FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Finanssektorens bruk av informasjons- og kommunikasjonsteknologi (IKT)

RISIKO- OG SÅRBARHETSANALYSE (ROS)

2021

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

1 Oppsummering

Den finansielle infrastrukturen i Norge er robust. I 2020 var det ingen IKT-hendelser med konsekvenser for finansiell stabilitet. Det var flere sikkerhetshendelser i 2020 enn i 2019, men færre operasjonelle hendelser. Samlet økte antall IKT-hendelser noe. Ut fra hendelsenes varighet, tidspunkt og antall berørte brukere har Finanstilsynet vurdert tilgjengeligheten til betalingstjenester og andre kunderettede tjenester i 2020 samlet sett som tilfredsstillende, men noe dårligere enn i 2019.

Det ble i tillegg til IKT-hendelser også rapportert flere avvik knyttet til kontotilbyderes dedikerte grensesnitt for tredjeparts betalingstjenestetilbydere. Avvikene gjaldt både tilgjengeligheten til grensesnittene og mangler i grensesnittenes funksjonalitet.

Finanstilsynet leder og er sekretariat for Beredskapsutvalget for finansiell infrastruktur (BFI). Utvalget følger opp beredskap og hendelser i den finansielle infrastrukturen. Under koronapandemien har Finanstilsynet og Beredskapsutvalget for finansiell infrastruktur (BFI) rettet særlig oppmerksomhet mot virksomheter som støtter viktige funksjoner, herunder kritiske samfunnsfunksjoner definert av Direktoratet for samfunnssikkerhet og beredskap. De sentrale foretakene i den norske finansielle infrastrukturen har gjennomgående gode beredskapsplaner. Aktørene har 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. Hendelser i 2020 avdekket imidlertid alvorlige sårbarheter hos enkelte foretak. Foretakene arbeider kontinuerlig med å styrke forsvarsverket, og angrep avverges hovedsakelig før de får alvorlige konsekvenser. 21 av de 211 rapporterte IKT-hendelsene i 2020 var sikkerhetshendelser og omfattet både digital kriminalitet og avdekkede sårbarheter, som SolarWind-saken, uten at sårbarhetene ser ut til å ha blitt utnyttet.

Gjennom tilsyn har Finanstilsynet observert sårbarheter som utgjør risiko for alvorlige hendelser i finanssektoren. Finanstilsynet har blant annet påpekt svakheter i foretaks arbeid med IKT-risiko, at leverandøravtaler ikke gir foretak rett til å kontrollere leverandører og risiko som følge av at leverandører har ansvar for applikasjonsutvikling og samtidig har tilgang til produksjonsmiljøet. Det ble også påpekt utilstrekkelig oppfølging av tilgangsrettighetene til ansatte hos leverandører og mangler i foretakenes løsninger for overvåking av transaksjoner for å avdekke hvitvasking og terrorfinansiering. Finanstilsynet har også merket seg utfordringer i styring og kontroll av IKT-virksomheten der foretak er del av en gruppe. Det er også avdekket svakheter innen kontinuitets- og kriseledelse, blant annet ved utarbeidelse av forretningsmessige konsekvensanalyser (Business Impact Analyses) som grunnlag for kriseløsningene. Videre er det avdekket svakheter knyttet til at tester og øvelser ikke omfatter scenarioer som dekker både tekniske avbrudd og ondsinnede angrep, og utilstrekkelig testing av flytting av drift til sekundært driftssted.

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

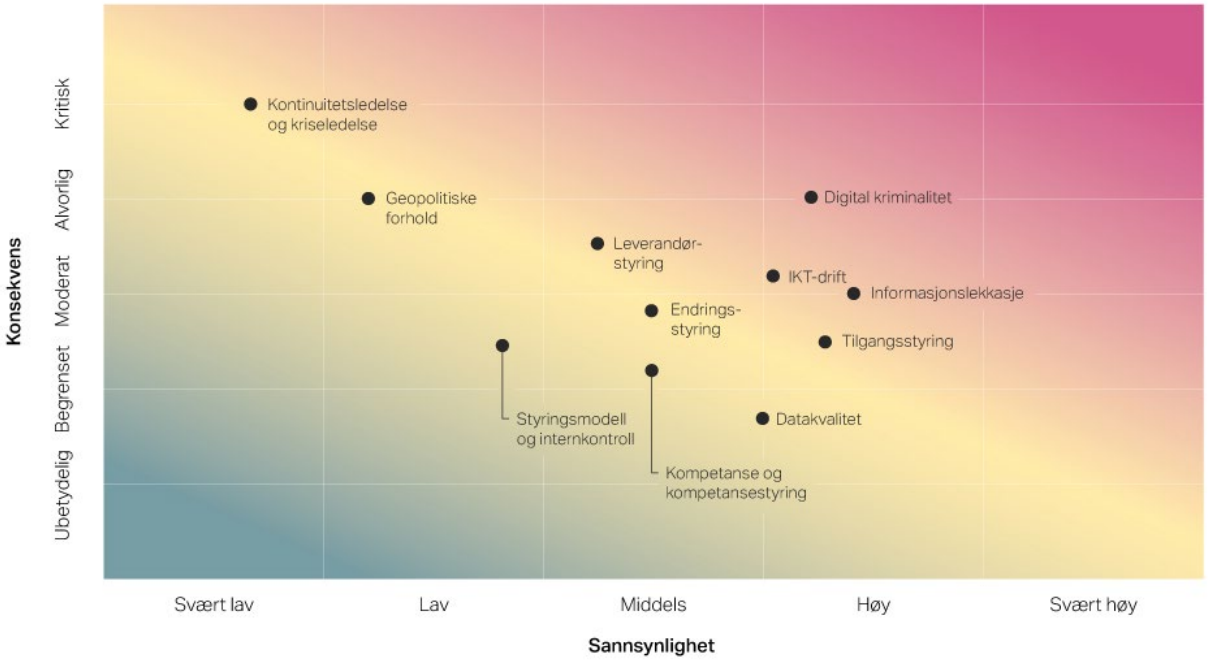
Risiko knyttet til sårbarheter og trusler i foretakenes IKT-virksomhet

Finanstilsynet vurderer sårbarheter knyttet til foretaks forsvarsverk mot digital kriminalitet og IKT-drift som de to mest sentrale truslene knyttet til foretakenes bruk av IKT, der den samlede risikoen vurderes til å være høy. Informasjonslekkasje er også en sentral trussel, der den samlede risikoen vurderes som middels til høy. Mens risikoen knyttet til foretaks forsvarsverk mot digital kriminalitet er vurdert som noe høyere i 2020, er risikoen for informasjonslekkasje vurdert å være noe lavere.

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

I figuren oppsummerer Finanstilsynets vurdering av områder med de mest sentrale truslene og sårbarhetene i finanssektoren. De ulike risikoområdene er klassifisert etter sannsynlighet for at en alvorlig negativ hendelse oppstår, og den tilhørende konsekvensen etter alvorsgrad for det enkelte foretak. Observasjoner og vurderinger som ligger til grunn for klassifiseringen, framgår 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 Finanstilsynets vurdering av risiko knyttet til sårbarheter og trusler



Kilde: Finanstilsynet

Tabell 1.1 Sårbarheter og trusler som kan utgjøre en risiko for uønskede hendelser

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 teknisk 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, økt bruk av skytjenester, manglende oppfølging av teknisk gjeld og mangelfull overvåking av IT-miljøet 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 brudd 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 og feil i risikovurderinger.	→

Kilde: Finanstilsynet

Foretakenes vurdering av risiko

Foretakenes vurderinger av operasjonell risiko og sikkerhetsrisiko, slik dette framkommer i deres rapportering og i dialog med foretakene, viser blant annet at

- fortsatt høy kompleksitet i systemporteføljen og stor teknisk gjeld medfører risiko på en rekke områder. Blant annet er IKT-porteføljen delt på flere plattformer og flere leverandører, noe som gir en mer krevende leverandøroppfølging.
- det er, som tidligere år, middels til høy risiko knyttet til tilgang på nødvendig kompetanse, særlig innenfor informasjonssikkerhet.
- det er økt risiko knyttet til mengden av ny eller endret regulering som medfører behov for endringer i IKT-systemene. Rapporteringen av hendelser viser at mange av feilene skyldes endringer.
- halvparten av foretakene mener det er middels risiko for at de ikke har tilstrekkelig oversikt over virksomhetskritisk IKT-utstyr og programvare.
- et flertall av foretakene mener det er middels til høy risiko for at de ikke har tilstrekkelig oversikt over de ulike kontrolltiltakene i virksomheten. Flere foretak viser til at der IKT-driften er utkontraktert, blir også mye av kontrollarbeidet utført av leverandøren.
- de fleste foretakene vurderer risikoen som middels eller høy for at ikke alle betalingstransaksjoner blir fanget opp av systemene for transaksjonsovervåking.
- foretakene ser at digitale angrep fra kriminelle aktører blir stadig mer sofistikerte, og at enkelte foretak mener det fortsatt er høy risiko for dataangrep og et behov for ytterligere sikkerhetstesting. Flere foretak viser også til behov for ytterligere IKT-sikkerhetstiltak.
- mange av foretakene har iverksatt eller planlegger tiltak for å redusere risikoer.
- svært mange av foretakene ser behov for å iverksette ytterligere tiltak for å beskytte brukerne av betalingstjenester mot svindel og andre uønskede hendelser.

Risiko knyttet til kunders bruk av digitale tjenester

Digitaliseringen gir nye og ofte bedre og billigere tjenester. Samtidig skapes det nye risikoer, både for tjenesteytere og for deres kunder.

Bruk av ID-løsninger er et av disse risikoområdene. BankID har blitt en form for "universalnøkkel" for tilgang til både privat og offentlig tjenesteyting, uten at brukere kan reservere seg mot bruksområder og redusere mulighetsrommet for misbruk. Tilliten til ID-løsninger gjør at det i liten grad har vært etablert supplerende kontroller i samsvar med risikoen, slik som ved større låneopptak. At BankID benyttes "overalt hele tiden", kombinert med at konteksten som innloggingen skjer i varierer, medfører risiko for at brukerne ikke er tilstrekkelig årvåkne og kan bli lurt til falske innlogginger.

Et annet risikoområde er knyttet til betalingstjenestene og tjenester der betalingstjenestene benyttes, der stadig mer funksjonalitet blir automatisert og integrert i betalingstjenestene. Det kan være vanskelig for brukerne å overskue konsekvensene ved endringer i "relasjoner" mellom blant annet betalingsmottaker, betalingsmottakers tjeneste, betaler og betalingstjenesten. Et eksempel er

parkeringsapper der betalingskortnummer er knyttet opp mot registreringsnummeret til en bil, som siden kan bli solgt uten at eier tenker på at parkeringsappen må oppdateres.

Mangel på informasjon om betalingstjenester, knyttet til for eksempel endringer i bruken av disse, kan innebære en risiko for at brukerne ikke får gjennomført kjøp eller andre ønskede handlinger. Et eksempel på dette var brukere som ikke fikk gjennomført kjøp av billetter i Ruters app, etter at det fra 1. januar 2021 ble innført krav om sterk kundeautentisering ved bruke av betalingskort ved handel på internett.

Tap knyttet til svindel

Svindelrapporteringen ble noe endret fra og med andre halvår 2019 som følge av innføringen av det reviderte betalingstjenestedirektivet (PSD2). På enkelte områder vil det derfor bare være relevant å sammenligne 2020-tallene med tilsvarende tall for andre halvår 2019.

I 2020 var det 205.000 svindeltransaksjoner med kort, mot 110.000 i andre halvår 2019, noe som indikerer at omfanget var omtrent uendret. Tapene på kortsvindel utgjorde 148 mill. kroner, mot 189 mill. kroner i 2019, en nedgang på 22 prosent. Totalt ble det gjennomført i underkant av 2,5 milliarder betalinger med kort i 2020. Av disse utgjorde svindeltransaksjoner 0,008 prosent. Andelen var størst for grensekryssende transaksjoner. Svindeltransaksjoner utgjorde hele 0,3 prosent av antall transaksjoner med land utenfor EØS-området i 2020.

For kontooverføringer, hovedsakelig nettbank, utgjorde tapene 355 mill. kroner i hele 2020, mot 301 mill. kroner i andre halvår i 2019 alene. Av dette utgjorde svindel ved sosial manipulering, dvs. der betaler er lurt til å iverksette svindeltransaksjonen, 250 mill. kroner. Selv om antall svindelforsøk økte fra 2019 til 2020, ble de samlede tapene redusert med ca. 50 prosent. Reduksjonen er trolig en konsekvens av bankenes intensiverte arbeid med å avdekke denne type svindel, samt økt oppmerksomhet i befolkningen om svindel ved sosial manipulering.

Utkontraktering av IKT og melding om betalingstjenester

Finanstilsynet mottok i 2020 over 250 meldinger om utkontraktering. Flest meldinger gjaldt endringer knyttet til leverandører av felles betalingsinfrastruktur til bankene, herunder Nets' salg av konto-til-konto-tjenester til Mastercard og Vipps' planlagte flytting av driften av BankID, samt oppstart av Kontanttjenester i butikk. Det har vært behov for omfattende oppfølging av bankenes meldinger knyttet til Nets' salg til Mastercard og bytte av driftsleverandør for BankID.

Meldingene om utkontraktering viser, som de foregående årene, en tendens til økt bruk av skytjenester for både applikasjons- og infrastrukturtjenester. Dette medfører ofte et økt antall plattformer foretakene må forholde seg til, som for eksempel systemer hos en driftsleverandør i kombinasjon med ulike skytjenester. Det gir økt kompleksitet og et mer sammensatt risikobilde.

Kvaliteten på foretakenes analyser og vurderinger av risiko forut for gjennomføring av IKT-utkontrakteringer synes å øke. Kvaliteten på avtaler med leverandører, samt foretakenes forankring av

avtaler om utkontraktering i egen ledelse, viser også en positiv utvikling. Enkelte foretak må imidlertid forbedre sitt arbeid med utkontrakteringer.

Av søknadene om konsesjon til å yte betalingstjenester framgikk det at flere foretak hadde mangelfull forståelse av regelverket knyttet til utkontraktering og vesentlige svakheter i egne rutiner.

Finanstilsynets oppfølging av foretakene

Hovedtema for tilsynsvirksomheten i 2021 er:

- foretakenes styring og kontroll av IKT-virksomheten
- foretakenes organisering av IKT-/cybersikkerhetsarbeidet
- sikkerhet 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 (PSD2), med særlig vekt på bankenes grensesnitt for tiltrodde tredjeparters tilgang til kunders betalingskonto
- større endringer i den finansielle infrastrukturen
- foretakenes IKT-løsninger for å avdekke hvitvasking og terrorfinansiering, og bankenes tilbud av kontanttjenester og kontantberedskap

Finanstilsynet følger opp IKT-hendelser hos foretakene. Det vektlegges at foretakene avdekker årsaker og iverksetter forebyggende tiltak. 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 følges 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 koronapandemien, vil BFI særlig følge opp IKT-virksomheten hos de viktigste aktørene.

For nærmere omtale av Finanstilsynets oppfølging av foretak under tilsyn, se vedlegg 3.

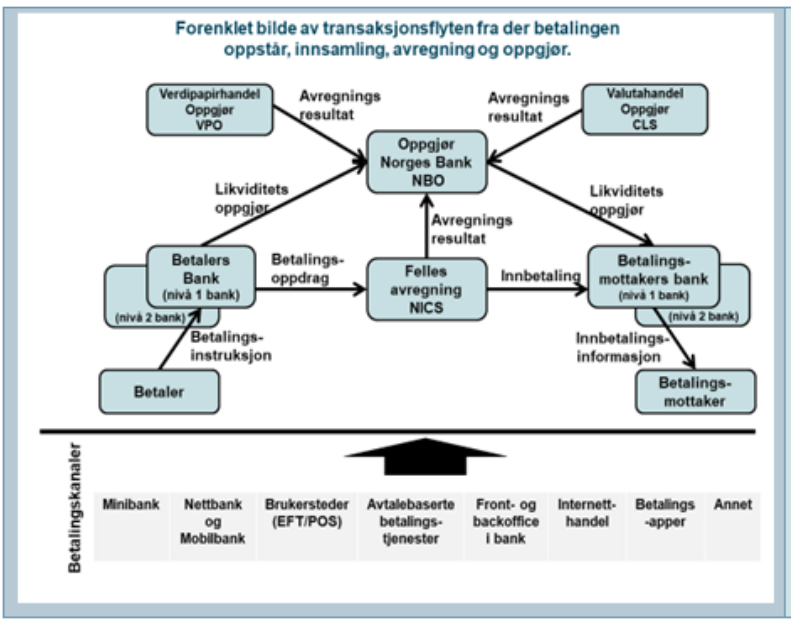
2 FINANSIELL INFRASTRUKTUR

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

Betalingssystemet omfatter 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 i lovverket blant annet gjennom betalingssystemloven, forskrift om systemer for betalingstjenester og forskrift om betalingstjenester, samt gjennom finansnæringens selvregulering forvaltet av Finans Norge og Bits.

Transaksjonsflyten i det norske betalingssystemet



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

Kilde: Finanstilsynet

Verdipapirsektoren reguleres gjennom blant annet verdipapirhandelloven, verdipapirforskriften og verdipapirsentralloven. Verdipapirsektoren 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[1] har utpekt finansielle tjenester som samfunnskritisk funksjon. Videre angir sikkerhetsloven økonomisk stabilitet og handlefrihet, som bl.a. omfatter stabilitet i den finansielle infrastrukturen og finansmarkedene, og samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet, som omfatter infrastruktur og objekter som er avgjørende for at sivilsamfunnet skal fungere, som nasjonale sikkerhetsinteresser[2].

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 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 infrastruktur som el-forsyning og telekommunikasjon, herunder nettverk.

Finanstilsynet og Norges Bank samarbeider om tilsyn med 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 2020 ingen større IKT-hendelser som hadde konsekvenser for finansiell stabilitet. Tjenestenes driftsstabilitet var tilfredsstillende.

Det var samlet sett noen flere hendelser i 2020 enn i 2019. Mens det var flere sikkerhetshendelser i 2020 enn i 2019, var det færre operasjonelle hendelser. Selv om det ble rapportert noen færre operasjonelle hendelser, har Finanstilsynet ut fra hendelsenes varighet, tidspunkt og antall berørte brukere vurdert tilgjengeligheten til betalingstjenester og andre kunderettede tjenester som noe dårligere i 2020.

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

Det var i 2020 i hovedsak god regularitet på avregnings- og oppgjørssystemene, selv om det var enkelte 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. Imidlertid ble det i 2020 funnet noen alvorlige sårbarheter hos enkelte foretak. Selv om sårbarheter har blitt avdekket og alvorlig operasjonell svikt med store konsekvenser har forekommet, er systemkriser foreløpig unngått.

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

2.3 Endringer i den finansielle infrastrukturen

Det ble i løpet av 2020 gjennomført og varslet flere vesentlige endringer i den norske finansielle infrastrukturen, herunder for sentral tjenesteyting. Enkelte av endringene realiseres i 2021 og 2022.

Nets[3], som var leverandør til blant annet det norske avregningssystemet NICS, felles operasjonell infrastruktur (FOI) [4], BankAxept, BankID og flere av bankenes betalingstjenester, har solgt sine konto-til-konto-tjenester (avregning, sanntidsbetalinger samt betalinger av digitale regninger, inkludert AvtaleGiro/eFaktura) til Mastercard. Endringen trådte i kraft 5. mars 2021.

For den resterende delen av Nets, som omfatter blant annet forhandlertjenester, kortutsteder- og innløsertjenester og digitale sikkerhetstjenester (Merchant Services og Issuer & eSecurity Services) har Nets inngått en fusjonsavtale med italienske Nexi[5], med Nexi som overtakende selskap. Det innebærer at øvrige deler av den norske betalingsinfrastrukturen, eid av bankene frem til 2014, også er gjenstand for vesentlige endringer i eierskap. Endringen forventes gjennomført i andre kvartal 2021.
BankID, den sentrale ID-løsningen innenfor finanssektoren som også offentlig sektors tjenester overfor publikum er en stor bruker av, har siden etableringen vært driftet av Nets. BankID er en felles operasjonell infrastruktur (FOI)[4] som fortsatt eies av bankene. Vipps besluttet i 2018 å skifte leverandør for drift og forvaltning av BankID-infrastruktur fra Nets til DXC[6]. Flyttingen har blitt utsatt flere ganger og er nå planlagt gjennomført i 2021.

[3] Nets Norge Infrastruktur AS og Nets Branch Norge, nå Mastercard Payment Services Infrastructur AS og Mastercard Payment Services Norge AS
[4] Felles Operasjonell Infrastrukturer omfatter E-faktura, Konto- og Adresseregisteret (KAR) og løsning for straksbetalinger. I tillegg omfattes også BankAxept og BankID
[5] Nexi S.p.A https://www.nexi.it/en.html
[6] DXC Technology Norge AS

Samlet innebærer disse endringene en større fragmentering av eierskapet til og drift av den finansielle infrastrukturen i Norge og kan bidra til redusert konsentrasjonsrisiko.

Bankene i Eika Alliansen har siden 2004 benyttet danske SDCs bankløsninger. Eika Alliansen inngikk i 2020 avtale med TietoEVRY om leveranse av kjernebankløsninger til lokalbankene i alliansen. Overgangen til TietoEVRYs løsninger forventes gjennomført i 2022–2023. Når overgangen er gjennomført, vil andelen norske banker som benytter TietoEVRY som driftsleverandør til finanssektoren, øke betydelig. Dette vil medføre høyere konsentrasjonsrisiko.

Bankene som har forlatt Eika Alliansen og dannet Lokalbank-samarbeidet, vil videreføre kjøp av bankløsninger fra SDC. SDC benyttes også av enkelte andre norske banker. Det innebærer at SDC fortsatt vil være en sentral driftsleverandør for den norske finansielle infrastrukturen.

DNB avviklet i 2020 sin Post i butikk-løsning, slik at det ikke lenger er mulig å få utført enkle banktjenester, som bl.a. kontanttjenester, ved Postens betjeningssteder. Med henvisning til den geografiske spredningen av Post i butikk vurderte Finanstilsynet i 2018 at det samlede tilbudet av kontanttjenester var tilfredsstillende. I 2020 ble Kontanter i butikk, basert på bruk av BankAxepts infrastruktur, etablert. Mer enn 90 banker har sluttet seg til tjenesten, noe som i stor grad kompenserer for nedleggelsen av Post i butikk.

I 2013 ble felles operasjonell infrastruktur for straksbetalinger (Straks FOI) etablert, og løsningen ble gradvis tatt i bruk av de fleste bankene. I løpet av 2021 vil bankenes straksbetalinger sendes direkte til avregningsløsningen Nics Real[7], og Straks FOI-en fra 2013 vil etter hvert bli sanert.

Euronext, som også opererer børsene i Frankrike, Belgia, Portugal, Nederland, Irland og Storbritannia, kjøpte i 2019 konsernet Oslo Børs VPS Holding ASA[8]. Kjøpet omfattet blant annet den regulerte markedsplassen Oslo Børs ASA og VPS ASA. Høsten 2020 tok Oslo Børs i bruk Euronexts handelsplassløsninger.

Innføring av muligheten for egen pensjonskonto[9] medførte stort behov for samhandling og informasjonsutveksling mellom arbeidsgivere, arbeidsgivers pensjonsleverandør, eventuelle selvvalgte leverandører og arbeidstakere for enkel flytting av pensjonskapitalbevis (PKB) mellom aktører i markedet. Det ble derfor besluttet å etablere et pensjonskontoregister som felles infrastruktur for samhandling. Pensjonskontoregisteret AS ble opprettet for å forvalte driften av pensjonskontoregisteret.

[7] Clearingløsningen i Norge for straksbetalinger
[8] https://no.wikipedia.org/wiki/Oslo_B%C3%B8rs
[9] Pensjonsopptjening fra innskuddspensjonsordninger på en egen pensjonskontohttps://lovdata.no/dokument/NL/lov/2000-11-24-81

2.4 Beredskapsutvalget for finansiell infrastruktur (BFI)

Beredskapsutvalget for finansiell infrastruktur (BFI)[10] er opprettet for å:

- komme fram til og koordinere tiltak for å forebygge og 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.
- forestå nødvendig koordinering av beredskapssaker innenfor finansiell sektor. Herunder skal det, på grunnlag av sivilt beredskapssystem, samordne utarbeidelse og iverksettelse av varslingsplaner og beredskapstiltak ved sikkerhetspolitiske kriser og krig.

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

2.5 Koronapandemien

Finanstilsynet har hatt stor oppmerksomhet rettet mot finansiell infrastruktur siden koronapandemien eskalerte i Norge. BFI hadde i mars, april og mai 2020 hyppige møter, og siden mer sporadiske møter, for å følge opp de sentrale foretakene i den norske finansielle infrastrukturen og deres ivaretakelse av god, sikker og stabil drift, jf. utvalgets mandat. BFI-møtene har bidratt til informasjonsutveksling om forhold som kan resultere i forstyrrelser i den finansielle infrastrukturen eller ha betydning for finansiell stabilitet, samt om tiltak som foretakene har iverksatt eller planlegger å iverksette. Aktørene viste at de hadde god kontroll på driftssituasjonen og iverksatte nødvendige tiltak. Finanstilsynet finner dette betryggende.

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

Finanstilsynet og BFI har rettet særlig oppmerksomhet mot virksomheter som støtter kritiske funksjoner, herunder funksjonene i finanssektoren som er definert som samfunnskritiske av Direktoratet for samfunnssikkerhet og beredskap. Dette er evnen 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

[10] Beredskapsutvalget for finansiell infrastruktur (BFI)

Som ledd i smittevernet for egne ansatte gjennomgikk flere foretak kritiske roller, funksjoner og bemanning og iverksatte tiltak som oppdeling av organisasjonen og klargjøring eller bruk av reservelokasjoner. Foretakenes tiltak ble revidert gjennom året i samsvar med utviklingen i pandemien. Foretakene utvidet kapasiteten for systemoppkobling hjemmefra og har under pandemien vært særlig oppmerksomme på den økte risikoen forbundet med arbeid fra hjemmekontor. 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. Det ble i de første månedene iverksatt strenge regimer med begrensning eller stans av endringer i IKT-systemene, men restriksjonene ble etter hvert myket opp. Oppfølgingen av kritisk drift og leverandører var tett. Bankenes og deres tjenesteleverandørers håndtering av kontanttjenester ble fulgt opp. I tråd med kriseplaner hentet enkelte foretak hjem driftsoperasjoner fra utlandet og beholdt av beredskapsgrunner en begrenset del av virksomheten i utlandet. Flere foretak gjennomgikk planene for den fysiske sikringen av lokalene, herunder lokasjoner for IKT-drift.

2.6 Samarbeid innen sikkerhetsområdet

Samfunnskritiske virksomheter i finanssektoren

I sikkerhetsloven[11] er økonomisk stabilitet og handlefrihet angitt som en av flere nasjonale sikkerhetsinteresser[2] 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. På Finanstilsynets ansvarsområde er det så langt ikke fattet slikt vedtak. Departementene skal også holde à jour oversikt over foretak av vesentlig betydning for GNF.

Foretak som understøtter en GNF, kan være mer utsatt for trusler fra utenlandsk etterretning. Det stilles derfor strengere krav til foretakets sikkerhetsarbeid, herunder underleverandører og samarbeidspartnere. Trusler fra utenlandske statlige aktører er beskrevet under punkt 3.5.1.

Samhandling og informasjonsutveksling gir bedre risikoforståelse

Samarbeid og erfaringsutveksling om informasjonssikkerhet mellom finansforetakene i Norge gjennom Nordic Financial CERT (NFCERT)[12] bidrar til å heve kunnskapen om det aktuelle trussel- og risikobildet og gjør foretakene bedre rustet til å håndtere digitale trusler og uønskede hendelser. NFCERT utarbeider regelmessig trusselrapporter. Finanstilsynet erfarer at foretak som ikke deltar i dette samarbeidet, kan være dårligere rustet til å håndtere digitale trusler og uønskede hendelser.

[11] Lov om nasjonal sikkerhet (sikkerhetsloven)
[12] Nordic Financial CERT

Finanstilsynet er utpekt av Finansdepartementet som sektorvis responsmiljø (SRM)[13] med oppgave å håndtere IKT-sikkerhetshendelser i finanssektoren innenfor Finanstilsynets ansvarsområde. Finanstilsynet utøver rollen sammen med NFCERT.

Finanstilsynet deltar som partner i Nasjonalt cybersikkerhetssenter, som er etablert av Nasjonal sikkerhetsmyndighet (NSM) for å styrke landets motstandsdyktighet og beredskap på det digitale feltet. Deltakelsen gir Finanstilsynet tilgang til oppdatert kunnskap om risikobildet på cybersikkerhetsområdet. Finanstilsynet kan gjennom senteret samhandle og utveksle informasjon med samarbeidspartnere og aktører ved håndtering av cybertrusler og -angrep. Gjennom partnersamarbeidet deltar Finanstilsynet også i NSMs SIG[14] IKT, som er et samarbeidsforum for myndigheter som fører tilsyn med IKT-sikkerhet i sin sektor.

Finanstilsynet og Norges Bank samarbeider om implementering og bruk av TIBER-rammeverket**Feil! Bokmerke er ikke definert.** (threat intelligence-based ethical red-teaming) for sikkerhetstesting i Norge og vil etablere nødvendige fora for overordnet oppfølging, styring og involvering av næringsaktører og andre relevante myndigheter. Hensikten bak TIBER-NO er å bidra til finansiell stabilitet gjennom økt motstandsdyktighet mot cyberangrep for kritiske funksjoner i det norske finansielle systemet. Se nærmere omtale under punkt 3.5.2.

[13] Rammeverk for håndtering av IKT-hendelser NSM
[14] SIG står for spesialinteressegruppe

3 FINANSTILSYNETS OBSERVASJONER OG VURDERINGER

3.1 Tilsyn med IKT og betalingstjenester

Det ble i 2020 gjennomført færre tilsyn enn planlagt der IKT og betalingstjenester var tema, og hovedårsaken var koronapandemien. De fleste tilsynene i 2020 ble gjennomført digitalt. Av de 18 tilsynene var fem i banker, tre i forsikringsforetak, fire i verdipapirforetak, to i inkassoforetak, ett i eiendomsmeglerforetak, to i revisjonsselskaper og ett i regnskapsførerforetak. To av tilsynene i bank var tematilsyn om antihvitvasking, hvor bankenes systemer for elektronisk overvåking av mistenkelige transaksjoner var en del av tilsynet.

3.1.1 Styring og kontroll

Finanstilsynet har gjennom tilsyn merket seg utfordringer i foretaks styring og kontroll av IKT-virksomheten der foretaket er del av en gruppe, og der gruppen på vegne av foretakene ivaretar deler av IKT-virksomheten. Å inngå i en gruppe gir foretaket fordeler i form av felles infrastruktur og tilgang til ressurser og spisskompetanse. Finanstilsynet ser imidlertid at enkelte foretak i grupper kan mangle egen risikoanalyse av IKT-virksomheten og egen IT-strategi, og at det blir flere ledd mellom foretaket og den utkontrakterte virksomheten. Det er risiko for rolleblanding og for at det oppstår misforståelser når det gjelder ansvar, roller og sikkerhetsnivå. Foretak skal uansett gruppetilhørighet sikre egen styring og kontroll av IT-virksomheten. Dette skal dokumenteres gjennom instrukser og rutiner som beskriver hvem som skal utføre hvilke kontroller og oppgaver.

3.1.2 Beredskap

Mangelfulle beredskapsplaner og manglende eller utilstrekkelig testing av kriseløsninger ble avdekket ved flere tilsyn i 2020. Finanstilsynet observerte at forretningsmessige konsekvensanalyser (Business Impact Analysis) hadde blitt utarbeidet på for svakt grunnlag og ikke ga et tilstrekkelig grunnlag for etablering av kriseløsningene. Det ble også observert at det manglet test av om kommunikasjonen i en krisesituasjon vil virke som forutsatt, både internt i foretaket og eksternt mot kunder og medlemmer av handelsplasser.

Finanstilsynet fant også at flytting av driften til sekundært driftssted ikke var tilstrekkelig testet. For en del foretak krever slik flytting mange manuelle operasjoner som det er spesielt viktig å teste, blant annet for å få fastslått at krav til gjenopprettelsestid kan etterleves. For handelsplassene i

verdipapirsektoren skal det ses hen til hvordan en flytting til sekundært driftssted påvirker medlemmene av handelsplassen.

Finanstilsynet har ved tilsyn påpekt betydningen av å gjennomføre øvelser med alvorlige sikkerhetshendelser (cyberhendelser) som tema. Foretakenes beredskap skal være et forsvar både mot operasjonelle hendelser og mot hendelser som følge av elektroniske angrep. Konsekvensene av hendelsene kan i første omgang være sammenfallende, og det kan ta tid før foretaket vet om hendelsen er operasjonell eller knyttet til sikkerhet. Beredskapen og kriseløsningene må omfatte begge typer hendelser. Tilsvarende må test og øvelser omfatte både scenarier der årsaken viser seg å være tekniske avbrudd, og scenarier der årsaken er ondsinnede angrep.

3.1.3 Hvitvasking og terrorfinansiering

Tilsyn med bankenes systemer for overvåking av mistenkelige transaksjoner knyttet til å avdekke hvitvasking og terrorfinansiering i 2020 viste at foretakene har etablert kundespesifikke regler. Slike regler har likevel redusert effekt når risikoklassifiseringen av kundene, som er utgangspunktet for riktig bruk av reglene, ikke er godt nok ivaretatt. Tilsynene avdekket også at kontrollfrekvensen ved bruk av de kundespesifikke reglene ikke var optimal og begrenset effekten av transaksjonsovervåkningen. Når alarmer ikke utløses i sanntid, øker risikoen for at hvitvasking og terrorfinansiering ikke avdekkes.

3.1.4 Leverandøroppfølging

Finanstilsynet avdekket ved flere tilsyn i 2020 at risikoen knyttet til utkontrakterte tjenester ikke syntes å være tilstrekkelig håndtert, herunder i oppfølgingen av leverandørene. I avtalene med leverandørene skal det vises til IKT-forskriften og foretakets rett til å kontrollere leverandørens aktiviteter. Selv om revisjonsforetak og regnskapsførerforetak ikke er underlagt IKT-forskriften, gjelder tilsvarende plikt etter risikostyringsforskriften[15].

Finanstilsynet pekte i flere tilsyn på den økte risikoen knyttet til at en leverandør har ansvar for applikasjonsutvikling og samtidig har tilganger i produksjonsmiljøet. Dette må håndteres med klare retningslinjer og strenge kontroller for å beskytte mot uønskede handlinger, enten bevisste eller ubevisste.

3.1.5 Sikkerhet

Tilgangsstyring

Som i tidligere år fant Finanstilsynet også i 2020 svakheter i tilgangsstyringen. Spesielt gjaldt dette foretakenes oppfølging av tilgangene til ansatte hos leverandører av utkontrakterte tjenester. Ved utkontraktering av IKT-virksomhet får ofte ansatte hos leverandøren utvidete brukerrettigheter. Feil bruk eller misbruk av utvidete brukerrettigheter kan forårsake stor skade. Det er derfor spesielt viktig for foretaket å ha kontroll med slike tilganger.

[15] Se punkt 7.1 Veiledning om utkontraktering, og punkt 6 i rundskriv 3/2020.

Sikkerhetstester

Gjennom tilsyn i 2020 observerte Finanstilsynet at stadig flere foretak bestiller sikkerhetstester fra tredjeparter. Som oftest er tredjepartene profesjonelle sikkerhetsselskap. Finanstilsynet vurderer at dette er et viktig bidrag til foretakenes testing av den digitale forsvarsevnen, men påpeker samtidig at slik testing bør gjennomføres i henhold til anerkjente standarder og beste praksis, og at foretaket bør ha dokumenterte retningslinjer og rutiner for dette. Retningslinjene bør blant annet beskrive hvordan, og hvor ofte, slike tester skal gjennomføres og premisser for valg av tredjepartsleverandør.

Finanstilsynet pekte også på at sikkerhetsnivået i e-post-løsninger bør heves gjennom bruk av anerkjente teknikker og sikkerhetsløsninger.

Finanstilsynet observerte at foretak mangler retningslinjer og rutiner for å bevisstgjøre og instruere ansatte om hvordan de kan skjule sin rolle og ansvar i foretaket for omverdenen for å redusere risikoen for sosial manipulering og trusler.

3.2 Risiko knyttet til betalingstjenester

Den offentligrettslige og delvis den privatrettslige delen av EUs reviderte betalingstjenestedirektiv (PSD2) ble innført i norsk rett 1. april 2019. PSD2 skal fremme innovasjon og konkurranse på like vilkår og gjennom dette bidra til et velfungerende marked for betalingstjenester.

De nye reglene definerer to nye foretakstyper; betalingsfullmektig og opplysningsfullmektig. Det er innført konsesjonsplikt for to nye betalingstjenester omtalt som fullmakttjenester, henholdsvis betalingsfullmakttjenester og kontoinformasjonstjenester. Videre er regler for sikker autentisering av betalere, fullmektiger og kontotilbydere, samt sikker kommunikasjon mellom disse, beskrevet i delegert kommisjonsforordning (EU) 2018/389 (RTS), som er inntatt i forskrift om systemer for betalingstjenester.

Finanstilsynet har etter innføringen av PSD2 identifisert følgende risikoer knyttet til betalingstjenesteområdet, herunder manglende etterlevelse av det nye regelverket:

Konkurransemessige forhold

- Tilgang til betalingskonto: En rekke banker tilbyr ikke fullmektiger grensesnitt, med tilhørende funksjonalitet og informasjon, som samsvarer med funksjonalitet og informasjon i egne brukergrensesnitt slik kravet er.
- Autentiseringsmekanismer: Banker gir ikke fullmektiger tilgang til samme brukervennlige autentisering av kunden som banken selv gjør bruk av.
- Avtaler: Banker har gjennom avtaler gitt enkelte tredjepartsleverandører fordeler når det gjelder enklere autentisering og bedre funksjonalitet i grensesnittene.

Mulige sårbarheter knyttet til nye tjenester og nye aktører

- Nye aktører har ikke nødvendigvis samme erfaring som de etablerte. Dette kan gi opphav til "oppstartrisiko" som følge av blant annet manglende kunnskap om sentralt lovverk og forventninger, mindre kunnskap om kunden, mindre erfaring med ytelse av betalingstjenester og utfordringer ved operasjonalisering av nye rutiner. Kravene som stilles for å få konsesjon, skal redusere slike sårbarheter. Etter at tillatelsen er gitt, stilles det krav om løpende rapportering av hendelser og risiko samt om status for foretaket.
- Reglene for sikker kommunikasjon og autentisering og tilsyn er de samme for alle aktører i Europa, og foretakene kan drive grensekryssende. For å sikre lik etterlevelse av regelverket følger den europeiske banktilsynsmyndigheten (EBA) aktivt opp de enkelte lands tilsynsmyndigheter og deres oppfølging av gjeldende regler, og har igangsatt aktiviteter for å harmonisere tilsynsvirksomheten til de nasjonale myndighetene.
- Nye tjenester øker risikoen for at kriminelle kan gå via tredjeparter, som kan ha svakere kontrollmiljø og lavere sikkerhet i sin portal, for å omgå bankenes sikkerhetsmekanismer. Det å sikre ende-til-ende sikkerhet for en transaksjon (sesjonssikkerhet) har alltid vært ansett som utfordrende. Introduksjon av tredjeparter i en betalingskjede, der brukeren rutes fra tredjeparten til banken for autentisering, gir prinsipielt ikke ny risiko. Bankene har lang tradisjon for å autentisere brukere og brukersteder, også når brukeren ikke er i nettbanken. Det som kan være utfordrende for bankenes sikkerhetsmekanismer, er at metadata de får fra tredjeparten om brukeren, kan være mangelfull eller vanskelig å tolke.
- Finanstilsynet er kjent med at tredjeparters betalingsfullmakttjenester er blitt benyttet av kriminelle. Betaler er blitt styrt til en falsk nettside og lurt til å registrere betalinger til en betalingsmottaker, der betalingsmottakers løsninger også synes å ha bli benyttet av de kriminelle.
- Nye aktører innebærer risiko for ugyldige sertifikater, enten at det er utstedt til en svindler eller at et utgått sertifikat skulle vært trukket tilbake. Bankene er etter regelverket pliktige til å kontrollere fullmektigers sertifikater. Et eventuelt misbruk vil legge igjen mange spor, som gjør at slikt misbruk normalt vil oppdages. I tillegg vil myndigheter bli underrettet om, eller være delaktige i, prosessen ved et tilbakekall (revokering) av sertifikater. Risikoen for et stort antall falske fullmektiger anses for liten.
- Nye aktører kan ha en risiko knyttet til etterlevelse av pliktene etter hvitvaskingsloven dersom de ikke får tilstrekkelig informasjon (som kundenavn) fra banken i forbindelse med betalinger

3.3 Foretakenes vurderinger av risiko og sårbarhet

Foretakenes vurderinger av risiko og sårbarhet er nedenfor omtalt med utgangspunkt i en ny årlig rapportering[16], en undersøkelse av digital sårbarhet besvart av en rekke foretak og innhentet informasjon gjennom dialog med en rekke foretak og leverandører av IKT-tjenester til finanssektoren.

3.3.1 Foretakenes vurdering av viktige forhold

Foretak og leverandører av IKT-tjenester har i samtaler med Finanstilsynet pekt på flere forhold knyttet til IKT-virksomheten som er viktige for foretakene, samt gjennomførte tiltak for å redusere risiko.

Innenfor området informasjonssikkerhet er det stor etterspørsel etter IKT-sikkerhetsressurser. Foretakene peker blant annet på at ressursmangelen kan bli en utfordring for gjennomføring av IKT-prosjekter. Utfordringen med å rekruttere informasjonssikkerhetskompetanse synes hovedsakelig å være færre tilgjengelige ressurser enn det markedet har behov for. Det kan synes som tilgjengelige ressurser foretrekker å knytte seg til foretak eller grupperinger som har et etablert sikkerhetsmiljø av en viss størrelse.

Foretakene har styrket sin interne kompetanse for både innkjøp og oppfølging av utkontrakterte IKT-tjenester. Dette har vært prioritert fordi erfaring tilsier at god innkjøpskompetanse gir bedre leveranser og tjenester fra IKT-leverandører.

Flere foretak peker på betydningen av kontakt med IKT-leverandører på både strategisk, taktisk og operasjonelt nivå for å sikre at IKT-tjenestene leveres i tråd med foretakenes behov.

Foretak med multi-leverandørstrategi erfarer at dette er krevende når det gjelder både teknologi og sikkerhet, og krever ofte spesialtilpasninger ("skreddersøm") som kan gi utfordringer for kompatibiliteten mellom ulike plattformer.

Foretakene mener det er viktig å ha tilstrekkelig innsikt i IKT-tjenesters sikkerhetsarkitektur. Det vil bidra til å forbedre den generelle sikkerheten gjennom å bruke kunnskapen til å stille krav til egen organisasjon og gjennomføre risiko- og sårbarhetsanalyser.

Phishing er fortsatt den mest brukte metoden for digital kriminalitet. Det var knyttet spenning til om koronapandemien ville medføre økt digital kriminalitet, men foretakenes erfaringer så langt tyder ikke på det.

[16] Forskrift om systemer for betalingstjenester stiller krav om at betalingstjenestetilbydere 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. Forskriften omfatter 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.

Bruk av tofaktor-autentisering er økende og ses på som viktig og nødvendig for å sikre at brukernes/ansattes Active Directory-konto ikke tas over av uvedkommende eller kriminelle ved innlogging fra andre lokasjoner enn VPN eller kontorets nettverk.

Foretakenes erfaringer knyttet til digital kriminalitet viser at sabotasje kan se ut til å være mer skadelig enn spionasje. Ved sabotasje er det i hovedsak løsepengevirus ("ransomware") som benyttes.

Angrepene fra kriminelle aktører blir stadig mer sofistikerte, og det er observert flere hendelser der infrastrukturleverandørers systemer er kompromittert.

Økt bruk av sårbarhetsskanning av nettverk og sperrer for å hindre uautoriserte apper er etablert for å unngå installasjon av uønsket kode.

Foretakene framhever at økt kompleksitet og et stadig mer krevende trusselbilde forverrer risikobildet innenfor IKT-drift. Hoveddelen av bankenes IKT-drift kjøres fortsatt på stormaskiner, men trenden er at nye IKT-tjenester utvikles på andre plattformer, som Intel og Unix.

Når det gjelder informasjonssikkerhet, mener foretakene det er viktig å ha gode prosesser for å holde IKT-infrastrukturen oppdatert. For å sikre tilstrekkelig oversikt er det viktig at de ulike elementene i IKT-infrastrukturen er dokumentert (som maskinvare, basisprogramvare og system). God dokumentasjon vurderes også ofte som en forutsetning for at reetablering ved IKT-hendelser kan skje innenfor satte tidskrav.

3.3.2 Vurdering av operasjonell risiko og sikkerhetsrisiko

Finanstilsynet har innhentet vurderinger av operasjonell risiko og sikkerhetsrisiko fra betalingstjenestetilbydere og noen andre foretak. I det benyttede skjemaet er enkelte spørsmål særskilte for betalingstjenestetilbyderes rapportering. For nærmere detaljer vises det til vedlegg 1.

Styring og kontroll

Halvparten av foretakene mener det er middels eller høy risiko forbundet med å ikke ha tilstrekkelig oversikt over virksomhetskritisk IKT-utstyr og programvare, herunder kontroll med gyldig konfigurasjon av IKT-systemer. Et flertall av foretakene viser også til at det er middels til høy risiko knyttet til det å ikke ha god nok oversikt over de ulike kontrolltiltakene i virksomheten gjennom de tre forsvarslinjene førstelinjekontroll, risikostyring/etterlevelse og internrevisjon. Flere foretak forklarer dette med at der IKT-driften er utkontraktert, blir også mye av kontrollarbeidet utført av leverandøren.

En stor andel av foretakene mener det er middels risiko knyttet til mangler i retningslinjer for sikkerhet og i forbindelse med kartlegging og vurdering av risiko. For 2019 rapporterte flere foretak om at denne risikoen var økende, men for 2020 rapporterte foretakene at risikoen er stabil eller fallende. Årsaken er at flere av foretakene har gjennomført eller planlegger forbedringer på dette området, blant annet gjennom å implementere og/eller forbedre styringssystemet for informasjonssikkerhet (ISMS).

Svært mange av foretakene ser behov for å iverksette ytterligere tiltak for å beskytte brukerne av betalingstjenester.

Beslutningsstøtte

Svært mange av foretakene viser til at de har iverksatt tiltak for å sikre god datakvalitet, blant annet gjennom gode årsaksanalyser av oppståtte feil og kontinuerlig forbedring av arbeidsrutiner. Risiko forbundet med dårlig datakvalitet er redusert etter at det ble sett på som et økende problem for foretakene i 2019. Samlet sett virker foretakene å vurdere at deres IKT-systemer i større grad enn i 2019 gir tilstrekkelig beslutningsstøtte.

Drift og katastrofeberedskap

Et stort flertall av foretakene viser til at endringer i infrastrukturen gjennomføres i trafikkstille perioder for å redusere risiko. Foretakene rapporterer likevel at det er middels til høy risiko forbundet med kompleksiteten i IKT-systemene, noe som bidrar til større sannsynlighet for driftsproblemer. Foretakene legger vekt på gode testprosedyrer for å kompensere for dette. Enkelte foretak opplyser om fortsatt høy risiko for dataangrep og et behov for ytterligere sikkerhetstesting.

Foretakene har redusert omfanget av endringer for blant annet å sikre stabil drift og unngå at endringer skaper nedetid, særlig på grunn av utstrakt bruk av hjemmekontor under koronapandemien. Det er også lagt vekt på å ha gode fallback-løsninger.

Flertallet av foretakene viser også for 2020 til en middels til høy risiko knyttet til tilgang til nødvendig kompetanse. De fleste foretakene mener det er middels eller høy risiko knyttet til at IKT-porteføljen er fordelt på flere systemplattformer. Flere foretak informerer om at det arbeides med å flytte IKT-systemer over til sky for å redusere kompleksiteten.

Et stort flertall av foretakene viser til økt risiko ved at nye regulatoriske krav medfører behov for endringer i IKT-systemene. Dette bidrar også til økt press for å få gjennomført endringene i tide. Flere foretak håndterer dette gjennom å leie inn ekstern kompetanse eller ved utkontraktering av oppgaver.

Av foretakenes hendelsesrapportering (se punkt 5) framgår det at årsaken til mange uønskede hendelser er knyttet til endringer i programvare eller infrastruktur.

Beskyttelse av data

Manglende klassifisering av data med hensyn til blant annet sensitivitet og konfidensialitet utgjør fortsatt en risiko for foretakene. Trenden er imidlertid nedadgående. Flere foretak viser også til at retningslinjer for klassifisering av informasjon ble utarbeidet i løpet av 2020, samt at ytterligere tiltak knyttet til sikring av konfidensiell informasjon gjennomføres i løpet av 2021.

Foretakene som rapporterer om høy risiko forbundet med manglende beskyttelse av konfidensiell informasjon, vurderer også at det er høy risiko forbundet med manglende sikkerhetsmekanismer for å sikre data internt i egne nettverk (gjennom nettverkssegmentering, tilgangskontroller og kryptering).

ID-tyveri

De fleste foretakene vurderer at risikoen knyttet til misbruk av bruker-ID-er er lav og omtrent på nivå med 2019. De fleste foretakene vurderer også risikoen for "Card not present" og "skimming" til å være lav, slik de også gjorde i 2017 og 2018. Noen foretak mener imidlertid at risikoen er høy.

Interne misligheter

Flere foretak rapporterer om middels risiko knyttet til interne misligheter, som kan omfatte både økonomisk vinningskriminalitet og risiko for innsidere. Når det gjelder risiko for økonomisk kriminalitet fra egne ansatte, rapporterer flere foretak om at det gjennomføres regelmessige risikovurderinger knyttet til misligheter. Enkelte foretak inkluderer ikke misligheter i sine risikovurderinger, men baserer seg på screening og bakgrunnssjekk ved ansettelser. Svært få foretak beskriver imidlertid faren for innsidere som en risiko i sine vurderinger.

Det er verdt å merke seg at både PST og NSM viser til at utenlandsk statlig etterretning aktivt forsøker å rekruttere innsidere, se punkt 3.5.1.2. Foretakene bør ta høyde for dette i sine egne risikovurderinger.

Hvitvasking

De fleste foretakene vurderer risikoen som middels eller høy for at ikke alle hvitvaskings- og terrorfinansieringstransaksjoner blir fanget opp av systemene for transaksjonsovervåking. For eksempel kan det gå tid fra en ny kriminell metode blir tatt i bruk til den blir avdekket og hindret. Problemer kan også være forårsaket av manglende datakvalitet, blant annet ved at de ulike transaksjonstypene ikke kontrolleres opp mot de rette parameterne i transaksjonsovervåkningen.

3.4 Risiko knyttet til kunders bruk av digitale tjenester

3.4.1 Ansvar ved bruk av betalingstjenester

Betalingstjenestene, og tjenester der betalingstjenester benyttes, har innbakt funksjonalitet og roller i et omfang som kan gjøre det vanskelig for brukeren å overskue konsekvensene når rollene endres. Endringer i relasjonen mellom betaler, betalingsmottaker eller andre må gjenspeiles i tjenestene. Hvem som har ansvaret for å sikre at endringene ikke medfører uheldige følgekonsekvenser, vil avhenge av i hvilken relasjon endringen skjer.

Et eksempel er fraskilte som fire år etter en skilsmisse oppdager en uventet belastning fra en tidligere strømleverandør. Nærmere undersøkelser viste at den tidligere ektefellen hadde byttet tilbake til den strømleverandøren de i sin tid hadde sammen. Leverandøren tok fram den gamle avtalen (avtalegiro), med den konsekvens at feil person ble belastet for strømleveransen.

Avtalegiro er et register som kobler betaler og betalingsmottaker. Utfordringen er at en tjenestetilbyder, i dette tilfellet strømleverandøren, ikke kan se kontonummeret avtalen er knyttet til og

hvem som er eier av kontoen. Banken vet ikke hvem som er den egentlige strømkunden. Den eneste med innsikt i det fulle bildet er eieren av kontoen som belastes avtalegiroen.

Et annet eksempel er en bileier som registrerte sitt kredittkortnummer i en parkeringsapp og knyttet det til bilens registreringsnummer. Selv om bilen er solgt, belastes fortsatt tidligere eier for den nye eierens parkeringsavgifter.

Løsningen i begge tilfellene ville vært å terminere avtalene, men for forbrukere er det ikke alltid enkelt å huske hvilke avtaler som er inngått og avtalenes innhold. Dermed vil det i takt med økt automatisering være hensiktsmessig at kontotilbydere og kortutstedere regelmessig gir tips, råd og påminnelser knyttet til produkters virkemåte og kundenes ansvar.

3.4.2 Risiko knyttet til elektroniske ID-er

Kunden skal ikke dele innloggingskoder med andre og er tillagt et ansvar for å beskytte kodene mot urettmessig bruk. Utstederne av kodene må legge til rette for løsninger som ivaretar brukerens mulighet til å skjerme sine koder. Det er ulike oppfatninger om hvor grensen mellom kundens og utsteders ansvar skal trekkes. Spørsmålet har blant annet vært drøftet i forbindelse med utformingen av ny finansavtalelov, der utsteder er tillagt et større objektivt ansvar enn tidligere.

Utstedere av sikkerhetssystemer og koder for blant annet elektroniske ID-er tar beslutning om produktene som tilbys. De samme utstederne medvirker til at sikkerhetsløsninger tas i bruk i andre sammenhenger enn primærformålet, der konsekvensene blir en ID-løsning som kan påføre stor skade dersom den kommer på avveie. Blant annet har BankID blitt en "universalnøkkel" for tilgang til privat og offentlig tjenesteyting. Det kan hevdes at ingen pålegges elektroniske ID-er, men i dagens digitaliserte samfunn er BankID nærmest blitt en forutsetning for å få tilgang til blant annet konto- og betalingstjenester. I praksis er det vanskelig å velge bort BankID. Omfattende bruk av BankID påfører eieren økt risiko for at kriminelle kan skaffe seg tilgang til og misbruke en BankID i flere sammenhenger.

Det informeres i liten grad om risikoen som ID-utstedere indirekte påfører ID-brukere. ID-brukere bør gis større valgfrihet når det gjelder bruksområdet. Brukerne bør ha mulighet til å sette policy/retningslinjer for ID-en, for eksempel at den kun skal kunne brukes mot et avgrenset sett med tjenester der for eksempel større låneopptak ikke inngår.

Når de aller fleste nordmenn nå er påført en viss risiko forbundet med misbruk av ID-er, bør det stilles særdeles strenge krav til utstederen av ID-en. I dagens selvbetjeningssamfunn bør utstedere av ID-er etablere løsninger der brukeren kan reservere seg mot bruksområder og i større grad kontrollere aktiviteten og redusere mulighetsrommet for misbruk.

I misbrukssaker der offeret er påført betydelig skade, bør det stilles spørsmål om det er gjennomført tilstrekkelige tiltak for å forhindre skade fra ID-utsteder eller -brukerstedet. Er bankene for trygge på ID-en som banken (eller annen bank) utsteder, slik at ytterligere kontroller ikke utføres? For eksempel

ved lånesaker, der lån har vært tatt opp ved misbruk av annens ID, kan det stilles spørsmål ved om banken har foretatt en tilstrekkelig tilleggskontroll, som å kontakte debitor på telefon eller på annen måte.

3.4.3 "Slitasje" på ID-en

BankID er viktig i dagens digitale samfunn for å kunne logge seg på ulike finansielle og ikke-finansielle tjenester via apper og nettbaserte løsninger. Påloggingssidene på de ulike nettstedene og appene hvor BankID brukes, ser noe forskjellige ut, og det er en risiko for at brukeren etter hvert ikke vil være tilstrekkelig årvåken og kritisk i forbindelse med bruk av BankID. Kombinasjonen av den utstrakte bruken av BankID og variasjoner i innloggingskontekst gir en form for "slitasje" på ID-en og brukerens kritiske sans. Dette tilsier at det bør være mulig å reservere seg mot bruksområder for ID-en og i større grad kontrollere mulig bruk og redusere åpninger for misbruk.

3.4.4 Kundeinformasjon

Det reviderte betalingstjenestedirektivet (PSD2) stiller fra 1. januar 2021 krav om sterk kundeautentisering i forbindelse med betalinger for handel på internett. Innføringen har vært forberedt i en årrekke. Banker og andre kortutstedere har vært konsultert og involvert i forberedelsene og har vært godt kjent med at overgangen ville kunne ha merkbare konsekvenser for kundene og kundeopplevelsen i kjøpssituasjonen. Som en del av kravene er bankene og kortutstederne bedt om å informere sine kunder om endringene før innføringen.

Finanstilsynet gjennomgikk en rekke bankers nettsteder nær opp til innføringen. Ingen av bankene som ble undersøkt, hadde publisert informasjon til kundene på tidspunktet for undersøkelsen. Finanstilsynet oppfordret derfor bankene til å informere kundene om innføringen av sterk kundeautentisering. Undersøkelser i etterkant tydet på at svært få banker fulgte denne oppfordringen. Nær årsskiftet fant Finanstilsynet at bare én bank ga sine kunder informasjon om endringen.

Etter innføringen av sterk kundeautentisering ble det registrert flere reaksjoner fra publikum, og omleggingen var også tema i Stortingets spørretime[17]. Finanstilsynet publiserte derfor en beskrivelse av endringene på sitt nettsted, sammen med presiseringer av hvordan reglene skal forstås og hvilke valgmuligheter som foreligger.[18]

3.5 Trusselbildet og digital kriminalitet

Omfanget av kriminelle angrep mot finansforetakenes digitale systemer fortsatte å øke i 2020. Samtidig har foretakene utviklet sine systemer for overvåking, deres systemer for å avverge angrep er bedre, og angrepene avverges som oftest før de får konsekvenser for foretaket. Også foretakenes

[17] https://stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qid=83239
[18] https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2021/mulige-unntak-fra-kravet-om-sterk-kundeautentisering-i-forbindelse-med-betaling-for-handel-pa/

kompetanse er styrket. Som omtalt under punkt 2.6 bidrar god samhandling i finansnæringen gjennom NFCERT[12] til å heve kunnskapen om det aktuelle trussel- og risikobildet og til å gjøre foretakene bedre rustet til å håndtere digitale trusler og forebygge uønskede hendelser.

Det har etter hvert blitt vanskelig å trekke grensen mellom trusler fra henholdsvis organiserte kriminelle og fremmed etterretning, og en rekke kriminelle miljøer selger tjenester til blant andre statlige aktører. Både Forsvarets etterretningstjeneste (E-tjenesten) og Politiets sikkerhetstjeneste (PST) peker på en betydelig trussel fra statlige aktører, blant annet gjennom etterretnings- og nettverksoperasjoner (digital kartlegging og sabotasje av kritisk infrastruktur), mens Nasjonal sikkerhetsmyndighet (NSM) blant annet peker på trusler knyttet til rekruttering av innsidere.

Foretakene må videreføre sitt arbeid med å kartlegge risiko- og sårbarheter, iverksette preventive tiltak og forberede seg på å måtte håndtere angrep og følgeskadene av slike angrep. Et viktig arbeid for foretakene er å sikre beskyttelse av konfidensiell informasjon og bevisstgjøre egne ansatte om det digitale trusselbildet.

Finanstilsynet observerer store forskjeller i foretakenes modenhet når det gjelder å vurdere risikoen ved manglende beskyttelse av data. For å kunne forebygge er det viktig at foretakene kartlegger hvilke verdier som kan være utsatt. Den finansielle infrastrukturen utgjør i seg selv en verdi siden denne understøtter samfunnets grunnleggende funksjonalitet, som i sikkerhetsloven er definert som en nasjonal sikkerhetsinteresse[2].

3.5.1 Trusler rettet mot finansnæringen

3.5.1.1 Verdier i finanssektoren som er utsatt for trusler fra statlige aktører

Finanssektoren forvalter verdier som medfører at foretakene, deres ansatte, foretakenes systemer og foretakenes leverandører vil kunne bli utsatt for ulike former for trusler fra utenlandske aktører. Forsvarets etterretningstjeneste beskriver i rapporten Fokus 2021[19] sikkerhetsutfordringer som følge av en betydelig trussel mot norske interesser, herunder finanssektoren, fra nasjoner som Kina og Russland, i form av blant annet etterretnings- og nettverksoperasjoner.

I sitt forebyggende arbeid er det viktig at foretakene kartlegger hvilke verdier[20] som kan være utsatt for trusler fra statlige aktører. Finanstilsynet observer vesentlig varierende modenhet i foretakene knyttet til å vurdere risikoen og risiko knyttet til manglende beskyttelse av slike data.

Den finansielle infrastrukturen utgjør i seg selv en verdi[2]. Norske finansforetak, herunder deres leverandører, kan være utsatt for spionasje for å få tilgang til informasjon for å kunne planlegge nettverksangrep og sabotasje mot den finansielle infrastrukturen. PST viser i sin trusselvurdering for

[19] Fokus 2021, https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus
[20] NS 5830:2012 – Samfunnssikkerhet – beskyttelse mot tilsiktede uønskede handlinger - terminologi

2021[21] til at nettverksoperasjoner er et viktig element i utenlandsk etterretningsaktivitet rettet mot Norge. Nettverksangrepene mot Stortingets datasystemer høsten 2020 og i mars 2021 er eksempler på at det foreligger en reell trussel mot norske sikkerhetsinteresser.

Finanstilsynet og Norges Bank arbeider med forslag til rammeverk for penetrasjonstesting av finansielle institusjoner, slik at foretaket kan teste evnen til å motstå nettverksangrep. Se nærmere omtale i punkt 3.3.2.

3.5.1.2 Rekruttering av innsidere og bevisstgjøring av ansatte

PST legger i sin trusselvurdering for 2021[21] til grunn at russiske etterretningsoffiserer vil bruke mye tid på å pleie kontakt med personer i Norge for å rekruttere kilder i ulike foretak. I den forbindelse kan sensitiv informasjon om enkeltpersoner – for eksempel helseinformasjon innhentet gjennom nettverksangrep overfor helsesektoren – bli benyttet for å utøve press overfor enkeltpersoner innen finanssektoren for å få tilgang til informasjon eller påvirke beslutninger.

NSM har i sin rapport Risiko 2021[22] beskrevet at flere etterretningstjenester vil forsøke å rekruttere personer gjennom sosiale medier, for eksempel ved ta kontakt via LinkedIn. Vedkommende kan utgi seg for å arbeide for et rekrutteringsbyrå og gradvis utvikle en relasjon der man etter hvert vil bli bedt om å bidra med faglige artikler og kronikker mot betaling.

Bevisstgjøring av ansatte om mulige rekrutteringsforsøk er svært viktig, da enkeltpersoner ikke alltid selv vil være klar over hvilken verdi det kan ha for statlige aktører å få innsyn i informasjon om systemer, prosesser, policyvurderinger og organisasjoner. Det er derfor viktig at ansatte er oppmerksomme på hvem de deler informasjon med, hvem som kan fange opp informasjon, samt hvilke kommunikasjonskanaler som benyttes til informasjonsutveksling. Det er også viktig at foretakene i tillegg informerer og bevisstgjør egne ansatte om denne trusselen, samt hvordan ansatte skal varsle internt.

For å redusere sårbarheten er det viktig at foretakene begrenser tilgangen til sensitiv informasjon som rutiner, sikkerhetstiltak og IKT-infrastruktur, samt at de har god intern logging av tilganger og endringer i egne systemer.

Finansbransjen er en svært internasjonal bransje. Nordmenn som oppholder seg i land med autoritære styresett, kan bli lokket eller presset til å jobbe for vertslandets etterretningstjeneste. Utenlandske statsborgere i Norge kan også bli utsatt for press fra hjemlandets etterretningstjeneste ved arbeidsopphold i Norge.

[21] https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/
[22] https://nsm.no/aktuelt/risiko-2021-helhetlig-sikring-mot-sammensatte-trusler

Det er viktig å ta høyde for menneskelig sårbarhet ved utarbeidelse av helhetlige risikobilder, også med tanke på informasjonssikkerhet. Bevisstgjøring av ansatte og forebyggende sikkerhetstiltak bør inngå i foretakenes personalrutiner.

3.5.1.3 Målrettede investeringer i norsk infrastruktur

Finansbransjen bør merke seg at oppkjøp av norske foretak også kan utgjøre en trussel mot norske interesser. E-tjenesten omtaler Kinas målrettede strategiske oppkjøp i utlandet som en konkret trussel i rapporten Fokus 202118. Handelskrigen med USA understreket sårbarheten ved å være avhengig av globale markeder, og Kina prioriterte i 2020 teknologisk selvforsyning. I tillegg er strategien å gjøre Kina uunnværlig i internasjonale handelskjeder for å kunne motstå eksternt press. E-tjenesten påpeker også at selskaper som har fått kinesiske eiere, benyttes for å foreta nye oppkjøp, og at investeringer kanaliseres gjennom tredjeland.

PST viser i sin trusselvurdering[21] til at slike oppkjøp kan legge til rette for et avhengighetsforhold og kunne posisjonere en fremmed stat til å presse norske beslutningstagere til å handle i strid med norske sikkerhetsinteresser. Slike oppkjøp kan også gi direkte tilgang til teknologi som brukes i oppkjøpte selskaper. Det har flere vært eksempler på slike interessekonflikter det siste året[23].

Dette er utviklingstrekk som også finansnæringen bør være bevisst på. Oppkjøp i mindre bedrifter kan også være et middel for fremmede stater for å få innsyn og tilgang til digital infrastruktur, herunder finansiell infrastruktur.

3.5.1.4 Phishing

Gjennom 2020 var det periodevis høy phishingaktivitet, som resulterte i en del tap, se omtale under punkt 4.5. Phishingen er ofte målrettet og tilpasset den dagsaktuelle situasjonen. Koronapandemien la i 2020 grunnlag for nye phishingangrep.

Det ble i 2020 blant annet avdekket:

- **Falske forespørsler om legitimasjonskontroll**
  Svindlere utgir seg for å være banken gjennom å sende SMS eller e-post til kunden og forsøker å lure kunden til å gi fra seg fødselsnummer, koder, passord og/eller kortinformasjon, som svindleren kan bruke til å registrere betalinger fra kundens konto.
- **Falske meldinger om at betalingskort er sperret**
  Kunden mottar SMS eller e-post om at betalingskort er sperret av tekniske eller sikkerhetsmessige grunner. For å aktivere kortet må betaleren klikke på en lenke og deretter oppgi koder og passord, som svindleren kan bruke til å registrere betalinger fra kundens konto.

[23] Salg av Bergen Engines til det russiskkontrollerte selskapet TMH International ble stoppet https://e24.no/naeringsliv/i/PRngK0/derfor-er-salget-av-bergen-engines-saa-kontroversielt. Leasingselskapet BOC Aviation, eid av Bank of China, som igjen er heleid av den kinesiske staten, kjøpte eierandeler i Norwegian i 2020.

- **'Olga-svindel'**
  Svindlere ringer eldre mennesker og utgir seg for å være banken for å lure dem til å gi fra seg koder, passord og/eller kortinformasjon. Svindlerne bruker deretter informasjonen de har tilegnet seg til å registrere betalinger fra kundens konto(er) eller bruke kortopplysningene på nett.
- **Falske meldinger om pakker i posten**
  Mengden pakkeforsendelser har økt under koronapandemien. Kunden mottar SMS eller e-post om at en pakke er på vei. For å spore pakken kan de trykke på en lenke der de blir bedt om å logge seg inn med koder og passord, som svindleren deretter kan bruke til å gjennomføre utbetalinger fra kundens konto.
- **Svindel knyttet til støtteordninger som følge av koronapandemien**
  Svindlere har tilegnet seg statlige garantilån på falske premisser, jf. Norfund-saken[24].
- **Falsk inkassoinnkreving**
  Svindlere har tilegnet seg kundelister fra spillselskap og oversender fiktive inkassokrav til legale inkassoforetak.

3.5.1.5 Sårbarheter forbundet med bruk av leverandører og 'standard' programvare

NSM viser i sin rapport[22] til at trusselaktører kan utnytte programvare- og tjenesteleverandører for å få innpass i systemene til selskapets kunder. Leverandørkjedeangrep, hvor aktøren rammer en tredjepart eller tilgrensende virksomhet enten gjennom et angrep eller ved utnyttelse av sårbarheter i programvare, forekommer også i Norge. Virksomheter lengre nede i verdikjedene kan også være utsatt for sikkerhetstrusler, enten som mål i seg selv eller som ledd i å nå foretak høyere opp i verdikjedene.

Svakheter i nettverk og applikasjoner vil, inntil de er kjent av foretaket som utvikler eller bruker løsningen, kunne utgjøre en sårbarhet ved at potensielle angripere får kunnskap om den og utnytter den til kriminelle handlinger.

Nedenfor omtales to globale sikkerhetshendelser, SolarWind-saken i 2020 og Microsoft Exchange-saken i 2021, der også norske foretak ble berørt. Se også punkt 5.2.

Datainnbrudd i produktet SolarWinds Orion

IT-sikkerhetsselskapet FireEye avdekket i desember 2020 et datainnbrudd etter at produktet SolarWinds Orion, som brukes til overvåkning av nettverk, var kompromittert ved at en såkalt "bakdør", som har fått navnet Sunburst, var lagt inn i programvareoppdateringer distribuert til kundene.

Bakdøren ble trolig installert mot slutten av 2019 og ga tilgang til kompromitterte nettverk. Det antas at hensikten først og fremst var å hente ut informasjon. SolarWinds Orion er et svært utbredt produkt, også i finansnæringen. Finanstilsynet mottok rapporter fra flere finansforetak som selv eller gjennom

[24] https://www.norfund.no/no/norfund-er-utsatt-for-alvorlig-svindel/

underleverandør bruker SolarWinds Orion til overvåking av nettverksinfrastruktur. Foretakene gjennomførte grundige undersøkelser, men fant ingen spor av at bakdøren var utnyttet. En rekke parametere måtte være oppfylt for at bakdøren skulle kunne anvendes, og det antas at angriperne kun har utnyttet bakdøren i et svært lite antall kompromitterte nettverk. Flest tilfeller er kjent fra USA.

Utnyttet sårbarhet i programvaren til Microsoft Exchange

Microsoft publiserte i begynnelsen av mars 2021 en såkalt nulldags sikkerhetsoppdatering[25] etter at sårbarheter i programvaren til Microsoft Exchange Server, som er serverprogramvare hovedsakelig for e-post, var blitt utnyttet. Sårbarheten hadde sannsynligvis vært der siden slutten av 2020. Sårbarheten kunne utnyttes til å hente ut informasjon, men også til å plante ondsinnet kode. Utnyttelse av sårbarheten ble funnet i USA, i EU-land og i andre land. I følge ENISAs publikasjon "Microsoft Exchange Vulnerabilities"[26] var det per 5. mars 2021 rundt 250.000 sårbare servere globalt. Etter tiltak (patching) ble antall sårbare servere i løpet av de neste ti dagene redusert til rundt 60.000. Den europeiske banktilsynsmyndigheten (EBA) var utsatt for forsøk på utnyttelse av sårbarheten[27], og i Norge var blant annet Stortinget utsatt for det samme[28]. For det enkelte foretaket er det et omfattende arbeid å kartlegge om utnyttelse av slike sårbarheter har fått konsekvenser i form av at informasjon er hentet ut eller systemene på annen måte er misbrukt. Finanstilsynet mottok meldinger fra enkelte finansforetak om at de benytter denne typen servere, men at det etter grundige undersøkelser ikke var spor av at sårbarheten var utnyttet.

3.5.2 TIBER-NO

Norges Bank og Finanstilsynet besluttet i første halvår 2020, blant annet på bakgrunn av positive tilbakemeldinger fra finansnæringen, at det skulle utarbeides et forslag til rammeverk for testing av cybersikkerheten i den norske finansielle sektoren[29]. Verktøyet vil bygge på et rammeverk som er utarbeidet av den europeiske sentralbanken (TIBER-EU[30]). Forslag til nasjonalt rammeverk for testing av cybersikkerhet, "TIBER-NO", ble sendt på høring i mars 2021, med høringsfrist 12. mai.

Målsettingen for TIBER-NO er å bidra til finansiell stabilitet gjennom økt motstandsdyktighet mot cyberangrep for kritiske funksjoner i det norske finansielle systemet. TIBER-NO er ikke ment som et verktøy for tilsyn og overvåking av foretak og enkeltsystemer, men Finanstilsynet vil kunne be foretakene om informasjon om resultater fra gjennomførte tester.

For at TIBER-NO skal kunne bidra til økt motstandsdyktighet mot cyberangrep, og gjennom det bidra til å styrke den finansielle stabiliteten i Norge, må sentrale kritiske funksjoner i den finansielle

[25] Nulldags-sikkerhetsoppdatering vil si oppdatering mot en sårbarhet som er blitt utnyttet før den er blitt offentlig kjent
[26] https://www.enisa.europa.eu/news/enisa-news/statement-on-microsoft-exchange-vulnerabilities
[27] Cyber-attack on the European Banking Authority - UPDATE 3 | European Banking Authority (europa.eu)
[28] https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/Nyhetsarkiv/Hva-skjer-nyheter/2020-2021/stortinget-utsatt-for-it-angrep/
[29] https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2020/rammeverk-for-testing-av-cybersikkerhet-tiber-no/
[30] https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

sektoren testes. Det vil derfor være viktig at foretak ansvarlige for slike funksjoner tar del i TIBER-NO. I tillegg til å omfatte foretak i den finansielle sektoren er det foreslått at TIBER-NO skal legge til rette for å inkludere sentrale IKT-leverandører og datasentre i testingen.

Finanstilsynet og Norges Bank samarbeider om implementering og bruk av TIBER-NO og vil etablere nødvendige fora for overordnet oppfølging, styring og involvering av både næringsaktører og relevante myndigheter. Norges Bank vil organisere og bemanne et "TIBER-NO Cyber Team" (TCT-NO) for å forvalte og operasjonalisere TIBER-NO.

3.5.3 IMFs vurdering av cybermodenhet i finansiell sektor

Som del av IMFs gjennomgang av det norske finanssystemet i 2019 og 2020 («Financial Sector Assessment Program», FSAP) vurderte IMF også det norske rammeverket for å håndtere cyberrisiko.[31]

Det norske rammeverket for håndtering av cyberhendelser og Norges arbeid med cyberrisiko karakteriseres av IMF som avansert, men det er også områder som kan forbedres for å redusere risikoen knyttet til digitale trusler. IMF fremhever at systemet for informasjonsdeling mellom myndighetene er godt etablert på dette feltet. Rapporteringen av cyberhendelser bør likevel styrkes ved å etablere klarere terskelverdier for rapportering og tydeligere spesifisering av hva som skal rapporteres. IMF anbefaler også at tilsynet med cyberrisiko for betalingssystemer bør intensiveres, blant annet ved mer strukturerte og omfattende tilnærminger. For nærmere informasjon henvises det til IMFs rapporter.

[31] https://www.imf.org/en/Publications/CR/Issues/2020/08/07/Norway-Financial-System-Stability-Assessment-Press-Release-and-Statement-by-the-Executive-49670
https://www.imf.org/en/Publications/CR/Issues/2020/08/07/Norway-Financial-Sector-Assessment-Program-Technical-Note-Cybersecurity-Risk-Supervision-and-49673

4 SVINDEL OG SVINDELSTATISTIKK

4.1 Rapportering av svindelstatistikk

Etter forskrift om systemer for betalingstjenester § 2 skal banker, kredittinstitusjoner, e-pengeforetak, betalingsforetak og filialer av slike foretak med hovedsete i annen EØS-stat rapportere svindelstatistikk til Finanstilsynet minimum én gang i året. Finanstilsynet har besluttet at foretakenes rapportering om svindel skal skje halvårlig, som er i henhold til det reviderte betalingstjenestedirektivet (PSD2)[32].

Svindelrapporteringen ble noe endret etter innføringen av PSD2, gjeldende fra og med andre halvår 2019. 2020 er det første året hvor svindelrapportering for både første og andre halvår er i tråd med PSD2s retningslinjer. På enkelte områder vil det derfor kun være relevant å sammenligne 2020-tallene med tilsvarende tall for andre halvår 2019. Det er likevel referert til svindeltallene for 2019, som er en kombinasjon av rapportering på det tidligere formatet definert av Bits og det nye PSD2-formatet, der dette har vært mulig. I tillegg er det i noen grad referert til tidligere år.

Rapporteringen omfatter det totale volumet av både transaksjoner og svindeltransaksjoner. Det gjør det mulig å angi svindel som andel av det totale transaksjonsvolumet. Det rapporteres både verdi av transaksjonene og antall transaksjoner. I rapporteringen skilles det mellom transaksjoner innenlands, grensekryssende transaksjoner innenfor EØS og grensekryssende transaksjoner utenfor EØS. Videre inndeles 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

Svindel med betalingskort er hovedsakelig svindel der svindleren utsteder betalingen. Den største underkategorien er tyveri av kortdetaljer.

Kortutstedere rapporterte at tap på svindel med kortbetalinger i 2020 utgjorde ca. 143 mill. kroner. Tapene var omtrent likt fordelt mellom første og andre halvår, henholdsvis 69,6 og 73,4 mill. kroner. I tillegg kommer tap på 4,5 mill. kroner gjennom urettmessig bruk av betalingskort for kontantuttak, som fordelte seg på første og andre halvår med henholdsvis 3,3 og 1,2 mill. kroner. Samlet var det

[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

totale tapet ved misbruk av betalingskort 147,5 mill. kroner. Dette er en nedgang fra 2019 på 22 prosent. Det er også nedgang i forhold til andre halvår i 2019, da rapporteringen av svindel fulgte samme format som i 2020.

Tabell 4.1 viser samlede tap for betalingskort eid av norske kunder de siste årene, uavhengig av om tapet dekkes av kunden selv, banken eller kortselskapet.

Tabell 4.1 Tap ved misbruk av betalingskort

Svindeltype betalingskort (beløp i hele tusen kroner)	2015	2016	2017	2018	2019	2020
Totalt	**188.659**	**206.503**	**145.591**	**148.732**	**189.147**	**147.602**[33]

Kilder: Finanstilsynet og Bits AS

Samlede tap i 2020 knyttet til svindel ved betalinger med betalingskort utgjorde 0,02 prosent av total transaksjonsverdi. Andelen svindel er størst for grensekryssende transaksjoner utenfor EØS. Her utgjorde svindel 0,3 prosent av transaksjonsverdien.

Tap ved kortbetalinger som er ikke er initiert elektronisk[34], utgjorde i 2020 ca. 20 mill. kroner av det samlede tapet på 143 mill. kroner. Dette er korttransaksjoner der informasjon fra betalingskortet er kommunisert fra kjøper til selger muntlig, over telefon eller via e-post. Andelen svindel er her over 0,1 prosent og for grensekryssende transaksjoner utenfor EØS hele 0,6 prosent.

Svindelandelen er større ved bruk av betalingskort ved fjernhandel, som typisk er handel på internett, enn ved nærhandel (bruk av betalingskort i terminal på fysisk brukersted). For betaling uten sterk kundeautentisering ved fjernhandel utgjør svindel 0,07 prosent av transaksjonsverdiene, og for grensekryssende transaksjoner utenfor EØS 0,35 prosent.

Totalt ble det gjennomført i underkant av 2,5 mrd. betalinger med kort i 2020. Av disse var ca. 205.000 transaksjoner svindel. Dette utgjør 0,008 prosent. Sammenlignet med andre halvår 2019, hvor antall svindeltransaksjoner var 110.000, var omfanget omtrent uendret fra 2019 til 2020.

Andelen svindel er vesentlig større for grensekryssende enn for innenlandske transaksjoner. For grensekryssende transaksjoner utenfor EØS utgjør svindel 0,3 prosent (3 av 1.000 transaksjoner). For kortbetalinger som er initiert ikke-elektronisk, utgjør svindel 0,5 prosent (1 av 200 transaksjoner).

Gjennomsnittsverdien av en svindeltransaksjon med betalingskort er 699 kroner, mens gjennomsnittverdien av en transaksjon med betalingskort er 372 kroner.

[33] Betalinger og kontantuttak med kort
[34] Korttransaksjonene er initiert manuelt ved at informasjon fra betalingskortet er kommunisert gjennom samtale, telefon eller e-post.

Tabell 4.2 Verdi av transaksjoner og svindeltransaksjoner med betalingskort rapportert av kortutsteder. Tall for 2020

Transaksjonsverdi (beløp i hele tusen kroner)	Transaksjoner i Norge	Grensekryssende transaksjoner i EØS	Grensekryssende transaksjoner utenfor EØS	Totale transaksjoner
Kortbetalinger (utsteder)				
Totalt	731.878.546	163.656.849	11.212.122	906.747.517
- Hvorav svindel	6.235	103.977	32.828	**143.040**
Svindel i prosent	0,001	0,064	0,293	0,016
Hvorav initiert ikke-elektronisk[34]:				
Totalt	9.776.674	10.271.445	1.391.905	21.440.024
- Hvorav svindel	437	14.867	7.899	23.203
Svindel i prosent	0,004	0,145	**0,567**	0,108
Hvorav initiert elektronisk:				
Svindleren utsteder betalingen, hvorav	5.806	81.001	23.182	109.989
- Tapt eller stjålet kort	1.400	2.802	810	5.012
- Ikke mottatt kort	706	1.351	121	2.178
- Forfalsket kort	159	554	1.104	1.817
- Tyveri av kortdetaljer	1.946	61.063	18.377	81.386
- Annet	1.595	15.231	2.770	19.596
Svindleren endrer eller modifiserer betalingsordre	146	908	142	1.196
Svindleren manipulerer betaleren til en kortbetaling	117	7.435	1.616	9.168
Fjernbetaling (internetthandel)				
Totalt	69.648.557	98.666.610	6.201.971	174.517.138
- Hvorav svindel	2.850	82.446	21.788	107.084
Svindel i prosent	0,004	0,084	**0,351**	0,061
Nærbetaling (på fysisk brukersted)				
Totalt	652.453.314	54.718.793	3.618.245	710.790.352
- Hvorav svindel	2.943	6.664	3.142	12.749
Svindel i prosent	0,000	0,012	0,087	0,002
Fjernbetaling uten sterk kundeautentisering				
Totalt	44.748.384	56.725.513	4.781.138	106.255.035
- Hvorav svindel	2.399	56.027	16.698	75.124
Svindel i prosent	0,005	0,099	**0,349**	0,070

Kilde: Finanstilsynet

Tabell 4.3 Antall transaksjoner og svindeltransaksjoner med betalingskort rapportert av kortutsteder i 2020

Antall	Transaksjoner i Norge	Grensekryssende i EØS	Grensekryssende utenfor EØS	Totalt
Totalt	1.986.894.640	433.122.094	20.470.498	2.440.487.232
Hvorav svindel	9.711	140.576	54.318	204.605
Svindel i prosent	0,001	0,032	**0,265**	0,008
Initiert ikke-elektronisk:	19.340.195	42.062.726	2.591.058	63.993.979
- Hvorav svindel	935	15.012	13.560	29.507
Svindel i prosent	0,005	0,036	**0,523**	0,046
Fjernbetaling	194.433.015	236.867.520	12.394.085	443.694.620
- Hvorav svindel	3.751	116.485	37.934	158.170
Svindel i prosent	0,002	0,049	**0,306**	0,036
Nærbetaling	1.773.121.430	154.191.848	5.485.355	1.932.798.633
- Hvorav svindel	5.015	9.079	2.824	16.918
Svindel i prosent	0,000	0,006	0,052	0,000

Kilde: Finanstilsynet

4.3 Tap knyttet til kontooverføringer

Svindel med kontooverføringer er svindel der svindleren utsteder eller modifiserer betalingen eller manipulerer betaleren til selv å utstede betalingen.

Tabell 4.4 Transaksjoner og svindeltransaksjoner – kontooverføringer (nettbank m.m.). 2020

Kontooverføringer initiert elektronisk (beløp i hele 1000 kroner)	Transaksjoner i Norge	Grensekryss-ende i EØS	Grensekryss-ende utenfor EØS	Totalt	Svindel-prosent
Totalt	189.996.583.878	27.582.143.072	5.972.119.064	223.550.846.014	
- Hvorav svindel	118.672	97.570	139.245	**355.487**	0,00016
Hvorav ulike typer svindler:					
- Svindleren utsteder betalingen	36.777	12.758	6.888	56.423	
- Svindleren modifiserer betalingsordren	721	34.456	11.891	12.363	
- Svindleren manipulerer betaleren til å utstede betalingsordren	81.155	49.019	120.467	285.344	

Kilde: Finanstilsynet

Tap ved kontooverføringer, hovedsakelig nettbank, utgjorde ca. 355 mill. kroner i 2020, mot 301 mill. kroner i andre halvår i 2019. Dette indikerer en vesentlig nedgang i forhold andre halvår 2019. Tallene viser samlede tap for nettbanksvindel mot norske kunder for de siste årene, uavhengig av om tapet dekkes av kunden selv eller banken.

4.4 Tap ved svindel gjennom sosial manipulering

Rapporterte tall på svindel ved sosial manipulering, dvs. der svindleren manipulerer betaleren til å gjennomføre en transaksjon, utgjorde i 2020 ca. 295 mill. kroner, hvorav 285 mill. kroner for transaksjoner i nettbank og 10 mill. kroner for betalingskort. Dette er på nivå med 2018, hvor rapporterte tap var i underkant av 300 mill. kroner, men vesentlig lavere enn rapporterte tall i 2019, som indikerte tap på over 500 mill. kroner.

Omfanget av svindel ved sosial manipulering er usikre fordi betaleren selv bærer tapet og mange svindler av denne typen trolig ikke blir meldt til banken. Det antas at de faktiske tapene er 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 transaksjoner som er unormale for kunden.

Fra de største bankene er Finanstilsynet kjent med at antall svindelforsøk ved sosial manipulering stadig øker. Forsøkt svindlet beløp (angrepssum) er mange ganger større enn kundenes materialiserte tap. Bankene forhindrer en stadig større andel av svindelforsøkene, og den prosentvise andelen av forsøkt svindlet beløp som gir et reelt tap, synker. At bankene stopper en stadig større andel av forsøkene er trolig hovedårsaken til at de rapporterte svindeltallene for 2020 er lavere enn i 2019. Økt oppmerksomhet i befolkningen om svindel ved sosial manipulering antas også å innvirke på nedgangen.

Svindel gjennom sosial manipulering ser fortsatt ut til å være den mest lønnsomme metoden for kriminelle. Hvilken type sosial manipulering de kriminelle vurderer som mest lønnsom, endrer seg. Rapporteringen i henhold til PSD2s retningslinjer differensierer ikke mellom ulike typer av sosial manipulering, men Finanstilsynet har fra enkelte større banker fått oppgitt tall for underkategorier. I 2020 var det størst tap på svindel med endring av mottakerkonto og på investeringer i falske selskaper.

4.5 Tap ved svindel der svindler utsteder betalingen

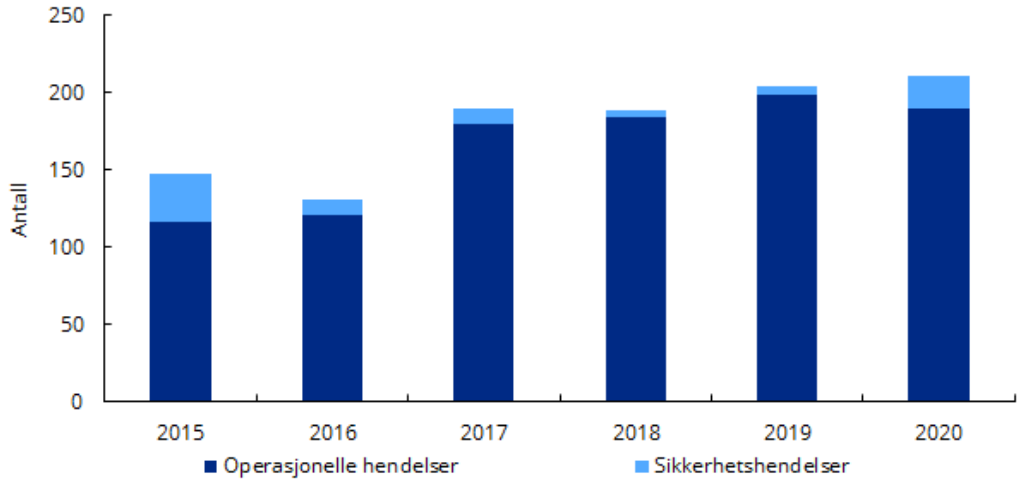
I PSD2-rapporteringen er sosial manipulering definert som betalingstransaksjoner der svindleren manipulerer betaleren til å gjennomføre en transaksjon. Svindel med phishing omfatter imidlertid også elementer av sosial manipulering. Ved phishing avlures kontakt- og betalingsinformasjon fra betaleren som svindleren bruker til å utstede en betaling på vegne av betaleren. I PSD2-rapporteringen blir dette rapportert som svindel der svindler utsteder betalingen. Tap for denne kategorien i 2020 var for transaksjoner i nettbank 56 mill. kroner og for betalingskort 110 mill. kroner.

5 Hendelsesrapportering

5.1 Statistikk over hendelser

Det var samlet sett noen flere hendelser i 2020 enn i 2019. Mens det var flere sikkerhetshendelser i 2020 enn i 2019, var det færre operasjonelle hendelser. 21 av de 211 rapporterte hendelsene var sikkerhetshendelser (10 prosent). Finanstilsynet har ikke observert at koronapandemien påvirket hendelsesmønsteret i 2020.

Figur 5.1 Antall rapporterte IKT-hendelser i 2020



Kilde: Finanstilsynet

Tabell 5.1 Antall rapporterte hendelser

År	Operasjonelle hendelser	Sikkerhets-hendelser	Totalt antall hendelser
2015	116	32	148
2016	121	10	131
2017	180	10	190
2018	184	5	189
2019	200	6	206
2020	190	21	211

Kilde: Finanstilsynet

5.2 Sikkerhetshendelser

De fleste sikkerhetshendelsene gjaldt digital kriminalitet, herunder vinningskriminalitet. Ti av sikkerhetshendelsene som ble rapportert til Finanstilsynet i 2020, gjaldt DDoS-angrep, hvor noen av rapportene var knyttet til DDoS-angrep hos en felles leverandør. Det ble i 2020, henholdsvis i begynnelsen og i slutten året, rapportert om to ulike varianter av angrep med infisert programvare. En av dem var SolarWind-saken i 2020, se nærmere omtale i punkt 3.3.1.5. Angrepene kunne gjøre det mulig å komme på innsiden av nettverket og ødelegge eller hente ut data. Ingen av foretakene som rapporterte om disse hendelsene, fant at noen skade hadde skjedd. Det ble videre rapportert om utnyttelse av sårbarhet i egenutviklet applikasjon som var avdekket av en av foretakets kunder, om omfattende phishing-kampanjer med misbruk av foretaksnavn og logo, og om falsk passorddistribusjon.

I tillegg til sikkerhetshendelsene mottok Finanstilsynet fire rapporter der foretakene selv avdekket sårbarheter gjennom sikkerhetstester eller lignende uten at disse var blitt utnyttet.

5.3 Operasjonelle hendelser (driftshendelser)

Rapportering av hendelser fra banker og betalingsforetak

Finanstilsynet mottok i 2020 flest rapporter om hendelser fra banker og betalingsforetak. De fleste rapportene omhandlet driftshendelser. Dette er hendelser som i stor grad rammer betalingstjenestene på ulike måter, fortrinnsvis i form av manglende tilgang til betalingstjenestene, men det kan også være forsinkelser og feil i betalinger. En overvekt av driftshendelsene inntreffer på mandager, etter vedlikehold og oppgraderinger i helgene. I 2020 var det flere driftshendelser som Finanstilsynet vurderte som svært alvorlige. Hendelsen som fikk størst oppmerksomhet, var en driftshendelse i DNB i juni som forårsaket flere dagers forsinket utbetaling av lønn og feriepenger til et stort antall kunder. Videre rammet en driftshendelse hos Nets i juli mange foretaks tilbud av betalingstjenester i flere timer en ettermiddag/kveld. Det var også andre hendelser hos fellesleverandører våren og sommeren 2020 som førte til gjentagende avbrudd i betalingstjenestene. Det ble meldt om to hendelser om manglende levering av data til gjeldsregistre.

Rapportering av hendelser knyttet til systemer for å avdekke hvitvasking og terrorfinansiering

I hvitvaskingsloven stilles det krav om at banker, kredittforetak og finansieringsforetak skal ha elektroniske overvåkningssystemer (AML-systemer) for å avdekke forhold som kan indikere hvitvasking og terrorfinansiering. Finanstilsynet vurderer feil og avvik i disse systemene som alvorlige hendelser som skal rapporteres i henhold til IKT-forskriften. Finanstilsynet mottok i 2020 åtte hendelsesrapporter om ulike typer avvik i AML-systemene. Flere av avvikene i 2020 gjaldt feilaktig behandling av utenlandstransaksjoner som medførte mangelfull overvåkning av disse. Det er et begrenset antall leverandører av AML-systemer, slik at systemfeil hos en av leverandørene kan ramme flere foretak.

Rapportering fra inkassoforetak

Det ble i 2020 rapportert sju hendelser fra inkassoforetak, som er flere enn tidligere år. Finanstilsynet har tidligere mottatt relativt få rapporter om hendelser fra inkassoforetakene og har stilt spørsmål ved om bransjens forståelse av rapporteringsplikten i henhold til IKT-forskriften er god nok. I 2020 sendte Finanstilsynet brev om dette til inkassoforetakene med eksempler på hendelser som skal rapporteres, og etter dette økte antall rapporteringer. Finanstilsynet vurderer systemavbrudd og systemfeil som medfører forsinkelser og avvik fra de lovfestede fristene for kontaktpunktene med skyldnerne i betalingsløpet, som særlig alvorlige hendelser.

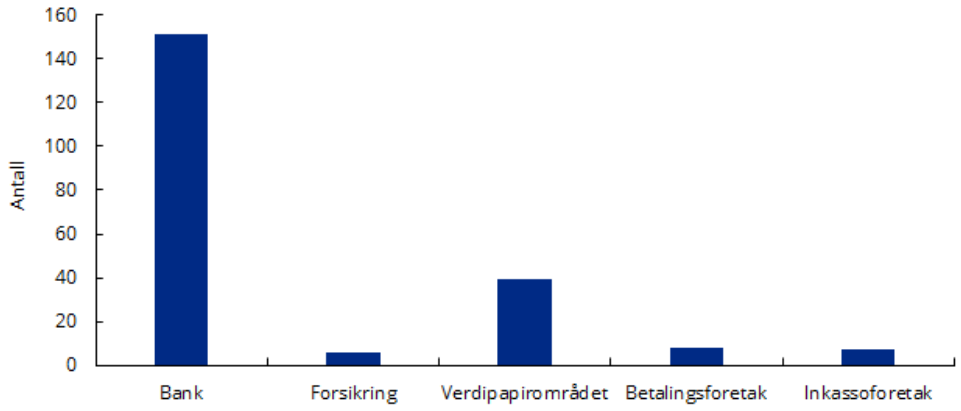
Rapportering fra verdipapirområdet

I 2020 mottok Finanstilsynet 15 rapporter fra sentrale handelsplasser og infrastrukturforetak. Noen få hendelser medførte redusert tilgang, men det var ingen langvarige avbrudd knyttet til handelsplasser i 2020. Finanstilsynet mottok rapporter om 22 hendelser fra verdipapirforetak og forvaltningsforetak, hvorav de fleste beskrev driftsproblemer med redusert tilgang til nettbasert aksjehandel eller manglede lydopptak. Finanstilsynet mottok også to rapporter knyttet til flyttingen av Oslo Børs' handelssystem til Euronext. Disse to rapportene omhandlet problemer som hadde relativt liten innvirkning på tjenestene.

Rapportering fra forsikringsforetak

Finanstilsynet mottok seks rapporter fra forsikringsforetak i 2020. Disse omfattet brudd på konfidensialitet med eksponering av kundedata til andre kunder og brudd på integritet med utsending av forsikringsbevis til kunder som hadde fått avslag på forsikring.

Figur 5.2 Rapporterte hendelser i 2020 fordelt på type foretak



Kilde: Finanstilsynet

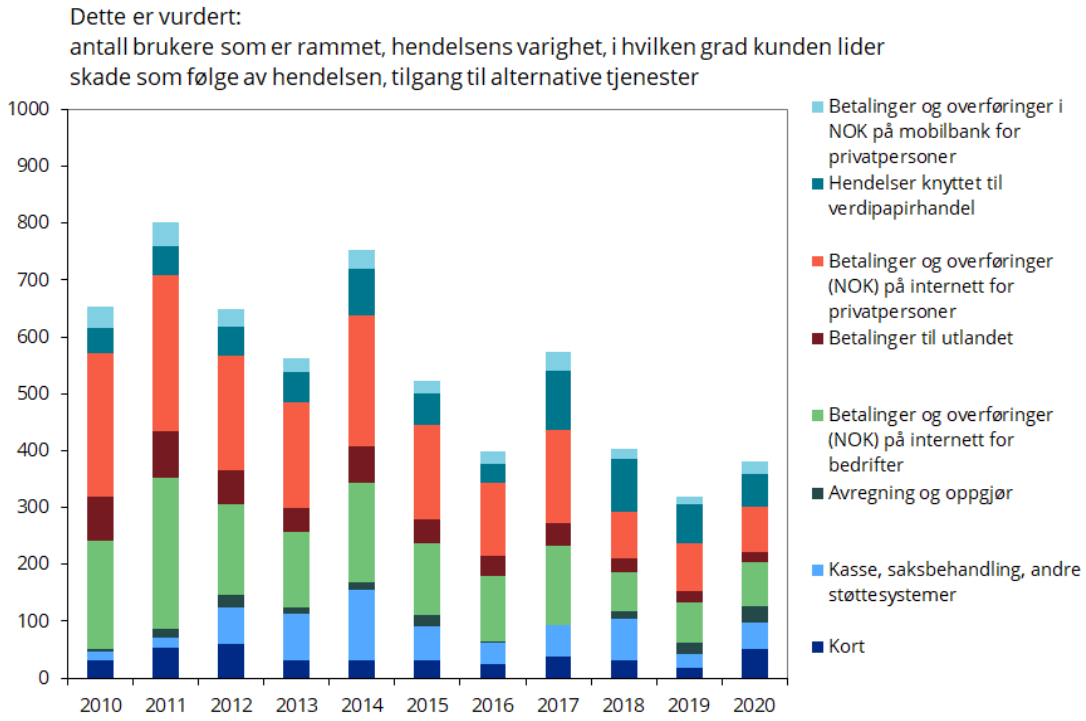
5.4 Analyse av hendelsene som mål på tilgjengelighet

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, mens 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 utviklingen kan følges over tid.

Det framgår av figur 5.3 at betalingstjenestene og kunderettede løsninger var mindre tilgjengelige for kundene i 2020 enn i 2019, men bedre enn tidligere år. Tilgjengeligheten til tjenestene vurderes samlet sett som tilfredsstillende i 2020. 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

Enkelte hendelser har vært alvorlige og har rammet et stort antall brukere. Flere av hendelsene var knyttet til kategorien "Kort" (kortsystemene), som hadde redusert tilgjengelighet i 2020.

Kategorien "Avregning og oppgjør" omfatter alle hendelser som kan ramme betalingene etter at kunden har godkjent dem, slik som forsinkelser, doble reservasjoner og doble posteringer. Innenfor denne kategorien var det flere feil enn tidligere år.

Hendelser knyttet til kategorien "Verdipapirhandel" dekker hendelser knyttet blant annet til aksjehandelsløsninger på internett og hendelser i VPS.

Kategorien "Betalinger og overføringer i NOK på mobilbank for privatpersoner" dekker apper og nettbanker på mobil. Denne kategorien er vektet noe opp fordi bruken av PC-bank synker og mobilbank øker. Tilsvarende er hendelser knyttet til kategorien "PC-bank" vektet noe ned.

Kategorien "Kasse, saksbehandling, andre støttesystemer" dekker også rapporteringssystemer. Reduksjonen i tilgjengelighet for denne kategorien har sammenheng med at det blant annet har vært hendelser som har rammet bredt i bankens systemer.

5.5 Rapportering av avvik i dedikerte grensesnitt (API-er) etter PSD2

Finanstilsynet mottok i 2020 flere meldinger om avvik knyttet til dedikerte grensesnitt. Flesteparten av disse ble rapportert fra tredjeparts betalingstjenestetilbydere, og kun noen få ble rapportert fra kontotilbydere. Avvikene var knyttet både til manglende tilgang til grensesnittene, til dels av lang varighet, og mangler i grensesnittenes funksjonalitet.

Der avvikene ikke ble rettet innen rimelig tid etter at tredjepartstilbydere meldte avvik til kontotilbyder, fulgte Finanstilsynet opp avvik overfor kontotilbyderne.

Ved flere av avvikene informerte ikke kontotilbyderne tredjepartstilbyderne om avviket, tiltak for reetablering eller beskrivelse av mulige alternative løsninger.

Plikten til å rapportere om avvik i dedikerte grensesnitt

Betalingstjenestetilbydere, både kontotilbydere og ytere av de nye betalingstjenestene betalingsfullmakt og kontoinformasjon, skal omgående rapportere om problemer knyttet til dedikerte grensesnitt (API-er) til Finanstilsynet.[35]

Videre skal kontotilbydere ved slike avvik informere tredjepartstilbydere om avviket, tiltak for reetablering og beskrivelse av mulige alternative løsninger.

Terskelen for å rapportere problemer knyttet til dedikerte grensesnitt skal være lavere enn for hendelser etter IKT-forskriften.

Betalingstjenestetilbyderne må selv fastsette rutiner for å ivareta pliktene som følger av regelverket.

[35] https://www.finanstilsynet.no/tema/psd-2---eus-reviderte-betalingstjenestedirektiv/psd2---presiseringer-og-avklaringer-om-regelverket/

6 Utkontraktering

6.1 Melding om utkontraktering

Finanstilsynet mottok i 2020 over 250 meldinger om utkontraktering. I tillegg vurderte Finanstilsynet avtaler om utkontraktering av IKT-virksomhet i forbindelse med behandling av konsesjonssøknader.

Flest av meldingene om utkontraktering var knyttet til endring av leverandører av felles betalingsinfrastruktur til bankene, herunder Nets' salg av konto-til-konto-tjenester til Mastercard og Vipps' planlagte flytting av driften av BankID. Det var behov for omfattende oppfølging av bankenes meldinger knyttet til Nets' salg av konto-til-konto-tjenester til Mastercard, samt Vipps planlagte bytte av driftsleverandør for BankID. Det ble også mottatt et betydelig antall meldinger i forbindelse med oppstart av "Kontant-tjenester i butikk". En del av meldingene ble gitt fra samarbeidende grupper av banker på vegne av flere banker. Av øvrige meldinger var 36 fra forsikringsforetak og 13 fra finansieringsforetak.

Meldingene Finanstilsynet mottar har blitt mer omfattende og detaljerte. Kvaliteten på foretakenes analyser og vurderinger av risiko forut for gjennomføring av IKT-utkontrakteringer synes å øke. Kvaliteten på leverandøravtaler og foretakenes forankring av avtaler om utkontraktering i egen ledelse, viser også en positiv utvikling. Nye foretak er imidlertid ikke like godt kjent med regelverket. Finanstilsynet har også mottatt meldinger der foretak anser en databehandleravtale til å være dekkende som utkontrakteringsavtale når det gjelder rett til innsyn og tilsyn etter regelverket, noe som ikke er tilfelle.

Meldingene om utkontraktering har de siste årene vist en tendens til økt bruk av skytjenester, både for applikasjons- og infrastrukturtjenester. Gjennom utkontrakteringer får foretakene også flere plattformer, som for eksempel systemer hos en driftsleverandør i kombinasjon med ulike skytjenester. Dette gir økt kompleksitet og et mer sammensatt risikobilde. Samtidig kan bruk av skytjenester også gi en rekke positive effekter, som bedre IKT-sikkerhet og billigere tjenester.

Foretakene er selv ansvarlige for at IKT-virksomheten, inkludert tjenester som er utkontraktert, oppfyller alle krav som stilles i IKT-forskriften, jf. forskriftens §12. I tillegg kan også annen sektorlovgivning omfatte detaljerte regler om utkontraktering. Foretakene må etablere leverandøravtaler som tilfredsstiller regelverket, og påse at leverandør og eventuelle underleverandører yter IKT-tjenester i tråd med disse kravene. Finanstilsynet får innsyn i foretakenes utkontrakteringsavtaler ved behandling av meldinger om utkontraktering, jf. finansforetaksloven § 4 c[36], i forbindelse med konsesjonsbehandling, og gjennom tilsyn.

[36] Finanstilsynet har foreslått, og hatt til høring, endringer i meldepliktforskriften, se også punkt 7.7.

6.2 Vipps' planlagte bytte av driftsleverandør for BankID

Vipps, som eier av BankID, planlegger å flytte driften av BankID fra dagens driftsleverandør Nets til DXC, se også punkt 2.3. I forbindelse med byttet har Finanstilsynet mottatt og behandlet endringsmeldinger fra bankene.

Den omfattende bruken av BankID både innen finansnæringen og offentlige tjenester har medført at tjenesten vurderes som samfunnskritisk. For foretak i finansnæringen som kjøper BankID-tjenester, krever IKT-forskriften at banken skal ha innsikt og kunnskap om risikoen knyttet til den utkontrakterte tjenesten. Selv om BankID kan ses på som en fellestjeneste, er det likevel det enkelte foretak som kjøper tjenesten som er ansvarlig for forsvarlig drift og risiko.

Finanstilsynet har bedt både Vipps og bankene som kjøper BankID-tjenester om å gjennomføre risiko- og sårbarhetsvurderinger. Finanstilsynet har også fulgt opp at både Vipps og bankene har på plass beredskapsplaner dersom BankID-tjenesten ikke fungerer som planlagt i forbindelse med flytteoperasjonen.

På bakgrunn av vesentlige forsinkelser i gjennomføringen av flytteprosjektet, har Finanstilsynet fulgt opp at Vipps har gjennomført grundige vurderinger av ny driftsleverandør og at Vipps vil følge leveransene tett opp etter at flyttingen er gjennomført.

6.3 Nets' salg av konto-til-konto-tjenester til Mastercard

Mastercard inngikk i 2019 avtale om kjøp av Nets' virksomhetsområde "konto-til konto-tjenester", som inkluderer blant annet realtidsbetalinger (FOI straksbetalinger), digital regningsbetaling (eFaktura/Avtalegiro) og interbank clearing (NICS), se også punkt 2.3. Salget omfattet virksomheten i det norske foretaket Nets Norge Infrastruktur AS og deler av virksomheten i Nets Branch Norway (NUF). Kjøper av virksomhetsområdene er henholdsvis Mastercard-selskapene Mastercard Payment Services Infrastructure (Norway) AS (MPSI) og Mastercard Payment Services Norway AS (MPSN).

Overdragelsen til Mastercard medførte endringer i bankenes utkontrakteringsforhold, både når det gjaldt deres direkte kjøp av betalingstjenester og deres tilslutning til avtaler om felles operasjonell infrastruktur (FOI) inngått av Bits AS[37]. Bankene var derfor forpliktet til å melde endringene i utkontrakteringsforholdet til Finanstilsynet.

Fra og med høsten 2019 og fram til og med januar 2021 mottok og behandlet Finanstilsynet forhåndsmeldinger og ordinære meldinger om endringer i utkontrakteringsavtalene. Totalt 15 banker sendte ikke melding til Finanstilsynet og ble purret av Finanstilsynet sommeren 2020.

[37] https://www.bits.no/

I tilknytning til behandlingen av utkontrakteringsmeldingene har Finanstilsynet hatt omfattende dialog med en rekke enkeltbanker og bankallianser, samt med Bits AS, når det gjelder FOI-avtalene. I tillegg har Finanstilsynet også hatt dialog med ni filialer av norske banker.

Ved behandlingen av bankenes meldinger ble det avdekket store forskjeller i bankenes interne prosesser for håndtering av avtaler om utkontraktering av IKT-virksomhet.

Mange av meldingene inneholdt gode risikovurderinger av den nye leverandøren, herunder vurdering av leverandørens eiere, landrisiko, samt konkret risikovurdering av det nye avtaleforholdet med angivelse av risikoreduserende tiltak. Meldingene inneholdt også opplysninger om driftsmiljø for IKT-systemene som er omfattet av avtalen.

Behandlingen avdekket også at det var flere banker som ikke hadde sikret ivaretakelse av IKT-forskriftens krav til styrebehandling eller vurdert om avtalen ivaretok IKT-forskriftens krav til avtalens innhold. Flere banker hadde heller ikke overholdt finanstilsynslovens meldeplikt ved inngåelse av avtalene.

Manglene som ble avdekket medførte et omfattende veiledningsarbeid for Finanstilsynet, samt at disse bankene måtte gjennomføre omfattende revisjon av interne rutiner, inkludert rutiner for styrebehandling, gjennomføre risikovurderinger og styrebehandling av bankens risikovurdering og avtalene, samt følge opp dialogen med Finanstilsynet. Bankene ble også bedt om å oversende ytterligere utfyllende og supplerende dokumentasjon som

- risikovurdering av leverandør og underleverandør, samt de nye avtalene, med presisering av risikoreduserende tiltak. Vurdering av om avtalen sikret banken kontroll med drift av tjenestene, om banken hadde sikret at den ble varslet om sub-utkontraktering av tjenester, herunder konsernintern utkontraktering.
- styrebehandling av risikovurdering og avtalene.
- kvalitetssikring av at IKT-forskriften § 12 er ivaretatt i avtalen, herunder at utkontrakteringsavtalen sikrer at leverandørens underleverandører er pålagt å overholde forskriftskravene.
- exit- og beredskapsplaner og vurdering av om disse bør inneholde krav som sikrer at tjenestene omfattet av avtalen ved behov kan driftes fra Norge.

Finanstilsynet hadde, som en del av behandlingen, spørsmål knyttet til flere bankers oppfølging av den nye leverandørens midlertidige utkontraktering av drift og håndtering av eventuell framtidig endring av driftsforholdene, herunder kontroll med den nye leverandørens eventuelle framtidige konserninterne utkontraktering av drift. Flere av disse ble bedt om å revidere/presisere avtalevedlegg som gir informasjon om leverandørens underleverandører.

De fleste meldingene Finanstilsynet mottok manglet informasjon om bankenes FOI-avtaler, med henvisning til at Bits AS håndterte denne avtalen i en egen prosess. Dette avdekket blant annet mangler

i bankenes prosedyrer, mangler i bankenes egne risikovurderinger og manglende styrebehandling av FOI-avtalene. Finanstilsynets behandling og oppfølging av bankenes meldinger har ført til at flere banker har endret sine rutiner og prosesser, noe som gjenspeiler seg i senere meldinger om IKT-utkontraktering.

I dialogen med Bits AS og bankene har Finanstilsynet påpekt at norske bankers tidligere eksklusive rettighet til de norske betalingssystemene opphørte ved etableringen av den nye FOI-rammeavtalen og at dette muligens kan svekke norsk påvirkning/innflytelse på løsningene.

6.4 Kontanttjenester i butikk (KIB)

Vipps, ved BankAxept, etablerte i 2020 i samarbeid med norske banker "Kontanttjenester i butikk" (KIB), se også punkt 2.3. Tjenesten er etablert for å møte finansforetakslovens krav om at "Banker skal i samsvar med kundenes forventninger og behov, motta kontanter fra kundene og gjøre innskudd tilgjengelig for kundene i form av kontanter". Tjenesten erstatter delvis avtalen mellom DNB og Posten om Banktjenester i butikk, som utløp i september 2020.

Mer enn 90 banker har sluttet seg til samarbeidet og tilbyr tjenesten til sine kunder[38]. Kontanttjenester i butikk er så langt tilgjengelig gjennom NorgesGruppens matbutikker og gjør det mulig å ta ut og sette inn kontanter i til sammen 1.431 matbutikker og har en dekningsgrad på 98 prosent av Norges befolkning.

Ved etablering av tjenesten mottok og behandlet Finanstilsynet utkontrakteringsmeldinger fra bankene om å ta i bruk tjenesten, og der meldingen omfattet bankens rolle som konto- og/eller brukerstedsbank. Ved behandling av meldingene ba Finanstilsynet bankene om å bekrefte at en rekke forhold knyttet til utkontrakteringen var ivaretatt før oppstart. Finanstilsynet la særlig vekt på at meldingene var behandlet og godkjent i bankens styre og at kontoførende bank hadde implementert AML-overvåking av kontanttransaksjonene for å ivareta hvitvaskingsregelverkets krav og at det var etablert og gjennomført AML-opplæring av involverte parter i ytelsen av kontanttjenesten.

6.5 Konsesjon til å yte betalingstjenester

I 2020 mottok Finanstilsynet seks søknader om konsesjon til å yte betalingstjenester. Regelverket stiller strenge krav til at foretakene har godt dokumenterte rutiner på områder relatert til IKT- og betalingstjenester. Selv om enkelte av foretakene hadde på plass gode rutiner på områder relatert til IKT- og betalingstjenester, var det også foretak som hadde manglende forståelse av regelverket, vesentlig svakheter i egne rutiner og behov for utstrakt veiledning. Observasjonene viste at kravene for å bidra til å redusere risikoen knyttet til nye ytere av betalingstjenester er viktig.

[38] https://vipps.no/produkter-og-tjenester/privat/kontanter/kontanttjenester-i-butikk/

7. Regulatoriske endringer

Nedenfor omtales fastsatt eller foreslått nytt regelverk og retningslinjer som stiller nye eller endrede krav til foretakenes arbeid på IKT-området, samt veiledninger som beskriver Finanstilsynets forventninger til foretakene.

7.1 Veiledning om utkontraktering

Finanstilsynet publiserte 2. oktober 2020 en veiledning om utkontraktering, herunder utkontraktering av IKT-virksomhet, se rundskriv 3/2020[39]. Rundskrivet gir veiledning om hva som regnes som utkontraktering, begrensninger i adgangen til å utkontraktere og hvordan foretak under tilsyn må identifisere, vurdere og håndtere risikoen knyttet til utkontraktering. Rundskrivet omtaler også finanstilsynsloven § 4c om utkontraktering og meldeplikt til Finanstilsynet.

Rundskrivet opphevet rundskriv 14/2010 om utflytting av bankenes IKT-oppgaver.

7.2 EBAs retningslinjer om IKT-sikkerhet og -risiko

EBA publiserte retningslinjer om IKT-sikkerhet og -risiko (Guidelines on ICT and security risk management) 28. november 2019[40], med virkning fra 30. juni 2020. Finanstilsynet har bekreftet at retningslinjene vil bli fulgt i Norge og har oppdatert sin tilsynspraksis og krav til behandling av IKT-sikkerhetsrisiko i tråd med de nye retningslinjene.

Retningslinjene retter seg mot banker, betalingsforetak og e-pengeforetak, og inneholder blant annet detaljerte krav til hvordan foretak skal sikre seg mot IKT-sikkerhetsrisikoen de eksponeres for. På et overordnet nivå har den norske IKT-forskriften siden 2003 regulert områdene som retningslinjene omfatter. Ett av hovedmålene med retningslinjene er å tydeliggjøre kravene til hvordan IKT-sikkerhetsrisiko skal håndteres i foretakene.

[39] https://www.finanstilsynet.no/nyhetsarkiv/rundskriv/2020/veiledning-om-utkontraktering/
[40] https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2020/eba-har-fastsatt-retningslinjer-om-ikt-sikkerhet-og-risiko/

7.3 EIOPAs retningslinjer om utkontraktering til skytjenesteleverandører

EIOPA publiserte retningslinjer om utkontraktering til skytjenesteleverandører (Guidelines on outsourcing to cloud service providers)[41] 6. februar 2020. Retningslinjene gjelder fra 1. januar 2021. Finanstilsynet har bekreftet at retningslinjene vil bli fulgt i Norge og har oppdatert sin tilsynspraksis i tråd med de nye retningslinjene.

Retningslinjene retter seg mot forsikringsforetak og vil gjelde for alle avtaler om utkontraktering til skytjenesteleverandører som inngås eller endres fra og med 1. januar 2021. Eksisterende utkontrakteringsavtaler av kritiske/viktige oppgaver må tilpasses de nye retningslinjene innen 31. desember 2022. Finanstilsynet skal varsles dersom foretaket innen fristen ikke får tilpasset eksisterende avtaler til de nye retningslinjene. Varselet må inneholde en framdriftsplan med planlagte tiltak for å få utkontrakteringsforholdet i tråd med de nye retningslinjene, eller avviklingsstrategi for å avslutte utkontrakteringsavtalen.

Målet med retningslinjene er blant annet å klargjøre hvilke krav som stilles ved utkontraktering til skytjenesteleverandører og forhold knyttet til skytjenester for kunder og leverandører for å unngå regulatorisk arbitrasje (foretak skal underlegges samme regulatoriske krav til tjenestene i alle EU/EØS-land).

7.4 EIOPAs retningslinjer om IKT-sikkerhet og governance

EIOPA publiserte retningslinjer om IKT-sikkerhet og governance (Guidelines on Information and Communication Technology Security and Governance)[42] 12. oktober 2020. Retningslinjene vil gjelde fra 1. juli 2021. Finanstilsynet legger til grunn at retningslinjene vil bli fulgt i Norge og vil oppdatere sin tilsynspraksis i tråd med de nye retningslinjene.

Retningslinjene retter seg mot forsikringsforetak og inneholder blant annet detaljerte krav til hvordan foretak skal sikre seg mot IKT-sikkerhetsrisikoen de eksponeres for. På et overordnet nivå har den norske IKT-forskriften siden 2003 regulert de områdene som retningslinjene omfatter og retningslinjene vil gi en nyttig utdyping av IKT-forskriftens bestemmelser. Hovedmålene med retningslinjene er å klargjøre kravene til behandling av IKT-sikkerhetsrisiko i foretakene, fastsette minimumskrav til forventede nivåer for informasjons- og cybersikkerhet og unngå potensiell regulatorisk arbitrasje (foretak skal underlegges samme regulatoriske krav til tjenestene i alle EU/EØS-land).

[41] https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2020/nye-retningslinjer-fra-eiopa-for-utkontraktering-til-skyleverandorer/
[42] https://www.eiopa.europa.eu/content/eiopa-finalises-guidelines-information-and-communication-technology-security-and-governance_en

7.5 ESMAs retningslinjer om utkontraktering til skytjenesteleverandører

ESMA publiserte retningslinjer om utkontraktering til skytjenesteleverandører (Guidelines on outsourcing to cloud service providers)[43] 18. desember 2020. Retningslinjene gjelder fra 1. juli 2021. Finanstilsynet legger til grunn at retningslinjene vil bli fulgt i Norge og vil oppdatere sin tilsynspraksis i tråd med de nye retningslinjene.

Retningslinjene retter seg mot infrastrukturforetak, verdipapirforetak og forvaltningsforetak. Målet med retningslinjene er blant annet å hjelpe foretakene med å identifisere, adressere og overvåke risikoen som følger av utkontraktering til skytjenesteleverandører. De gir blant annet foretakene veiledning om hvilke risikovurderinger og due diligence de bør gjennomføre, hvilke styrings-, organisasjons- og kontrollrammeverk som bør innføres og hvordan utkontraktering av skytjenester kan avsluttes, hvilke kontraktselementer avtalene bør inneholde, hva utkontrakteringsavtalene bør omfatte og hvilken informasjon som skal rapporteres til tilsynsmyndighetene.

7.6 Forslag til regelverk om digital operasjonell motstandsdyktighet

EU-kommisjonens forslag til ny lovgivning for digital operasjonell motstandsdyktighet (Digital Operational Resilience Act, DORA)[44,45], skal sikre at alle deltakere i det finansielle systemet har nødvendige tiltak på plass for å redusere faren for cyberangrep og andre risikoer. Den foreslåtte lovgivningen vil kreve at alle foretak skal kunne håndtere alle typer forstyrrelser av og trusler mot informasjons- og kommunikasjonsteknologi (IKT). Forslaget introduserer også et tilsynsrammeverk for IKT-leverandører, for eksempel leverandører av skytjenester. Det foreslåtte regelverket anses EØS-relevant og antas å bli tatt inn i norsk rett når det fastsettes.

For å sikre en helhetlig gjennomføring av kravene til finanssektorens styring av IKT-risiko, omfatter den foreslåtte forordningen en rekke foretakstyper regulert på EU-nivå, noe som vil gjøre det mulig å få til en homogen anvendelse av kravene til risikostyring på IKT-relaterte områder, hensyntatt at det er betydelige forskjeller mellom foretak når det gjelder størrelse, forretningsprofiler og foretakenes eksponering for digital risiko. Det foreslåtte regelverket stiller krav til styring og kontroll av IKT-virksomheten, krav til styring av IKT-risiko, rapportering av IKT-hendelser, testing av operasjonell motstandsdyktighet og oppfølging av leverandører. IKT-forskriften inneholder allerede en rekke av disse kravene, slik at endringene trolig i liten grad vil medføre vesentlige endringer for norske foretak. I tillegg åpner det foreslåtte regelverket opp for deling av informasjon og etterretning knyttet til cybertrusler og sårbarheter, slike norske foretak allerede gjør gjennom samhandlingen med Nordic Financial CERT (NFCERT).

[43] https://www.esma.europa.eu/press-news/esma-news/esma-publishes-cloud-outsourcing-guidelines
[44] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN
[45] https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2020/des/forslag-til-forordning-om-digital-operasjonell-motstandsdyktighet-i-finanssektoren/id2791266/

I tilknytning til forslaget til ny lovgivning for digital operasjonell motstandsdyktighet, er det også foreslått et direktiv med utfyllende bestemmelser[46,47]. Disse omhandler endringer i flere direktiver, enten om endringer i operasjonelle risiko- eller risikostyringskrav eller krysshenvisninger, blant annet i kapitaldekningsdirektivet (CRD), direktivet om markeder for finansielle instrumenter (MiFID II), direktivet om omsettelige verdipapirer (UCITS) og i direktivet om opptak og virksomhet innen forsikring og reassuranse (Solvens II).

7.7 Forslag til endringer i forskrift om unntak fra meldeplikt ved utkontraktering

Finanstilsynet har hatt på høring forslag til endringer i forskrift om unntak fra meldeplikt ved utkontraktering av virksomhet, med høringsfrist 31. mars 2021[48].

Hovedtrekkene i forslaget

Finanstilsynet mener at flere foretakstyper bør omfattes av meldeplikt ved utkontraktering. Dette er dels begrunnet i krav i EU-direktiv, og dels begrunnet i at Finanstilsynet har behov for løpende informasjon om foretakenes utkontraktering. Videre er det foreslått at meldeplikten bare skal gjelde for utkontraktering av virksomhet som er kritisk eller viktig for foretakene, og innebærer at det for en del avtaler gjøres unntak fra meldeplikten.

I tillegg er det foreslått en presisering av hvilke opplysninger meldinger om utkontraktering skal omfatte, og en bestemmelse som stiller krav om at alle foretak under tilsyn skal ha en oppdatert oversikt over alle sine utkontrakteringsavtaler.

[46] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0596&from=EN
[47] https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2020/des/digital-finans-forslag-til-endringsbestemmelser-knyttet-til-kryptoaktiva-og-operasjonell-sikkerhet/id2791267/
[48] https://www.finanstilsynet.no/nyhetsarkiv/horinger/2021/forslag-til-endringer-i-forskrift-om-unntak-fra-meldeplikt-ved-utkontraktering-av-virksomhet/

Vedlegg 1: Foretakenes vurdering av sårbarhet

Nedenfor oppsummeres betalingstjenestetilbyderes vurdering av operasjonell risiko og sikkerhetsrisiko, samt noen øvrige foretaks vurderinger. Finanstilsynet har benyttet det samme skjemaet for begge formål, men enkelte spørsmål er særskilte for betalingstjenestetilbyderes rapportering av operasjonell risiko og sikkerhetsrisiko.

Oppsummeringen omfatter vurderinger fra 124 foretak. Spørsmålene er inndelt i sju temaer:

1. Styring og kontroll
2. IKTs verdi som støtte for beslutninger
3. Drift og katastrofeberedskap
4. Beskyttelse av data
5. ID-tyveri
6. Interne misligheter
7. Hvitvasking

Foretakene er bedt om å vurdere situasjonen/modenheten i foretaket for hver av risikoene beskrevet i skjemaet, og angi om foretaket vurderer at det har en høy, moderat eller lav risiko knyttet til forholdene som beskrives. Dersom risikoen anses å være høy, er foretaket bedt om å om å angi årsaken til dette. Foretakene er også bedt om å vurdere om risikoen anses å være økende, minkende eller stabil. Videre skal foretakene gi en kort omtale av hvilke tiltak som er satt i verk i løpet av det siste året, og en vurdering av om tiltakene anses tilstrekkelige. I tillegg er foretakene bedt om å angi forhold med høyest risiko. Nærmere beskrivelse om utfyllingen av spørreskjemaet er gjengitt etter tabellene.

Tabellene oppsummerer resultatet av spørreundersøkelsen. 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.

Trenden, dvs. om sårbarhetene anses å være økende, stabile eller minkende, 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. "i/a" i kolonnen for 2019 innebærer at spørsmålet ikke var med i fjorårets undersøkelse.

Styring og kontroll

	Sårbarhet	Foretakenes svar	Trend 2019	Trend 2020
1	Vi etterlever prinsippet om 3 Lines of Defence.		→	→
2	Vi har en godt innarbeidet prosess for risikoanalyse. Ansatte er kjent med prosessen og bidrar aktivt og løpende inn i den.		→	→
3	Vi har oversikt over virksomhetskritisk IKT-utstyr og programvare, inklusive lisenser. Vi har oversikt over gyldig konfigurasjon av tekniske løsninger.		i/a	→
4	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.		↗	→
5	Ansatte har stillingsbeskrivelser. Ansattes ansvar når det gjelder kontroll og rapportering inngår i stillingsbeskrivelsen.		→	→
6	Vi har en prosess for utvikling og forbedring av a) rutiner for utvikling og drift og b) kontroll av at rutinene etterleves.		i/a	→
7	Utkontrakteringsavtalene sikrer oss rett til innsyn i alle forhold som gjelder leveransen.		→	→
8	Vi har gode retningslinjer knyttet til sikkerhet. Vi gjør detaljert risikovurdering av betalingstjenestevirksomheten, og en beskrivelse av kontrollen med sikkerheten og tiltak for å beskytte brukerne av betalingstjenestene mot risikoene som er identifisert, inkludert svindel og ulovlig bruk av sensitive opplysninger og		i/a	→
9	Vi har god bestillerkompetanse, juridisk og teknisk.		i/a	→
10	Vi har løpende oppfølging av våre leverandører og leveransene.		i/a	↗
11	Vi har en oversikt som viser hvilke kontroller vi bygger på innenfor hhv. førstelinjekontroll, risikostyring/etterlevelse og internrevisjon (de tre forsvarslinjer), brutt ned på områder som bidrar til å sikre integritet, konfidensialitet og tilgjengelighet. Hvem, og hvilket foretak, som er ansvarlig for å gjennomføre kontrollene inngår i oversikten.		i/a	↘
12	har fokus på bevisstgjøring av medarbeidere og opplæring av medarbeidere.		i/a	→

Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: i/a.

Beslutningsstøtte

	Sårbarhet	Foretakenes svar	Trend 2019	Trend 2020
1	IKT-systemene henter informasjon fra eksterne og interne kilder og sammenstiller og synkroniserer informasjonen til et bilde av foretakets risiko til bruk i styringsøyemed og til		↗	→
2	IKT-systemet gir automatisk et totalbilde av risikoen, for eksempel slik at hvis en hjørnestensbedrift går konkurs, så varsler systemet automatisk om lån til ansatte i bedriften og lån til leverandører til bedriften, slik at vi kan vurdere å tapsavskrive på disse.		→	→
3	IKT-systemene reflekterer kundens evne til å betjene gjelden.		↗	→
4	Informasjonen i våre systemer og registre er korrekte (datakvalitet).		↗	↘
5	Integrasjon mellom systemene skjer på en automatisert måte så langt det er mulig.		→	↘
6	Omfanget av mangler og feil i systemene går ned.		→	→
7	Vi samler inn statistiske opplysninger om drift, transaksjoner og svindel i betalingsformidlingstjenestene, og benytter informasjonen til å gjøre tjenestene sikrere.		i/a	→
8	Vi vurderer fortløpende tiltak for å beskytte kunden, som at 1) kunden kan slå av funksjoner i betalingstjenesten (eksempelvis regionsperre, internettsperre), 2) kunden blir varslet (sms, e-post) når det skjer bevegelser på kundens kontoer / kort, eller ved avviste forsøk på tilgang til kundens kontoer / kort, 3) kunden har god tilgang til kundestøtte.		i/a	→

Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: i/a.

Drift

	Sårbarhet	Foretakenes svar	Trend 2019	Trend 2020
1	Det er risiko knyttet til mangelfulle eller manglende rutiner for endringshåndtering og etterlevelse av rutiner. Hovedårsaken (root cause) til at feil oppstår blir ikke avdekket og/eller korrigert.		i/a	→
2	Når nye IT-løsninger skal utvikles, tar vi i betraktning behovene og løsningene til alle avdelinger som kan bli berørt. Dette for å unngå utfordringer forbundet med "silo-løsninger", slik som omfattende vedlikehold av programmer, komplisert drift og utfordringer med synkronisering av data.		i/a	→
3	Test-systemene er "produksjonslike", dvs. at testdata (anonymiserte), applikasjoner, programvare, styresystemer (SW) og maskinvare er de samme i 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	Før produksjonssetting utføres det sikkerhetstesting. Testingen gjøres av personer som ikke har vært involvert i utviklingen av tjenesten som testes.		→	→
6	Vi gjør regelmessig tester for å teste sikkerheten i tjenestene våre. (Eks. penetrasjonstesting, testing etter TIBER standarden, sårbarhets-scanning).		i/a	→
7	Det er høy grad av kompleksitet i IT-systemene.		i/a	→
8	Vi benytter i høy grad tiltak for å sikre oss mot angrep (Advanced Persistence Threat, trojaner, ransomware, DDoS, e-post angrep). Eksempler på tiltak: Intrusion Detection og Intrusion Prevention, brannmur, antivirus, kontroll av web-trafikk, sikring av e-post, patching og andre tiltak for å sikre stabil drift.		→	→
9	Vi benytter logging i utstrakt grad, og vi har et opplegg for å kunne reagere raskt og adekvat på "unormale forhold" i loggen.		→	→
10	Vi overvåker "tikkende bomber", 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).		→	→
11	Vi har gode tiltak for å avdekke avvik (unormal belastning, unormale porter/ protokoller, avvikende svarstider) i datatrafikken og ta aksjon før skade.		→	→
12	Vi tester kriseløsningene våre i et omfang som gjør oss sikre på at de fungerer som forutsatt.		→	→
13	Vi har gjort risikoanalyse, identifisert områder med høy risiko for nedetid (for eksempel Single Point of Failure) og satt in tiltak for å sikre kontinuerlig drift.		i/a	↗
14	Samarbeidsrutinene og ansvarsforholdene mellom oss og leverandørene er presise og detaljerte.		→	→
15	Det er stort leveransepress.		→	→
16	Det er ikke tilstrekkelig tilgang på kompetanse, herunder kompetanse til å stille krav til leverandører og følge opp leveransene.		↘	→
17	Stor "teknisk gjeld" gir oss unødig risiko når det gjelder endringshåndtering og når det gjelder drift.		i/a	→
18	Mange nye regulatoriske krav gjør at vi stadig må endre systemene våre.		↘	↗
19	Vi har god oversikt over hvor datalinjene går. Vi har god redundans når det gjelder datalinjer.		→	→
20	Vi har gode rutiner for tilgangskontroll og adgangskontroll for egne ansatte, innleide og leverandører.		→	↘
21	Våre medarbeidere gjennomgår opplæring når det gjelder trusler og angrepsscenarier.		↗	→
22	Grensesnittene som tredjeparter benytter for å få tilgang til betalingskontoer er testet og godkjent i samarbeid med		i/a	→
23	Grensesnittene som tredjeparter benytter er sikret i tråd med bestemmelsene i RTS.		i/a	→

Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: i/a.

Beskyttelse av data

	Sårbarhet	Foretakenes svar	Trend 2019	Trend 2020
1	Vi har gode retningslinjer for klassifisering og beskyttelse av strukturert (databaser) og ustrukturert (word, e-post, personlige filområder) informasjon og beskyttelse av informasjonen.		→	→
2	Vi har gode tilgangskontroller når det gjelder ansatte, konsulenter, leverandører, applikasjoners tilganger, systemtilganger, administratortilganger.		↗	→
3	Vi logger tilganger til data og systemer og vi kan skru på varsling dersom det forekommer uautorisert tilgang eller forsøk på tilgang.		→	→
4	Vi har inndelt nettverket i sikkerhetssoner basert på en sikkerhetsgradering av data og funksjoner. Graderingen bestemmer fysisk og logisk (tilgangskontroller, kryptering mv.) sikring av data og funksjoner i sonen.		→	→
5	Vi sikrer data på bærbart utstyr.		→	↗
6	Ved terminering av avtaler om datalagring må leverandøren dokumentere at data er fullstendig slettet.		→	→
7	Vi har rutiner for lagring og overvåkning av sensitiv betalingsinformasjon (informasjon som kan misbrukes til å begå svindel, f.eks. kortdetaljer og påloggingsinformasjon), samt begrensninger i og oversikt over adgang til denne informasjonen.		i/a	→

Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: i/a.

ID-tyveri

	Sårbarhet	Foretakenes svar	Trend 2019	Trend 2020
1	Vi har gode tiltak for å forhindre at en angriper tar over en bruker-ID og misbruker denne.		→	→
2	Vi har god kontroll når det gjelder utlevering, bruk og sletting av logon-id og passord til kunder.		→	→
3	Vi benytter kontroller som forhindrer "skimming" og "Card not present"-svindel.		→	→
4	Vi krever sterk kundeautentisering i forbindelse med betalinger for handel på internett.		→	→

Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: i/a.

Interne misligheter

	Sårbarhet	Foretakenes svar	Trend 2019	Trend 2020
1	Vi har gjort en detaljert risikovurdering og definert		i/a	↘
2	Vi benytter tjenestedeling (dual kontroll) så langt som mulig.		→	→
3	Vi har etablert særskilt logging og varsling når det gjelder situasjoner, scenarier eller kontobevegelser der det etter risikovurderingen under pkt. 1 konkluderes med at det er sannsynlig at det kan skje misligheter. Dette kan være tilbakevaluteringer, bevegelser på interne kontoer, bevegelser på passive kontoer, overføring fra kunde til ansatt og tilbake, ansatte som er i en presset økonomisk situasjon, høy gjeldsgrad)		→	→
4	Vi overvåker ansattes egenhandel.		→	→

Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: i/a.

Hvitvasking

	Sårbarhet	Foretakenes svar	Trend 2019	Trend 2020
1	Vi samarbeider med andre foretak for å få kartlagt midlenes opprinnelse og midlenes bruk.		i/a	→
2	Våre IT-systemer gir et samlet bilde av kunde, kunderelasjoner og kundeadferd (KYC – Know Your Customer).		→	→
3	Vi har elektronisk overvåking av transaksjoner og transaksjonsmønstre.		↗	→
4	Vi har en stadig bedre presisjon når det gjelder flagging av mistenkelige transaksjoner.		i/a	→
5	Det er en risiko for at transaksjonsovervåkingssystemet ikke fanger opp alle betalingstransaksjoner.		i/a	↘
6	AML-systemene benytter i utstrakt grad data fra øvrige systemer.		i/a	→
7	AML-systemene gjenkjenner mistenkelige mønstre over tid.		i/a	→
8	AML-systemene fanger opp at en person har flere kundeforhold på tvers av forretningsenheter.		i/a	→
9	Sanksjonsscreeningssystem har høy presisjon i treff av listeførte personer og foretak.		i/a	→

Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: i/a.

Utfyllingsveiledningen til foretakene

"Finanstilsynet ber foretaket vurderer risikoene som er beskrevet i tabellen nedenfor. I den første kolonnen beskrives risikoen på overordnet nivå. I kolonne to beskrives forhold som kan innvirke på risikoen. Foretaket skal vurdere situasjonen / modenheten i foretaket, og angi i kolonne tre om foretaket vurderer at det har en høy, moderat eller lav risiko knyttet til forholdene som beskrives. Dersom risikoen anses å være høy, ber vi foretaket om å angi i kolonne fire årsaken€ til at verdien er satt til høy. I kolonne fem skal foretaket gi en vurdering av om risikoen anses å være økende, minkende eller stabil. I kolonne seks ber vi foretaket kort omtale hvilke tiltak som er satt i verk siste året, og en vurdering av om tiltakene anses tilstrekkelige. Forhold som ikke er relevant for foretaket besvares med blankt eller I/A.

Eksempel: Foretaket har hatt flere hendelser som har kommet overraskende på foretaket. Det tok fire timer å finne årsaken til feilen og ytterligere to timer å rette den. Foretaket finner at påstanden "Vi har en godt innarbeidet prosess for risikoanalyse. Ansatte er kjent med prosessen og bidrar aktivt og løpende inn i den", ikke er helt dekkende for situasjonen slik den er i foretaket, og foretaket svarer "Høy" i kolonne tre. Basert på analyse av hendelsene, angir foretaket i kolonne fire hovedårsakene til at hendelsene oppstod, og at hendelsene kom overaskende på foretaket. I kolonne seks omtaler foretaket kort tiltak som er gjort for å forbedre dette i løpet av siste år.

Til slutt ber vi foretaket oppgi de forhold foretaket anser utgjør høyest risiko for foretaket. Dette kan være en eller flere risikoer som er spesielt aktuelle for foretaket. Vi ber om at dette angis i kommentarfeltet under tabellene."

Vedlegg 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 som er gjengitt i figur 1.1 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 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: 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 manglende kontroll av foretakets operative ledelse, vurderes som *lav til middels* 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* til *middels* 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 *begrenset* 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 at manglende sikkerhetskompetanse i foretaket medfører vesentlige operasjonelle risikoer, vurderes som *middels til høy* og med *moderat til alvorlig* 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 *middels* 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 til høy* og med *moderat* konsekvens.
- Sannsynligheten for uønsket leverandøravhengighet som følge av foretakets mangelfulle kompetanse om foretakets utkontrakterte tjenester, vurderes som *middels til høy* 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.
- Sannsynligheten for at manglende kvalitetssikring av tjenester anskaffet fra ulike leverandører og underleverandører, som følge av mangelfull oppfølging og kompetanse, samt forankring av egne krav hos leverandøren og underleverandørene, 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**. Samlekarakteren er ikke endret i årets rapport, men Finanstilsynet vurderer at risikoen er noe forhøyet fra 2020 med bakgrunn i økt kriminell aktivitet. Sannsynligheten for uønskede hendelser vurderes som *høy* og konsekvensen som *alvorlig*. Dette er basert på følgende vurderinger:

- Sannsynligheten for at alvorlige svakheter i et foretaks 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 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 kriminelle lykkes med å utnytte sårbarheter i nettverk og applikasjoner før de oppdages (til patch foreligger), vurderes som *middels til høy* og med *alvorlig* konsekvens.
- Sannsynligheten for at alvorlige sikkerhetshull ikke blir tidsnok tettet som følge av mangelfulle sikkerhetsoppdateringer (patch-management), inklusive hos leverandører og underleverandører, 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, eller hvor ansatte i foretaket / personell hos leverandører gjennom trusler ufrivillig benyttes som redskap for digitale angrep, 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 utro medarbeider utnytter svakheter i systemet for økonomisk vinning, vurderes som *lav til middels* og med *begrenset* 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 **middels til høy**. Finanstilsynet observerer at foretakene har blitt bedre på arbeidet med å forhindre informasjonslekkasjer og jobber aktivt med området for å sikre sine verdier. 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 *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 *middels* 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 konfidensiell informasjon som kan benyttes til å skade foretaket sendes eller formidles uautorisert, bevisst eller ubevisst, vurderes som *høy* og med *moderat* konsekvens.
- Sannsynligheten for at ansatte eller personell hos leverandører opererer som innsider og overleverer eller sender konfidensiell informasjon, eksempelvis liste over epostadresser og påloggingsinformasjon, til kriminelle, vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for at konfidensiell informasjon kommer på avveie som følge av manglende kontroll eller feil ved utsendelse av informasjon til kunder vurderes som *middels* og med *moderat* konsekvens..
- Sannsynligheten for at konfidensiell informasjon kommer på avveie på grunn av bruk av bærbart utstyr utenfor kontorets nettverk vurderes som *middels til høy* 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 alvorlig*. 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 *høy* og med *alvorlig* konsekvens.
- Sannsynligheten for driftsproblemer som følge av feil i felles infrastruktur, vurderes som *middels til høy* og med *alvorlig* konsekvens.

- Sannsynligheten for driftsproblemer som følge av manglende kompetanse og tilstrekkelig helhetlig forståelse for og oversikt over arkitektur og de digitale forretningsprosessene, vurderes som *middels* og med moderat til *alvorlig* konsekvens.
- Sannsynligheten for redusert datakvalitet som følge av kompleks integrasjon mellom tjenesteleverandører, vurderes som *lav* og med *moderat* konsekvens.
- Sannsynligheten for driftsproblemer som følge av mangelfull endringsstyring (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 at overvåking av IT-miljøet ikke avdekker unormale forhold ved driften (eks. utgåtte sertifikater, databaser, minnelekkasjer og elektroniske komponenter), vurderes som *middels* og med *alvorlig* konsekvens.
- Sannsynligheten for driftsproblemer grunnet manglende oppfølging av teknisk gjeld, vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for at testsystemene ikke er tilstrekkelig likt produksjonssystemet, vurderes som *middels til høy* 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* dersom 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 *kritisk* 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 mangler i teknisk oppsett og infrastruktur og testing av kriseløsningene, samt evaluering, vurderes som *lav til middels* og med *kritisk* konsekvens.
- Sannsynligheten for manglende oppdateringer, inklusive 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 cyberangrep 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**. Selv om det har vært store endringer i geopolitiske forhold i 2020 grunnet bl.a. pga. koronapandemien, har foretakene vist ved sine tiltak at de håndterer forholdene rundt pandemien på en god måte. 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 *lav til 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 svakheter i rutinene for endringshåndtering (herunder mangelfull testing), vurderes som *middels* 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 middels til *høy* og med *alvorlig* konsekvens.
- Sannsynligheten for at funksjonelle endringer (programvare) introduserer sårbarheter i foretakets forsvarsverk, vurderes som *lav* og med *moderat* konsekvens.
- Sannsynligheten for at en høy endringstakt grunnet ny forretningsfunksjonalitet og regulatoriske krav medfører at løsninger settes i produksjon uten nødvendig kvalitetssikring, 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 *lav til 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 *middels til 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, vurderes som *middels til høy* og med *moderat* konsekvens
- Sannsynligheten for at AML-systemet ikke fanger opp alle betalingstransaksjoner, vurderes som *middels* og med *begrenset til moderat* konsekvens

Sannsynligheten for at risikoer ikke identifiseres, vurderes som *middels* og med *begrenset* konsekvens

Vedlegg 3: Finanstilsynets oppfølging

Sentrale områder for Finanstilsynets 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-/cybersikkerhetsarbeidet vektlegges, samt sikkerhet knyttet til foretakenes IKT-løsninger og organiseringen av overvåkingen. 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 anti-hvitvaskingssystemene er komplette.

Bruk av ny teknologi, større endringer på IKT-området og større endringer i den finansielle infrastrukturen er også aktuelle tema.

Foretakenes styring og kontroll med og regelmessig risikovurdering av, utkontraktert IKT-virksomhet, kvalitet på avtaleverk og foretakenes oppfølging av avtaler mellom foretak og leverandør vil også bli fulgt opp.

Arbeid med betalingssystemer

EUs reviderte betalingstjenestedirektiv (PSD2) 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[49], 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, jf. også uttalelse fra den europeiske banktilsynsmyndigheten (EBA)[50]. I konsesjonsbehandlingen vil det påses at foretakene har godt dokumenterte rutiner på områder relatert til IKT- og betalingstjenester.

Samarbeidet med Norges Bank omkring betalingssystemet og finansiell infrastruktur videreføres.

[49] Lovdata: Forskrift om systemer for betalingstjenester
[50] https://www.eba.europa.eu/eba-calls-national-authorities-take-supervisory-actions-removal-obstacles-account-access-under

Oppfølging av hendelser

I tilsynsvirksomheten er oppfølging av IKT-hendelser er et prioritert område. Finanstilsynet vil i 2021 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.

Det vil også bli fulgt opp at både kontotilbydere og tredjepartstilbydere i samsvar med PSD2 rapporterer avvik og at kontotilbyderne korrigerer avvikene og informerer tredjepartstilbyderne.

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.

Tilsynsvirksomheten omfatter oppfølging av at foretakene gjennomfører risikoanalyser og 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 2021, og tiltak knyttet til funn i tidligere øvelser vil bli fulgt opp.

Særskilte hendelser som koronapandemien 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[51]. Finanstilsynet har ansvaret 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.

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

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

Sammen med Norges Bank har Finanstilsynet sendt på høring forslag til rammeverk for testing av cybersikkerhet i finanssektoren (TIBER-NO) og tar, sammen med Norges Bank, sikte på å implementere dette i løpet av 2021.

Finanstilsynet vil gjennom regelmessige møter med foretak, Nordic Financial CERT og deltakelse i Nasjonalt cybersikkerhetssenter (NCSC) holde seg orientert om utviklingen i trusselbildet.

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[52] 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[53].

[52] Lov om finansforetak og finanskonsern (finansforetaksloven)
[53] Forskrift om finansforetak og finanskonsern (finansforetaksforskriften)

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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

05.2021