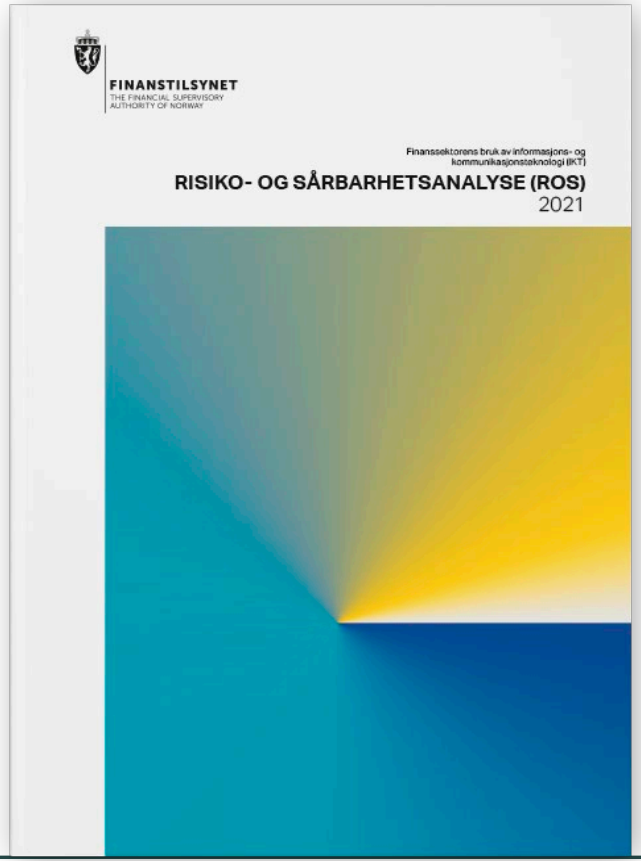
FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Risiko- og sårbarhetsanalyse (ROS) 2021

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi

Olav Johannessen, Seksjonssjef tilsyn IT og betalingstjenester, Pressebrief 12. mai 2021



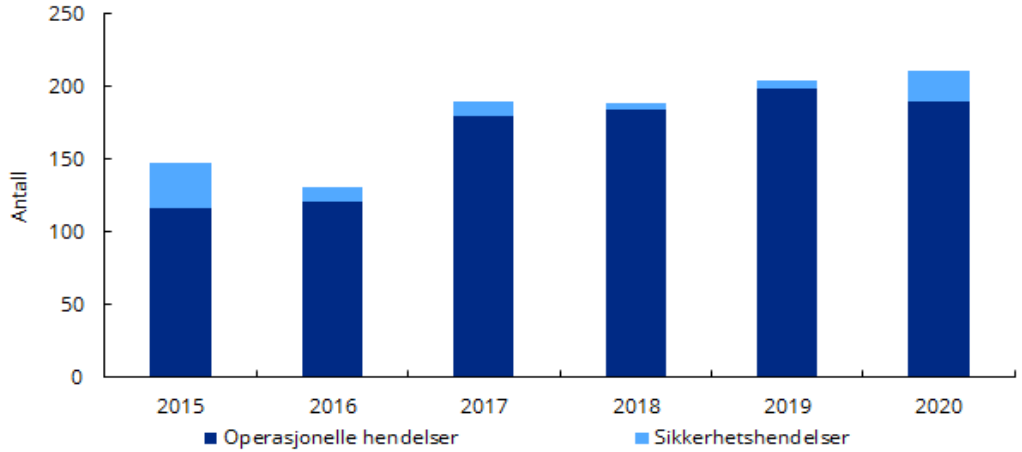
- ✓ **Hendelser**
- ✓ **Svindel**
- ✓ **Funn og observasjoner**
- ✓ **Utkontraktering IKT-virksomhet**
- ✓ **Koronapandemien**
- ✓ **Digital kriminalitet**
- ✓ **Cyber robusthet**
- ✓ **Regelverk**
- ✓ **Foretakenes vurderinger**
- ✓ **Risiko knyttet til digitale tjenester**
- ✓ **Risiko knyttet til betalingstjenester**
- ✓ **Risikobildet**
- ✓ **Hovedfokus tilsyn**
- ✓ **Oppsummerende vurdering**

- Den norske finansielle infrastrukturen er robust
- Ingen IKT-hendelser i 2020 med konsekvenser for finansiell stabilitet
- Tilgjengeligheten til tjenestene samlet sett tilfredsstillende i 2020
- Omfanget av digital kriminalitet øker, ingen alvorlige konsekvenser
- Nedgang i tap ved svindel fra 2019
- Nye ledd i betalingskjeden gir ny risiko


Foto: Einar Aslaksen

Rapporterte hendelser

- Ingen IKT-hendelser med konsekvenser for finansiell stabilitet
- Høyere antall hendelser i 2020 enn i 2019
  - Flere sikkerhetshendelser i 2020 enn tidligere år
  - Lavere antall operasjonelle hendelser i 2020 enn i 2019
- Tilgjengeligheten til tjenestene noe lavere i 2020 enn i 2019



	Operasjonelle hendelser rapportert	Sikkerhets hendelser rapportert
2015	116	32
2016	121	10
2017	180	10
2018	184	5
2019	200	6
2020	190	21

Kilde: Finanstilsynet

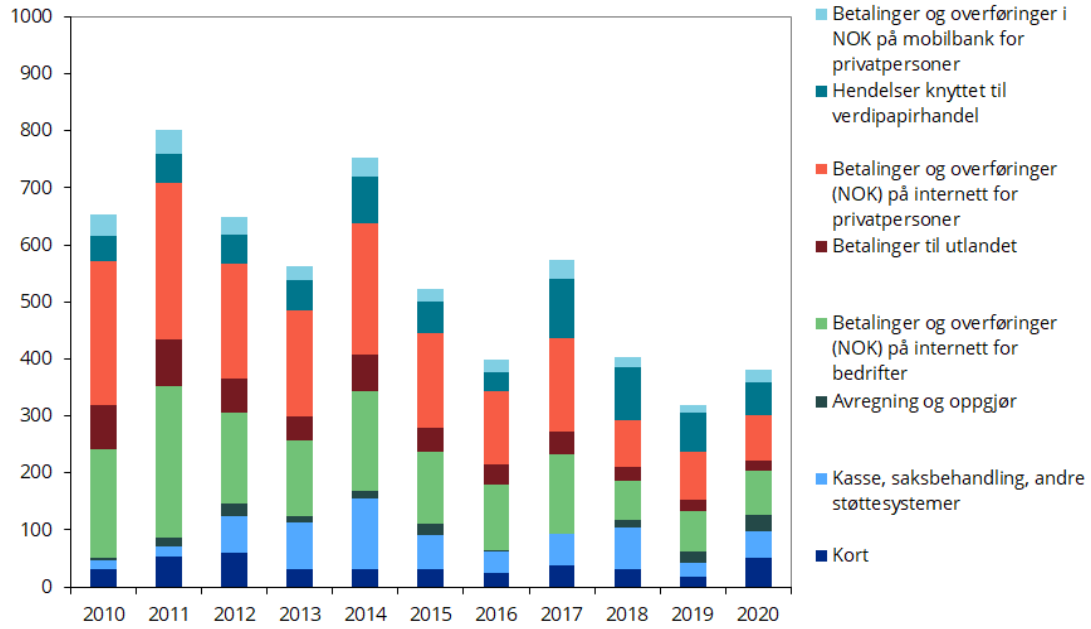
Hendelser med alvorlige konsekvenser

- Driftshendelse i DNB i juni
- Driftshendelse hos Nets i juli
- Hendelser hos felles leverandører
- Avvik i foretakenes AML-systemer
- 21 av de 211 rapporterte IKT-hendelsene i 2020 var såkalte sikkerhetshendelser
  - DDoS-angrep
  - utnyttelse av sårbarhet i applikasjon
  - omfattende phishingkampanjer med misbruk av finansforetaks navn og logo
  - falsk passorddistribusjon
  - angrep med infisert programvare
- Avdekkede sårbarheter
- Foretakenes proaktive arbeid med IKT-sikkerhet viktig
- *Hendelser knyttet til kontotilbyderes grensesnitt*

Hendelser – tilgjengelighet

Tilgjengeligheten til betalingstjenestene og øvrige kunderettede løsninger var noe lavere i 2020 enn i 2019

Dette er vurdert:
antall brukere som er rammet, hendelsens varighet, i hvilken grad kunden lider skade som følge av hendelsen, tilgang til alternative tjenester



Kilde: Finanstilsynet

Tap ved svindel og angrep mot betalingstjenester

(tall i hele tusen)		2015	2016	2017	2018	2019	2020
TOTAL SVINDEL BETALINGSKORT		188 659	206 503	145 591	148 732	189 147	147 602
ANTALL KORT RAMMET AV MISSBRUK	(H1 2019)	38 541	44 900	68 162	65 024	34 999	
ANTALL TRANSAKSJONEER MED MISSBRUK	(H2 2019)					110580	205 000
TOTAL SVINDEL NETTBANKER	(H1 2019)	12 548	18 631	7 587	26 840	3 637	
TOTAL SVINDEL KONTOBETALINGER	(H2 2019)					301 000	355 000
TAP VED SOSIAL MANIPULERING					298 000	500 000	295 000

(tall i prosent)	2019H2	2020
SVINDEL BETALINGSKORT AV TOTAL TRANSAKSJONSVERDI	0,018	0,016
SVINDEL BETALINGSKORT VED NETTHANDEL AV TOTAL TRANSAKSJONSVERDI	0,089	0,06
SVINDEL BETALINGKORT AV TOTALT ANTALL TRANSAKSJONER	0,0068	0,008
SVINDEL KONTOBETALINGER AV TOTAL TRANSAKSJONSVERDI (1)	0,000137	0,00016
(1) SVINDEL KONTOBETALINGER OMFATTER OGSÅ TAP VED SOSIAL MANIPULERING		

Funn og observasjoner fra tilsynsvirksomheten

Svakheter og sårbarheter som utgjør risiko for at alvorlige hendelser kan inntreffe

Det er gjennom tilsynene blant annet pekt på

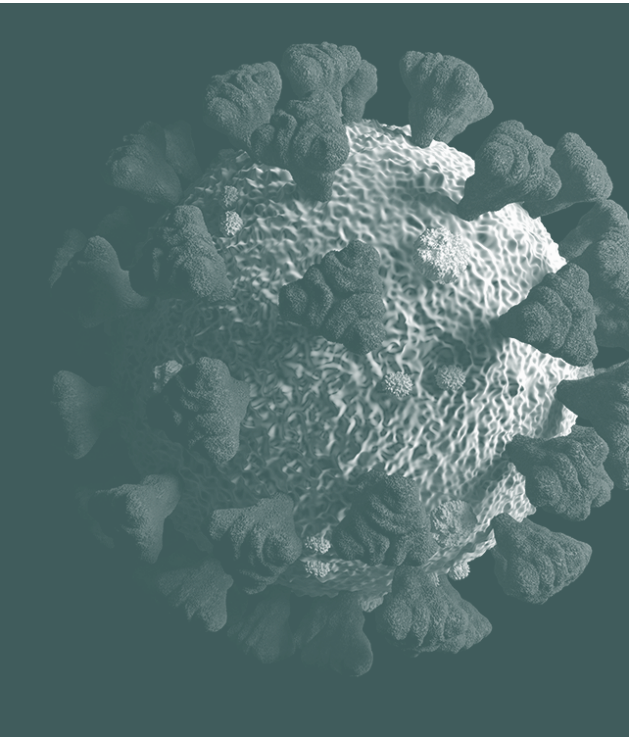
- svakheter i foretaks arbeid med IKT-risiko
- leverandøravtaler ikke gir foretak rett til å kontrollere leverandøren
- risiko ved at leverandører har samtidig ansvar for applikasjonsutvikling og tilganger i produksjonsmiljøet
- utilstrekkelig oppfølging av tilgangene til ansatte hos leverandører
- mangler i foretakenes transaksjonsovervåkningløsninger for å avdekke hvitvasking og terrorfinansiering
- utfordringer i styring og kontroll av IT-virksomheten der foretak er del av en gruppe.
- svakheter innen kontinuitets- og kriseledelse blant annet ved
  - utarbeidelse av forretningsmessige konsekvensanalyser (BIA) som grunnlag for kriseløsningene
  - at tester og øvelser ikke omfatter scenarioer som omfatter både tekniske avbrudd og ondsinnede angrep
  - utilstrekkelig testing av flytting av drift til sekundært driftssted

Utkontraktering av IKT-virksomhet

- Finanstilsynet mottok i 2020 over 250 meldinger om ny eller endret utkontraktering
  - En del av meldingene ble gitt fra samarbeidende grupper
- Utkontraktering i forbindelse med konsesjonsbehandling
- Flest meldinger gjaldt knyttet til leverandører av felles betalingsinfrastruktur og -løsninger til bankene
  - Nets' salg av konto-til-konto-tjenester til Mastercard
  - Vipps' planlagte flytting av driften av BankID
  - Oppstart av "Kontanttjenester i butikk"

  Behov for omfattende oppfølging
- Fortsatt økt bruk av skytjenester
- Flere plattformer, økt kompleksitet og mer sammensatt risikobilde
- Kvaliteten på arbeidet med utkontraktering og kvalitet på avtalene synes å øke
- Forankring av avtaler i egen ledelse bedre
- Nye foretak ikke like godt kjent med regelverket
- Databehandleravtale ikke dekkende for rett til innsyn og tilsyn etter finans regelverket

Oppfølging av koronapandemi-situasjonen



- Virksomheter som støtter viktige funksjoner
- Kritiske samfunnsfunksjoner, jf. DSB
  - Sikker formidling av kapital nasjonalt og til og fra utlandet
  - Gjennomføre betalinger og andre finansielle transaksjoner
  - Opprettholde tilgang til nødvendige betalingsmidler
- Hyppige møter i BFI
- Foretakene god kontroll på driftssituasjonen
  - Endringsregimer
- Gode beredskapsplaner
- Raskt iverksatt nødvendige tiltak
  - Hjemmekontor

Digital kriminalitet

- Fortsatt betydelig økning i angrep, digital kriminalitet, mot foretakenes systemer
- Systemer for overvåking blir stadig bedre
- Som oftest avverges angrepene før de får konsekvenser
- Ingen sikkerhetshendelser innen finansnæringen som kan kategoriseres alvorlig eller kritisk
- Hendelser i 2020 avdekket alvorlige sårbarheter
- Mest aktuelle truslene for Norge og norske interesser er nettverksoperasjone
- Foretakene må fortsette sitt gode arbeid med å kartlegge risiko- og sårbarheter, iverksette preventive tiltak og forberede seg på å måtte håndtere angrep og følgeskadene av slike angrep
- For å forebygge skader ved angrep, er det viktig at foretakene kartlegger hvilke verdier som kan være utsatt
- Samhandling gjennom NFCERT gir gevinster

Cyber-robusthet

TIBER-NO – rammeverk for testing av cybersikkerhet i finanssektoren

- Finanstilsynet og Norges Bank samarbeider om implementering og bruk av TIBER-NO
- Målsettingen er å bidra til finansiell stabilitet gjennom økt motstandsdyktighet mot cyberangrep for kritiske funksjoner i det norske finansielle systemet
- Forslag til rammeverk er sendt på høring
- Rammeverket er ikke et verktøy for tilsyn og overvåking av foretak og enkeltsystemer

DORA – Digital Operational Resilience act

- Foreslått EU-regelverk
- Skal sikre at alle deltakere i det finansielle systemet har de nødvendige tiltak på plass for å redusere faren for cyberangrep og andre risikoer
- Omfatter bredt spekter av foretakstyper
- IKT-forskriften stiller en rekke av de samme kravene
- Et av kravene er testing av operasjonell motstandsdyktighet tilsvarende TIBER-NO
- Åpner opp for deling av informasjon og etterretning knyttet til cybertrusler

Regelverk IKT-sikkerhet

- Veiledning om utkontraktering
- EBAs retningslinjer om IKT-sikkerhet og -risiko
- EIOPAs retningslinjer om utkontraktering til skytjenesteleverandører
- EIOPAs retningslinjer om IKT-sikkerhet og governance
- ESMAs retningslinjer om utkontraktering til skytjenesteleverandører
- Forslag til regelverk om digital operasjonell motstandsdyktighet
- Forslag til endringer i forskrift om unntak fra meldeplikt ved utkontraktering
  - Flere foretak
  - Kritisk og viktig

Foretakenes vurdering av risiko

De mest fremtredende vurderingene:

- Kompleksitet i systemporteføljen, Teknisk gjeld og IKT-porteføljen fordelt på flere plattformer
- Tilgang til kompetanse, særlig IKT-sikkerhets kompetanse
- Mengden av ny eller endret regulering med behov for IKT-endringer
- Mangelfull oversikt over virksomhetskritisk IKT-utstyr og programvare
- Mangelfull oversikt over de ulike kontroll-tiltakene knyttet til IKT-virksomheten
- Betalingstransaksjoner ikke blir fanget opp av systemene for transaksjonsovervåking
- Mer krevende trusselbilde og økning i digitale angrep
- Sårbare betalingstjenester

Risiko knyttet til kundenes tilgang til digitale tjenester

ID-løsninger

- Manglende reservasjonsmuligheter
  - Mot bruksområder
  - Redusere mulighetsrommet for misbruk
- Tilliten til ID-løsninger, liten grad av supplerende kontroller i samsvar med risikoen
- BankID "universalnøkkel"
- BankID benyttes "overalt hele tiden"
  - Fare for redusert årvåkenhet
  - Lurt til falske innlogginger

Betalingstjenester

- Funksjonalitet blir automatisert og integrert i betalingstjenestene
- Vanskelig for brukerne å overskue konsekvensene ved endringer i "relasjoner"
  - Eksempel er parkeringsapper
- Mangel på informasjon om betalingstjenester, kan innebære en risiko for at brukerne ikke får gjennomført kjøp
  - Eksempel er kjøp av billett i Ruter app etter krav om SKA

Risiko knyttet til betalingstjenester ifm. PSD2

Konkurransemessige forhold

- Tilgang til betalingskonto
- Autentiseringsmekanismer
- Avtaler

Mulige sårbarheter knyttet til nye tjenester og nye aktører

- Nye aktører har ikke nødvendigvis samme erfaring som etablerte
- Reglene for sikker kommunikasjon og autentisering og tilsyn er de samme
- Nye tjenester øker risikoen for at kriminelle kan gå via tredjeparter, som kan ha svakere kontrollmiljø og lavere sikkerhet
- Nye aktører innebærer risiko for ugyldige sertifikater
- Nye aktører kan ha en risiko knyttet til etterlevelse av pliktene etter hvitvaskingsloven

Finanstilsynets oppsummerende vurdering av risikobildet - Foretakene

De ulike risikoområdene er klassifisert etter sannsynlighet for at en uønsket hendelse oppstår og konsekvensene dersom hendelsen oppstår.

- **Finanstilsynets vurderer fortsatt risikoen knyttet til sårbarheter i**
  - **Forsvarsverk mot digital kriminalitet**
  - **Driftsløsninger**

  som de to mest sentrale truslene knyttet til foretakenes bruk av IKT

- **Risikoen knyttet til sårbarheter ved skjerming av konfidensiell informasjon er også en sentral trussel**

Digital kriminalitet

Område	Sårbarheter og trusler som kan utgjøre en risiko for uønskede hendelser	Trend
Digital kriminalitet	Manglende sikkerhetstester, sikkerhetsoppdateringer, opplæring og bevisstgjøring av ansatte samt mangelfull overvåking av aktiviteter i egen tekniske infrastruktur, herunder nettverk og systemer, kan føre til at kriminelle påfører foretaket skade gjennom digitale angrep.	↗

Manglende

- Sikkerhetstester
- Sikkerhetsoppdateringer
- Opplæring
- Bevisstgjøring
- Overvåking av teknisk infrastruktur; nettverk og systemer

kan føre til uønskede hendelser


Foto: Colourbox

Hovedtema for tilsynsvirksomheten på IKT- og betalingstjenesteområdet fremover

- Styring og kontroll med IKT-virksomheten
- Organisering av IKT-/cyber-sikkerhetsarbeidet
- Sikkerheten knyttet til IKT-løsninger
- Beredskapsarbeid og testing av kontinuitets- og kriseløsninger
- Styring, kontroll og oppfølging av utkontraktert IKT-virksomhet
- Betalingstjenester, herunder etterlevelse av det reviderte betalingstjenestedirektivet
- Sikkerheten i betalingstjenestene og kunderettede løsninger
- IKT-løsninger for å avdekke hvitvasking og terrorfinansiering
- Tilbud av kontanttjenester og kontantberedskap
- Oppfølging av IKT-hendelser
- Beredskapsarbeid rettet mot digital sårbarhet og digital sikkerhet
- Trusselbildet knyttet til digital kriminalitet

Oppsummering

- Den norske finansielle infrastrukturen er robust
- Tilgjengeligheten til tjenestene samlet sett tilfredsstillende, men noe dårlige i 2020 enn i 2019
- Tap ved svindel er redusert fra tidligere år
- Svindel med sosial manipulering synes fortsatt å være en lukrative metode for de kriminelle
- Kompleksiteten i den tekniske infrastrukturen øker og IKT-porteføljen er fordelt på flere systemplattformer, gir risiko på flere områder, bl.a. økt risiko for IKT-driften
- Kvaliteten på arbeidet med utkontraktering og kvalitet på avtalene synes å øke, bl.a. er forankring av avtaler i egen ledelse blitt bedre
- Fortsatt anses sårbarheter knyttet til foretakenes forsvarsverk mot digital kriminalitet, driftsløsninger og skjerming av konfidensiell informasjon som de mest sentrale truslene knyttet til foretakenes IKT-virksomhet
- Korona-situasjonen viste at de sentrale foretakene i den norske finansielle infrastrukturen har gode beredskapsplaner og kan raskt iverksette nødvendige tiltak
- Det digitale trusselbildet er økende og gis større oppmerksomhet, bl.a. samarbeider Finanstilsynet med Norges Bank om etablering av rammeverk for testing av cybersikkerhet og EU har foreslått nytt regelverk om digital operasjonell motstandsdyktighet
- Foretakene bør fortsatt styrke arbeidet på IKT-området, både for å redusere sannsynligheten for avvik og for å forbedre IKT-sikkerheten

FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY