FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Finanssektorens bruk av informasjons- og kommunikasjonsteknologi (IKT)

RISIKO- OG SÅRBARHETSANALYSE (ROS)

2022

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. Samtidig er trusselbildet i stadig endring. Under koronapandemien og i forbindelse med krigen i Ukraina 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.[1] De sentrale foretakene i den norske finansielle infrastrukturen har gjennomgående gode beredskapsplaner. Aktørene har hatt kontroll på driftssituasjonen og har raskt iverksatt nødvendige tiltak.

I 2021 var det ingen IKT-hendelser med konsekvenser for finansiell stabilitet. Antall sikkerhetshendelser var omtrent som i 2020 og lavere enn i 2019, mens det var vesentlig flere operasjonelle hendelser. Samlet økte antall rapporterte IKT-hendelser med over 40 prosent, til 292. Ut fra hendelsenes varighet, tidspunkt på døgnet og antall berørte brukere anser Finanstilsynet at tilgjengeligheten til betalingstjenester og andre kunderettede tjenester i 2021 samlet sett var bedre enn i de foregående årene.

Omfanget av digital kriminalitet synes å ha vært på samme nivå i 2021 som i 2020. Hendelser i 2021 avdekket imidlertid alvorlige sårbarheter hos enkelte foretak. Det ble observert forsøk på å utnytte sårbarhetene, men uten at angriperne lyktes med å få tilgang til foretakets IT-systemer.
Så langt har ikke digital kriminalitet rettet mot foretak i den norske finanssektoren ført til alvorlige hendelser.

Foretakene arbeider kontinuerlig med å styrke forsvarsverket. Finansnæringens samhandling gjennom NFCERT[2] bidrar 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.

Hendelser ved bytte av driftsleverandør har de siste årene vist at oppdragsgiver må bli bedre til å kvalitetssikre at leverandøren har tilstrekkelige prosesser, kompetanse og kapasitet til effektivt å håndtere alvorlige hendelser som rammer kritiske tjenester.

Gjennom tilsyn har Finanstilsynet avdekket sårbarheter som utgjør risiko for alvorlige hendelser i finanssektoren. Finanstilsynet har blant annet påpekt svakheter i foretaks arbeid med kontinuitets- og beredskapsplaner. Videre har Finanstilsynet påpekt mangler i dokumentasjon av foretakets egen IKT-

[1] Beredskapsutvalget for finansiell infrastruktur (BFI) er ledet av Finanstilsynet og følger opp beredskap og hendelser i den finansielle infrastrukturen. Lenken viser til temaside på Finanstilsynets nettsted.
[2] Nordic Financial CERT Lenken viser til NFCERTs nettsted.

infrastruktur og mangler knyttet til oppfølging av leverandører. Det er også påpekt svakheter ved sikkerhetsarbeidet, blant annet oppfølging av leverandørers tilgang til foretakets systemer og data.

Ved fusjoner, som ofte er krevende og langvarige prosesser, bør det blant annet foreligge en omforent teststrategi med tydelig ansvarsfordeling. Testingen bør ta utgangspunkt i fastsatte akseptansekriterier og dekke ulike kundetyper, produkter og tjenester og interne produksjons- og kontrollprosesser. Det er også viktig med høy beredskap og kapasitet i kundesentre ved gjennomføring av fusjoner.

For å sikre robustheten i den finansielle infrastrukturen mener Finanstilsynet at foretakene fortsatt bør styrke arbeidet på IKT-området, både for å redusere sannsynligheten for operasjonelle hendelser og for å bedre IKT-sikkerheten. Utviklingen i det digitale trusselbildet må vektlegges.

Beredskapen i det elektroniske betalingssystemet ble i 2021 styrket ved at kapasiteten i reserveløsningen i betalingsterminaler ved bruk av BankAxept-betalingskort er vesentlig økt.

Finanstilsynet anser sårbarheter i foretakenes forsvarsverk mot digital kriminalitet som den mest sentrale IKT-risikoen, der den samlede risikoen anses å være høy og hvor sannsynligheten vurderes høy og konsekvensen alvorlig. Sårbarheter knyttet til IKT-drift, tilgangsstyring og informasjonslekkasje er også sentrale risikoer, der den samlede risikoen anses som middels til høy. Mens risikoen knyttet til foretaks forsvarsverk mot digital kriminalitet og tilgangsstyring er ansett som noe høyere for 2021, er risikoen knyttet til IKT-drift ansett å være noe lavere.

Foretakenes vurderinger av operasjonell risiko og sikkerhetsrisiko, slik dette framkommer i deres rapportering og i dialog med Finanstilsynet, viser blant annet at trusselen fra digital kriminalitet har økt, angrepsflatene har blitt flere, og flere foretak har registrert økt antall angrep. Det pekes på behov for ytterligere IKT-sikkerhetstiltak, kompetanseheving og økte ressurser. Videre vises det til at det er utfordrende å ha gode oversikter over virksomhetskritisk utstyr, programvare, forretningsfunksjoner, prosesser og informasjon, noe som er viktig for å ha kontroll med IKT- og sikkerhetsrisiko, samt at det er viktig å ha tilstrekkelig innsikt i sikkerhetsarkitektur i egne og leverandørers IKT-tjenester. Det vises også til at det er, som i tidligere år, utfordringer knyttet til å rekruttere ansatte med kompetanse innenfor informasjonssikkerhet og oppfølging av utkontraktert virksomhet, og at det er økt risiko knyttet til ny regulering som medfører behov for endringer i IKT-systemene.

Digitaliseringen gir kundene nye, og ofte bedre, tjenester til lavere kostnad. Samtidig skapes det nye risikoer, både for tjenesteytere og for deres kunder. Manglende bruk av sterk kundeautentisering (SKA) ved handel på internett på enkelte brukersteder utsetter kortholdere for risiko for svindel.

At BankID benyttes i stort omfang til både private og offentlige tjenester, og med variasjoner i innloggingskonteksten, medfører en fare for at brukerne ikke er tilstrekkelig årvåkne og kan bli lurt til falske innlogginger. Brukerne kan heller ikke reservere seg mot bruksområder og redusere mulighetsrommet for misbruk. For å redusere risikoen for svindel, utfører tjenesteyter såkalte back-

end-kontroller (etterkontroller) i form av transaksjonsanalyser og kundeanalyser som ledd i godkjenningsprosessen ved innlogging og ved igangsetting av transaksjoner.

Misbruk knyttet til ID-kjennetegn er også et risikoområde. For å redusere risikoen for svindel ved misbruk av ID-kjennetegn anbefaler Datatilsynet forbrukere å aktivere sperre mot kredittvurdering hos kredittopplysningsbyråene[3]. En slik aktivering er i dag krevende for forbrukeren siden hvert enkelt kredittvurderingsbyrå må kontaktes for å legge inn sperren. Datatilsynet har tatt initiativ til en felles sperreløsning i Brønnøysundregistrene.

Finansnæringen har et pågående prosjekt for å utarbeide og implementere tiltak for sikker bruk av digitale banktjenester, der formålet er å bidra til å redusere sannsynligheten for at svindel skal inntreffe og avhjelpe konsekvenser av svindel.

I 2021 var det 147.000 svindeltransaksjoner med kort, mot 205.000 i 2020. Til tross for nedgangen i antall svindeltransaksjoner økte tapene på kortsvindel med 9,9 prosent, til 162 mill. kroner i 2021. Andelen svindeltransaksjoner var størst for grensekryssende transaksjoner. For alle transaksjoner under ett var andelen 0,006 prosent, mens den var 0,2 prosent for transaksjoner utført i land utenfor EØS. For kortbetalinger som er initiert ikke-elektronisk, utgjorde andelen svindeltransaksjoner 0,24 prosent i 2021.

For kontooverføringer, hovedsakelig nettbank, utgjorde tapene 346 mill. kroner i 2021, som er 2,5 prosent lavere enn året før. Tapene er knyttet både til transaksjoner der svindleren utsteder eller modifiserer betalingen, og til transaksjoner der svindleren manipulerer betaleren til selv å gjennomføre betalingen.

Tap som følge av svindel ved sosial manipulering, dvs. der betaler er lurt til å iverksette svindeltransaksjonen, utgjorde 240,6 mill. kroner i 2021. Av dette var 224 mill. kroner knyttet til kontooverføringer og 16,6 mill. kroner knyttet til bruk av betalingskort. Selv om antall svindelforsøk stadig øker, var svindlet beløp i 2021 lavere enn i 2020, da svindel ved sosial manipulering samlet utgjorde 295 mill. kroner. En viktig årsak til nedgangen er trolig at bankene forhindrer en stadig større andel av svindelforsøkene. Svindel gjennom sosial manipulering ser fortsatt ut til å være den mest lønnsomme metoden for kriminelle.

Foretakene har ansvar for hele IKT-virksomheten, også når deler av denne er utkontraktert. Ved utkontraktering må foretakene vurdere en rekke risikoforhold, blant annet knyttet til styring og kontroll, oppfølging av tjenesteleveransene, sikkerhet og kontinuitet og beredskap. Tilnærmet alle foretak under tilsyn av Finanstilsynet har inngått avtaler som innebærer utkontraktering av deler av IKT-virksomheten.

[3] Datatilsynets nettside om kredittvurdering, herunder om sperre mot kredittvurdering hos kredittopplysningsbyråene

Finanstilsynet mottok i 2021 i overkant 170 meldinger om utkontraktering. Finanstilsynet fulgte særskilt opp bankenes planer for beredskap ved gjennomføringen av Vipps' bytte av driftsleverandør for BankID.

Som i de foregående årene viser meldingene om utkontraktering økt bruk av skytjenester for både applikasjons- og infrastrukturtjenester. Foretakene får ofte et høyere antall plattformer de må forholde seg til. Flere plattformer gir økt kompleksitet og et mer sammensatt risikobilde.

Etter Finanstilsynets vurdering er kvaliteten på foretakenes analyser og vurderinger av risiko forut for gjennomføringen av IKT-utkontrakteringer blitt bedre. Kvaliteten på avtaler med leverandører, samt foretakenes forankring av avtaler om utkontraktering i egen ledelse, viser også en positiv utvikling. Enkelte foretak trenger imidlertid å forbedre sitt arbeid med utkontrakteringer.

Hovedtema for Finanstilsynets tilsynsvirksomhet med IKT og betalingstjenester i 2022 er foretakenes styring og kontroll av IKT-virksomheten, foretakenes arbeid med sikkerhet knyttet til foretakenes IKT-løsninger, inkludert cybersikkerhet, og foretakenes beredskapsarbeid og testing av kontinuitets- og kriseløsninger. Videre vil Finanstilsynet gjennom tilsynsvirksomheten vurdere foretakenes styring, kontroll og oppfølging av utkontraktert IKT-virksomhet, foretakenes betalingstjenester og større endringer i den finansielle infrastrukturen.

Finanstilsynet vil fortsatt følge opp IKT-hendelser og sårbarheter i foretakenes IKT-løsninger. 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. Gjennom tilsynsvirksomheten følger Finanstilsynet opp at foretakene ikke deler kundenes data uten samtykke, og at data ikke kommer uvedkommende i hende.

Beredskapsutvalget for finansiell infrastruktur (BFI) følger opp beredskap og hendelser i den finansielle infrastrukturen. I spesielle situasjoner, som ved koronapandemien og krigen i Ukraina, vil BFI særlig følge opp IKT-virksomheten og beredskapen hos de viktigste aktørene.

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

2 FINANSIELL INFRASTRUKTUR

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 betalinger og transaksjoner i finansielle instrumenter blir registrert, avregnet og gjort opp.

Svikt hos sentrale aktører i finansnæringen eller i infrastrukturen kan få betydelige samfunnsmessige konsekvenser.[4] Den finansielle infrastrukturen er kompleks, sammensatt og omfatter mange aktører og leverandører. Manglende robusthet eller lavt sikkerhetsnivå hos én enkelt aktør eller leverandør kan utgjøre et svakt ledd i de samlede verdikjedene og hendelser kan smitte over på andre aktører. Direktoratet for samfunnssikkerhet og beredskap (DSB) har utpekt finansielle tjenester som en samfunnskritisk funksjon.[5] DSB har på oppdrag fra Justis- og beredskapsdepartementet et pågående arbeid med å revidere oversikten over kritiske samfunnsfunksjoner, der Finanstilsynet har gitt innspill.

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 uvedkommende får tilgang til kunde- og kontodata og kompromitterer disse eller gjør data utilgjengelige, kan kunder og foretak få betydelige utfordringer. De samfunnsmessige konsekvensene vil kunne bli særlig store dersom foretak som opererer på vegne av mange eller alle foretak, rammes. Finanssektoren er også avhengig av infrastruktur som el-forsyning og telekommunikasjon.

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

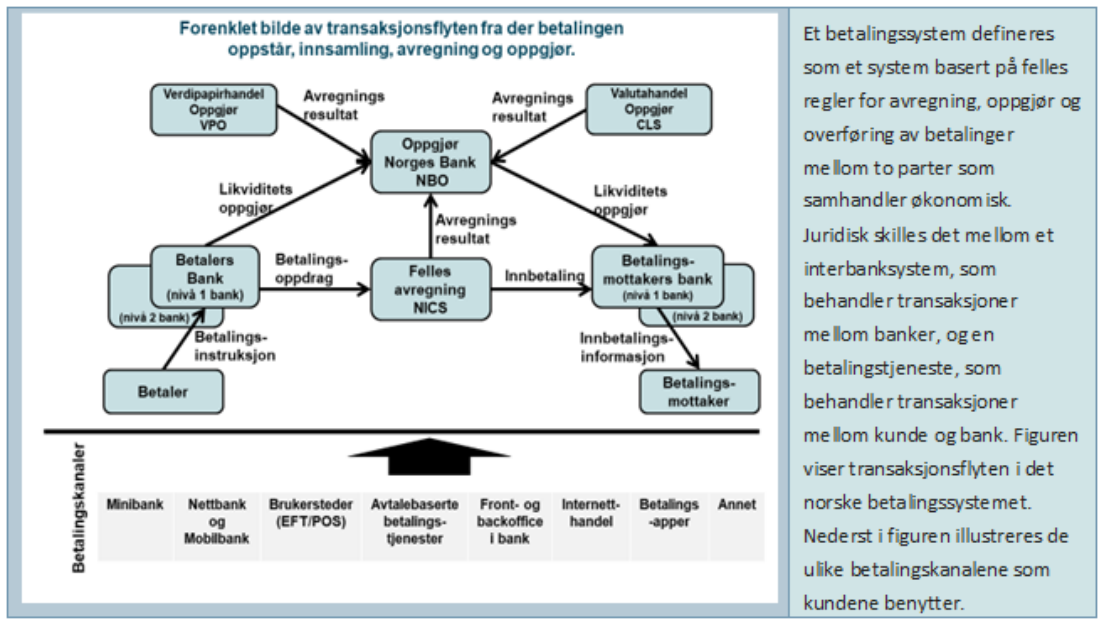
[4] Sikkerhetsloven angir blant annet økonomisk stabilitet og handlefrihet som nasjonale sikkerhetsinteresser, jf. sikkerhetsloven §1-5 Definisjoner (Lovdata). Dette omfatter finansiell infrastruktur og objekter som er avgjørende for at sivilsamfunnet skal fungere.
[5] Direktoratet for samfunnssikkerhet og beredskap (DSB): Samfunnets kritiske funksjoner

Transaksjonsflyten i det norske betalingssystemet

Den finansielle infrastrukturen består av betalingssystemet og verdipapiroppgjørssystemet, samt verdipapirregisteret, 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.



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.

2.2 Beredskapsutvalget for finansiell infrastruktur

Beredskapsutvalget for finansiell infrastruktur (BFI) 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 leder og er sekretariat for utvalget. I utvalget deltar sentrale myndigheter og aktører i den finansielle infrastrukturen. BFI har regelmessige møter og gjennomfører årlige beredskapsøvelser. Arbeidet i BFI, der blant annet alvorlige og kritiske hendelser gjennomgås, bidrar til at Finanstilsynet får et bredt og godt bilde av tilstanden i den finansielle infrastrukturen. Nærmere omtale finnes på Finanstilsynets nettsted, på nettsiden om Beredskapsutvalget for finansiell infrastruktur.

2.3 Samarbeid innen sikkerhetsområdet

Samfunnskritiske virksomheter i finanssektoren

I sikkerhetsloven[6] er økonomisk stabilitet og handlefrihet angitt som én av flere nasjonale sikkerhetsinteresser[4] 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 innen finanssektoren er det Finansdepartementet som fatter vedtak om at foretaket helt eller delvis skal underlegges sikkerhetsloven. Departementet har truffet vedtak overfor enkelte private aktører, men ikke innenfor Finanstilsynets ansvarsområde. Arbeidet er ikke ferdigstilt.

Foretak som er av avgjørende eller vesentlig betydning for en GNF, kan være mer utsatt for angrep fra utenlandsk etterretning. Trusler fra utenlandske statlige aktører er beskrevet under punkt 3.2.2.

Samarbeid og informasjonsutveksling gir bedre risikoforståelse

Samarbeid og informasjonsutveksling mellom finansforetakene i Norge gjennom Nordic Financial CERT (NFCERT)[2] 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.

Finanstilsynet er utpekt av Finansdepartementet som sektorvist responsmiljø (SRM)[7] med oppgave å håndtere IKT-sikkerhetshendelser i finanssektoren innenfor Finanstilsynets ansvarsområde. Finanstilsynet utøver rollen sammen med NFCERT.

[6] Lovdata: Lov om nasjonal sikkerhet (sikkerhetsloven)
[7] Nasjonal sikkerhetsmyndighet (NSM): Rammeverk for håndtering av IKT-hendelser

Finanstilsynet deltar som partner i Nasjonalt cybersikkerhetssenter (NCSC), 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 samt mulighet for å samhandle og utveksle informasjon med andre aktører ved håndtering av cybertrusler og -angrep. Finanstilsynet deltar også i NSMs SIG[8] IKT, som er et samarbeidsforum for myndigheter som fører tilsyn med IKT-sikkerhet i sin sektor.

Finanstilsynet og Norges Bank etablerte i 2021 rammeverket TIBER-NO[9] for testing av cybersikkerhet i finansiell sektor. Det er også etablert fora for overordnet oppfølging, styring og involvering av næringsaktører og andre relevante myndigheter. Formålet med 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 3.2.5.

Europeisk samhandling og informasjonsutveksling

Det europeiske systemrisikorådet (ESRB) publiserte i januar 2022 en strategi for å redusere risikoen for finansiell ustabilitet som følge av cyberhendelser.[10] Det pekes blant annet på behovet for å utvikle makroreguleringsvirkemidler som fanger opp systemisk cyberrisiko. Videre anbefaler ESRB at det opprettes et europeisk rammeverk for koordinering ved systemiske cyberhendelser (EU-SCICF), jf. bestemmelse om tverrsektorielt samarbeid i forslag til forordning om digital operasjonell motstandsdyktighet i finanssektoren (DORA)[11]. Formålet er å sikre rask kommunikasjon og koordinering mellom tilsynsmyndigheter og med andre relevante myndigheter for å unngå koordineringssvikt dersom en alvorlig hendelse oppstår.

2.4 Endringer i den finansielle infrastrukturen og fellestiltak innen finansnæringen

Det ble i løpet av 2021 gjennomført og varslet flere vesentlige endringer i den norske finansielle infrastrukturen. Enkelte av de planlagte endringene gjennomføres i 2022, andre i 2023–2024.

Mastercard besluttet i 2021 å overta driften av bankenes betalingsformidlingstjenester, bankenes felles

[8] SIG står for "spesialinteressegruppe"
[9] TIBER står for "Threat Intelligence-based Ethical Red Teaming", se Finanstilsynets nyhetssak 21. oktober 2021: Norges Bank og Finanstilsynet etablerer rammeverk for testing av cybersikkerhet i finansiell sektor (TIBER-NO)
[10] European Systemic Risk Board (ESRB): Mitigating systemic cyber risk (januar 2022)
[11] EUs forslag til regelverk om digital operasjonell motstandsdyktighet: Digital Operational Resilience Act. Se også omtale i ROS 2021 og regjeringens EØS-notatbase: Forslag til forordning om digital operasjonell motstandsdyktighet i finanssektoren

avregningssystem for norske kroner (NICS) og felles operasjonell infrastruktur (FOI-tjenester)[12]. Nets har bistått Mastercard med drift av disse løsningene etter overdragelsen av Nets' konto-til-konto-tjenester til Mastercard i 2021. Det er ventet at overføringen vil starte i løpet av 2022 med sluttdato i 2024.

Vipps AS endret i oktober 2021 driftsleverandør for BankID. Skiftet av leverandør fra Nets til DXC medførte vesentlige kapasitetsutfordringer, særlig for vanlig (banklagret) BankID. BankID på mobil var i liten grad berørt, se punkt 5.5.

I 2013 ble felles operasjonell infrastruktur for straksbetalinger ("Straks FOI") etablert, og løsningen ble gradvis tatt i bruk av de fleste bankene. Løsningen er nå under videreutvikling som en del av moderniseringsprosjektet knyttet til NICS, hvor blant annet meldingsformatet som sendes inn, skal endres fra NISOK/NIBE til ISO 20022-format. I løpet av 2022 vil bankene, etter migrering til ISO 20022, sende sine straksbetalinger direkte til avregningsløsningen NICS Real. Straks FOI-en fra 2013 vil saneres etter at alle bankene har migrert til nytt meldingsformat og til NICS Real.

Norges Bank bistår bankene med oppgjør av transaksjoner gjennom oppgjørsfunksjonen NBO. I juni 2021 sendte Norges Bank på høring en utredning om sentralbankens rolle som oppgjørsbank ved innføring av realtidsbetalinger også for oppgjør av interbanktransaksjoner. Norges Bank skisserte to alternative løsninger:

1) anskaffelse og etablering av et eget system for oppgjør av realtidsbetalinger i Norges Bank
2) samarbeid med andre sentralbanker i Europa gjennom tilknytning til eurosystemets TIPS-løsning[13]

Både banker, bankallianser og sentrale leverandører i Norge avga høringssvar. Norges Bank besluttet høsten 2021 å innlede forhandlinger med ECB om deltakelse i Eurosystemets TIPS-løsning.[14]Endringene som følger av Norges Banks beslutning, vil kunne ha vesentlig betydning for betalingssystemet og -tjenester i Norge.

Eika Alliansen inngikk i 2020 avtale med Tietoevry om leveranse av kjernebankløsninger til lokalbankene i alliansen. Overgangen fra SDC til Tietoevry er planlagt gjennomført i 2022–2023.

[12] Felles operasjonell infrastruktur omfatter områder der banknæringen i fellesavtaler i regi av oppdragsgiver har fastsatt at alle banker skal benytte leveranser fra én operasjonell enhet for gjennomføring av bestemte betalingsformidlings- og/eller informasjonsformidlingsoppdrag som BankAxept, BankID og flere av bankenes betalingstjenester, deriblant AvtaleGiro og eFaktura. Se Rammeavtale om utvikling, forvaltning og drift av felles operasjonell infrastruktur (FOI) (lenke til BITS' nettsted)
[13] Target Instant Payment System (TIPS) – Eurosystemets infrastruktur for realtidsbetalinger
[14] Norges Bank, 3. november 2021): Norges Bank vil forhandle med ECB om deltakelse i Eurosystemets TIPS-løsning

Avtalen innebærer at andelen norske banker som benytter Tietoevry som driftsleverandør til finanssektoren, øker betydelig. Det vil gi økt konsentrasjonsrisiko.

For å levere bedre tjenester over landegrensene i Norden inngikk Vipps i 2021 avtale om en felles løsning for Vipps lommebok og betalingsløsninger, Danske Banks lommebok Mobilpay og OP Financial Groups lommebok Pivo. Gjennomføringen krever tillatelse fra myndigheter i flere land. Avtalen innebærer også at BankAxept og BankID skilles ut fra lommebokvirksomheten i Vipps og etableres i eget selskap.

Forbedret beredskap i det elektroniske betalingssystemet

Beredskapen i det elektroniske betalingssystemet ble i 2021 styrket ved at kapasiteten for bruk av BankAxept betalingskort i betalingsterminaler ble vesentlig økt. Forbedringene er gjennomført hos samfunnskritiske aktører i detaljhandelen tilknyttet kjeder med nasjonal eller regional utbredelse, som tilbydere av dagligvarer, medisin og drivstoff. Kravet til tilbydernes brukersteder er at sju døgns forventet omsetning skal kunne håndteres i reserveløsninger. For beløp over 1.500 kroner skal det fortsatt innhentes særskilt autorisering. Bedre reserveløsninger reduserer kontantenes betydning i beredskapssammenheng og gir tilbydere av kontanttjenester noe bedre tid til å fremskaffe økt mengde kontanter.

Bedre sikkerhet i digitale kanaler

Finansnæringen startet i 2019 gjennom Bits et prosjekt for å analysere, vurdere, anbefale og implementere tiltak for sikker bruk av digitale banktjenester. Formålet er å bidra til å redusere sannsynligheten for at svindel skal inntreffe og avhjelpe konsekvenser av svindel. Prosjektet skal også fremme forebyggende arbeid mot svindel og styrke overvåkingen. Det ses på både preventive, avvergende og oppfølgende tiltak av både kort- og langsiktig karakter. Mange av tiltakene er knyttet til BankID og bruken av digital ID, men omfatter også tiltak som supplerer bruken av digital ID. Et av tiltakene er innføring av en bransjenorm knyttet til opptak av usikret kreditt, mens andre tiltak er knyttet til bedre og tydeligere informasjon om BankID. Flere av tiltakene reduserer risiko som Finanstilsynet har påpekt i tidligere ROS-rapporter.

Digitalt samarbeid offentlig privat (DSOP)

Offentlig sektor og finansnæringen har fortsatt sitt samarbeid om digitalisering og effektivisering av viktige tjenester i samfunnet gjennom DSOP[15].

Den mest kjente tjenesten, samtykkebasert lånesøknad, er tatt i bruk av mer enn 95 prosent av alle norske banker. Det er samtidig flere prosjekter som er i realiserings- eller planleggingsfasen, blant annet innenfor antihvitvasking. For noen av tjenestene er det behov for regulatoriske avklaringer før fullstendig funksjonalitet kan tas i bruk.

[15] BITS' nettsted: Digital Samhandling Offentlig Privat og Aktivitetsrapport DSOP 2021

Flere av løsningene bygger på eksisterende infrastruktur og løsninger i enten offentlig eller privat regi. Målet er at tjenestene skal gi betydelig effektivisering og kostnadsbesparelser. Erfaringen fra flere av prosjektene er at tversektoriell utveksling av data gir regelverksutfordringer som må løses. Både opprinnelig formål for datainnhenting og sektorspesifikt regelverk kan legge føringer for videre deling av informasjon.

3 FINANSTILSYNETS OBSERVASJONER OG VURDERINGER

3.1 Den finansielle infrastrukturen er robust

Finanstilsynet anser den norske finansielle infrastrukturen som robust. Det var i 2021 ingen større IKT-hendelser som hadde konsekvenser for finansiell stabilitet. Foretakenes driftsstabilitet var tilfredsstillende og bedre enn tidligere år.

Det ble rapport vesentlig flere hendelser i 2021 enn i 2020. Andelen sikkerhetshendelser var omtrent som i 2020. Selv om det ble rapportert langt flere operasjonelle hendelser, har Finanstilsynet ut fra hendelsenes varighet, tidspunkt og antall berørte brukere vurdert tilgjengeligheten til betalingstjenester og andre kunderettede tjenester som bedre i 2021 enn i de to foregående årene.

Det var i 2021 i hovedsak god regularitet på avregnings- og oppgjørssystemene, selv om det var noen enkelthendelser. Det var også god regularitet på kommunikasjonen med det internasjonale meldingsnettverket for betalinger og verdipapiroverføringer SWIFT[16] og det internasjonale oppgjørssystemet CLS[17].

Omfanget av digital kriminalitet øker år for år, og foretakene må forholde seg til et trusselbilde i kontinuerlig endring. Så langt har digital kriminalitet ikke ført til systemkriser eller alvorlige hendelser hos foretak i den norske finanssektoren. Imidlertid ble det også i 2021 funnet noen alvorlige sårbarheter hos enkelte foretak, som kunne medført store konsekvenser dersom de hadde blitt utnyttet.

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

[16] SWIFTs nettsted: About us
[17] CLS' (Continuous Linked Settlement) nettsted: About us. Amerikansk finansinstitusjon som tilbyr oppgjørstjenester til sine medlemmer i valutamarkedet (FX)

3.2 Det digitale trusselbildet er i endring

Trusselbildet er i endring også for finansiell sektor. Blant annet har det 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 i foretakene.

Trusselen fra aktører som leter etter sikkerhetshull i programvare med stor utbredelse ser ut til å øke. Sikkerhetshull som utnyttes kan medføre informasjonslekkasje og/eller uautoriserte endringer i foretakenes systemer og infrastruktur.

Omfanget av kriminelle angrep mot finansforetakenes digitale systemer synes å ha vært på omtrent samme nivå i 2021 som i 2020. Samtidig fortsetter foretakene arbeidet med å videreutvikle sine systemer for overvåking av unormal aktivitet, automatisk håndtering av oppdagede hendelser og avverging av angrep. Angrep avverges som oftest før de får konsekvenser for foretaket og foretakets kunder.

Foretakene arbeider kontinuerlig med å styrke sin kompetanse innenfor cybersikkerhet. Som omtalt under punkt 2.3 bidrar finansnæringens gode samhandling gjennom NFCERT[7] 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.

Foretakene må videreføre sitt arbeid med å kartlegge risiko- og sårbarheter, iverksette preventive tiltak og forberede seg på å måtte håndtere angrep og følgeskader av slike angrep. Beskyttelse av konfidensiell informasjon og bevisstgjøring av egne ansatte om det digitale trusselbildet er viktige deler av dette arbeidet.

Finanstilsynet observerer fortsatt 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.

3.2.1 Organisert kriminalitet som trusselfaktor

Organisert cyberkriminalitet har oftest et finansielt formål. Det vil si at de kriminelle går etter mål som gir størst mulig gevinst til lavest mulig kostnad. Såkalte løsepengevirus (ransomware) er en typisk metode.

Organiseringen av angrepene har utviklet seg, med økt spesialisering og samarbeid mellom ulike grupperinger. Tjenester fra kriminelle aktører omfatter blant annet informasjonsinnhenting, salg av informasjon om digitale sårbarheter, phishing-kampanjer og kompetanse på penetrering av foretakenes

digitale beskyttelsesmekanismer. Bruken av løsepengevirus[18] er generelt økende blant kriminelle organisasjoner, men har til nå ikke fått store konsekvenser for foretak i finanssektoren. Det er sannsynlig at det vil komme stadig mer avanserte angrep fra slike grupperinger, noe som stiller økende krav til det digitale forsvaret hos foretak og institusjoner i finansiell sektor i Norge.

Finanstilsynet anser at organisert cyberkriminalitet fortsatt vil representere en betydelig trussel for norske finansinstitusjoner.

3.2.2 Andre stater som trusselfaktor

Stater er i besittelse av store ressurser som kan benyttes til cyberangrep. Blant annet anser NSM at truslene mot finansiell sektor i Norge kommer fra blant andre Russland og Kina. NSM publiserer jevnlig oppdaterte risiko- og trusselvurderinger, herunder om angrep fra stater.[19]

I etterkant av oppstarten av krigen i Ukraina ble det ikke registrert noen økning i uønsket digital aktivitet mot norske foretak i finanssektoren. Risikoen vurderes likevel som forhøyet, særlig dersom konflikten eskalerer ytterligere eller varer ved. Situasjonen krever forsterket overvåking, forhøyet beredskap og gjennomgang av responsplaner og -kapasitet blant foretak i finansiell sektor. Det er særlig viktig å fjerne passive og utdaterte systemer og komponenter som ikke er i bruk, gjennomføre sikkerhetsoppdateringer og verifisere at egne systemer er fri for korrumpert kode.

Det er avdekket at ukrainske IT-systemer ble korrumpert med skadelig kode lenge før krigen i Ukraina ble igangsatt.[20] Disse erfaringene understreker betydningen av at foretakene allerede før en konflikt eller situasjon oppstår, må ha fokus på å hindre at uvedkommende kan komme seg inn i foretakets systemer og introdusere ondsinnet kode. Erfaringer fra krigen i Ukraina bør inngå i foretakenes risikovurderinger.

3.2.3 Angrep på verdikjeder

Finansielle tjenester er ofte kjennetegnet ved leveranser fra ulike leverandører og underleverandører i tillegg til koblinger mellom aktørene. Cyberkriminelles utnyttelse av slike digitale verdikjeder har vist en økning i senere tid, og trusselnivået for denne formen for angrep ventes fortsatt å øke. Slike angrep kan for eksempel utføres ved at cyberkriminelle introduserer sikkerhetshull i koden hos en kompromittert underleverandør. Den korrumperte koden distribueres så videre i verdikjeden og kan resultere i at et stort antall foretak påføres et sikkerhetshull i sine IT-systemer, noe som en trusselaktør kan utnytte på et senere tidspunkt.

[18] Se blant annet blogg 16. mai 2021 på Dataequiments nettsted: NSM informer om økning i løsepengevirus
[19] Nasjonal sikkerhetsmyndighet (NSM) – temaside: Nasjonalt cybersikkerhetssenter (NCSC)
[20] Digi.no – artikkel 24. februar 2022: Skadevare viser at angrepet på Ukraina har vært forberedt i flere måneder, mener cybersikkerhetsselskap

Kjente eksempler på verdikjedeangrep er SolarWinds i 2020, Microsoft Exchange Server i 2021 og Apache Log4j i 2021, som alle rammet store organisasjoner på flere kontinenter, og Kaseya-angrepet i 2020, som blant annet medførte at flere hundre svenske butikker midlertidig måtte stenge.

Avdekking av verdikjedeangrep kan være vanskelig av flere årsaker. Digitale verdikjeder er ofte komplekse og kan krysse landegrenser og involvere flere nasjonale myndigheter. En stadig økende grad av utkontraktering og økt bruk av komponenter i komplekse løsninger vanskeliggjør kontrollen med innholdet i systemene. Anerkjent god praksis er å holde systemer oppdatert for å redusere risikoen for cyberangrep. Det kan derfor være utfordrende for foretakene å balansere mellom det å snarest mulig oppdatere egne systemer med programvareoppdateringer (patcher) og endringer fra leverandører og å gjennomføre tilstrekkelig testing av programvareoppdateringer og endringer før de installeres i produksjonsmiljøet.

Tiltak som bør vurderes mot verdikjedeangrep:

- Mikrosegmentering[21] og kryptering av interne nettverk for å hindre uønskede tilganger og spredning av kode.
- Overvåking av nettverkstrafikk for å avdekke avvikende mønster i datatrafikk eller atferd.
- Styrke kontrollen med systemleveranser, leverandører og leverandørers bruk av underleveranser, samt utkontrakteringer som omfatter IT-avhengigheter generelt.

3.2.4 Angrep på sentrale tjenesteleverandører og datasentre

IKT-driften i finanssektoren er i betydelig grad utkontraktert til et relativt lite antall sentrale tjenesteleverandører og datasentre, som ofte også leverer viktige tjenester til andre sektorer. Hvis det først oppstår problemer hos en sentral tjenesteleverandør, kan det få ringvirkninger til store deler av finanssystemet og andre viktige samfunnsfunksjoner i Norge. Slike aktører kan derfor være attraktive mål for en angriper. Samtidig kan sentrale tjenesteleverandører ha mer ressurser og kompetanse til å utvikle robuste løsninger og nødvendig beredskap enn foretakene enkeltvis. Bruk av tjenesteleverandører kan dermed også bidra til å redusere risikoen for at cyberangrep fører til alvorlige hendelser i finanssektoren.

Foretakene bør ha oversikt over avhengigheter av sentrale tredjeparter, for eksempel driftssentraler, tjenesteleverandører, herunder utkontraktering, og andre foretak og organisasjoner man samarbeider med, og vurdere sårbarheten som følge av eventuelle vellykkede angrep mot disse.

Foretakene bør også gjennomføre realistiske beredskapsøvelser der scenarioet er bortfall av enkelte eller flere av tredjepartene som framkommer av sårbarhetsanalysen omtalt ovenfor.

[21] Mikrosegmentering er å dele nettverk, datasentre og skyimplementeringer i segmenter for å blant annet etablere sikkerhetskontroller og beskytte dem individuelt.

3.2.5 Nasjonalt tiltak – TIBER-NO

Norges Bank og Finanstilsynet besluttet høsten 2021 å etablere rammeverket TIBER-NO[22] for testing av cybersikkerhet i den norske finansielle sektoren. Formålet med rammeverket er å bidra til finansiell stabilitet gjennom økt motstandskraft mot cyberangrep i virksomheter som har funksjoner som er kritiske for det norske bank- og betalingssystemet. Flere europeiske land, herunder Nederland, Danmark og Sverige, har innført tilsvarende rammeverk og startet testing og kvalitetssikring av kritiske og viktige funksjoner i egen finansiell sektor.

3.2.6 Tiltak i foretakene

Det enkelte foretak har ansvar for digital sikring av egne systemer. Dette omfatter også de delene av virksomheten som er utkontraktert. Arbeidet er tredelt og består av kapasitet til å motvirke og til å avdekke angrep og ha gode planer og løsninger for reetablering av systemer etter angrep.

Tiltak for å motvirke angrep

Et viktige tiltak for å kunne motvirke digitale angrep er at produksjonssystemene er oppdatert med nye, kontrollerte og godkjente versjoner og sikkerhetsoppdateringer. Det er i tillegg viktig å fjerne passive og utdaterte systemer og komponenter som ikke er i bruk. Ved å gjennomføre risikovurderinger og etablere hensiktsmessige kontrollfunksjoner for endringshåndtering forebygges verdikjedeangrep. Nødvendig opplæring og kompetanseheving på IT-sikkerhetsområdet for organisasjonen generelt og IT-sikkerhetsorganisasjonen spesielt, er også viktig.

Tiltak for å avdekke angrep

For å kunne avdekke angrep må foretakene selv ha nødvendig kompetanse og vurdere bruk av eksterne spesialisttjenester. Videre er overvåkingsverktøy som kan avdekke uønsket aktivitet påkrevd.

I tillegg anbefales det at foretakene gjennomfører sikkerhetstester basert på anerkjente prinsipper.

Beredskap

Finansforetak må sørge for at virksomheten kan gjenopprettes etter digitale angrep og ha oppdaterte og testede planer for dette. I tillegg til at de må ha planer for å gjenopprette systemer og eventuelt tapte data, må de ha planer for å håndtere en hendelse inntil systemer og eventuelt tapte data er gjenopprettet. Foretaket må også sørge for å ha kommunikasjonsplaner.

Foretakene bør gjennomføre scenariobaserte beredskapsøvelser jevnlig. Erfaringer fra beredskapstestene bør gjennomgås systematisk for å eliminere svakheter og mangler i beredskapssystemer og -rutiner.

[22] Finanstilsynets nyhetssak 21. oktober 2021: Norges Bank og Finanstilsynet etablerer rammeverk for testing av cybersikkerhet i finansiell sektor (TIBER-NO)

Det er også viktig at foretakene tester hvor raskt man kan reetablere foretakets systemer ved ulike scenarioer og vurdere hvilke konsekvenser en eventuell nedetid vil kunne ha for foretaket og foretakets kunder.

3.3 Koronapandemien og krigen i Ukraina

Finanstilsynet har de siste par årene rettet stor oppmerksomhet mot risiko og utfordringer i den finansielle infrastrukturen som følge av koronapandemien, og siden februar i år også krigen i Ukraina. I tillegg til ordinære møter, har BFI i denne perioden avholdt flere ekstraordinære møter for å følge opp de sentrale foretakene i den norske finansielle infrastrukturen og deres ivaretakelse av sikker og stabil drift, i tråd med utvalgets mandat. Møtene i BFI 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 for å forbedre overvåkingen og sikre økt beredskap og responskapasitet ved hendelser. Sentrale temaer er konsekvenser av endringer i det geopolitiske landskapet og det digitale trusselbildet, herunder avhengighet av leveranser fra landene som er i krig, og til besluttede sanksjoner, blant annet utestengelse av flere russiske banker fra SWIFT-nettverket[16].

Erfaringene viser at de sentrale foretakene i den norske finansielle infrastrukturen har beredskapsplaner som raskt kan iverksettes. Foretakene og deres leverandører har vist at de har kontroll på driftssituasjonen og har etablert tiltak.

Finanstilsynet og BFI retter særlig oppmerksomhet mot virksomheter som støtter kritiske funksjoner i finanssektoren, herunder funksjoner som er definert som samfunnskritiske av Direktoratet for samfunnssikkerhet og beredskap. Disse funksjonene omfatter 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

Nasjonalt cybersikkerhetssenter (NCSC) har etablert et forum for sektorvise responsmiljø (SRM-forum[7]). Blant annet har Finanstilsynet, i samarbeid med NFCERT[2], redegjort for arbeidet i finanssektoren og vurderinger av konsekvenser for sektoren av sikkerhetssituasjonen som følge av krigen i Ukraina.

3.4 Tilsyn med IKT og betalingstjenester

Det ble i 2021 gjennomført 21 tilsyn der IKT og betalingstjenester var tema, herav i ni banker, tre betalingsforetak, to forsikringsforetak, ett fondsforvaltningsforetak, ett infrastrukturforetak, tre gjeldsinformasjonsforetak og to revisjonsselskap. Som følge av koronapandemien ble de fleste

tilsynene gjennomført digitalt. I tillegg til de særskilt omtalte tilsynstemaene nedenfor ble det også gjennomført tilsyn med kontotilbyderes grensesnitt for tredjeparter i henhold til betalingstjenestedirektivet (PSD2), tilsyn med de tre forsvarslinjene i styringen og kontrollen av foretakets IKT-systemer og tematilsyn hos flere banker om antihvitvasking, hvor systemer for elektronisk overvåking av mistenkelige transaksjoner var hovedtema for tilsynet.

Nærmere omtale av utførte tilsyn finnes på temasiden på Finanstilsynets nettsted[23].

3.4.1 Kontinuitets- og beredskapsplaner

De gjennomførte tilsynene i 2021 avdekket at mange foretak mangler en forretningsmessig konsekvensanalyse som underlag for sine beredskapsplaner, en såkalt Business Impact Analysis (BIA). En slik analyse er viktig for hvor godt kontinuitets- og beredskapsplaner vil fungere og for å optimalisere kriseløsninger. Beredskapsplaner må testes tilstrekkelig og verifiseres slik at man vet at de vil fungere i en krise. For banker i en gruppe er det viktig at den enkelte bank stiller krav om å bli involvert i testplanleggingen i større grad enn i dag. Den enkelte bank må sikre at den får innsikt i testingen og at de områder banken har karakterisert som kritiske, blir tilstrekkelig testet. Infrastrukturforetak og andre større foretak med samfunnskritiske funksjoner må utarbeide en særskilt beredskapsplan for videreføring av tjenestene.

Forretningsmessig konsekvensanalyse

Forretningsmessig konsekvensanalyse (BIA[24]) er en analyse som gjennomføres for å kartlegge effekten en hendelse vil kunne ha på et foretaks forretningsprosesser og tjenester. En slik analyse tar utgangspunkt i kartlegging og vurdering av prosesser og tjenester som er kritiske for foretakets virksomhet. Vurderingen omfatter også en kartlegging og klassifisering av de aktiviteter og ressurser som behøves for å levere virksomhetskritiske prosesser og tjenester. Den forretningsmessige konsekvensanalysen legger videre grunnlaget for foretakets kontinuitets- og kriseplaner. Foretaket må sikre at test- og øvelsesaktiviteter, også utkontraktert virksomhet, tar utgangspunkt i foretakets forretningsmessige konsekvensanalyser for å sikre at kontinuitet i kritiske forretningsprosesser og -tjenester ivaretas ved en uønsket hendelse. Foretaket bør etablere rutiner for gjennomføring av forretningsmessige analyser for å sikre at kontinuiteten i forretningskritiske tjenester og prosesser ivaretas.

Både i Den europeiske bankstilsynsmyndighetens (EBA) retningslinjer om IKT-sikkerhet og -risiko[25] og i Den europeiske forsikringstilsynsmyndighetens (EIOPA) retningslinjer om IKT-sikkerhet og styring[26] framgår det at foretakene bør utarbeide forretningsmessige konsekvensanalyser.

[23] Finanstilsynets: Tilsynsrapporter for IT og betalingstjenester
[24] Business Impact Analysis
[25] EBA: Guidelines on ICT and security risk management
[26] EIOPA: Guidelines on information and communication technology security and governance

3.4.2 Dokumentasjon av komponentene i IKT-infrastrukturen

Finanstilsynet fant ved tilsyn mangler i foretakenes dokumentasjon av egen IKT-infrastruktur. En oppdatert og fullstendig oversikt over komponentene i IKT-infrastrukturen, inkludert informasjon om programvare og programvareversjoner, er en viktig del av sikkerhetsarbeidet. Kravet til dokumentasjon omfatter både komponenter foretaket selv drifter, og komponenter driftet av leverandører. For sistnevnte må foretaket sikre at den enkelte leverandør vedlikeholder en slik oversikt.

3.4.3 Leverandøroppfølging

Finanstilsynet påpekte ved flere tilsyn i 2021 at foretak manglet dokumenterte risikovurderinger av utkontraktering av IT-oppgaver eller anskaffelser av nye IT-systemer. Finanstilsynet avdekket også at foretak hadde avtaler om utkontraktering som manglet krav om at foretaket skal sikres rett til innsyn og kontroll med den utkontrakterte IKT-virksomheten.

3.4.4 Sikkerhet

Tilgangsstyring

Tilsynene i 2021 avdekket at mange foretak mangler tilstrekkelige rutiner for kontroll og oppfølging av leverandørenes tilganger til foretakets systemer og data. Spesielt alvorlig er dette dersom det også mangler logging eller rutiner for oppfølging av logger. Finanstilsynet forventer at foretakene har kontroll med hvilke tilganger medarbeidere hos leverandøren(e) har, og kan dokumentere dette, herunder privilegerte tilganger og tilganger til sensitive data. Finanstilsynet anbefaler også en større bruk av rollebaserte tilganger, hvor tilgangene tildeles basert på en forhåndsdefinert rolle med rettigheter.

Finanstilsynet påpekte etter tilsyn i 2021 at bruk av lokale administratorrettigheter på foretakets arbeidsstasjoner ikke bør forekomme. Slike rettigheter medfører at foretakets systemportefølje blir lettere tilgjengelig for uønskede hendelser og digitale angrep. Kun medarbeidere i foretakets IT-avdeling bør ha slike administrasjonsrettigheter.

Sikkerhetstester

Foretakenes bruk av sikkerhetstesting øker. Testing er viktig for å avdekke sårbarheter i applikasjoner, nettverk og arkitektur. Imidlertid kan sikkerhetstesting medføre situasjoner der leverandøren av testene eller ansatte i foretaket urettmessig får tilgang til sensitiv informasjon, og det kan oppstå uønskede hendelser som påvirker sikkerheten og stabiliteten til systemene. Finanstilsynet merket seg gjennom tilsyn i 2021 at flere foretak mangler retningslinjer for gjennomføring av sikkerhetstesting. Slike retningslinjer skal blant annet beskrive risikovurderinger som skal utføres knyttet til testingen, frekvens på testingen, vilkår for valg av tredjepartsleverandør og hvordan uønskede hendelser skal håndteres. Retningslinjene bør bygge på internasjonalt anerkjente standarder.

3.4.5 Gjeldsinformasjonsforetak

Gjeldsinformasjonsloven, som trådte i kraft høsten 2017, åpner for at private aktører kan få konsesjon til å etablere registre for å motta og utlevere gjeldsopplysninger. Formålet med ordningen er å bidra til bedre kredittvurderinger og forebygge gjeldsproblemer blant enkeltpersoner.

Finanstilsynet gjennomførte i 2021 tilsyn med de tre foretakene som etablerte gjeldsregistre i 2019. Tema for tilsynene var virksomhetenes IKT- og risikostyringssystemer med vekt på sikkerhet for at persondata ikke kommer på avveie og at gjeldsinformasjonen til enhver tid er korrekt og tilgjengelig for aktuelle brukere. Gjeldsinformasjonsforetakene har få medarbeidere innenfor IKT, og Finanstilsynet pekte blant annet på tiltak for ajourhold av dokumentasjon av daglige kvalitetskontroller og å redusere avhengigheten av nøkkelpersonell.

3.4.6 Fusjoner mellom banker

Fusjoner av banker er ofte krevende operasjoner med varighet over lengre perioder, ofte over år. Prosessen krever stor grad av planlegging, testing og nøyaktighet ved gjennomføring av endringene og flytting av data.

Det ble også i 2021 gjennomført fusjoner av banker. Finanstilsynet fulgte prosessene og identifiserte noen områder som må tas særlig hensyn til i en fusjon. Banker som fusjonerer, bør ha en omforent teststrategi med tydelig ansvarsfordeling. Testingen av IKT-systemene bør ta utgangspunkt i fastsatte akseptansekriterier og dekke ulike kundetyper, utlån/ innlån, betaling, AML, depot/sikkerheter, arkiv og disposisjonsrett/verge, produksjon av kontoutskrifter og reaktivering av betalingsavtaler knyttet til spareavtaler.

Ved gjennomføring av endringer i IKT-systemene er det viktig å ha høy beredskap og kapasitet i kundesenteret for å håndtere henvendelser, både for å gi kundene trygghet for sine midler og for tidlig å avdekke eventuelle større problemer som måtte oppstå.

3.5 Kontotilbyderes PSD2-grensesnitt

Den offentligrettslige og deler av 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.

PSD2 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.

I flere andre land er konkurransetilsynsmyndighetene også gitt plikter i forbindelse med PSD2 og har i den sammenheng vært pådrivere i arbeidet med å øke konkurransen i markedet for betalingstjenester, se blant annet henvisning til rapport datert 5. november 2021 fra Competition and Markets Authority om Governance of Open Banking[27].

Kontotilbydere (banker og e-pengeforetak) skal etter loven tilby minst ett grensesnitt som gir foretak med konsesjon rett til å få tilgang til kundens konto etter avtale med kunden, se Artikkel 30 i delegert kommisjonsforordning (EU) 2018/389[28]. Nærmere regler om egenskaper ved grensesnittet og informasjonen som inngår, framgår av forskrift om betalingstjenester og forskrift om systemer for betalingstjenester.

Finanstilsynet følger opp at kontotilbyderne tilbyr grensesnitt i samsvar med regelverket. Blant annet fikk enkelte banker i 2021 varsel om pålegg om retting. Finanstilsynet gir på en egen temaside[29] nærmere veiledning om forhold kontotilbyderne må ivareta i sine grensnitt, herunder presiseringer og avklaringer om regelverket. Etter Finanstilsynets oppfatning er det fortsatt enkelte mangler i grensesnittene som flere kontotilbydere tilbyr, noe som kan skape utfordringer for betalingsfullmektiger og opplysningsfullmektiger sin bruk av disse.

3.6 Foretakenes vurderinger av risiko og sårbarhet

Foretakenes vurderinger av risiko og sårbarhet er nedenfor omtalt med utgangspunkt i betalingstjenesteyteres årlige rapportering til Finanstilsynet[30] av operasjonell risiko og sikkerhetsrisiko samt informasjon innhentet gjennom dialog med en rekke foretak.

3.6.1 Foretakenes vurdering av viktige forhold

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

Knapphet på ressurser

Innenfor informasjonssikkerhet er det stor etterspørsel etter IKT-sikkerhetsressurser. Foretakene peker blant annet på at ressursmangelen kan bli en utfordring for områder som krever krysskompetanse, for eksempel sikkerhetstjenester ved bruk av skytjenester. Utfordringen med å rekruttere informasjonssikkerhetskompetanse synes hovedsakelig å være færre tilgjengelige ressurser enn det

[27] Competition and Markets Authority (CMA): Governance of Open Banking 5. november 2021
[28] Lovdata: Delegert kommisjonsforordning (EU) 2018/389
[29] Finanstilsynets nettsted: PSD2 – Presiseringer og avklaringer om regelverket
[30] 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.

markedet har behov for. Intern rekruttering og opplæring kan avhjelpe ressursknappheten. Foretakene trekker fram at det kan synes som ressurspersoner foretrekker å knytte seg til foretak eller grupperinger som har et etablert sikkerhetsmiljø av en viss størrelse.

Utkontraktering – oppfølging av tredjepart

Foretakene har styrket sin interne kompetanse innen både innkjøp og oppfølging av utkontrakterte IKT-tjenester. Området 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 flerleverandørstrategi erfarer at konseptet øker kompleksiteten når det gjelder både teknologi og sikkerhet. Samhandling mellom ulike plattformer kan gi utfordringer for kompatibiliteten og krever ofte spesialtilpasninger ("skreddersøm").

Datakriminalitet

Foretakene er samstemte om at risikoen for digital kriminalitet har økt og at angrepsflatene har blitt flere. Flere foretak har registrert økninger i antall angrep. 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.

Foretakene peker på at phishing fortsatt er den mest brukte metoden for digital kriminalitet. Profesjonaliteten blant kriminelle aktører har økt, og foretakene har observert at de spesialiserer seg på ulike typer trusler. Det har igjen medført at verdikjeden for trusselaktører har blitt lengre. For mange foretak er det viktig å knytte seg til nettverk med datakriminalitet som tema, eller å holde seg oppdatert gjennom å tilegne seg innsikt fra internasjonale og nasjonale myndigheter.

Foretakenes bruk av tofaktorautentisering 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 arbeidsstedets nettverk eller annen sikker tilkobling (VPN).

Foretakenes erfaringer med digital kriminalitet tyder på at sabotasje kan 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.

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 systemer). God dokumentasjon vurderes også ofte som en forutsetning for at reetablering etter IKT-hendelser kan gjennomføres innenfor fastsatte tidskrav.

Kontinuitetsledelse og kriseledelse

For mange foretak har det vært et skifte i retning av å ha egne ansatte med ansvar for kontinuitets- og kriseledelse. Forretningsområdene trekkes oftere inn i diskusjonen siden disse miljøene best kan vurdere forretningsmessige konsekvenser ved driftsavbrudd. Videre er testing av gjenopprettingsrutiner viktig for å sikre at foretakets løsninger fungerer etter hensikten.

Tilgangsstyring

Foretakene gir uttrykk for at de har store utfordringer med å følge opp tilgangsstyring for utkontrakterte IKT-tjenester. Særlig gjelder dette brukeridentiteter med utvidede tilgangsrettigheter, for eksempel ved ettersyn av logger for å kontrollere at bruken er basert på tjenstlige behov. Stadig flere foretak vurderer bruk av zero trust-prinsippene[31] for tilgangsstyring. Tilgangsstyring og bruk av utvidede rettigheter har tradisjonelt sett vært tillitsbasert.

Styringsmodell og internkontroll

Finanstilsynet er gjennom dialog med foretakene blitt kjent med at det i stadig økende grad legges vekt på å sikre klare skiller mellom første- og andrelinje i internkontrollen. Arbeidet med å skille mellom første- og andrelinje er tidkrevende og krever ofte endringer i organisasjonen. Det tar ofte lang tid før de ulike rollene fungerer etter hensikten og andrelinjefunksjonen blir en tydelig premissgiver for førstelinjen; dette fordi kompetansen sitter i ulike enheter i organisasjonen. Basert på Finanstilsynets erfaringer er foretakenes størrelse av betydning for evnen til å sette opp en organisasjon med en klar deling av første- og andrelinjens internkontrolloppgaver.

Datakvalitet

Sikring av god datakvalitet er et område foretakene prioriterer i større grad enn tidligere. Foretakets medarbeidere er gjennom sitt daglige virke sentrale i arbeidet med å sikre kvaliteten. Faren for at feil i data svekker beslutningsgrunnlaget er størst innenfor arbeidet med anti-hvitvasking. Styring og kontroll av data har alltid vært en viktig oppgave for foretakene, men vurderes nå som et av de aller viktigste satsingsområdene. I sine strategier legger foretakene vekt på at å være datadrevet. Erfaringene viser at konsekvensene av dårlig datakvalitet har blitt mer alvorlige.

Geopolitiske forhold

Vurdering av landrisiko og andre geopolitiske forhold har fått økt oppmerksomhet av foretakene på grunn av krigen i Ukraina. Rapporter fra både norske myndigheter og samarbeidsorganer som NFCERT viser at situasjonen er spent og at trusselnivået vurderes som høyt. Til tross for dette har det knapt vært økning i aktiviteter som innebærer en sikkerhetstrussel mot den norske finansnæringen. Foretakenes beredskap mot cyberangrep var allerede før konflikten på et høyt nivå. Beredskapen er derfor i liten grad hevet etter Russlands angrep på Ukraina.

[31] Zero trust-prinsippet betyr kort at man aldri skal stole på noen og alltid sjekke.Wikipedia.org: Zero trust security model

Foretakenes vurderinger av risiko knyttet til utkontrakterte tjenester fra utenlandske leverandører, særlig utenfor EØS, har økt i frekvens og får stor oppmerksomhet i foretakene. Om vurderinger viser at risikoen er høyere enn foretakets fastsatte risikotoleranse, er tjenesteutførelse i flere tilfeller hentet tilbake fra utlandet til leverandører i Norge eller foretaket selv.

3.6.2 Vurdering av operasjonell risiko og sikkerhetsrisiko

Finanstilsynet har innhentet vurderinger av operasjonell risiko og sikkerhetsrisiko fra betalingstjenestetilbydere[32] (foretak). For nærmere detaljer vises det til vedlegg 1.

Styring og kontroll

Basert på innrapportert materiale framgår det at de fleste foretak på et overordnet nivå anslår risikoen forbundet med styring og kontroll som lav. Omkring halvparten av foretakene melder om middels risiko knyttet til manglende eller mangelfulle oversikter over virksomhetskritisk utstyr og programvare, inkludert lisenser. Foretakene viser til at de utarbeider oversikter over virksomhetskritisk utstyr og programvare og holder disse oppdatert. Noen bruker programmer som Intune[33] for slik oversikt.

Oversikter over virksomhetskritisk utstyr, programvare, forretningsfunksjoner, prosesser og informasjon

For å ha kontroll med IKT- og sikkerhetsrisiko stilles det krav til foretakenes systematiske arbeid med å ha oversikt over virksomhetskritisk utstyr, programvare, forretningsfunksjoner, prosesser og informasjon og risikoene forbundet med disse.

EBAs retningslinjer om IKT-sikkerhet og -risiko (Guidelines on ICT and security risk management)[25] og EIOPAs retningslinjer om IKT-sikkerhet og governance (Guidelines on information and communication technology security and governance)[26] er viktige retningslinjer å se hen til i arbeidet med etablering av slike oversikter.

Retningslinjene inneholder anbefalinger om at foretakene bør etablere et utstyrsregister og en oversikt over funksjoner og prosesser. Videre framgår det at foretakene bør gjennomføre risikovurdering og klassifisering av funksjoner, prosesser og utstyr.

For nærmere omtale av retningslinjene for oversikter over virksomhetskritisk utstyr, programvare, forretningsfunksjoner, prosesser og informasjon, se vedlegg 5.

[32] Fristen for innrapportering var 15. februar 2022. Foretakene sendte dermed inn sine svar i forkant av krigen i Ukraina.
[33] Microsoft Intune er et skybasert styringsverktøy for mobilenheter som har som mål å sørge for felles styring av både foretakets og ansattes eget (BOYD) utstyr på en måte som beskytter foretakets informasjon.

Et markant flertall av foretakene mener det er middels risiko forbundet med manglende eller mangelfulle retningslinjer knyttet til sikkerhet, herunder risikovurderinger av betalingstjenestevirksomheten, kontroller med sikkerhet og tiltak for å beskytte brukere mot identifiserte risikoer. Flere viser til at det stort sett foreligger risikovurderinger og retningslinjer, som revideres jevnlig.

Halvparten av foretakene mener det er en moderat risiko knyttet til tilstrekkelig bevisstgjøring og opplæring av medarbeidere. Flere foretak rapporterer om at opplæring vektlegges, særlig av nyansatte, at sikkerhetskurs avholdes, og at det gjennomføres tiltak for bevisstgjøring av ansatte.

Beslutningsstøtte

Halvparten av foretakene mener risikoen for at mangler og feil i systemene øker, er moderat. Flere av foretakene viste til at BankIDs overgang til ny driftsleverandør medførte et høyere antall feil i perioden etter overgangen. Flere større foretak viser også til at antall feil generelt er økende grunnet blant annet økt kompleksitet og større endringer i løsninger. Flere betalingsforetak har rapportert at mangler og manglende driftsstabilitet i bankenes PSD2-grensesnitt innvirker på drift og stabilitet i deres betalingstjenester.

Drift og katastrofeberedskap

Et stort flertall av foretakene anser risikoen i forbindelse med nye regulatoriske krav som moderat eller høy. Nye krav medfører ofte at systemene må endres, og foretakene viser til at dette er utfordrende, siden det kan kreve kompetanse som kan være vanskelig å få tak i. Særlig pekes det på det reviderte betalingstjenestedirektivet (PSD2), personopplysningslovgivingen (GDPR), ny finansavtalelov og hvitvaskingsloven og -forskriften som regelverk som krever særskilt oppmerksomhet og ressurser. Over halvparten av foretakene viser også til at det foreligger en moderat risiko knyttet til såkalt teknisk gjeld i etablerte IT-systemer, og til at kompleksiteten i IT-systemene er høy.

Flere foretak peker på at det stadig blir vanskeligere å sikre tilgangen til nødvendig kompetanse for å utforme krav til leverandører og følge opp leveranser. Flere foretak viser også til en generell mangel på ressurser som kan følge opp utkontraktert virksomhet. Videre viser noen foretak til at komplekse systemporteføljer og eierstrukturer bidrar til økende risiko.

> Flere betalingstjenestetilbydere trekker fram at regulatoriske krav og ønsker om utvikling krever god tilpasningsevne og behov for riktig kompetanse, som det er stadig mer krevende å få tak i.

Over halvparten av foretakene mener at risikoen for at testsystemene ikke samsvarer med produksjonssystemene, er moderat. Flere foretak melder om at de jobber med å forbedre og videreutvikle testsystemene. Mer enn halvparten av foretakene mener utførelse av sikkerhetstesting før

produksjonssetting er forbundet med moderat risiko. Enkelte foretak melder om at det benyttes eksterne for dette.

Når det gjelder risikoanalyse, herunder å identifisere områder med høy risiko for nedetid og tiltak for å sikre kontinuerlig drift, mener litt over halvparten at risikoen er moderat. Foretakene viser til at systemene testes jevnlig og at risikobildet varierer og derfor må vurderes fortløpende.

Mer enn halvparten av foretakene anser komponenter som gradvis slites, eller verdier som gradvis når nivåer som krever inngrep som en moderat risiko. Enkelte foretak kategoriserer også slike "tikkende bomber" som forbundet med høy risiko. Flere foretak viser til at oppfølgingen ligger hos driftsleverandør.

Flere foretak trekker fram trusselen om cyberangrep, spesielt løsepengevirus, som en risiko som er økende og krever preventive tiltak. Et mer komplekst trusselbilde gjør at det blant enkelte foretak påpekes et behov for kompetanseheving og økte ressurser.

Omtrent halvparten av foretakene mener det er en moderat risiko knyttet til manglende opplæring av medarbeidere i håndtering av trusler og angrepsscenarioer. Flesteparten av foretakene har gjennomført sikkerhetskurs, og flere gjør dette på årlig basis.

Mange betalingstjenestetilbydere trekker fram at et stadig mer komplekst cybersikkerhets-trusselbilde fordrer økt bruk av eksterne kompetansemiljøer i tillegg til opplæring av interne medarbeidere. Det arbeides derfor aktivt med å bevisstgjøre alle ansatte om potensielle trusler, slik at de kan bli best mulig rustet til å møte trusler som de kan bli eksponert for i en hektisk arbeidshverdag.

Beskyttelse av data

Over halvparten av foretakene mener det er lav risiko knyttet til beskyttelse av både ustrukturerte og strukturerte data, og til det å ha gode retningslinjer for klassifisering av data. Resterende foretak mener imidlertid at denne risikoen er moderat. Foretakene viser til at de har etablerte retningslinjer og benytter ulike verktøy for å øke sikkerheten.

ID-tyveri

De fleste foretakene mener at risikoen for ID-tyveri er lav. En mindre andel mener imidlertid at manglende kontroller som forhindrer uautorisert kopiering av betalingskort (skimming) og misbruk av kortinformasjon der det fysiske kortet ikke er til stede ("Card not present"-svindel), er forbundet med høy eller moderat risiko. Foretakene viser til at de overvåker transaksjoner med tanke på svindel, og at sikkerhetsmekanismer, som sikker kundeautentisering og 3D-Secure, er tatt i bruk.

Interne misligheter

Omtrent halvparten av foretakene anslår risikoen som moderat når det gjelder kontrollen med interne misligheter og mislighetsscenarioer. Tilbakemeldingene indikerer at foretakene har fokus på dette trusselområdet. Omtrent halvparten melder om moderat risiko knyttet til at logging og varsling ikke er tilstrekkelig. De fleste foretakene viser til at de har innført systemer for overvåking, kontroller eller stikkprøver, men ikke alle har etablert særskilt loggføring av aktiviteter i sine systemer.

Det er verdt å merke seg at både PST og NSM viser til at utenlandsk statlig etterretning aktivt forsøker å rekruttere innsidere, se punkt 3.2. Foretakene bør ta høyde for dette i sine risikovurderinger.

Hvitvasking

Hvitvasking er generelt et område hvor foretakene viser til moderat risiko, men enkelte foretak viser også til høy risiko. Flere foretak anser at det er moderat eller høy risiko for at det ikke er tilstrekkelig presisjon knyttet til flagging av mistenkelige transaksjoner. Det vises i mange tilfeller til at et stort antall av flaggingene er falske positive. Et flertall av foretakene mener også at det er en moderat eller høy risiko for at systemene for transaksjonsovervåking ikke fanger opp alle betalingstransaksjoner. Foretakene viser til at de har stor oppmerksomhet på dette området, at systemene videreutvikles og forbedres, og at eksterne systemer kjøpes inn.

Et flertall av foretakene mener det er middels eller høy risiko for at antihvitvaskingssystemene (AML-system) ikke i tilstrekkelig grad benytter data fra foretakets øvrige systemer. Det er blant annet vist til at systemavhengighet utgjør en risiko. Flere foretak melder om at det overføres informasjon fra eksterne systemer ved innhenting og validering av informasjon i forbindelse med opprettelse av kundeforhold.

Flere betalingstjenestetilbydere trekker fram at forbrukeres handel med kryptovaluta innvirker på etterlevelsesrisikoen knyttet til foretakenes arbeid med antihvitvasking og terrorfinansiering.

Et flertall av foretakene mener at det er moderat eller høy risiko forbundet med AML-systemenes gjenkjennelse av mistenkelige mønstre over tid. Flere foretak melder at de har tatt i bruk maskinlæring og scenarioer som benytter kundenes tidligere adferd sammenholdt med statistiske data for å gjenkjenne mistenkelige mønstre.

3.7 Risiko knyttet til kunders bruk av digitale tjenester

3.7.1 Sterk kundeautentisering

Med sterk kundeautentisering (SKA) menes en løsning basert på bruk av to eller flere elementer som er uavhengige av hverandre, slik at kompromittering av ett element ikke vil påvirke øvrige elementer,

jf. forskrift om systemer for betalingstjenester § 5[34]. Den europeiske banktilsynsmyndigheten (EBA) har publisert en anbefaling[35] som nærmere definerer kravene til sterk kundeautentisering.

Finanstilsynet er kjent med at EBAs anbefalinger enkelte steder ikke følges. Blant annet erfarer Finanstilsynet at det i forbindelse med handel på internett for enkelte kort kun kreves kortdetaljer og en kode sendt som SMS til mobiltelefonen, noe som etter EBAs definisjon ikke tilfredsstiller kravene til SKA. Mangel på etterlevelse gjør at kunden i mindre grad er beskyttet mot misbruk av kortet.

3.7.2 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 forskjellig 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 kan gi en form for slitasje på ID-en og brukerens forsiktighet i anvendelse av den. Det tilsier at det bør være mulig å reservere seg mot bruksområder for ID-en.

3.7.3 Utfordringer i anti-svindelanalyser

For å avhjelpe faren for svindel gjør tjenesteyter etterkontroller i form av transaksjonsanalyse og kundeanalyse som et ledd i godkjenningen av innlogging og igangsatte transaksjoner. Når brukeren benytter BankID til innlogging til andre tjenester enn nettbank, kan banken (utsteder av BankID) ikke gjøre de samme analysene basert på transaksjoner, det vil si analyse basert på innholdet i tjenesten. Utsteder av BankID kan fremdeles gjøre enkelte kundeanalyser, for eksempel geokontroller basert på hvor og når BankID siste gang ble brukt.

3.7.4 Misbruk av ID-kjennetegn

For å skaffe seg privilegier i offerets navn benytter angripere ID-kjennetegn som er lette å få tak i. Et eksempel er personnummer. Dersom noen har offerets personnummer, er det relativt enkelt å opprette en falsk legitimasjon i offerets navn, men med eget bilde. Deretter kan svindlerne opprette nye kredittkort, mobiltelefonabonnementer o.l. Svindlerne benytter disse som legitimasjon, tilegner seg nye privilegier i offerets navn og kan i verste fall overta offerets identitet i en rekke sammenhenger.

3.7.5 Opprette sperre for kredittopplysninger

For å redusere risikoen for svindel ved misbruk av ID-kjennetegn anbefaler Datatilsynet forbrukere å etablere en sperre mot kredittvurdering hos kredittopplysningsbyråene.[3] For å kunne etablere en slik sperre må forbrukere til enhver tid vite hvilke byråer som finnes. Datatilsynet vedlikeholder opplysninger om dette. Brukeren får ikke varsel om nye byråer, men må selv holde seg orientert. Med hensyn til å redusere svindel ved misbruk at ID-kjennetegn ville det fra et forbrukerståsted vært bedre

[34] Lovdata: Forskrift om systemer for betalingstjenester
[35] EBA: Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2

om utgangspunktet var sperring for alle, hvor forbrukeren selv kunne fjerne sperringen ved behov. Datatilsynet har tatt initiativ til en felles sperreløsning i Brønnøysundregistrene.

3.7.6 Bruk av lenker i kommunikasjon med kundene

Finanstilsynet har observert at enkelte foretak sender kundene lenker via e-post eller SMS. Kriminelle opererer tilsvarende når de bedriver phishing via e-poster eller SMiShing via SMS der de ber mottaker trykke på lenker med formål å enten stjele informasjon eller overføre ondsinnet kode. Finanstilsynet er kjent med at det skaper utrygghet hos kunder når foretak sender e-poster eller SMS-er med lenker som de bes gjøre bruk av.

Finanstilsynet legger vekt på at foretakene kommuniserer med sine kunder på en trygg og forsvarlig måte. Framfor å legge ved lenker i e-poster eller SMS-er bør foretakene be sine kunder logge seg inn på foretakets nettsted for å hente eller sende inn informasjon.

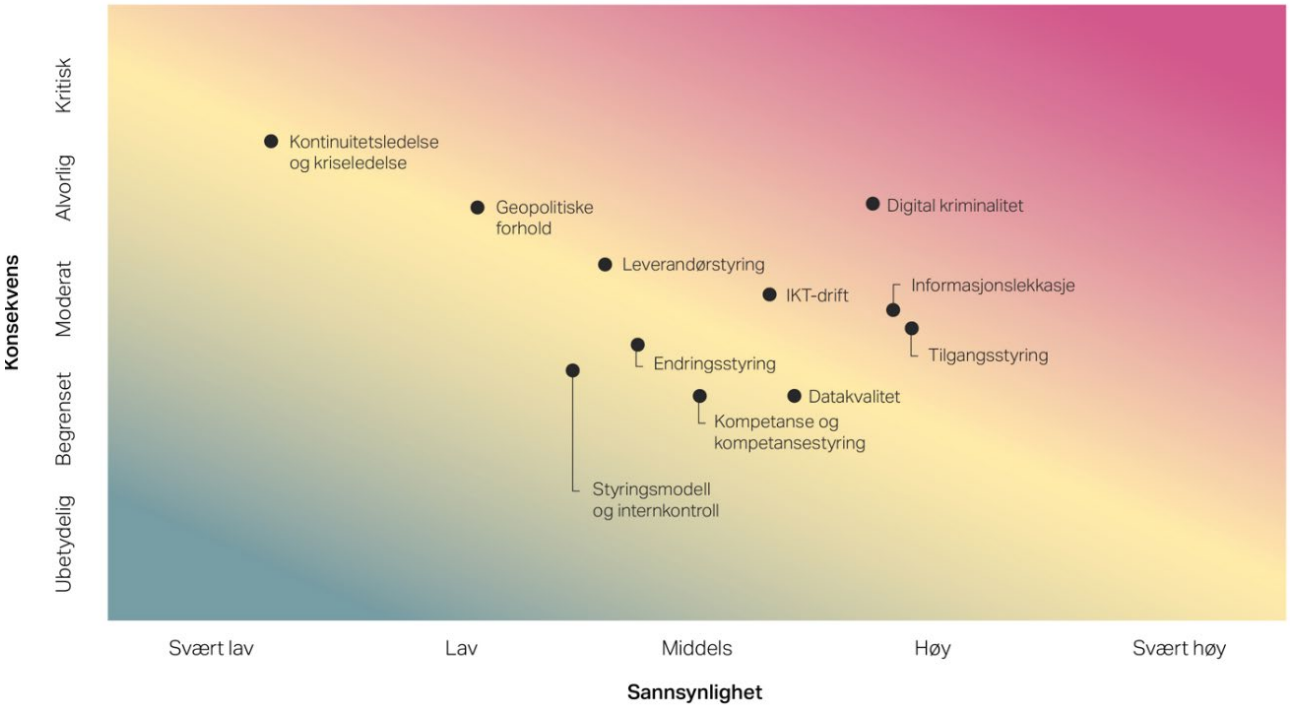
3.8 Risiko knyttet til sårbarheter i foretakenes IKT-virksomhet

Finanstilsynet anser sårbarheter knyttet til foretaks forsvarsverk mot digital kriminalitet som den mest sentrale risikoen knyttet til foretakenes bruk av IKT, der den samlede risikoen anses å være høy, se figur 3.1. Sårbarheter knyttet til IKT-drift, tilgangsstyring og informasjonslekkasje er også sentrale risikoer, der den samlede risikoen anses som middels til høy. Mens risikoen knyttet til foretaks forsvarsverk mot digital kriminalitet og tilgangsstyring er ansett som noe høyere i 2021 enn året før, er risikoen knyttet til IKT-drift ansett å være noe lavere.

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

Figur 3.1 oppsummerer Finanstilsynets vurdering av de mest sentrale sårbarhetene i finanssektoren for 2021. De ulike sårbarhetene er klassifisert etter sannsynlighet for at en alvorlig negativ hendelse oppstår, og den tilhørende konsekvensen etter alvorlighetsgrad for det enkelte foretak. Observasjoner og vurderinger som ligger til grunn for klassifiseringen, framgår av tabell 3.1 og er nærmere omtalt i øvrige punkter i kapittel 3 samt kapitlene 4 til 6. Metodikken og detaljer som ligger til grunn for vurderingene, er omtalt i vedlegg 2.

Figur 3.1 Finanstilsynets vurdering av sårbarheter og risiko for 2021



Kilde: Finanstilsynet

Tabell 3.1 Sårbarheter som kan utgjøre en risiko for uønskede hendelser, vurdering for 2021

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

Kilde: Finanstilsynet

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)[36].

Det rapporteres både svindlet beløp og antall svindeltransaksjoner, samt det samlede transaksjonsbeløpet og totalt antall transaksjoner i perioden. I rapporteringen skilles det mellom transaksjoner innenlands, grensekryssende transaksjoner innenfor EØS og grensekryssende transaksjoner utenfor EØS. Videre inndeles svindeltransaksjonene i tre kategorier basert på om svindleren utsteder betalingen, endrer/modifiserer betalingen eller manipulerer betaleren til selv å utstede betalingen. Som følge av innføringen av PSD2 ble svindelrapporteringen endret med virkning fra og med andre halvår 2019, noe som gir et brudd i tallseriene.

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 2021 utgjorde 159,3 mill. kroner. Tapene var omtrent likt fordelt mellom første og andre halvår, henholdsvis 78,5 og 80,8 mill. kroner. I tillegg kommer tap på 2,8 mill. kroner gjennom urettmessig bruk av betalingskort for kontantuttak, som fordelte seg på første og andre halvår med henholdsvis 0,8 og 1,9 mill. kroner. Samlet var det totale tapet ved misbruk av betalingskort 162,1 mill. kroner. Dette er en oppgang fra 2020 på 9,9 prosent, men lavere enn nivået i andre halvår 2019.

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

[36] Artikkel 96 nr. 6 i PSD2 (Lovdata) og Guidelines on fraud reporting under PSD2 (EBA)

Tabell 4.1 Tap ved misbruk av betalingskort

Svindeltype betalingskort (beløp i hele tusen kroner)	2016	2017	2018	2019	2020	2021
Totalt	206.503	145.591	148.732	189.147	147.602	162.145*

* Betalinger og kontantuttak med kort. Kilder: Finanstilsynet og Bits AS

Samlede tap i 2021 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 0,2 prosent av transaksjonsverdien, som er en nedgang fra 2020.

Tabell 4.2 Verdi av transaksjoner og svindeltransaksjoner med betalingskort rapportert av kortutsteder. Tall for 2021

Transaksjonsverdi (beløp i hele tusen kroner)	Transaksjoner i Norge	Grensekryssende transaksjoner i EØS	Grensekryssende transaksjoner utenfor EØS	Totale transaksjoner
Kortbetalinger (utsteder)				
Totalt	712.504.725	211.058.563	25.467.535	949.030.823
- Hvorav svindel	6.277	97.722	55.356	159.355
Svindel i prosent	0,001	0,046	0,217	0,016
Hvorav initiert ikke-elektronisk*:				
Totalt	4.808.934	6.122.447	2.989.278	13.920.659
- Hvorav svindel	535	6.295	7.185	14.013
Svindel i prosent	0,011	0,21	0,24	0,10
Hvorav initiert elektronisk:				
Svindleren utsteder betalingen, hvorav	4.643	78.355	44.122	127.120
- Tapt eller stjålet kort	767	1.429	1.174	3.370
- Ikke mottatt kort	375	594	377	1.346
- Forfalsket kort	29	935	1.002	1.966
- Tyveri av kortdetaljer	2.667	51.724	35.077	89.468
- Annet	806	23.675	6.491	30.972
Svindleren endrer eller modifiserer betalingsordre	265	571	576	1.412
Svindleren manipulerer betaleren til en kortbetaling	835	12.336	3.473	16.644
Fjernbetaling (internetthandel)				
Totalt	67.787.034	138.953.771	18.857.705	225.598.510
- Hvorav svindel	3.869	87.340	44.794	136.003
Svindel i prosent	0,006	0,063	0,238	0,060
Nærbetaling (på fysisk brukersted)				
Totalt	639.908.756	65.982.346	3.620.639	102.200.353
- Hvorav svindel	1.875	3.921	3.377	57.355
Svindel i prosent	0,00029	0,006	0,093	0,0013
Fjernbetaling uten sterk kundeautentisering				
Totalt	27.475.944	63.050.575	11.673.834	102.200.353
- Hvorav svindel	1.535	27.795	28.025	57.355
Svindel i prosent	0,005	0,044	0,24	0,056

* Korttransaksjonene er initiert manuelt ved at informasjon fra betalingskortet er kommunisert gjennom samtale, telefon eller e-post. Kilde: Finanstilsynet

Tap ved kortbetalinger som ikke er initiert elektronisk, utgjorde i 2021 ca. 14 mill. kroner av det samlede tapet ved misbruk av kort på 162 mill. kroner. Dette er korttransaksjoner der informasjon fra betalingskortet er kommunisert fra kjøper til selger over telefon eller via e-post. Målt som andel av samlet transaksjonsverdi utgjorde tapene 0,1 prosent, mens andelen for grensekryssende transaksjoner utenfor EØS utgjorde 0,24 prosent. Dette er en nedgang fra 2020, hvor samlet tap ved kortbetalinger som ikke er initiert elektronisk utenfor EØS, utgjorde 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 utgjorde tapene 0,06 prosent av transaksjonsverdien i 2021, som er en nedgang fra 0,07 prosent i 2020. For grensekryssende transaksjoner utenfor EØS utgjorde tapene 0,24 prosent, som er en nedgang fra 0,35 prosent i 2020.

Totalt ble det gjennomført rundt 2,5 mrd. betalinger med kort i 2021. Av disse var ca. 147.000 transaksjoner svindel, noe som utgjør 0,006 prosent av samlet antall transaksjoner. Dette er en nedgang sammenlignet med 2020, hvor antall svindeltransaksjoner var 205.000 og andelen svindeltransaksjoner utgjorde 0,008.

Gjennomsnittsverdien av en svindeltransaksjon med betalingskort er 1.082 kroner, mens gjennomsnittverdien av en kundeinitiert transaksjon med betalingskort er 375 kroner.

Tabell 4.3 Antall transaksjoner og svindeltransaksjoner med betalingskort rapportert av kortutsteder i 2021

Antall	Transaksjoner i Norge	Grensekryssende i EØS	Grensekryssende utenfor EØS	Totalt
Totalt	1.922.541.608	532.744.284	70.009.565	2.525.295.457
- Hvorav svindel	6.971	85.948	54.318	147.286
Svindel i prosent	0,0004	0,016	0,076	0,006
Initiert ikke-elektronisk:	9.240.296	22.415.653	21.613.880	53.269.829
- Hvorav svindel	392	3.961	5.423	9.776
Svindel i prosent	0,010	0,018	0,25	0,018
Fjernbetaling	169.899.737	328.366.752	41.726.143	539.992.632
- Hvorav svindel	3.252	76.890	47.186	127.326
Svindel i prosent	0,002	0,023	0,113	0,024
Nærbetaling	1.743.401.575	181.961.879	6.669.542	1.932.032.996
- Hvorav svindel	3.329	5.097	1.758	10.184
Svindel i prosent	0,0002	0,003	0,026	0,00005

Kilde: Finanstilsynet

4.3 Tap knyttet til kontooverføringer

Svindel med kontooverføringer inkluderer situasjoner der svindleren utsteder eller modifiserer betalingen eller manipulerer betaleren til selv å gjennomføre betalingen.

Tap ved kontooverføringer, hovedsakelig nettbank, utgjorde 346 mill. kroner i 2021, mot 355 mill. kroner i 2020. Tallene viser samlede tap for nettbanksvindel mot norske kunder for de siste årene, uavhengig av om tapet dekkes av kunden selv eller av banken.

Tabell 4.4 Transaksjoner og svindeltransaksjoner – kontooverføringer (nettbank m.m.). 2021

Kontooverføringer initiert elektronisk (hele 1000 kroner)	Transaksjoner i Norge	Grensekryss-ende i EØS	Grensekryss-ende utenfor EØS	Totalt	Svindel-prosent
Totalt	28.889.907.250	5.692.685.875	1.142.318.500	35.724.911.625	
- Hvorav svindel	140.555	140.996	64.925	346.476	0,00097
Hvorav ulike typer svindler:					
- Svindleren utsteder betalingen	44.904	54.769	8.674	108.347	
- Svindleren modifiserer betalingsordren	5.065	8.318	277	13.660	
- Svindleren manipulerer betaleren til å utstede betalingsordren	90.586	77.908	55.962	224.456	

Kilde: Finanstilsynet

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 2021 240,6 mill. kroner, hvorav 224 mill. kroner for kontooverføringer og 16,6 mill. kroner for betalingskort. Det samlede tapet som følge av sosial manipulering var noe lavere enn i 2020, hvor det utgjorde 295 mill. kroner, men det har vært en vesentlig økning i tap der brukeren har gjennomført transaksjonen ved bruk av betalingskort.

Det reelle omfanget av svindel ved sosial manipulering er usikkert fordi betaleren selv bærer det økonomiske tapet og mange svindler av denne typen trolig ikke blir meldt til banken. Det antas derfor 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 høyere enn kundenes materialiserte tap. Bankene forhindrer en stadig større andel av svindelforsøkene. Dette er trolig en viktig årsak til at

de rapporterte svindeltallene for 2021 er lavere enn i 2020. 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. Disse tallene tyder på at den største svindelkategorien i 2021 var phishing, der summen forsøkt svindlet var noe høyere enn tidligere.

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. Phishing omfatter imidlertid også svindel hvor betaleren avlures kontakt- og betalingsinformasjon som svindleren bruker til å utstede en betaling på vegne av betaleren. I PSD2-rapporteringen blir dette rapportert som svindel der svindler utsteder betalingen. I 2021 utgjorde tap knyttet til transaksjoner i nettbank 108 mill. kroner, som er omtrent en dobling fra 2020, mens tap knyttet til betalingskort utgjorde 145 mill. kroner.

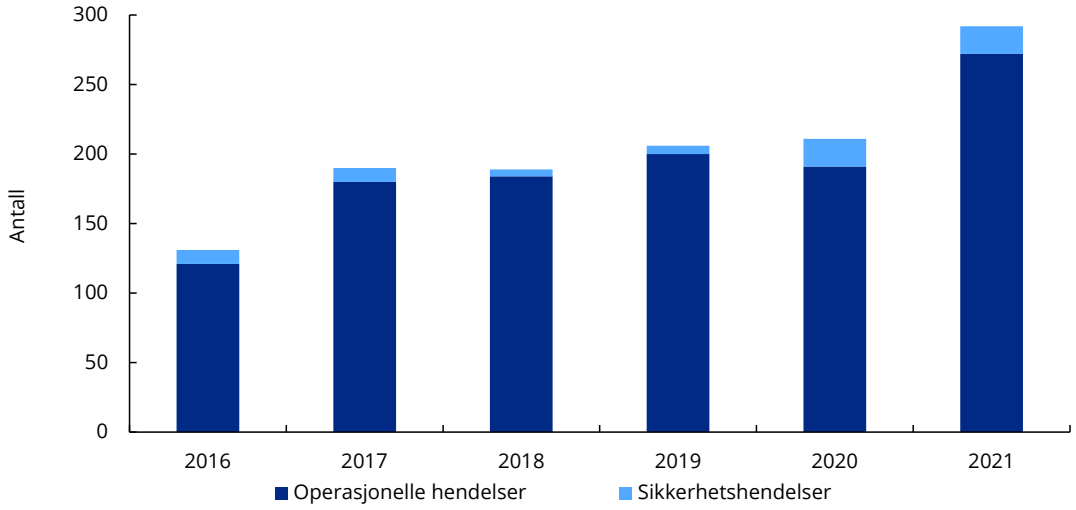
5 Hendelsesrapportering

5.1 Statistikk over hendelser

Foretakene rapporterte 292 IKT-relaterte hendelser til Finanstilsynet i 2021, som er et betydelig større antall enn i 2020. Økningen skyldes i hovedsak at flere foretak rapporterte, som inkassoforetak (se punkt 5.5), og at foretakene rapporterte om flere typer hendelser, herunder hendelser knyttet til systemer for å avdekke hvitvasking og terrorfinansiering og grensesnitt for tredjeparters tilgang til kunders betalingskonto etter PSD2.

Ved hendelser legger Finanstilsynet vekt på at foretaket avdekker årsaker, iverksetter tiltak for å hindre gjentakelser og utarbeider en sluttrapport. Ved alvorlige avvik vil hendelsen følges løpende gjennom hele forløpet.

Figur 5.1 Antall rapporterte IKT-hendelser



Kilde: Finanstilsynet

Tabell 5.1 Antall rapporterte hendelser

År	Operasjonelle hendelser	Sikkerhetshendelser	Totalt antall hendelser
2016	121	10	131
2017	180	10	190
2018	184	5	189
2019	200	6	206
2020	191	20	211
2021	272	20	292

Kilde: Finanstilsynet

5.2 Sikkerhetshendelser

Det ble rapportert 20 sikkerhetshendelser i 2021. Mange av disse var knyttet til en sårbarhet i et såkalt loggverktøy (Apache Log4j), som ble avdekket i desember 2021. Sårbarheten rammet virksomheter i alle sektorer i samfunnet og ble ansett som svært kritisk, siden den gjør det mulig å kjøre skadelig kode på en berørt server uten å måtte legge inn brukernavn og passord. Foretak i finanssektoren observerte en rekke forsøk på å utnytte sårbarheten uten at angriperne lyktes med å få tilgang til IT-systemene. Foretakene kartla, sammen med sine leverandører, om den sårbare komponenten var i bruk i foretakets IT-systemløsninger, gjorde nødvendige oppdateringer av IT-systemene og gjennomførte tiltak for å overvåke og håndtere eventuelle forsøk på å unytte sårbarheten. Finanstilsynet er i 2022 blitt kjent med at angripere i ett tilfelle har lyktes med å infisere en server hos et mindre finansforetak med ondsinnet kode, men undersøkelser tydet på at angriperne ikke rakk å utnytte tilgangen før inntrengingen ble oppdaget og serveren tatt ut av drift.

For øvrige rapporterte sikkerhetshendelser var mindre finansforetak overrepresentert. Her ble det blant annet rapportert om virusangrep på e-postservere og infeksjon med ondsinnet kode i teksteditor. Det ble rapportert kun ett tjenestenektangrep i 2021. Flere banker rapporterte om spesielt aggressive phishing-kampanjer.

En sentral leverandør til finanssektoren ble utsatt for et løsepengeangrep i februar. Foretak i finanssektoren ble ikke rammet.

Finanstilsynet har dialog med NFCERT[2] når det er gjort forsøk på og/eller avdekket utnyttelse av sårbarheter i bredt anvendt programvare, som potensielt kan ramme mange foretak. Finanstilsynet publiserte informasjon om sårbarheten i loggverktøyet Log4j på sitt nettsted.

5.3 Rapportering av sårbarheter

Finanstilsynet mottok i 2021 flere rapporter om sårbarheter foretakene hadde avdekket i egne applikasjoner eller systemer. Foretakene har i sine undersøkelser ikke avdekket at sårbarhetene er forsøkt utnyttet. Dersom de hadde blitt det, kunne det ført til stor skade, fortrinnsvis med brudd på konfidensialitet. Sårbarheter blir oftest oppdaget av kunder eller ansatte, men kan også oppdages gjennom sikkerhetstesting. Ofte er det problemer i sesjonshåndteringen, for eksempel i utloggingen, som gjør at en kunde får tilgang til en annen kundes data, eller at en saksbehandler får tilgang til andre bankers data. Størst risiko for at det oppstår sårbarheter er etter systemendringer.

5.4 Sikkerhetsbrudd

Finanstilsynet mottok i 2021 rapporter fra banker om at det var avdekket et større antall oppslag på deres kunder fra en IKT-tjenesteleverandør enn hva det tjenstlige behovet skulle tilsi. Undersøkelser viste at det var ansatte hos tjenesteleverandøren som hadde misbrukt sine tilgangsrettigheter. I tillegg

til å være et sikkerhetsbrudd er det også brudd på personopplysningsloven og personvernforordningen (GDPR). I overkant av 800 kunder fordelt på 35 banker var berørt av hendelsen.

Dette vurderes av Finanstilsynet som et alvorlig brudd på avtalen mellom banken og IKT-tjenesteleverandøren. For å forebygge slike hendelser bør banken benytte konseptet "zero trust"[31] hvor bruken av tilganger er underlagt et strengt regime. I tillegg er det viktig å dokumentere og følge opp at bruken av tilgangsrettigheter er i henhold til tjenstlige behov.

5.5 Operasjonelle hendelser (driftshendelser)

Rapportering av hendelser fra banker og betalingsforetak

Den vanligste årsaken til driftshendelser er nettverksproblemer. Risikoen for hendelser er klart størst etter endringer i IT-systemene, og fortsatt er mangelfull testing før løsninger tas i bruk årsak til driftsavvik. Med unntak av en driftshendelse i Danske Bank 13. oktober var det ingen driftshendelser i 2021 av lengre varighet. Imidlertid var det hendelser der flere banker rapporterte om gjentagende ustabilitet og periodevise utilgjengelige betalingstjenester grunnet driftsproblemer hos leverandør.

Finanstilsynet vurderte problemene med BankID-appen og kodebrikke etter Vipps' flytting av driften til ny leverandør som alvorlige. Finanstilsynet hadde jevnlige statusmøter med Vipps og prosjektledelsen for å følge opp prosjektframdriften og hvordan løsningens stabilitet ble ivaretatt under flytteprosjektet. Overføring av driften ble gjennomført i siste del av oktober 2021 uten store problemer. Mot slutten av november oppsto det problemer med bruk av BankID på app. Finanstilsynet avholdt i en periode, inntil driftsituasjonen ble stabilisert, hyppige statusmøter med Vipps. I møtene var det gjennomgang av driftssituasjonen, aktuelle tiltak og arbeidet med å finne fram til rotårsaken.

Blant annet ble det redegjort for de tre hovedårsakene til problemene som oppstod og løsninger som var iverksatt med sikte på å stabilisere BankID. Løsningene viste seg å fungere som forventet når trafikken tok seg opp til normalt nivå 3. januar 2022.

Hendelser de siste årene, knyttet til bytte av driftsleverandør, har vist at leverandøren i noen tilfeller ikke hadde etablert en prosess for hendelseshåndtering som samsvarte med tjenestens kritikalitet.

Ved bytte av driftsleverandør må oppdragsgiver kvalitetssikre at oppdragstaker har etablert tilstrekkelige prosesser, kompetanse og kapasitet til effektivt å kunne håndtere hendelser som rammer kritiske tjenester.

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

Det ble meldt 14 hendelser fra banker og betalingsforetak om avvik i den elektroniske transaksjonsovervåkingen mot hvitvasking (AML-systemene). Rapportering av hendelser knyttet til AML-systemene øker sakte, men sikkert fra år til år. Avvikene gjelder manglende eller mangelfull screening og/eller transaksjonsovervåking. Oftest er det avvik i kortere perioder, men også i 2021 mottok Finanstilsynet rapporter om avvik som strakk seg flere år tilbake i tid med store restanser på transaksjoner som ikke er kontrollert.

Ved de mest alvorlige hendelsene som rammer AML-systemene, er det nesten utelukkende system-endringer som er årsaken. Verdikjeden er kompleks. Endringer i kildesystemene, herunder bytte eller sammenslåing av kildesystemer, påvirker uttrekket til AML-systemene. Endringer i datavarehus-løsninger og i selve AML-systemet øker også risikoen for avvik. Erfaringene understreker hvor viktig det er at foretakene etter endringer tester og kontrollerer screeningen og transaksjonsovervåkingen, både i første- og andrelinjen. Finanstilsynet forventer at foretakene rutinemessig kontrollerer at uttrekket av transaksjoner til det elektroniske overvåkingssystemet er komplett.

Avvik i driften er ofte årsaken til kortere perioder med manglende screening og/eller transaksjonsovervåking. Finanstilsynet forventer at foretakene har rutiner for å håndtere avvikssituasjoner der dataoverføringene til det elektroniske overvåkingssystemet, eller det elektroniske overvåkingssystemet selv, ikke fungerer som forutsatt.

Rapportering fra verdipapirområdet

Omtrent halvparten av hendelsene som ble rapportert på verdipapirområdet i 2021, var knyttet til de regulerte markedsplassene. Ingen av hendelsene fikk alvorlige konsekvenser. Det oppsto imidlertid en alvorlig driftshendelse i Verdipapirsentralen (ESO)[37] 1. februar 2021. Det siste verdipapiroppgjøret denne dagen kunne ikke gjennomføres og ble forskjøvet til neste dag.

Tre sikkerhetshendelser ble i 2021 rapportert fra selskap på verdipapirområdet. Alle var meldinger knyttet til håndteringen av globale sårbarheter, blant annet den mye brukte åpne kildekoden log4j. Det var ikke indikasjoner på at kriminelles forsøk på å utnytte sårbarhetene lyktes i å skade data eller systemer, se også omtale i avsnittet om sikkerhetshendelser. Øvrige rapporter på verdipapirområdet var dominert av problemer med tilgang til netthandel med verdipapirer.

Rapportering fra forsikringsforetak

Rapporterte hendelser i forsikringsforetakene har i hovedsak vært hendelser som har påvirket konfidensialitet eller integritet og i mindre grad tilgjengelighet. Finanstilsynet ser imidlertid at forsikringsforetakene i større grad enn før rapporterer om driftshendelser som rammer tilgjengeligheten til nettbaserte kundetjenester, som er en stadig viktigere del av kundebetjeningen. Enkelte av driftshendelsene i 2021 var sammenfallende med driftshendelser hos en driftsleverandør

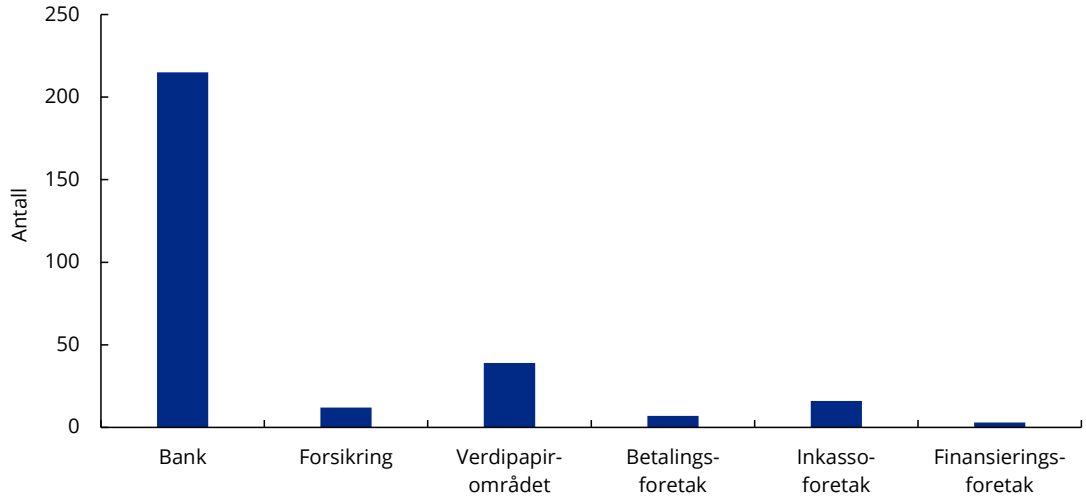
[37] Verdipapirsentralen ASA (VPS) (Euronext Securities Oslo – ESO).

som er felles med en del av bankene. Det ble også rapportert om driftshendelser som rammet forsikringsforetakenes egenutviklede systemer, og som medførte forsinkelser i saksbehandlingen. To av sikkerhetshendelsene i 2021 ble rapportert fra forsikringsforetak og gjaldt ulike former for kompromittering av e-postkontoer. Det ble rapportert en hendelse med konfidensialitetsbrudd som følge av at kunder mottok annen kundes faktura sammen med sin egen. Det ble også rapportert en hendelse hvor kunder mottok feilaktig informasjon om innhenting av skattekort fra Skatteetaten.

Rapportering fra inkassoforetak

I brev til inkassoforetakene i desember 2020 understreket Finanstilsynet at foretakene er underlagt krav til hendelsesrapportering i henhold til IKT-forskriftens § 9. Finanstilsynet mottok i 2021 flere hendelsesrapporter fra inkassoforetakene enn tidligere. I 2021 rapporterte flere foretak, uavhengig av hverandre, om at svikt i IKT-systemene hadde medført at kravbrev ikke ble sendt. Felles for avvikene var at det i saksbehandlingssystemet framsto som at brevene var sendt til skyldner og at avviket ble avdekket først ved nærmere undersøkelser foranlediget av et vesentlig antall henvendelser fra skyldnere om at brev ikke var mottatt. Finanstilsynet sendte på den bakgrunn brev til alle inkassoforetakene der de gjorde foretakene oppmerksomme på risikoen for svikt i IKT-systemene som kan medføre slike avvik.

Figur 5.2 Rapporterte hendelser i 2021 fordelt på type foretak



Kilde: Finanstilsynet

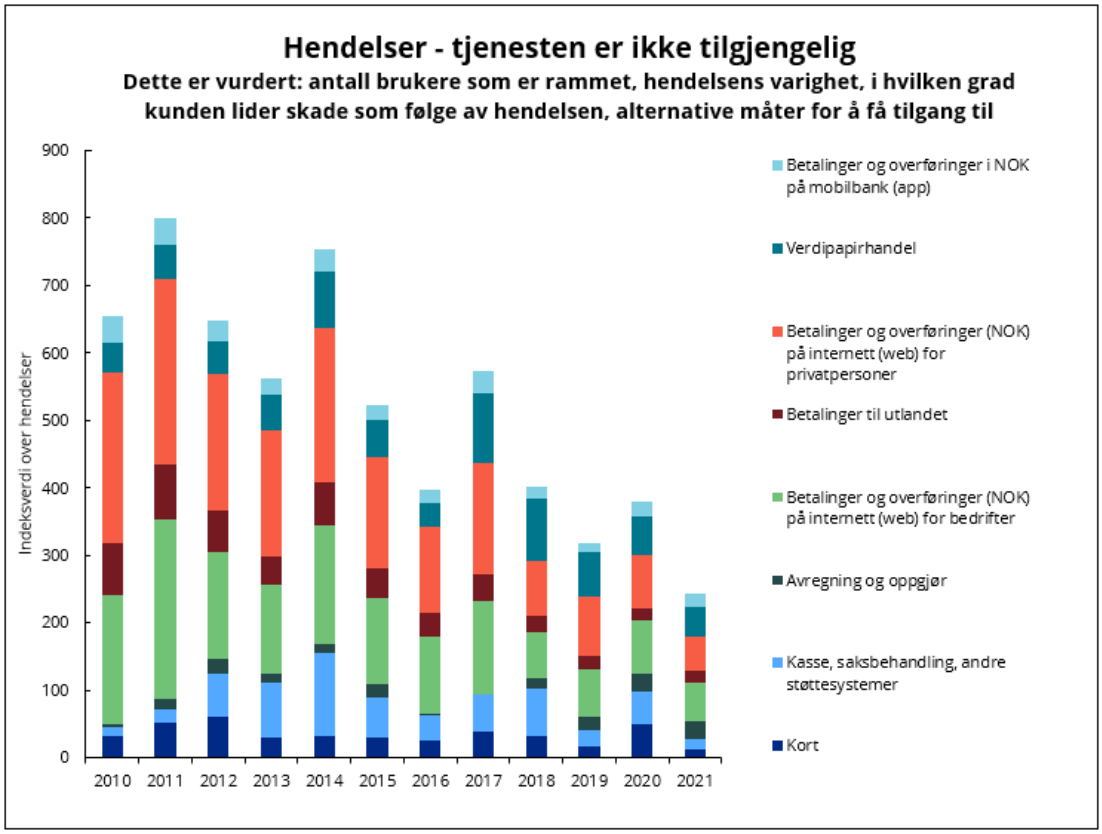
5.6 Analyse av hendelsene som mål på tilgjengelighet

De rapporterte hendelsene har ulik alvorlighetsgrad. For hendelser som har medført redusert tilgjengelighet, har Finanstilsynet vurdert og vektet hendelsene ut fra tidspunktet for og avbruddets lengde, antall foretak som er berørt, hvor mange kunder som er rammet, og om det eksisterer alternative tjenester som dekker kundens behov (som for eksempel at mobilbanken er utilgjengelig,

men nettbanken kan benyttes). Vektingen av hendelsene gir en indeks som framkommer på y-aksen i figur 5.3. Funnene sammenstilles i en tidsserie, slik at utviklingen kan følges over tid.

Det framgår av figur 5.3 at betalingstjenester og kunderettede løsninger var mer tilgjengelige for kundene i 2021 enn i tidligere år. Tilgjengeligheten til tjenestene vurderes samlet sett som tilfredsstillende i 2021.

Figur 5.3 Hendelser med redusert tilgjengelighet for brukere. Vektet etter vurdert konsekvens*



* Skalaen på y-aksen er en indeks som er basert på vektingen av hver enkelt hendelse. Lavere indeksverdi angir lavere forekomst av driftsavbrudd med konsekvenser for brukerne.
Kilde: Finanstilsynet

Det var færre driftshendelser med lang varighet i 2021 enn tidligere år, men en del hendelser rammet et stort antall brukere.

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 noen flere feil enn i 2020.

Hendelser knyttet til kategorien "Verdipapirhandel" dekker hendelser knyttet blant annet til aksjehandelsløsninger på internett og hendelser i ESO40 (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.

5.7 Hendelser knyttet til problemer med dedikerte PSD2-grensesnitt

Både kontoførende betalingstjenestetilbydere og betalingstjenestetilbydere (TTP-er) skal etter regelverket rapportere til Finanstilsynet om eventuelle problemer med grensesnitt for tredjepartstilbyderes tilgang til kunders betalingskonto, se omtale i egen ramme. Finanstilsynet mottok rundt 30 slike rapporter fra kontoførende betalingstjenestetilbydere og 13 fra TTP-er i 2021, hvor ti av disse var driftshendelser som samtidig var rapportering i henhold til IKT-forskriftens § 9, annet ledd[38] krav om rapportering av hendelser.

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.[39]

Videre skal kontotilbydere ved slike avvik informere tredjepartstilbydere om avviket og tiltak for reetablering og beskrive 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.

[38] Lovdata: Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT)
[39] Finanstilsynet om plikten til å rapportere om avvik i dedikerte grensesnitt: PSD 2 – Presiseringer og avklaringer om regelverket

6 Utkontraktering

6.1 Melding om utkontraktering

Finanstilsynet mottok i 2021 i overkant av 170 meldinger om utkontraktering. I tillegg vurderte Finanstilsynet avtaler om utkontraktering av IKT-virksomhet i forbindelse med behandling av konsesjonssøknader.

De fleste meldingene om utkontraktering i 2021 var knyttet til skifte 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. I forbindelse med behandlingen av meldinger om Vipps' bytte av driftsleverandør for BankID fulgte Finanstilsynet opp bankenes planer for beredskap i forbindelse med gjennomføringen av byttet.

Finanstilsynet vil understreke viktigheten av at felles betalingsinfrastruktur behandles som utkontrakterte IKT-tjenester og at bankene stiller krav til og følger opp tjenestene i henhold til gjeldende regelverk og egne retningslinjer for oppfølging av utkontrakterte IKT-tjenester.

Meldingene Finanstilsynet mottar, er i stor grad av bedre kvalitet og mer omfattende, detaljerte og fullstendige enn tidligere. Kvaliteten på foretakenes analyser og vurderinger av risiko forut for gjennomføring av IKT-utkontrakteringer viser også bedring. Kvaliteten på leverandøravtaler og foretakenes forankring av avtaler om utkontraktering i egen ledelse, viser også en positiv utvikling. Nye foretak som søker om konsesjon, er imidlertid ikke like godt kjent med regelverket.

Meldingene om utkontraktering tyder på økt bruk av skytjenester de siste årene for både applikasjons- og infrastrukturtjenester. Gjennom utkontrakteringer får ofte foretakene flere plattformer å forholde seg til, 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 ha en rekke positive effekter, som bedre IKT-sikkerhet i løsningene, økt funksjonalitet og tjenester til lavere kostnad.

Tilnærmet alle foretak under tilsyn av Finanstilsynet har inngått avtaler som innebærer utkontraktering av deler av IKT-virksomheten. Finanstilsynet veileder[40] om hva som regnes som utkontraktering, begrensninger i adgangen til å utkontraktere og hvordan foretak under tilsyn må identifisere, vurdere og håndtere risiko knyttet til utkontraktering.

[40] Finanstilsynet: Veiledning om utkontraktering (rundskriv 7/2021)

6.2 Endring i regelverk for og veiledning om utkontraktering

Forskrift om meldeplikt ved utkontraktering av virksomhet mv. (meldepliktforskriften)[41] ble vedtatt av Finanstilsynet i september 2021 og trådte i kraft 1. januar 2022. Enkelte forhold knyttet til håndtering av utkontraktering er nærmere presisert i Finanstilsynets nye Veiledning om utkontraktering[40], rundskriv 7/2021.

Meldepliktforskriften presiserer at meldeplikten etter finanstilsynsloven § 4c[42] kun gjelder for utkontraktering av virksomhet som er kritisk eller viktig for foretaket, noe som utgjør en endring sammenlignet med tidligere. Forskriften stiller også krav til at foretakene skal ha en oppdatert oversikt over alle utkontrakterte avtaler og krav til meldingen.

IKT-forskriftens[43] bestemmelser om utkontraktering gjelder i utgangspunktet for all IKT-utkontraktering og har samme krav til behandling uavhengig av den utkontrakterte tjenestens viktighet. Den nye veiledningen om utkontraktering lemper på kravet i IKT-forskriftens § 2, siste ledd, om at utkontrakteringsavtaler knyttet til IKT-virksomhet, og endringer i slike, skal behandles av foretakets styre. Veiledningens kapittel 8.1 gir styret mulighet for å gi administrasjonen fullmakt til å håndtere og beslutte IKT-utkontrakteringsavtaler som ikke anses som kritiske eller viktige for foretaket. Utkontrakteringsforhold som er behandlet av administrasjonen i henhold til fullmakten, skal rapporteres til styret. Bestemmelsene i § 2 siste ledd om at det ved utkontraktering skal etableres planer, risikovurderinger og en beskrivelse av hvordan foretaket skal sikre leveransen, gjelder uavhengig av tjenestens viktighet.

Relevante retningslinjer ved utkontraktering fra EBA[44], EIOPA[45], og ESMA[46], som utdyper regelverket, er angitt i vedlegg 4.

6.3 Styring og kontroll

Det følger av IKT-forskriften at foretaket har ansvar for hele IKT-virksomheten, også når deler av denne er utkontraktert. Blant annet følger det av § 2 at foretaket skal etablere planer, risikovurderinger og sikringstiltak for å følge opp de utkontrakterte IKT-tjenestene, jf. også Veiledning om utkontraktering[40]40 Finanstilsynet forventer at foretaket etablerer styring og kontroll med utkontrakteringen basert på proporsjonalitetsprinsippet[47], der de utkontrakterte tjenestenes viktighet bestemmer styringsmodellen.

[41] Lovdata: Forskrift om meldeplikt ved utkontraktering av virksomhet mv.
[42] Lovdata: Lov om tilsynet med finansforetak mv. (finanstilsynsloven)
[43] Lovdata: Forskrift om bruk av informasjons- og kommunikasjonsteknologi
[44] EBA: European Banking Authority (nettsted)
[45] EIOPA: The European Insurance and Occupational Pensions Authority (nettsted)
[46] ESMA: The European Securities and Markets Authority (nettsted)
[47] Krav om forholdsmessighet mellom mål og middel

6.4 Risiko knyttet til utkontraktering

Sikkerhetsutfordringer

Finansbransjen har **lange og til dels komplekse verdikjeder, med et stort antall mellomledd**. Som eksempel kan man ta utgangspunkt i banker og hvordan disse opererer innen felles operasjonell infrastruktur (FOI)[12] i Norge, avhengigheter til SWIFT[16] og det internasjonale oppgjørssystemet CLS[17] samt kravene i det reviderte betalingstjenestedirektivet (PSD2)[48], der bankene må tilrettelegge tjenester for at tjenestetilbydere skal få tilgang til data. Videre opererer bankene sammensatte tjenester, som for eksempel samtykkebasert lånesøknad (SBL).[15]

Kompleksiteten og de gjensidige avhengighetene gjør foretakenes arbeid for å redusere sannsynligheten for avvik og forbedre IT-sikkerheten viktig for å sikre stabile og robuste driftsløsninger. Foretakene bør kartlegge muligheten for tilgang til alle deler av tjenesteleveranser slik at man kan vurdere risiko og hvilke muligheter som finnes for å styre og kontrollere IT-tjenestene som er utkontraktert.

I foretakenes **tekniske infrastruktur** inngår ofte lokalt utstyr, datasenterløsninger og skyplattformer. De ulike plattformene, operativsystemene og systemløsningene fordrer spesialisert kompetanse, der ulikheter i sikkerhetsløsninger også krever spesialistkompetanse. Sikkerhetsutfordringene knyttet til utkontraktering øker med den samlede kompleksiteten. Finanstilsynet har de siste årene merket seg at foretakene, ved bruk av skytjenester, søker å minimere antall plattformer og verktøy for å redusere behovet for spesialistkompetanse. Dette bidrar til å redusere foretakenes eksponering for angrep, herunder også alternative angrepsmetoder, men medfører samtidig større konsentrasjonsrisiko.

Et av de vanligste funnene i tilsyn med foretakenes IKT-virksomhet er at de ikke har tilfredsstillende **tilgangsstyring** for brukerne. Dette gjelder også foretakenes styring og kontroll med tilganger for personell hos IT-tjenesteleverandørene, som gjerne er satt opp med utvidede tilgangsrettigheter for å kunne utføre nødvendige oppgaver knyttet til de utkontrakterte IT-tjenestene.

Konsentrasjonsrisiko

Samlokasjon av flere foretaks IT-virksomhet eller kjøp av IT-tjenester hos én eller et lite antall leverandører kan medføre konsentrasjonsrisiko. En hendelse som rammer leverandøren, kan få alvorlige konsekvenser for flere foretak.

Norsk finansiell infrastruktur er i stor grad bygget opp rundt fellesløsninger, herunder bankenes felles operasjonelle infrastruktur (FOI), BankID og BankAxept.

Salget av Nets' konto-til-konto-tjenester i 2021 medførte at flere banker fikk en ny leverandør av betalingsformidlingstjenester, hhv. Mastercard Payment Services Infrastructure (MPSI) for FOI-tjenester og Mastercard Payment Services (MPS) for betalingsformidlingstjenester. Flere banker

[48] Lovdata: Om betalingstjenester i det indre marked (PSD2)

opererer samtidig med avtaler om kort-, ID- og signeringsløsninger fra Nets. Salget av Nets kan vurderes å ha redusert konsentrasjonsrisikoen, siden betalingsformidlingstjenester og kort- og ID-tjenester er fordelt på flere leverandører. Det er samtidig et stort antall foretak som er avhengige av leveranser fra hhv. MPS og MPSI knyttet til sine betalingsformidlingstjenester.

Eika Gruppen inngikk i 2020 avtale med Tietoevry om leveranse av kjernebankløsninger til lokalbankene i alliansen. Eika Gruppens overgang fra SDC til Tietoevry vil medføre høyere konsentrasjonsrisiko, fordi et større antall norske banker vil benytte Tietoevry som driftsleverandør for kjernebankløsninger.

Kontinuitet og beredskap

Å sikre kontinuitet i tjenesteleveransene er målet for fastsettelsen av kontinuitets- og beredskapsplaner i foretaket. Grunnlaget for planene er en forretningsmessig konsekvensanalyse for å identifisere foretakets kritiske forretningsprosesser. Med utgangspunkt i disse prosessene vil konsekvensene av ulike former for forstyrrelser bli analysert. I dette inngår konsekvensanalyser av hvordan de utkontrakterte IT-tjenestene blir påvirket av forstyrrelser. Med bakgrunn i denne kartleggingen vil foretaket søke å redusere konsekvensene av mulige forstyrrelser ved å gjennomføre risikoreduserende tiltak inntil kontinuitets- og beredskapsevnen er i tråd med foretakets risikoappetitt (dvs. viljen til å ta risiko i forhold til konsekvens).

Styring av risiko

Foretak som planlegger utkontraktering av IT-tjenester, må være oppmerksomme på at dette vil endre IT-risikobildet. Som et eksempel vil den potensielle angrepsflaten mot IT-infrastrukturen i de fleste tilfeller øke, og risikoen forbundet med IT-drift vil endres. IKT-forskriftens bestemmelser om risikovurdering ved utkontraktering skal sikre at foretaket identifiserer endringer i risiko som følge av IT-utkontrakteringen, og at foretaket tilpasser seg det nye, helhetlige IT-risikobildet.
I Finanstilsynets Veiledning om utkontraktering inngår anbefalinger for vurdering av oppdragstaker og utforming av utkontrakteringsavtaler. De mest relevante IT-risikoene i forbindelse med IT-utkontraktering er gjengitt nedenfor.

Vurderinger i forbindelse med valg av oppdragstaker (se kapittel 5 i Veiledning om utkontraktering og IKT-forskriften for ytterligere detaljer)

Foretaket (oppdragsgiver) må:

- Vurdere egen evne til å styre og kontrollere utkontraktert IT-virksomhet. Dersom foretaket mangler erfaring med IT-utkontraktering, må foretaket skaffe seg tilstrekkelig kompetanse (IKT-forskriftens § 12, siste ledd). Styrking av kompetanse kan være relevant både ved inngåelse av avtale og i styring og kontroll med de løpende leveransene i IT-utkontrakteringsforholdet.
- Sikre at IT-tjenesteleverandøren (oppdragstaker) har tilstrekkelig kapasitet, kompetanse og erfaring til å utføre oppgavene på en forsvarlig måte (veiledningen kapittel 5, c).
- Sikre at oppdragstaker har etablert et tilfredsstillende system for risikostyring og internkontroll (IKT-forskriften § 12, siste ledd).

- Sikre at oppdragstaker kan ivareta foretakets krav til kontinuitet og beredskap, herunder håndtere avvik i tjenesteleveransen (veiledningen kapittel 5, c).
- Sikre at risiko forbundet med oppdragstakers lokalisering og stedet oppgavene utføres fra blir vurdert. Eksempler på slike forhold er lovgiving/regulering, politisk stabilitet, stabilitet i infrastruktur (strøm, vann m.m.), kulturelle forskjeller og korrupsjon (veiledningen kapittel 5, g).
- Sikre at det er kontroll med nøkkelpersonrisiko i foretaket og hos oppdragstaker. I foretaket kan redusert motivasjon oppstå blant egne ansatte som følge av at tjenester skal utkontrakteres, og stor gjennomtrekk hos oppdragstaker kan få følger for tjenesteleveransene.

Utforming av avtalen (se kapittel 6 i Veiledning om utkontraktering for ytterligere detaljer)

Foretaket (oppdragsgiver) må:

- Sikre at oppdragsbeskrivelsen klart spesifiserer hva oppdraget går ut på, herunder krav til kvalitet. Foretaket bør etablere planer for hvordan man skal håndtere dårlig kvalitet og hvordan utfordringer ved manglende eller forsinkede leveranser skal håndteres. Relevante krav i forhold til dette bør innlemmes i avtalen(e). som et eksempel vil virksomhetskritiske funksjoner fordre at tjenesteleveranser opprettholdes selv om det igangsettes streik blant oppdragstakers personell. Dette må ivaretas, for eksempel med egne avtaler med fagforening/myndigheter (jf. veiledningen kapittel 6, b, IKT-forskriftens § 4).
- Sikre foretakets mulighet for å bringe avtalen til opphør, enten dette skyldes konflikter med tjenesteleverandøren eller skjer med bakgrunn i foretakets egne strategiske valg. Foretakene bør sikre exit-bestemmelser i avtalene som inngås, slik at det kan gjennomføres en styrt og kontrollert avvikling av leverandørforholdet. Avtalen bør definere partenes plikter, herunder oppdragstakers forpliktelser til å bistå i avviklingsfasen (veiledningen kapittel 6, d og m).
- Sikre at foretaket og Finanstilsynet har mulighet til å kontrollere oppdragstakers utførelse av de utkontrakterte tjenestene. Dette inkluderer adgang til å kontrollere oppgaver som er utkontraktert videre til underleverandører, og eventuelle bestemmelser om oppdragstakers mulighet for å bytte underleverandør (veiledningen kapittel 6, e, h, i, o, p og q samt IKT-forskriftens § 12, første og andre ledd).
- Sikre at oppdragstaker etterlever regulatoriske bestemmelser, som for eksempel finanstilsynsloven, hvitvaskingsloven og personopplysningsloven.
- Sikre at oppdragstaker forplikter seg til å ivareta oppgavene som foretaket fastsetter i sine beredskaps- og kontinuitetsplaner (veiledningen kapittel 5, m).

Oppfølging av tjenesteleveransene

For å ivareta en helhetlig styring og kontroll med IT-virksomheten bør foretaket etablere en styringsmodell med møteplasser og fora for å følge opp leverandører og leveranser på et strategisk (ledelse og styre), taktisk (oppfølging av leverandør) og operasjonelt nivå (daglig oppfølging av leveranser). Styringsmodellen som etableres, bør inkludere representanter fra oppdragsgiver i alle fora der man fastsetter hvordan samhandling og oppfølging skal foregå. På det overordnede, strategiske nivået er det viktig at foretakets ledelse og styre har inngående kjennskap til risiko, utfordringer og

handlingsalternativer knyttet til foretakets utkontrakterte virksomhet. Dette gjelder også når foretaket har utkontraktert all IT-virksomhet.

Ved utkontraktering til flere leverandører (multisourcing) må foretaket vurdere om det bør etableres møteplasser der flere/alle leverandører deltar.

Vedlegg 1: Foretakenes vurdering av sårbarhet

Nedenfor oppsummeres betalingstjenestetilbyderes vurdering av operasjonell risiko og sikkerhetsrisiko med utgangspunkt i deres årlige rapportering til Finanstilsynet[49]. Rapporteringsfristen var 15. februar 2022.

Oppsummeringen er inndelt i sju tema og omfatter vurderinger fra 168 foretak:

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 bes om å vurdere situasjonen/modenheten i foretaket for hver av risikoene beskrevet i skjemaet, og angi om foretaket anser at risikoen er høy, moderat eller lav. Dersom risikoen anses å være høy, bes foretaket angi årsaken. Foretakene bes også angi om risikoen anses å være økende, minkende eller stabil, og kort omtale hvilke tiltak som er satt i verk i løpet av det siste året og om tiltakene anses tilstrekkelige. I tillegg bes foretakene å angi forhold med høyest risiko. Nærmere beskrivelse om utfyllingen av spørreskjemaet er gjengitt under tabellene.

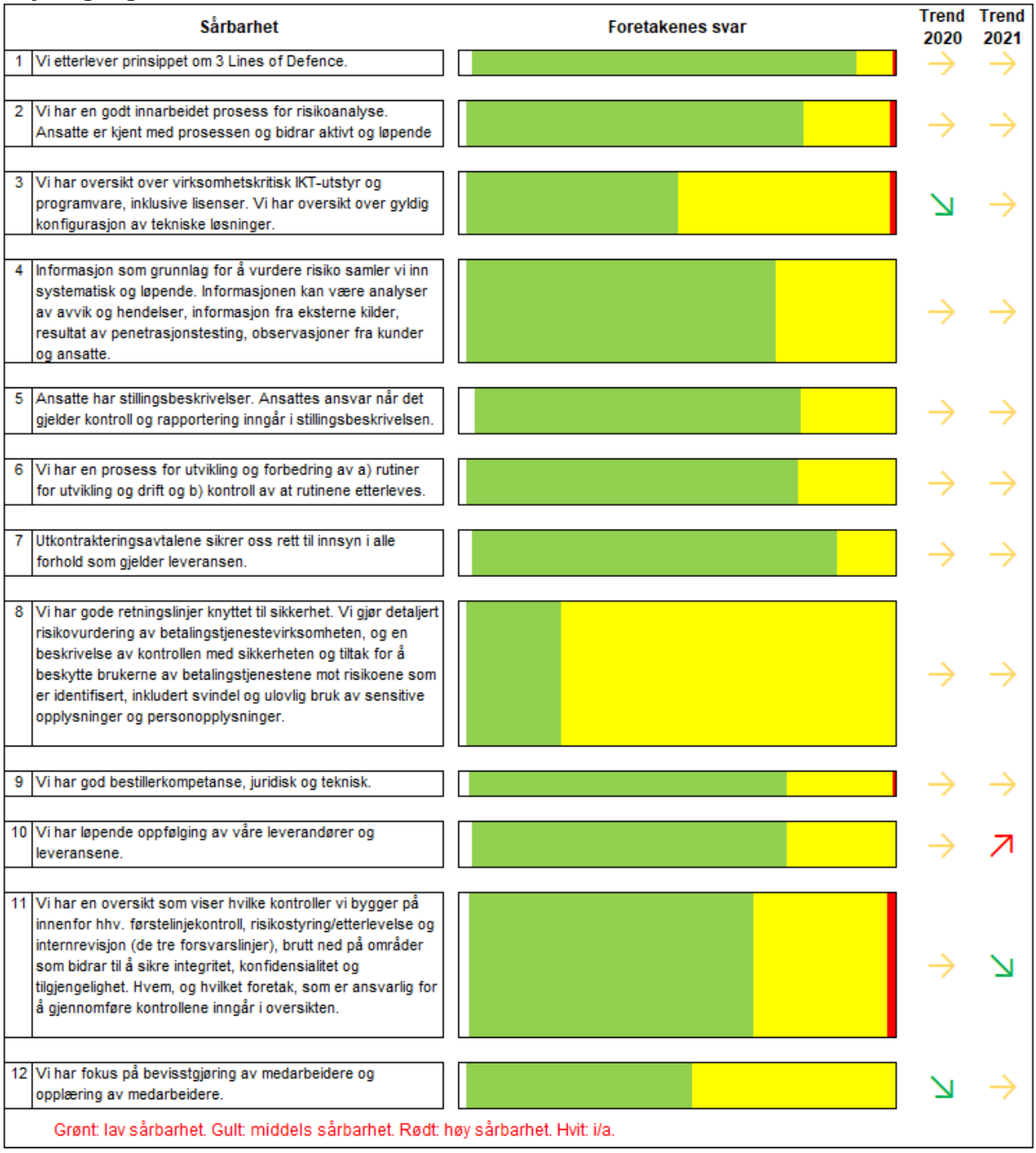
Tabellene oppsummerer resultatet av spørreundersøkelsen. Foretakenes svar er angitt med fargekoder. Grønt gir uttrykk for lav sårbarhet, gult innebærer middels sårbarhet, og rødt uttrykker høy sårbarhet. Ingen farge innebærer at foretak ikke har svart.

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

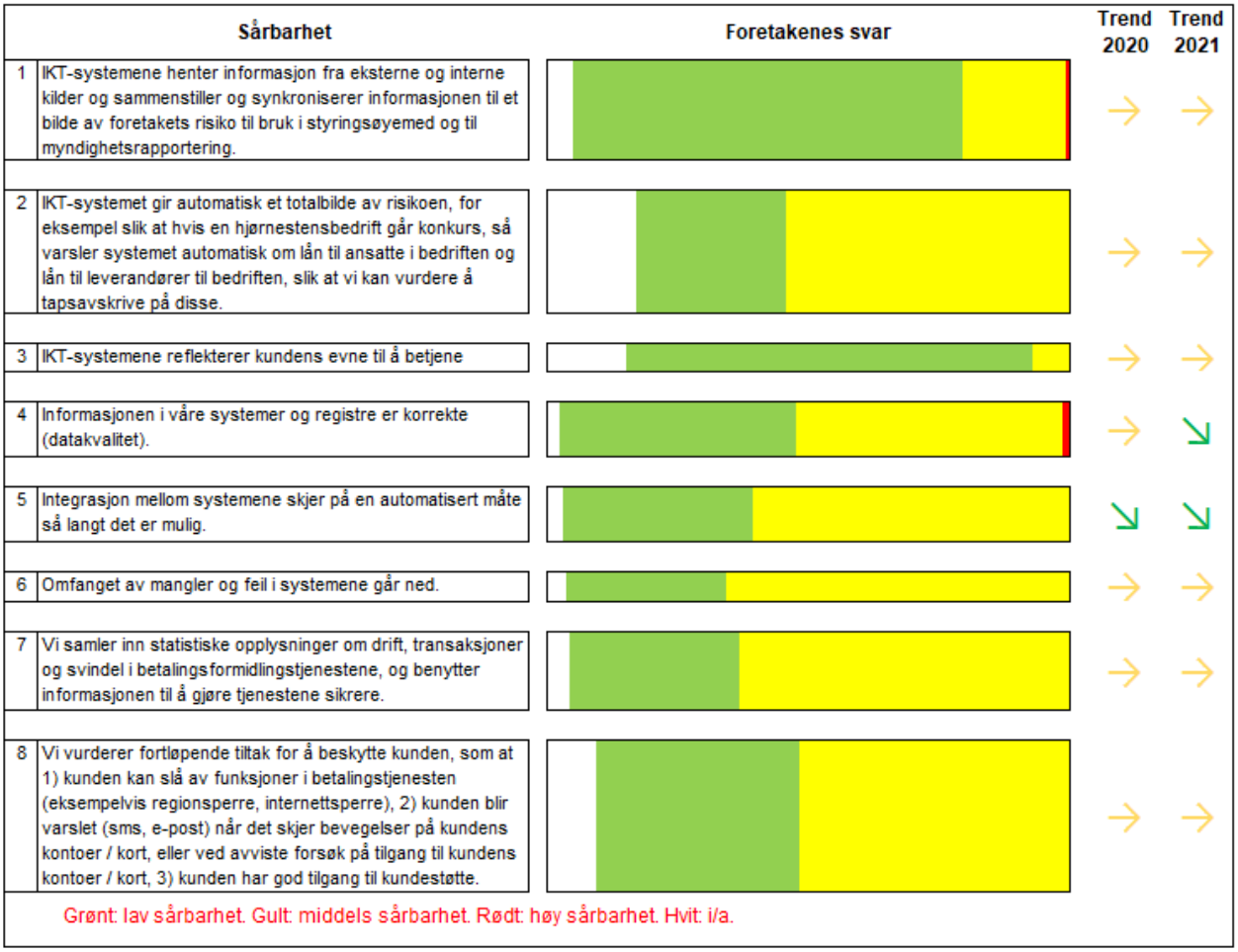
[49] Forskrift om systemer for betalingstjenester stiller krav om at betalingstjenestetilbydere årlig skal rapportere til Finanstilsynet en samlet vurdering av operasjonell risiko og sikkerhetsrisiko knyttet til tilbyderens betalingstjenester og en vurdering av om tilbyderens tiltak er tilstrekkelige. 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.

anses å være økende (intervallet +0,2 til +1), og piler som peker nedover, indikerer at sårbarheten anses å være minkende (intervallet -0,2 til -1). For hvert spørsmål er det beregnet et aritmetisk gjennomsnitt av foretakenes svar.

Styring og kontroll



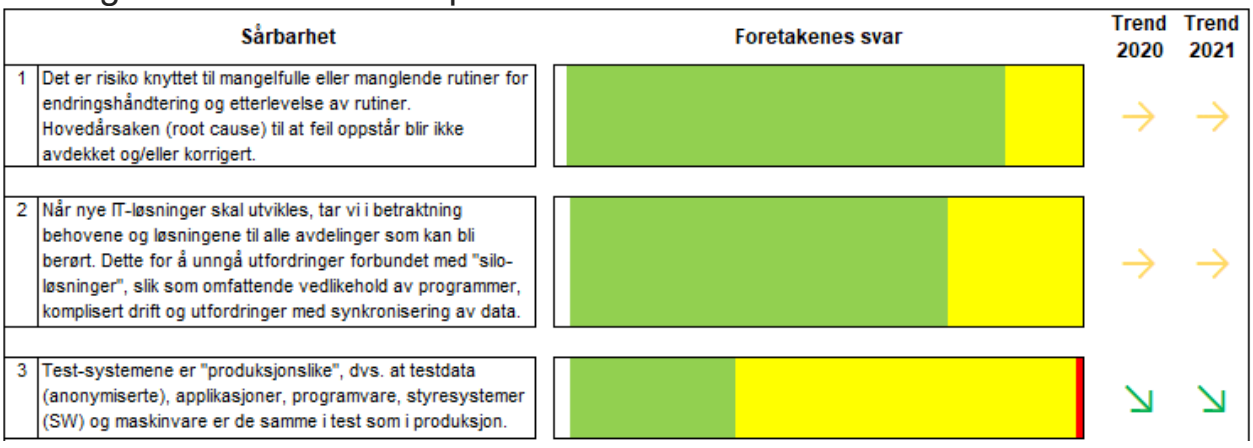
Beslutningsstøtte



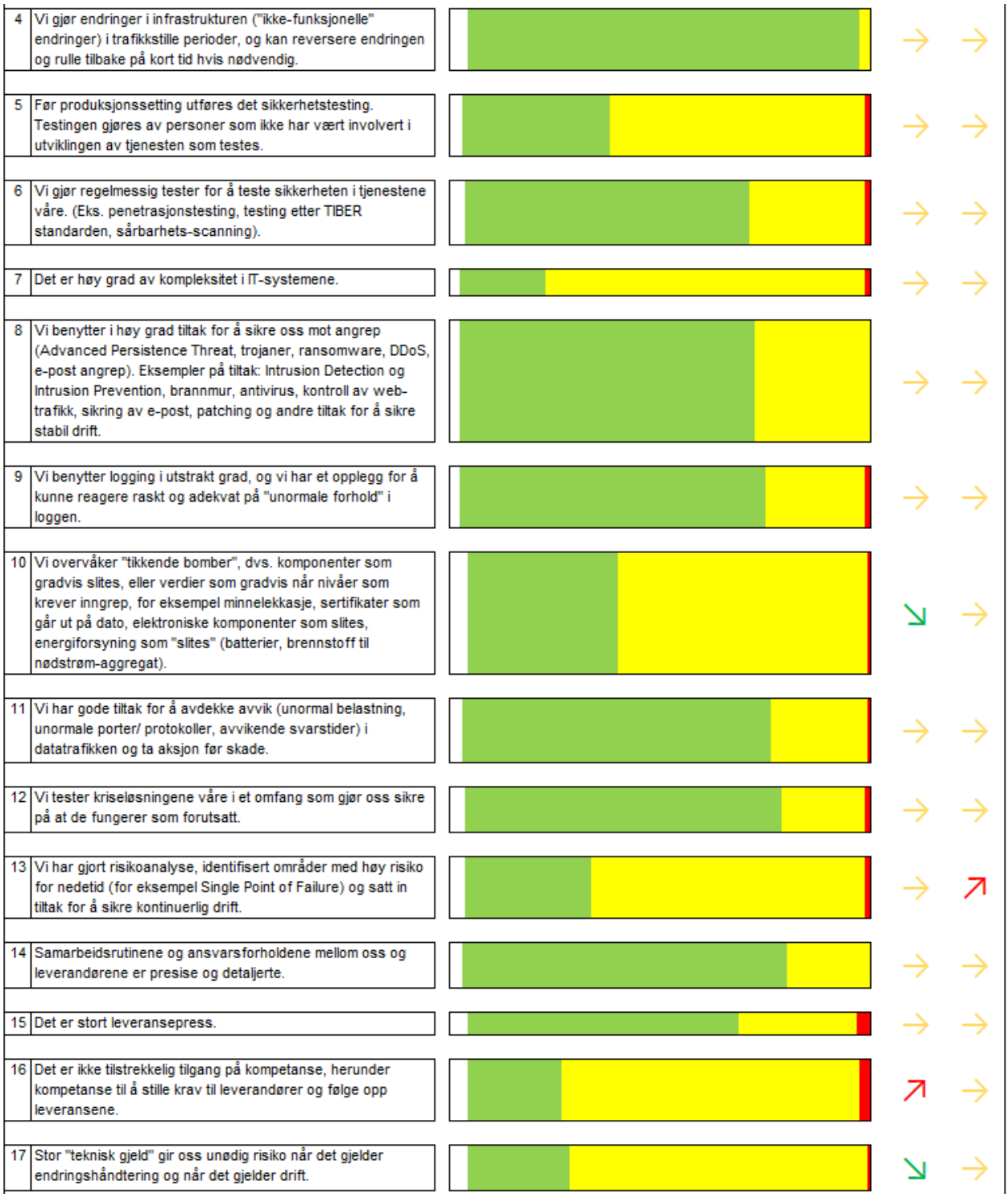
	Sårbarhet	Trend 2020	Trend 2021
1	IKT-systemene henter informasjon fra eksterne og interne kilder og sammenstiller og synkroniserer informasjonen til et bilde av foretakets risiko til bruk i styringsøyemed og til myndighetsrapportering.	→	→
2	IKT-systemet gir automatisk et totalbilde av risikoen, for 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	→	→
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.	→	→
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.	→	→

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

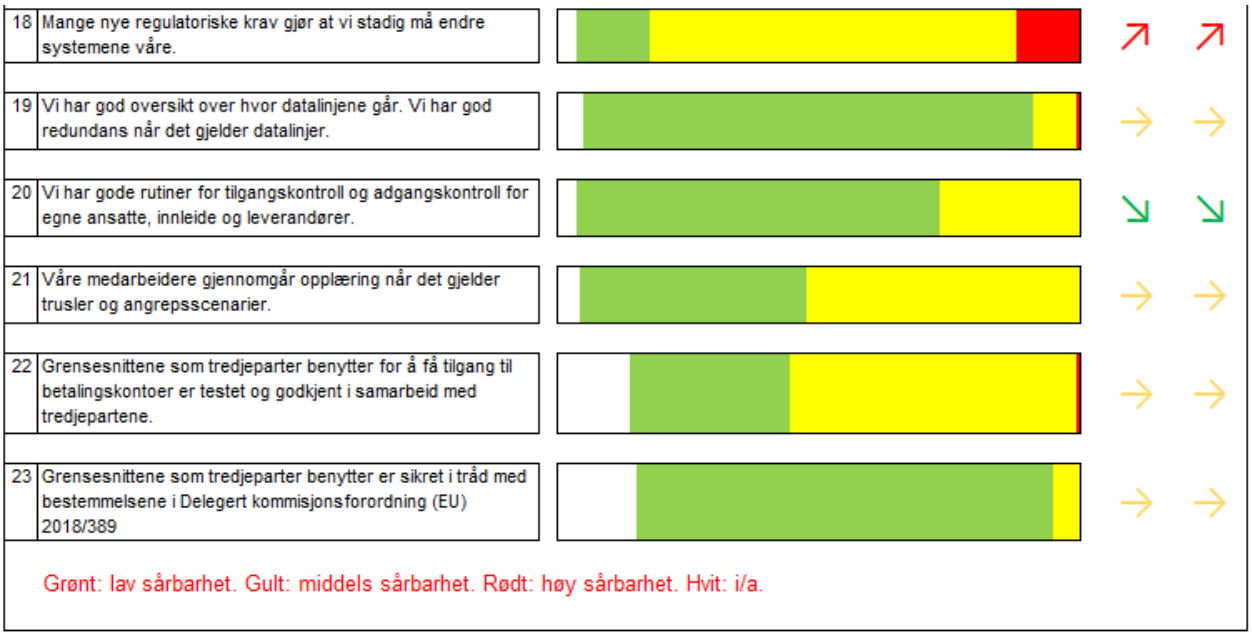
Drift og katastrofeberedskap



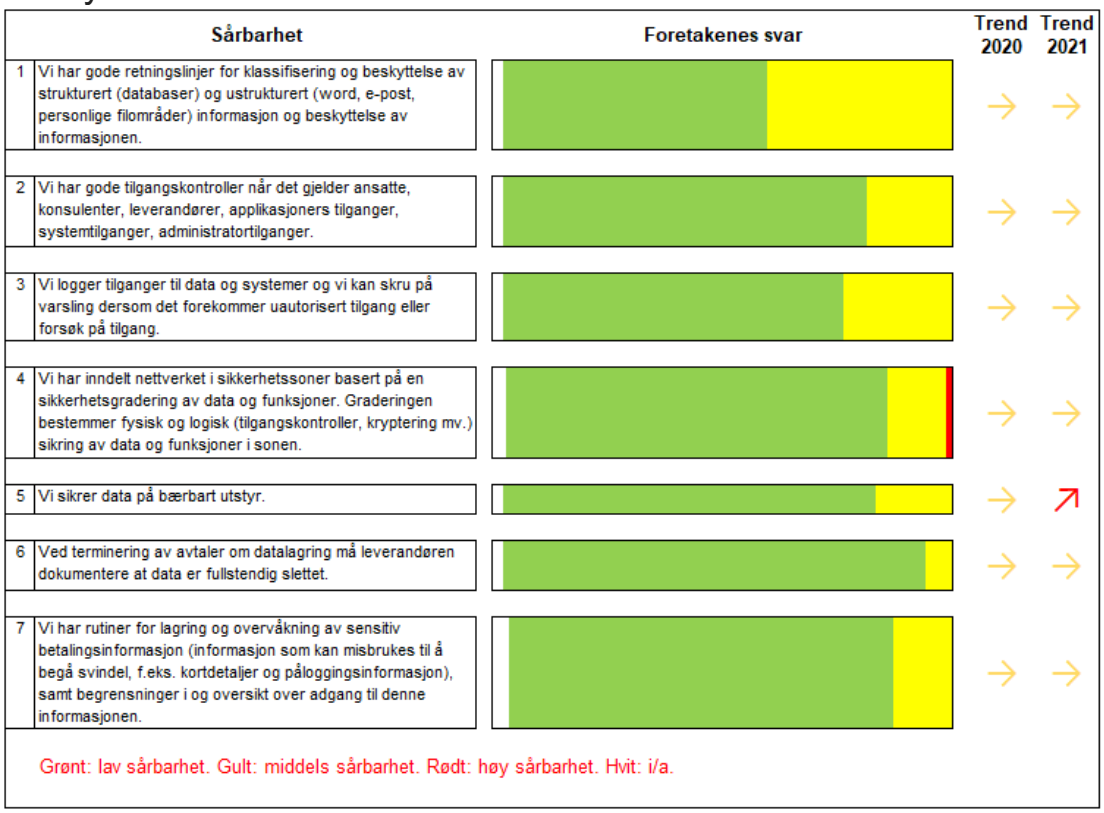
	Sårbarhet	Trend 2020	Trend 2021
1	Det er risiko knyttet til mangelfulle eller manglende rutiner for endringshåndtering og etterlevelse av rutiner. Hovedårsaken (root cause) til at feil oppstår blir ikke avdekket og/eller korrigert.	→	→
2	Når nye IT-løsninger skal utvikles, tar vi i betraktning behovene 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.	→	→
3	Test-systemene er "produksjonslike", dvs. at testdata (anonymiserte), applikasjoner, programvare, styresystemer (SW) og maskinvare er de samme i test som i produksjon.	↘	↘



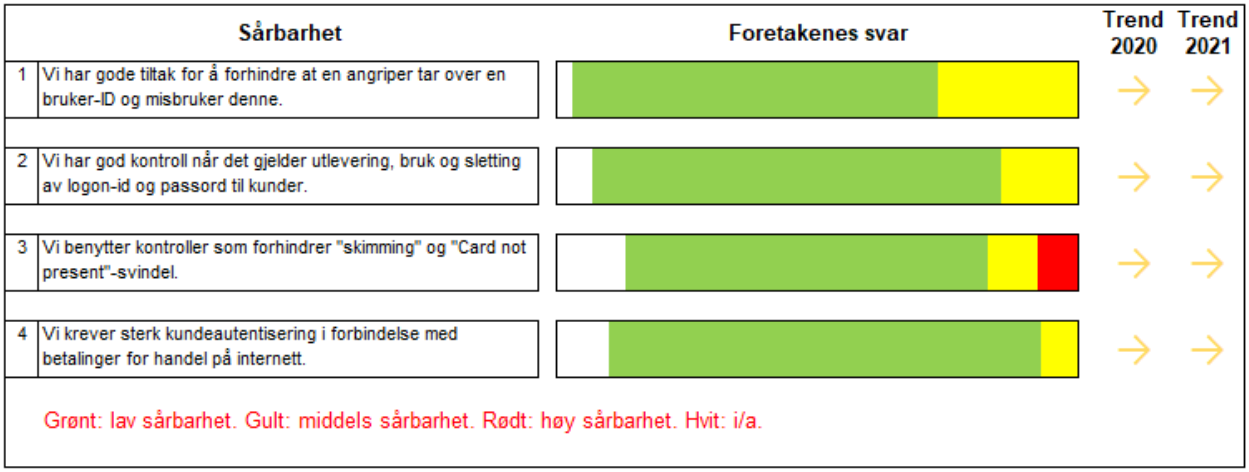
4	Vi gjør endringer i infrastrukturen ("ikke-funksjonelle" endringer) i trafikkstille perioder, og kan reversere endringen og rulle tilbake på kort tid hvis nødvendig.	→	→
5	Før produksjonssetting utføres det sikkerhetstesting. Testingen gjøres av personer som ikke har vært involvert i utviklingen av tjenesten som testes.	→	→
6	Vi gjør regelmessig tester for å teste sikkerheten i tjenestene våre. (Eks. penetrasjonstesting, testing etter TIBER standarden, sårbarhets-scanning).	→	→
7	Det er høy grad av kompleksitet i IT-systemene.	→	→
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.	→	↗
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.	↘	→



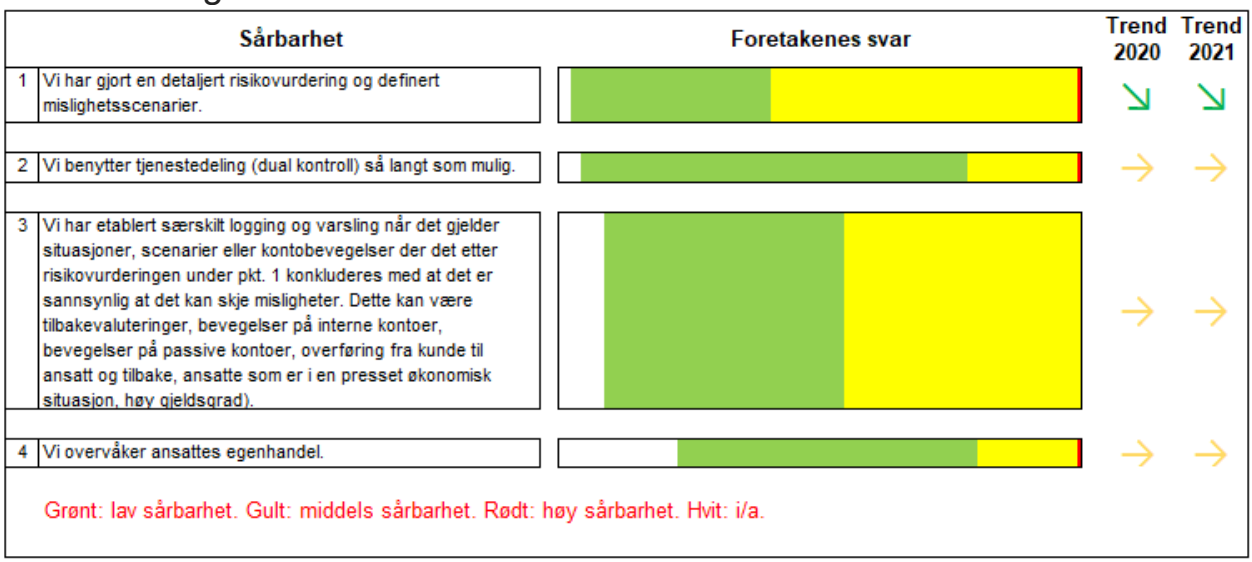
Beskyttelse av data



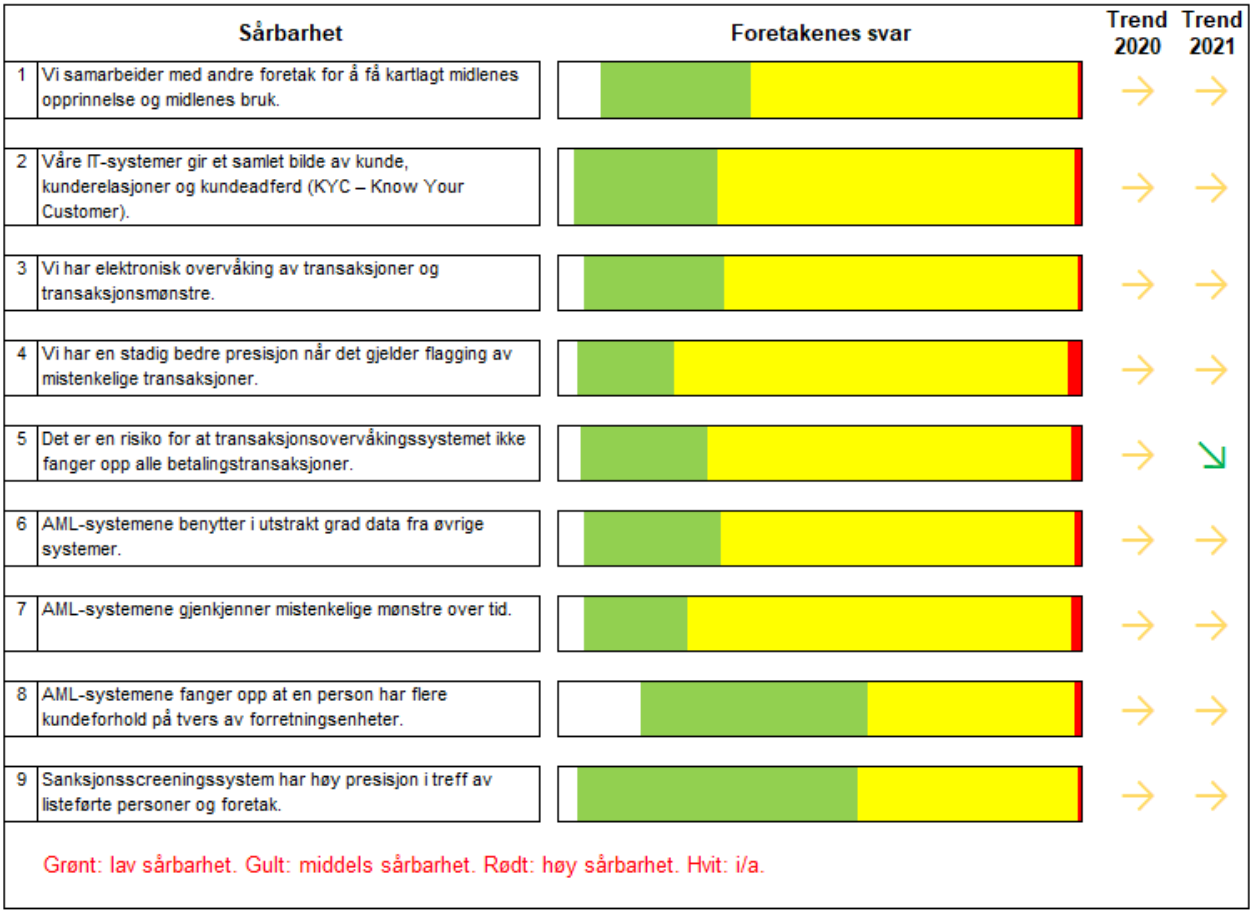
ID-tyveri



Interne misligheter



Hvitvasking



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(e) 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 relevante 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 svarer "Høy" i kolonne tre. Basert på en analyse av hendelsene angir foretaket i kolonne fire hovedårsakene til at hendelsene oppstod, og til at hendelsene kom overraskende på foretaket. I kolonne seks omtaler foretaket kort tiltak som er gjort for å forbedre dette i løpet av siste år.

Til slutt bes foretaket oppgi de forholdene som anses å utgjøre 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 3.1 i kapittel 3.

Følgende definisjoner benyttes:

Sårbarhet: Svakhet i teknisk infrastruktur, funksjoner og prosesser som kan resultere i at uønskede hendelser inntreffer.
Trussel: Forhold med potensial til å forårsake en uønsket hendelse.
Risiko: Uttrykkes som kombinasjonen av sannsynligheten for at en hendelse inntreffer og konsekvensen dersom den inntreffer. Utilstrekkelige eller sviktende interne prosesser eller systemer, menneskelige feil eller eksterne aktører kan medføre økende sannsynlighet for at en hendelse inntreffer, med tilhørende konsekvenser.
Konsekvens: Følger 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 anser 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 middels og konsekvensen som moderat. Dette er basert på følgende vurderinger:

- Sannsynligheten for at mangler i etterlevelsen av lover og regler ikke oppdages som følge av manglende kontroll av foretakets operative ledelse, vurderes som *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 ikke nødvendig

forståelse av risikobildet til å sikre en stabil og sikker IKT-drift, vurderes som *middels til høy* og med *moderat* konsekvens.

- Sannsynligheten for uklare roller mellom foretakets første- og andrelinjeforsvar som fører til alvorlige svakheter i overvåkingen av og kontrollen med foretakets styring og kontroll, vurderes som *middels* og med *begrenset til middels* konsekvens.
- Sannsynligheten for at alvorlige sårbarheter ikke avdekkes som følge av mangelfull risikostyring mellom operative enheter 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 anser den samlede risikoen, på nåværende tidspunkt, knyttet til sårbarheter ved kompetanse og kompetansestyring som middels. Sannsynligheten for at 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 framtidige behov som følge av mangelfull kompetansestyring, vurderes som *lav til middels* og med *begrenset til moderat* 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 *middels* og med *moderat til høy* 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 *lav til middels* og med *moderat* konsekvens.
- Sannsynligheten for at manglende forståelse av risikoene ved bruk av 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 anser 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 til høy* 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 *lav til middels* 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 til middels* 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 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 anser 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 2021 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 som følge av mangelfull eller manglende sikkerhetstest, vurderes som *middels til 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* 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 svake punkter i forsvarsverket fordi foretaket ikke har kontroll med sårbarhetsstyringen av software og hardware med tilhørende konfigurasjon, vurderes som *middels* med *alvorlig* konsekvens.
- Sannsynligheten for at nye applikasjoner eller endringer i eksisterende applikasjoner settes i produksjon med alvorlige sikkerhetshull, inklusive hos leverandører og underleverandører, vurderes som *middels* med *alvorlig* konsekvens.
- Sannsynligheten for at tredjeparts applikasjoner som tredjepart integrerer i eller mellom foretakets systemer og foretakets kunder, fører til uønskede sikkerhetshendelser, vurderes som middels til høy med *moderat* til *alvorlig* 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 *lav til middels* 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 for at 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 utro medarbeidere utnytter svakheter i systemet for økonomisk vinning, vurderes som *lav til middels* og med *begrenset* konsekvens.

- Sannsynligheten for at utro ansatte i foretaket 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.
- Sannsynligheten for at foretak benytter kommunikasjonsmåter som også benyttes av kriminelle ved forsøk på sosial manipulering vurderes som *middels* og med *begrenset til moderat* konsekvens.

Informasjonslekkasje

Finanstilsynet anser 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 middels til 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 *middels* 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 til *høy* og med *moderat* 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 innsidere og overleverer eller sender konfidensiell informasjon, eksempelvis liste over e-postadresser 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 anser den samlede risikoen knyttet til sårbarheter ved IKT-drift som middels til høy. Samlekarakteren er ikke endret i årets rapport, men Finanstilsynet vurderer at risikoen er noe redusert fra 2021 med bakgrunn i den bedrede tilgjengeligheten til betalingstjenester og kunderettede løsninger. 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 *middels til høy* og med *moderat til 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 *lav til middels* og med *moderat til alvorlig* 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 *moderat til alvorlig* konsekvens.
- Sannsynligheten for at overvåking av IT-miljøet ikke avdekker unormale forhold ved driften (f.eks. utgåtte sertifikater, databaser, minnelekkasjer og elektroniske komponenter), vurderes som *middels* og med *moderat til alvorlig* konsekvens.
- Sannsynligheten for driftsproblemer grunnet manglende oppfølging av teknisk gjeld vurderes som *middels* og med *moderat* konsekvens.
- Sannsynligheten for at testsystemet ikke er tilstrekkelig likt produksjonssystemet, vurderes som *middels til høy* og med *moderat til alvorlig* konsekvens.

Kontinuitetsledelse og kriseledelse

Finanstilsynet anser 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 alvorlig til 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 til høy* 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 *middels* 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 i evalueringen, 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* og med *kritisk* konsekvens.

Geopolitiske forhold

Finanstilsynet anser risikoen knyttet til sårbarheter overfor utenlandske aktører som leverer kritiske IKT-tjenester til foretakene i Norge, som middels til høy. Selv om det var store endringer i geopolitiske forhold i 2021, blant annet grunnet koronapandemien, har foretakene ved sine tiltak vist at problemene pandemien medførte, er håndtert på en god måte. Foretakene har informert Finanstilsynet om at krigen i Ukraina har endret trusselbildet i et cybersikkerhetsperspektiv, men samtidig har det ikke vært rapportert noen økning hendelser. 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 tilgjengelige, 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 der utenlandske leverandører ikke er tilgjengelige, vurderes som *lav til middels* og med *alvorlig* konsekvens.
- Sannsynligheten for kommunikasjonsbrudd med utlandet hvor konsekvensen er at utenlandske leverandører er avskåret fra å utføre kritiske IKT-tjenester, vurderes som *lav* og med *alvorlig* konsekvens.

- Sannsynligheten for at foretak blir rammet av geopolitiske forhold knyttet til IKT-drift, vurderes som *lav til middels* og med *alvorlig* konsekvens.

Endringsstyring

Finanstilsynet anser 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 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* og med *moderat til alvorlig* konsekvens.
- Sannsynligheten for at funksjonelle endringer (programvare) introduserer sårbarheter i foretakets forsvarsverk, vurderes som *lav til middels* 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 *middels* og med *moderat* konsekvens.

Tilgangsstyring

Finanstilsynet anser den samlede risikoen knyttet til sårbarheter ved tilgangsstyring som middels til høy. Samlekarakteren er ikke endret i årets rapport, men Finanstilsynet vurderer at risikoen er noe forhøyet fra 2020 med bakgrunn i rapporterte hendelser og gjennomførte tilsyn. 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 til middels* og med *moderat* konsekvens.
- Sannsynligheten for at personell hos en leverandør med utvidede tilgangsrettigheter utfører ulovlige handlinger, vurderes som *middels* og med *alvorlig* konsekvens.
- Sannsynligheten for at ansatte eller personell hos leverandører har tilgangsrettigheter uten at foretakets ledelse er klar over dette, vurderes som *middels til høy* og med *moderat* konsekvens.
- Sannsynligheten for at ansatte eller personell hos leverandører har utvidede tilgangsrettigheter uten at ledelsen er klar over dette, vurderes som *middels til høy* og med *moderat til alvorlig* 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 til høy* og med *alvorlig* konsekvens.

Datakvalitet

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

- Sannsynligheten for at beslutninger tas på feil grunnlag, vurderes som *middels* og med *moderat* konsekvens
- Sannsynligheten for at AML-systemet ikke fanger opp alle betalingstransaksjoner, vurderes som *middels til høy* og med *moderat* konsekvens

Vedlegg 3: Finanstilsynets oppfølging

Finanstilsynets tilsyn med IKT og betalingstjenester – sentrale områder

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-/cybersikkerhets-arbeidet 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 av mulig inntrenging i deres systemer.

Andre prioriterte tema 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 områder som følges opp.

Arbeid med betalingssystemer

EUs reviderte betalingstjenestedirektiv (PSD2)[48] er tatt inn i norsk lovgivning og ligger til grunn for tilsynet med foretakenes betalingstjenester. Foretakene vil blant annet bli fulgt opp med hensyn til etterlevelse av ny forskrift om systemer for betalingstjenester[50], risiko knyttet til betalingstjenestene og etterlevelse av meldeplikten ved nye eller endrede betalingstjenester. Kontotilbyderes grensesnitt (API-er) for tiltrodde tredjeparters tilgang til konto vil også bli fulgt opp, jf. uttalelse fra den europeiske banktilsynsmyndigheten (EBA)[51]. I konsesjonsbehandlingen vil det påses at foretakene har godt dokumenterte rutiner på områder relatert til IKT- og betalingstjenester.

Foretakene vil også bli fulgt opp på at betalingsløsningene er robuste, at tilfredsstillende beredskap er etablert for løsningene, og at beredskapen i det elektroniske betalingssystemet er forsvarlig.

Samarbeidet med Norges Bank knyttet til betalingssystemet og finansiell infrastruktur videreføres.

[50] Lovdata: Forskrift om systemer for betalingstjenester
[51] EBAs uttalelse om tiltrodde tredjeparters tilgang til konto: EBA calls on national authorities to take supervisory actions for the removal of obstacles to account access under the Payment Services Directive

Oppfølging av hendelser

I tilsynsvirksomheten er oppfølging av IKT-hendelser et prioritert område. Finanstilsynet vil i 2022 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. Også avdekkede sårbarheter i foretakenes IKT-løsninger vil bli fulgt opp.

Finanstilsynet vil videreføre sin årlige gjennomgang av hendelsesrapporteringen til 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 endret avtale om utkontraktering av IKT-virksomhet som er kritisk eller viktig for foretaket, melder denne til Finanstilsynet, slik finanstilsynsloven § 4c krever, jf. meldepliktforskriften[52].

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 hendelsesscenarioer, og det vurderes om ansvarsforhold ved krisesituasjoner er tilstrekkelig klare. Det er planlagt gjennomføring av beredskapsøvelser også i 2022, og tiltak knyttet til funn i tidligere øvelser vil bli fulgt opp.

Særskilte hendelser som koronapandemien, krigen i Ukraina og foretakenes innretning av sin IKT-virksomhet vil bli fulgt opp, 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[53]. Finanstilsynet er sektorvis responsmiljø (SRM) på finansmarkedsområdet og utøver rollen i samarbeid med Nordic Financial

[52] Lovdata: Forskrift om meldeplikt ved utkontraktering av virksomhet mv.
[53] Nasjonal sikkerhetsmyndighet (NSM): Rammeverk for håndtering av IKT-hendelser

CERT i tråd med avtalte regler for informasjonsutveksling. NSMs rammeverk ligger til grunn for samhandlingen mellom Finanstilsynet og Nordic Financial CERT.

Oppfølging av trusselbildet knyttet til digital kriminalitet

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

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

Sammen med Norges Bank etablerte Finanstilsynet i 2021 et rammeverk for testing av cybersikkerhet i finanssektoren (TIBER-NO). Målet er å bidra til finansiell stabilitet gjennom økt motstandsdyktighet mot cyberangrep for kritiske funksjoner i norsk finansiell sektor. Arbeidet vil bli fulgt opp av en styringsgruppe ledet av Norges Bank med deltakelse fra Finanstilsynet.

Finanstilsynet vil gjennomføre regelmessige møter med foretak og Nordic Financial CERT og delta i Nasjonalt cybersikkerhetssenter (NCSC), europeiske tilsynsmyndighetenes arbeid med IKT-sikkerhet og European Systemic Cyber Group (ESCG) under Det europeiske systemrisikorådet (ESRB).

Forbrukervern

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 også bli lagt vekt på at foretakene ivaretar kundenes sikkerhet ved bruk av deres løsninger og tjenester.

Finanstilsynet vil også følge opp at foretakene ikke deler kundenes data uten samtykke, og at data ikke kommer tredjepart urettmessig i hende. Det vil videre bli fulgt opp at foretakene kommuniserer med sin kunder på en trygg og forsvarlig måte, blant annet at de ikke sender eller ber om informasjon om kunden eller kundens engasjement i e-poster eller gjør kundene usikre ved å vedlegge lenker i e-poster eller SMS-kommunikasjon.

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, for eksempel gjennom mulighet for å sperre 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[54] bestemmelser om kontanttilbud. 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[55].

[54] Lovdata: Lov om finansforetak og finanskonsern (finansforetaksloven)
[55] Lovdata: Forskrift om finansforetak og finanskonsern (finansforetaksforskriften)

Vedlegg 4: Retningslinjer fra EBA, EIOPA og ESMA

Relevante retningslinjer ved utkontraktering fra European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA) og European Securities and Markets Authority (ESMA) som utdyper regelverket.

EBA:	
EBA/GL/2021/05	Guidelines on internal governance under Directive 2013/36/EU
EBA/GL/2019/02	Guidelines on outsourcing arrangements
EBA/GL/2019/04	Guidelines on ICT and security risk management
EIOPA:	
EIOPA-BoS-14/253	Guidelines on system of governance
EIOPA-BoS-20-002	Guidelines on outsourcing to cloud service providers
EIOPA-BoS-20/600	Guidelines on information and communication technology security and governance
ESMA:	
ESMA50-157-2403	Guidelines on outsourcing to cloud service providers

Vedlegg 5: Oversikt over virksomhetskritisk utstyr, programvare, forretningsfunksjoner, prosesser og informasjon

De siste årenes tekniske utvikling har bidratt til at foretakene i finanssektoren i stadig større grad opererer med koblede/sammensatte IKT-tjenester, flere plattformer (on-premises, tradisjonelt datasenter og skytjenester) og multisourcing (flere leverandører, der disse igjen kan ha underleverandører). Det gir et mer komplekst risikobilde og en utvidet angrepsflate for ondsinnede handlinger. For å ha kontroll med IKT- og sikkerhetsrisiko stiller denne utviklingen større krav til foretakenes systematiske arbeid med å ha oversikt over kritiske prosesser, programvare, utstyr og informasjon og risikoene forbundet med disse.

I de to retningslinjene fra europeiske tilsynsmyndigheter som særlig berører IKT, framgår det at foretakene bør etablere slike oversikter:

EBA: Guidelines on ICT and security risk management[56] (EBA GL)
EIOPA: Guidelines on information and communication technology security and governance[57] (EIOPA GL)

Finanstilsynet presiserer at retningslinjene for etablering av de ulike oversiktene beskriver ønsket resultat. Det er foretaket selv som beslutter antall oversikter og hvor mange systemer som inngår.

Utstyrsregister

Foretaket bør etablere en IT-utstyrsoversikt (utstyrsregister) som holdes løpende oppdatert (EBA GL, retningslinje 50 og EIOPA GL, retningslinje 44.). Utstyrsoversikten bør inkludere IT-systemer, nettverksutstyr og databaser mv. Videre bør utstyrsoversikten være tilstrekkelig detaljert til at foretaket umiddelbart skal kunne identifisere utstyr, plassering, sikkerhetsklassifisering og eierskap (EBA GL, retningslinje 53 og EIOPA GL, retningslinje 44). Utstyrsoversikten bør også dokumentere konfigurasjonen til utstyret, den enkelte utstyrsenhets relasjon til annet utstyr og de gjensidige

[56] EBAs retningslinjer om IKT-sikkerhet og -risiko: EBA Guidelines on ICT and security risk management
[57] EIOPAs retningslinjer om IKT-sikkerhet og governance: Guidelines on information and communication technology security and governance

avhengighetene mellom utstyrsenheter (EBA GL, retningslinje 53 og EIOPA GL, retningslinjer 31 og 45).

Oversikt over funksjoner og prosesser

Foretaket bør etablere og vedlikeholde en oppdatert oversikt over **forretningsfunksjoner, roller og støtteprosesser, der funksjonene/prosessene bør dokumenteres** med informasjon om data som behandles i prosessen, IT-systemer, ansatte, kontraktører, tredjeparter og avhengigheter til andre interne og eksterne systemer og prosesser. Som et minimum bør foretaket ha registerført og dokumentert kritiske forretningsfunksjoner og prosesser (EBA GL, retningslinjer 15 og 16 og EIOPA GL, retningslinje 17).

Risikovurdering og klassifisering av funksjoner, prosesser og utstyr

Utstyr, forretningsfunksjoner og støtteprosesser bør klassifiseres i henhold til viktighet, der klassifiseringen som et minimum bør ta høyde for beskyttelseskrav med tanke på konfidensialitet, integritet og tilgjengelighet (EBA GL, retningslinjer 17, 18 og 19 og EIOPA GL, retningslinje 17). Data/informasjon må behandles og lagres i tråd med klassifiseringen.

Foretaket bør **identifisere og dokumentere IKT- og sikkerhetsrisikoer** som kan innvirke på utstyr, forretningsfunksjoner og støtteprosesser, og sørge for at risikoene revurderes periodisk samt når større endringer påvirker utstyr, forretningsfunksjoner og prosesser (EBA GL, retningslinje 20 og EIOPA GL, retningslinje 17).

Klassifiseringen og informasjonen om forretningsfunksjoner og støtteprosesser bør revurderes/ajourføres i forbindelse med periodisk risikovurdering og ved større endringer som påvirker utstyr, forretningsfunksjoner og prosesser (EBA GL retningslinjer 17, 18 og 53 og EIOPA GL, retningslinje 17).

Praktisk bruk av oversiktene

Oversiktene er viktige ved blant annet:

- forretningsmessige konsekvensanalyser (Business Impact Analysis)
- styring og kontroll med kontinuitetsarbeidet
- utvikling av respons- og gjenopprettingsplaner, der dokumentasjon av de gjensidige avhengighetene mellom utstyr kan for eksempel benyttes i oppfølgingen av sikkerhets- og operasjonelle hendelser, inkludert cyberangrep.
- arbeidet med konfigurasjons- og endringsstyring
- informasjonsbeskyttelse for å hindre at data kommer på avveie
- prioritering av utbedringer ved sårbarhetsstyring (det viktigste utstyret først) – viktig å ha kontroll med siste versjoner av programvare
- livsløpshåndtering (life cycle management) av maskinvare og programvare for ha kontroll med utrangert utstyr og tjenester som ikke lenger supporteres

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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

05.2022