FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Risiko og sårbarhetsanalyse

Nytt på reguleringsfronten for betalingsformidling

TIBER-NO

Olav Johannessen, Betalingsformidlingskonferansen 05. November 2020

Risiko og sårbarhetsanalyse

2020

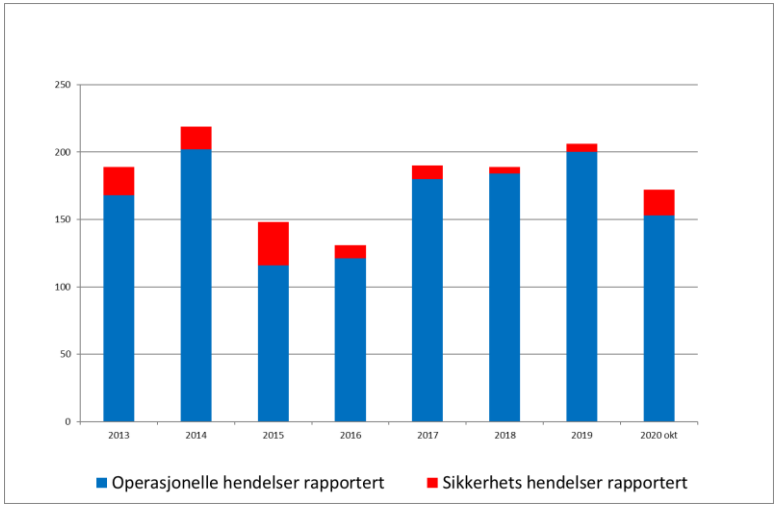
Oppsummering ROS 2020

- Den norske finansielle infrastrukturen er robust
- Tilgjengeligheten til tjenestene samlet sett bedre i 2019 enn i 2018, og tilfredsstillende
- Angrep (digital kriminalitet) mot foretakenes systemer øker betydelig fra år til år. Angrepene avverges som oftest før de får konsekvenser for foretaket
- Korona-situasjonen viste at de sentrale foretakene i den norske finansielle infrastrukturen har gode beredskapsplaner og kan raskt iverksette nødvendige tiltak
  - Foretakene må ta høyde for at tilsvarende og mer alvorlige kriser, inklusive med geopolitiske konsekvenser, kan inntreffe i fremtiden
- Foretakene bør fortsatt styrke arbeidet innen IKT-området, både for å redusere sannsynligheten for avvik og for generelt å forbedre IKT-sikkerheten
- Foretakene har blitt bedre til å håndtere utkontrakteringsavtaler
- Svindel med sosial manipulering øker betydelig. Lukrative metode for kriminelle
- Øvrig svindel øker. Utgjør liten andel av total transaksjonsverdi
- Kompleksiteten i den tekniske infrastrukturen øker og gir risiko på flere områder
- