt tiltak som foretakene har eller planlegger å iverksette. Aktørene har så langt hatt god kontroll på driftssituasjonen og har iverksatt nødvendige tiltak. Finanstilsynet finner dette betryggende.

Erfaringene så langt viser at de sentrale foretakene i den norske finansielle infrastrukturen har gode beredskapsplaner som raskt kan iverksettes. Foretakene satte krisestab i takt med utviklingen av koronapandemien og myndighetstiltak for å begrense smitten.

Finanstilsynet og BFI har hatt særlig oppmerksomhet på virksomheter som støtter kritiske funksjoner, herunder de samfunnsfunksjonene i finanssektoren som er definert som kritiske av Direktoratet for samfunnssikkerhet og beredskap. Disse er evne til å

i) opprettholde sikker formidling i finansmarkedet av kapital mellom aktører nasjonalt og til og fra utlandet
ii) gjennomføre betalinger og andre finansielle transaksjoner på en sikker måte
iii) opprettholde befolkningens tilgang til nødvendige betalingsmidler[2].

Som ledd i smittevernet for egne ansatte, gjennomgikk flere foretak kritiske roller, funksjoner og bemanning, og iverksatte tiltak som splitt av organisasjonen og klargjøring eller bruk av reservelokasjoner. Foretakene utvidet kapasiteten for systemoppkobling hjemmefra. Det ble åpnet for bruk av enkelte funksjoner fra hjemmekontor som normalt bare nås fra kontorlokasjonen, og strenge sikkerhetstiltak og utvidet overvåkning ble iverksatt for å heve sikkerheten for hjemmekontor. Det ble iverksatt strenge regimer med begrensning eller stans av endringer i IKT-systemene. Oppfølgingen av kritisk drift og kritiske leverandører til denne var tett. Bankenes og deres tjenesteleverandørers håndtering av tilbudet av kontanttjenester ble fulgt opp. I tråd med kriseplaner, hentet enkelte foretak hjem driftsoperasjoner fra utlandet og beholdt en begrenset del av virksomheten i utlandet som en beredskapsordning. Flere foretak gjennomgikk planene for den fysiske sikringen av lokalene, herunder lokasjoner for IKT-drift.

2.5. Samarbeid innen sikkerhetsområdet

Samfunnskritiske virksomheter i finanssektoren

Drift og sikkerhet i finansforetakenes IKT-systemer er i forbindelse med den pågående korona-pandemien utpekt til å være samfunnskritisk virksomhet[5]. Dette er tiltak som er iverksatt på nasjonalt nivå for å sikre at de finansielle foretakene i Norge leverer fungerende betalings- og handelssystemer.

I den nye sikkerhetsloven[6] som trådte i kraft 1. januar 2019, er finansiell stabilitet og handlefrihet definert som en av flere nasjonale sikkerhetsinteresser[3] som skal følges opp av ansvarlig sektordepartement. Departementene skal identifisere og holde oversikt over virksomheter som har avgjørende eller vesentlig betydning for grunnleggende nasjonale funksjoner (GNF) og melde disse inn til Nasjonal sikkerhetsmyndighet. For foretak av *avgjørende betydning* for GNF, skal ansvarlig departement fatte vedtak om at loven helt eller delvis skal omfatte foretaket. Departementene skal også ajourholde oversikt over foretak av *vesentlig betydning* for GNF.

Finanstilsynet utarbeidet i 2019 analyser og råd til Finansdepartementet om identifisering av grunnleggende nasjonale funksjoner, samt vurderinger av virksomheter som kan ha vesentlig betydning for de grunnleggende nasjonale funksjonene. Dette arbeidet fortsetter i 2020.

Foretak som understøtter grunnleggende nasjonale funksjoner, kan være mer utsatt for trusler fra utenlandsk etterretning. Det stilles derfor strengere krav til foretakets sikkerhetsarbeid, herunder også underleverandører og samarbeidspartnere. Trusler fra utenlandske statlige aktører er beskrevet under punkt 3.4.2.

Samhandling og informasjonsutveksling gir bedre risikoforståelse

Samarbeid og erfaringsutveksling om informasjonssikkerhet mellom finansforetakene i Norge vil bidra til å heve kunnskapen om det aktuelle trussel- og risikobildet, og gjøre foretakene bedre rustet til å håndtere digitale trusler og uønskede hendelser.

Finanstilsynet ble i 2019 utpekt av Finansdepartementet som sektorvis responsmiljø (SRM)[7] med oppgave å håndtere IKT-sikkerhetshendelser i finanssektoren innenfor Finanstilsynets ansvarsområde. Finanstilsynet utøver rollen sammen med Nordic Financial CERT (NFCERT)[8].

Finanstilsynet deltar som partner i Nasjonalt cybersikkerhetssenter, som ble etablert av Nasjonal sikkerhetsmyndighet (NSM) i 2019 for å styrke Norges motstandsdyktighet og beredskap på det digitale feltet. Deltakelsen gir Finanstilsynet tilgang til oppdatert kunnskap om risikobildet på cyber-sikkerhetsområdet. Finanstilsynet har tilgang til senteret, og kan samhandle og utveksle informasjon med andre partnere og aktører ved håndtering av cybertrusler og -angrep.

[5] Koronaviruset: Samfunnskritiske virksomheter i finanssektoren
[6] Lov om nasjonal sikkerhet (sikkerhetsloven)
[7] Rammeverk for håndtering av IKT-hendelser NSM
[8] Nordic Financial CERT

3. Finanstilsynets observasjoner og vurderinger

I tillegg til funn, observasjoner og vurderinger fra tilsynsvirksomheten omtales også foretakenes egne vurderinger av de mest fremtredende sårbarheter og trusler, innhentet gjennom spørreskjema og intervjuer. Disse er nærmere omtalt i vedlegg 1.

Videre omtales IKT-sikkerhet, digitale trusler og utvikling i trusselbildet, samt hvordan foretakene bør ruste seg mot digitale trusler. Dette omfatter også trussel- og risikovurderinger fra nasjonale sikkerhetstjenester og -myndigheter med særlig betydning for finansnæringen. Andre områder som omtales, er blant annet tilgangsstyring, endringsstyring, kontinuitetsledelse og kriseledelse, kompetansestyring, samt planlegging og organisering av IKT-virksomheten. Teknologiske utviklingstrekk som antas å kunne få betydning for risikoen knyttet til foretakenes bruk av IKT, er også omtalt.

3.1. Styringsmodell og internkontroll

3.1.1. Styre og ledelse

Foretakene har ansvar for at IKT-virksomheten oppfyller alle krav i forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT). Dette gjelder også der hele eller deler av IKT-virksomheten er utkontraktert.

Finanstilsynet forventer at foretakenes styre og ledelse er kjent med forskriftens innhold, og at policyer, retningslinjer og leverandøravtaler understøtter forskriftens krav. Det er styrets og ledelsens ansvar at internkontrollen er etablert med en struktur og et format, i tråd med foretakets størrelse og virksomhet, som sikrer at operative enheter utfører nødvendige kontroller. Compliancefunksjonen skal overvåke og kontrollere at kravene etterleves, og rapportere status til styre og ledelse. Styret, og eventuelle revisjonskomitéer, må i tillegg vurdere om foretakets internrevisjon i tilstrekkelig grad gjennomfører revisjoner som samsvarer med foretakets operasjonelle risikotoleranse på IKT-området.

Det forventes at styret har nødvendig kompetanse og innsikt for å bidra til at IT-investeringer understøtter foretakets strategi og behov. En forankring og forståelse av risikobildet hos styret og ledelsen er en viktig forutsetning for å sikre en stabil og sikker IKT-drift.

Etter Finanstilsynets vurdering har IKT-modenheten i foretakenes styre og ledelse økt de senere år. Økt digitalisering og endringsbehovet som følger av dette (digital transformasjon), har etter Finanstilsynets syn forsterket styret og ledelsens oppmerksomhet, spesielt rettet mot digitalisering av forretningsprosesser og mot informasjonssikkerhet.

Foretakenes styre og ledelse må kontinuerlig vurdere om kompetansen og teknologiforståelsen som er nødvendig for å styre og kontrollere foretakets IKT-virksomhet et til stede.

3.1.2. Internkontrollfunksjoner

Samhandling mellom operative enheter og de uavhengige funksjonene i foretakenes første- og andrelinje, herunder risikostyring, compliance og internrevisjon, er viktige for å sikre en effektiv og god internkontroll i foretakene. Foretak som ikke sikrer en uavhengig overvåking og kontroll, løper en risiko for underrapportering og feil i rapporteringen. Dette medfører igjen en risiko for at vesentlige avvik i etterlevelsen av lover og krav ikke avdekkes, og at vesentlige risikoer ikke identifiseres.

Samtidig er det viktig å understreke at det er den operative ledelsen i foretakets førstelinje som må sørge for at føringer og instrukser gitt av styret og ledelsen, følges og etterleves. Foretakets strategi, policyer og retningslinjer (styrende rammeverk), og underliggende instrukser samt leverandøravtaler står helt sentralt i foretakets internkontroll.

Internkontrollfunksjonene er nærmere beskrevet i vedlegg 4.

3.1.2.1. Operativ ledelse

Foretakene legger som regel mest ressurser på kontrollfunksjonene i de operative enhetene, i samsvar med god praksis. Finanstilsynet har inntrykk av at det er god kompetanse og forståelse av kontrollfunksjonen i førstelinjen. Finanstilsynet erfarer imidlertid at mindre foretak har begrenset med ressurser og kompetanse innen IKT-området. Slike foretak er ofte avhengig av gode samhandlingsmodeller innen en allianse.

Det understrekes at hvert foretak likevel er ansvarlig for å innhente informasjon om etterlevelsen av kravene som fremgår av styrende rammeverk, jf. punkt 3.1.4.

3.1.2.2. Risikostyring

Risiko innen IKT-området er del av foretakets operasjonelle risiko, og omfatter risiko for informasjonslekkasje (brudd på konfidensialitet), uautoriserte endringer (brudd på integritet) eller sabotasje mot foretakets tekniske infrastruktur (utilgjengelighet). Risikobildet inkluderer alle interne og eksterne sårbarheter og trusler mot et foretaks systemer, teknologiske infrastruktur og ansatte. Også risikoer knyttet til strategiske valg, foretakets organisering, kompetanse og sikkerhet er omfattet.

Risikobildet innen IKT-området er omfattende, komplisert og stadig i endring. Det medfører at foretakenes strategier, policyer og retningslinjer må fastsettes og revideres, og nye kontroller må etableres. Risikostyring er derfor helt grunnleggende for foretakets forvaltning av styringsmodellen for IKT-området, og utøvelsen av internkontrollen. Risikobildet innen IKT-området skal prioriteres av foretakets styre og ledelse på lik linje med annen operasjonell risiko.

Det er Finanstilsynets inntrykk at foretakene gjennomgående har en akseptabel modenhet i utførelsen av risikostyringen. Gjennom tilsyn er det likevel avdekket at risikostyringen ikke alltid omfatter hele risikobildet på IKT-området. En av årsakene til dette kan være at risikostyringsfunksjonen i foretakets andrelinje ikke har tilstrekkelig med ressurser, kompetanse eller forståelse for kompleksiteten i risikobildet. Finanstilsynet erfarer at foretak mangler rutiner som instruerer de operative enhetene i IT-

avdelingen og forretningsområdene, sammen med risikostyringsfunksjonen, til å arbeide metodisk og koordinert med risiko på IKT-området.

Finanstilsynet har også observert mangelfulle eller fraværende risikovurderinger av sentrale IKT-leverandører, blant annet risikovurderinger knyttet til leverandørenes finansielle stabilitet, organisering, kompetanse, samhandling og andre relevante forhold knyttet til de utkontrakterte tjenestene. Finanstilsynet mener relevante deler av IKT-leverandørenes egne risikovurderinger bør inngå som grunnlag for foretakets egne vurderinger.

Finanstilsynet understreker styrets og ledelsens ansvar for at risikovurderingene har en helhetlig tilnærming. Foretak som ikke har en helhetlig tilnærming til risikobildet innen IKT-området vil naturlig nok kunne være eksponert for alvorlige risikoer uten at dette er kjent for styret og ledelsen, og det vil være knyttet stor usikkerhet til om den faktiske risikoeksponeringen er innenfor foretakets risikotoleranse.

3.1.2.3. Compliancefunksjonen

Mangelfull overvåking, herunder overvåking av de operative enhetenes kontroll med etterlevelse av kravene slik disse er formulert i policyer, retningslinjer og leverandøravtaler, utgjør en risiko ved at foretakets styre og ledelse ikke mottar en uavhengig vurdering som i tilstrekkelig grad bekrefter eller avkrefter om foretakets operasjoner utføres i henhold til fastsatte krav.

Gjennom tilsyn har Finanstilsynet observert compliancefunksjoner som i begrenset grad overvåker og kontrollerer operative enheters etterlevelse av nevnte krav. Etter Finanstilsynets vurdering skyldes dette hovedsakelig at compliancefunksjonen mangler ressurser, samt innsikt og forståelse av kontrollregimet innen IKT-området. Videre involveres ikke compliancefunksjonen i tilstrekkelig grad i arbeidet med å etablere kontrollene som skal utføres av de operative enhetene, og som er en forutsetning for compliancefunksjonen mulighet for oppfølging.

Selv om kontrollene som utføres av de operative enhetene vurderes som gode fra styrets og ledelsens side, vil mangelfull overvåking og kontroll fra compliancefunksjonen medføre en betydelig svekkelse av foretakets internkontroll, for eksempel der operative enheter rapporterer feil eller unnlater å gjennomføre kritiske kontroller. Uavhengig kontroll er etter Finanstilsynets syn strengt nødvendig og en forutsetning for en tilfredsstillende internkontroll.

3.1.2.4. Internrevisjonen

Foretakets internrevisjon er styrets selvstendige og uavhengige overvåkingsfunksjon. Internrevisjonen skal blant annet vurdere om beskrivelsen av kontrollene som skal utføres på IKT-området er i tråd med foretakets risikotoleranse og de krav som er fastsatt i styrende rammeverk, jf. punkt 3.1.4. Videre skal internrevisjonen vurdere kvaliteten på de operative enheters utførelse av kontrollene, og om disse faktisk er blitt utført. Internrevisjonen skal også vurdere om internkontrollrapporteringen til styret og ledelsen stemmer med de faktiske forhold. Finanstilsynet understreker også internrevisjonens ansvar for å øke bevisstheten og kunnskapen hos medlemmer av revisjonskomiteen, styrets medlemmer og hos ledelsen om trusler og sårbarheter innen IKT-området og sikkerhetsområdet.

IKT-forskriften § 12 stiller krav om at foretak skal sikre at avtalen med IKT-leverandøren gir rett til å kontrollere, herunder revidere, leverandørens avtalefestede aktiviteter. Finanstilsynet ser at internrevisjonen ofte begrenser revisjonen til å omfatte sårbarhets- og sikkerhetstester. Dette er viktig, men dekker kun en liten del av den operasjonelle risikoen. Banker i enkelte bankallianser har valgt å samarbeide om revisjonsgjennomganger av leverandører, som er en hensiktsmessig modell der foretak benytter de samme utkontrakterte tjenestene.

Finanstilsynet har ved enkelte tilsyn konstatert at revisjonsgjennomgang av foretakets andrelinje ikke utføres, herunder med manglende vurdering av hvordan funksjoner som risikostyring og compliance ivaretar sin rolle og sitt ansvar. Etter Finanstilsynets vurdering er det viktig med uavhengige vurderinger av alle kontrollfunksjoner i foretaket innen IKT-området.

Finanstilsynet har gjennom tilsyn erfart at foretaks internrevisjon i for liten grad favner helheten i sitt revisjonsarbeid, noe som svekker styrets mulighet til å innhente en uavhengig vurdering av kontrollstatus. Internrevisjonen bør etter Finanstilsynets vurdering revidere alle områder som anses å ha høy operasjonell risiko, både internt i foretaket og for de utkontrakterte IKT-tjenestene. Foretakets styre, og en eventuell revisjonskomité, bør sammen med internrevisjonens ledelse etablere en revisjonssyklus som viser hvilke operasjonelle risikoer som skal dekkes av internrevisjonen innen IKT-området.

Leverandørenes uavhengige revisjonserklæringer, som ISEA 3402, kan inngå som grunnlag for vurdering av kontrollsituasjonen hos leverandørene. Finanstilsynets nærmere vurdering fremgår av vedlegg 6.

3.1.3. Regulatoriske krav

Regulatoriske krav innen blant annet personvern (GDPR), antihvitvasking og terrorfinansiering (AML) og innen betalingstjenester (PSD 2), gjør det nødvendig at foretakene og deres leverandører gjennomfører nødvendige endringer og tilpasninger i IKT-systemene.

Foretakene anser nye reguleringer å utgjøre en betydelig utfordring og risiko. Reguleringene kan innebære større endringer i systemene, ofte med kort tid til tilpasning. Det kan også være behov for å fortolke og konkretisere reguleringene, og det gis inntrykk av at konkretiseringene mv. fra berørte myndigheter kommer for sent.

Finanstilsynets mener etterlevelse av IKT-forskriften bør få økt oppmerksomhet av foretakenes styre og ledelse. Brudd på IKT-forskriften kan medføre alvorlige konsekvenser for sikker og stabil drift. Alvorlige hendelser kan medføre tap av omdømme og hendelser kan i ytterste konsekvens true et foretaks eksistens.

3.1.4. Policyer og retningslinjer (Styrende rammeverk)

Finanstilsynet observerer gjennom tilsyn at det er ulik kvalitet på foretakenes rammeverk innen IKT-området. Skillet mellom policy (førende) og retningslinjer og instrukser (instruerende) er ikke alltid

tydelig nok. Foretaket mangler rutiner for å sikre at policyer operasjonaliseres som retningslinjer og rutiner, det er mangler i instruerende dokumenter og dokumentasjonen er ikke ajourført.

Gjennom tilsyn konstaterer Finanstilsynet at foretak mangler oversikt over kontroller og beskrivelse av kontroller som skal utføres av operative enheter internt i foretaket, og kontroller som skal utføres av leverandørene. Dette fører blant annet til at foretakets compliancefunksjon, jf. punkt 3.1.2.3, ikke har tilstrekkelig grunnlag for å overvåke, kontrollere og vurdere foretakets etterlevelse.

En velfungerende internkontroll forutsetter at styre og ledelse innhenter nødvendige bekreftelser på at kontroller er utført i tråd med de krav som er satt, både fra operative enheter, inkludert leverandørene, og fra compliancefunksjonen og foretakets internrevisjon. Om kontrollene ikke gjennomføres, er det fare for at alvorlige sårbarheter ikke avdekkes, og at foretak dermed heller ikke iverksetter nødvendige risikoreduserende tiltak.

Finanstilsynet understreker ansvaret styret og ledelsen har for at 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. Brudd på foretakets risikotoleranse kan være en av konsekvensene som følger av mangelfull styring og kontroll.

Utfyllende informasjon fremgår av vedlegg 5.

3.1.5. Endringsledelse og digital transformasjon

Den digitale transformasjonen som pågår, stiller store krav til foretakenes endringsledelse. Finanstilsynet konstaterer imidlertid gjennom samtaler med foretak at de mangler rutiner og prosesser som i tilstrekkelig grad ivaretar den digitale transformasjonen av forretningsprosessene, herunder at endringer i organisasjonen gjennomføres i takt med digitaliseringen.

Endringer i tankesett, kultur, organisering og kompetanse er utfordrende for foretakene. Omstillinger kan skape usikkerhet, utrygghet og motvilje som kan forsterkes om prosessene for omstilling ikke er tydelige og forankret i hele organisasjonen. Organisasjonsutvikling ved at organisasjonen må endres i takt med den teknologiske utviklingen kan også være svært krevende. Endringer i kompetansebehov utfordrer også den enkelte, samtidig som foretaket må balansere mellom utvikling ved bruk av ny teknologi, og utvikling, forvalting og drift av eksisterende infrastruktur og teknologi.

Finanstilsynet mener det er en ikke ubetydelig risiko dersom foretak i sin styringsmodell mangler en tydelig strategi for hvordan organisasjonen skal endres og tilpasses i takt med den teknologiske utviklingen.

3.2. Kompetanse og kompetansestyring

Hvordan et foretak forvalter ansattes IKT-kompetanse vil i stor grad påvirke foretakets evne til å opprettholde blant annet stabilitet, sikkerhet, målrettet innovasjon, endringsledelse gjennom digital transformasjon, og leverandørstyring. Det vil også ha betydning for å identifisere fremtidige behov,

ressursstyring, motivasjon og rekruttering, og ikke minst beholde kritisk kompetanse i en omstillingsfase, og sikre omskolering av ansatte.

3.2.1. Kompetansestyring

Kompetansestyring innen IKT-området bør inngå i foretakets styringsmodell og som del av foretakets endringsledelse, jf. punkt 3.1.5. Gjennom kompetansestyring vil foretaket være bedre i stand til løpende å vurdere tilgjengelig kompetanse opp mot foretakets behov for å nå sine mål, og hvilken kompetanse som ikke lenger er nødvendig. Bruk av ny teknologi, som fører til økt digitalisering og digital transformasjon, påvirker i stor grad kompetansekrav og -behov.

Økt grad av utkontraktering stiller krav til foretakenes bestillerkompetanse, som er viktig både for å sikre at foretakets egne krav gjenspeiles i avtaler med leverandører og at leverandørstyringen utøves i tråd med foretakets egne krav til styring og kontroll.

Gjennom tilsyn konstaterer Finanstilsynet at kompetansestyring innen IKT-området er mangelfull. Det er risiko forbundet med at styre og ledelse ikke har tilstrekkelig oversikt over ansattes kompetanse, og heller ikke har oversikt over nåværende og fremtidig behov. Finanstilsynet mener foretak som mangler oversikt, løper en risiko for å møte store utfordringer i den digitale transformasjonen, og utfordringer i leverandørstyringen, både når det gjelder anskaffelser av nye IKT-tjenester og kontroll av leverandører.

3.2.2. Kompetansesituasjonen i Norge

Mange foretak har gjennom årene flyttet IKT-oppgaver ut av egen virksomhet, både til norske og utenlandske IKT-leverandører. Leverandørene på sin side har utkontraktert hele eller deler av sine oppgaver til aktører utenfor Norge, blant annet som en følge av knapphet på ressurser med kompetanse i Norge.

Som Finanstilsynet drøftet i fjorårets ROS, utgjør sårbarheter knyttet til mangel på tilgang til IKT-kompetanse i Norge en risiko for ytterligere avhengighet av utenlandske aktører. Dette gjelder spesielt innen operativ drift og informasjonssikkerhet. Finanstilsynet mener fortsatt at IKT-kompetanse som ikke lenger forvaltes og utvikles i Norge, kan utgjøre en vesentlig risiko, blant annet som følge av usikre geopolitiske forhold, se nærmere omtale i punkt 3.6.2.

Foretakenes svar på spørreundersøkelsen om sårbarhet viser at foretakene selv vurderer kompetansesituasjonen innenfor blant annet operativ IKT-drift som utfordrende.

Finanstilsynet mener foretakene grundig må vurdere omfanget av IKT-kompetanse som til enhver tid må være tilgjengelig for å opprettholde sikker og stabil drift av foretakenes infrastruktur, systemer og applikasjoner under en krise. Herunder må det vurderes i hvilken grad foretak som opererer i Norge, skal kunne håndtere driften i situasjoner der utenlandske aktører er forhindret fra å utføre kritiske IKT-tjenester.

Finanstilsynet opprettholder anbefalingen fra i fjor om at foretakene og deres leverandører bør vurdere hvilke konsekvenser mangel på kompetanse i Norge kan medføre, både på kort og lang sikt.

3.2.3. Helhetlig forståelse av arkitektur og de digitale forretningsprosessene

Foretak uttrykker bekymring for at de ikke har en tilstrekkelig helhetlig forståelse for og oversikt over arkitektur og de digitale forretningsprosessene. Dette blant annet som følge av manglende tilgang til IT-arkitekter, økende kompleksitet i løsningene og stadig flere IKT-leverandører involvert i verdikjeden. Foretakene gir også uttrykk for bekymring om den høye graden av personell med spesialkompetanse hos IKT-leverandører går på bekostning av leverandørens helhetlige forståelse for IKT-tjenestene som er utkontraktert.

Manglende oversikt over den komplekse infrastrukturen i et foretaks teknologiske økosystem, herunder arkitektur og systemporteføljе, er etter Finanstilsynets vurdering alvorlig. Dette kan føre til feil i konfigureringer i sikkerhetsoppsettet, mangelfull kapasitetsstyring og feil oppsett på kriseløsninger. Videre kan dette medføre krevende feilretting ved alvorlige hendelser, som det var eksempler på i 2019, og det kan føre til at foretak prioriterer feil i sine IKT-investeringer og valg av sikkerhetsløsninger.

3.2.4. Tiltak fra foretak og fra myndighetene

Enkelte foretak har etablert ordninger for omskolering av IT-personell, og annet personell, for å legge til rette for omstilling fra gammel til ny teknologi. Kunnskapsdepartementet har igangsatt arbeid med ny digitaliseringsstrategi for universitets- og høyskolesektoren[9]. Strategien skal lanseres 1. januar 2021. I NOU 2019: 2 [10] peker Kompetansebehovsutvalget på relevante forhold vedrørende det fremtidige kompetansebehovet innen IKT-området. Finanstilsynet anser dette som viktige tiltak for å møte kompetanseutfordringene i årene fremover.

Som følge av koronapandemien, oppretter regjeringen 4.000 nye studieplasser høsten 2020, hvorav en andel vil være studieplasser for teknologistudier.

3.3. Leverandørstyring

I IKT-forskriftens § 12 fremgår det at foretaket er ansvarlig for å oppfylle alle krav i IKT-forskriften også når hele eller deler av IKT-virksomheten er utkontraktert til tredjepart.

Økt antall leverandører med tjenester som inngår i foretakenes verdikjeder fører til mer kompliserte modeller for både samhandling med den enkelte leverandør, felles samhandlingsmodeller med flere leverandører, og samhandlingsmodeller mellom leverandører. Samhandlingene styres og koordineres gjennom foretakets leverandørstyring og stiller store krav til foretakets strategiske, administrative og operative funksjoner. Om strategisk viktige leverandører velger å benytte underleverandører på deler

[9] Ny digitaliseringsstrategi for universitets- og høyskolesektoren - invitasjon til åpen innspillsrunde
[10] NOU 2019: 2 Fremtidige kompetansebehov II — Utfordringer for kompetansepolitikken

av sine leveranser, kompliseres leverandørstyringen ytterligere. Finanstilsynet mener kompleksiteten gir økt risiko, som særlig kan materialiseres dersom alvorlige hendelser inntreffer.

Foretak under tilsyn er ansvarlig for å sikre nødvendig styring og kontroll med sine leverandører. God leverandørstyring forutsetter kompetanse om gjeldende lover og regler, samt etablering og oppfølging av avtaler som ivaretar foretakets forpliktelser. Finanstilsynet forventer derfor at foretak under tilsyn har nødvendig og tilstrekkelig bestiller-kompetanse, herunder kompetanse til å stille krav til utforming av avtalene som inngås med leverandør av IKT-løsninger eller -tjenester og kompetanse til å kontrollere om avtalene etterleves.

Finanstilsynet erfarer at foretakene i sine avtaler med leverandørene i hovedsak har dokumentert gode styrings- og samhandlingsmodeller. Foretakenes policyer innen IKT-området og informasjonssikkerhet er som regel gjort gjeldende i avtalene. Som nevnt i punkt 3.1, kan foretak ha foretak utfordringer med å innhente bekreftelser på leverandørenes etterlevelse av avtalekrav.

Foretakenes svar på spørreundersøkelsen om sårbarhet viser også at svakheter i samhandlingsmodellen med leverandørene forekommer, og at bestillerkompetanse, som kreves for å følge opp leverandørene i tråd med IKT-forskriftens bestemmelser, er utfordrende. Finanstilsynet konstaterer gjennom tilsyn at allianser med flere foretak har utfordringer med å etablere samhandlingsmodeller som sikrer at det enkelte foretak, på selvstendig grunnlag, kan rapportere kontrollsituasjonen på utkontrakterte tjenester til eget styre og ledelse.

Finanstilsynet erfarer gjennom tilsyn at det er foretak som i for liten grad har etablert et koordinerende kontrollregime mellom foretaket og strategisk viktige IKT-leverandører. Finanstilsynet mener foretakene i større grad bør innhente leverandørbekreftelser på at kontroller på områder med høyest operasjonell risiko, utføres i tråd med avtalens krav. Foretakets compliancefunksjon kan på sin side overvåke at bekreftelser mottas, jf. punkt 3.1.2.3. Der foretak har egen internrevisjon, kan en forsterket kontroll, og vurdering av kvaliteten på kontrollen, utføres av internrevisor, jf. punkt 3.1.2.4. Ved en slik tilnærming vil foretaket i større grad være i stand til å avdekke alvorlige avvik i en leverandørs internkontroll. Dette vil også styrke foretakets internkontrollrapportering.

Finanstilsynet mener foretakene, i samarbeid med leverandørene, bør vurdere å etablere integrerte kontrollsystemer, der foretakene kan hente ut informasjon og dokumentasjon knyttet til leverandørenes internkontroll for tjenestene som leveres, slik de største skytjenesteleverandørene tilbyr.

3.4. Informasjonssikkerhet og digital kriminalitet

Finansforetakene observerer at angrep, dvs. digital kriminalitet, mot deres systemer fortsatt øker betydelig fra år til år. Samtidig blir foretakenes systemer for overvåking og systemer for å avverge angrep stadig bedre, og angrepene stanses som oftest før de får konsekvenser for foretaket.

Finanstilsynet erfarer at foretakene i økende grad er oppmerksomme på at angrepsform og -metodikk er i kontinuerlig endring. Finanstilsynet understreker at styret og ledelsen i alle foretak bør rette særlig

oppmerksomhet mot endringer i trusselbildet, og foretakene må fortsette sitt arbeid med å kartlegge risiko og sårbarheter, iverksette preventive tiltak og ha beredskap for å håndtere angrep og følgeskader.

Enkelte områder innen informasjonssikkerhet og digital kriminalitet er nærmere omtalt i vedlegg 7.

3.4.1. Trend innen digitale angrep

Nasjonal sikkerhetsmyndighet (NSM) og Kripos har registrert en sterk økning i målrettede digitale angrep mot foretak med bruk av løsepengevirus og utga i 2019 en egen temarapport[11]. Finansforetak i Norge utsettes stadig for denne typen angrep, jf. punkt 5.2, men klarer i all hovedsak å avverge disse. Finanstilsynet forventer at foretakene etablerer nødvendige tiltak for å kunne håndtere denne typen trusler, samt gjennomfører nødvendige øvelser.

3.4.2. Nasjonale vurderinger av trusler og sårbarheter

Både etterretningstjenesten (E-tjenesten), Politiets Sikkerhetstjeneste (PST) og Nasjonal Sikkerhetsmyndighet (NSM) utgir årlig rapporter med informasjon om trusler, sårbarheter og risiko overfor Norge og norske interesser.

E-tjenesten har i sin rapport Fokus 2020[12] beskrevet at kinesisk og russisk etterretning utgjør den største trusselen mot norske interesser. Blant annet fremheves trusler knyttet til Kinas verdensomspennende utbygging av digital infrastruktur, og at denne kan legge grunnlaget for en storstilt, global etterretningskapasitet.

PST har i Nasjonal trusselvurdering 2020[13] definert digital kartlegging og sabotasje av kritisk infrastruktur som én av de tre mest aktuelle truslene mot Norge og norske interesser. Dette er en trussel mot store foretak og deres leverandører, men også en trussel mot mindre foretak og nisjebedrifter og deres leverandører. Med begrensede ressurser til eget sikkerhetsarbeid kan de små være særlig utsatte. Et nyttig verktøy for foretakene kan være NSMs veileder om håndtering av trusler fra fremmed etterretning[14].

I rapporten Helhetlig digitalt risikobilde 2019[15] fremhever NSM at digitaliseringen av tjenester fra offentlig og privat sektor bidrar til at Norge er blitt mer avhengig av den internasjonale digitale infrastrukturen. Dette er spesielt aktuelt for finansiell infrastruktur, der mange av de grunnleggende finansielle tjenestene er basert på internasjonalt samarbeid eller utføres fra andre land, jf. punkt 3.6.2.

NSM påpeker at organiserte kriminelle og statlige aktører utgjør de største truslene mot norske mål, inkludert virksomheter som ivaretar viktige samfunnsfunksjoner. Gjennom datanettverksoperasjoner utføres rekognosering og innhenting av informasjon om samfunnskritiske funksjoner, sårbarheter i

[11] NSM og Kripos gir ut temarapport om løsepengevirus
[12] Fokus 2020 Etterretningstjenesten
[13] Nasjonal trusselvurdering 2020 PST
[14] Handtering av digital spionasje NSM
[15] Helhetlig digitalt risikobilde 2019 NSM

infrastruktur, krisehåndtering og beredskap som senere kan utnyttes. Norske foretak er også utsatt for tyveri eller manipulering av sensitiv informasjon, som aktørene senere kan benytte for å forstyrre eller ødelegge kritisk infrastruktur.

Fremmed etterretning kan også forsøke å rekruttere personell for å få tilgang til informasjon om sårbarheter i digital infrastruktur eller annen informasjon om foretaket, jf. NSMs temarapport om innsiderisiko[16] og punkt 3.4.5.

Kriminelle digitale operasjoner blir stadig vanskeligere å oppdage og metodene er sammensatte. Finanstilsynet anbefaler at foretakene gjør bruk av NSMs veileder med råd om hvordan man kan forebygge og håndtere dataangrep[17].

Skillet mellom fremmed etterretning og organiserte kriminelle med økonomiske motiver viskes stadig mer ut. Fremmed etterretning vil ønske å skjule sin tilgang til systemene, og kan villede ved å gi inntrykk av at formålet med et angrep er å få tilgang til finansielle midler, for eksempel gjennom angrep med løsepengevirus.

Rapportene beskriver også Cybercrime as-a-Service", der svært datakyndige aktører kartlegger sårbarheter ved og etablerer tilganger til foretak, og selger dette videre til andre kriminelle eller statlig etterretning som utnytter sårbarhetene.

3.4.3. Foretakenes forsvarsverk

Samtaler med foretak og foretakenes svar på undersøkelse om sårbarhet viser at digitale angrep anses som en alvorlig og aktuell risiko og at risikoen knyttet til angrep er økende. Etableringen av et helhetlig forsvar mot digitale angrep er krevende som følge av bruk av ny teknologi og kompleksitet, bredde og omfang av digitaliseringen. Undersøkelsen viser også at det er svakheter innen nettverkssegmentering, perimetersikring[18] og kryptering, slik Finanstilsynet også har observert gjennom tilsyn.

Foretakene har i hovedsak arbeidet med å sikre sine nettverk mot angrep utenfra, men det er avdekket at flere selskaper nasjonalt og internasjonalt har opplevd at angripere over lengre tid har operert på innsiden av nettverkene. etter hvert som angrepsmetodene utvikles, vil foretakets evne til å oppdage og fjerne uønskede aktører på innsiden være avgjørende for å redusere risiko og potensielt skadeomfang.

Finanstilsynet mener det er viktig at foretakene sikrer at overvåking og kontroll ikke bare etableres gjennom den tradisjonelle perimetersikringen, men at det også legges til grunn at kriminelle kan ha etablert ett eller flere digitale fotfester på innsiden av nettverket.

[16] NSM publiserer temarapport om innsiderisiko
[17] Hvordan forebygge, oppdage og håndtere målrettede digitale angrep NSM NorCERT
[18] Grunnsikring av komponenter i IKT-infrastrukturen, som brannmurer og svitsjer i nettverk

3.4.4. Sikkerhetskultur og opplæring

Foretakets styre og ledelse har ansvar for at nødvendig sikkerhetskultur etableres i foretaket gjennom opplæringsprogram og løpende bevisstgjøring, og at det etableres nødvendige kontroller for å følge opp at den enkelte overholder de sikkerhetskrav som er satt.

Gjennom tilsyn konstaterer Finanstilsynet at foretakene har etablert opplæringsprogrammer som hovedsakelig omfatter grunnleggende holdninger, som skal begrense risikoen for at foretakets medarbeidere i strid med gjeldende sikkerhetskrav utfører uaktsomme handlinger som følge av blant annet sosial manipulering.

Foretakenes svar på undersøkelsen om sårbarhet viser at det er svakheter når det gjelder ansattes årvåkenhet for trusler og angrep og at problemet er økende. Enkelte foretak har særlige utfordringer.

Finanstilsynet mener foretakene må legge til rette for at ansatte blir gjort kjent med foretakets policyer blant annet innen informasjonssikkerhet, og hvilke retningslinjer som gjelder. Foretakets operative enheter bør gjennomføre kontroller for å påse at retningslinjenes krav overholdes av de ansatte, og compliancefunksjonen må overvåke dette arbeidet.

3.4.5. Sårbarhet og trusler – den menneskelige faktoren

Utro medarbeidere utgjør en trussel og uaktsomme medarbeidere utgjør en sårbarhet som kan undergrave sikringen av foretakets og kundenes verdier. Ubevisste eller bevisste handlinger kan påføre foretak betydelig skade.

Sårbarhet

Ansatte og personell hos leverandører med roller og ansvar innen teknisk arkitektur, systemutvikling, sikkerhet og med utvidede tilgangsrettigheter vil kunne være i målgruppen for kriminelle. Kriminelle opererer på sosiale plattformer, særskilt for teknikere, for å kartlegge relevante personer og få innsikt foretaks tekniske infrastruktur.

Finanstilsynet konstaterer at foretak ikke har etablert særskilte tiltak for å skjerme personinformasjon for omgivelsene, herunder foretaks ansatte og personell hos leverandører, som har roller som kan være av interesse for og utnyttes av kriminelle. Det fremgår heller ikke klart hvilke tiltak foretak har etablert for å redusere risikoen for at informasjon som kan utnyttes av kriminelle legges ut på sosiale medier, som for eksempel LinkedIn[19] og reddit[20]. Finanstilsynet mener foretak bør øke ansattes bevissthet gjennom foretakets sikkerhetsprogram.

Finanstilsynet viser til vedlegg 8 vedrørende den europeiske banktilsynsmyndighetens (EBA) standard for å identifisere ansatte med vesentlig innvirkning på foretaks risikoprofil, og som foretakene bør rette en spesiell oppmerksom mot.

[19] https://www.linkedin.com/
[20] https://www.reddit.com/

Trussel

Finanstilsynets mener det fortsatt er økende risiko for at kriminelle samarbeider med, herunder lykkes med å plassere, personer på innsiden av et foretak, eller hos dets leverandører. Innsidere med utvidede tilgangsrettigheter til betalingssystemene kan med kløkt gjennomføre svindel uten å bli oppdaget, og innsidere kan gjennomføre operative handlinger som medfører alvorlige driftsavbrudd. Finanstilsynet ser det også som en risiko at innsidere samarbeider med kriminelle for å sluse midler gjennom bankenes systemer.

Det mørke nettet

Det er en risiko for at kriminelle kan benytte "det mørke nettet" (Darknet[21]) for utveksling av informasjon fremskaffet av en innsider[22]. Dette kan være sensitiv informasjon om et foretak, som benyttes i planleggingen av cyberangrep, herunder liste over epostadresser og påloggingsinformasjon, sensitiv informasjon om internt anliggende i foretaket, eller sensitiv informasjon om foretakets kunder. Finanstilsynet anser det som krevende å avdekke slike forhold og er heller ikke kjent med om foretak har blitt utsatt for denne type kriminalitet. Foretakene vil gjennom forebyggende tiltak kunne redusere innsiderisikoen, jf. punkt 3.4.6.

Kontroll av personell

Finanstilsynet mener foretakene bør rette særskilt oppmerksomhet mot, og vurdere en utvidet bakgrunnssjekk av, personell som skal utføre kritiske funksjoner innen områder som operativ drift, informasjonssikkerhet og transaksjonsovervåking. I dette arbeidet anbefaler Finanstilsynet å følge rådene i veilederen "Sikkerhet ved ansettelsesforhold – før, under og ved avvikling" utgitt av Politiets sikkerhetstjeneste, NSM, Politiet og Næringslivets Sikkerhetsråd.[23]

Ansattes aktiviteter i IKT-systemene blir i begrenset grad analysert. Finanstilsynet mener foretakene innenfor fastsatte regler og i tråd med personvernet og foretakets etiske retningslinjer, bør innføre proaktive kontroller for å avdekke unormale aktiviteter. Dette vil etter Finanstilsynets syn være et viktig tiltak for å forebygge og avdekke kriminelle handlinger begått av ansatte eller av personell hos leverandører.

Foretakenes svar på spørreundersøkelsen om sårbarhet, viser at foretakene har utfordringer med å i tilstrekkelig grad analysere logger for å avdekke unormale aktiviteter og reagere på avvik.

3.4.6. Informasjonslekkasjer

Foretakene har en tillitsbasert tilnærming og legger til grunn at ansatte som gis tilgang til konfidensiell informasjon om foretakenes kunder og om foretakets interne forhold opptrer aktsomt og lojalt. Denne tilliten gjelder også foretakenes leverandører og personell som har tilgang til konfidensiell informasjon.

[21] https://en.wikipedia.org/wiki/Darknet
[22] www.darkreading.com
[23] Sikkerhet ved ansettelsesforhold

Finanstilsynet har gjennom tilsyn observert at foretak mangler klassifisering av informasjon og kontroller for overvåking av dokumenter som sendes ut av foretaket på e-post, dokumentasjon som kopieres til eksterne lagringsenheter eller kopieres til private skytjenester. Foretakenes svar på spørreundersøkelsen om sårbarhet viser at det er mangler knyttet til klassifisering av strukturerte og ustrukturerte data. Manglende klassifisering gjør det vanskelig å utføre kontroller for å hindre informasjonslekkasjer. Med dagens praksis, anser Finanstilsynet det som lite sannsynlig at sensitiv informasjon som sendes uautorisert, bevisst eller ubevisst, til eksterne kilder vil bli oppdaget. I tillegg til de åpenbare konsekvenser dette kan medføre, anser Finanstilsynet at det er risiko for at ansatte ubevisst bidrar til informasjonslekkasje som følge av sosial manipulering.

Finanstilsynet konstaterer gjennom tilsyn at foretak løper en høy risiko for bevisst eller ubevisst informasjonslekkasje til det offentlige rom, medier, konkurrenter eller enkeltindivider. Tap av omdømme, tap av kunder og betydelige bøter, som eksempelvis følge av brudd på personvernet, kan være noen av konsekvensene. Denne formen for risiko kan reduseres gjennom bevisstgjøring og opplæring av ansatte. Finanstilsynet anser det som uforsvarlig om foretak ikke har etablert kontroller for å redusere risikoen for lekkasje av sensitiv informasjon.

3.4.7. Reaksjonstid ved cyberangrep

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- og kriseplaner, og hvor det framgår hvilke aktiviteter som skal iverksettes og hvem som er bemyndiget til å beslutte iverksettelse. Foretakene bør i størst mulig grad identifisere hvilke konsekvenser det vil kunne få dersom nettverket helt eller delvis må tas ned, noe som kan være nødvendig for å begrense skadeomfanget. Forhåndsbestemte og veloverveide tiltak vil bidra til at raske beslutninger kan tas, og at de tas i riktig rekkefølge.

Finanstilsynet mener generelt at mange foretak ikke er tilstrekkelig forberedt på å håndtere alvorlige cyber-hendelser. Det er 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 slik hendelse inntreffer.

3.4.8. Digital kriminalitet ved bruk av kunstig intelligens

Finanstilsynet opprettholder sin vurdering fra fjorårets ROS om at "falske nyheter" vil kunne ramme foretakene ved bruk av kunstig intelligens. Dette kan være i form av falske framstillinger rettet mot ansatte, ledelse, styremedlemmer og foretakets kunder. Det kan også være falske nyheter med det formål å skade et foretak eller å påvirke kursen for børsnoterte foretak. Kunstig intelligens kan benyttes både til angrep og forsvar, og foretakene bør også være oppmerksomme på denne typen trusler.

3.4.9. **Kvanteteknologi – en sikkerhetstrussel**

Forskere og analytikere innen cybersikkerhet er bekymret for utviklingen innen kvanteteknologi, herunder kvantemaskiner og kvantekommunikasjon. Teknologien er basert på kvantefysikk, mens dagens datamaskiner er basert på standard elektronikk. Uroen skyldes at dagens kryptografi, som benyttes i internettkommunikasjon og datalagring, ikke er tilstrekkelig robust dersom kvanteteknologi benyttes til dekryptering. Dette vil utgjøre en svært stor sikkerhetstrussel når teknologien tas i bruk av kriminelle aktører. Dagens sikkerhetsarkitektur innen de fleste områder i samfunnet er basert på de samme byggeklossene, og brytes dette ned vil de samfunnsmessige konsekvensene være svært alvorlige. Imidlertid er utviklingen ikke kommet langt nok til at kvanteteknologien foreløpig utgjør en trussel.

For å møte trusselen, mener Finanstilsynet at foretakene og deres leverandører allerede nå bør følge utviklingen og bygge nødvendig kompetanse. Finanstilsynet mener det er viktig at næringen ligger i forkant slik at sikkerhet i den teknologiske infrastrukturen utvikles i takt med utviklingen innen kvanteteknologi.

3.4.10. **Sårbarhets- og sikkerhetstest (TIBER)**

Flere av de utenlandske bankene med filial eller datterselskap i Norge, gjennomfører eller planlegger sikkerhetstesting av foretakets forsvarsverk i sine respektive hjemland basert på den europeiske sentralbankens (ECB) TIBER-rammeverk[24]. Sikkerhetstestene tilrettelegges og koordineres av det enkelte lands myndigheter.

Gjennom TIBER-rammeverket får foretak tilgang til trusselinformasjon fra og kompetansen til nasjonale etterretningstjenester, kompetansen til en samlet europeisk sikkerhetsbransje, samt sikkerhetskompetansen i de største europeiske finansforetakene.

Norges Bank og Finanstilsynet samarbeider med sikte på å etablere et rammeverk for sikkehetstesting basert på TIBER-rammeverket for finansnæringen i Norge. Norske finansforetak er små i europeisk målestokk, og har naturlig nok mindre ressurser enn store europeiske foretak. Kompetansedeling mellom norske foretak i et slikt testrammeverk vil kunne innebære en betydelig styrking, spesielt med tanke på forebygging av uønskede hendelser..

TIBER-rammeverket er videre omtalt i vedlegg 8.

3.4.11. **Cyberforsikring som risikoreduserende tiltak**

Finanstilsynet oppfordrer foretakene til å vurdere behovet for å sikre seg både økonomisk og operasjonelt på IKT-området. I tillegg til cyber-relaterte angrep, bør ulike andre scenarier inngår i vurderingen, slik som eksempelvis driftsavbrudd. For å sikre at foretaket har forsikringsdekninger tilpasset egne behov, jf. vedlegg 10, bør foretaket systematisk gjennomgå egne og leverandørenes

[24] Threat Intelligence-Based Ethical Read-teaming

forsikringsdekninger for å avdekke eventuelle svakheter, for eksempel at en leverandør ikke er forsikret mot svik/svindel fra egne ansatte.

Finanstilsynet understreker at forsikringer ikke reduserer betydningen av risikoreduserende tiltak i tråd med foretakets risikotoleranse.

Se vedlegg 7 for nærmere omtale om informasjonssikkerhet.

3.5. IKT-drift

Finanstilsynet vurderer utfordringene som omtales i punktene nedenfor, som de største operasjonelle risikoene for foretakenes drift av IKT-virksomheten. Viktigheten av at foretakene identifiserer forhold, både organisatoriske og tekniske, som kan true sikker og stabil drift understrekes.

3.5.1. Drift av et komplekst økosystem

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 IKT-leverandører 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 gjennom stort omfang av endringer øker også risikoen for at feil kan oppstå.

Foretakenes svar på spørreundersøkelsen om sårbarhet viser at kompleksiteten i systemporteføljene øker, noe som medfører risikoer på en rekke områder. Feilsøking og problemløsning fremstår som komplisert og krevende, og det er utfordrende å etablere gode kriseløsninger. Foretakene ser også utfordringer med å etablere et helhetlig forsvarsverk mot cyberangrep. De peker også på at det er krevende å sammenstille og analysere logger.

Kompleksiteten i den teknologiske infrastrukturen fører også til at det er utfordringer knyttet til grundige og helhetlige risikovurderinger av den operasjonelle driften.

3.5.2. Sanering av utdaterte systemer

Mangelfull dokumentasjon og tilgang til personell med kompetanse på utdaterte systemer skaper utfordringer i arbeidet med å både sanere og migrere funksjonaliteten over til moderne utviklingsplattformer. Vedlikeholdskostnadene for utdaterte systemer er som regel høye, og for enkelte systemer er vedlikeholdet avsluttet. Systemkoden har sårbarheter som følge av at systemet ble utviklet i en tid med svært begrensede sikkerhetskrav.

I dialog med foretak kommer det frem at sanering av gamle systemer medfører komplekse operasjoner og krever grundig planlegging. En høy grad av integrasjon mellom ulike systemer, og systemer i porteføljen hvor funksjonalitet og bruksområde ikke er kjent, gjør saneringsarbeidet svært vanskelig.

Systemer utviklet med moderne teknologi og metodikk, og som skal erstatte gamle systemer, fører til utfordringer ved at systemer som skal saneres må være i drift mens nye systemer settes i produksjon og gjennomgår godkjenningsprosesser. Foretak opplever at dette er forhold som utgjør risiko for alvorlige driftsavbrudd.

Finanstilsynet er kjent med at foretak velger å gjennomføre organisatoriske endringer parallelt med utskifting av utdaterte systemer. Dette har imidlertid vist seg å gi foretakene ekstra og unødige utfordringer i den teknologiske omstillingen. Finanstilsynet mener dette er et forhold som foretak må hensynta gjennom sin risikovurdering og planlegging for å sikre nødvendig koordinering mellom teknologiske og organisatoriske omstillingsprosjekter.

3.6. Kontinuitetsledelse og kriseledelse

3.6.1. Kartlegging av bankenes evne til å håndtere en krise

Finanstilsynet gjennomførte i 2019 en omfattende spørreundersøkelse om kontinuitetsledelse og kriseledelse, rettet mot norske banker og internasjonale banker med filial i Norge. Formålet var å innhente opplysninger som skal gi Finanstilsynet grunnlag for å vurdere i hvilken grad bankene er forberedt på og i stand til å håndtere krisesituasjoner.

Hovedfokuset var rettet mot håndtering av alvorlige IKT-hendelser, hvor kriseplan og eventuelt kriseløsning skal iverksettes. Foretakene svarte også på spørsmål om styring og kontroll, og organisering for å ivareta foretakets helhetlige arbeid for å forberede foretaket på og å gjøre foretaket i stand til å håndtere alvorlige hendelser som defineres som en krise eller katastrofe som vil påvirke foretakets normale aktivitetsnivå. Dette omfattet, i tillegg til operasjonelle hendelser i driften, cyberangrep, naturkatastrofer, terror, sykdomsutbrudd som rammer en stor andel av de ansatte, trusselsituasjoner, alvorlige brudd i infrastruktur som nettverk og strøm og avbrudd i kritiske IKT-tjenester.

Identifiserte svakheter

Gjennom analyse av svarene fremkom det at bankene i stor grad har etablert kriseløsninger, også omtalt som beredskapsløsninger eller reserveløsninger, som skal iverksettes dersom normal driftsløsning ikke er tilgjengelig. Analysen indikerer tydelig at mangler som kan gi banker utfordringer med å håndtere en krise forekommer, spesielt dersom kriseløsning må iverksettes. Dette gjelder spesielt banker som har mangler i styrende dokumenter, opplæring, trening, øvelse og test av kriseløsning. Analysen viste også at bankene hadde utarbeidet begrenset med scenarioer til grunn for trening og øvelser.

Forretningsmessig konsekvensanalyse, eller Business impact analysis (BIA), er en prosess for å identifisere konsekvensene av å miste tilgang til forretningskritiske tjenester og prosesser og å definere i hvilken rekkefølge tjenester og prosesser skal reetableres basert på forretningsmessig kritikalitet. Den forretningsmessige konsekvensanalysen legger grunnlaget for utarbeidelse av foretakets kontinuitets- og kriseplan. Analysen bør omfatte ulike scenarioer og mulige konsekvenser av disse scenarioene.

Gjennom tilsyn og samtaler med foretak konstaterer Finanstilsynet at det er utfordrende for forretningssiden å forstå og definere i hvilket omfang og hvilke konsekvenser det vil få dersom alvorlige hendelser oppstår, herunder tap av data. Forretningssiden har lav risikoappetitt for nedetid, men det viser seg å være utfordrende å identifisere hvilke forretningsprosesser som er de viktigste. Analysen viste at foretak mangler forretningsmessige konsekvensanalyser for kritiske forretningsprosesser. Undersøkelsen viser også at kun en tredjedel av bankene har vurdert og analysert samfunnsmessige konsekvenser som en del av sine forretningsmessige konsekvensanalyser.

Analysen viste at de fleste bankene har tilrettelagt for alternativt arbeidssted, men en tredjedel av bankene hadde ikke etablert rutiner for å iverksette en slik flytting. En fjerdedel av bankene hadde ikke vurdert bankens beredskap innen IKT-området. Hver femte bank manglet oversikt over alternativt personell dersom ansatte av ulike årsaker ikke er tilgjengelig når krisen inntreffer, eller under krisens forløp.

Digitaliseringen av forretningsprosessene har etter det Finanstilsynet erfarer medført at forretningssiden i enda større grad overlater arbeidet med de forretningsmessige konsekvensanalysene til IT-avdelingen. Videre synes det som om foretak mangler oversikt over hvilke konsekvensanalyser som er utarbeidet, og i hvilken grad foretak har gjort samlede og tilstrekkelig vurderinger for å opprettholde forretningsdriften dersom det oppstår brudd eller forstyrrelser i kritiske systemer, og i tilfeller der foretaket utsettes for et alvorlig cyberangrep. Det gis også inntrykk av at foretak ikke har den nødvendige forståelsen for hvordan en alvorlig IKT-hendelse skal håndteres i samarbeid med leverandører. Det er videre Finanstilsynets inntrykk at foretakene i for liten grad vurderer endringer i konsekvensanalysen som følge av endringer i trussel- og risikobildet.

Undersøkelsen viser at foretakene må forbedre sitt arbeid med kontinuitetsledelse og kriseledelse, herunder risikovurderinger og konsekvensanalyser, og beredskap. Finanstilsynet påpeker styrets og ledelsens ansvar for at foretaket har etablert en organisering og infrastruktur som sikrer stabile driftsløsninger, tilstrekkelig beredskap og effektive kriseløsninger også ved alvorlige kriser.

3.6.2. Geopolitiske forhold

Finanstilsynet har tidligere pekt på avhengighet av eksterne leverandører som en sårbarhet dersom alvorlige kriser eller katastrofer rammer globale aktører som leverer kritiske IKT-tjenester til finansnæringen. Dette gjelder spesielt der operativt personell fra utlandet er avskåret fra å utføre sine oppgaver. Slike hendelser vil kunne medføre vesentlige utfordringer med å opprettholde samfunnskritiske tjenester på en sikker og god måte, spesielt om krisen vedvarer. Tilsvarende usikkerhet ble knyttet til forvalting, herunder håndtering av alvorlige feilsituasjoner og sikkerhetshendelser, som kan medføre behov for et tett samarbeid med flere involverte leverandører i Norge og utlandet.

Finanstilsynet konstaterer gjennom hendelsesrapporteringen at foretakene i samarbeid med sine leverandører i stor grad klarer å løse til dels alvorlige avbrudd i tjenestene. Koronakrisen har også vist at foretakene har opprettholdt stabil drift, jf. punkt 2.4. Det er imidlertid knyttet usikkerhet til i hvilken

grad foretakene ville evnet å gjenopprette driften ved IKT-hendelser eller cyberangrep som medfører alvorlig avbrudd.

Finanstilsynet mener foretakene må ta høyde for at tilsvarende og mer alvorlige kriser kan inntreffe i fremtiden, og at næringen i slike situasjoner må være i stand til å opprettholde sikker og stabil drift av den finansielle infrastrukturen. 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. Foretakene også må være i stand til å håndtere alvorlige IKT-hendelser under kriser som oppstår. Dette vil også gjelde kriser, herunder geopolitiske forhold, som fører til at utenlandske leverandører er avskjermet fra å utføre kritiske IKT-tjenester, jf. punkt 3.4.2.

Finanstilsynet anser at erfaringene foretakene og myndigheten har tilegnet seg gjennom koronapandemien vil ha stor verdi i foretakenes evaluering og videre strategi for utkontraktering av IKT-tjenester til utlandet.

Finanstilsynet forventer at foretakene og deres leverandører gjennomfører en grundig evaluering av sårbarheter, risikoer og konsekvenser i lys av koronapandemien. Samtidig understreker Finanstilsynet viktigheten av at foretakene tar hensyn til geopolitisk usikkerhet i sine risikovurderinger og beslutningsprosesser.

3.6.3. Hjemmekontor som del av kriseløsningen

Flere foretak har etablert løsninger som gjør at oppgaver kan utføres fra hjemmekontor. Løsningene kan også benyttes som del av foretakets kriseløsning, og der tilgangene til foretakets systemer vil avhenge av den inntrufne situasjonen.

For å håndtere situasjonen som oppsto med koronapandemien, åpnet flere foretak for at egne ansatte og personell hos leverandører, også i utlandet, kunne utføre oppgaver fra hjemmekontor. Dette omfattet blant annet oppgaver innen overvåking og drift av kritisk infrastruktur. Slikt personell har ofte utvidede tilgangsrettigheter og kan ved misbruk eller ved feil påføre foretakene skade, som for eksempel avbrudd på kritiske tjenester. Finanstilsynet anser det som en spesielt høy risiko der personell hos leverandører i høyrisikoland har tilganger til foretakenes kritiske infrastruktur og systemer fra sitt hjemmekontor.

Selv med utvidede sikkerhetstiltak, mener Finanstilsynet sårbarheten for uautoriserte handlinger og cyberangrep kan øke ved utstrakt bruk av hjemmekontor. Et hjemmenettverk har som oftest svakere sikkerhetsmekanismer enn foretakenes interne nettverk. Teknologi tilkoblet ansattes hjemmenettverk kan ha sårbarheter som eksponerer nettverket for digital kriminalitet. Et cyberangrep mot et foretaks infrastruktur i kombinasjon med DDoS-angrep mot hjemmenettverket til beredskapspersonell som utfører viktige drifts- og sikkerhetsoppgaver, hvor målet er å hindre oppgaveutførelsen, kan være et relevant trusselscenario. Slike angrep kan også ramme ansatte som utfører viktige oppgaver på forretningssiden.

Finanstilsynet forutsetter at foretakene har sikret at trafikken krypteres gjennom VPN-forbindelser, at utvidede sikkerhetstiltak, herunder overvåking og kontroll, er etablert og at utvidede tilgangsrettigheter ikke kan benyttes ved bruk av åpne nett.

3.6.4. Nasjonale og internasjonale kommunikasjonslinjer

Finanssektoren er avhengig av et velfungerende elektronisk kommunikasjonsnett både innenlands og mot utlandet. At nær all trafikk mot utlandet føres i et begrenset antall fiberforbindelser fra Oslo-området via Sverige utgjør en sårbarhet for foretak som har egen eller utkontraktert virksomhet i utlandet, jf. rapport fra NKOM[25]. Det vises også til at klimaendringer kan føre til alvorlige naturkatastrofer i Norge og i våre naboland, men også i India og regioner som Baltikum og Øst-Europa.

EFTAs overvåkingsorgan (ESA) godkjente i 2019 støtte til kapasitetsøkning gjennom i nye sjøfiberkabler til utlandet, som skal bidra til å redusere sårbarheten i den elektroniske kommunikasjonen til og fra Norge.

Finanstilsynet påpeker at sårbarhetene som NKOM omtaler bør inngå som en viktig del av foretakenes risikovurdering for kriseløsninger, og at foretakenes må etablere kriseløsninger som tar høyde for kommunikasjonsbrudd i Norge eller mot utlandet. Finanstilsynet mener 5G bør vurderes som en viktig del av kommunikasjonsberedskapen for kritiske tjenester.

3.7. Utvikling og innovasjon

Den teknologiske utviklingen åpner opp for nye forretningsmodeller, og økt digitalisering og automatisering. Nye aktører etableres med moderne tekniske plattformer, og konkurransesituasjonen for foretakene er endret ved at nye aktører etablerer løsninger i grensesnittet mellom foretakene og foretakenes kunder. Systemporteføljen er kompleks, og sammensatt av ny og gammel teknologi, ulike plattformer og mange aktører i verdikjeden. Dette er forhold som stiller store krav til utviklings- og forvaltningsmetodikk.

Svarene på spørreundersøkelsen om sårbarhet, viser at foretakene likevel mener risikoen knyttet til kompleksitet i IKT-systemene er minkende.

3.7.1. Utviklingsmål

Finanstilsynet mener det er viktig at styre og ledelse retter et kritisk blikk på hvilke interessenter som skaper forventninger 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, unødvendige og/eller mislykkede organisatoriske og teknologiske endringsprosjekter.

[25] NKOM Årsrapport 2017 og NKOM Årsrapport 2019

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 eller bør realiseres. Spesielt gjelder dette der ny teknologi skal anvendes.

3.7.2. Smidig utviklingsmetodikk

Bruk av smidig (agil) utviklingsmetodikk, som blant annet DevOps[26] (Development and Operations), forutsetter at foretakene og dens leverandører følger strenge retningslinjer for å redusere risikoen for at applikasjoner settes i produksjon med sårbarheter, herunder sikkerhetshull som kan utnyttes av kriminelle. I den tradisjonelle vannfallsmetodikken har sårbarhet i kode blitt avdekket blant annet ved kodegjennomgang og penetrasjonstesting, og gjennom god endringsstyring.

Foretakenes svar på spørreundersøkelsen om sårbarhet viser at økt krav og behov for nye løsninger, med kort tid til markedet, kan føre til høyt leveransepress og svekket kvalitet i løsningen som utvikles.

Den økte bruken av smidig utviklingsmetodikk, hvor nye funksjonalitet i applikasjonen testes og settes i produksjon fortløpende for raskere å kunne levere nye løsninger og funksjonalitet til markedet, kan medføre en økt risiko for feil. Det skaper behov for å tilpasse og innlemme sikkerhetsdimensjonen gjennom de ulike utviklingsstegene og i driftsoppsett for å redusere risikoen for at rask utviklingstakt går på bekostning av sikkerheten. Finanstilsynet anser det som en reell risiko at sikkerhetsdimensjonen ikke gis tilstrekkelig prioritet i krevende utviklingsprosjekter med korte frister i en stadig sterkere konkurransesituasjon.

Finanstilsynet understreker at det er ledelsens ansvar å kontrollere at sikkerhet inngår som en sentral funksjon i alle utviklingsprosjekter, og at det stilles til rådighet nødvendige ressurser for at sikkerhetsnivået i alle foretakets systemer er i tråd anbefalinger og god praksis. Dette gjelder også der tredjepart tilbyr systemer i kundegrensesnittet som er integrert gjennom bankens API-er.

Finanstilsynet mener kodegjennomgang med grundig analyse av kildekoden, for å avdekke sårbarheter for uautorisert tilgang eller eksponering av personopplysninger, for eksempel gjennom bruk av sikkerhetsteknologi for skanning, bør står sentralt i utviklingsprosessen, og at dette skjer gjennom alle utviklingstegene. En kodegjennomgang skal også verifisere at koden er i tråd med den standarden som er benyttet. Det bør også gjennomføres koderevisjoner av systemer og applikasjoner som er i produksjon, og penetrasjonstester.

3.7.3. Digital transformasjon gjennom bruk av applikasjonsgrensesnitt (API)

Bruken av applikasjonsgrensesnitt har blitt en viktig del av finansnæringens digitale transformasjon. Gjennom systemløsninger kommuniseres det i 'dialogmodus' mellom foretak ved å stille spørsmål og få svar i sanntid. Via samhandlingspartnere kan foretakene på den måten distribuere tjenestene til sine

[26] https://en.wikipedia.org/wiki/DevOps

kunder på nye måter. Forutsatt at kunden gir sitt samtykke, kan andre foretak (tredjepartsaktører) yte tjenester ved bruk av andre foretaks data, enten dette skjer gjennom regulerte tilganger, avtalebaserte tilganger eller på andre måter.

Den økte bruken av applikasjonsgrensesnitt skjer innenfor både bank, forsikring, betalingsområdet og verdipapirområdet, og kalles gjerne Open Banking eller Open Insurance. Reguleringen har kommet lengst innenfor betalingstjenesteområdet, der det stilles strenge sikkerhetskrav til foretakene, både til foretakene som har dataene og tredjepartsaktører som ønsker tilgang til dataene, og ansvarsforholdene er regulert. I sektorer uten etablert regelverk, må tilgangen til data gis gjennom avtaler, der også sikkerhet og ansvar er ivaretatt.

Selv om GDPR gir kunden eierskap til og rett på tilgang til egne data, er det viktig at denne tilgangen gis på betryggende vis. Foretakene har klare plikter når det gjelder oppbevaring og sikring av kundenes data, jf. IKT-forskriften § 5, herunder at disse ikke kommer uvedkommende i hende, og at de ikke blir brukt for andre formål enn kunden har gitt samtykke til. Har en kunde gitt en tredjepart samtykke til tilgang til sine data, slik at denne har fullmakt til å opptre på vegne av kunden, stilles det likevel krav til at foretaket som har dataene sikrer at tredjepart legitimerer seg på lik linje som i fullmaktsforhold for øvrig.

Der tilgangen er regulert, stilles det strenge krav til at tredjepartsaktører som gis konsesjon har godt dokumenterte rutiner, blant annet knyttet til IKT-sikkerhet. Der tilgangen ikke er regulert, må foretakene som har dataene gjennom avtaler selv sikre at IKT-sikkerheten blir ivaretatt, og at tredjepartsaktører også ivaretar tilstrekkelig IKT-sikkerhet.

Selv om bruken av API-er har flere fordeler, medfører bruken også risikoer og utfordringer, både for foretakene og for kundene. Foretakene må håndtere risikoer som følger med økt deling av kundedata og økende tilkobling til andre foretak, og iverksette hensiktsmessige risikoreduserende tiltak i tråd med vurderinger gjort i risikoanalyser og der sikkerhet må balanseres mot brukervennlighet. Bruken av API-er kan komplisere utformingen av gode kriseløsninger og kan gjøre det utfordrende å etablere helhetlig forsvar mot dataangrep. Oversikt over tredjeparter kan være begrenset, særlig der tilgangen ikke skjer avtalebasert. Flere tekniske leverandører, også fra ulike jurisdiksjoner, kan være involvert i verdikjeden, noe som kan gjøre den uoversiktlig å overvåke. Ansvarsforhold kompliseres når antall involverte aktører øker. Selv om det er etablert regler for plassering av ansvar, kan foretakenes omdømmerisiko øke.

Jo flere foretak dataene deles med, jo mer sårbare blir systemene for datainnbrudd. Angrepsflaten vil endres ved at kriminelle også vil kunne rette sin aktivitet mot tredjepartsaktører. Angrep kan skje gjennom utnyttelse av sårbarheter i applikasjonene fra tredjepart, og kunder kan i større grad bli utsatt for sosial manipulering. Foretakenes utfordring er først og fremst å sikre en riktig forståelse av sikkerhetskravene i dette nye økosystemet, både hos foretak som har dataene og hos den enkelte tredjepart og i forhold til kunders bruk av tredjepartsløsninger.

3.7.4. **Bruk av ny teknologi**

Foretak som er datadrevet, har en faktabasert tilnærming hvor foretaket benytter tilgjengelige interne og eksterne data (Big Data) for å underbygge beslutninger fremfor å bruke skjønn og synsing. Til hjelp i dette arbeidet benyttes tilgjengelig teknologi med målsetting om reduserte kostnader, økte inntekter, bedre kundeopplevelser og/eller økt presisjon i beslutningsstøtte. Teknologiene og tjenestene som skal sikre måloppnåelse er eksempelvis skybaserte tjenester og teknologier (Cloud), robotisert prosessautomatisering (RPA), stordata (Big Data), effektive analyseverktøy (herunder bruk av kunstig intelligens og maskinlæring), blockchain og tingenes internett (IoT).

De nevnte teknologiene og tjenestene som utvikles basert på teknologien, har hver sitt kompliserte risikobilde. Når virksomhetene kobler flere nye teknologier i systemløsninger, oppstår et fasettert risikobilde. Risikobildet kompliseres ytterligere dersom foretaket har eller anskaffer samme type tjeneste/teknologi fra flere leverandører. Det er samtidig viktig å understreke at ny teknologi også vil redusere risiko, for eksempel ved å erstatte manuelle analyser og oppgaver.

Når foretaket vurderer risikobildet for tjenester og teknologier som er i bruk, vil det være krevende å etablere oversikt og kontroll med samtlige risikoer. Risikobildet må ses i forhold til hvordan teknologien benyttes, og i hvilken grad mulighetene i teknologien utnyttes. Foretakene bør i sitt risikoarbeid derfor sørge for å identifisere risikoene forbundet med tjenester og tekniske løsninger som er i bruk. En praktisk tilnærming er å vurdere risikoen i den enkelte forretningsprosess, slik at man sørger for å identifisere risikoer som går på tvers av IT-systemer, teknologier og leverandørforhold.

Regelverksutvikling

Den teknologiske utviklingen og endringer i risikobildet medfører behov for regelverksendringer. For å møte foretakenes utfordringer knyttet til implementering og bruk av ny teknologi, deltar Finanstilsynet aktivt i de europeiske tilsynsmyndighetenes (EBA, EIOPA, ESMA) prosjekt- og arbeidsgrupper som utvikler og etablerer reguleringer, retningslinjer og tekniske standarder for anvendelse av teknologi. Aktuelle tema er PSD 2, Open Banking, sikker kundeidentifisering (KYC), sikker bruk av betalingskort, Big Data, Avansert analyse (AI, ML), etisk bruk av IKT, hendelsesrapportering og sikkerhetsarbeid (TIBER/TLPT).

Finanstilsynets regulatoriske sandkasse gir foretak mulighet til å prøve ut nye, innovative produkter, teknologier og tjenester under oppfølging av Finanstilsynet. Den regulatoriske sandkassen vil også kunne bidra til å øke Finanstilsynets forståelse av nye teknologiske løsninger i finansmarkedet og gi Finanstilsynet verdifull innsikt i tilknyttet risiko.

Uavhengig av hvilken ny teknologi foretakene tar i bruk, gjelder prinsippene om forsvarlig virksomhet, styring og kontroll med bruken, sikkerhet i løsningen og operasjonell kontinuitet, og at lik risiko bør behandles likt.

Noen av teknologiene, og risikoene ved implementering og bruk, er nærmere beskrevet i vedlegg 9.

3.8. Logisk tilgangsstyring og -kontroll

Sårbarheter knyttet til mangelfull styring av tilganger utgjør en risiko for informasjonssikkerhetsbrudd, herunder brudd på konfidensialitet, integritet og tilgjengelighet. Konsekvensene ved slike brudd kan blant annet være tap av omdømme, bøter som følge av brudd på regulatoriske krav, uautoriserte handlinger som kan medføre alvorlige driftsproblemer og digital kriminalitet.

Finanstilsynet har avdekket tilfeller der det mangler skiller mellom utviklingsmiljøer og testmiljøer, og hvor det ikke gjennomføres periodisk gjennomgang av alle kritiske tilganger.

Foretakenes svar på spørreundersøkelsen om sårbarhet viser at risikoen knyttet til tilgangskontroll er økende. Finanstilsynet mener dette kan ha sammenheng med at foretakene i større grad utkontrakterer tjenester, og kjøper tjenester hvor eksterne konsulenter gis midlertidige tilganger.

Finanstilsynet understreker viktigheten av at personer med utvidede tilgangsrettigheter underlegges særskilt bakgrunnssjekk før tildeling, og at det løpende kontrolleres hvem som har fått tilgangene og om behovet til enhver tid samsvarer med oppgavene som skal utføres. Spesielt gjelder dette der ansatte endrer oppgaver, bytter avdeling eller slutter. Finanstilsynet forutsetter at foretak og dens leverandører benytter særskilte systemer for kontroll med denne type tilgangsrettigheter.

3.9. Fysisk sikring og adgangskontroll

3.9.1. Fysisk adgangskontroll

Finanstilsynet har ved tilsyn observert at besøkende til foretak som skal gis midlertidig adgang til foretakets lokaler, ikke blir bedt om å legge frem gyldig legitimasjon ved innregistrering, noe som kan innebære en risiko for foretakets IKT-virksomhet.

Finanstilsynet anser det som en reell risiko at utspekulerte kriminelle for eksempel som utgir seg for å være konsulenter eller rådgivere fra anerkjente selskaper, vil utnytte foretaks manglende besøkskontroll. Gjennom fysisk sosial manipulering vil kriminelle kunne tilegne seg informasjon som kan benyttes i planleggingen av kriminelle handlinger, herunder cyberangrep.

Finanstilsynet anbefaler foretak å vurdere behovet for å innskjerpe kontrollen der den besøkende for eksempel vil kunne tilegne seg informasjon som kan benyttes til å skade foretaket eller uautorisert koble seg til foretakets IKT-systemer med eksempelvis en keylogger[27](omtales også som keyboard eller key stroke logger).

3.9.2. Inntrengere

I hvilken grad et foretak er eksponert for terrorangrep eller ustabile personer, som velger å påføre ansatte eller leverandørpersonell skade, eller skade kritisk infrastruktur gjennom å ta seg inn i

[27] https://en.wikipedia.org/wiki/Keystroke_logging

foretakets lokaler, er vanskelig å fastslå eller forutse. Samtidig mener Finanstilsynet at foretak ikke kan se bort fra at denne type hendelser kan inntreffe.

Finanstilsynets observerer gjennom tilsyn at foretak i liten grad har etablert fysisk sikringer som vil begrense inntrengeres mulighet til å ta seg inn i lokasjoner ved bruk av makt. Forsterket sikring, for eksempel ved bruk av Mantrap[28], for tilgang til lokasjoner hvor kritiske funksjoner utføres, er ikke ansett som nødvendig, og foretak har i liten eller ingen grad vurdert å etablere prosedyrer, herunder for nedstengning og evakuering av ansatte, ved denne type situasjoner[29]. Når det gjelder fysisk adgangssikring til datasentre mener Finanstilsynet dette i hovedsak er godt ivaretatt.

I ytterste konsekvens kan sårbarheter i den fysiske sikringen føre til at for eksempel kritisk IT-personell rammes, med alvorlige menneskelige konsekvenser og alvorlige konsekvenser for IKT-virksomheten. Finanstilsynet mener at foretakene bør vurdere å etablere nedstengingsprosedyrer og evakueringsprosedyrer, og at prosedyrene inngår som del av foretakets kontinuitetsplan på lik linje med prosedyrer ved brann og bombetrusler.

