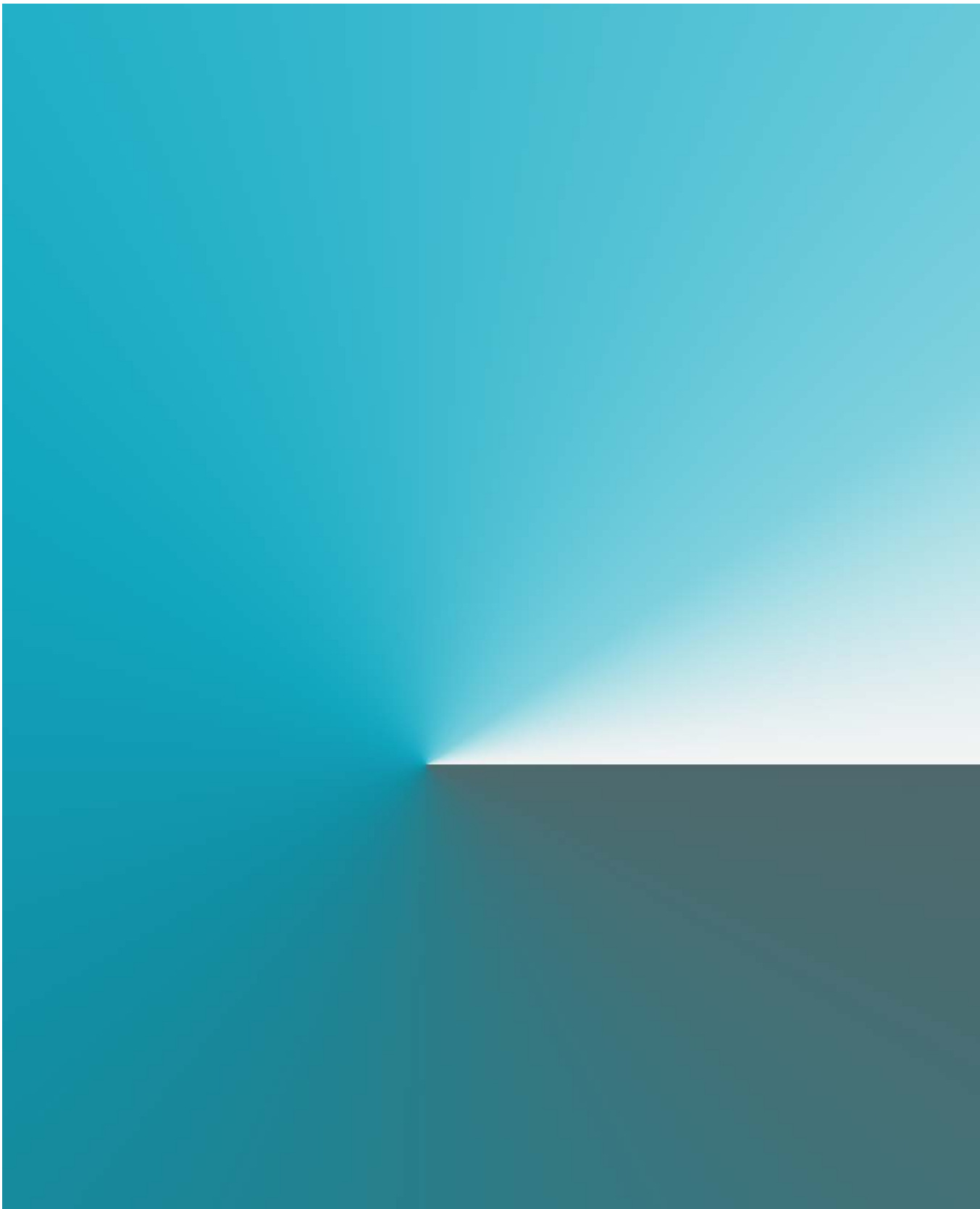
FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Finanssektorens bruk av informasjons- og kommunikasjonsteknologi (IKT)

RISIKO- OG SÅRBARHETSANALYSE (ROS)

2023



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

Risiko- og sårbarhetsanalyse 2023

1. OPPSUMMERING 4
2. FINANSIELL INFRASTRUKTUR 7
2.1 Betydning 7
2.2 Beredskapsutvalget for finansiell infrastruktur 8
2.3 Endringer i den finansielle infrastrukturen og fellestiltak innen finansnæringen 9
3. DIGITAL KRIMINALITET OG TRUSSELBILDE 11
3.1 Det digitale trusselbildet er i endring 11
3.2 Organisert kriminalitet som trusselfaktor 11
3.3 Andre stater som trusselfaktor 12
3.4 Digitale angrep som politisk virkemiddel 12
3.5 Angrep på verdikjeder 13
3.6 Angrep på sentrale tjenesteleverandører og datasentre 14
3.7 Kriminelles bruk av kunstig intelligens 14
3.8 Nasjonalt tiltak – TIBER-NO 14
3.9 Tiltak i foretakene 15
3.10 Samarbeid innen sikkerhetsområdet 16
4. FINANSTILSYNETS OBSERVASJONER OG VURDERINGER 18
4.1 Tilsyn med IKT og betalingstjenester 18
4.2 Leverandøroppfølging av tilgangsstyring 20
4.3 Foretakenes vurdering av viktige forhold knyttet til IKT-virksomheten 21
4.4 Oppsummering av foretakenes rapportering av risiko og sårbarhet 23
4.5 Styrket forbrukervern i ny finansavtalelov 27
4.6 Misbruk av innloggingsinformasjon 27
4.7 Risiko knyttet til bruk av samtaleroboter 29
5. SVINDEL OG SVINDELSTATISTIKK 30
5.1 Rapportering av svindelstatistikk 30
5.2 Tap knyttet til misbruk av betalingskort 30
5.3 Tap knyttet til misbruk av betalingskort PÅ NORSKE BRUKERSTEDER 33
5.4 Tap knyttet til kontooverføringer 33
5.5 Tap knyttet til kontooverføringer initiert av betalingsfullmektiger 34
5.6 Tap ved svindel gjennom sosial manipulering 34
5.7 Tap der svindler utsteder betalingen 35
6. HENDELSESRAPPORTERING 36
6.1 Antall IKT-relaterte hendelser 36

6.2 Sikkerhetshendelser 36
6.3 Feil og sårbarheter hos skyleverandører 38
6.4 Hendelser I systemer for å avdekke hvitvasking og terrorfinansiering 38
6.5 Årsaker til operasjonelle hendelser 38
6.6 Hendelser etter foretakstype 39
6.7 Analyse av hendelsene som mål på tilgjengelighet 41
6.8 Hendelser knyttet til problemer med dedikerte PSD2-grensesnitt 42
7. UTKONTRAKTERING 43
7.1 Melding om utkontraktering 43
7.2 Styring og kontroll 44
7.3 Avtalebestemmelser for opphør av utkontrakteringsavtaler 44
7.4 Risiko knyttet til utkontraktering 44
8. VURDERING AV DEN FINANSIELLE INFRASTRUKTUREN OG FORETAKENES IKT-VIRKSOMHET 47
8.1 Den finansielle infrastrukturen er robust 47
8.2 Risiko knyttet til sårbarheter i foretakenes IKT-virksomhet 47
9. NYTT REGELVERK OM DIGITAL MOTSTANDSDYKTIGHET – DORA-FORORDNINGEN 50

Redaksjon avsluttet 3. mai 2023
Figurdata oppdatert per 3. mai 2023

1. OPPSUMMERING

Den finansielle infrastrukturen i Norge er robust. Endringer i det digitale trusselbildet, blant annet som følge av Russlands angrep på Ukraina og økt digital kriminalitet, har bidratt til økt oppmerksomhet rettet mot faren for systemiske cyberhendelser og viktigheten av digital robusthet og motstandsdyktighet innen finanssektoren.

Finanstilsynet og Beredskapsutvalget for finansiell infrastruktur (BFI) har særlig oppmerksomhet mot virksomheter som støtter viktige funksjoner, herunder kritiske samfunnsfunksjoner fastsatt av Direktoratet for samfunnssikkerhet og beredskap[1]. De sentrale foretakene i den norske finansielle infrastrukturen har gjennomgående gode beredskapsplaner. Aktørene har løpende kontroll med driften og har ved behov iverksatt nødvendige tiltak raskt.

I 2022 var det ingen IKT-hendelser med konsekvenser for finansiell stabilitet. Både antall sikkerhetshendelser og antall operasjonelle hendelser var omtrent som i 2021. Negative følger av hendelser er redusert de siste årene, og Finanstilsynet anser at tilgjengeligheten til betalingstjenester og andre kunderettede tjenester samlet sett var om lag uendret fra 2021 til 2022 og noe bedre enn i de foregående årene.

Det var færre angrep på den finansielle infrastrukturen i 2022 enn i 2021, men omfanget av digital kriminalitet med konsekvens for finanssektoren synes fortsatt å øke. Selv om digital kriminalitet rettet mot foretak i den norske finanssektoren ikke har ført til systemkriser eller alvorlige hendelser, er det avdekket alvorlige sårbarheter som kunne fått store konsekvenser dersom de hadde blitt utnyttet. I tillegg var det sikkerhetshendelser hos leverandører som fikk konsekvenser for berørte foretak.

Foretakene i finanssektoren arbeider kontinuerlig med å styrke forsvarsverket og automatisere håndteringen av uønskede hendelser. Angrep avverges som oftest før de får konsekvenser for foretaket og foretakets kunder. Finansnæringens samhandling gjennom NFCERT[2] bidrar til å heve kunnskapen om risikobildet og aktuelle trusler og gjør foretakene bedre rustet til å håndtere digitale angrep.

For å opprettholde en robust finansiell infrastruktur mener Finanstilsynet at foretakene fortsatt bør styrke arbeidet på IKT-området ved å redusere sannsynligheten for operasjonelle hendelser, øke motstandsdyktigheten mot digital kriminalitet og bedre IKT-sikkerheten generelt. Arbeidet må tilpasses utviklingen i det digitale trusselbildet.

Gjennom tilsynsvirksomheten ble det i 2022 avdekket svakheter og sårbarheter i foretakenes arbeid med IKT. Finanstilsynet påpekte blant annet svakheter i ulike foretaks arbeid med krisehåndterings- og beredskapsplaner, som for eksempel manglende eller mangelfulle forretningsmessige konsekvensanalyser. Videre ble det påpekt mangler i etterlevelsen av gjeldende regelverk ved utkontraktering av IKT-virksomhet, herunder at avtaler i enkelte tilfeller ikke er behandlet av foretakets styre. Det ble også påpekt at enkelte foretak har mangelfull oppfølging av leverandørers etterlevelse av foretakets sikkerhetskrav. Det er også funnet manglende involvering i leverandørens test av krisehåndteringsløsninger, manglende IKT-kompetanse i foretaks andre forsvarslinje og mangler i foretakenes transaksjonsovervåking knyttet til hvitvasking og terrorfinansiering.

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

Etter et sikkerhetsbrudd hos en IKT-tjenesteleverandør høsten 2021 fulgte Finanstilsynet i 2022 opp at foretakene forbedrer sin oppfølging av IKT-tjenesteleverandører når det gjelder administrasjon, oppfølging og kontroll av tilgangsrettigheter.

Beredskapen i det elektroniske betalingssystemet vil bli ytterligere styrket i 2023 gjennom innføring av såkalt offline PIN i BankAxepts kortordning. PIN-koden kan da verifiseres mot informasjon i betalingskortet dersom betalingsterminaler er uten nettforbindelse.

Finanstilsynet anser sårbarheter i foretakenes forsvarsverk mot digital kriminalitet som den mest sentrale IKT-risikoen. Det skyldes både høy sannsynlighet for angrep og alvorlig konsekvens om angrep lykkes. Risikoen knyttet til svikt i foretaks forsvarsverk mot digital kriminalitet anses også å være noe høyere enn i 2021. Sårbarheter knyttet til leverandørstyring, tilgangsstyring og informasjonslekkasje er også sentrale risikoer, der den samlede risikoen anses som middels til høy. Risikoen knyttet til mangelfull leverandørstyring er ansett som høyere i 2022 enn året før, mens risikoen knyttet til foretaks forsvarsverk mot informasjonslekkasje er ansett som noe lavere.

Gjennom rapportering og i dialogen med Finanstilsynet peker foretak og leverandører av IKT-tjenester på flere sentrale risiko- og sårbarhetsforhold knyttet til IKT-virksomheten. Det trekkes fram at manglende oversikt over hvilke kontroller som inngår i foretakets internkontroll, kan føre til at operasjonell risiko ikke avdekkes. Manglende kompetanse kan føre til at problemer og feil som oppstår kan være utfordrende å løse, og mer komplekse leverandørforhold kan føre til svakere oppfølging og kontroll med kritiske og utkontrakterte IKT- tjenester. Foretakene peker også på at mangler i sikkerhetsarbeidet kan føre til at kriminelle påfører foretaket skade gjennom digitale angrep.

Andre risikofaktorer foretakene trekker fram, er komplekse verdikjeder og knapphet på IKT-ressurser. Det pekes videre på en økende trend når det gjelder omfanget av ID-tyveri, og risikoen for ID-tyveri blir omtalt som en av de høyeste risikoene. Økt kompleksitet i systemporteføljen kan føre til lavere driftsstabilitet, og høy utviklingstakt gir risiko knyttet til endringshåndtering. Det trekkes også fram at mangler i beredskapsarbeidet kan gi utfordringer med å opprettholde kritiske IKT-tjenester ved alvorlige hendelser som berører normalt driftssted. Foretakene trekker også fram at mangler i tilgangsstyringen kan medføre skade som følge av bevisste eller ubevisste handlinger, og at mangler eller feil i data kan føre til at analyser, kontroller og beslutninger i foretaket foretas på feil eller for svakt grunnlag.

Det var i 2022 økt phishing-aktivitet, både mot kunder og mot ansatte i foretakene, der kriminelle forsøkte å få tilgang til brukernes innloggingsdetaljer (engangskode, passord, e.l.). I ett tilfelle ble en ansatt frastjålet innloggingsdetaljer. Angriperen tilegnet seg alle rettighetene til den ansatte og benyttet disse til kriminelle handlinger.

At BankID benyttes i stort omfang til både private og offentlige tjenester utenom finanssektoren, og til innlogging til ulike typer tjenester, medfører fare for at brukerne ikke er tilstrekkelig årvåkne mot falske innlogginger og blant annet kan bli fralurt sikkerhetsinformasjon. Det store omfanget av bruksområder gir kriminelle mulighet for å benytte seg av et bredt spekter av moduser i svindelvirksomheten.

I 2022 var det 156 000 svindeltransaksjoner med kort, mot 147 000 i 2021. Til tross for en liten økning i antall svindeltransaksjoner økte tapene på kortsvindel med 35 prosent, til 219 mill. kroner i 2022. Andelen svindeltransaksjoner var størst for grensekryssende transaksjoner, særlig for transaksjoner utført i land utenfor EØS.

For kontooverføringer, hovedsakelig nettbank, utgjorde tapene 395 mill. kroner i 2022, en økning fra 346 mill. kroner i 2021. I prosent av samlede kontooverføringer var imidlertid tapene noe lavere i 2022 enn i 2021. Tapene er knyttet både til transaksjoner der svindleren utsteder eller modifiserer betalingen og transaksjoner der svindleren manipulerer betaleren til selv å gjennomføre betalingen.

Tap som følge av svindel ved sosial manipulering, der betaler er lurt til å iverksette svindeltransaksjonen, utgjorde 290 mill. kroner i 2022, mot 240 mill. kroner i 2021. Av dette var 269 mill. kroner knyttet til kontooverføringer, mens resten var knyttet til bruk av betalingskort. En andel av svindeltransaksjonene der svindleren iverksetter transaksjonen basert på stjålet informasjon anses også å være en konsekvens av sosial manipulering. I tillegg er det trolig mørketall, noe som gjør at det er vanskelig å anslå det samlede omfanget av tap knyttet til sosial manipulering.

Bankene forhindrer en stadig større andel av svindelforsøkene, noe som bidrar til å begrense tapene. Svindel gjennom sosial manipulering ser fortsatt ut til å være den mest lønnsomme metoden for kriminelle.

Finanstilsynet mottok i 2022 i overkant av 240 meldinger om utkontraktering, noe som er om lag 20 prosent flere enn året før. Som i de foregående årene viser meldingene økt bruk av skytjenester for både applikasjons- og infrastrukturtjenester. Som følge av utkontraktering får foretakene ofte et høyere antall plattformer å forholde seg til, noe som kan gi økt kompleksitet og et mer sammensatt risikobilde.

Ved utkontraktering av IKT-virksomhet må foretakene vurdere en rekke risikoforhold, blant annet knyttet til styring og kontroll, sikkerhet, oppfølging av tjenesteleveranser, beredskap og krisehåndtering. Videre må de besitte tilstrekkelig kompetanse, blant annet til å kunne stille nødvendige krav til leverandørens løsninger og IKT-sikkerhet, og fullt ut forstå leverandørens leveranser. Oppfølgingen av utkontraktert IKT-virksomhet må innlemmes i foretakets system for risikostyring og internkontroll.

Hovedtemaet for Finanstilsynets tilsynsvirksomhet med IKT og betalingstjenester i 2023 er foretakenes styring og kontroll av IKT-virksomheten, foretakenes arbeid med IKT-sikkerhet, inkludert cybersikkerhet, og foretakenes beredskapsarbeid og testing av beredskaps- 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 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.

Finanstilsynet følger 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.

BFI følger opp beredskap og hendelser i den finansielle infrastrukturen. I spesielle situasjoner, som ved koronapandemien og krigen i Ukraina, følger BFI særlig 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 BETYDNING

Effektive, robuste og stabile betalings- og oppgjørssystemer og markedsplasser, samt tillit mellom aktørene, er grunnleggende for finansiell stabilitet og velfungerende markeder. Direktoratet for samfunnssikkerhet og beredskap (DSB) har utpekt finansielle tjenester som en samfunnskritisk funksjon.[3] Dersom det ikke er mulig å gjennomføre eller gjøre opp betalinger eller handel med finansielle instrumenter, vil viktige samfunnsfunksjoner etter kort tid ikke lenger fungere tilfredsstillende. De samfunnsmessige konsekvensene vil kunne bli særlig store dersom foretak som opererer på vegne av mange eller alle foretak rammes.

Den finansielle infrastrukturen skal sørge for at betalinger og transaksjoner i finansielle instrumenter blir registrert, avregnet og gjort opp. Infrastrukturen er kompleks og omfatter mange aktører og leverandører, se boks 2.1. Manglende robusthet eller lavt sikkerhetsnivå hos en enkelt aktør eller leverandør kan utgjøre et svakt ledd i verdikjedene, slik at hendelser kan smitte over på andre aktører. Finanssektoren er også avhengig av infrastruktur som kraftforsyning og elektronisk kommunikasjon. Svikt hos sentrale aktører i finansnæringen eller i infrastrukturen kan få betydelige samfunnsmessige konsekvenser[4] og i verste fall true den finansielle stabiliteten, uavhengig av om svikten er forårsaket av kriminell aktivitet eller operasjonelle avvik.

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.

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

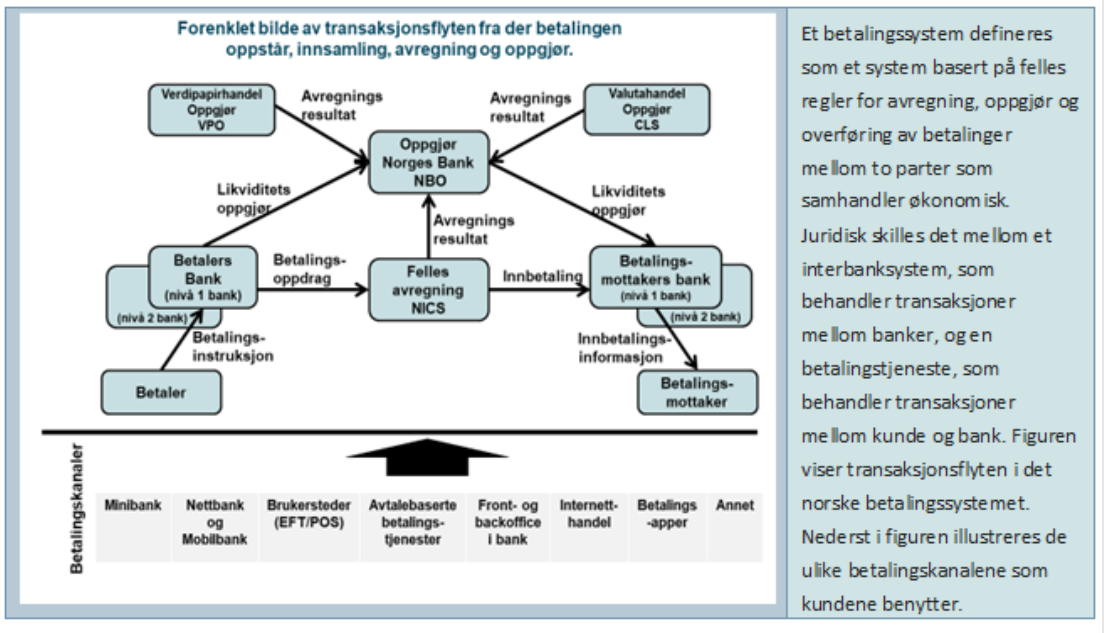
[3] Direktoratet for samfunnssikkerhet og beredskap (DSB): Samfunnets kritiske funksjoner
[4] Sikkerhetsloven angir blant annet økonomisk stabilitet og handlefrihet som nasjonale sikkerhetsinteresser, jf. sikkerhetsloven § 1-5 Definisjoner (Lovdata). Dette omfatter finansiell infrastruktur og objekter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

Boks 2.1 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 finansavtaleloven, 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 med ansvar for kritiske funksjoner 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 av BFIs arbeid er gitt i utvalgets årsrapporter, se Finanstilsynets nettsted, temasiden Beredskapsutvalget for finansiell infrastruktur.

2.3 ENDRINGER I DEN FINANSIELLE INFRASTRUKTUREN OG FELLESTILTAK INNEN FINANSNÆRINGEN

Det ble i løpet av 2022 både gjennomført og varslet flere vesentlige endringer i den norske finansielle infrastrukturen.

Bankene i Eika Alliansen inngikk i 2020 avtale med Tietoevry om leveranse av kjernebankløsninger til lokalbankene i alliansen. Overgangen fra SDC til Tietoevry skjer i puljer og er planlagt ferdigstilt i 2023. For flere av bankene er overgangen allerede gjennomført uten vesentlige avvik. Avtalen innebærer at andelen norske banker som benytter Tietoevry som driftsleverandør, øker betydelig.

Verdipapirsentralen AS (Euronext Securities Oslo) har planlagt å flytte sin IKT-drift til Tietoevry i løpet av mai 2023.

Overgangen til Tietoevry for Verdipapirsentralen AS og bankene i Eika Alliansen innebærer isolert sett økt konsentrasjonsrisiko siden flere foretak i finanssektoren allerede benyttet Tietoevry som driftsleverandør.

For å utvikle tjenester over landegrensene i Norden inngikk Vipps i 2021 avtale om en felles løsning for Vipps lommebok og betalingsløsninger, Danske Banks lommebok Mobilepay og OP Financial Groups lommebok Pivo. Innsigelser fra det europeiske konkurransetilsynet førte til at Pivo måtte trekke seg fra sammenslutningen. Vipps overtok i 2022 Mobilepay, og virksomheten ble innfusjonert i det nye selskapet Vipps Mobilepay AS mai 2023. Avtalen har medført at BankAxept og BankID er skilt ut fra lommebokvirksomheten i Vipps og etablert som et eget selskap, BankID BankAxept AS.

BankID BankAxept AS lanserte i 2020 løsningen BankID-app. I 2022 ble en gradvis utfasing av BankID på mobil påbegynt. Det er ikke lenger mulig å aktivere ny BankID på mobil for den enkelte bruker, men løsningen vil fungere i en overgangsfase.

Modernisering av betalingsinfrastrukturen

Straksbetalinger

I 2021 satte Bits, som er bank- og finansnæringens infrastrukturselskap, i gang "Straks 2.1"-prosjektet for overgang til ISO20022 i transaksjonsutvekslingen for straksbetalinger og direkte innsending til avregningssystemet NICS Real. Prosjektet er planlagt ferdigstilt i løpet av første halvår 2023. Ved utgangen av 2022 hadde mer enn 60 banker tatt i bruk Straks 2.1-løsningen. For å øke bruken av straksbetalinger må bedriftsmarkedets behov for formidling av strukturert kundeinformasjon imøtekommes.

Modernisering av Norwegian Interbank Clearing System (NICS)

Moderniseringen av NICS er et viktig langsiktig tiltak iverksatt av Bits for å opprettholde en effektiv og sikker infrastruktur for avregning mellom bankene. Formålet er å rendyrke NICS som avregningsløsning, standardisere ved å tilpasse NICS til ISO 20022 og fjerne bindinger mellom NICS og andre tjenester i tillegg til å redusere leverandøravhengigheten. Prosjektet vil påvirke en rekke bank- og fellesløsninger i tillegg til NICS-løsningen.

Bankbytte (AvtaleGiro)

Bits har utviklet funksjonalitet for at kunder via selvbetjening enkelt skal kunne flytte faste AvtaleGiro-betalingsoppdrag mellom banker ved bankbytte, noe som vil forenkle bankbytter. Løsningen ble tatt i bruk i begynnelsen av 2023.

BankAxept-reserveløsning

Den norske finansnæringen har etablert en reserveløsning for BankAxept for å styrke beredskapen i det elektroniske betalingssystemet. Deltakelse i reserveløsningen er frivillig for brukersteder som tar imot BankAxept-betalingskort. Reserveløsningen ble i 2021 styrket ved at kapasiteten for bruk av BankAxept-betalingskort i betalingsterminaler ble vesentlig økt. Forbedringen tilbys samfunnskritiske aktører i detaljhandelen med bred utbredelse, som dagligvarekjeder, apotekkjeder og utsalgssteder av drivstoff.

En forutsetning for at reserveløsningen skal kunne utgjøre en fullgod beredskapsløsning, er at brukerstedene tiltrer reserveløsningen og regelmessig tester om den fungerer som forutsatt. En hendelse 16. mai 2022 viste at en rekke brukersteder ikke hadde etablert reserveløsning, og at testing av betalingsterminalene var mangelfull, se punkt 6.5. For å bedre beredskapen i det elektroniske betalingssystemet må bankene og BankAxept arbeide for å øke antall brukersteder tilsluttet reserveløsningen, herunder flere samfunnskritiske aktører i detaljhandelen.

Offline PIN

Finansnæringen arbeider kontinuerlig med å forbedre beredskapen i det elektroniske betalingssystemet. Et tiltak fra Bits er å styrke BankAxepts kortordning ved å innføre såkalt offline PIN, som innebærer at PIN-koden kan verifiseres mot informasjon i betalingskortet dersom betalingsterminaler er uten nettforbindelse. Løsningen kan blant annet benyttes ved bruk av BankAxepts reserveløsning dersom kortet er klargjort for dette. Prosjektet ble påbegynt i 2022, og det er forventet at utstedelse av kort med støtte for offline PIN vil starte i løpet av 2023. Alle ordinære BankAxept-kort må skiftes ut, noe som vil ta ca. tre år.

Digitale fellesløsninger for forsikringsnæringen

Forsikringsforetakene i Norge har et omfattende samarbeid om etablering og drift av fellesløsninger gjennom Finans Norge Forsikringsdrift (FNF). FNF er en sentral aktør i infrastrukturen for den norske forsikringsnæringen og har som formål å ivareta drift av oppgaver og aktiviteter som medlemsbedriftene anser som formålstjenlig å utføre i fellesskap. Noen av de mest sentrale løsningene er:

- TFFAuto	Register over forsikringspliktige motorkjøretøy i Norge.
- DBS	Takseringssystem for skader på motorkjøretøy.
- Finans-FREG	Finansnæringens oppkobling til modernisert folkeregister, FREG.
- Norsk pensjon	Pensjonsportal som gir en samlet oversikt over forventet alderspensjon fra ulike pensjonsordninger.
- Pensjonskontoregisteret	Register over pensjonskontoer.

Digitalt samarbeid offentlig privat (DSOP)

Offentlig sektor og finansnæringen samarbeider om digitalisering og effektivisering av viktige tjenester i samfunnet gjennom DSOP[5]. Løsningene gir betydelige gevinster for finansnæringen, kunder og det offentlige. Flere prosjekter er under utvikling. For noen av tjenestene har det vært behov for regulatoriske avklaringer før full funksjonalitet kunne tas i bruk. Både opprinnelig formål for datainnhenting og sektorspesifikt regelverk kan legge føringer for videre deling av informasjon. Et sentralt prinsipp i DSOP er gjenbruk av funksjonalitet etablert i tidligere prosjekter og eksisterende nasjonale fellesløsninger i enten offentlig eller privat regi.

[5] BITS' nettsted: Digital Samhandling Offentlig Privat og Aktivitetsrapport DSOP 2022

3. DIGITAL KRIMINALITET OG TRUSSELBILDE

3.1 DET DIGITALE TRUSSELBILDET ER I ENDRING

Det digitale trusselbildet er i stadig endring, blant annet som følge av krigen i Ukraina og det sikkerhetspolitiske bildet, herunder spenningene mellom Kina og USA. Kriminelle utvikler kontinuerlig sine metoder og samhandling. Det er også vanskelig å skille mellom trusler fra henholdsvis organiserte kriminelle og fremmed etterretning, siden kriminelle miljøer kan selge tjenester til 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.

I 2022 bidro det digitale trusselbildet og digital kriminalitet til økt oppmerksomhet om faren for systemiske cyberhendelser og viktigheten av digital motstandsdyktighet. Også innenfor finanssektoren vet trusselaktører å utnytte at sårbarhetsflatene utvides som følge av digitaliseringen.

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

Foretakene arbeider kontinuerlig med å videreutvikle sine systemer for overvåking av unormal aktivitet, automatisk håndtering av avdekkede hendelser og avverging av angrep. Selv om foretakenes systemer stadig blir bedre og hendelser i økende grad håndteres automatisk, er det likevel behov for betydelig manuell gjennomgang av avdekkede hendelser. Angrep avverges som oftest før de får konsekvenser for foretaket og foretakets kunder.

Foretakene arbeider kontinuerlig med å styrke sin kompetanse innen cybersikkerhet. Som omtalt under punkt 3.10 bidrar samhandling gjennom NFCERT til å heve kunnskapen i finansnæringen 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 egne risikoer og sårbarheter, iverksette forebyggende tiltak og forberede seg på å 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 varierende modenhet i foretakene knyttet til å vurdere risikoen ved manglende beskyttelse av data. For å kunne forebygge og håndtere hendelser effektivt er det viktig at foretakene gjennom en forretningsmessig konsekvensanalyse kartlegger hvilke verdier som kan være utsatt.

3.2 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. Kriminelle kan også ha som mål å skade IT-systemer og data, blant annet ved å gjøre tjenester utilgjengelige for bruk og informasjonsuthenting.

Organiseringen av angrepene har utviklet seg, med økt samarbeid og spesialisering mellom ulike grupperinger og ved etablering av nye konstellasjoner i forbindelse med hendelser. 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 (ransomware) er utbredt blant kriminelle organisasjoner, men har til nå ikke fått store konsekvenser for foretak i finanssektoren. Det er også økt kriminell aktivitet knyttet til nettsvindel. Det kan forventes stadig mer avanserte angrep fra kriminelle 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 mot norske finansinstitusjoner.

3.3 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.[6]

Krigen i Ukraina har så langt ikke ført til noen registrert økning i uønsket digital aktivitet mot norske foretak i finanssektoren. Risikoen vurderes likevel som forhøyet med bakgrunn i krigens varighet og en registrert økning av sikkerhetshendelser som kan relateres til krigen.

Det er avdekket at ukrainske IT-systemer ble korrumpert med skadelig kode lenge før krigen i Ukraina ble igangsatt.[7] Dette understreker betydningen av at foretakene allerede før en konflikt eller situasjon oppstår, må hindre at uvedkommende tar seg inn i systemer og introduserer ondsinnet kode. Erfaringene i Ukraina bør inngå i foretakenes risikovurderinger.

3.4 DIGITALE ANGREP SOM POLITISK VIRKEMIDDEL

Truslene fra ekstreme religiøse grupper og politisk motiverte aktører, som pro-russiske hacktivister, er økende. Angrep fra slike kriminelle aktører kan oppstå raskt. Et eksempel på dette er følgene av koran-brenningen i Stockholm, som medførte at muslimske grupperinger gjennomførte tjenestenektangrep (DDoS) mot svenske foretak og offentlige etater i februar 2023. Dersom angriperne ikke annonserer denne typen angrep i forkant eller påtar seg ansvar i etterkant, er det er ofte vanskelig å avdekke hvem som står bak.

Hensikten med slike angrep er vanligvis ikke økonomisk vinning, men å påkalle oppmerksomhet, spre usikkerhet, uro og desinformasjon eller demonstrere misnøye med et land eller foretak. Dette kan også ramme foretak i finanssektoren, noe tjenestenekt-angrepet mot BankID og andre finansielle foretaks nettsteder sommeren 2022 er et eksempel på. Angrepet kunne blant annet bidra til å så tvil om bankenes ID-løsning fungerte.

Omfanget av tjenestenektangrep fra hacktivister har økt. Slike angrep utgjør en begrenset trussel mot foretakenes virksomhet. DDoS-angrep rammer som oftest kun tilgjengeligheten til nettbaserte løsninger midlertidig. Slike angrep har ofte ikke større konsekvenser for de rammede foretakene enn at kunderettede selvbetjeningsløsninger og informasjonssider er ute av drift inntil foretaket har gjennomført mottiltak. Imidlertid kan slike angrep ha betydelige negative konsekvenser for brukerne dersom foretakene ikke raskt avhjelper situasjonen. De rammede foretakene evner i hovedsak fortsatt å utføre oppgaver som er uavhengige av nettbaserte løsninger.

[6] Nasjonal sikkerhetsmyndighet (NSM) – temaside: Nasjonalt cybersikkerhetssenter (NCSC)
[7] Digi.no – artikkel 24. februar 2022: Skadevare viser at angrepet på Ukraina har vært forberedt i flere måneder, mener cybersikkerhetsselskap

Tjenestenektangrep er godt egnet som verktøy for politiske ytringer fordi de kriminelle enkelt og til lav kostnad kan oppnå bred publisitet. Brukere opplever at rammede tjenester ikke kan nås gjennom vante nettsteder, og det kan skapes inntrykk av at sikkerheten i foretakets løsninger er truet.

Det er viktig å merke seg at i tillegg til gode løsninger og rutiner for å motvirke og avdekke angrep bør foretakene håndtere informasjon som omhandler et angrep med varsomhet, for at ikke angriperen skal nå sine mål om publisitet, og for å unngå usikkerhet og uro.

3.5 ANGREP PÅ VERDIKJEDER

Cyberkriminelles utnyttelse av sårbarheter i digitale verdikjeder har vist en økning i senere tid. Lange og uoversiktlige leverandørkjeder utgjør en sårbarhet som trusselaktører vet å utnytte. Trusselnivået for denne formen for angrep ventes fortsatt å øke. Verdikjedeangrep kan oppstå ved at en kompromittert underleverandør av komponenter, kode eller tjenester til leverandører som leverer til foretak i finansiell sektor, får installert korrumpert kode eller bakdører i sine løsninger, slik at angripere kan utnytte dette for å kompromittere foretakets løsning i ettertid. Slike angrep kan få betydelige konsekvenser for foretak som rammes.

Et eksempel på verdikjedeangrep er løsepengehendelsen som i 2022 fikk konsekvenser for minst sju norske finansforetak (inkludert banker, forsikringsforetak og fondsforvaltningsforetak) gjennom en systemleverandørs bruk av en underleverandør. Resultatet ble betydelige avbrudd i foretakenes drift, kostbar gjenoppretting av løsningene og et potensielt tap av anseelse for foretakene som ble rammet, se nærmere omtale i punkt 6.2. Andre eksempler på denne type angrep er utnyttelsen av kritiske sårbarheter i Microsoft Exchange Server og Apache Log4j i 2021, som rammet store organisasjoner på flere kontinenter.

Det er flere årsaker til at et verdikjedeangrep kan være vanskelig avdekke. 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.

Det finnes en rekke tiltak mot verdikjedeangrep som foretakene bør vurdere å iverksette eller følge opp at deres leverandører iverksetter

- mikrosegmentering[8] og kryptering av interne nettverk for å hindre uønskede tilganger og spredning av kode
- overvåking av nettverkstrafikk, inkludert intern nettverkstrafikk, for å avdekke avvikende mønster i datatrafikk eller adferd
- styrking av kontrollen med systemleveranser, leverandører og leverandørers bruk av underleveranser samt utkontrakteringer som omfatter IT-avhengigheter generelt
- bruk av systemer og løsninger for automatisert kontroll og verifisering av programkode.

Verdien for foretakene av å overvåke nettverkstrafikk vil reduseres ved at stadig større deler av foretakenes systemporteføljer utkontrakteres til skyleverandører. Imidlertid krever utkontrakteringen tett kontroll med leverandørenes arbeid med IKT-sikkerhet og oppfølging av underleverandører. I lys av den økende trusselen om verdikjedeangrep forventer Finanstilsynet at foretakene bruker nødvendige ressurser for forsvarlig oppfølging av sine leverandører.

[8] Mikrosegmentering er en metode og framvoksende beste praksis for å lage soner i datasentre og skymiljøer for å begrense brukertilganger og gir flere fordeler i forhold til mer etablerte tilnærminger som nettverkssegmentering og applikasjonssegmentering.

3.6 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 den finansielle infrastrukturen 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 leverandører, for eksempel driftssentraler, tjenesteleverandører, herunder utkontrakteringer, og andre foretak og organisasjoner man samarbeider med, og vurdere sårbarheten som følge av eventuelle vellykkede angrep mot disse og tiltak for å sikre forretningsmessig kontinuitet for kritiske forretningsfunksjoner.

Foretakene forventes også å gjennomføre realistiske beredskapsøvelser der scenarioet er bortfall av enkelte eller flere leverandører.

3.7 KRIMINELLES BRUK AV KUNSTIG INTELLIGENS

Kriminelle vil ta i bruk kunstig intelligens som ChatGPT til svindel og annen kriminalitet[9]. Potensialet for kriminell utnyttelse av denne typen kunstig intelligenssystemer, samtaleroboter (chatboter[10]), gir dystre utsikter, konstaterer Europol.

Kunstig intelligens kan utnyttes av kriminelle til raskt å innhente informasjon om nye og ukjente temaer. Det kan blant annet omfatte innsamling av opplysninger om hvordan man kan bryte seg inn i systemer, lage krypteringsverktøy eller fralure personer informasjon til svindelforsøk ved å lage overbevisende tekst med godt språk. Verktøyet kan brukes til å produsere mer sofistikerte e-poster og SMS-er, øke tempoet på produksjonen og omgå antivirusløsninger og spamfiltre.

Samtaleroboters evne til å produsere tekst gjør disse særlig effektive i forbindelse med såkalt phishing. Brukeren lures med tekst og lenke til en falsk nettside, der brukeren ledes til å gi fra seg påloggingsinformasjon eller annen informasjon som kan unyttes i kriminell hensikt, se punkt 4.6.

Jo mer avansert denne typen løsninger blir, jo mer krevende blir det for foretakene å beskytte seg. Det vil også kreve større aktsomhet fra brukere av finansielle tjenester for å unngå å bli fralurt informasjon.

3.8 NASJONALT TILTAK – TIBER-NO

Norges Bank og Finanstilsynet besluttet høsten 2021 å etablere et rammeverk for sikkerhetstesting av kritiske funksjoner i finansiell sektor i Norge.[11] Det norske rammeverket TIBER-NO[12] er basert på den europeiske sentralbankens TIBER-rammeverk (Threat Intelligence-based Ethical Red-Teaming). Målet er å bidra til finansiell stabilitet gjennom økt motstandsdyktighet mot cyberangrep i virksomheter som har funksjoner som er kritiske for det norske bank- og betalingssystemet.

---

[9] Europol 27. mars 2023: The criminal use of ChatGPT – a cautionary tale about large language models .
[10] En chatbot er et dataprogram utviklet for å samhandle med mennesker ved hjelp av skrift- eller talespråk.
[11] Finanstilsynets nyhetssak 21. oktober 2021: Norges Bank og Finanstilsynet etablerer rammeverk for testing av cybersikkerhet i finansiell sektor (TIBER-NO).
[12] Norges Banks nettsted: TIBER.

Rammeverket gir retningslinjer for testing av finansielle institusjoners evne til å oppdage, beskytte seg mot og håndtere avanserte cyberangrep. Bruk av trusseletterretning og eksterne testspesialister ("Red Team") skal bidra til at testingen blir realistisk.

Norges Bank bemannet i 2022 et TIBER Cyber Team (TCT-NO), som har det formelle ansvaret for å forvalte TIBER-NO og oppfølging av foretak for gjennomføring av TIBER-NO-testing.

Norges Bank og Finanstilsynet identifiserte i 2022 kritiske funksjoner og hvilke virksomheter som er ansvarlige for disse. Disse virksomhetene og andre virksomheter som viste spesiell interesse for sikkerhetstesting, ble i andre kvartal 2022 invitert til å delta i tester ved hjelp av TIBER-NO og på møteplassen TIBER-NO-forum. I fjerde kvartal 2022 startet de første foretakene opp testingen. TIBER-NO vil prioritere testing og sikring av funksjoner i finansiell sektor der konsekvensene blir størst dersom de blir kompromittert eller faller bort.

3.9 TILTAK I FORETAKENE

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

Tiltak for å motvirke angrep

Et viktig 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 komponenter som ikke er i bruk og passive og/eller utdaterte systemer. Det er også en tydelig sammenheng mellom eldre systemer i bruk og økt risiko for hendelser, samt kostnader for å sikre disse. 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.

Finanstilsynet anbefaler foretak som ikke omfattes av TIBER-NO, å vurdere bruk av TLPT-testing (Threat Led Penetration Test) og å forholde seg til anerkjente prinsipper og standarder ved gjennomføring av slike tester.

Beredskap

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

Det bør gjennomføres vurderinger og tiltak for å sikre at foretakenes beredskapsløsninger og sikkerhetskopier av systemer og informasjon er beskyttet mot digitale angrep.

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

Det er også viktig at foretakene tester hvor raskt egne systemer kan reetableres ved ulike scenarioer og vurderer hvilke konsekvenser eventuell nedetid vil kunne ha for foretaket og foretakets kunder.

Finanstilsynet oppfordrer foretak til å vurdere bruk av informasjons- og erfaringsdelingstjenester og CERT-er[13]. Bruk av slike tjenester har vist seg formålstjenlig for å styrke foretakenes kapasiteter både når det gjelder proaktive tiltak og som støtte under faktiske angrepssituasjoner.

3.10 SAMARBEID INNEN SIKKERHETSOMRÅDET

Samfunnskritiske virksomheter i finanssektoren

Sikkerhetsloven[6] angir økonomisk stabilitet og handlefrihet som én av flere nasjonale sikkerhetsinteresser.[4] Ansvarlig sektordepartement skal identifisere og holde oversikt over grunnleggende nasjonale funksjoner (GNF) samt virksomheter som har avgjørende eller vesentlig betydning for disse. For finanssektoren er det Finansdepartementet som fatter vedtak om at foretak som har avgjørende betydning for GNFer 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 digital kriminalitet og angrep fra utenlandsk etterretning. Trusler fra utenlandske statlige aktører er beskrevet under punkt 3.2.

Samarbeid og informasjonsutveksling gir bedre risikoforståelse

Næringen i Norden samarbeider om Nordic Financial CERT[13] (NFCERT)[2], der hensikten er å styrke den nordiske finansnæringens motstandskraft mot cyberangrep. Samarbeid og informasjonsutveksling mellom finansforetakene bidrar til å heve kunnskapen om det aktuelle trussel- og risikobildet, styrker motstandskraften mot cyberangrep og gjør foretakene bedre rustet til å reagere raskt og effektivt på cybersikkerhetstrusler og nettkriminalitet. NFCERT utarbeider og distribuerer regelmessig trusselrapporter til sine medlemmer. 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) med oppgave å håndtere IKT-sikkerhetshendelser i finanssektoren innenfor Finanstilsynets ansvarsområde. Finanstilsynet utøver rollen sammen med NFCERT.

Finanstilsynet deltar som partner i Nasjonalt cybersikkerhetssenter (NCSC), som er en arena for nasjonalt og internasjonalt samarbeid innen deteksjon, håndtering, analyse og rådgivning knyttet til digital sikkerhet. NCSC ble etablert for å styrke Norges motstandsdyktighet og beredskap på det digitale feltet og er en del av Nasjonal sikkerhetsmyndighet (NSM). 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 samarbeidsforum for myndigheter som fører tilsyn med IKT-sikkerhet i sin sektor. Samarbeidsforumet er nyttig for å utveksle informasjon og dele erfaringer mellom tilsynsmyndigheter. Finanstilsynet presenterte i 2022 sin tilsynsmodul for beredskap og krisehåndtering for forumet.

Sikkerhetstesting i finanssektoren

Finanstilsynet og Norges Bank etablerte i 2021 et rammeverk for testing av cybersikkerhet i finansiell sektor (TIBER-NO). Se nærmere omtale under punkt 3.8.

[13] Computer Emergency Response Team

Europeisk samhandling og informasjonsutveksling

Det europeiske systemrisikorådet (ESRB) publiserte i januar 2022 en strategi[14] for å redusere risikoen for finansiell ustabilitet som følge av cyberhendelser. Det pekes blant annet på behovet for å utvikle makroreguleringsvirkemidler som fanger opp systemisk cyberrisiko. ESRB har opprettet en arbeidsgruppe (ESCG)[15] for å undersøke systemisk cyberrisiko og om og hvordan en cyberhendelse kan forårsake en systemisk krise. Videre anbefaler ESRB at det opprettes et europeisk rammeverk for koordinering ved systemiske cyberhendelser (EU-SCICF),[16] jf. bestemmelsen om tverrsektorielt samarbeid i forordningen om digital operasjonell motstandsdyktighet i finanssektoren (DORA), se kapittel 9. Formålet er å sikre rask kommunikasjon og koordinering mellom tilsynsmyndigheter og andre relevante myndigheter for å unngå svikt dersom en alvorlig hendelse oppstår. I påvente av opprettelsen av EU-SCICF har ESCG etablert et forum for utveksling av informasjon om cyberhendelser.

Veikart for cybersikkerhet i finansnæringen

For å møte en økende og mer kompleks cybertrussel samt bidra til å sette foretakene bedre i stand til å etterleve et stadig mer komplekst og detaljert regelverk på IKT-området, har finansnæringen ved Finans Norge igangsatt et arbeid for å etablere et veikart for cybersikkerhet for finansnæringen. Hensikten er blant annet å utvikle en helhetlig tilnærming, hvor næringen kan samles om en felles strategisk retning og legge til rette for etablering av arena(er) for strategiske diskusjoner om cybersikkerhet innad i næringen og/eller med andre sektorer (eksempelvis etter modellen til DSOP[5]).

[14] European Systemic Risk Board (ESRB) 27. januar 2022: ESRB recommends establishing a systemic cyber incident coordination framework
[15] European Systemic Cyber Group (ESCG)
[16] Pan-European systemic cyber incident coordination framework (EU-SCICF)

4. FINANSTILSYNETS OBSERVASJONER OG VURDERINGER

4.1 TILSYN MED IKT OG BETALINGSTJENESTER

Informasjon fra gjennomførte tilsyn

Det ble i 2022 gjennomført 22 tilsyn der IKT og betalingstjenester var tema. Av de 22 tilsynene var ni i banker, to i betalingsforetak, to i forsikringsforetak, ett i infrastrukturforetak, tre i verdipapirforetak, ett i fondsforvaltningsforetak, ett i inkassoforetak, ett i eiendomsmeglingsforetak og to i revisjonsselskap. Tre av tilsynene i bank inngikk i tematilsyn om antihvitvasking, hvor bankens systemer for elektronisk overvåking av mistenkelige transaksjoner var hovedtema for tilsynet. Noen av funnene fra tilsyn i 2022 er sammenfallende med funn fra tilsyn i 2021.

Nærmere omtale av utførte tilsyn med IKT og betalingstjenester finnes på Finanstilsynets nettsted.[17]

Utkontraktering

Flere mangler knyttet til utkontraktering av IKT-virksomhet ble påpekt under tilsyn i 2022. Finanstilsynet fant blant annet ved flere tilsyn at foretak ikke har etterlevd kravet i meldepliktforskriften om å ha en oversikt over alle sine avtaler om utkontraktering.
Finanstilsynet fant også mangler i etterlevelsen av IKT-forskriften § 2, fjerde ledd, som sier at avtaler om utkontraktering av IKT-virksomhet og endringer i slike avtaler skal behandles av foretakets styre.
Tilsyn i 2022 viste også at det fortsatt er avtaler om utkontraktering som ikke oppfyller kravene i IKT-forskriften § 12 om at avtalen må sikre at foretak under tilsyn gis rett til å kontrollere, herunder revidere, leverandørens aktiviteter som er knyttet til avtalen, og sikre at Finanstilsynet gis tilgang til opplysninger fra og tilsyn hos IKT-leverandøren der Finanstilsynet finner det nødvendig som et ledd i tilsynet med foretaket.

Mangelfull oppfølging av leverandører

Finanstilsynet fant ved tilsyn i 2022 mangler i foretakenes oppfølging av utkontrakterte IKT-tjenester, spesielt i oppfølgingen av leverandørenes etterlevelse av foretakenes krav til sikkerhet. Videre ble en avdekket hendelse i 2021, der ansatte hos en leverandør misbrukte sine tilgangsrettigheter til å gjøre ikke-tjenstlige oppslag i kundedata, fulgt opp (se punkt 4.2). Finanstilsynet fant mangelfulle rutiner knyttet til tilgangsstyring og logging hos leverandøren, noe som gjør det vanskelig å avdekke misbruk av tilganger til ikke-tjenstlige oppslag. Finanstilsynet understreket i tilsynsrapportene foretakenes ansvar for styring og kontroll med tilgangsrettigheter, også ved utkontraktering.

Finanstilsynet understreket også den enkelte banks ansvar for oppfølging av kjøp og bruk av fellestjenester fra en leverandør. Videre påpekte Finanstilsynet at IKT-forskriftens bestemmelser gjelder uavhengig av om utkontrakteringen er konsernintern eller ekstern.

Manglende involvering i leverandørens test av kriseløsninger

Finanstilsynet påpekte i flere tilsyn at det manglet involvering fra foretakene i planleggingen av tester av kriseløsninger hos leverandør. Uten foretakenes involvering kan det ikke sikres at det foretaket har kategorisert som forretningskritiske prosesser og systemer, inngår i testene hos leverandøren.

[17] Finanstilsynet: Tilsynsrapporter for IT og betalingstjenester

Manglende IKT-kompetanse og IKT-kyndige ressurser i andre forsvarslinje

Finanstilsynet fant ved flere tilsyn i 2022 grunn til å påpeke betydningen av at foretaket har tilstrekkelig IKT-kompetanse og IKT-kyndige ressurser i uavhengige kontrollfunksjoner i andrelinjen. Andre forsvarslinje skal gjøre selvstendige og uavhengige vurderinger i tillegg til å gjennomføre kontroller av IKT-området.

Tre forsvarslinjer

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

Andre forsvarslinje (risikostyring og etterlevelse (compliance)): Andre forsvarslinje består av risikostyrings- og etterlevelsesfunksjoner som overvåker og følger opp den operative ledelsens styring og kontroll. Risikostyringsfunksjonens oppgave er å legge til rette for implementering av rammeverket for foretakets risikostyring. Videre skal risikostyringsfunksjonen assistere førstelinjen i implementering av risikostyringen og sikre at prosesser og kontroller som er etablert i førstelinjen, er effektive og riktig utformet. Videre er oppgaven å identifisere, overvåke, analysere og rapportere risikoer basert på førstelinjens risikorapportering og ut fra det gi et helhetlig bilde av foretakets risikosituasjon. Etterlevelsesfunksjonens oppgave er å overvåke etterlevelsen av juridiske og regulatoriske krav, og foretakets interne krav. Funksjonen skal være rådgivende overfor ledelsen og andre interessenter når det gjelder etterlevelse av nevnte krav og skal etablere retningslinjer og prosesser for å håndtere etterlevelsesrisiko og sikre etterlevelse. Andre forsvarslinje kan også bestå av andre ikke-operative funksjoner, for eksempel innen informasjonssikkerhet.

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

Manglende eller mangelfulle forretningsmessige konsekvensanalyser

Tilsyn i 2022 avdekket at forretningsmessige konsekvensanalyser (Business Impact Analysis, BIA) fortsatt mangler eller er mangelfulle i mange foretak. Den forretningsmessige konsekvensanalysen er et viktig grunnlag for foretakets arbeid med beredskaps- og kriseplaner, herunder for utkontrakterte tjenester.

Datakvalitet

Ved flere tilsyn viste Finanstilsynet til at et rammeverk for styring og kontroll med data kan være nødvendig for å sikre datakvaliteten. Ikke minst gjelder dette for større foretak/konsern med tverrgående forretningsprosesser og komplekse verdikjeder. Styring og kontroll med data skal sikre konsistente og pålitelige data og hindre misbruk, og er en forutsetning for automatisering og effektivisering av forretningsprosessene. Finanstilsynet fant også manglende klassifisering av informasjon og manglende vurdering av risiko for tap av data. Klassifisering av informasjon og vurdering av konsekvenser ved tap av data utgjør grunnlaget for å fastsette tilgangs- og beskyttelseskrav for data og bør inngå i den forretningsmessige konsekvensanalysen.

Tilsyn med overvåkingssystemer

I tilsyn med bankenes systemer for overvåking av mistenkelige transaksjoner knyttet til hvitvasking og terrorfinansiering (AML) fant Finanstilsynet at det i transaksjonsovervåkingen ikke ble kontrollert mot innhentet informasjon om kunden (KYC-data[18]) og heller ikke mot bransje eller produkter. I mange tilfeller var det få regler[19] rettet mot kunder med høy risiko, få kundespesifikke regler og få regler rettet mot terrorfinansiering. Finanstilsynet påpekte ved flere tilsyn at manglende referanser til reglene i AML-risikoanalysen gjør det umulig å vurdere i hvilken grad transaksjonsovervåkingen er dekkende for foretakets risiko for hvitvasking og terrorfinansiering. Tilsyn viste videre til at foretak som hadde gjort større endringer i regelsettet med basis i grundige risikoanalyser opplevde signifikante forbedringer i form av bedre treffsikkerhet og flere reelle alarmer.

Tilsyn med betalingsforetak

Finanstilsynet pekte på manglende rutiner for håndtering av sikkerhetsrelaterte kundeklager i henhold til pliktene som følger av finansforetaksforskriftens § 3-2 bokstav a. Finanstilsynet pekte også på at det manglet kontaktinformasjon til brukerne (kundene), slik at foretaket vanskelig kunne oppfylle krav i forskrift om systemer for betalingstjenester om at brukerne skal underrettes ved hendelser som kan påvirke deres økonomiske interesser. Det ble også pekt på at brukerne hadde begrenset mulighet til å nå foretaket på en effektiv måte ved behov for å instruere foretaket til å stoppe tilgangen til bestemte kontoer eller endre utvalget av kontoer foretaket skal ha tilgang til.

For å ivareta sikker kommunikasjon i hele betalingstjenesteløpet og hindre at det videresendes kontoforespørsler som er i strid med reglene i den regulatoriske tekniske standarden[20] til PSD2, viste Finanstilsynet til at kommunikasjonen mellom foretaket og foretakets kunder bør være sikret ved hjelp av eIDAS-sertifikater[21] eller tilsvarende.

4.2 LEVERANDØROPPFØLGING AV TILGANGSSTYRING

Finanstilsynet fulgte i 2022 opp en sikkerhetshendelse i 2021, der ansatte hos en leverandør hadde misbrukt tilganger til ikke-tjenstlige oppslag. Oppfølgingen omfattet alle foretak som benytter leverandøren. I tillegg ble det, som omtalt under punkt 4.1, gjennomført tilsyn med enkelte foretak. I oppfølgingen har Finanstilsynet lagt vekt på foretakenes rutiner for å følge opp IKT-tjenesteleverandører når det gjelder administrasjon, oppfølging og kontroll av tilgangsrettigheter, herunder hvilke internkontrollaktiviteter og eventuelle revisjoner som har vært gjennomført på foretakets bestilling, jf. IKT-forskriften §§ 12 og 5.

Sikkerhetshendelsen i 2021, samt oppfølging av foretakenes tilgangsstyring, viser at det er behov for bedre rutiner for å avdekke misbruk av tilganger til ikke-tjenstlige oppslag.

Videre ser Finanstilsynet at foretakenes styring og kontroll med tilgangsrettigheter ved utkontrakterte løsninger har mangler. Det forventes at foretaket, sammen med IKT-tjenesteleverandør, iverksetter tiltak for å sikre at denne er tilstrekkelig, og at foretaket etablerer løsninger og kontrollrutiner for tilgangsstyring som sikrer at tilganger i størst mulig grad tildeles for det enkelte oppdrag utfra tjenstlige behov.

[18] Know Your Custumer (KYC)
[19] Elektroniske transaksjons- og/eller kundekontroller kan betegnes som regler, filtre, kontroller, risikoparametre eller scenarier. Betegnelsen 'regler' er brukt her.
[20] Regulatory Technical Standard (RTS)
[21] eIDAS (electronic IDentification, Authentication and trust Services)-sertifikater er virksomhetssertifikater kvalifisert for bruk i hele Europa i henhold til eIDAS-forordningen. PSD2 stiller krav om at det skal benyttes kvalifiserte sertifikater for elektroniske segl (eIDAS-sertifikat) i kommunikasjonen mellom betalingstjenestetilbyder og kontotilbydere, jf. artikkel 34 i delegert kommisjonsforordning (EU) 2018/389 (RTS).

4.3 FORETAKENES VURDERING AV VIKTIGE FORHOLD KNYTTET TIL IKT-VIRKSOMHETEN

Foretak og leverandører av IKT-tjenester har i samtaler med Finanstilsynet pekt på flere viktige forhold knyttet til IKT-virksomheten.

