

VEDLEGG 3: FINANSTILSYNETS OPPFØLGING

Finanstilsynets tilsyn med IKT og betalingstjenester – sentrale områder

Tilsynsvirksomheten er risikobasert, og Finanstilsynet prioriterer tilsyn med foretak som har størst betydning for finansiell stabilitet og velfungerende markeder. IKT-risiko vurderes, og foretakenes egne årlige vurderinger av IKT-risiko gjennomgås. Tilsyn med organisering av IKT-/cybersikkerhetsarbeidet vektlegges, samt sikkerhet knyttet til foretakenes IKT-løsninger og organiseringen av overvåkingen. Tilsynene omfatter blant annet overordnet styring og kontroll med IKT, beredskapsarbeid knyttet til kontinuitet og kriseløsninger og testing av disse, foretakenes styring, kontroll og oppfølging av utkontraktert IKT-virksomhet, foretakenes kontroll med tilganger til systemer, foretakenes betalingstjenester og IKT-løsninger for å avdekke hvitvasking og terrorfinansiering. Bruk av ny teknologi, større endringer på IKT-området og større endringer i den finansielle infrastrukturen er også aktuelle områder som følges opp.

Arbeid med betalingssystemer

EUs reviderte betalingstjenestedirektiv (PSD2)¹ er tatt inn i norsk lovgivning og ligger til grunn for tilsynet med foretakenes betalingstjenester. Foretakene vil blant annet bli fulgt opp med hensyn til etterlevelse av ny forskrift om systemer for betalingstjenester², risiko knyttet til betalingstjenestene og etterlevelse av meldeplikten ved nye eller endrede betalingstjenester. Kontotilbyderes grensesnitt (APIer) for tiltrodde tredjeparters tilgang til konto vil også bli fulgt opp, jf. uttalelse fra den europeiske banktilsynsmyndigheten (EBA)³. I konsesjonsbehandlingen vil det påses at foretakene har godt dokumenterte rutiner på områder relatert til IKT- og betalingstjenester. Foretakene vil også bli fulgt opp på at betalingsløsningene er robuste, at tilfredsstillende beredskap er etablert for løsningene, og at beredskapen i det elektroniske betalingssystemet er forsvarlig. Samarbeidet med Norges Bank knyttet til betalingssystemet og finansiell infrastruktur videreføres.

Oppfølging av hendelser

I tilsynsvirksomheten er oppfølging av IKT-hendelser et prioritert område. Finanstilsynet vil i 2023 fortsatt overvåke utviklingen nøye. Ved hendelser vil det bli lagt vekt på at foretaket avdekker årsaker og iverksetter tiltak for å hindre gjentakelser. Ved alvorlige avvik vil hendelsen følges løpende gjennom hele forløpet. Særlige tiltak vil bli vurdert. Også avdekkede sårbarheter i foretakenes IKT-løsninger vil bli fulgt opp. Finanstilsynet vil videreføre sin årlige gjennomgang av hendelsesrapporteringen til de største aktørene. Det vil også bli fulgt opp at både kontotilbydere og tredjepartstilbydere i samsvar med PSD2 rapporterer avvik og at kontotilbyderne korrigerer avvikene og informerer tredjepartstilbyderne.

Utkontraktering av IKT-virksomhet

Finanstilsynet vil fortsatt følge opp foretakenes utkontraktering av IKT-virksomhet og påse at foretakene ved inngåelse av ny eller endret avtale om utkontraktering av IKT-virksomhet som er kritisk eller viktig for foretaket, melder denne til Finanstilsynet, slik finanstilsynsloven § 4c krever, jf. meldepliktforskriften⁴. Tilsynsvirksomheten omfatter oppfølging av at foretakene gjennomfører risikoanalyser og en forsvarlig vurdering av utkontrakteringsforholdet, at avtalene er i tråd med regelverket, og at utkontrakteringen er forsvarlig behandlet i foretaket, jf. IKT-forskriften § 2.

¹ Lovdata: [Om betalingstjenester i det indre marked](#) (PSD2)

² Lovdata: [Forskrift om systemer for betalingstjenester](#)

³ EBAs uttalelse om tiltrodde tredjeparters tilgang til konto: [EBA calls on national authorities to take supervisory actions for the removal of obstacles to account access under the Payment Services Directive](#)

⁴ Lovdata: [Forskrift om meldeplikt ved utkontraktering av virksomhet mv.](#)

Beredskapsarbeid

Arbeidet i Beredskapsutvalget for finansiell infrastruktur (BFI) videreføres. BFI gjennomgår blant annet hendelsesscenarioer, og det vurderes om ansvarsforhold ved krisesituasjoner er tilstrekkelig klare. Det er planlagt gjennomføring av beredskapsøvelser også i 2023, og tiltak knyttet til funn i tidligere øvelser vil bli fulgt opp.

Særskilte hendelser som koronapandemien, krigen i Ukraina og foretakenes innretning av sin IKTvirksomhet vil bli fulgt opp, særlig hos sentrale aktører i den finansielle infrastrukturen.

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

Finanstilsynet vil innrette sitt beredskapsarbeid og håndtering av IKT-sikkerhetshendelser i tråd med NSMs rammeverk for håndtering av IKT-sikkerhetshendelser⁵. Finanstilsynet er sektorvis responsmiljø (SRM) på finansmarkedsområdet og utøver rollen i samarbeid med Nordic Financial CERT i tråd med avtalte regler for informasjonsutveksling. NSMs rammeverk ligger til grunn for samhandlingen mellom Finanstilsynet og Nordic Financial CERT.

Oppfølging av trusselbildet knyttet til digital kriminalitet

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

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

Sammen med Norges Bank etablerte Finanstilsynet i 2021 et rammeverk for testing av cybersikkerhet i finanssektoren (TIBER-NO). Målet er å bidra til finansiell stabilitet gjennom økt motstandsdyktighet mot cyberangrep for kritiske funksjoner i norsk finansiell sektor. Arbeidet følges opp av en styringsgruppe ledet av Norges Bank med deltakelse fra Finanstilsynet. Finanstilsynet vil gjennomføre regelmessige møter med foretak og Nordic Financial CERT og delta i Nasjonalt cybersikkerhetssenter (NCSC), europeiske tilsynsmyndighetenes arbeid med IKT-sikkerhet og European Systemic Cyber Group (ESCG) under Det europeiske systemrisikorådet (ESRB).

Forbrukervern

Finanstilsynet vil følge opp at foretakene etablerer digitale løsninger i tråd med regelverket, og at løsninger som lanseres, har innebygd sikkerhet og funksjonalitet i tråd med forbrukernes forventninger. Det vil også bli lagt vekt på at foretakene ivaretar kundenes sikkerhet ved bruk av deres løsninger og tjenester.

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

⁵ Nasjonal sikkerhetsmyndighet (NSM): [Rammeverk for håndtering av IKT-hendelser](#)

Det vil bli fulgt opp at løsninger for betalingstjenester ikke krever at forbrukerne må akseptere tilleggsfunksjonalitet for å kunne benytte seg av betalingstjenesten, og at forbrukerne gis mulighet til å beskytte seg mot uønskede hendelser, for eksempel gjennom mulighet for å sperre kort for bruk på internett.

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

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

Finanstilsynet vil fortsette å følge opp at bankene ivaretar sine plikter når det gjelder etterlevelse av finansforetakslovens⁶ bestemmelser om kontanttilbud. Finanstilsynet vil også følge opp at bankene har etablert løsninger i tråd med finansforetaksforskriftens bestemmelser om løsninger for å møte økt etterspørsel etter kontanter i en krisesituasjon⁷.

⁶ Lovdata: [Lov om finansforetak og finanskonsern \(finansforetaksloven\)](#)

⁷ Lovdata: [Forskrift om finansforetak og finanskonsern \(finansforetaksforskriften\)](#)