3.10. Endringsstyring og sikkerhetsoppdateringer

3.10.1. Endringsprosessen

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, jf. punkt 3.7.2, er forhold som øker risikoen for at sårbarheter introduseres ved endringer i IKT-systemene som følge av for svak styring og kontroll.

Både funksjonelle og ikke-funksjonelle endringer utgjør en risiko om endringene ikke underlegges kontroll i alle steg fra endringsforslag foreligger til endringen er testet og satt i produksjon. God endringsstyring er en av de viktigste faktorene for å sikre kontinuitet i foretakets forretningsprosesser.

Finanstilsynet erfarer at både mindre alvorlige og alvorlige feil som oppstår ved endringer, jf. kapittel 5, ofte skyldes mangler i de kontroller som forventes utført, eller at foretakets retningslinjer ikke er tilstrekkelig etterlevd. Foretakene og dens leverandører har som regel dokumenterte prosesser og verktøy for å sikre at kontrollene ikke kan omgås. Finanstilsynet ser gjennom hendelsesrapporteringen at uautoriserte endringer forekommer uten at dette nødvendigvis oppdages før i ettertid og at kontroller ikke utføres med nødvendig kvalitet. Konsekvensen er ustabilitet og nedetid.

Finanstilsynet mener en høy endringstakt øker risikoen for at utviklings- og testteamene ikke gis nødvendig tid for å sikre at alle forhold ved løsningene ivaretas med forventet kvalitet. Foretakenes svar på spørreundersøkelsen om sårbarhet viser at omfanget av endringer er utfordrende for foretakene. Det fremgår også at leveransepresset og nye regulatoriske krav utgjør risiko i utviklingsløpene.

[28] https://en.wikipedia.org/wiki/Mantrap_(access_control)
[29] Eksempel på sentrale og viktige forhold ved en terrorsituasjon

3.10.2. **Sikkerhetsoppdateringer (Patch)**

Mangelfulle rutiner for sikkerhetsoppdateringer (patcher) utgjør en stor sårbarhet for foretakenes IKT-virksomhet. Det stilles derfor store krav til foretakenes og leverandørenes styring og kontroll med sikkerhetsoppdateringer (Patch management). Ettersom sårbarheter som identifiseres blant annet i applikasjoner, operativsystem og maskinvarekomponenter gjøres offentlig kjent, vil kriminelle raskt gjøre forsøk på å utnytte sikkerhetshullene. Reaksjonstiden, altså tiden fra sårbarheten blir kjent til sikkerhetsoppdateringen er testet og satt i produksjon, er kritisk for å unngå at foretaket eksponeres for angrep knyttet til identifiserte sårbarheter.

Finanstilsynet erfarer at foretak av ulike grunner velger å utsette sikkerhetsoppdateringer. Det understrekes at foretakene bør sørge for at risiko knyttet til innmeldte sikkerhetsoppdateringer vurderes og klassifiseres, og at konsekvensene ved å utsette oppdateringer synliggjøres. Foretakene har et selvstendig ansvar for å påse at deres leverandører har etablerte rutiner og kontroller for dette arbeidet.

3.11. Data og informasjon

3.11.1. **Styring og kontroll med data**

Styring og kontroll med foretakets data (Data management), og kundenes data, omfatter blant annet å sikre at dataene er beskyttet, tilgjengelige, pålitelige, at de benyttes på riktig måte og at dataene er lagret på de riktige stedene. Foretakets data har høy verdi og krever god styring og kontroll.

I foretakenes svar på spørreundersøkelsen om sårbarhet viser trenden at datakvaliteten svekkes. Foretakene erkjenner at det å sikre god datakvalitet er utfordrende og gir til kjenne at tiltakene for å forbedre datakvaliteten må videreføres.

Redusert datakvalitet kan være forårsaket av flere forhold, og øker risikoen på en rekke områder, for eksempel ved at kredittvurderinger eller hvitvaskingskontroller gjennomføres på bakgrunn av mangelfulle eller feilaktige data. Dette kan også føre til at risikovurderinger, og tiltak som følge av risikovurderingene, blir basert på mangelfull eller feilaktig informasjon.

Finanstilsynet mener det er viktig at foretakene fortsetter sitt arbeid med å bedre kvaliteten på sine data.

3.11.2. **Sikring av data (Backup)**

Løsepengevirus (Ransomware)[30] er en form for skadevare som kan medføre at systemer og/eller data ikke er tilgjengelig for brukerne. Dette skjer ved at en angriper låser systemene, stjeler data, sletter data eller krypterer disse, for deretter å kreve penger for å gi foretaket/brukere tilbake tilgangen til systemer og data. Selv om et foretak som kommer i en slik situasjon velger å innfri kravet, er det ingen garanti for at tilgangene gjenopprettes.

[30] https://en.wikipedia.org/wiki/Ransomware

Finanstilsynet viser til at skytjenester synkroniserer filer på det tidspunkt filen endres, herunder uautorisert krypteres eller skades. Tilsvarende løsninger antas benyttet for forretningsapplikasjoner og kundedata som er lagt til skyen.

I Finanstilsynets dialog med foretak rettes det en bekymring mot den økte bruken av onlineløsninger for backup, og risikoen dette utgjør for tap av både produksjonsdata og backup-data ved et angrep. Foretak er også bekymret for mulige konsekvenser av et omfattende angrep mot en skyleverandør, eller angrep mot leverandører av tjenester på stormaskin og Unix. Tap av både produksjonsdata og backup-data vil naturlig nok medføre svært alvorlige konsekvenser for den som rammes.

Finanstilsynet understreker viktigheten av at foretakene i sin backup-strategi bør ta utgangspunkt i at alle kritiske data, jf. klassifisering av informasjon og kode, må sikre foretaket mot datatap ved angrep og andre uønskede hendelser. Dette kan blant annet være segmentering mellom systemer og backup-løsningen (offline-løsninger), eller sikring av filsystemer ved at filer ikke kan overskrives før backup er gjennomført.

Videre må foretaket selv ta ansvar for regelmessig testing for å verifisere at reetablering fra backup fungerer etter intensjonen. Dette bør være en viktig del av foretakets internkontroll.

3.12. Transaksjonsovervåking (AML)

Finanstilsynet gjennomførte i 2019 flere tematilsyn med styring og kontroll av risikoen for hvitvasking og terrorfinansiering enn noe tidligere år. Vurdering av elektronisk kunde- og transaksjonsovervåkning var et av kontrollområdene ved disse tilsynene. Banker, kredittforetak og finansieringsforetak har krav til elektroniske overvåkingssystemer for å avdekke forhold som kan indikere hvitvasking og terrorfinansiering. Det gjennomføres imidlertid tilsyn utover dette der foretak benytter elektroniske systemer for å oppfylle øvrige forpliktelser i loven.

3.12.1. Kvaliteten på kunde- og transaksjonskontrollene

Finanstilsynet pekte i flere av tilsynene på at det manglet referanser mellom identifiserte risikoer og etablerte regler, og Finanstilsynet har stilt spørsmål ved om regelsettingen ivaretar risikoene tilstrekkelig. Foretakene har i mange tilfeller ikke utnyttet all funksjonaliteten som eksisterer i AML-systemet til å komponere målrettede regler. I flere tilfeller har kvaliteten på foretakets elektroniske kunde- og transaksjonsovervåkning er for lav og kan ha medført mangelfull løpende oppfølging av kunder og transaksjoner. Det har eksempelvis vært mangler i regelsettingen i systemet, herunder manglende bransjespesifikke regler, egenproduserte regler, fastsatte terskelverdier for kunder med forsterket kontroll og kundespesifikke regler. Finanstilsynet påpekte også at foretak hadde for få dedikerte regler på de enkelte forretningsområdene. Finanstilsynet har merket seg at bankene har økt analyseressursene på området, og tester bruk av systemer basert på maskinlæring og kunstig intelligens for å tilpasse reglene til kundens forventede transaksjonsmønster.

Det fremgår av foretakenes svar på spørreundersøkelsen om sårbarhet at de har utfordringer når det gjelder å få et samlet og godt datagrunnlag, og å formulere gode spørringer, for å få ut korrekte funn

når det gjelder mistenkelig transaksjoner. Det meldes om både mangelfull systemstøtte, og utfordringer når det gjelder datagrunnlaget som ligger til grunn for analysene.

3.12.2. Kvalitetssikring og oppfølging av reglene

Finanstilsynet påpekte også hvor viktig det er med testing av reglene og med rutinemessig og regelmessig evaluering av effekten av reglene. Finanstilsynet gjennomførte stikkprøvekontroller av dokumentasjonen på implementeringen av enkelte regler, og det ble påvist mangler i implementeringen. Videre er det ofte for mange regler med få treff eller med svært mange treff over tid, noe som kan indikere at reglene er lite treffsikre. Disse forholdene kan medføre at reglene ikke avdekker risiko de er ment å avdekke.

3.12.3. Driften av systemene for elektronisk kunde- og transaksjonsovervåkning

Større avvik knyttet til manglende overvåkning ble avdekket i 2019, jf. punkt 5.2. Den største risikoen for mangelfull kunde- og transaksjonsovervåkning er at kunder og transaksjoner ikke kommer med i data-uttrekkene fra kildesystemene og dermed ikke blir kontrollert. Avvik i 2019 oppsto ved endringer i kildesystemene uten tilsvarende tilpasning av uttrekket til AML-systemet. Manglende kontroller oppsto også som følge av feil etter endringer i AML-systemet. Mangler i kunde- og transaksjonsovervåkningen ble avdekket av internkontrollen i foretaket en tid etter feilen oppsto. Foretakene må forbedre akseptansetesting av systemendringer som kan påvirke AML-kontrollene, slik at feil avdekkes før produksjonsfasen.

Under tilsynene stilte Finanstilsynet også spørsmål om tilgangsstyringen av AML-systemet, og pekte på at ikke flere personer enn nødvendig skal ha tilgang på hvert autorisasjonsnivå i AML-systemet. Finanstilsynet etterspurte kontroller for å avdekke eller forhindre at ansatte bevisst eller ubevisst slår av transaksjonskontrollene i korte eller lengre perioder.

3.12.4. Transaksjonsovervåking og kundevurdering ved bruk av kunstig intelligens

Det er utfordrende for bankene å vurdere kundeadferd basert på transaksjonshistorikk og andre kundespesifikke data. I mange tilfeller er disse dataene veldig kompliserte. Finanstilsynet erfarer at maskinlæring og kunstig intelligens diskuteres for bruk innen transaksjonsovervåking, og at det er en trend internasjonalt at banker arbeider med å erstatte tradisjonelle systemene for kundevurderinger og regler for transaksjonsovervåking med systemer basert på maskinlæring og kunstig intelligens. Finanstilsynet mener utfordringene med et høyt antall falske positive treff, og utfordringer med å analysere tilstrekkelig mengde data i arbeidet med å risikoklassifisere kunder og fange opp mistenkelige aktiviteter som illegal virksomhet eller terrorfinansiering, kan reduseres ved bruk av kunstig intelligens.

3.13. Risiko knyttet til foretakets kunder

3.13.1. Påloggingsinformasjon på avveie og misbruk av BankID

Den økte digitaliseringen har medført at foretakenes kunder ofte ikke har noe valg, men må bruke digitale identifiserings- og autoriseringsløsninger for å få tilgang til tjenestene. Dette gjør spesielt kunder med lite digital erfaring sårbare, jf. punkt 3.13.6.

Passord og PIN-koder kan for enkelte være vanskelig å huske, og kunden velger å skrive ned denne informasjonen. 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 få utført finansielle tjenester. Dette utgjør en risiko for at informasjonen kommer uvedkommende i hende og at kunden blir svindlet, enten av nære relasjoner eller av andre. Svindel i nære relasjoner der midlene blir brukt til spill er et kjent scenario. Dersom uvedkommende får tilgang til en annens BankID, kan denne misbrukes på mange områder, som inngåelse av låneavtaler, kjøpekontrakter, tegning av forsikring og handel. Svindelstatistikken for andre halvår 2019 viser at tallene for svindel ved kontooverføringer der årsaken er at svindleren utsteder betalingen, er nær 42 millioner kroner. Den største andelen antas å være svindel der kunden er avlurt sine sikkerhetsmekanismer.

3.13.2. Tiltak for å redusere svindel og misbruk

For å redusere omfanget av misbruk og svindel med betalingstjenester, er det for mange av tjenestene satt beløpsgrenser av foretaket, delvis med utgangspunkt i regelverk, og/eller kunden, og det er etablert gode overvåkningsrutiner hos betalingstjenesteyterne. Når det gjelder andre tjenester, er det i liten grad etablert tilsvarende tiltak som kan bidra til redusert misbruk.

3.13.3. Sosial manipulering

Svindelstatistikken viser at også i 2019 utgjør tapene som følge av sosial manipulering den største andelen. Rapporterte tall indikerer tap på over 500 millioner kroner i 2019, mens til sammenligning var tap med betalingskort rundt 190 millioner kroner. Svindlerne er tilpasningsdyktige og utvikler svindelscenarier i tråd med det de til enhver tid antar vil høste størst gevinst. I 2019 var det store tap på direktørsvindel, fakturaer med falsk mottakerkonto og investeringsfirmaer, mens tap på kjærlighetssvindel var lavere enn året før.

Situasjonen vil ofte oppleves som svært krevende for den som rammes av sosial manipulering, og dens nærstående. Finanstilsynet er kjent med at bankene tar initiativ ovenfor kunden dersom det oppstår 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. Siden denne type svindel stadig øker, oppfordrer Finanstilsynet foretakene til å fortsette arbeidet med å finne effektive tiltak ovenfor de ulike kundegruppene.

3.13.4. **Kundegrensesnitt gjennom nye tjenestetilbydere**

Det er et økende omfang av tredjeparts tjenestetilbydere som tilbyr løsninger hvor kunden kan operere sine kundeforhold eller benytte finansielle tjenester, jf. punkt 3.7.3. Det kan for kundene være vanskelig å forstå om tjenesteyteren er underlagt finansregulatorisk regelverk og om tjenesten som benyttes forvaltes forsvarlig i tråd med regelverket eller avtaler er inngått mellom partene.

Når tjenester fra tredjeparts tjenestetilbydere benyttes, kan det være uklart for kundene hvor de skal henvende seg dersom de blir utsatt for digital kriminalitet eller hvis alvorlige hendelser medfører manglende tilgang til sine kundeforhold eller til finansielle tjenester.

Finanstilsynet mener eksisterende aktører, som blant annet banker og forsikringsselskap, og de nye aktørene sammen har et ansvar for god kundeopplysning og -informasjon og at kunder informeres om reelle forhold, og hva disse innebærer.

3.13.5. **Kommunikasjon med kunder over epost**

Finanstilsynet mottar henvendelser fra kunder som uttrykker bekymring for at banken sender informasjon på epost som kunden selv anser som sensitiv. Dette kan for eksempel være opplysninger om kundens kontantuttak eller at kontoinformasjon sendes ukryptert på e-post. Kunder er redde for at denne type opplysninger kommer på avveie, og kan utnyttes av kriminelle. Finanstilsynet forventer at foretakene opptrer aktsomt i kommunikasjonen med sine kunder, og at sikre kanaler benyttes, for eksempel kundeportal, og i tråd med personvernet.

3.13.6. **Analoge kunder**

Ifølge Pensjonistforbundet er det i dag minst 200.000 ikke-digitale eldre (analoge kunder). Pensjonistforbundet påpeker at denne gruppen er avhengig av digital hjelp fra pårørende, naboer, frivillige og venner, noe som utgjør en risiko for svindel, jf. punkt 3.13.1.

Finanstilsynet omtalte i ROS 2017 bankkunder i Norge som ikke benyttet bankenes digitale tjenester. Noen av årsakene kan være at det er krevende og at det ikke er tilstrekkelig villighet til, å tilrettelegge for enkle digitale løsninger for de eldre og andre som av ulike årsaker ikke kan benytte dagens løsninger. Dette vil kunne bli forsterket i en krisesituasjon, som nå under koronapandemien, der eldre i mindre grad kan benytte seg av de tradisjonelle betalingstjenestene som brevgiro, betaling over skranke eller uttak i minibank. Finanstilsynet anser det som foretakenes ansvar å ivareta disse kundenes behov, også når de ikke er i stand til å benytte seg av analoge banktjenester.

Finanstilsynet mener et teknologisk samarbeid mellom ulike næringer vil kunne bidra til at det etableres integrerte og enkle digitale løsninger som kan dekke analoge kunders behov. Dette kan være løsninger for bestilling av matvarer, apotekvarer, banktjenester og varslingstjenester.

3.13.7. **Identitetskontroll for analoge kunder**

Høsten 2019 fikk Finanstilsynet spørsmål fra privatpersoner og media knyttet til enkelte bankers krav om re-legitimering av enkelte kunder og publisering av et skjema for re-legitimering på bankenes nettsteder. Kravet var iverksatt for å etterkomme kravene til løpende kundeoppfølging i henhold til hvitvaskingslovens § 12. Kravet om re-legitimering gjaldt bankkunder som ikke hadde etablert BankID, men som likevel hadde tilgang til nettbank, og som hadde vanskelig for å gjennomføre et personlig fremmøte i banken. Det skapte imidlertid usikkerhet hos kundene når banken ba kundene om å sende identitetsinformasjon på en måte som er mye benyttet av svindlere, og som banken i andre sammenhenger advarer kundene mot. Finanstilsynets vurdering var at slike løsninger for re-legitimering av kundene ikke skal brukes, og at sikre kanaler må benyttes. De aktuelle bankene måtte finne andre løsninger for dokumentasjon av identitet for denne kundegruppen.

3.13.8. **Manglende tillit som følge av driftshendelser**

IKT-hendelser kan føre til at brukerne ikke får gjennomført sine finansielle tjenester som planlagt. Alvorlige IKT-hendelser kan også skape uro. Finanstilsynet blir jevnlig kontaktet av kunder som er bekymret for sikkerheten omkring bruken av tjenestene og informasjon om deres kundeforhold, manglende tillit til tjenesteyter og usikkerhet om riktigheten av informasjonen som fremkommer. Flere av hendelsene i 2019, jf. punkt 5.2, viser tilfeller der kundene ikke har kunnet bruke tjenesten som planlagt eller ikke har kunnet stole på riktigheten av informasjonen.

3.13.9. **Foretakenes integritet som følge av digital kriminalitet**

Digital kriminalitet eller alvorlige IKT-hendelser kan skape usikkerhet hos brukere av finansielle tjenester. Finanstilsynet har blitt kontaktet av kunder som er bekymret for tap av egne midler ved slike hendelser. Finanstilsynet kjent med at kunder i slike situasjoner har gjort vesentlige uttak av kontanter eller har ønsket å flytte midler til andre valutaer enn norske kroner. Dette er en bekymring som foretakene må ta på alvor.

4. Svindel og svindelstatistikk

4.1. Ny rapportering av svindelstatistikk

Rapporteringen av tap som følge av svindel med betalingstjenester ble lagt om fra og med andre halvår 2019. For første halvår 2019 ble det rapportert til Bits AS[31] på samme format som tidligere år. Fra og med andre halvår 2019 rapporteres det til Finanstilsynet i henhold til det reviderte betalingstjeneste-direktivet (PSD 2)[32]. Tallene for andre halvår er dermed ikke direkte sammenlignbare med rapporterte tall for tidligere perioder.

I henhold til forskrift om systemer for betalingstjenester § 2, skal banker, kredittinstitusjoner, e-pengeforetak, betalingsforetak og filialer av slike foretak med hovedsete i annen EØS-stat levere svindelstatistikk til Finanstilsynet minimum én gang i året. Finanstilsynet har besluttet at foretakenes rapportering om svindel skal skje halvårlig. Det er en videreføring av tidligere praksis med halvårlig rapportering av svindel til Bits.

PSD 2s retningslinjer for svindelrapportering omfatter krav til rapportering av svindelstatistikk fra betalingstjenestetilbyderne til nasjonale myndigheter og rapportering av aggregerte data fra nasjonale myndigheter til EBA og ECB. Rapporteringen er mer omfattende enn tidligere rapportering og har vært utfordrende for foretakene å implementere.

Foretakene skal rapportere både det totale volumet av transaksjoner og svindeltransaksjoner. Det gjør det mulig å angi svindel som andel av det totale transaksjonsvolumet. Det skal rapporteres både verdi av transaksjonene og antall transaksjoner. Rapporteringen skiller også mellom transaksjoner innenlands, grensekryssende transaksjoner innenfor EØS og grensekryssende transaksjoner utenfor EØS. Videre deles svindeltransaksjonene i tre kategorier; etter om svindleren utsteder betalingen, endrer/modifiserer betalingen, eller manipulerer betaleren til selv å utstede betalingen.

4.2. Tap knyttet til misbruk av betalingskort

Rapporterte tap på kortsvindel utgjorde i underkant av 95 millioner kroner i både første og andre halvår 2019. Til sammen er det en økning på 28 prosent fra 2018. Sammenligningen med tidligere år, samt mellom første og andre halvår, er usikker som følge av at rapporteringen ble lagt om fra andre halvår 2019. Tallene viser samlede tap for betalingskort mot norske kunder de siste årene, uavhengig av om tapet dekkes av kunden selv, banken eller kortselskapet.

Tallene for første halvår 2019 viser en økning i tap knyttet til misbruk av betalingskort sammenlignet med tidligere år. Det var særlig misbruk av kortinformasjon ved internetthandel som økte, og dette

[31] Bank- og finansnæringens infrastrukturselskap (Bits AS) www.bits.no
[32] Artikkel 96 nr. 6, med tilhørende retningslinjer for svindelrapportering: https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2

misbruket sto også for de største tapene i første halvår 2019, se tabell 4.1. Tallene for første halvår 2019 indikerer en økning i antall betalingskort utsatt for misbruk, se tabell 4.2.

Tabell 4.1 Tap ved misbruk av betalingskort

Svindeltype betalingskort (beløp i hele tusen kroner)	2015	2016	2017	2018	*1. halvår 2019*
Misbruk av kortinformasjon, Card-Not-Present (CNP) (Internett-handel m.m.)	98.410	137.015	102.908	114.932	*76.546*
Stjålet kortinformasjon (inkludert skimming[33]):					
- Misbruk med falske kort i Norge	2.670	1.360	483	3.304	*1.298*
- Misbruk med falske kort utenfor Norge	48.447	41.762	17.452	11.203	*2.613*
Originalkort tapt eller stjålet:					
- Misbruk med PIN i Norge	18.875	12.857	10.194	9.676	*9.146*
- Misbruk med PIN utenfor Norge	14.224	10.223	9.663	7.696	*3.327*
- Misbruk uten PIN	6.033	3.286	4.891	1.921	*1.536*
Totalt	**188.659**	**206.503**	**145.591**	**148.732**	***94.466***

Kilder: Finanstilsynet og Bits AS

Tabell 4.2 Antall betalingskort utsatt for misbruk

	2015	**2016**	**2017**	**2018**	***1. halvår 2019***
Antall kort rammet av misbruk	44.900	68.162	65.024	60.266	*39.918*

Kilder: Finanstilsynet og Bits AS

For andre halvår 2019 er det rapportert svindel med betalingskort for i underkant av 95 millioner kroner. Det tilsvarer 0,02 prosent av total transaksjonsverdi for betalinger med betalingskort i denne perioden. Andelen svindel er størst for fjernbetaling uten sterk kundeautentisering, en kategori som i hovedsak omfatter handel på internett. Her utgjorde svindel 0,09 prosent av transaksjonsverdien.

[33] Wikipedia: Skimming (fraud)

Tabell 4.3 Transaksjoner og svindeltransaksjoner med betalingskort rapportert av kortutsteder 2. halvår 2019

Transaksjonsverdi i hele tusen NOK	Transaksjoner i Norge	Grensekryssende transaksjoner i EØS	Grensekryssende transaksjoner utenfor EØS	Totale transaksjoner
Kortbetalinger (utsteder)				
Totalt	414.632.690	103.472.005	12.385.305	530.490.001
Hvorav svindel	7.091	67.236	20.354	94.681
Hvorav initiert elektronisk:				
Svindleren utsteder betalingen, hvorav	8.447	48.593	15.855	72.896
- Tapt eller stjålet kort	2.091	3.831	915	6.837
- Ikke mottatt kort	1.122	961	327	2.410
- Forfalsket kort	69	451	1.034	1.554
- Tyveri av kortdetaljer	2.411	36.383	12.127	50.921
- Annet	2.650	6.953	1.453	11.056
Svindleren endrer eller modifiserer betalingsordre	22	549	1.668	2.239
Svindleren manipulerer betaleren til en kortbetaling	49	6.886	393	7.328
Fjernbetaling uten sterk kundeautentisering				
Totalt	23.266.936	28.853.569	3.275.446	55.395.951
Hvorav svindel	2.500	34.749	12.033	49.282

Kilde: Finanstilsynet

Det ble rapportert ca. 40 000 kort rammet av misbruk i første halvår og ca. 110 000 svindeltransaksjoner med kort i andre halvår 2019. "Økningen" må ses i sammenheng med at det etter retningslinjene nå skal rapporteres antall svindeltransaksjoner og ikke bare antall misbrukte kort.

Av totalt antall transaksjoner med betalingskort andre halvår 2019 er 0,007 prosent av transaksjonene svindel. Gjennomsnittsverdien av en svindeltransaksjon med betalingskort er 856 kroner, mens gjennomsnittverdien av en transaksjon med betalingskort er 327 kroner.

Tabell 4.4 Antall transaksjoner og svindeltransaksjoner med betalingskort rapportert av kortutsteder 2. halvår 2019

Antall	Transaksjoner i Norge	Grensekryssende i EØS	Grensekryssende utenfor EØS	Totalt	Svindel (prosent)
Totalt	1.339.988.557	259.784.056	18.990.578	1.618.763.191	
Svindel	10.796	69.702	30.082	110.580	0,007

Kilde: Finanstilsynet

4.3. Tap knyttet til nettbanksvindel

Tap ved bruk av nettbank utgjorde 3,6 millioner kroner i første halvår 2019, som er lavt sammenlignet med tidligere år. Rapporteringen for andre halvår er vesentlig høyere, med tap knyttet til kontooverføringer på over 300 millioner kroner.

Rapporteringene for første og andre halvår er, som nevnt, ikke direkte sammenlignbare. Først og fremst skyldes dette at tallene for andre halvår omfatter tap som følge av sosial manipulering, noe bankene tidligere rapporterte i en separat rapportering. Fratrukket tap grunnet sosial manipulering, er tapstallene på kontooverføringer for andre halvår rundt 46,5 millioner kroner. Mens det tidligere kun var bankene som rapporterte tapstall, omfatter rapporteringen nå alle foretak som yter betalingstjenester. Rapporteringen på kontooverføringer omfatter dessuten både nettbank, mobilbank og andre plattformer. Tallene viser samlede tap for nettbanksvindel mot norske kunder for de siste årene, uavhengig av om tapet dekkes av kunden selv eller banken.

Tabell 4.5 Tap ved bruk av nettbank (beløp i hele tusen kroner)

Svindeltype – nettbank (beløp i hele tusen kroner)	2015	2016	2017	2018	*1. halvår 2019*
Angrep ved bruk av ondartet programkode på kundens PC eller sikkerhetsmekanisme	3.055	2	727	1.252	201
Tapt/stjålet sikkerhetsmekanisme	963	8.758	1.892	1.959	69
Phishing og falske BankID-brukersteder	5.815	2.428	2.057	16.858	1.435
Annet/ukjent	2.715	7.444	2.911	6.723	1.932
Totalt	**12.548**	**18.632**	**7.587**	**26.840**	**3.637**

Kilder: Finanstilsynet og Bits

Tabell 4.6 Transaksjoner og svindeltransaksjoner for kontooverføringer (nettbank m.m.) 2. halvår 2019

Kontooverføringer initiert elektronisk (beløp i hele 1000 kroner)	Transaksjoner i Norge	Grensekryss-ende i EØS	Grensekryss-ende utenfor EØS	Totalt	Svindel-prosent
Totalt	188.219.191.694	25.188.476.543	5.978.582.637	219.386.250.875	
Svindel	41.716	130.886	129.027	301.629	0,00014
Hvorav ulike typer svindler:					
- Svindleren utsteder betalingen	21.297	9.700	10.876	41.873	
- Svindleren endrer eller modifiserer betalingsordren	475	4.069	0	4.544	
- Svindleren manipulerer betaleren til å utstede betalingsordren	19.944	117.944	118.151	256.039	

Kilde: Finanstilsynet

4.4. Tap ved svindel gjennom sosial manipulering

Svindel gjennom sosial manipulering, dvs. at svindleren manipulerer betaleren til å gjennomføre en transaksjon, økte ytterligere i 2019. Rapporterte tall indikerer tap på over 500 millioner kroner, mot i underkant av 300 millioner kroner i 2018. Svindel gjennom sosial manipulering synes å være en lønnsom metode for kriminelle. Tapene er omtrent like store for grensekryssende transaksjoner innenfor og utenfor EØS, men vesentlig lavere for innenlandske transaksjoner. Tap som følge av sosial manipulering skjer først og fremst ved kontooverføringer (nettbank m.m.).

Tall for svindel gjennom sosial manipulering er særlig usikre, fordi betaleren selv bærer tapet og mange svindler av denne typen trolig ikke blir meldt til banken. De faktiske tapene er antakelig vesentlig større enn rapportert. Kundene som er svindlet kontakter ofte banken for å få stanset transaksjoner og for å få tilbakeført beløpet. Banker varsler også kunder der banken, basert på kunnskap om kunden, identifiserer gjentagende unormale transaksjoner for kunden.

Rapporteringen i henhold til retningslinjene differensierer ikke mellom ulike typer av sosial manipulering. Finanstilsynet vurderer at nedbrytingen i underkategorier av manipulering av brukeren, slik dette har blitt presentert i ROS-analysene for 2017 og 2018, gir viktig informasjon for å forstå svindelbildet. Finanstilsynet ba derfor større banker og bankgrupperinger rapportere dette separat for 2019. Den prosentvise fordelingen av underkategorier av sosial manipulering rapportert fra disse foretakene, antas å gi et tilnærmet riktig bilde av fordelingen for alle foretak og fremgår av tabellen nedenfor. I 2019 er det størst tap på direktørsvindel og svindel med endring av mottakerkonto, mens det i 2018 var mest tap ved kjærlighetssvindel og investeringer i falske selskaper.

Tabell 4.7 Tap ved manipulering av betaleren fordelt prosentvis på underkategorier

	2018	2019
Betaling for å leie et objekt mottager av pengene ikke eier	0,3 %	0,2 %
Innskudd etter løfter om store utbetalinger senere	3,1 %	2,4 %
Kjærlighet	29,7 %	8,7 %
Investeringer i falske selskaper	31,0 %	19,8 %
Betaling for varer som ikke leveres	4,0 %	0,8 %
Endret mottakerkonto	2,9 %	22,7 %
Direktørsvindel	11,4 %	37,6 %
Falsk faktura	11,1 %	4,1 %
Andre/nye typer	6,6 %	3,7 %

Kilder: Finanstilsynet og Bits

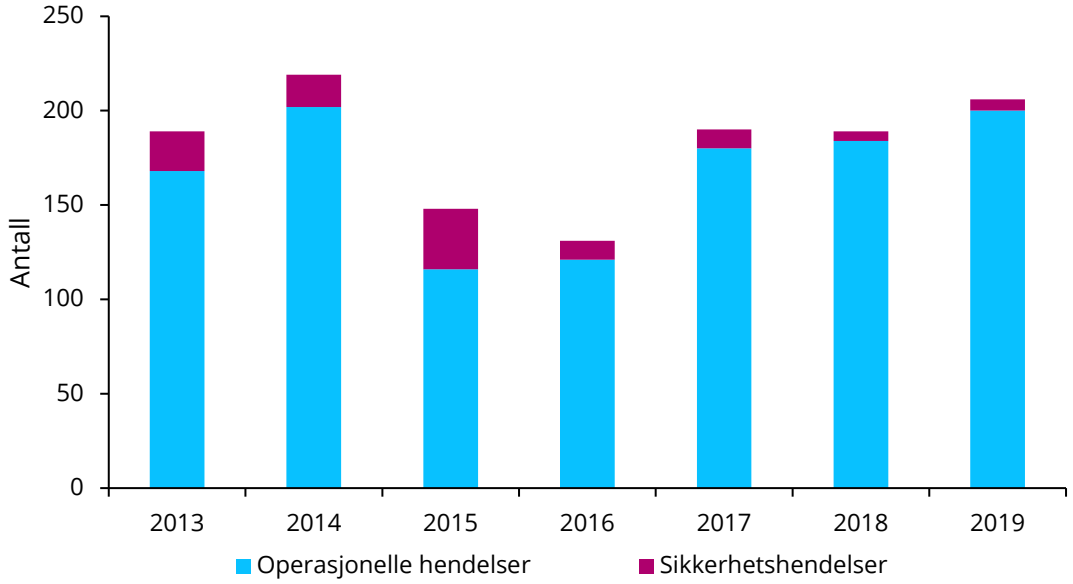
5. Rapporterte hendelser i 2019

5.1. Statistikk over hendelser

I 2019 rapporterte foretakene om 206 IKT-hendelser til Finanstilsynet, som er 17 flere enn året før. Antall rapporteringspliktige foretak økte fra 2018 til 2019, og ved flere av hendelsene mottok Finanstilsynet rapporter fra flere verdipapirforetak eller banker om samme hendelse hos foretakenes felles leverandør

Det var i 2019 ikke hendelser av lengre varighet som rammet tilgjengeligheten til betalingstjenestene til mange banker samtidig. Finanstilsynet vurderer tilgjengeligheten til betalingstjenestene og kunderettede løsninger som noe bedre i 2019 enn i 2018.

Figur 5.1 Rapporterte hendelser fordelt på operasjonelle hendelser og sikkerhetshendelser



Kilde: Finanstilsynet

Sammenliknet med tidligere år, mottok Finanstilsynet i 2019 flere rapporter om hendelser som berørte andre forhold enn tilgjengelighet. Blant annet økte antallet rapporter om hendelser og/eller avvik i systemene for elektronisk kunde- og transaksjonsovervåking.

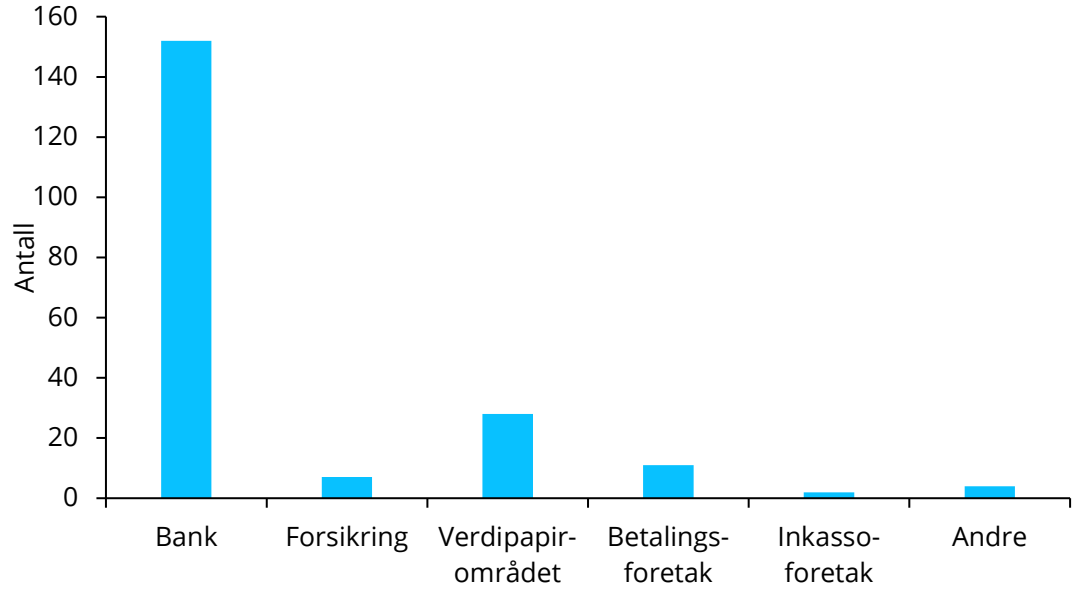
Figur 5.2 viser at bankene sto for 75 prosent av de rapporterte hendelsene i 2019.

Tabell 5.1 Antall rapporterte hendelser

Årstall	Operasjonelle hendelser	Sikkerhets-hendelser	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
2019	200	6	206

Kilde: Finanstilsynet

Figur 5.2 Rapporterte hendelser i 2019 fordelt på type foretak



Kilde: Finanstilsynet

5.2. Hendelser med spesielt alvorlige konsekvenser

Nettverksproblem i Gjensidige Forsikring AS

Gjensidige ble rammet av et alvorlig nettverksproblem fredag 8. og lørdag 9. mars 2019. Fra fredag morgen kl. 07:00 til kl. 02:30 natt til lørdag var det ikke mulig å komme inn på nettstedet, verken nettsidene til banken eller forsikringsselskapet. Intranettet var også utilgjengelig. Hendelsen viste seg å ha oppstått som følge av oppgradering av en sikkerhetsløsning, men fikk konsekvenser først flere dager etter selve oppgraderingen.

Vipps 17. mai

Midt i den travleste perioden på 17. mai sluttet Vipps å fungere for betalinger fra person til bedrift, slik at brukere ikke fikk betalt for brus, pølser og is. Problemet varte i ca. én time. Vipps hadde økt

kapasiteten for å ta høyde for forventet økt bruk på 17. mai. Det manglet imidlertid nødvendig kapasitetsøkning på en komponent som Vipps ikke var klar over hadde betydning for kapasiteten i betalingsløsningen.

Doble VISA-trekk

22. og 23. mai 2019 hadde DNB problemer med VISA-kort-reservasjoner. Reservasjonene ble ikke slettet når kapitaltransaksjonene ble bokført. Berørte kunder opplevde dobbelt beløpstrekk, og en del kunder fikk negativ saldo på konto. Banken brukte lenger tid enn forventet på å rydde opp i og slette reservasjonene. Først på ettermiddagen 23. mai ble det verifisert at alle kontoene var oppdatert med korrekt saldo. Feilen avdekket svakheter i bankens endringshåndtering og testing.

Feil implementering av eFaktura-tjeneste

I juli 2019 mottok Finanstilsynet hendelsesrapport fra Vipps og henvendelser fra sluttbrukere om at eFakturaer ble delt med andre personer enn personen som sto som mottaker på fakturaen, samt at rette mottaker av eFakturaen ikke hadde mottatt den. Problemet knyttet til bankenes tjenestetilbud "Ja Takk Til Alle eFakturaer" ble spesielt synlig da Vipps introduserte funksjonaliteten "regningsbetaling" i Vipps-applikasjonen med samtidig valg for "Alltid Vipps eFaktura".

Det skal være mulig å inngå eFaktura-avtale på vegne av en annen person for fakturaer fra en spesifikk utsteder, såkalt "Ja Takk Til Bestemte (JTTB)", men alternativet skal ikke være mulig med valget "Ja Takk Til Alle". Enkelte banker hadde imidlertid implementert "Ja Takk Til Alle" på feil måte. Konsekvensen ble at kunder som hadde betalt én enkelt papirfaktura på vegne av en annen person, også mottok senere faktura fra denne utstederen som eFaktura til seg, istedenfor at den ble sendt til den fakturaen var adressert til. Det er Bits AS som fastsetter bankenes felles regler for eFaktura. Finanstilsynet har fulgt opp Bits, som har iverksatt tiltak og oppfølging både ovenfor bankene og fakturautstederne.

Hendelser knyttet til bankenes elektroniske kunde- og transaksjonsovervåknings-systemer for å avdekke hvitvasking og terrorfinansiering (AML-systemer)

Det ble i 2019 rapportert flere hendelser knyttet til avvik i bankenes AML-systemer enn noe tidligere år. Dette kan ha sammenheng med at oppmerksomheten på området har økt de siste årene. Rapporterte hendelser i 2019 gjaldt feil i uttrekket fra bankenes kildesystemer til AML-systemet, feil etter endringer i selve AML-systemet og driftsfeil. Konsekvensene var mangelfulle AML-kontroller av kunder og transaksjoner. Noen av de rapporterte hendelsene skyldtes feil som hadde eksistert i flere år og har medført store avvik i kunde- og transaksjonskontrollene.

BankID-hendelser

Også i 2019 mottok Finanstilsynet mange rapporter om ulike problemer med BankID. Problemene oppstår særlig når særlig mange benytter BankID samtidig, for eksempel på datoene for publisering av skatteoppgjøret og for tilbakebetaling av skatt. BankID er en sammensatt tjeneste. Finanstilsynet observerer at det er mange ulike årsaker til hendelser der hele eller deler av BankID-tjenesten ikke

fungerer. Av de rapporterte hendelsene i 2019, var avbruddet på datoen for publisering av skatteoppgjøret 20. juni det alvorligste.

Sikkerhetshendelser

Finanstilsynet observerer at foretakenes forsvarsverk er styrket, slik at angrep i større grad avverges før de får konsekvenser. Kun seks rapporterte hendelser i 2019 var sikkerhetshendelser. Sikkerhetshendelsene gjaldt angrep med kryptovirus som krypterte filer og gjorde deler av foretakets IT-systemer utilgjengelige, phishing med forsøk på uthenting av informasjon, uautorisert uthenting av foretaksinformasjon fra innsiden av foretaket og angrep for å hindre tilgang til tjenester (DDoS-angrep).

Rapporterte sårbarheter

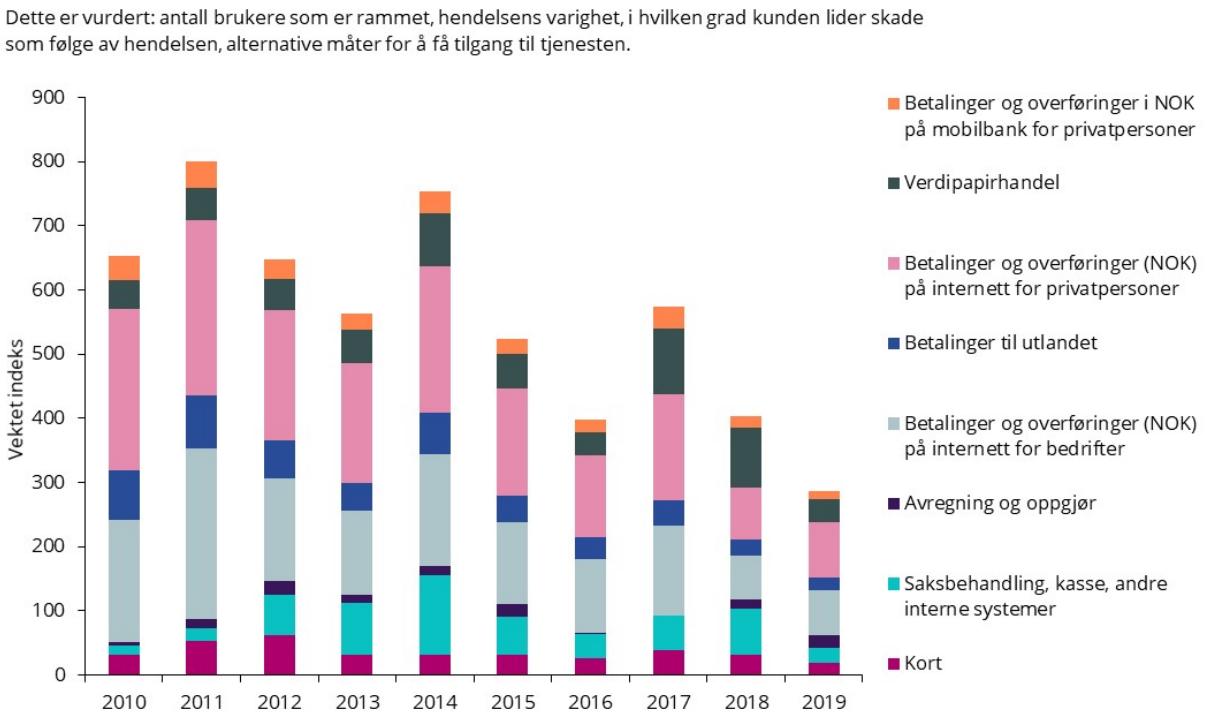
Finanstilsynet blir gjennom hendelsesrapporter og tilsyn kjent med sårbarheter foretakene avdekker, uten at sårbarhetene nødvendigvis blir utnyttet. Rapporter Finanstilsynet har mottatt, understreker viktigheten av at foretakene videreutvikler verktøystøtte og rutiner for raskt å oppdage, varsle og håndtere nylig avdekkede kritiske sårbarheter, og regelmessig gjennomgår og kontrollerer status på sikkerhetsoppdateringer for å avdekke manglende oppdateringer. Tiltakene gjelder for alle plattformer og for eksponering både mot internt nett og mot internett. Streng kontroll med administrasjons-rettighetene reduserer risikoen for uautoriserte oppdateringer.

5.3. Analyse av hendelsene som mål på tilgjengelighet

De rapporterte hendelsene har ulik alvorlighetsgrad. For hendelser som har medført redusert tilgjengelighet, har Finanstilsynet vurdert avbruddets lengde, antall foretak som er berørt, 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). Hendelsene vektes ut fra antall berørte brukere, varighet på hendelsen, tidspunkt og tilgangen til erstatningstjenester. Funnene sammenstilles i en tidsserie, slik at Finanstilsynet kan følge utviklingen over tid.

Figur 5.3 viser at betalingstjenestene og kunderettede løsninger var mer tilgjengelige for kundene i 2019 enn i 2018 og tidligere år. Skalaen på y-aksen er en indeks som er basert på vektingen av hver enkelt hendelse. Lavere indeksverdi angir mindre forekomst av driftsavbrudd med konsekvenser for brukerne.

Figur 5.3 "Tjenesten ikke tilgjengelig" – hendelser veiet med konsekvens



Kilde: Finanstilsynet

6. Meldinger fra foretakene

6.1. Melding om utkontraktering

Finanstilsynet mottok 135 meldinger om utkontraktering av IKT-virksomhet i 2019. I tillegg vurderte Finanstilsynet avtaler om utkontraktering av IKT-virksomhet ved behandling av konsesjonssøknader. Som i 2018, var tendensen i 2019 økt bruk av skytjenester både for applikasjons- og infrastrukturtjenester.

Meldingene om utkontraktering har over tid blitt mer omfattende og kompleksiteten i utkontrakteringsforholdene har økt. Finanstilsynet ser imidlertid en forbedring i foretakenes håndtering av utkontrakteringsavtaler. Det gjelder både innholdet i foretakenes risikoanalyser knyttet til utkontraktert virksomhet, styrebehandling av utkontrakteringsavtaler og foretakenes risikovurderinger, og kvaliteten på avtalene med foretakets leverandører av IKT-tjenester.

Foretakene er selv ansvarlige for at IKT-virksomheten, inkludert tjenester som er utkontraktert, oppfyller alle krav som stilles i IKT-forskriften, jf. forskriften §12. I tillegg kan også annen sektorlovgivning inneholde detaljerte regler om utkontraktering. Foretakene må etablere leverandøravtaler som tilfredsstiller lover og regler, og påse at leverandør og eventuelle underleverandører leverer IKT-tjenester i tråd med disse kravene. Finanstilsynet får innsyn i foretakenes utkontrakteringsavtaler ved behandling av mottatte meldinger om utkontraktering, jf. finansforetaksloven § 4 c, i forbindelse med konsesjonsbehandling, og gjennom tilsyn.

6.2. Melding om systemer for betalingstjenester

I 2019 behandlet Finanstilsynet 21 meldinger fra foretak under tilsyn om endrede eller nye betalingstjenester. Sentrale punkter som vurderes er blant annet om det er utført risikovurderinger, om det foreligger beskrivelse av sikkerhetsmekanismer, om det er gjennomført stress- og ende-til-ende tester og om det er etablert kriseberedskap og plan for gjenoppretting. Enkelte av meldingene ble fulgt opp. Samarbeid mellom banker om betalingsløsninger og nye mobilløsninger for betaling var temaer som gikk igjen.

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. Meldeplikten utløses ved innføring av nytt system for betalingstjeneste, ny versjon som vesentlig påvirker andre berørte parter som inngår i betalingstjenesten, og ny versjon med endret eller ny funksjonalitet som er vesentlig for systemet for betalingstjenesten.

6.3. Reautorisering og konsesjon til å yte betalingstjenester

Den offentligrettslige delen av EUs reviderte betalingstjenestedirektiv (PSD 2) ble innført i Norge 1. april 2019. De nye lovbestemmelsene gir konsesjonsplikt for to nye betalingstjenester omtalt som fullmakttjenester, hhv. betalingsfullmakttjenester og kontoinformasjonstjenester.

Forskrift om endring i forskrift om finansforetak og finanskonsern punkt IV, fastsatte overgangsbestemmelser (krav om reautorisering) for e-pengeforetak, betalingsforetak med ordinær tillatelse, betalingsforetak med begrenset tillatelse, samt foretak som kunne dokumentere at det før forskriftens ikrafttredelse tilbød betalingsfullmaktstjenester og/eller kontoinformasjonstjenester.

Det nye regelverket (finansforetaksforskriftens § 3-2) stiller strenge krav til at foretakene har godt dokumenterte rutiner på områder relatert til IKT- og betalingstjenester. Foretak som per 1. april 2019 hadde konsesjon som betalingsforetak og/eller e-pengeforetak, måtte innen 1. september 2019 dokumentere at de oppfylte de nye kravene. Finanstilsynet mottok 20 søknader om reautorisering. I tillegg mottok Finanstilsynet ti søknader om konsesjon til å yte betalingstjenester. Søknadene viste at flere av foretakene hadde på plass gode rutiner for IKT- og betalingstjenesterer, men også at flere foretak hadde manglende forståelse av regelverket og behov for å vesentlig forbedre sine rutiner. Funnene viste viktigheten av kravene for å bidra til å redusere risikoen knyttet til ytere av betalingstjenester.

14. september 2019 trådte regler i samsvar med delegert kommisjonsforordning (EU) 2018/389 i kraft i Norge. Reglene omfatter krav om at betalingskontotilbydere (banker) skal gi betalingsforetak som yter betalingsfullmakttjeneste og/eller kontoinformasjonstjeneste tilgang til samme kontoinformasjon som kontoinnehaver selv har tilgang til gjennom bankens kundegrensesnitt. Bankene er forpliktet til å gjøre minst ett grensesnitt for tilgang til betalingskontoinformasjon tilgjengelig for fullmaktsforetak. I henhold til kommisjonsforordningen, kan banker som har valgt å utvikle dedikert grensesnitt for tilgang til betalingskontoinformasjon, på visse vilkår, søke om fritak fra kravet om å ha en reserveløsning. Finanstilsynet mottok 111 søknader fra banker om fritak fra kravet om reserveløsning. En rekke banker har ved utgangen av april 2020 fortsatt ikke oppfylt vilkårene for fritak.

PSD 2 definerer sikkerhetskrav som skal beskytte kundedata, slå fast brukerens identitet og redusere risikoen for svindel, såkalt sterk kundeautentisering (SKA). Disse reglene ble innført i Norge både ved forskrift om systemer for betalingstjenester og gjennom reglene som gjennomfører delegert kommisjonsforordning (EU) 2018/389 i Norge. Kravet til sterk kundeautentisering trådte i kraft i EØS-området 14. september 2019.

På bakgrunn av en rekke henvendelser til EBA og nasjonale tilsynsmyndigheter om hvilke autentiseringsmetoder som ble vurdert å være i samsvar med reglene for SKA, ble dette i juni 2019 presisert i en uttalelse fra den europeiske banktilsynsmyndigheten (EBA). For å unngå negative konsekvenser for brukere som betaler med kort når de handler på nett, ble det åpnet for at nasjonale tilsynsmyndigheter kan gi utstedere og innløsere av kort og foretak som driver netthandel utsatt frist for å etablere sikker kundeautentisering (SKA) ved bruk av betalingskort ved netthandel. Nær alle

banker og betalingsforetak har søkt Finanstilsynet om utsatt frist. EBA besluttet i oktober 2019 at utstedere og innløsere av kort og foretak som driver netthandel skal ha ferdigstilt, testet og iverksatt SKA innen 31. desember 2020. Finanstilsynet vil følge opp fremdriften i foretakene.

6.4. Risikorapportering for betalingstjenestetilbydere

Ny forskrift om systemer for betalingstjenester, som trådte i kraft 1. april 2019, stiller i § 2 krav om at betalingstjenestetilbydere[34] årlig skal rapportere til Finanstilsynet en samlet vurdering av operasjonell risiko og sikkerhetsrisiko knyttet til tilbyderens betalingstjenester og en vurdering av om tilbyderens tiltak er tilstrekkelige.

For denne innrapporteringen har Finanstilsynet under utarbeidelse et eget skjema, som er basert på skjemaet som Finanstilsynets benytter i forbindelse med den årlige spørreundersøkelse om sårbarhet, se vedlegg 1. Utkast til skjema, sammen med en oversikt som viser sammenhengen mellom spørsmålene i skjemaet og kontrollmålene i COBIT, er publisert[35] på Finanstilsynet nettsted.

Frist for første innrapportering var satt til 30. juni 2020. Grunnet utfordringene foretakene må håndtere som følge av koronakrisen har Finanstilsynet utsatt fristen.

[34] Banker, kredittinstitusjoner, e-pengeforetak, betalingsforetak, opplysningsfullmektiger og filialer av slike foretak med hovedsete i annen EØS-stat. Betalingsforetak med begrenset tillatelse, jf. finansforetaksloven § 2-10, fjerde ledd, er særskilt unntatt fra forskriftens virkeområde.
[35] PSD2 – Årlig rapportering av risikovurderinger knyttet til foretakenes betalingstjenester

Vedlegg

1 – Foretakenes svar på spørreundersøkelse om sårbarhet

Finanstilsynet gjennomførte i desember 2019 sin årlige spørreundersøkelse om sårbarhet. Finanstilsynet ba foretakene vurdere sin sårbarhet for trusler. I alt besvarte 16 foretak undersøkelsen. Resultatene framgår av tabellene nedenfor.

Foretakenes svar er angitt med fargekoder. Grønt gir uttrykk for lav sårbarhet, gult innebærer middels sårbarhet og rødt uttrykker høy sårbarhet. Ingen farge innebærer at foretak ikke har svart.

Foretakene ble også bedt om å vurdere sårbarhetene framover, dvs. om sårbarhetene anses å være økende, stabile eller minkende. Trenden kommer til uttrykk i kolonnen lengst til høyre i tabellene og er et gjennomsnitt 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). For hvert spørsmål er det beregnet et aritmetisk gjennomsnitt av foretakenes svar.

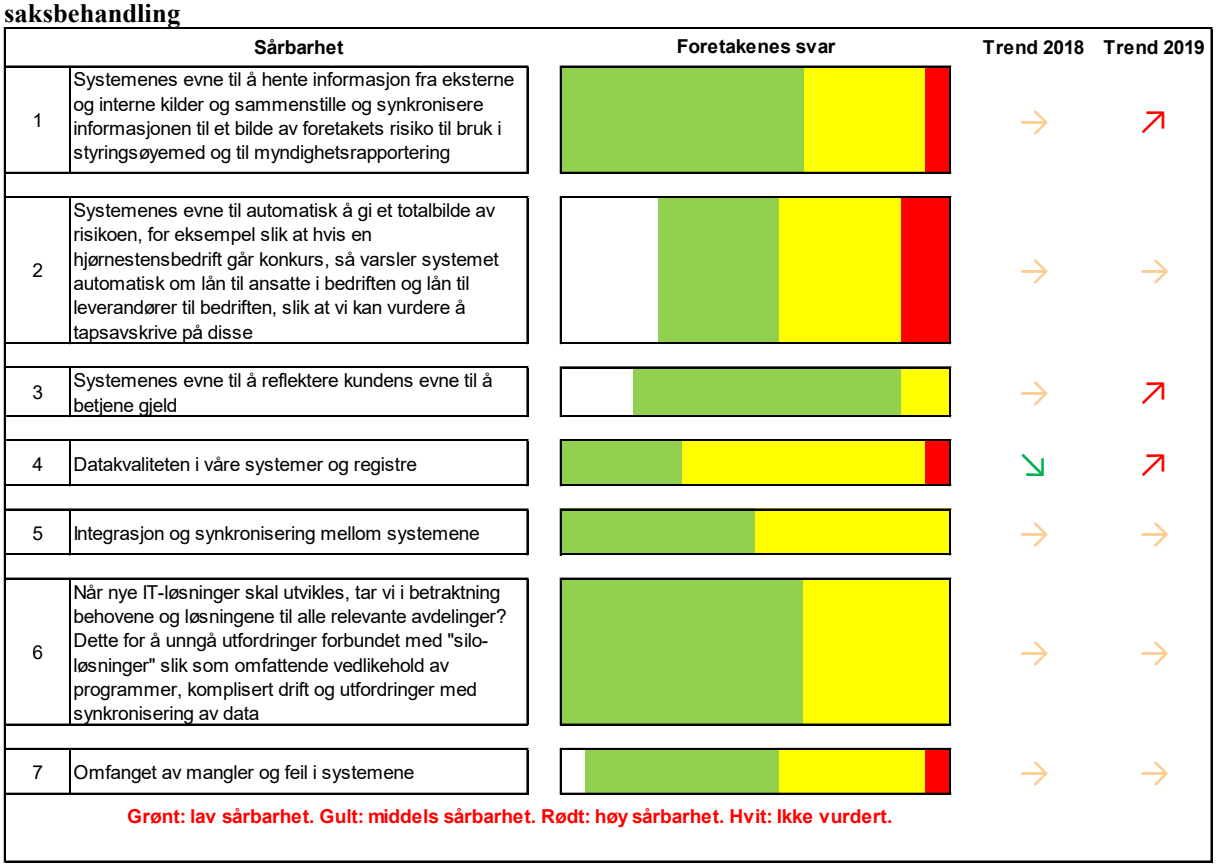
Styring og kontroll

	Sårbarhet	Foretakenes svar	Trend 2018	Trend 2019
1	Vi etterlever prinsippet om 3 Lines of Defence.		I/A	→
2	Vi har en godt innarbeidet prosess for risikoanalyse. Ansatte er kjent med prosessen og bidrar aktivt og løpende inn i den.		I/A	→
3	Informasjon som grunnlag for å vurdere risiko samler vi inn systematisk og løpende. Informasjonen kan være analyser av avvik og hendelser, informasjon fra eksterne kilder, resultat av penetrasjonstesting, observasjoner fra kunder og ansatte.		I/A	↗
4	Vi gjør tester for å teste sikkerheten i tjenestene våre. (Eks. penetration-testing, testing etter TIBER standarden, sårbarhetsscanning).		I/A	→
5	Det utføres sikkerhetstesting av personer som ikke har vært involvert i utviklingen av tjenesten som testes.		I/A	→

Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert.

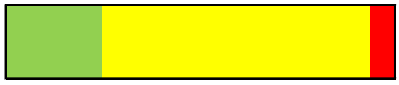
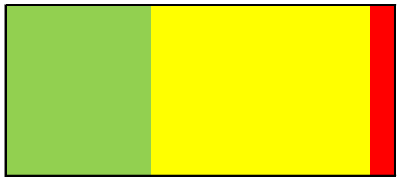
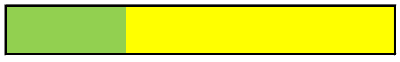
Foretakene melder om stadig økende kompleksitet i systemporteføljen. Dette gjør at arbeidet med risikoanalyser blir mer krevende og omfattende.

IT-systemene fungerer ikke tilfredsstillende som støtte for beslutninger, kundebehandling eller saksbehandling



Foretakene synes å anta at grunnlaget fra IT-systemene fremover vil være beheftet med større grad av usikkerhet, når de skal ta beslutninger. Jf. blant annet at datakvaliteten vurderes å være dårligere enn i 2018 og at foretakene anser at dette kan bli et økende problem fremover. Det kan synes som IT-systemene i mindre grad enn tidligere, grunnet blant annet nye krav, gir tilstrekkelig og nødvendig forretningsstøtte. Dette gjelder systemenes evne til å gi et totalbilde av foretakets eksponering mot bransjer og kunder.

Drift

	Sårbarhet	Foretakenes svar	Trend 2018	Trend 2019
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	Vår evne til å avdekke "tikkende miner", dvs. komponenter som gradvis slites, eller verdier som gradvis når nivåer som krever inngrep, for eksempel minnelekkasje, sertifikater som går ut på dato, elektroniske komponenter som slites, energiforsyning som "slites" (batterier, brennstoff til nødstrøm-aggregat)		→	→
9	Vår evne til å avdekke avvik (unormal belastning, unormale porter/protokoller, avvikende svartider) i datatrafikken og ta aksjon før skade		→	→
10	Vår beskyttelse mot dataangrep (Advanced persistence threat, trojaner, ransomware, DDoS)		→	→
11	Kvaliteten på kontinuitets- og katastrofeløsningene våre, jf. IKT-forskiften § 11		→	→
12	Samarbeidsrutiner med leverandører		→	→
13	Leveransepresset vi er utsatt for i markedet gjør kvaliteten i løsningene ikke alltid er god nok		↗	→
14	Tilgang på kompetanse, herunder kompetanse til å stille krav til leverandører og følge opp leveransene		→	↘
15	Omfanget av endringer		↗	→
16	Nye regulatoriske krav som gjør at vi må endre systemene våre		↗	↘
17	Vår kunnskap om hvor datalinjene går og redundans når det gjelder datalinjer		→	→
18	Tilgangskontroll, adgangskontroll og dual kontroll		→	→
19	Medarbeideres årvåkenhet når det gjelder trusler og angrep. Opplæring.		→	↗

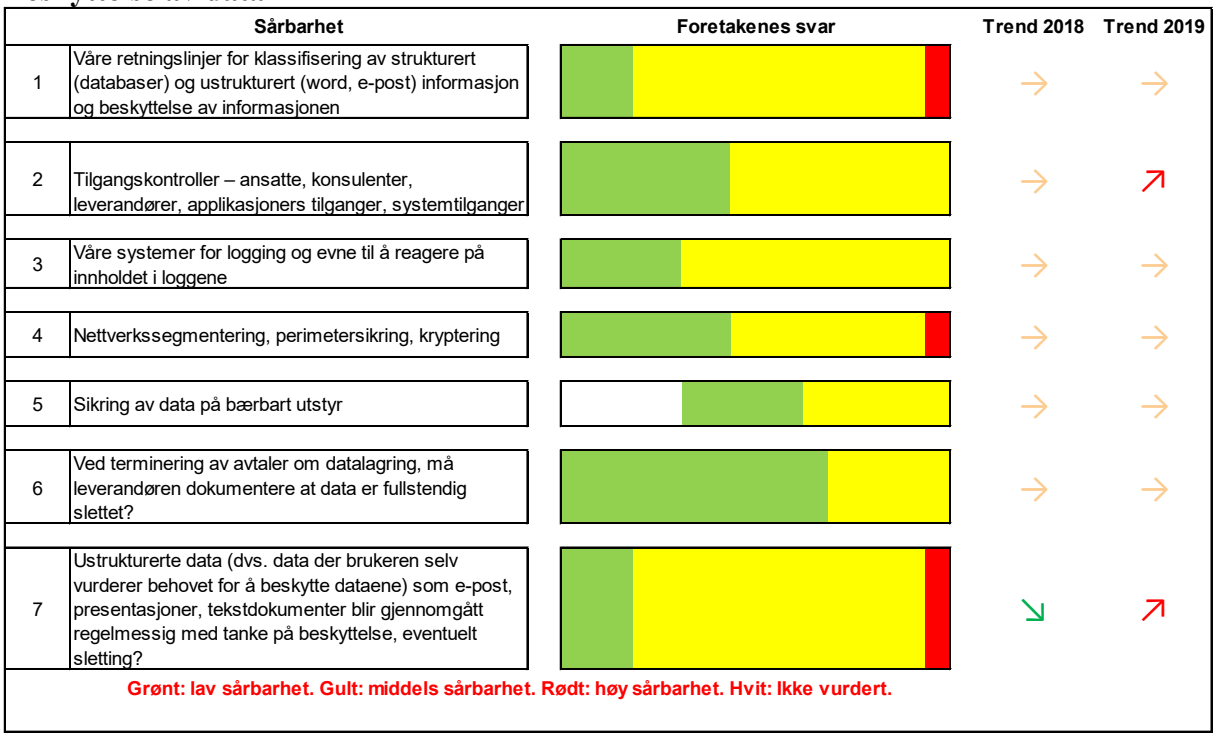
Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert.

I likhet med 2018, anses leveransepresset å utgjøre en risiko, men foretakene forventer en utflating av risikoen. Blant annet er trenden for omfanget av endringer (punkt 15) stabil i 2019. Selv om foretakene melder om en stadig økende kompleksitet i IT-systemene synes risikoen knyttet til kompleksiteten (punkt 5) å ha gått ned i 2019, og at trenden går fra økende til minkende risiko.

Risikoen knyttet til angrep synes å ha økt fra 2018 til 2019, se punkt 6 og 10. Det er fortsatt høy risiko knyttet til systemendringer som følge av nye regulatoriske krav, men foretakene forventer at denne risikoen vil avta. Dette kan ha sammenheng med at en rekke regulatoriske endringer nå er gjennomført, jf. PSD 2, MiFID II og GDPR.

Risiko som følge av medarbeidernes manglende sikkerhetsbevissthet har økt noe, og kan ha sammenheng med at angrepene er blitt mer sofistikerte. Også et mer komplisert leverandørbilde, der mange og stadig nye eksterne medarbeidere er inne i bildet, kan spille inn. Det er fremdeles risiko knyttet til tilgang på kompetanse, men risikoen er på vei ned. Dette kan ha sammenheng med at leveransepresset og regulatoriske krav anses å bli redusert fremover.

Beskyttelse av data



Risikoen knyttet til tilgangskontroller viser en økende trend og kan skyldes at en rekke eksterne medarbeidere er inne i bildet ved utkontraktering eller kjøp av tjenester. Ustrukturerte data rapporteres å utgjøre en større risiko i 2019.

ID-tyveri

	Sårbarhet	Foretakenes svar	Trend 2018	Trend 2019
1	En angriper tar over en brukerid og misbruker denne		→	→
2	Kontroll når det gjelder utlevering, bruk og sletting av logon-id og passord til kunder		→	→
3	Kontroller som forhindrer "skimming" og "Card not present"-svindel		→	→
4	Vi krever sterk kundeautentisering i forbindelse med betalinger for handel på internett		I/A	→

Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert.

Risikoen knytte til "Card not present" rapporteres å være høyere i 2019 enn 2018, men trenden er uendret. For øvrig vurderes risikoen å være omtrent den samme som i 2018.

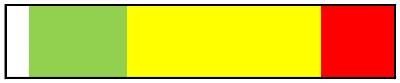
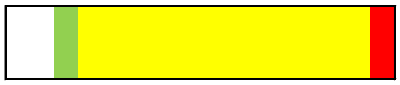
Interne misligheter

	Sårbarhet	Foretakenes svar	Trend 2018	Trend 2019
1	Våre rutiner når det gjelder tjenestedeling (dual kontroll)		→	→
2	Logging og varsling		→	→
3	Analyse av "mistenkelige" transaksjoner som tilbakevalutering, bevegelser på interne kontoer, overføring fra kunde til ansatt og tilbake		→	→
4	Overvåking av ansattes egenhandel		→	→

Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert.

Risikoen knyttet til mangelfull logging og varsling synes å være større i 2019 enn i 2018. Ellers er bildet omtrent det samme i 2019 som i 2018.

Hvitvasking

	Sårbarhet	Foretakenes svar	Trend 2018	Trend 2019
1	Markedsovervåking		↘	→
2	IT-systemenes evne til å samle informasjon om kunde, kunderelasjoner og kundeadferd (KYC – Know Your Customer)		→	→
3	Elektronisk overvåking av transaksjoner og transaksjonsmønstre – presisjon i flagging av mistenkelige transaksjoner		→	↗

Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert.

Foretakene rapporterer om økt risiko knyttet til IT-systemenes evne til å samle informasjon om kunde, kunderelasjoner og kundeatferd. Risikoen knyttet til manglende presisjon i flagging av mistenkelige transaksjoner antas å øke.

2 – Grunnlag for risikomatrisen

Finanstilsynets vurdering av risiko innen de ulike områdene, med angivelse av sannsynlighet og graden av konsekvens, er omtalt i dette vedlegget. Sammen med observasjoner og vurderinger i kapittel 3 til 6 danner dette grunnlaget for risikomatrisen i kapittel 1.

Følgende definisjoner benyttes:

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.

Styringsmodell og internkontroll

Finanstilsynet vurderer den samlede risikoen knyttet til sårbarheter ved **foretakets styringsmodell og internkontroll** som **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, herunder kontroller, vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for at compliancefunksjonen ikke avdekker alvorlige svakheter i operative enheters kontroll, vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for at foretakets styre og ledelse ikke har informasjon som bekrefter eller avkrefter etterlevelse av interne og eksterne krav, vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for at foretakets styre og ledelse *ikke* har tilstrekkelig kompetanse og innsikt for å bidra til at IT-investeringer understøtter foretakets strategi og behov, og forståelse av risikobildet innen IKT-området som er nødvendig for å sikre en stabil og sikker IKT-drift, vurderes som *middels* og med *moderat* konsekvens.

- Sannsynligheten for uklare roller mellom foretakets første- og andrelinjeforsvar, som fører til alvorlige svakheter i overvåkingen av og kontroll med foretakets styring og kontroll, vurderes som *lav* og med *begrenset* konsekvens.
- Sannsynligheten for at alvorlige sårbarheter ikke avdekkes, som følge av mangelfull risikostyring mellom operative enhet og risikostyringsfunksjonen i andrelinjen, vurderes som *lav* til *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.
- Sannsynligheten for alvorlige organisatoriske utfordringer som følge av svak endringsledelse, vurderes som *middels* og med *moderat* konsekvens.

Kompetanse og kompetansestyring

Finanstilsynet vurderer den samlede risikoen, på nåværende tidspunkt, knyttet til sårbarheter ved **kompetanse og kompetansestyring** 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* til *moderat*. Dette er basert på følgende vurderinger:

- Sannsynligheten for at styre og ledelse ikke har tilstrekkelig oversikt over ansattes kompetanse, og heller ikke har oversikt over nåværende og fremtidig behov, som følge av mangelfull kompetansestyring, vurderes som *lav* til *middels* og med *begrensett* konsekvens
- 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 *middles* 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 *lav* til *middels* og med *begrenset* konsekvens.
- Sannsynligheten for en økt avhengighet av leverandører i utlandet, som følge av mangel på ressurser og et økt behov i Norge, vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for at manglende forståelse av risikoene ved bruk skytjenester fører til uønskede hendelser, vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for at manglende kompetanse innen ny teknologi, som RPA, AI og blokkjede medfører at vesentlige operasjonelle risikoer ved bruk ikke avdekkes, vurderes som *middels* og med *begrenset* til *moderat* konsekvens.

Leverandørstyring

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

- Sannsynligheten for at vesentlige avvik i leverandørens internkontroll ikke oppdages av foretaket, vurderes som *middels* og med *moderat* til *alvorlig* 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 *alvorlig* 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.

Digital kriminalitet

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

- Sannsynligheten for at alvorlige svakheter i et fortetaks forsvarsverk ikke avdekkes om følge av mangelfull eller manglende sikkerhetstest, vurderes som *høy* og med *alvorlig* konsekvens.
- Sannsynligheten for at et foretak har vesentlige feil i sikkerhetskonfigureringen av kritiske systemer som følge av manglende gradering av systemene, vurderes som *middels* og med *alvorlig* konsekvens.
- Sannsynligheten for at et foretak har vesentlige feil i sikkerhetskonfigureringen av skytjenester, vurderes som *middels* og med *alvorlig* konsekvens.

- Sannsynligheten for at kriminelle lykkes med å utnytte sårbarheter i maskinvare (CPU) eller fastvare (UEFI), som rammer et foretak, vurderes som *lav* med *moderat* konsekvens.
- Sannsynligheten for at foretak rammes av løsepengevirus med tap av forretningskritiske data, som følge av skadevare (kryptering), vurderes som *middels* og med *kritisk* 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 tidsnok tettet som følg av mangelfulle 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.
- Sannsynligheten for at tredjeparts applikasjoner, som tredjepart integrerer mellom foretakets systemer og foretakets kunder, fører til uønskede sikkerhetshendelser, vurderes som *middels* med *moderat* konsekvens.
- Sannsynligheten for at ansatte eller personell hos leverandører utgjør en vesentlig sårbarhet, som følge av uaktsomhet og manglende kompetanse om sikker bruk av foretakets systemer, vurderes som *høy* og med *alvorlig* konsekvens.
- Sannsynligheten for at kriminelle eller fremmed etterretning forsøker å rekruttere ansatte eller personell hos leverandører for å få tilgang til informasjon om sårbarheter i digital infrastruktur eller annen informasjon om foretaket, vurderes som *middels* og med *alvorlig* konsekvens.
- Sannsynligheten for at ansatte gjennom sosial manipulering ufrivillig benyttes som middel for digitalt angrep, vurderes som *høy* og med *alvorlig* konsekvens.
- Sannsynligheten for at kriminelle lykkes med å ta seg inn i foretaks lokaler som følge av svak besøkskontroll, vurderes som *lav* og med *begrenset* konsekvens.
- Sannsynligheten for at kriminelle vil lykkes med å ta seg inn i et foretaks lokaler med makt, vurderes som *høy* og med *alvorlig* konsekvens.
- Sannsynligheten for at ansatte gjennom trusler ufrivillig benyttes som middel for digitalt angrep, vurderes som *lav* og med *moderat* konsekvens.
- Sannsynligheten for at personell hos leverandører gjennom trusler ufrivillig benyttes som middel for digitalt angrep, vurderes som *lav* og med *moderat* konsekvens.
- Sannsynligheten for at utro ansatte i foretakets eller personell i leverandørers utviklingsmiljø plasserer ondsinnet kode i forretningskritiske applikasjoner, vurderes som *lav* og med *moderat* konsekvens.
- Sannsynligheten for at ansatte eller personell hos leverandører hjelper kriminelle med å sluse kriminelle transaksjoner gjennom et foretaks systemer, vurderes som *middels* og med *alvorlig* konsekvens.
- Sannsynligheten for at personinformasjon, herunder informasjon om foretaks ansatte og personell hos leverandører, som har roller som kan være av interesse for og utnyttes av kriminelle, kommer kriminelle i hende, vurderes som *middels* til *høy* og med *alvorlig* konsekvens.

Informasjonslekkasje

Finanstilsynet vurderer den samlede risikoen knyttet til sårbarheter og trusler som kan føre til skade som følge av **informasjonslekkasje** som **høy**. Sannsynligheten for uønskede hendelser vurderes som *høy* og konsekvensen som *moderat*. Dette er basert på følgende vurderinger:

- Sannsynligheten for at klassifisert dokumentasjon sendes uautorisert ut av foretaket som følge av manglende klassifisering og kontroll, vurderes som *høy* og med *moderat* konsekvens.
- Sannsynligheten for at konfidensiell informasjon kommer på avveie som følge av manglende 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 manglende 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 manglende kontroll av personell hos leverandører, vurderes som *middels* og med *alvorlig* konsekvens
- Sannsynligheten for at sensitiv informasjon som kan benyttes til å skade foretaket sendes eller formidles uautorisert, bevisst eller ubevisst, til eksterne kilder *ikke* vil bli oppdaget, vurderes som *høy* og med *moderat* konsekvens.
- Sannsynligheten for at ansatte eller personell hos leverandører opererer som innsider og overleverer eller sender sensitiv informasjon, eksempelvis liste over epostadresser og påloggingsinformasjon, til kriminelle, vurderes som *middels* og med *moderat* konsekvens.

IKT-drift

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

- Sannsynligheten for ustabile og /eller utilgjengelige tjenester som følge av økt grad av integrasjon mellom ulike tjenesteleverandører, vurderes som *middels* til *høy* og med *alvorlig* konsekvens.
- Sannsynligheten for driftsproblemer som rammer felles operasjonell infrastruktur, vurderes som *middels* og med *alvorlig* konsekvens.
- Sannsynligheten for driftsproblemer som følge av en manglende og tilstrekkelig helhetlig forståelse for og oversikt over arkitektur og de digitale forretningsprosessene, vurderes som *middels* til *høy* og med *moderat* konsekvens.
- Sannsynligheten for redusert datakvalitet som følge av kompleks integrasjon mellom tjenesteleverandører, vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for driftsproblemer som følge av mangelfull konfigurasjonsstyring (maskinvare applikasjoner, databaser, operativsystem m.m.), vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for at avtalt tid for retting av kritiske feil ikke overholdes, som følge av kompleksitet i systemporteføljen med integrasjon mellom nye og gamle systemer, vurderes som *middels* og med *alvorlig* konsekvens.

- Sannsynligheten for utilgjengelige tjenester som følge av mangelfull kapasitetsstyring, vurderes som *middels* til *høy* 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 *lav* og med *moderat* konsekvens.
- Sannsynligheten for driftsproblemer i prosessen med sanering av utdaterte og kritiske systemer, vurderes som *høy* og med *moderat* til *alvorlig* konsekvens.
- Sannsynligheten for driftsproblemer som følge av manglende tilgang på kompetanse innen driftstøtte for stormaskin, vurderes som *middels* og med *moderat* konsekvens.

Kontinuitetsledelse og kriseledelse

Finanstilsynet vurderer den samlede risikoen knyttet til sårbarheter ved **kontinuitetsledelse og kriseledelse som middels** til **høy**. Sannsynligheten for uønskede hendelser som medfører at kriseløsning for kritiske forretningsprosesser må iverksettes vurderes som *svært lav* til *lav* og konsekvensen som *kritisk* denne ikke fungerer som forutsatt. 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 *lav* til *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 *lav* til *middels* og med *kritisk* konsekvens.
- Sannsynligheten for manglende sikkerhetsoppdateringer av kriseløsningen, vurderes som *lav* til *middels* og med *alvorlig* konsekvens.
- Sannsynligheten for at et foretak 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 *middels* til *høy* og med *kritisk* konsekvens.

Geopolitiske forhold

Finanstilsynet vurderer risikoen knyttet til sårbarheter overfor utenlandske aktører som leverer kritiske IKT-tjenester til foretakene i Norge, som **middels** til **høy**. Sannsynligheten for uønskede hendelser, der

utenlandske leverandører blir avskåret fra å levere sine tjenester, vurderes som *lav* og konsekvensen som *alvorlig*. Dette er basert på følgende vurderinger:

- Sannsynligheten for at et foretaks beredskapspersonell *ikke* vil være i stand til å opprettholde sikker og stabil drift, der utenlandske leverandører ikke er tilgjengelig, vurderes som *lav* og med *alvorlig* konsekvens.
- Sannsynligheten for at et foretaks beredskapspersonell *ikke* vil være i stand til å opprettholde sikker og stabil drift ved alvorlige IKT-hendelser, og der utenlandske leverandører ikke er tilgjengelig, vurderes som *middels* og med *alvorlig* konsekvens.
- Sannsynligheten for at kommunikasjonsbrudd med utlandet hvor konsekvensen er at utenlandske leverandører er avskåret fra å utføre kritiske IKT-tjenester, vurderes som *lav* og med *alvorlig* konsekvens.

Endringsstyring

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

- 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, funksjonelle og ikke-funksjonelle, 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.

Tilgangsstyring

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

- Sannsynligheten for at ansatte 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 ansatte eller personell hos leverandører har administrasjonsrettigheter uten at ledelsen er klar over dette, vurderes som *middels* og med *moderat* konsekvens.

- Sannsynligheten for at konfidensiell informasjon kommer på avveie som følge av mangelfull tilgangsstyring og -kontroll med ansattes tilganger, vurderes som *høy* og med *moderat* konsekvens.
- Sannsynligheten for at konfidensiell og/eller gradert informasjon kommer på avveie, som følge av sikkerhetsbrudd hos leverandøren, vurderes som *middels* til *høy* 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.

Datakvalitet

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

- Sannsynligheten for at beslutninger tas på feil grunnlag som følge av dårlig datakvalitet eller manglende data, vurderes som *middels* til *høy* og med *moderat* konsekvens.
- Sannsynligheten for at svakheter i hvitvaskingskontroll som følge av dårlig datakvalitet eller manglende data, vurderes som *middels* og med *begrenset* til *moderat* konsekvens.
- Sannsynligheten for at risikoer ikke identifiseres som følge av dårlig datakvalitet eller manglende data, vurderes som *middels* og med *begrensett* konsekvens.
- Sannsynligheten for at overvåking av driften ikke avdekker unormaliteter ikke identifiseres som følge av dårlig datakvalitet eller manglende data, vurderes som *middels* og med *begrenset* til *moderat* konsekvens.

3 – Finanstilsynets oppfølging

Sentrale områder for Finanstilsynet IKT-tilsyn

Tilsynsvirksomheten er risikobasert, og Finanstilsynet prioriterer tilsyn med foretak som har størst betydning for finansiell stabilitet og velfungerende markeder. IKT-risiko vurderes og foretakenes egne årlige vurderinger av IKT-risiko gjennomgås. Tilsyn med organisering av IKT-/cyber-sikkerhetsarbeidet, sikkerhet knyttet til foretakenes IKT-løsninger og organiseringen av overvåkingen vektlegges. Tilsynene omfatter blant annet foretakenes kontroll med tilganger til systemer, særlig systemer som inneholder sensitiv informasjon, og foretakenes testing mht. inntrenging i foretakenes systemer.

Andre prioriterte temaer for tilsynsvirksomheten er overordnet styring og kontroll med IKT, beredskapsarbeid knyttet til kontinuitet og kriseløsninger og testing av disse, foretakenes styring, kontroll og oppfølging av utkontraktert IKT-virksomhet, foretakenes betalingstjenester og IKT-løsninger for å avdekke hvitvasking og terrorfinansiering. Finanstilsynet legger blant annet vekt på 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 omfatter foretakenes risikovurderinger ved utkontraktering av IKT, og kvalitet på avtaleverk og oppfølging av avtaler mellom foretak og leverandør.

Arbeid med betalingssystemer

EUs reviderte betalingstjenestedirektiv (PSD 2) er tatt inn i norsk lovgivning, og vil ligge til grunn for tilsynet med foretakenes betalingstjenester. Foretakene vil blant annet bli fulgt opp mht. etterlevelse av ny forskrift om systemer for betalingstjenester[36], risiko knyttet til betalingstjenestene og etterlevelse av meldeplikten ved nye eller endrede betalingstjenester. Kontotilbyderes grensesnitt (API-er) for tilgang til konto vil også bli fulgt opp. I konsesjonsbehandlingen vil det påses at foretakene har godt dokumenterte rutiner på områder relatert til IKT- og betalingstjenestene.

Samarbeidet med Norges Bank omkring betalingssystemet og finansiell infrastruktur vil videreføres.

Oppfølging av hendelser

I tilsynsvirksomheten er oppfølging av IKT-hendelser er et prioritert område. Finanstilsynet vil i 2020 fortsatt overvåke utviklingen nøye. Ved hendelser vil det bli lagt vekt på at foretaket avdekker årsaker og iverksetter tiltak for å hindre gjentakelser. Ved alvorlige avvik vil hendelsen følges løpende gjennom hele forløpet. Særlige tiltak vil bli vurdert.

Finanstilsynet vil videreføre sin årlige gjennomgang av hendelsesrapporteringen med de største aktørene.

[36] Lovdata: Forskrift om systemer for betalingstjenester

Utkontraktering av IKT-virksomhet

Finanstilsynet vil fortsatt følge opp foretakenes utkontraktering av IKT-virksomhet og påse at foretakene ved inngåelse av ny eller endring av eksisterende avtale om utkontraktering melder denne til Finanstilsynet, slik finansforetaksloven § 4c krever.

Det følges opp at foretakene gjennomfører en forsvarlig vurdering av utkontrakteringsforholdet, at avtalene er i tråd med regelverket og at utkontrakteringen er forsvarlig behandlet i foretaket, jf. IKT-forskriften § 2.

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 2020, og tiltak knyttet til funn i tidligere øvelser vil bli fulgt opp.

Særskilte hendelser som koronakrisen og foretakenes innretning av sin IKT-virksomhet vil bli fulgt tett, særlig hos sentrale aktører i den finansielle infrastrukturen.

Finanstilsynet deltar i relevant beredskapsarbeid initiert av andre sektorer og samhandling innenfor nasjonalt rammeverk for håndtering av IKT-sikkerhetshendelser, blant annet gjennom Nasjonalt cybersikkerhetssenter (NCSC), som Nasjonal sikkerhetsmyndighet (NSM) har etablert.

Finanstilsynet vil innrette sitt beredskapsarbeid og håndtering av IKT-sikkerhetshendelser i tråd med NSMs rammeverk for håndtering av IKT-sikkerhetshendelser[37]. Finansdepartementet oppnevnte i 2019 Finanstilsynet som sektorvis responsmiljø (SRM) på finansmarkedsområdet. Finanstilsynet utøver rollen i samarbeid med Nordic Financial CERT, i tråd med avtalte regler for informasjonsutveksling. NSMs rammeverk ligger til grunn for samhandlingen mellom Finanstilsynet og Nordic Financial CERT.

Oppfølging av trusselbildet knyttet til digital kriminalitet

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

- digitalt trusselbilde
- beredskapsarbeid rettet mot digital sårbarhet og digital sikkerhet
- foretakenes organisering og oppfølging av sikkerhetsarbeidet
- endringene i betalingsformidlingen ved utnyttelse av ny teknologi (FinTech),
- grensekryssende virksomhet

[37] NSM: Rammeverk for håndtering av IKT-hendelser

Finanstilsynet vil sammen med Norges Bank vurdere og eventuelt gjennomføre et nasjonalt tilpasset testrammeverk for cybersikkerhet (TIBER-rammeverket).

Forbrukervern

Finanstilsynet legger vekt på at foretakene ivaretar kundenes sikkerhet. 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 digitale løsninger i tråd med regelverket, og at løsninger som lanseres har innebygd sikkerhet og funksjonalitet i tråd med forbrukernes forventninger.

Det vil 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.

Basert på nye krav om rapportering av svindel ved bruk av betalingstjenester, jf. forskrift om systemer for betalingstjenester § 2, vil Finanstilsynet følge opp samlet omfang av svindler, og ved behov også enkeltaktører.

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

Finanstilsynet vil fortsette å følge opp at bankene ivaretar sine plikter når det gjelder etterlevelse av finansforetakslovens[38] bestemmelser om kontanttilbud. Ny løsning for kontanter i butikk (KIB) vil få særlig oppmerksomhet. 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[39].

[38] Lov om finansforetak og finanskonsern (finansforetaksloven)
[39] Forskrift om finansforetak og finanskonsern (finansforetaksforskriften)

4 – Internkontrollfunksjoner

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 funksjonene 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 legge til rette for 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.

Compliancefunksjonens 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 uavhengig internrevisjon, som gjennomfører risikobaserte samt 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.

For mindre foretak er det ikke vanlig med egne og dedikerte ressurser i de tre forsvarslinjene. Compliance-rollen i andrelinjen har som regel ikke nødvendig IKT-kompetanse til å overvåke foretakets etterlevelse av IKT-forskriften, og tredjelinjeforsvarets internrevisjon er som regel utkontraktert.

Foretak som ikke er pålagt å ha egen internrevisjon, eller som ikke besitter IKT- kompetanse i risikostyrings- og compliancefunksjonen, bør vurdere å benytte eksterne ressurser for å vurdere om

foretakets rammeverk, herunder policyer og retningslinjer, samsvarer med god praksis og krav til leverandørstyring. Andre elementer som bør omfattes er om compliancefunksjonens overvåking samsvarer med styrets og ledelsens behov for bekreftelse på etterlevelse av de krav som er satt gjennom lover og regler, og om uavhengige vurderinger av kontroller som utføres internt i foretaket og hos leverandører skjer med den kvaliteten som må forventes.

Kunnskap om foretakets risikobilde og trusselsituasjon står sentralt i arbeidet med å identifisere områder som skal prioriteres for internrevisjon. Raske endringer 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 internrevisorene innehar en viss forretningsforståelse i tillegg til IKT-kompetanse.

Det er viktig at foretakets internrevisjon har tilstrekkelig kompetanse og risikoforståelse, samt at styret ivaretar sitt ansvar for at internrevisjonen har nødvendig kompetanse og ressurser til å utøve sin rolle i tråd med risikobildet og endringer i dette.

Finanstilsynet vil i tilsynsarbeidet vurdere foretakenes styring og kontroll innen IKT-området, og gjennom dette søke å avdekke sårbarheter som kan utgjøre en risiko. Finanstilsynet vil også kunne påpeke forbedringsområder som kan redusere foretakets risiko. Åpen dialog og god samhandling er viktig for at Finanstilsynet skal kunne danne seg et riktig bilde av risiko- og kontrollsituasjonen hos foretakene. Finanstilsynet viser også til EBAs "Guidelines on internal governance"[40].

[40] Guidelines on internal governance under Directive 2013/36/EU EBA

5 – Styrende rammeverk: Strategi, policy og retningslinjer

Foretakets strategi, policyer, retningslinjer og instrukser (rammeverket), skal blant annet understøtte regulatoriske krav og foretakets egne definerte krav. IKT-strategien omfatter blant annet foretakets mål, og en plan som legges til rette for å nå målene. Strategien bør blant annet være tydelig på hvilke målsettinger som er fastlagt, for eksempel innen området informasjonssikkerhet, og skal også understøtte foretakets overordnede forretningsstrategi. Videre skal en strategi justeres i forhold til blant annet endringer i risikobildet og endringene skal forankres i organisasjonen. En policy gir den operative ledelsen føringer om krav styret og ledelsen har fastsatt, blant annet gjennom strategien. Retningslinjer og/eller instrukser beskriver hvordan kravene skal implementeres og operasjonaliseres, ofte understøttet av detaljert driftsdokumentasjon. Ettersom foretakene i stor grad har utkontraktert sine IKT-tjenester, er det viktig med transparens mellom foretakets rammeverk og avtalens bestemmelser og krav.

Rammeverket og avtaler med leverandører gir naturlig nok ingen garanti for at foretakets operative enheter i førstelinjen og foretakets leverandører etterlever de krav som er satt. Det er derfor viktig at foretakene beslutter og beskriver hvilke kontroller som de operative enhetene, både internt i foretaket og hos leverandørene, skal utføre for bekreftelse av at kravene etterleves. Rammeverket legges også til grunn for andre- og tredjelinjevurderinger av foretakets risikostyring og internkontroll, herunder vurdering av foretakets etterlevelse av eget rammeverk gjennom de kontroller som er utført.

Endringer i foretakets strategi, endringer i trusselbildet, endringer i teknologi og endrede regulatoriske krav vil kunne medføre revisjon av styrende dokumenter. Finanstilsynet understreker foretakets ansvar for at forvaltningsrutinene for rammeverket sikrer en løpende oppdatering, og at nødvendige endringer eller nye kontroller beskrives og operasjonaliseres.

6 – Utkontraktering

Følgende temaer er beskrevet:

- Krav ved utkontraktering av IKT-tjenester
- Uavhengige revisjonserklæringer (ISAE 3402) og bekreftelse fra leverandører

Krav ved utkontraktering av IKT-tjenester

Det er utkontraktering når et foretak velger å la en annen juridisk enhet ("oppdragstaker") utføre oppgaver på vegne av foretaket som foretaket ellers selv ville ha utført. Utkontrakterte oppgaver kan gjelde kjøp av kompetanse, tjenester eller IKT-løsninger. Det er utkontraktering også når oppgaver settes bort til en annen juridisk enhet i samme konsern eller gruppering som foretaket.

Hvor viktig oppgaven er for foretakets virksomhet er uten betydning for om en avtale innebærer utkontraktering. Hvilken betydning den utkontrakterte oppgaven har for foretakets virksomhet er imidlertid avgjørende for hvilke regler som kommer til anvendelse. Det kan blant annet være begrensninger i adgangen til å utkontraktere de aktuelle oppgavene, og utkontrakteringsavtalen kan være meldepliktig til Finanstilsynet.

Det er en grunnleggende forutsetning at virksomheten skal drives forsvarlig i foretak underlagt tilsyn. Det er også en grunnleggende forutsetning at Finanstilsynet skal kunne føre tilsyn med utkontraktert virksomhet. Disse to forutsetningene vil alltid utgjøre en begrensning i adgangen til å utkontraktere virksomhet.

Bare oppgaver kan utkontrakteres. Foretakets ansvar overfor kunder, offentlige myndigheter og andre gjelder uavhengig av det kontraktsrettslige ansvaret som avtales mellom foretaket og den som påtar seg å utføre oppdraget på vegne av foretaket. Foretak som utkontrakterer IKT-virksomhet, må vurdere om utkontrakteringen er i tråd med regelverket foretakets konsesjon. Utkontraktering av IKT-virksomhet må være forankret i foretakets strategi.

For hver utkontrakteringsavtale må foretaket vurdere hvilken risiko utkontrakteringen innebærer for foretakets virksomhet. Vurderingen må konkretisere de ulike risikoene, sannsynligheten for at de aktuelle hendelsene inntreffer og konsekvensen for foretakets virksomhet dersom noen av disse inntreffer. Sårbarhet som følger av at samme oppdragstaker utfører mange oppgaver på vegne av foretaket, må inngå i risikovurderingen. I tillegg må foretaket vurdere muligheten for å reversere utkontrakteringsavtalen.

Foretaket må beslutte hvilke risikoreduserende tiltak som skal iverksettes. Enkelte risikoreduserende tiltak er ansett som så viktige at de fremkommer som krav i sektorregelverket. Foretaket må sikre at iverksatte tiltak virker etter sin hensikt og at risikoen, etter iverksettelse av tiltakene, er akseptabel.

Foretak kan tilpasse sin risikostyring og internkontroll etter arten, omfanget av og kompleksiteten i foretakets virksomhet. Prinsippet om forholdsmessighet innebærer blant annet at foretaket, i vurderingen av hvilke risikoreduserende tiltak som skal iverksettes, kan se hen til hvilken betydning utkontrakteringen har for virksomheten. Eventuelle tiltak som følger av krav i regelverket eller konsesjonsvilkår, må uansett iverksettes.

De europeiske tilsynsmyndighetene EBA, EIOPA og ESMA har fastsatt retningslinjer som ligger til grunn for Finanstilsynets håndheving av sektorregelverket, jf. vedlegg 8.

Uavhengige revisjonserklæringer og bekreftelse fra leverandører

Av IKT-forskriftet §12 framgår det blant annet at "Avtalen må sikre at foretak under tilsyn også gis rett til å kontrollere, herunder revidere de av leverandørens aktiviteter som er knyttet til avtalen."

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 på et overordnet nivå gode indikasjoner på kvaliteten i leverandørens kontroller innen prosesser som blant annet endringsstyring, tilgangsstyring, tilgjengelighet og sikkerhet.

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 typer kontroller som ønskes gjennomført.

Bekreftelse på etterlevelse fra skyleverandører

De største skytjenesteleverandørene, herunder Microsoft, Google og Amazon, har etablert tjenester med integrerte kontrollsystemer, der kundene kan hente ut informasjon og dokumentasjon knyttet leverandørens internkontroll for tjenesteleveransene. Foretak som benytter skytjenester må etablere nødvendig kompetanse og innsikt i kontrollsystemene, og velge tjenenester som samsvarer med kontrollkravet.

7 – Informasjonssikkerhet og digital kriminalitet

Følgende temaer er beskrevet i dette vedlegget:

- Informasjonssikkerhet
- Vurdering av informasjon
- Beskyttelse av kundeinformasjon
- Kartlegging av trusler
- Økonomisk motiverte trusler
- Kartlegging av risiko
- Sårbarhetsrapportering fra eksterne som et risikoreduserende tiltak

Informasjonssikkerhet

Informasjonssikkerhet omfatter tiltak for å sikre integritet, konfidensialitet og tilgjengelighet for informasjon og informasjonssystemer. I en risikovurdering knyttet til informasjonssikkerhet er det viktig at organisasjonen har en felles forståelse av hva som utgjør en trussel, sårbarhet eller risiko.

Det er tatt utgangspunkt i definisjonene i standardene NS 5830[41] og NS 5832[42] fra Standard Norge.

Vurdering av informasjon

For at foretakene skal kunne iverksette tiltak innen informasjonssikkerhet, må det være avklart hvilken informasjon som må beskyttes. Dette omtales som en verdivurdering.

Det kan være behov for å begrense tilgangen til informasjonen (informasjonen er konfidensiell), informasjonen må være korrekt og beskyttes mot manipulering (integriteten er sikret) eller informasjonen må være tilgjengelig ved tjenstlige behov (tilgangen er sikret). Tiltak kan også omfatte at informasjonen kun er tilgjengelig for andre informasjonssystemer gjennom godkjente grensesnitt for informasjonsutveksling.

Informasjonssikkerhet omfatter imidlertid ikke beskyttelse av kontante betalingsmidler selv om kontanter i seg selv utgjør en reell verdi. Det kan imidlertid være behov for å begrense tilgangen til informasjon om hvordan man kan få tilgang til oppbevarte kontanter. Eksempler på informasjon som må beskyttes kan i denne sammenheng være informasjon om en planlagt pengetransport, mens adgangskontrollsystemet kan være et skjermingsverdig informasjonssystem siden dette kan manipuleres for å gi uvedkommende adgang til områder der kontanter oppbevares, eller systemet inneholder informasjon om hvem som allerede har tilganger til slike områder. Dette er eksempler på forhold som bør vurderes i forbindelse med en verdivurdering av informasjon.

41 NS 5830:2012 – Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi

42 NS 5832:2014 Samfunnssikkerhet – beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse (Norsk Standard)

Beskyttelse av kundeinformasjon

Informasjon om de enkelte kundene i et foretak er i seg selv data som må beskyttes. For banker kan informasjon om enkeltkunder og deres betalingsopplysninger være sensitiv informasjon som må skjermes. For verdipapirregistre vil det i tillegg være behov for å skjerme informasjon om eierforhold, både for å sikre at informasjonen er korrekt og beskyttet mot manipulasjon, og fordi informasjon om handelstransaksjoner kan være børssensitive. For et livsforsikringsforetak vil det spesifikt være behov for å skjerme helseinformasjon, jf. krav i Normen[43].

Kartlegging av trusler

Når et foretak gjennom verdivurderingen har kartlagt informasjon som krever skjerming, foreligger et grunnlag for å kartlegge hvilke trusler informasjonen må beskyttes mot. Standarden NS 5832 definerer trussel som et produkt av faktorene intensjon og kapasitet. Med intensjon menes hvilke handlinger en trussel-aktør kan være villig til å utføre, samt hvorvidt aktøren er ute etter en økonomisk gevinst eller ønsker å innhente informasjon om sentral infrastruktur. Med kapasitet menes hvilken evne aktøren har til å gjennomføre et angrep, for eksempel gjennom tilgang til nødvendig IKT-kompetanse og tilstrekkelig med finansielle midler.

Flere finansielle foretak som opererer i Norge, har etablert egne cybersikkerhetssentre (incident respons team – IRT) som håndterer konkrete hendelser. De største finansielle foretakene har i tillegg etablert egen trusseletterretning. Større internasjonale aktører og norske filialer av disse nyter også godt av de store foretakenes kapasitet og tilgang til kompetente IKT-ressurser for å kunne håndtere trusler mot informasjonssikkerheten.

Både E-tjenesten, PST og NSM utarbeider årlige rapporter med informasjon om det aktuelle trusselbildet og risiko knyttet til informasjonssikkerhet, som foretakene i finanssektoren bør sette seg inn i, jf. punkt 3.4.2.

Kartlegging av risiko og bruk av scenarier for å avdekke sårbarheter og risiko

Informasjon om relevante trusler og trusselaktører gir foretakene grunnlag for å utarbeide scenarier for trusler mot verdier skal beskyttes.

Av de tre faktorene verdi, trussel og sårbarhet, er det for foretakene kun mulig å påvirke sårbarheten. For å kartlegge sårbarheten bør ulikes scenarier vurderes. Sårbarheten kan reduseres gjennom ulike tiltak, som vil variere avhengig av hvilke verdier man ønsker å beskytte samt hvilke trusselaktører man ønsker å beskytte seg mot. Identifiserte tiltak kan være av forebyggende og korrigerende karakter, og tiltakene må være tilstrekkelige for at foretaket skal kunne opprettholde et akseptabelt risikonivå.

[43] Normen - Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren

Sårbarhetsrapportering fra eksterne som et risikoreduserende tiltak

Det er foretak som på fastsatte vilkår aksepterer uanmeldte tester og forsøk på hacking mot egne nettsider. Blant annet har Oslo Børs siden 2018 åpnet for at privatpersoner kan rapportere om sårbarheter som oppdages i børsens IKT-løsninger.

Denne formen for testing har vist seg svært effektiv for å styrke foretakenes digitale forsvar, men er ikke egnet for alle organisasjoner eller systemer og må implementeres med omhu i de foretak og systemer som egner seg for dette. For foretak som egner seg for sårbarhetsrapportering og har riktige forutsetninger, kan dette medføre en betydelig heving av kvaliteten på foretakets digitale forsvar.

En rekke forutsetninger må være oppfylt for at en organisasjon skal kunne åpne for slike tester på en trygg måte. Dette omfatter blant annet følgende:

- Organisasjonen må ha tilstrekkelig kompetanse på elektronisk sikkerhet for å håndtere situasjoner og hendelser som kan oppstå under testingen.
- Programmet for sårbarhetsrapportering må være godt forankret hos ledelsen i organisasjonen og i IT-organisasjonen
- Grundige risikovurderinger av programmet for sårbarhetsrapportering
- Tjenester og sårbarheter som ikke ønskes testet må uttrykkelig ekskluderes. (For eksempel tjenestenektangrep, sosial manipulasjon og kontorlokalers fysiske sårbarheter.)
- Organisasjonen må være forberedt og ha riktig og tilstrekkelig kompetanse til å ta imot henvendelser når det åpnes for sårbarhetsrapportering
- Ansvarlig for mottak av sårbarhetsrapportering må kunne vurdere kritikalitet av sårbarheter, teste angrepskode mot egne systemer og svare sikkerhetsforskere på en profesjonell måte.
- Sårbarheter rapporteres på godkjent måte, uten at svakhetene utnyttes eller avsløres for andre.

8 – Internasjonale rammeverk knyttet til IKT-sikkerhet

I dette vedlegg beskrives:

- Retningslinjer for utkontraktering fra den europeiske banktilsynsmyndigheten (EBA)
- Retningslinjer om IKT-sikkerhet og risiko fra EBA
- Rammeverk for informasjonssikkerhet (CSA, CIS, NIST, ISO 27001, OWASP, COBIT)
- Rammeverk for sikkerhetstesting (TIBER)

Retningslinjer for utkontraktering fra EBA

Den europeiske banktilsynsmyndigheten (EBA) publiserte "Guidelines on outsourcing arrangements" 25. februar 2019. Retningslinjene ble gjort gjeldende fra 30. september 2019.

De nye retningslinjene erstatter hhv. "Guidelines on outsourcing" fastsatt i 2006 av EBAs forløper CEBS og EBAs "Recommendations on outsourcing to cloud service providers" fra 2017. Retningslinjene retter seg mot banker, kredittforetak, verdipapirforetak, betalingsforetak og e-pengeforetak, og inneholder blant annet detaljerte krav for å sikre at foretak har tilstrekkelig styring og kontroll ved utkontraktering av virksomhet. Retningslinjene omfatter også kriterier for å fastslå om en avtale med en tredjepart er utkontraktering.

Finanstilsynet har bekreftet at retningslinjene følges i Norge. Finanstilsynet har imidlertid bemerket at foretakenes meldeplikt ved utkontraktering er strengere etter norske regler enn det retningslinjene fra EBA legger opp til. Retningslinjene fra EBA stiller ikke eksplisitt krav om meldeplikt, men at tilsynsmyndighetene skal overvåke utkontrakteringsordninger. Etter finanstilsynsloven § 4 skal foretak under tilsyn melde fra til Finanstilsynet blant annet ved inngåelse av avtale om utkontraktering. Tilsynsenhetenes meldeplikt etter § 4 c gjelder uavhengig av utkontrakteringens art, omfang eller varighet og omfatter også utkontraktering innenfor et konsern. Meldingen skal gis minst 60 dager før iverksettelsen av avtalen, avtaleendringen eller bytte av oppdragstaker. Det er imidlertid gitt en del unntak fra meldeplikten i egen forskrift. Blant annet er verdipapirforetakene unntatt fra meldeplikten.

Adgangen til utkontraktering er mer omfattende i retningslinjene fra EBA enn etter norsk rett. Etter retningslinjene kan såkalte "critical or important functions" utkontrakteres. Banktjenester og betalingstjenester kan også utkontrakteres, men kun til foretak med konsesjon eller tillatelse til slik virksomhet. Etter finansforetaksloven § 13-4 er det ikke tillatt å utkontraktere kjerneoppgaver, eller utkontraktere i et slikt omfang eller på en måte som ikke kan anses som forsvarlig eller som gjør tilsynet med den utkontrakterte virksomhet eller foretakets samlede virksomhet vanskeligere. Det finnes ingen tilsvarende begrensning for utkontraktering av kjerneoppgaver i verdipapirforetak, men investeringstjenester kan kun utkontrakteres til foretak med tillatelse til å yte den aktuelle tjenesten.

Retningslinjer om IKT sikkerhet og risiko fra EBA

EBA har utarbeidet retningslinjer om IKT-sikkerhet og -risiko og publiserte "Guidelines on ICT and security risk management" 28. november 2019. Retningslinjene bygger på kravene i det reviderte

betalingstjenestedirektivets "Guidelines on security measures for operational and security risks of payment services", som gjelder fra 30. juni 2020.

Retningslinjene retter seg mot banker, betalingsforetak og e-pengeforetak, og inneholder blant annet detaljerte krav for hvordan foretak skal sikre seg mot IKT-sikkerhetsrisikoen de eksponeres for. På et overordnet nivå har den norske IKT-forskriften siden 2002 regulert de samme områdene som retningslinjene omfatter. Et av hovedmålene med retningslinjene er å gi foretakene en bedre forståelse av tilsynsmyndighetenes forventninger til hvordan IKT-sikkerhetsrisiko skal behandles. Finanstilsynet vil oppdatere sin tilsynspraksis i tråd med de nye retningslinjene.

Finanstilsynet har bekreftet at retningslinjene vil bli fulgt i Norge.

Rammeverk for informasjonssikkerhet

For foretak som ikke har ekspertise og detaljkunnskap om hvilke krav som er i tråd med god praksis, er det utarbeidet flere rammeverk og veiledninger som kan være til god hjelp, for eksempel Centre for Internet Security (CIS), Cloud Security Alliance (CSA) med rammeverk for sikkerhet ved skytjenester, NISTs rammeverk for cyber-sikkerhet, ISO med standardene ISO27001/27002 for informasjonssikkerhet, OWASP for sikkerhet i webbaserte applikasjoner og ISACA med sitt COBIT-rammeverk.

Rammeverk for sikkerhetstesting (TIBER)

Formålet med trusselbaserte sikkerhetstester er forbedring og kvalitetssikring av foretakenes digitale forsvarsevne. Slike tester benytter militære termer og metoder, slik som “red-teaming". Gjennomføring av slik sikkerhetstesting består av metodeverk som optimaliseres for å identifisere svakheter mest mulig effektivt og samtidig begrense risikoene som påføres foretaket som testes. Et viktig aspekt ved metodikken er at også testerfaringene formidles til foretaket for oppfølging. Den europeiske sentralbanken (ECB) har utarbeidet rammeverket TIBER, threat intelligence-based ethical red-teaming, og anbefaler myndighetsinvolvering i testene. Medvirkning fra myndighetene i TIBER-testingen begrunnes med at dette vil sikre testens kvalitet. Videre er det ønskelig at de nasjonale tilsynsmyndighetene i EU/EØS-området kontrollerer at finansielle institusjoner samfunnet er avhengig av, sørger for effektiv sikring mot digital kriminalitet.

Landene som har implementert slikt testrammeverk har etablert en nasjonal "TIBER-enhet" som blant annet bidrar i utforming av regelverket for testingen, i overvåkingen av testenes gjennomføring, samt i oppsummeringen av TIBER-tester gjennomført i det enkelte land. Hensikten er å bygge gode erfaringsbaser som kan benyttes ved senere tester. Regelverket for sikkerhetstester kan omfatte store deler av IKT-sikkerhetsområdet i et foretak. Erfaringene fra gjennomførte tester har vist at man avdekker viktigere og langt flere svakheter enn ved tradisjonell kvalitetsstyring og revisjon.

Erfaringer fra andre nordiske land viser at tilgang på leverandører som har kompetanse og erfaring med metodisk trusselbasert “red-teaming” er en forutsetning for å kunne lykkes med TIBER-tester.

Mangel på slik kompetanse har vist seg å være et forsinkende, kvalitetsforringende og kostnadsdrivende element for testgjennomføring.

Man kan forvente at første gjennomføring av en TIBER-test vil medføre økte kostnader for foretak som er involvert i testen. Kostnadene forventes imidlertid vesentlig redusert ved senere tester. Erfaringer fra tester gjennomført i andre land, tilsier at testene likevel er lønnsomme for foretakene og kan bidra til bedret digital forsvarsevne hos foretak viktig for kritiske samfunnsfunksjoner.

Finanstilsynet forventer at foretak uavhengig av deltakelse i sikkerhetstesting under et testrammeverk, som TIBER, systematisk bruker liknende trusselbaserte "red-teaming"-metoder, for å sikre foretakets IT-systemer mot digital kriminalitet.

9 – Bruk av ny teknologi i finanssektoren

Følgende temaer er beskrevet i dette vedlegg, jf. punkt 3.7.4.

Teknologi som endrer forretningsprosessene, herunder

- Robotisert prosessautomatisering (RPA)
- AI og dataanalyse
- Blokkjede

Teknologi som endrer forretningsprosessene

Ny teknologi kan utgjøre en risiko dersom foretak tar i bruk teknologien før den er tilstrekkelig utprøvd, og før forståelsen av hva bruken innebærer, er etablert.

Robotisert prosessautomatisering (RPA)

Robotisert prosessautomatisering (RPA) går i enkelthet ut på at man bruker et spesialisert utviklingsverktøy for RPA til å lage et program som skal utføre samme oppgave som en medarbeider. Et slikt program utfører da den samme serie/sekvens av handlinger medarbeideren utfører når en arbeidsoppgave gjennomføres. Et slikt program omtales gjerne som en BOT, som er en forkortning for robot.

Eksempel på funksjonalitet/handlinger som en BOT kan utføre er pålogging til ulike systemer, søk/oppslag i et eller flere systemer for å hente ut data som skal inngå i behandlingen, kopiering av data fra et system til et annet, ulike beregninger og håndtering av korrespondanse.

Manglende koordinert innføring, med involvering av ledelse, IT-avdelingen, compliance- og risikofunksjonen kan gi utfordringer med styring og kontroll av anvendelsen av RPA.

Tidlig involvering av compliancefunksjonen vil reduseres risikoen for at RPA-løsningen ikke utformes og etableres i henhold til gjeldende regelverk og interne retningslinjer og rutiner. Risikofunksjonen må sørge for å ha kontroll både med risikoen som RPA-teknologien utgjør, og risikoen i den enkelte automatiserte prosess i foretaket. Eksempel på risikoer/konsekvenser som bør vurderes, i tillegg til de tekniske, er økonomisk/forretningsmessig, feil/avvik (kvalitet), evnen til å produsere/levere, nøkkelpersonrisiko, evnen til å korrigere feil (kunnskap og/eller tilgang på kunnskap) og hvordan endringer i RPA og i tilliggende systemer/infrastruktur kan påvirke leveransene til foretaket.

RPA må underlegges samme regime for styring og kontroll som øvrig IKT-virksomhet for å redusere risiko knyttet til patching, endringshåndtering (test/produksjonssetting), logging, overvåkning, avvikshåndtering og rapportering.

Den tekniske implementeringen av RPA vil kunne ha sikkerhetsmessige konsekvenser ved at det introduseres sårbarheter i måten RPA-programvaren kommuniserer med systemene som inngår i RPA-prosessen.

For å unngå at brukerid og passord kommer på avveie, noe som kan resultere i datalekkasje, brudd på personvern, interne misligheter mv., er det viktig å ha kontroll med hvem som kan se og endre passord og tilganger.

RPA-prosessen (BOT) bør kun settes opp med de rettigheter som er nødvendige for å kunne utføre arbeidsoppgaven den er tildelt. Foretaket må sørge for at det finnes teknisk funksjonalitet som hindrer eksponering av brukeridentitet og passord når informasjonen sendes/overføres fra RPA til systemer som inngår i RPA-prosessen. Foretaket bør vurdere metoder for kryptering for lagring av brukerid/passord, samt hindre at dette blir blottlagt i klartekst i de skript som styrer RPA-prosessen. Samme krav til skjerming gjelder også for persondata og sensitiv informasjon for innsyn i flyten i prosessene og de produserte resultatene (output) fra RPA-prosessen.

Avhengighet av RPA i produksjonen av tjenester vil kunne utgjøre en sårbarhet dersom foretaket ikke har etablerert mulighet for alternativ håndtering/behandling (workarounds) dersom BOT skulle slutte å fungere.

I sammenheng med kontinuitetsarbeidet er det viktig å anerkjenne rollen RPA har som del av den totale virksomhetsarkitekturen. På lik linje med øvrig IKT-infrastruktur, er det nødvendig at det etableres beredskapsplaner, og at test av beredskapsplanene inngår som en naturlig del av IKT-kontinuitetsarbeidet.

AI og dataanalyse

Foretakene ønsker i større grad å bli datadrevne, som innebærer en faktabasert tilnærming hvor foretaket benytter tilgjengelige interne og eksterne data (Big Data) for å underbygge beslutninger fremfor å bruke skjønn og synsing. Typer av beslutninger foretaket søker å underbygge er hvordan foretaket best når målsettinger om økt lønnsomhet, reduksjon i kostnader, forbedrede kundeopplevelser, økt kundelojalitet mv. Overgangen til en mer datadrevet organisasjon påvirker forretningsstrategi, teknologianvendelse og hvordan foretaket drives. Hele foretaket vil ikke bli datadrevet over natten, men vil skje gradvis ved at foretaket endrer hvordan data samles inn, struktureres, prosesseres og presenteres som beslutningsgrunnlag for de ulike målsettingene.

Overordnet kan man si at Big Data (BD) er et samlebegrep for både samlingen av tilgjengelige data og teknologien som håndterer store volumer av ulike typer data. Avansert analyse er et samlebegrep for teknikker for å analysere ulike problemstillinger. Når BD skal analyseres, benytter foretakene seg i økende grad av avanserte analyseteknikker (AA = Advanced Analytics). Eksempel på slike teknikker er preskriptiv analyse (hva, når og hvorfor skjer ting) og prediktiv analyse (hvordan kunder handler og reagerer gitt ulike situasjoner). I begrepet avansert analyse inngår også bruk av verktøy for maskinlæring (ML), som er en undergruppe av kunstig intelligens (AI). Ved bruk av moderne verktøy er man i dag i stand til å gjøre meningsfulle analyser av data lagret på hvilket som helst format (tekst, regneark, dokumenter, bilder, tale, video m.fl.).

For gjennomgang av noen av risikoene knyttet til det datadrevne foretaket, tar vi utgangspunkt i de to temaene Big Data (BD), og avansert analyse (AA). Gjennomgangen baserer seg på rapport[44] utarbeidet i regi av den europeiske Banktilsynsmyndigheten (European Banking Authority), der Finanstilsynet har vært en av bidragsyterne.

Rapporten definerer fire pilarer som viktige for å ha kontroll med implementering og bruk av avansert analyse:

- Foretaket må ha etablert en dataforvaltning som har fokus på datakvalitet, datasikkerhet og overholdelse av regulatoriske krav for lagring og bruk av data.
- Det må etableres en teknologisk infrastruktur som er innrettet med tilstrekkelig behandlings- og lagringskapasitet, og dataplattformer og verktøy som støtter opp om bruken av avansert analyse.
- Det må etableres styring og kontroll gjennom en hensiktsmessig organisering, nødvendig opplæring, og et regime for hvordan BD og AA skal håndteres i hele foretaket.
- Foretaket må etablere en analysemetodikk som gir føringer for utvikling, implementering og bruk av AA. Et prosjekt for AA følger en livssyklus med faste steg som er forskjellig fra tradisjonelle IT-utvikling. Eksempelvis utgjør et maskinlæringsprosjekt (ML) stegene datapreparering, modellering og overvåkning.

Problemstillinger knyttet til bruk av data (hvilke data), nøyaktighet i data (integritet), forklarbarhet i løsninger (grunnlag for konklusjon), muligheter for å revidere/etterprøve svar (historikk), og etikk (bruk av data og resultater) er kjent for foretakene. Manglende kontroll innen et eller flere av nevnte forhold kan resultere i tap av omdømme og tillit, og de negative konsekvensene kan forsterkes ved bruk av BD og AA.

Etikk

Ved anvendelse av moderne analyseteknikker, herunder maskinlæring og kunstig intelligens, IT-verktøy og Big Data, har man muligheter for å finne nye forklaringsvariabler og flere sammenhenger. Foretakene bør derfor være særskilt oppmerksom på de etiske dilemmaene som bruken av AA og BD gir. Utvikling, implementering og bruk AA-løsninger bør baseres på noen grunnleggende etiske prinsipper. Dette vil påvirke styringsstrukturen for prosjekter knyttet til AI. Som eksempel kan det innføres en rutine der ethvert AA-basert prosjekt gjennomgår en etisk vurdering (av ledelse, eller en etisk komite) før det besluttes oppstart. Temaer knyttet til AI og etikk er omhandlet i "Ethics guidelines for trustworthy AI"[45] som er utarbeidet av Europakommisjonens High-Level Expert Group on AI.

[44] Final Report on Big Data and Advanced Analytics EBA
[45] Ethics guidelines for trustworthy AI European Commission

Muligheter for å forklare og tolke (Explainability og interpretability)

Man nevner transparens som grunnlag for å bygge pålitelige modeller, noe som handler om å gjøre data, funksjoner, algoritmer og treningsmetoder tilgjengelige for ekstern inspeksjon.
En modell kan forklares når dens indre oppførsel kan forstås direkte av mennesker (tolkbarhet), eller når forklaringer (begrunnelser) kan gis med bruk av hovedfaktorene som har ført til sluttresultatet. Kravet til forklarbarhet er større når beslutninger har direkte innvirkning på kunder/mennesker. Mangel på forklarbarhet kan også påvirke tillit og risiko dersom man anskaffer modeller som er utviklet av eksterne tredjeparter og som leveres som en 'black box" (ugjennomsiktig) løsning.

Rettferdighet og unngåelse av skjevhet (Fairness and avoidance of bias)

Rettferdighet krever at modellen sikrer beskyttelse av grupper mot (direkte eller indirekte) diskriminering. Diskriminering (tilsiktet eller utilsiktet) oppstår når en gruppe mennesker (med spesielle delte kjennetegn) påvirkes mer negativt av en beslutning (f.eks. resultatet fra en AI-/ML-modell) enn en annen gruppe. Diskriminering kan være en konsekvens av skjevhet i dataene når dataene ikke er representative for den aktuelle befolkningen. For å sikre rettferdighet, må AA-modellen være fri for skjevhet. Teknikker for å forhindre eller oppdage skjevhet finnes allerede. Det utvikles fortsatt nye teknikker og er et felt det forskes på.

Sporbarhet og muligheter for revisjon

For å kunne være trygg på at man har en modell som kan revideres, vil anvendelsen av et IT-verktøy som kan spore alle trinn, kriterier og valg gjennom hele utviklingsprosessen være til hjelp. Det vil da i ettertid være mulig å undersøke og repetere prosessene som resulterte i beslutningene i modellen.

Datakvalitet

Foretaket må være løpende opptatt av datakvalitet i alle stegene i analyseprosessen, også etter at modellen er tatt i bruk. At kvaliteten på grunnleggende dataelementer er tilfredsstillende, bidrar til å bygge tillit til modellen.

Sikkerhet

Nye teknologier, slik som AA gir muligheter for nye angrepsmåter, og gjør at det oppstår nye sårbarheter. Det er derfor viktig at foretaket overvåker den siste utvikling i typer av sikkerhetsangrep og forsvarsteknikker. Basert på en slik overvåkning/innsikt sørger man for at foretaket har tilstrekkelig styring og kontroll (governance) og en teknisk infrastruktur på plass som kan håndtere risiko knyttet til AA forbindelse med IKT-sikkerhet.

Data og resultater knyttet til AA-modellen må være tilstrekkelig beskyttet i samsvar med gjeldende databeskyttelsesregulering.

Forbrukerbeskyttelse

Forbrukere må forvente at de kan sende inn en klage og motta en forklaring på vanlig språk som kan forstås. At svaret fra modellen kan forklares (explainability) er nøkkelen for å løse denne forpliktelsen.

Blokkjede

Det kan sies at blokkjede fikk sin renessanse gjennom kryptovalutaen Bitcoin. Erfaringene som er gjort gjennom etterfølgende etablering av et høyt antall kryptovalutaer, og hvor bruk av teknologien vurderes og benyttes av både sentralbanker og foretak, er tydelige indikasjoner på at blokkjede er en teknologi som i vesentlig grad vil ha betydning for foretakene i årene fremover. Blokkjedeteknologi kan gi økt konkurranse, og økt risiko for tap av markedsandeler, ved at andre, ikke-finansielle aktører utvikler nye tjenester og etablerer tjenester i ny drakt. Teknologien vil blant annet kunne benyttes innen betalingstjenester, oppgjørsfunksjoner, Trade Finance og innen forsikring. Gartner har i en analyse[46] vurdert at frem til 2023 vil det være mye prøving og feiling, og at en stor del av dagens blokkjede-plattformer i løpet av den nærmeste tiden vil være utdatert.

Blokkjede er fortsatt en umoden teknologi, og det er begrenset med kompetanse innen området. Finanstilsynet mener risikoen ved bruk av teknologien i forretningsprosessene kan misforstås eller overses. Finanstilsynet ser det derfor som viktig at bruken vurderes nøye, og at bruken understøtter forretningsprosesser der dette er hensiktsmessig. Dette betyr at bruken må samsvare med de strategiske målene. Det er også viktig at foretak bygger nødvendig kompetanse, herunder forståelsen av asymmetrisk kryptering og distribuerte systemer (offentlig og privat), og at forretningssiden som ønsker å benytte teknologien i sine prosesser forstår hva bruken av teknologien innebærer. Dette kan være hvordan transaksjoner mellom banker gjennomføres, og forståelsen av sikkerhetsmekanismene, og hvordan bruken av smarte kontrakter skjer i henhold til juridiske krav.

[46] Gartner 2019 Hype Cycle Shows Most Blockchain Technologies Are Still Five to 10 Years Away From Transformational Impact

10 – Cyberforsikring

EUs strategi om et velfungerende felles digitalt marked[47] har som mål at personer og foretak skal ha tilgang til digitale goder og tjenester i et marked med rettferdig konkurranse, godt person- og forbrukervern og der databehandlingen utføres med tilstrekkelig sikkerhet uavhengig av personens eller foretakets geografiske lokalisering.

For å bidra til et velfungerende digitalt marked innen EU/EØS, har den europeiske forsikringsmyndigheten, European Insurance and Occupational Pensions Authority (EIOPA), utarbeidet en strategi (Cyber Underwriting Strategi[48]) for utvikling av forsikringsprodukter med sikte på å bedre foretakenes operasjonelle og økonomiske evne til å håndtere cyber-angrep. Denne typen forsikringsdekninger omtales gjerne med samlebegrepet cyberforsikring. Ytelsene foretakene kan motta fra forsikringsdekningene kan omfatte både økonomisk kompensasjon og tjenester/spesialistkompetanse for å reetablere normal drift. EIOPA antar at utviklingen av denne typen forsikringsprodukter med tilhørende forsikringsvilkår direkte og indirekte vil bidra til at:

- kundene (personer/foretak) erkjenner risikoen for økonomisk tap som følge av digitale angrep
- investeringer i risikoreduserende tiltak lønner seg (risikobaserte premier)
- foretak vil ha insentiver til å bedre sin kunnskap om styring av IT-sikkerhet og -risiko
- det etableres og utvikles til dels standardiserte tjenester som forsikringsforetakene tilbyr i forbindelse med cyber-angrep, og når normal driftssituasjon skal gjenopprettes etter angrep.

Basert på erfaringene fra tilsyn med finansforetak, oppfatter Finanstilsynets at det er ulike syn på hvordan forsikringsdekninger kan redusere finansiell og operasjonell risiko også blant store finansforetak. Argumentasjonen fra de som mener det er unødvendig med denne type forsikring, tar utgangspunkt i at IKT-virksomheten er utkontraktert, og at det er utkontrakteringspartneren som bærer denne risikoen.

[47] EU-kommisjonen: A digital single market strategy for Europe
[48] Cyber Underwriting Strategi EIPOA

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00
post@finanstilsynet.no
finanstilsynet.no

05.2020