Styrets ansvar for IKT-virksomheten

Styret har ansvar for å sikre at IKT-virksomheten er i samsvar med lover og regler, og med bedriftens etiske retningslinjer. Det gjelder også utkontraktert IKT-virksomhet, hvor styret må påse at avtaler og kontrakter er i tråd med bedriftens informasjonssikkerhetspolicy og sikrer at lover og forskrifter blir fulgt. Det er også viktig at styret har oversikt over hvilke IKT-tjenester som er utkontraktert, og at det er rutiner på plass for å sikre at utkontraktert IKT-virksomhet håndteres på en sikker og forsvarlig måte.

Styringsmodell og internkontroll

Finanstilsynet er gjennom dialog med foretakene blitt gjort kjent med at manglende oversikt over hvilke kontroller som inngår i foretakets internkontroll, og hvordan kontrollene skal utføres, overvåkes og revideres, kan føre til at operasjonell risiko ikke avdekkes. Det kan videre medføre at nødvendige risikoreduserende tiltak i tråd med foretakets risikotoleranse, ikke iverksettes.

Som året før, trekker foretakene fram at foretakenes størrelse har betydning for evnen til å etablere en organisasjon med en klar deling av første- og andrelinjens internkontrolloppgaver.

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 framtidens kompetansebehov. Dette gjelder innenfor både moden teknologi og ny teknologi, særlig innenfor skyteknologi. Det kan føre til at problemer og feil som oppstår kan være utfordrende å løse og at avhengigheten av tilgang til utenlandsk kompetanse kan øke.

Leverandørstyring

Det er en stadig større utfordring å håndtere komplekse leverandørkjeder. Med flere leverandører og underleverandører i verdikjeden blir samhandlingsmodellene, på både strategisk, taktisk og operasjonelt nivå, mer komplekse og omfattende. Mangler på dette området kan føre til svakere oppfølging og kontroll med kritiske utkontrakterte IKT-tjenester.

Det er helt vesentlig med god leverandøroppfølging innenfor klart definerte rammer med tydelig beskrivelse av hvilken informasjon foretaket ønsker fra leverandør.

Digital kriminalitet

I dialogen med foretakene ble det pekt på at manglende sikkerhetstester, sikkerhetsoppdateringer, opplæring og bevisstgjøring av ansatte, samt mangelfull overvåking av aktiviteter i egen teknisk infrastruktur, herunder nettverk og systemer, kan føre til at kriminelle påfører foretaket skade gjennom digitale angrep. Svindel mot bankkunder er den nye typen bankran, og foretakene anser dette som et samfunnsproblem.

Informasjonslekkasje

Manglende klassifisering av informasjon og kontroller for overvåking av informasjon som sendes ut på e-post, kopieres til eksterne lagringsenheter eller til private skytjenester, kan medføre at uvedkommende får tilgang til informasjonen og påføre foretaket eller deres kunder skade.

Klassifisering

Det er viktig at foretakene har klassifisert sine dokumenter med hensyn til blant annet konfidensialitet og kritikalitet, slik at de kan etablere løsninger som bidrar til å forhindre uautorisert uthenting eller deling av data.

IKT-drift

Sikker og stabil IKT-drift har høy prioritet hos alle foretak. Sikker og stabil drift utfordres imidlertid ved stadig økende kompleksitet som følge av integrasjon mellom systemer fra ulike leverandører, integrasjon mellom nye og gamle systemer, økt funksjonalitet i selvbetjente kanaler, økt bruk av skytjenester, manglende oppfølging av teknisk gjeld og mangelfull overvåking av IT-miljøet.

Beredskap og krisehåndtering

I kontakten med foretakene kom det fram at manglende analyser av konsekvenser ved en krise, mangelfull opplæring og øvelse i krisehåndtering, mangler i test av kriseløsninger og mangelfulle kriseløsninger kan gi foretak utfordringer med å opprettholde kritiske IKT-tjenester ved alvorlige brudd på normalt driftssted. Oppfølging av beredskapsløsninger er utfordrende, særlig der foretakene skal lage og kommunisere rammene for testing av beredskapsløsninger til tjenesteleverandør.

Beredskap – beredskapstester basert på scenarioer og forretningsmessige konsekvensanalyser

En forretningsmessig konsekvensanalyse (BIA*) skal kartlegge effekten en hendelse vil ha på et foretaks forretningsprosesser og -tjenester. Analysen tar utgangspunkt i prosesser og tjenester som er kritiske for foretakets virksomhet. Vurderingen omfatter også en kartlegging og klassifisering av aktiviteter og ressurser som er nødvendige for å levere de kritiske prosessene og tjenestene. Den forretningsmessige konsekvensanalysen legger videre grunnlaget for foretakenes beredskaps- og kriseplaner. Foretak må sikre at tester og øvelser tar utgangspunkt i foretakenes forretningsmessige konsekvensanalyser for å sikre at kritiske forretningsprosesser og -tjenester kan ivaretas ved en hendelse, inkludert utkontraktert virksomhet. Finanstilsynet understreker også viktigheten av at foretak i planleggingen av sine øvelser og testaktiviteter tar med scenarioer som også inkluderer tilsiktede cyberangrep. Foretakenes beredskapsarbeid bør ta utgangspunkt i forretningskritiske tjenester, sårbarheter og trusselbildet, også der hvor IKT-virksomheten er utkontraktert.

*Business Impact Analysis

Geopolitiske forhold

I kontakten med foretakene kom det fram at landrisiko og andre geopolitiske forhold vurderes likt som foregående år, og at det i liten grad har vært endringer i disse forholdene som innebærer økt sikkerhetstrussel mot den norske finansnæringen.

Endringsstyring

Høy utviklingstakt kan medføre press for å få satt en løsning i produksjon som kan gå på bekostning av kvalitet. Dette kan føre til funksjonelle feil og at sikkerhetshull ikke avdekkes. Manglende kontroll av endringer i driftsoppsettet kan føre til brudd i kritiske forretningsprosesser og til at foretaket eksponeres for digital kriminalitet. Foretakene er klar over at "Continuous deployment" er en endringshåndteringsstrategi

som har utfordringer, men at bruk av DevSecOps-prosessen [22] kan bidra til at denne strategien ikke skaper nye risikoer for foretaket.

Tilgangsstyring

Manglende kontroll med og overvåking av utvidede tilgangsrettigheter for ansatte og personell hos leverandører kan skade foretaket som følge av bevisste eller ubevisste operasjonelle feil. Dette kan også føre til informasjonslekkasje. Foretakene vurderer det som viktig at det tilbys systemstøtte for å følge opp tilganger ved at leverandørers tilgangsstyringssystemer blir satt opp med integrasjon mot foretakenes tilgangsstyringssystem for å gi foretakene bedre kontroll med leverandørens tilganger.

Datakvalitet

Mangler eller feil i data kan føre til at analyser, kontroller og beslutninger utføres på feil eller for svakt grunnlag. Dette kan blant annet omfatte feil i kredittvurderinger, feil i kontroller for å avdekke hvitvasking eller svindel og feil i risikovurderinger. Styring og kontroll av data er et område der foretakene i stadig større grad gjennomfører aktiviteter for å styrke arbeidet med oppfølging av datakvaliteten. Finanstilsynet har i dialogen med foretakene pekt på at det er viktig at foretakenes leverandører forstår betydningen av god datakvalitet.

4.4 OPPSUMMERING AV FORETAKENES RAPPORTERING AV RISIKO OG SÅRBARHET

Finanstilsynet har innhentet betalingstjenestetilbyderes og andre foretaks vurderinger av risiko og sårbarhet knyttet til IKT-virksomheten, jf. forskrift om systemer for betalingstjenester § 2, tredje ledd sammenholdt med IKT-forskriften § 3. 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 også i 2022. Mer enn tre av fire foretak rapporterer at de mener IKT-systemene gir et godt grunnlag for styring av og kontroll med virksomheten, at de har en godt innarbeidet prosess for risikoanalyse og at de har dokumenterte mål og prosedyrer for IKT-sikkerhet godkjent av ledelsen. De aller fleste rapporterer at de etterlever prinsippet om de tre forsvarslinjene. Imidlertid rapporterer flere at risikoen er moderat eller høy når det gjelder oversikt over hvilke kontroller foretaket bygger på innenfor de tre forsvarslinjene, brutt ned på kontroller som bidrar til å sikre hhv. integritet, konfidensialitet og tilgjengelighet. Det framgår av foretakenes kommentarer at de i varierende grad har fullstendig og enhetlig dokumentasjon av kontroller innen de enkelte ansvarsområdene og forsvarslinjene.

Om lag tre av fire foretak rapporterer lav risiko knyttet til løpende oppfølging av leverandører og leveranser med hensyn til leveransekvalitet. Selv om flertallet av foretakene også rapporterer at det er lav risiko når det gjelder bestillerkompetanse, framgår det av rapportene at flere foretak vurderer denne risikoen som én av de største risikoene. Enkelte foretak framhever også avhengighet av ekstern IKT-kompetanse.

Ett av tre foretak mener det er middels eller høy risiko forbundet med manglende eller mangelfulle retningslinjer knyttet til IKT-sikkerhet, herunder risikovurderinger av betalingstjenestevirksomheten, kontroller med sikkerhet og tiltak for å beskytte brukere mot identifiserte risikoer. Risikoen vurderes å være økende. Et solid flertall av foretakene mener det er lav risiko knyttet til tilstrekkelig bevisstgjøring og opplæring av medarbeidere.

[22] DevSecOps står for development, security, and operations. Det er en tilnærming til kultur, automatisering og plattformdesign, som påser at sikkerhet er et delt ansvar igjennom hele IKT-livssyklusen.

- *Finanstilsynet merker seg at foretakene generelt rapporterer om lav risiko knyttet til styring med og kontroll av IKT-virksomheten. Finanstilsynets erfaring fra tilsynsvirksomheten gir et noe mer variert bilde av foretakenes risiko på området. Tilsyn har avdekket at spesielt mindre og mellomstore foretaks styring med og kontroll av IKT-virksomheten har mangler, noe som gir sårbarheter og øker risikoen for hendelser.*

Beskyttelse av data

Et betydelig flertall av foretakene rapporterer om lav risiko for at det gjøres uautoriserte endringer, og for at tjenestene ikke lenger fungerer som de skal. Når nye løsninger utvikles, rapporterer foretakene at de tar i betraktning behovene til alle forretningsområdene. Foretakene rapporterer om lav risiko knyttet til sikring av data under både transport og lagring.

Foretakene samler inn informasjon om drift, transaksjoner og svindel, og benytter informasjonen til å gjøre tjenestene sikrere. Omfanget og konsekvensene av feil i applikasjoner og data som påvirker dataenes integritet var lavere i 2022 enn i 2021.

Endringshåndtering

Foretakenes vurdering av risiko forbundet med endringshåndtering er samlet sett stabil. Risikoen forbundet med at testsystemer ikke er produksjonslike, er synkende. Over halvparten av foretakene vurderer imidlertid risikoen som moderat eller høy. Høy grad av kompleksitet i IKT-systemene er forbundet med høy eller moderat risiko hos omtrent fire av fem foretak. I forbindelse med kompleksitet i IKT-systemene, viser foretakene til verdikjeder som én av årsakene til høy risiko. Endres et system tilknyttet en tjeneste, vil dette også kunne påvirke systemer for andre tjenester. Dette er også en problemstilling ved endringshåndtering, hvor flest foretak har vurdert risikoen som høy, men stabil.

Flere foretak har vurdert nye regulatoriske krav som én av de høyeste risikoene. Risikoen forbundet med at foretakene stadig må endre systemer som følge av nye regulatoriske krav, er økende. Det vises i den forbindelse i hovedsak til den nye finansavtaleloven, PSD2 og DORA (se kapittel 9). Av foretakenes kommentarer framgår det at endringstakten er høy og økende. Videre vises det til at endringene kan være utfordrende for mindre foretak. Mens noen foretak har vist til at endringene varsles tidlig, noe som medfører at endringene kan gjøres planlagt og kontrollert, viser andre til at implementeringstiden er kort. Det vises ellers til at det settes av betydelige ressurser for å håndtere nye krav.

For øvrig fokuserer foretakene på gode rutiner, kompetanse, ressurser og reduksjon av nøkkelpersonrisiko.

Drift

Risikoen knyttet til drift er jevnt over stabil. Omtrent halvparten av foretakene rapporterer at denne risikoen er moderat eller høy. Foretakenes vurdering av risiko som følge av teknisk gjeld har avtatt, selv om et flertall av foretakene fortsatt vurderer risikoen som moderat eller høy. Risikoen for at grensesnittene tredjeparter benytter seg av, ikke er sikret i tråd med sikkerhetskravene i delegert kommisjonsforordning (EU) 2018/389[23] rapporteres å være lav, men trenden er økende.

Godt over halvparten av foretakene vurderer risikoen knyttet til å ha en oppdatert oversikt over IKT-utkontraktering, med tilknyttet risiko, som moderat eller høy. Foretakene viser til at de holder oversikt og følger opp avtaler, og at det gjennomføres kontroller. I noen tilfeller vises det til at oppfølgingen må forbedres.

[23] Delegert kommisjonsforordning (EU) 2018/389

Bytte av bankenes kjerneløsninger trekkes fram som et tiltak for å få bedre oversikt over hvilke forretnings-prosesser som påvirkes ved stopp eller avvik i driften. Det pekes også på at det i noen tilfeller utføres testing av PSD2-grensesnitt av tjenesteleverandør.

Sikkerhet

Et flertall av foretakene vurderer IKT-sikkerhet som den høyeste risikoen. Nivået rapporteres generelt å være stabilt. Spesielt trekkes de økte geopolitiske spenningene fram som grunnlag for økt risiko for cyberangrep. Foretakene viser til verdikjeder som en del av risikoen for å ivareta IKT-sikkerheten. Knappheten på IKT-ressurser trekkes også fram av flere som en av de høyeste risikoene. Når det gjelder tilgang til IKT-sikkerhetskompetanse, herunder å være kravstiller i forbindelse med utkontrakteringer, anser omtrent to av tre foretak risikoen som høy eller moderat, og trenden er økende.

- *Manglende tilgang på IKT-ressurser i kombinasjon med økt fare for angrep representerer etter Finanstilsynets vurdering en vesentlig risiko.*

Litt under halvparten av foretakene vurderer risikoen som moderat eller høy for at tiltak for å beskytte seg mot angrep ikke er tilstrekkelig høy. Foretakene viser i stor grad til tiltak som anskaffelse av sikkerhetsprodukter, innføring av eksempelvis antivirusverktøy, brannmur på hjemme-PC og bruk av sandkasse til analyse av filer.

Foretakene benytter seg jevnlig av sikkerhetstesting, herunder penetrasjonstesting. Litt under halvparten av foretakene vurderer risikoen forbundet med testing som moderat eller høy. Noen foretak viser også til at det er iverksatt ukentlige sårbarhetsskanninger. Flere av foretakene oppgir i tillegg bruk av eksterne leverandører i forbindelse med sikkerhetstestingen.

Beskyttelse av data

Et betydelig flertall 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. Risikoen relatert til tildeling og vedlikehold av rettigheter som ansatte, leverandører, konsulenter og applikasjoner i systemene vurderes også å være lav. En større andel av foretakene vurderer imidlertid risikoen knyttet til logging av tilganger til data og systemer som moderat eller høy. Mens flere foretak rapporterer om tilgang til loggverktøy og -analyser, er det mange foretak som rapporterer at logging av tilganger og alarmer følges opp av eksterne leverandører eller andre foretak i allianser. Enkelte foretak rapporterer at logging av og varsling om mistenkelig adferd er et prioritert område i 2023.

ID-tyveri

Sammenlignet med 2021 anser foretakene risikoen forbundet med ID-tyveri som noe høyere. Spesielt vurderer flere foretak at det er en stigende risiko forbundet med at tiltak for å forhindre en angriper i å overta en kundes ID og misbruke denne, ikke er tilstrekkelige. Videre er det i motsetning til i 2021 nå foretak som vurderer risikoen for ikke å ha gode tiltak for å forhindre at en angriper tar over en bruker-ID og misbruker denne, som høy. Risikoen samlet sett er imidlertid stabil, og uendret. Risikoen for ID-tyveri blir av flere foretak vist til som en av de høyeste risikoene. Foretakene peker på det er en økende trend i forsøk på ID-tyverier, og konsekvensene av tyveriene for dem som blir rammet, herunder både foretak og kunde. Se egen omtale om skjerpede krav til foretakene.

For øvrig har foretakene fokus på kontroller, oppfølging av svindelsaker, informasjon til kunder og bruk av sterk kundeautentisering.

Skjerpede krav til foretakene

Høyesterett slo fast i dom av 13. september 2022* at banken var ansvarlig for tap etter at en kunde ble forledet til å oppgi kode og passord for BankID per telefon og det deretter ble tatt ut penger av kundens bankkonto. Etter avtalen med banken hadde kunden plikt til å ikke oppgi kode og passord. Dette gjaldt også overfor banken. Høyesterett kom imidlertid til at dersom kunden skulle være ansvarlig for tapet, jf. finansavtaleloven (1999) § 35**, måtte kunden være klar over pliktbruddet, noe kunden ikke var i dette tilfellet.

Høyesterettsdommen skjerper ansvaret for bankene, som ser ut til å ha medført et økt fokus på området fra foretakenes side. Dette kan forklare hvorfor foretakene anser risikoen som høyere enn tidligere. Ny finansavtalelov trådte i kraft 1. januar 2022, og tilsvarende bestemmelser er videreført i den nye loven.

* Høyesterettsdom HR-2022-1752-A
**Tidligere finansavtalelov

Interne misligheter

Omtrent halvparten av foretakene anslår risikoen som moderat når det gjelder kontrollen med interne misligheter og mislighetsscenarioer. Tilbakemeldingene indikerer at foretakene hadde fokus på dette trusselområdet også i 2022. Risikoen knyttet til at logging og varsling ikke er tilstrekkelig vurderes også å være moderat av halvparten av foretakene, selv om andelen som vurderer risikoen til å være høy er noe større.

Hvitvasking og terrorfinansiering

Hvitvasking og terrorfinansiering er generelt et område hvor foretakene viser til moderat eller høy risiko. Et klart mindretall av foretakene vurderer risikoene som lav, og flere foretak vurderer risikoen for hvitvasking og terrorfinansiering som en av de største risikoene.

Et betydelig flertall av foretakene vurderer at det er moderat risiko knyttet til at IKT-systemer ikke gir et samlet bilde av kunden, kunderelasjoner og kundeadferd. Tilbakemeldingene indikerer at foretakene hadde oppmerksomhet rettet mot kjenn-din-kunde-relaterte oppgaver (KYC) i 2022, og flere rapporterer at foretakene har fått, eller er i ferd med å få, forbedrede IKT-løsninger for relevant kundeinformasjon.

Flere foretak anser fortsatt 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 moderat eller høy risiko for at systemene for transaksjonsovervåking ikke fanger opp alle betalingstransaksjoner som bør undersøkes nærmere. Foretakene viser til at de har stor oppmerksomhet på dette området, at systemene videreutvikles og forbedres, og at eksterne systemer kjøpes inn. Det rapporteres at det vil være løpende arbeid og utvikling på området også framover.

Et betydelig 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 og videreutviklet maskinlæring og scenarioer som benytter kundenes tidligere adferd sammenholdt med statistiske data for å gjenkjenne mistenkelige mønstre.

Risikoen for at sanksjonsscreeningsystemet har høy presisjon i treff av listeførte personer og foretak vurderes å være moderat eller høy av et betydelig flertall av foretakene. Flere foretak framhever den usikre geopolitiske situasjonen og at det har vært en utfordring å holde AML-systemene oppdatert i forhold til

sanksjonsregler og endringer i navnelister. Foretakene rapporterer at IKT-systemer for sanksjonsscreening har blitt forbedret og gitt økt treffsikkerhet, blant annet som følge av Finanstilsynets tematilsyn i 2022.

Andre observasjoner

Finanstilsynet har merket seg at svarene til mange foretak i allianser er svært like. Risikoer og sårbarheter som trekkes fram kan være høyst relevante for mange foretak med tilnærmet lik forretningsmodell og størrelse og begrenset kompleksitet. Imidlertid plikter ethvert foretak å gjøre en selvstendig vurdering av foretakets risiko og sårbarhet. Dokumentasjonen av foretakets egen vurdering mangler i flere av rapportene.

Også enkelte datterselskap av finansforetak har ikke dokumentert at de har utført en vurdering av egen risiko og sårbarhet, men henviser kun til morselskapets rapport.

Finanstilsynet minner om at foretak underlagt IKT-forskriften eller tilsvarende regelverk plikter å gjennomføre risikoanalyser for å påse at risiko styres innenfor akseptable grenser i forhold til foretakets egen virksomhet, jf. kravene i IKT-forskriften § 3.

4.5 STYRKET FORBRUKERVERN I NY FINANSAVTALELOV

Ny finansavtalelov[24] trådte i kraft 1. januar 2022. Loven styrker forbrukervernet og gjør i større grad bankene erstatningsansvarlige ved misbruk av BankID.

Etter lovens § 2-7, første ledd har forbrukere rett til kortreklamasjon dersom de svindles etter å ha betalt med et kredittkort. Loven er også gjeldende for defekte varer, feil beløp eller bestillinger som aldri dukker opp. Bruk av debetkort er ikke lovregulert på samme måte, men avtalevilkårene til Visa og Mastercard debetkort kan ha bestemmelser om reklamasjon og erstatning.

Etter finansaataleloven skal bankene sikre forbrukere tilgang til en klar, hurtig og sikker prosedyre for bytte av betalingskonto som er enkel for forbrukerne å benytte, jf. § 4-34 og omtalen om bankbytte i punkt 2.3. Prosessen for flytting av faste betalingsavtaler og bankenes plikter i denne forbindelse er regulert i §§ 4-37 og 4-38. Dette omfatter blant annet flytting av faste betalingsoppdrag og direktebelastningsfullmakter som AvtaleGiro.

4.6 MISBRUK AV INNLOGGINGSINFORMASJON

Finanstilsynet observerer i økende grad aktivitet der kriminelle forsøker å få tilgang til brukernes innloggingsdetaljer (engangskode, passord, e.l.), såkalt phishing. Innloggingsdetaljene benyttes for å logge seg inn, og den kriminelle har da tilegnet seg offerets rettigheter på det innloggede stedet, og misbruker disse til egen vinning. Så godt som alle brukere opplevde trolig forsøk på phishing i 2022, og svært mange opplevde å bli utsatt for forsøk flere ganger. Flere av ofrene ble frastjålet penger, se punkt 5 om svindel og svindelstatistikk.

Misbruk av ansattes innloggingsinformasjon

Finanstilsynet er kjent med at også ansatte i finansnæringen er blitt frastjålet innloggingsdetaljer, der angriperen har tilegnet seg alle rettighetene til den ansatte og benyttet disse til å sende e-post med falske

[24] Lov om finansavtaler

betalingsoppfordringer i den ansattes navn. Finanstilsynet er ikke kjent med tilfeller der angripere har lykkes i å tilegne seg midler.

Ved slike angrep får angriperen et elektronisk adgangsbevis, såkalt sesjonsobjekt, etter en vellykket innlogging. Adgangsbeviset har en levetid som er satt av nettstedet som utsteder beviset. Levetiden er ofte så lang at angriperen har god tid til å gjennomføre svindelforsøk, for eksempel med falske e-poster.

Forbindelsen mellom brukeren og nettstedet er oftest kryptert og dermed beskyttet mot denne formen for ID-tyveri. Brukeren kan kontrollere nettstedets navn og at forbindelsen er kryptert før innloggingsdetaljer oppgis. I tillegg til at mange nok er lite kjent med disse kontrollmulighetene, er det antakelig heller ikke særlig mange brukere som foretar slike kontroller. Fordi brukerne i liten grad er opplært til å sjekke hva som står i sertifikatet, vil brukerne ikke oppdage at angriperen har etablert en kryptert forbindelse til sitt nettsted.

Det er mulig for foretaket å angi hvilke arbeidsstasjoner som skal ha tilgang. Da vil det være vanskeligere foren angriper å gjennomføre phishing-forsøk. Men arbeidsstasjonens IP-adresse kan forfalskes og er derfor ikke en sikker identifikasjon av arbeidsstasjonen. Ved bruk av arbeidsstasjonens fysiske adresse, den såkalte MAC-adressen, kan gi bedre sikerhet.[25]

Finanstilsynet er kjent med at leverandører av skytjenester tilbyr tilleggstjenester som gir beskyttelse mot angrep. Tjenestene tilbys som egne tjenester utover basistjenesten. Finanstilsynet har grunn til å tro at ikke alle brukere av skytjenester er bevisst konsekvensene av å avstå fra å benytte slike tilleggstjenester.

Tyveri og misbruk av innloggingsinformasjon for finansielle tjenester

I tillegg til å være den sentrale ID-en innen finansiell sektor benyttes BankID en rekke andre steder, både i privat og offentlig sektor. BankID-innloggingen ser forskjellig ut for brukeren fra ett nettsted til et annet. Brukeren har ofte ikke grunnlag for å avgjøre om nettstedet har rett til å be brukeren om BankID-innlogging og til å be brukeren oppgi innloggingsdetaljer i denne forbindelse. Dette setter brukeren i en vanskelig situasjon i og med at brukere i kontrakten med banken har forpliktet seg til å holde innloggingsdetaljene hemmelig. Det er en risiko for at en angriper står bak og benytter seg av phishing for å tilrane seg brukerens innloggingsdetaljer.

Ved innlogging til finansielle tjenester som benyttes ofte, slik som nettbanker, benytter foretakene seg av kontroller som kommer i tillegg til BankID for autentisering av brukeren. Slike kontroller kan være brukerens inntastingsbiometri, kontroll av at brukerens arbeidsstasjon (mobil, PC, nettbrett) er oppdatert med siste versjon av operativsystem og sikkerhetsoppdatering, at brukerens geolokasjon er som forventet og at transaksjonen stemmer overens med brukerens vanlige adferd ("NN pleier da ikke overføre større beløp til utlandet klokken to om natten"). Der BankID sjelden benyttes for innlogging, for eksempel Altinn, Helse-Norge og grunnboken, kan det være mer utfordrende å utføre tilleggskontroller basert på adferd. Disse nettstedene kan dermed være mer sårbare enn tjenester fra en BankID-utsteder når en stjålet ID benyttes.

At BankID benyttes i stort omfang til både private og offentlige tjenester utenom finanssektoren, og med variasjoner i innloggingskonteksten, medfører en fare for at brukerne ikke er tilstrekkelig årvåkne og kan bli lurt til falske innlogginger og bli fralurt sikkerhetsinformasjon. Det store omfanget av bruksområder gir de kriminelle mulighet for å benytte seg av et bredt omfang av moduser i svindelvirksomheten og kan medvirke til økt svindel.

[25] MAC-adressen er normalt ikke en del av den digitale forsendelsen. Foretaket som er ansvarlig for nettstedet må i tilfelle programmere applikasjonen sin slik at den transporterer MAC-adressen, eventuelt annen informasjon som er egnet til å identifisere arbeidsstasjonen.

Tiltak mot tyveri og misbruk av innloggingsinformasjon

For å redusere omfanget av ID-tyverier mener Finanstilsynet at innsatsen bør intensiveres på en rekke områder, herunder

- vurdere tiltak i forhold til skadepotensialet som tjenesten innebærer
- opplæring av brukere i hvilke kontroller brukeren kan/skal gjøre
- bevisstgjøring av brukere og av teknisk personell på brukerstedene
- vurdere mulige tiltak og tilleggskontroller, som avgrenset levetid på sesjonsobjektene, segmentering, geografisk avgrensing av avsenderadresse, definisjon av hvilke maskiner som kan benyttes, kontroll av sikkerhet på avsenders utstyr (operativsystemnivå, nivå på sikkerhetsoppdatering), kontroll mot brukerens "normale" bruksmønster (beløp, brukerfrekvens) og krav om at flere må godkjenne transaksjoner.

4.7 RISIKO KNYTTET TIL BRUK AV SAMTALEROBOTER

Kunstig intelligente samtaleroboter (chatboter[10]) som OpenAIs ChatGPT er teknologi som er på vei til å bli integrert i vanlige arbeidsverktøy. Store aktører som Google og Microsoft satser tungt på å utvikle og integrere funksjonalitet som baseres på kunstig intelligensi nettlesere og Office-produkter. Samtaleroboter som ChatGPT er avanserte tekstgenereringsmodeller som, i tillegg til å skrive tekster, kan brukes til å svare på spørsmål og utføre oppgaver, samt oversette tekst fra ett språk til et annet. ChatGPT kan også brukes til systemprogrammering siden den er designet for å forstå, feilsøke og foreslå kode.

Bruk av digitale verktøy som ChatGPT kan gi store gevinster for foretak siden de er brukervennlige, tilgjengelige hele døgnet, kan svare på et bredt spekter av spørsmål og er kostnadseffektive. Imidlertid er bruk av samtaleroboter ikke uten utfordringer eller risikoer. Systemet kan samle inn og lagre informasjon som er sensitiv eller personlig, og dette kan utfordre etterlevelsen av personvernregelverket (GDPR).

Samtalerobotene er språkmodeller, ikke kunnskapsmodeller, og det er en risiko for at samtaleroboter gir feilinformasjon eller misforstår brukerens spørsmål. De kan gi feilaktige framstillinger av informasjonen de finner, eller presentere svar som ser plausible ut, men som er ufullstendige, unøyaktige eller upassende.

Samtalerobotene er trent på store datasett. Hvilket svar man får, påvirkes av kildene til datasettene og om informasjonen som benyttes oppdateres kontinuerlig eller har en tidsavgrensning. Hvis datasettene modellen er trent på ikke er diversifiserte og representative, øker risikoen for skjevheter og uønskede resultater. Maskinbaserte modeller som samtaleroboter har videre ingen bevissthet om moralske aspekter eller etikk.

Som annet IKT-verktøy, bør bruk av samtaleroboter være basert på risikovurderinger og skje på en ansvarlig og bevisst måte. Brukere bør være klar over samtalerobotenes begrensninger og risikoene ved bruk.

5. SVINDEL OG SVINDELSTATISTIKK

5.1 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 betalingstjenestedirektivets (PSD2) retningslinjer for svindelrapportering[26].

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 initiere betalingen.

Tabell 5.1 viser en oversikt over tap ved kontooverføringer og kortbetalinger med kort utstedt av norske kortutstedere samt samlede tap per år. Tallene viser at det var en økning i samlede tap på 106 mill. kroner fra 2021 til 2022.

Tabell 5.1 Samlede tap ved svindel

Beløp i mill. kroner	Svindeltransaksjoner – kontooverføringer (nettbank m.m.)	Svindeltransaksjoner med betalingskort rapportert av kortutsteder	Samlede tap
H1 2022	162	98	
H2 2022	233	121	
Totalt 2022	**395**	**219**	**614**
H1 2021	188	79	
H2 2021	159	83	
Totalt 2021	**346**	**162**	**508**
H1 2020	225	73	
H2 2020	130	75	
Totalt 2020	**355**	**148**	**503**

Kilde: Finanstilsynet

5.2 TAP KNYTTET TIL MISBRUK AV BETALINGSKORT

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

Kortutstedere rapporterte at tap grunnet svindel med kortbetalinger i 2022 utgjorde 215,8 mill. kroner. Tapene økte med 18 prosent fra første til andre halvår, henholdsvis 96,8 og 119 mill. kroner. I tillegg kommer tap på 3,4 mill. kroner gjennom urettmessig bruk av betalingskort for kontantuttak, som fordelte seg på første og andre halvår med henholdsvis 1,5 og 1,9 mill. kroner. Samlet var det totale tapet ved misbruk av betalingskort 219,2 mill. kroner. Dette er en oppgang fra 2021 på 35 prosent.

[26] Artikkel 96 nr. 6 i PSD2 (Lovdata) og Guidelines on fraud reporting under PSD2 (EBA). Se også forskrift om systemer for betalingstjenester § 2 fjerde ledd.

Tabell 5.2 viser samlede tap knyttet til svindel ved betalinger med betalingskort eid av norske kunder de tre siste årene, uavhengig av om tapet dekkes av kunden selv, banken eller kortselskapet. De samlede tapene utgjorde 0,021 prosent av total transaksjonsverdi, noe som er en oppgang fra 0,016 prosent i 2021.

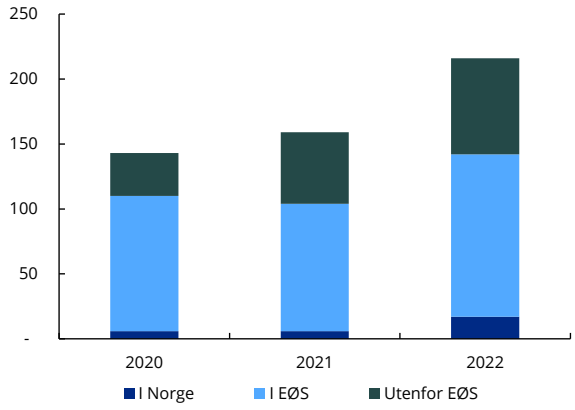
Tabell 5.2 Tap ved misbruk av betalingskort (både betalinger og kontantuttak)

Svindeltype betalingskort (beløp i mill. kroner)	Svindeltype betalingskort (beløp i mill. kroner)	2020	2021	2022
Totalt	Samlet transaksjonsbeløp	953 960	985 699	1 061 408
	– Hvorav svindel	147,6	162,0	219,2
	Svindel i prosent	0,015	0,016	0,021
Svindel ved kontantuttak	Samlet transaksjonsbeløp	47 204	36 664	41 828
	– Hvorav svindel	4,6	2,8	3,4
	Svindel i prosent	0,010	0,008	0,008
Svindel ved kortbruk initiert elektronisk og ikke-elektronisk	Samlet transaksjonsbeløp	906 756	949 036	1 019 580
	– Hvorav svindel	143,0	159,2	215,8
	Svindel i prosent	0,016	0,017	0,021

Kilde: Finanstilsynet

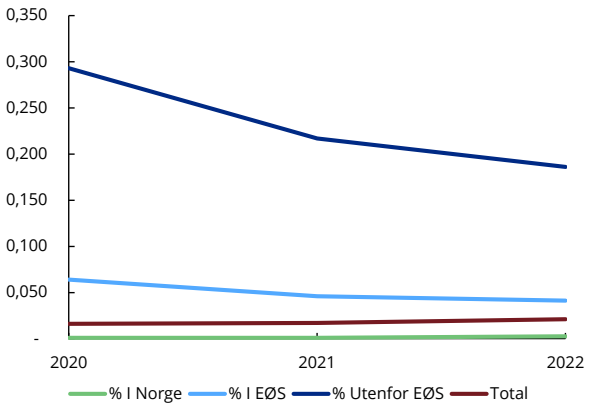
Selv om det var en oppgang i tap grunnet svindel med kortbetalinger på om lag 35 prosent fra 2021 til 2022, var oppgangen i prosent av totalt beløp noe lavere på 31 prosent.

Figur 5.1 Tap knyttet til kortbetalinger fordelt på geografi i mill. kroner



Kilde: Finanstilsynet

Figur 5.2 Tap i prosent av totale kortbetalinger fordelt på geografi



Kilde: Finanstilsynet

Tabell 5.3 viser tapene fordelt på transaksjoner i Norge, grensekryssende transaksjoner innen EØS og grensekryssende transaksjoner utenfor EØS, samt andelen som er initiert henholdsvis ikke-elektronisk og elektronisk. Tallene er eksklusiv svindel ved kontantuttak. Andelen svindel er størst for grensekryssende transaksjoner utenfor EØS. Her utgjorde svindel 0,17 prosent av transaksjonsverdien, ned fra 0,22 prosent i 2021.

Tap ved kortbetalinger som er ikke er initiert elektronisk, utgjorde i 2022 13,6 mill. kroner av det samlede tapet på 215,8 mill. kroner. Dette er korttransaksjoner der informasjon fra betalingskortet er kommunisert fra kjøper til selger over telefon eller via e-post.

Tabell 5.3 Transaksjonsverdi og svindeltransaksjoner med betalingskort rapportert av kortutsteder*. Tall for 2022

Transaksjonsverdi (beløp i mill. kroner)	Transaksjoner i Norge	Grensekryssende transaksjoner i EØS	Grensekryssende transaksjoner utenfor EØS	Totale transaksjoner
Kortbetalinger (utsteder)				
Totalt	677 462	302 253	39 866	1 019 580
– Hvorav svindel	16,9	124,6	74,3	215,8
Svindel i prosent	0,002	0,041	0,186	0,021
Hvorav initiert ikke-elektronisk:				
Totalt	5 053	6 803	3 439	15 295
– Hvorav svindel	0,3	5,8	7,6	13,6
Svindel i prosent	0,005	0,085	0,220	0,089
Hvorav initiert elektronisk:				
Totalt	672 408	295 450	36 426	1 004 285
– Hvorav svindel	16,6	118,8	66,7	202,1
Svindel i prosent	0,002	0,040	0,183	0,020

* Tallene er eksklusiv misbruk ved kontantuttak. Kilde: Finanstilsynet

Svindelandelen er større ved bruk av betalingskort ved fjernhandel (typisk handel på internett) enn ved nærhandel (bruk av betalingskort i terminal på fysisk brukersted). For betaling uten sterk kundeautentisering ved fjernhandel utgjør svindel 0,07 prosent av transaksjonsverdiene i Norge i 2022, en oppgang fra 0,005 prosent i 2021. For grensekryssende transaksjoner utenfor EØS utgjør svindel 0,32 prosent, en oppgang fra 0,24 prosent i 2021. For nærmere detaljer, se tabeller i vedlegg 4.

Tabell 5.4 Transaksjoner og svindeltransaksjoner med betalingskort rapportert av kortutsteder i 2022

Betalingskorttransaksjoner (Volum) 2022	Transaksjoner i Norge	Grensekryssende i EØS	Grensekryssende utenfor EØS	Totalt
Totalt	1 809 504 351	739 213 179	77 436 653	2 626 154 183
– Hvorav svindel	6 656	94 483	55 263	156 402
Svindel i prosent	0,0004	0,0128	0,0714	0,0060

Kilde: Finanstilsynet

Totalt ble det gjennomført rundt 2,6 mrd. betalinger med kort i 2022. Av disse var ca. 156 000 transaksjoner svindel, som utgjør 0,006 prosent. Dette er om lag som i 2021. Andelen svindel er størst ved grensekryssende transaksjoner utenfor EØS.

Tabell 5.5 Transaksjoner og svindeltransaksjoner med betalingskort rapportert av kortutsteder

Svindeltransaksjonsvolum med betalingskort	2020	2021	2022
Totalt	2 440 487 232	2 553 179 043	2 626 154 183
– Hvorav svindel	204 603	149 169	156 402
Svindel i prosent	0,008	0,006	0,006

Kilde: Finanstilsynet

5.3 TAP KNYTTET TIL MISBRUK AV BETALINGSKORT PÅ NORSKE BRUKERSTEDER

Tabell 5.6 viser samlede tap knyttet til svindel ved betalinger med betalingskort rapportert av kortinnløsere. Tabellen viser tap ved svindel gjennomført ved norske brukersteder fordelt på svindel med norskutstedte betalingskort, betalingskort utstedt innen EØS og betalingskort utstedt utenfor EØS. Tabellen viser at tap knyttet til svindel er redusert både som samlet beløp og i prosent av total transaksjonsverdi.

Tabell 5.6 Transaksjoner og svindeltransaksjoner med betalingskort rapportert av kortutsteder

Transaksjonsverdi (beløp i mill. kroner)	Transaksjoner i Norge	Grensekryssende transaksjoner i EØS	Grensekryssende transaksjoner utenfor EØS	Totale transaksjoner
Tall for 2022				
Totalt	565 222	269 307	36 302	870 832
– Hvorav svindel	5	28	50	82
Prosent	0,001	0,010	0,137	0,009
Tall for 2021				
Totalt	541 292	182 249	22 199	745 739
– Hvorav svindel	3	42	43	88
Prosent	0,001	0,023	0,194	0,012

Kilde: Finanstilsynet

5.4 TAP KNYTTET TIL KONTOOVERFØRINGER

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

Tabell 5.7 Transaksjoner og svindeltransaksjoner – kontooverføringer

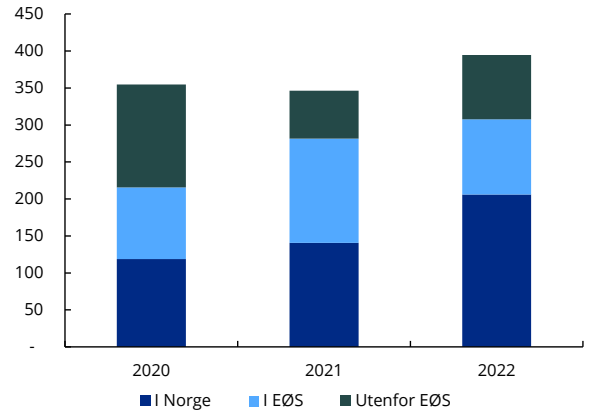
Kontooverføringer initiert elektronisk (beløp i mill. kroner)	2020	2021	2022
Totalt	38 454 037	35 724 912	46 091 136
– Hvorav svindel	355,5	346,5	394,8
Svindel i prosent	0,0009	0,0010	0,0009

Kilde: Finanstilsynet

Tap ved kontooverføringer (hovedsakelig nettbank, se tabell 5.8) utgjorde 395 mill. kroner i 2022 mot 346 mill. kroner i 2021, en oppgang på 14,2 prosent. Tallene viser samlede tap for nettbanksvindel av norske kunder de siste årene, uavhengig av om tapet dekkes av kunden selv eller banken. De innrapporterte tallene viser at svindel nå i større grad gjennomføres ved transaksjoner i Norge framfor ved grensekryssende transaksjoner. En årsak til dette er raskere gjennomføring av transaksjoner innlands.

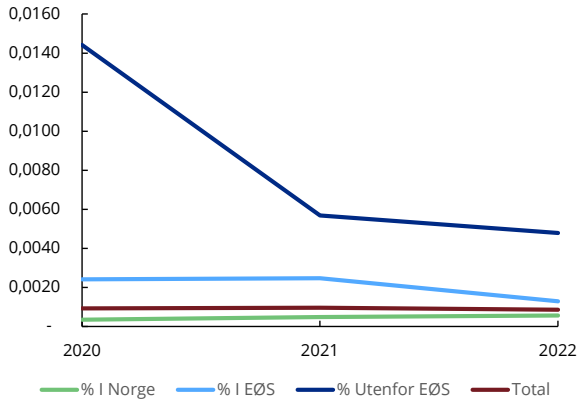
Selv om det var en oppgang i tap ved svindel med kontooverføringer i kroner, holder tapene i prosent av samlet transaksjonsbeløp seg relativt konstante, se figur 5.4.

Figur 5.3 Tap knyttet til kontooverføringer fordelt på geografi i mill. kroner



Kilde: Finanstilsynet

Figur 5.4 Tap i prosent av totale kontooverføringer fordelt på geografi



Kilde: Finanstilsynet

Tabell 5.8 Transaksjoner og svindeltransaksjoner – kontooverføringer (nettbank m.m.) 2022

Kontooverføringer initiert elektronisk (beløp i mill. kroner)	Transaksjoner i Norge	Grensekryssende i EØS	Grensekryssende utenfor EØS	Totalt
Totalt	35 273 723	7 727 106	1 805 789	44 806 618
– Hvorav svindel	206,1	101,6	87,0	394,8
Svindel i prosent	0,0006	0,0013	0,0048	0,0009
Hvorav ulike typer svindler				
– Svindleren utsteder betalingen	78,4	19,7	19,6	117,7
– Svindleren modifiserer betalingsordren	0,4	4,6	3,2	8,2
– Svindleren manipulerer betaleren til å utstede betalingsordren	127,3	77,4	64,2	268,8

Kilde: Finanstilsynet

5.5 TAP KNYTTET TIL KONTOOVERFØRINGER INITIERT AV BETALINGSFULLMEKTIGER

Rapporterte tall for tap knyttet til kontooverføringer initiert av betalingsfullmektiger viser en økning i svindeltransaksjoner fra 2021 til 2022 på om lag 100 prosent og en økning i tap på om lag 400 prosent.

5.6 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 2022 290,3 mill. kroner, der svindel med kontooverføringer i nettbank utgjorde 268,8 mill. kroner. Totalsummen er 21 prosent høyere enn i 2021 (240,6 mill. kroner). Det skyldes en økning i tap, både der svindler manipulerer betaler til en kortbetaling på 33 prosent og der svindler manipulerer betaler til en kontooverføring på 20 prosent.

Omfanget av svindel ved sosial manipulering er usikkert fordi betaleren selv bærer tapet og en del svindler av denne typen trolig ikke blir meldt til banken. Det antas at de faktiske tapene er vesentlig større enn rapportert. Kundene som er svindlet kontakter ofte banken for å få stanset transaksjoner og for å få tilbakeført beløpet. Banker varsler også kunder der banken blant annet oppdager gjentagende transaksjoner som er unormale for kunden.

Tabell 5.9 Sosial manipulering – svindleren manipulerer betaleren til å gjennomføre en transaksjon

Sosial manipulering (beløp i mill. kroner)	2020	2021	2022
Svindleren manipulerer betaleren til en kortbetaling	9,2	16,6	21,5
Svindleren manipulerer betaleren til en kontooverføring	285,3	224,00	268,8
Totalt	**294,5**	**240,6**	**290,3**

Kilde: Finanstilsynet

Også en del av tapene ved svindel der svindler initierer betalingen, skjer med bakgrunn i bruk av sosial manipulering, se punkt 5.7, noe som også bidrar til usikkerhet omkring omfanget av sosial manipulering. De største bankene[27] rapporterer til Finanstilsynet at antall svindelforsøk ved sosial manipulering stadig øker. Forsøkt svindlet beløp (angrepssum) er mange ganger større enn kundenes materialiserte tap. Bankene forhindrer et stadig større antall svindelforsøk, noe som gjør at svindlet beløp som andel av samlet transaksjonsbeløp er noe redusert fra 2021 til 2022. Dette skyldes i stor grad bankenes løpende forebygging og avdekking av svindel.

Svindel gjennom sosial manipulering ser fortsatt ut til å være den mest lønnsomme metoden for kriminelle. Hvilken type sosial manipulering de kriminelle lykkes mest med, endrer seg. Rapporteringen etter PSD2 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 2022 var phishing, der summen forsøkt svindlet var noe høyere enn tidligere.

5.7 TAP DER SVINDLER UTSTEDER BETALINGEN

I PSD2-rapporteringen er sosial manipulering definert som betalingstransaksjoner der svindleren manipulerer betaleren til å gjennomføre en transaksjon. Svindel ved phishing omfatter imidlertid også elementer av sosial manipulering. Ved phishing avlures kontakt- og betalingsinformasjon som svindleren bruker til å utstede en betaling på vegne av betaleren. I PSD2-rapporteringen blir dette kategorisert som svindel der svindler utsteder betalingen, se tabell 5.10. Tap ved denne kategorien svindel i 2022 utgjorde 117,7 mill. kroner for kontooverføringer, en oppgang på 9,4 mill. kroner fra 2021. Svindel med betalingskort utgjorde 202,1 mill. kroner i 2022, en oppgang fra 145,2 mill. kroner i 2021.

Tabell 5.10 Tap ved svindler der svindler utsteder betalingen

Svindler utsteder betalingen (beløp i mill. kroner)	2021	2022
Svindel med betalingskort	**145,2**	**202,1**
– Hvorav svindel initiert gjennom fjernbetalingskanal (internetthandel)	136,0	180,6
– Hvorav svindel initiert via nærbetaling	9,2	21,5
Svindel med kontooverføringer	**108,3**	**117,7**

Kilde: Finanstilsynet

[27] Blant annet DNBs Annual Fraud Report 2022

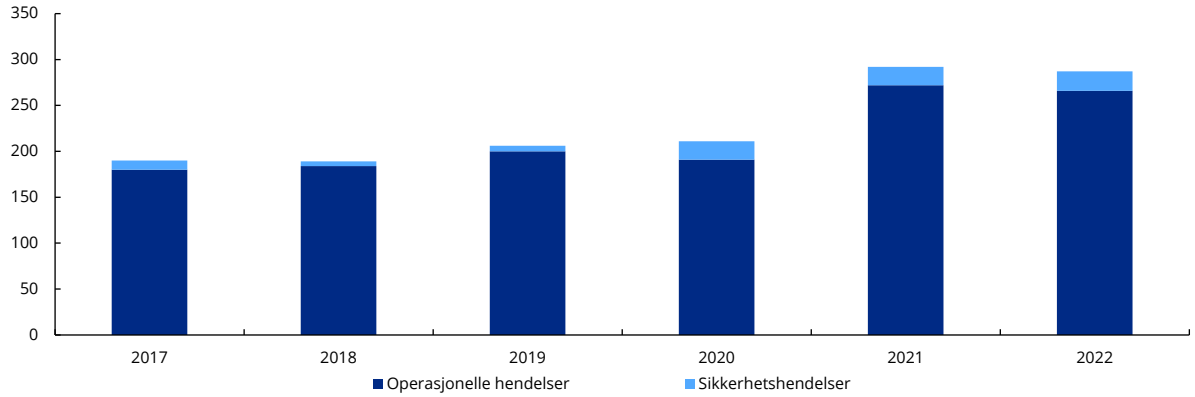
6. HENDELSESRAPPORTERING

6.1 ANTALL IKT-RELATERTE HENDELSER

Det følger av IKT-forskriften at operasjonelle hendelser eller sikkerhetshendelser skal rapporteres til Finanstilsynet uten ugrunnet opphold. Hendelsesrapporteringen bidrar til å sikre et korrekt og rettidig bilde av risikonivået i finanssektoren og til å avdekke mønstre og sammenhenger som det kan være vanskelig å oppdage for det enkelte foretak. Det viktigste er likevel det enkelte foretaks håndtering av hendelser for å sikre rask gjenoppretting og deretter oppfølging med relevante preventive tiltak.

Foretakene rapporterte 287 IKT-relaterte hendelser til Finanstilsynet i 2022, som er omtrent samme antall som året før.[28] 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.

6.1 Antall rapporterte IKT-hendelser



For nærmere informasjon om tallgrunnlaget, se vedlegg 5. Kilde: Finanstilsynet

6.2 SIKKERHETSHENDELSER

Det ble rapportert 21 sikkerhetshendelser i 2022, som er om lag som i de to foregående årene. Noen av hendelsene var alvorlige for foretakene som ble rammet, men ingen sikkerhetshendelser påvirket den finansielle infrastrukturen eller fikk alvorlige konsekvenser for de større finansforetakene.

Ett foretak rapporterte i 2022 at sårbarheten i loggverktøyet Log4j, som ble kjent i desember 2021, var blitt utnyttet til å få tilgang til en av foretakets servere. Foretaket fant ingen spor av at tilgangen var utnyttet før serveren ble stengt ned.

Sårbarheter ved bruk av åpen kildekode

Loggverktøyet Log4j er basert på åpen kildekode (open source). Slik programvare kan være sårbar fordi den tilgjengeliggjøres uten beskrivelse av innebyggede sikkerhetsmekanismer eller veiledning i hvordan den kan implementeres på en sikker måte. Mange slike verktøy inngår dessuten i rutinebibliotek med svært stor utbredelse i utviklingsmiljøer. Det kan derfor være meget krevende å kartlegge alle konsekvensene av en hendelse der sårbarheten i åpen kildekode er utnyttet. Bruk av åpen kildekode må være basert på risikovurderinger og være dokumentert.

[28] Økningen i antall hendelser fra 2020 til 2021 skyldes i hovedsak at flere typer foretak rapporterte, som inkassoforetak, og at foretakene rapporterte om flere typer hendelser, herunder hendelser knyttet til systemer for å avdekke hvitvasking og terrorfinansiering og grensesnitt for tiltrodde tredjeparters tilgang til kunders betalingskonto.

Nordea ble 2. mars 2022 utsatt for et tjenestenektangrep (DDoS-angrep) som hindret tilgang til bankens tjenester store deler av dagen. Flere norske virksomheter, herunder enkelte finansforetak, ble utsatt for tjenestenektangrep i perioden 29. juni til 5. juli. Angrepene fikk kun begrensede konsekvenser. Det er ofte vanskelig å avdekke hvem som står bak slike angrep med mindre angriperne selv gjør seg til kjenne.

I desember 2022 ble en IKT-leverandør i Sverige rammet av en sikkerhetshendelse, som førte til at leverandøren stengte ned sine tjenester i flere dager. Dette fikk konsekvenser for minst sju norske finansforetak, herunder banker, forsikringsforetak og fondsforvaltningsforetak. Ett av disse foretakene fant spor av angrepet på egne servere. For flere av de rammede norske foretakene innebar hendelsen at de elektroniske systemene for overvåking av transaksjoner ble satt ut av funksjon.

Angrep der konsekvensen er utilgjengelige systemer og/eller fare for publisering av data, forekommer stadig oftere. Angrep kan rettes mot foretaket selv eller mot leverandører foretaket er avhengig av til ulike oppgaver. Finanstilsynet vurderer det som viktig at risikoen for denne typen angrep blir inkludert i foretakets forretningsmessige konsekvensanalyse og i oppfølgingen av leverandører.

- *Sikkerheten er ikke bedre enn det svakeste leddet i en leverandørkjede. Finanstilsynet forventer at foretakene stiller krav til underleverandørers evne til å ivareta sikkerheten. Dette kan innebære at underleverandørene må dokumentere egen motstandsdyktighet basert på gjennomførte sikkerhetsanalyser og tiltak.*

I august 2022 klarte en angriper ved hjelp av phishing å kompromittere totrinnsbekreftelsen (tofaktor-autentisering) for en ansatts pålogging til et norsk finansforetaks skybaserte arbeidsflate. Den ansatte klikket på en lenke i en e-post, som førte til en side for pålogging til den skybaserte løsningen, og logget seg inn med tofaktorautentisering. Imidlertid ble påloggingen utført på angriperens enhet og ikke på den ansattes enhet, noe som medførte at angriperens maskin ble registrert som en godkjent enhet. I perioden før det ble krevet ny totrinnsbekreftelse, hadde angriperen tilsvarende tilganger som den ansatte til SharePoint, Teams, e-post m.m. I dette tilfellet benyttet angriperen tilgangen til å sende en e-post til økonomiansvarlig, i den ansattes navn, med beskjed om at økonomiansvarlig skulle betale en større faktura. Svindelforsøket ble oppdaget.

Microsoft beskrev det nye angrepsmoduset i en artikkel i juli 2022[29]. Fra begynnelsen av 2023 er det observert et økende antall slike angrep uten at Finanstilsynet er kjent med at flere finansforetak har vært rammet. Sårbarheten er ikke relatert til en spesifikk skyløsning. Et tiltak for å sikre seg mot slike angrep er å forhåndsregistrere alle enheter det er tillatt å logge seg på fra.

Øvrige sikkerhetshendelser i 2022 omfatter hacking av ansattes e-postadresser, forfalskning av betalingsinstruksjoner og phishingangrep sendt foretakets e-postadresse.

Finanstilsynet har kontakt med Nordic Financial CERT (NFCERT) om de fleste sikkerhetshendelsene. Ved sikkerhetshendelser hos foretak som ikke er medlem i NFCERT, anbefaler Finanstilsynet foretaket å dele informasjon om sikkerhetshendelsen med NFCERT.

[29] Microsofts artikkel 12. juli 2022 som beskriver hendelsesmodus: From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud

Sikkerhetstesting

Finanstilsynet fikk i 2022 rapportert en hendelse der en sikkerhetstest avdekket en sårbarhet i en nettbasert kundetjeneste som kunne medført urettmessig tilgang til person- og kontoinformasjon. For noen av søkene i nettjenesten var kontonummer en del av en URL*, som lett kan manipuleres. Å inkludere data som kontonummer i en URL er brudd på god praksis for utvikling av sikre nettapplikasjoner. For å unngå at slike og tilsvarende sårbarheter avdekkes mange år etter tjenesten ble tatt i bruk, som var tilfelle her, skal sikkerhetstesting gjennomføres som del av leveransen før produksjonssetting. Deretter bør det gjennomføres regelmessige sikkerhetstester.

* URL (Uniform Resource Locator) er den tegnstrengen som identifiserer adressen til en side på internett

6.3 FEIL OG SÅRBARHETER HOS SKYLEVERANDØRER

Finanstilsynet har mottatt flere rapporter om avvik og sårbarheter hos skyleverandører. I 2022 ble det først og fremst rapportert om driftsforstyrrelser som følge av endringer i IT-systemer hos leverandører av skytjenester. Slike hendelser rammer ofte flere foretak.

Et foretak rapporterte i 2022 å ha blitt eksponert for en sårbarhet (bluebleed) i en skybasert lagringstjeneste. Foretaket fikk etter etterforskning og analyser bekreftet at ingen av deres data var eksponert. Det ble også rapportert om en sikkerhetshendelse som gjaldt kompromittering av en skyleverandørs totrinnsbekreftelse, jf. punkt 6.2.

Skyløsninger

Bruken av skyløsninger innebærer ikke at risikoen for feilkonfigureringer, sikkerhetsinnbrudd eller menneskelige feil forsvinner. Risikoen kan reduseres, men på den andre siden kan bruk av skyløsninger introdusere nye risikoer, og konsekvensen av feil kan ramme svært bredt. Foretakene må kontinuerlig overvåke og vurdere risikoen ved bruk av skyløsninger.

6.4 HENDELSER I SYSTEMER FOR Å AVDEKKE HVITVASKING OG TERRORFINANSIERING

Det ble i 2022 rapportert 16 hendelser om avvik i foretaks elektroniske løsninger for transaksjonsovervåking for å avdekke hvitvasking og terrorfinansiering. Hendelsene var i hovedsak knyttet til feil i screeningen av kunder og/eller transaksjoner mot sanksjonslister eller lister over politisk eksponerte personer (PEP). De rapporterte feilene gjaldt ulike leverandører, men en fellesnevner var at feilene oppsto etter endringer i leverandørenes IT-systemer. Ved endringer i løsningene for transaksjonsovervåking er det viktig å påse at testplaner inkluderer både innenlands- og utenlandstransaksjoner og at kontroller gjennomføres mot oppdaterte sanksjons- og PEP-lister[30].

6.5 ÅRSAKER TIL OPERASJONELLE HENDELSER

Operasjonelle IKT-hendelser skyldes ofte feil som følge av endringer i IKT-systemene. Slike feil får oftest konsekvenser for tilgjengeligheten til tjenestene, men kan også medføre avvik som berører dataintegritet og -konfidensialitet.

[30] Oversikt over politisk eksponerte personer

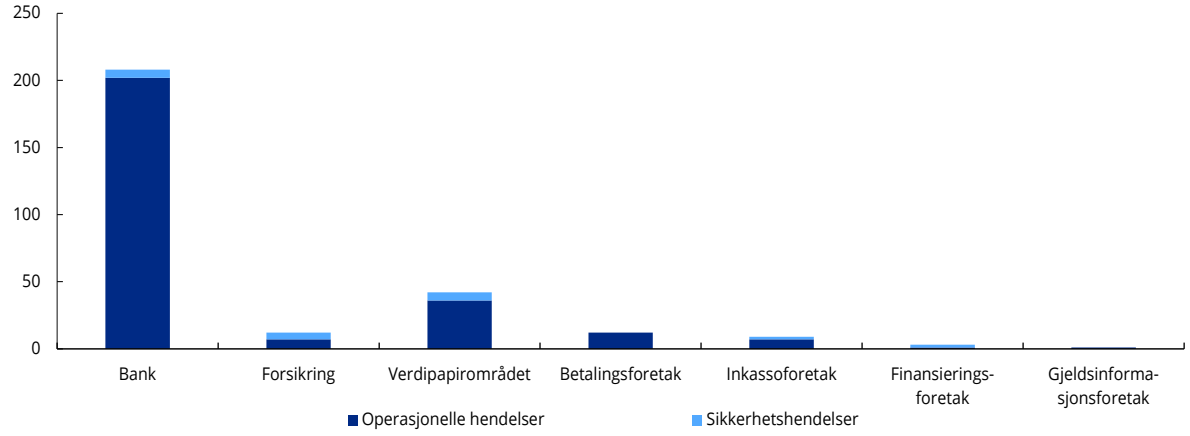
I 2022 ble det rapportert 266 operasjonelle hendelser, som er noe lavere enn i 2021. Flere av hendelsene gjaldt feil knyttet til behandling av transaksjoner etter at de var registrert av kunden, inkludert urettmessig tilgang til informasjon. Hendelsene rammet flere foretak samtidig som følge av feil etter endringer gjennomført hos en felles leverandør. Flere av de rapporterte avvikene ble avdekket først flere år etter at endringen ble gjennomført. Dette understreker betydningen av grundig testing hos leverandør og akseptansetesting og internkontroller av foretakene. Det enkelte foretak er ansvarlig for sine systemer og tjenester uavhengig av om det er leverandøren eller foretaket selv som har utviklet dem.

Andre årsaker til operasjonelle hendelser i 2022 omfatter blant annet ulike former for manglende kapasitetsovervåking, herunder sertifikater som utløp på dato eller for lite minneallokering, hardkoding av parametere i løsningene, feil i versjonsstyringen og forskjeller mellom reserveløsninger og produksjonsløsninger.

6.6 HENDELSER ETTER FORETAKSTYPE

Figur 6.2 gir en oversikt over antall hendelser etter foretakstype, fordelt på operasjonelle hendelser og sikkerhetshendelser. Hendelsene er nærmere omtalt nedenfor.

Figur 6.2 Rapporterte hendelser i 2022 fordelt på type foretak



Kilde: Finanstilsynet

Banker og betalingsforetak

Ingen av de operasjonelle IKT-hendelsene som rammet banker eller betalingsforetak i 2022 var av særlig lang varighet, men enkelte av hendelsene rammet tilgangen til betalingstjenester samtidig i mange banker samt Vipps og varte i to til fem timer. Det er økt risiko for operasjonelle IKT-hendelser etter endringer, særlig etter endringer i programvare, systemer, driftsprosesser, nettverk eller infrastruktur. Feil etter endringer får oftest konsekvenser for tilgjengeligheten, som er spesielt kritisk for banker og betalingsforetak. Det var også rapportert hendelser med feil i kundenes saldo på konto. Årsakene var driftsforstyrrelser som medførte ulike former for dupliserte transaksjoner. Dette er kritiske avvik, men feilene ble korrigert i løpet av kort tid.

På formiddagen 16. mai 2022 var det problemer ved bruk av betalingskort i en rekke butikker og utsalgssteder. Verken BankAxept eller internasjonale kort fungerte. Offline-reserveløsning med signatur fungerte for brukersteder som hadde aktivert dette. En del brukersteder, inkludert Vinmonopolet, hadde ikke tatt i bruk reserveløsningen. Årsaken til hendelsen var en nettverksendring utført i Nets. Det viste seg også å være en teknisk feil hos en av terminalleverandørene, noe som forsterket problemene.

De rapporterte sikkerhetshendelsene fra banker omfattet tjenestenektangrep, sårbarheten i loggverktøyet Log4j, angrep mot en dataleverandør i Sverige og forfalskning av betalingsinstruksjoner, jf. nærmere omtale i punkt 6.2.

Verdipapirområdet

Omtrent halvparten av hendelsene som ble rapportert på verdipapirområdet i 2022, var knyttet til de regulerte markedsplassene.

De rapporterte sikkerhetshendelsene fra foretak på verdipapirområdet gjaldt sårbarheten i loggverktøyet Log4j og angrep mot en dataleverandør i Sverige, jf. nærmere omtale i punkt 6.2.

I løpet av året var det tre operasjonelle hendelser i Euronext Securities Oslo (Verdipapirsentralen AS) som potensielt kunne blitt svært alvorlige. I april ble det avdekket en feil som i noen tilfeller medførte at aksjonærer ikke fikk deltatt og avgitt stemme på generalforsamlinger i noen norske allmennaksjeselskaper. Feilen ble oppdaget i forbindelse med en generalforsamling i april 2022 og viste seg å ha oppstått som følge av en oppdatering av IT-systemet i 2020. I mai var det en hendelse der enn deltaker i verdipapiroppgjøret manglet tilstrekkelig likviditet til å dekke sine forpliktelser. En uautorisert omstart av IT-systemet medførte feil i kalkuleringer, og en likviditetsbank ble trukket feil beløp. Feilen fikk begrensede konsekvenser, men kunne potensielt blitt svært alvorlig. I november oppstod en feil ved utbetaling av aksjeutbytte for et selskap på Oslo Børs, som medførte at en aksjonær fikk utbetalt et for høyt beløp. Ved beregning av betalingsgrunnlaget for utbetaling av aksjeutbytte stoppet normalt betalingsløp opp grunnet beløpsbegrensninger. En hasteendring ble implementert, og ved påfølgende manuell registrering ble det lagt inn feil beløp for denne aksjonæren. Feilen ble ikke avdekket i etterkontrollen.

Øvrige rapporter om operasjonelle hendelser på verdipapirområdet var dominert av problemer med tilgang til netthandel med finansielle instrumenter og kortere driftsavbrudd knyttet til tjenester på markedsplassene.

Forsikring

Rapporterte sikkerhetshendelser fra foretak på forsikringsområdet gjaldt tjenestenektangrep, hacking av ansattes e-postadresser, inkludert et tilfelle der hackerne klarte å omgå tofaktorautentisering, og foretak som var rammet av angrepet mot en dataleverandør i Sverige, jf. nærmere omtale i punkt 6.2.

Rapporterte operasjonelle hendelser gjaldt eksponering av sårbarhet, visning av feil navn på kunder og utilgjengelige kundetjenester.

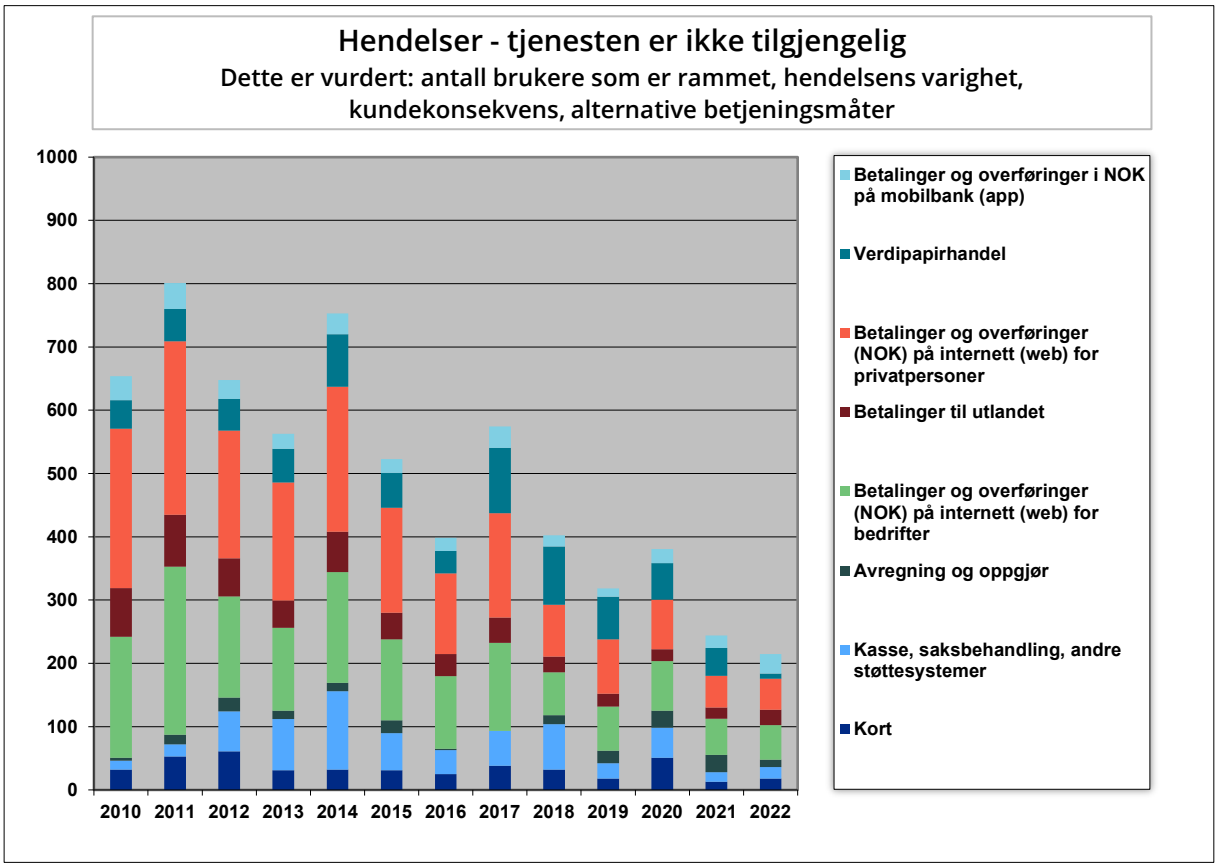
Inkassoforetak

Rapporterte hendelser fra inkassoforetak gjaldt fortrinnsvis avvik i saksbehandlingsløpet med feil frister for, eller manglende utsendelse av, faktura, inkassovarsel eller betalingsoppfordring. Det ble meldt én sikkerhetshendelse som gjaldt phishingangrep mot foretakets e-postadresse.

6.7 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. Vektingen av hendelsene gir en indeks som framkommer på den vertikale aksen i figur 6.3. Funnene sammenstilles i en tidsserie, slik at utviklingen kan følges over tid.

Figur 6.3 Hendelser med redusert tilgjengelighet for brukere. Vektet etter vurdert konsekvens*



* Skalaen på den vertikale aksen er en indeks som er basert på vektingen av hver enkelt hendelse. Lavere indeksverdi angir lavere forekomst av driftsavbrudd med konsekvenser for brukerne. For nærmere informasjon om tallgrunnlaget, se vedlegg 5.
Kilde: Finanstilsynet

Det framgår av figur 6.3 at tilgjengeligheten til betalingstjenester og kunderettede løsninger vurderes som om lag uendret fra 2021 til 2022 og noe bedre enn i tidligere år. Tilgjengeligheten til tjenestene vurderes samlet sett som tilfredsstillende i 2022.

Det var få hendelser med lang varighet i 2022, men det var noen hendelser som rammet et stort antall brukere. Transaksjoner som er belastet to ganger, doble reservasjoner og gebyr som er feilaktig belastet er inntatt i kategorien "Avregning og oppgjør".

I vurderingen av hendelsene er det tatt hensyn til i hvilken grad det eksisterer alternative tjenester som dekker kundens behov, for eksempel om kunden kan benytte internettbaserte tjenester dersom app-tjenester på mobiltelefon ikke fungerer. Videre er det forsøkt å hensynta at alternativene ikke nødvendigvis har samme tjenesteomfang, som at mobile betalingsløsninger som oftest ikke tilbyr alle tjenestene som nettbaserte løsninger har.

Det er en stor grad av redundans i det norske betalingssystemet

- Kunden kan ofte velge mellom flere plattformer (mobilbank, nettbank, mv.) for å få utført sentrale tjenester. Dersom én kanal er nede, kan kunden benytte en annen kanal.
- Dersom en betalingstjenesteyter (bank) er nede, kan kunden, dersom denne har flere bankforbindelser, benytte en annen betalingstjenesteyter som ikke er rammet av feilen. E-faktura er for eksempel synlig i alle kundens banker, og et nytt kundeforhold kan etableres elektronisk i løpet av få minutter.
- Betalingstjenesteytere tilbyr ulike løsninger når det gjelder autentisering og signering, biometri, biometri i kombinasjon med koder og BankID, for å nevne noen. Dersom én av disse er nede, kan kunden benytte en annen.
- Mange betalingsløsninger bygger på tjenester i sky, som gjennomgående har stor grad av redundans.

Redundansen gjør at tilgjengeligheten til betalingstjenester og kunderettede tjenester isolert sett øker. Det innebærer at selv om antall hendelser et år øker, kan tjenestene likevel oppleves å være mer tilgjengelige enn tidligere år.

6.8 HENDELSER KNYTTET TIL PROBLEMER MED DEDIKERTE PSD2-GRENSESNITT

Både kontotilbydere og betalingstjenesteytere skal etter regelverket rapportere til Finanstilsynet om eventuelle problemer med dedikerte grensesnitt for tredjepartstilbyderes tilgang til kunders betalingskonto, se omtale i egen ramme. DNB rapporterte i 2022 ukentlig status på sitt dedikerte grensesnitt, herunder om eventuelle problemer med tilgjengelighet eller funksjonalitet. Andre banker rapporterte dersom de hadde problemer med grensesnittene, enten det gjaldt tilgjengelighet eller funksjonalitet. Også tredjepartstilbydere rapporterte i 2022 hyppig om observert nedetid og manglende funksjonalitet i bankenes dedikerte grensesnitt for tilgang til kunders betalingskontoer.

Finanstilsynet har med bakgrunn i sin oppfølging av rapporterte mangler publisert presiseringer og avklaringer om regelverket.[31]

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.

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.

[31] PSD2 – Presiseringer og avklaringer om regelverket

7. UTKONTRAKTERING

7.1 MELDING OM UTKONTRAKTERING

Foretakene i finanssektoren er, med enkelte unntak, pliktige til å sende melding til Finanstilsynet når foretaket inngår avtale om kritisk eller viktig utkontraktering av blant annet IKT-virksomhet, ved endring av slik avtale eller ved bytte av oppdragstaker. Dersom utkontrakteringen ikke anses som forsvarlig, vanskeliggjør tilsyn eller er i strid med regelverket, kan Finanstilsynet sette vilkår for utkontrakteringen eller gi pålegg om å ikke iverksette eller om å avslutte oppdraget.

Finanstilsynet behandlet i 2022 ca. 240 meldinger om utkontraktering av IKT-leveranser, nesten 20 prosent flere enn året før. En del av meldingene ble gitt fra samarbeidende grupper av banker på vegne av flere banker.

De fleste meldingene om utkontraktering i 2022 var meldinger om utkontrakteringer til leverandører av skytjenester. Finanstilsynet vil understreke viktigheten av at det ved kjøp av IKT-tjenester sikres at avtalen er i henhold til gjeldende regelverk og at risikoen er innenfor foretakets risikotoleranse.

Enkelte avtaler oppfyller ikke IKT-forskriftens krav

Finanstilsynet har gjennom sin tilsynsvirksomhet avdekket avtaler om utkontraktering med tredjeparter som ikke oppfyller IKT-forskriftens krav. De vanligste avvikene som avdekkes gjelder krav om foretakenes rett til kontroll og revisjon av leverandørenes leveranser og begrensninger i Finanstilsynets tilgang til opplysninger fra og tilsyn hos IKT-leverandøren der det er nødvendig som et ledd i tilsynet med foretaket.

Finanstilsynet forutsetter at foretakene reviderer og oppdaterer sine avtaler i henhold til gjeldende reguleringer. I forbindelse med tilsyn vil Finanstilsynet framover øke oppmerksomheten mot utkontrakteringsavtaler som er inngått tilbake i tid og avtaler med leverandører der tilsynet tidligere har registrert avvik fra regelverket.

Foreløpig er det få foretak som har flyttet sine kjerneløsninger ut i offentlig sky, men det er flere foretak som nå vurderer å gjøre dette. Flytting av kjernesystemer til skybaserte løsninger vil ofte være omfattende og krevende, og foretakenes beslutninger om dette må bygge på grundige risikovurderinger.

Gjennom utkontrakteringer kan foretakene få flere plattformer å forholde seg til, som for eksempel systemer hos en driftsleverandør i kombinasjon med ulike skybaserte tjenester fra flere skytjenesteleverandører. Det gir økt kompleksitet og et mer sammensatt risikobilde på IKT-området. Finanstilsynet ser at det blir stadig mer krevende for foretakene å følge opp IKT-utkontrakteringer siden ansvarsfordelingen mellom leverandørene kan være uklar, noe som blant annet kan gjøre det vanskeligere å identifisere feil ved hendelser.

Økt utkontraktering av tjenester til noen få leverandører kan innebære konsentrasjonsrisiko, som vanskelig kan håndteres av det enkelte foretak. For å få bedre oversikt over bruken av underleverandører har Finanstilsynet nylig tatt i bruk et nytt Altinn-skjema for innsending av meldinger om utkontraktering. Løsningen omfatter både virksomhetsutkontraktering og utkontraktering av IKT-tjenester, og skal også legge til rette for å automatisere og standardisere Finanstilsynets behandling av innkommende meldinger om utkontraktering.

7.2 STYRING OG KONTROLL

Foretakene er ansvarlige for forsvarlig utkontraktering av IKT-virksomhet og for at de krav som følger av regelverket etterleves. Se Finanstilsynets veiledning om utkontraktering, rundskriv 7/2021.[32]

Foretakene må besitte god innkjøps- og oppfølgingskompetanse, men også benytte god funksjonell og teknisk kompetanse, herunder IKT-sikkerhetskompetanse, for både å kunne stille tilstrekkelige krav til leverandørens løsninger og IKT-sikkerhet, og fullt ut forstå leveransen.

Inngåelsen og oppfølgingen av hver enkelt utkontrakteringsavtale må operasjonaliseres i samsvar med etablerte interne retningslinjer og rutiner, og avtalens oppfølging må innlemmes i foretakets system for risikostyring og internkontroll på linje med annen virksomhet i foretaket. Dette må være etablert før foretaket iverksetter en avtale om utkontraktering.

7.3 AVTALEBESTEMMELSER FOR OPPHØR AV UTKONTRAKTERINGSAVTALER

De senere årene har det blitt økt oppmerksomhet rundt utfordringene ved bytte av tjenesteleverandør (oppdragstaker) ved utkontraktert virksomhet. For å ivareta tjenesteleveransene er det viktig at utkontrakteringsavtalene har bestemmelser som regulerer partenes plikter ved opphør av avtalen, herunder oppdragstakers plikt til å bistå foretaket (oppdragsgiver) i avviklingsfasen uansett årsak til avtalens opphør. Bestemmelsene bør også omfatte oppdragstakers plikt til å bistå oppdragsgiver med å få igangsatt tjenesteleveransene hos ny tjenesteleverandør.

Det er Finanstilsynets erfaring at detaljerte avtalebestemmelser knyttet til opphør av avtaler er særlig viktig for å sikre at foretakets tjenesteleveranser blir ivaretatt av oppdragstaker.

7.4 RISIKO KNYTTET TIL UTKONTRAKTERING

Skytjenester

I finanssektoren har det hittil ikke vært tradisjon for å legge kritiske og viktige IT-systemer i sky. Årsakene til dette er flere, men én av hovedårsakene synes å være knyttet til foretakenes vurdering av modenheten til skyplattformene og IKT-risikoen forbundet med utvikling og drift av kritiske og viktige systemer i sky.

De siste par årene har flere og flere foretak vurdert skyplattformer som tilstrekkelig modne og at risikoen knyttet til drift og utvikling i flere tilfeller er lavere enn på tradisjonelle plattformer. Foretakenes hovedargumenter er blant annet mulighetene for dynamisk skalering av prosesserings- og lagringskapasitet i forhold til behov og at skyplattformens kapasiteter gir reelle muligheter for å teste beredskaps- og kriseløsninger. Videre tilbyr skyplattformer nye verktøy for avansert feilhåndtering, der reserveløsninger etter definerte regler automatisk iverksettes på alternative geografiske lokasjoner.

Tradisjonelt har foretakene lagt vekt på å holde antall applikasjoner, utviklingsverktøy og tekniske plattformer på et minimum, blant annet fordi det gir lavere kostnader og IKT-risiko. Et større antall applikasjoner, verktøy og driftsplattformer vil stille større krav til styring og kontroll, inkludert økte krav til kapasitet for å håndtere IKT-risiko, og kan blant annet innebære mer omfattende samhandling mellom aktører ved både drift og håndtering av hendelser og øke angrepsflatene mot foretakets IKT-infrastruktur. Foretakene må foreta tilsvarende vurderinger når det gjelder utvikling og drift av løsninger basert på skytjenester som ved tradisjonelle plattformer.

[32] Finanstilsynet: Rundskriv 7/2021 Veiledning om utkontraktering

Fare for innlåsing

Tradisjonelt har mange foretak inngått langsiktige avtaler om utvikling og drift av kjernesystemer, typisk 10–15 års horisonter. Ved etablering av nye kjernesystemer, bortsett fra der leverandøren tilbyr både systemløsning og drift, har foretakene gjerne inngått et mer eller mindre "permanent" partnerskap med systemleverandøren, da denne besitter både teknisk og forretningsfaglig kompetanse knyttet til kjernesystemet, enn med valgt driftsleverandør.

I forbindelse med utvikling og drift av kjerneløsninger basert på skyteknologi kan bruk av skyplattformspesifikk funksjonalitet gi innlåsing med valgt leverandør. På den annen side kan utnyttelsen av plattformspesifikk funksjonalitet gi foretakene best verdi i form av effektiv utvikling, reduksjon av sikkerhetsrisiko, strømlinjeformede krise- og beredskapsløsninger og en mer stabil og sikker drift.

Finanstilsynets oppfatning er at det ikke nødvendigvis er annerledes innlåsingsrisiko ved en skybasert utkontrakteringsmodell, der kjernesystemet gjør bruk av skyplattformens spesifikke funksjonalitet, enn ved en tradisjonell utkontrakteringsmodell. Erfaringer viser at det å fratre avtaler knyttet til kjernesystemer basert på tradisjonelle utkontrakteringsmodeller krever en lang gjennomføringshorisont, da det ofte vil være teknologiske og funksjonelle bindinger, gjerne i kombinasjon med utdatert teknologi.

Risikoen for innlåsing må uansett inngå i foretakets risikovurdering ved beslutning om en utkontraktering.

Uttredelsesplaner

For at foretaket skal være best mulig rustet til å håndtere situasjoner der tjenesteleveranser opphører, enten det er foretaket eller tjenesteleverandør som velger å avslutte avtaleforholdet, er det viktig at foretaket har vurdert konsekvensene ved opphør av de enkelte leveransene som avtalen omfatter. Videre bør foretaket ha sikret at avtalebestemmelsene knyttet til terminering av avtalen er tilstrekkelige for å sikre overgangen til ny leverandør. Foretaket bør i sine uttredelsesplaner også inkludere en vurdering av alternative leverandører.

Leveransekjeder

Den teknologiske utviklingen har medført at kompleksiteten og avhengighetene mellom foretakenes IKT-systemer og driften av disse har økt. Slike avhengigheter kan gjøre at en utkontrakteringsavtale, som isolert sett ikke er vurdert som kritisk eller viktig, kan ha konsekvenser for tjenester som er kritiske eller viktige.

For at virksomheten skal drives forsvarlig og innenfor kravene som følger av sektorregelverket og eventuelle konsesjonsvilkår, må foretaket ha kapasitet og kompetanse til å inngå, følge opp og avvikle utkontrakteringsavtaler. Hvilken kapasitet og kompetanse som til enhver tid skal være i foretaket, må konkret besluttes. Blant annet bør det vurderes hvilken risiko en eventuell mangel på egen kapasitet eller kompetanse innebærer for foretakets virksomhet. Foretaket må også vurdere hvordan det skal sørge for tilgang til nødvendig kapasitet og kompetanse for å sikre stabilitet i tjenesteytingen dersom foretaket må hente de utkontrakterte tjenestene tilbake.

I mange av IKT-utkontrakteringsforholdene vil oppdragstaker kunne utkontraktere deler av oppdraget videre til egne underleverandører. Foretakene må å ha kontroll med risikoen knyttet til tjenester levert av oppdragstakers underleverandører, og det er dermed formålstjenlig med avtalebestemmelser som sikrer at foretaket har innflytelse på dette. Uplanlagte eller uønskede bytter av underleverandører vil blant annet kunne ha konsekvenser for renomme, kostnader, leveransetider og leveransekvalitet.

Når et foretak benytter IKT-systemer som er framforhandlet av flere foretak i fellesskap, må hvert enkelt foretak gjennomføre en selvstendig konsekvensanalyse for å vurdere hvilken betydning tilslutningen til fellessystemet har for egen virksomhet. Som eksempel på slike IKT-systemer nevnes bankenes

fellesoperasjonelle infrastruktur og IKT-systemer som inngår i pensjonskontoregisteret som forsikringsforetak kan knytte seg til.

8. VURDERING AV DEN FINANSIELLE INFRASTRUKTUREN OG FORETAKENES IKT-VIRKSOMHET

8.1 DEN FINANSIELLE INFRASTRUKTUREN ER ROBUST

Finanstilsynet anser den norske finansielle infrastrukturen som robust. Foretakenes tjenester synes å være godt beskyttet mot angrep. Det var i 2022 ingen større IKT-hendelser med konsekvenser for finansiell stabilitet, selv om en hendelse 16. mai fikk stor oppmerksomhet, se punkt 6.6. Foretakenes driftsstabilitet var tilfredsstillende og bedre enn i tidligere år.

Det ble rapportert noen færre hendelser i 2022 enn i 2021. Andelen sikkerhetshendelser var omtrent som i 2021, mens det ble rapportert noen færre operasjonelle hendelser. Finanstilsynet har ut fra hendelsenes varighet, tidspunkt og antall berørte brukere vurdert tilgjengeligheten til betalingstjenester og andre kunderettede tjenester som bedre i 2022 enn i de foregående årene, se punkt 6.7.

Det var i 2022 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[33] og det internasjonale oppgjørssystemet CLS[34].

Selv om angrepene på den finansielle infrastrukturen var færre i 2022[35] enn i 2021, synes omfanget av digital kriminalitet med konsekvens for finanssektoren fortsatt å øke. Særlig var det en betydelig økning i phishing. Så langt har digital kriminalitet ikke ført til systemkriser eller alvorlige hendelser hos foretak i den norske finanssektoren.

I 2022 ble det avdekket alvorlige sårbarheter hos enkelte foretak, som kunne fått store konsekvenser dersom de hadde blitt utnyttet. Det var også sikkerhetshendelser hos leverandører som fikk konsekvenser for berørte foretak. Sårbarheter og sikkerhetshull innebærer risiko for blant annet informasjonslekkasje eller uautoriserte endringer i foretakenes, eller deres leverandørers, systemer og infrastruktur. Foretakene må samtidig forholde seg til at det digitale trusselbildet er i kontinuerlig endring, blant annet som følge av Russlands angrep på Ukraina.

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 styrke IKT-sikkerheten generelt, er med på å sikre stabile driftsløsninger, avverge digital kriminalitet og redusere konsekvensene ved hendelser. Dette omfatter kriseløsninger og -beredskap, gjenopprettingsplaner og IKT-sikkerhetsarbeid, blant annet forsvarsverk mot digital kriminalitet.

8.2 RISIKO KNYTTET TIL SÅRBARHETER I FORETAKENES IKT-VIRKSOMHET

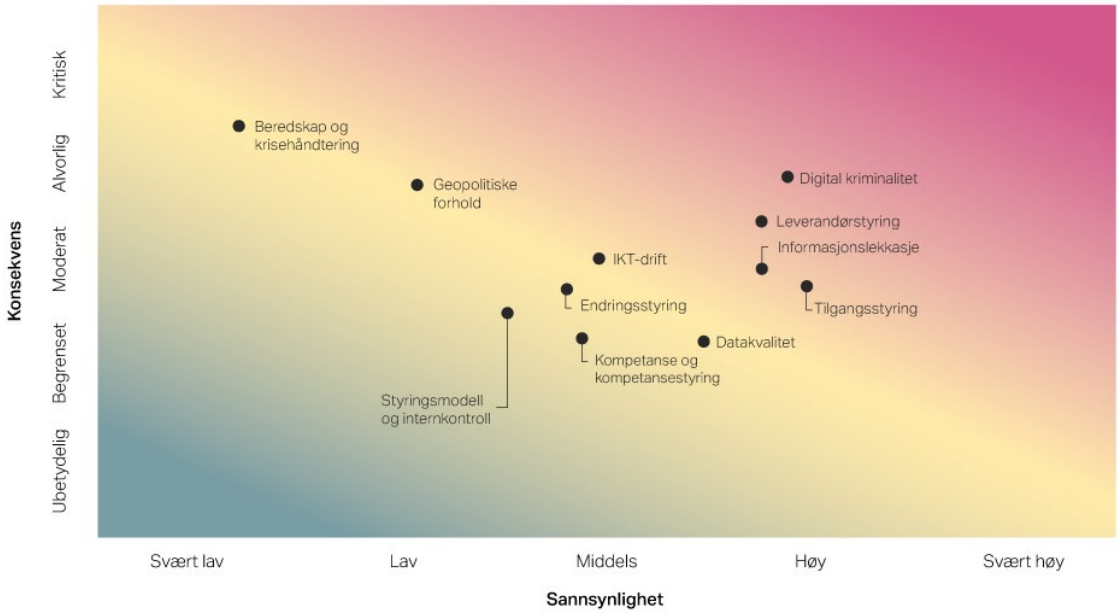
Figur 8.1 oppsummerer Finanstilsynets vurdering av de mest sentrale sårbarhetene i finanssektoren. De ulike sårbarhetene er klassifisert etter sannsynlighet for at en alvorlig negativ hendelse oppstår, og den tilhørende konsekvensen etter alvorlighetsgrad for det enkelte foretak. Observasjoner og vurderinger som ligger til grunn for klassifiseringen, framgår av tabell 8.1 og er nærmere omtalt i vedlegg 2.

[33] SWIFTs nettsted: About us
[34] CLS' (Continuous Linked Settlement) nettsted: About us. Amerikansk finansinstitusjon som tilbyr oppgjørstjenester til sine medlemmer i valutamarkedet (FX)
[35] Digi.no 18. mars 2023: Samarbeid er det beste forsvar i cyberkrigen

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. Sårbarheter knyttet til leverandørstyring, tilgangsstyring og informasjonslekkasje er også sentrale risikoer, der den samlede risikoen anses som middels til høy. Risikoen knyttet til leverandørstyring er ansett som høyere i 2022 enn året før. Mens risikoen knyttet til foretaks forsvarsverk mot digital kriminalitet er ansett å være noe høyere, er risikoen knyttet til foretaks forsvarsverk mot informasjonslekkasje ansett som noe lavere enn i 2021.

Risiko knyttet til sårbarheter i foretaks beredskap og krisehåndtering og geopolitiske forhold anses som middels til høy. Risiko knyttet til sårbarheter ved foretakenes endringsstyring, styringsmodell og internkontroll, IKT-drift, kompetanse og kompetansestyring samt datakvalitet anses å være middels. Risikoen knyttet til foretaks oppfølging av kompetanse og kompetansestyring er ansett som noe lavere i 2022 enn året før, mens risikoen knyttet til oppfølging av IKT-drift er ansett som lavere.

Figur 8.1 Finanstilsynets vurdering av sårbarheter og risiko for 2022



Kilde: Finanstilsynet

Tabell 8.1 Sårbarheter som kan utgjøre en risiko for uønskede hendelser

Område	Sårbarheter som kan utgjøre en risiko for uønskede hendelser (Grad av risiko, sannsynlighet og konsekvens framgår av figur 8.1)	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 utgjør en operasjonell risiko ikke avdekkes, og at risikoreduserende tiltak i tråd med foretakets risikotoleranse ikke iverksettes.	
Kompetanse og kompetansestyring	Knapphet på ressurser i Norge innen drift, arkitektur, sikkerhet og ny teknologi, samt mangelfull kompetansestyring, kan føre til at foretak ikke får dekket dagens og fremtidens kompetansebehov. Problemer og feil som oppstår, kan være utfordrende å løse. Avhengigheten til utlandet kan øke.	
Leverandørstyring	Komplekse leverandørkjeder, med flere leverandører og underleverandører i verdikjeden, krevende samhandlingsmodeller (strategisk, administrativt og operativt), og mangel på kompetanse kan føre til svakere oppfølging og kontroll med kritiske og utkontrakterte IKT-tjenester.	
Digital kriminalitet	Manglende sikkerhetstester, sikkerhetsoppdateringer, opplæring og bevisstgjøring av ansatte samt mangelfull overvåking av aktiviteter i egen teknisk infrastruktur, herunder nettverk og systemer, kan føre til at kriminelle påfører foretaket skade gjennom digitale angrep. Også svindel knyttet til bruk av finansielle tjenester kan påføre foretaket tap.	
Informasjonslekkasje	Manglende klassifisering av informasjon, herunder dokumentasjon, og kontroller for overvåking av informasjon som sendes ut på e-post, 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.	
Beredskap og krisehåndtering	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 tid går på bekostning av kvalitet, kan føre til funksjonelle feil i applikasjoner og systemer og til at sikkerhetshull ikke avdekkes. Manglende kontroll av endringer i driftsoppsettet kan føre til brudd i kritiske forretningsprosesser og til at foretaket eksponeres for digital kriminalitet.	
Tilgangsstyring	Mangelfull kontroll med og overvåking av utvidede tilgangsrettigheter, for ansatte og personell hos leverandører, kan skade foretaket og dets kunder som følge av informasjonslekkasjer og bevisste eller ubevisste operasjonelle feil.	
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.	

Pil-kategoriene: Økende, svakt økende, uendret/stabil, svakt minkende og minkende. Kilde: Finanstilsynet

9. NYTT REGELVERK OM DIGITAL MOTSTANDSDYKTIGHET – DORA-FORORDNINGEN

I september 2020 framla Europakommisjonen en digital finanspakke, "Digital Finance Package", med en digital finansiell strategi og regelverk for å sikre forbrukere tilgang til innovative finansielle produkter samtidig som forbrukervern og finansiell stabilitet er ivaretatt. Som en del av pakken ble forordningen om digital og operasjonell motstandsdyktighet i den finansielle sektoren (DORA-forordningen) lansert.[36] DORA-forordningen ble endelig vedtatt i Europaparlamentet og Europarådet i november 2022, og dato for ikrafttredelse er satt til 17. januar 2025. Det foreslåtte regelverket anses å være EØS-relevant.

DORA-forordningen skal bidra til at alle deltakere i det finansielle systemet har nødvendige tiltak på plass for å redusere faren for cyberangrep og andre risikoer knyttet til IKT-virksomheten. Den foreslåtte lovgivningen vil kreve at alle foretak skal kunne håndtere alle typer forstyrrelser av og trusler mot foretakets IKT-virksomhet. Forslaget introduserer også et tilsynsrammeverk for IKT-leverandører, for eksempel leverandører av skytjenester.

For å sikre en helhetlig gjennomføring av kravene til finanssektorens styring av IKT-risiko omfatter den foreslåtte forordningen en rekke foretakstyper regulert på EU-nivå. Det vil gjøre det mulig å få en homogen anvendelse av kravene til risikostyring på IKT-relaterte områder, hensyntatt at det er betydelige forskjeller mellom foretak når det gjelder størrelse, forretningsprofiler og eksponering mot digital risiko.

I Norge reguleres bruken av IKT innen finanssektoren i hovedsak gjennom IKT-forskriften. For noen foretakstyper reguleres bruken av IKT i særregelverk. Virkeområdet til DORA er mer omfattende enn, men samtidig ikke fullt dekkende for, IKT-forskriftens virkeområde. Videre reguleres Finanstilsynets tilsynsaktiviteter gjennom finanstilsynsloven. DORA inneholder bestemmelser som overlapper med både IKT-forskriften og finanstilsynsloven. I tillegg inneholder DORA bestemmelser som ikke er dekket i norsk rett i dag.

Det foreslåtte regelverket stiller krav til styring og kontroll av IKT-virksomheten, styring av IKT-risiko, rapportering av IKT-hendelser, testing av operasjonell motstandsdyktighet og oppfølging av leverandører. IKT-forskriften, tilsvarende særregelverk og de europeiske tilsynsmyndighetenes retningslinjer inneholder allerede en rekke av disse kravene, slik at det nye regelverket i utgangspunktet ikke vil medføre vesentlige endringer for norske foretak i praksis.

Regelverket åpner for å dele informasjon og etterretning knyttet til cybertrusler og sårbarheter, slik norske foretak allerede gjør gjennom samhandlingen med Nordic Financial CERT (NFCERT).

DORA medfører at flere forordninger innen finansområdet må endres. Disse framgår som endringsbestemmelser i DORA. I tillegg til DORA-forordningen er DORA-direktivet[37] vedtatt. Direktivet er også EØS-relevant. DORA-forordningen medfører behov for endring i flere direktiver på det finansielle området. Direktiver kan ikke endres gjennom forordninger, slik at endringsbestemmelsene må gis i direktivs form. De aktuelle endringsbestemmelsene gjelder endringer i operasjonelle risiko- eller risikostyringskrav eller krysshenvisninger, blant annet i kapitaldekningsdirektivet (CRD), direktivet om markeder for finansielle instrumenter (MiFID II), direktivet om omsettelige verdipapirer (UCITS) og direktivet om adgang til å starte og utøve virksomhet innen forsikring og gjenforsikring (Solvens II).

[36] Digital Operational Resilience Act,
[37] Europa-Parlamentets og Rådets direktiv (EU) 2022/2556

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

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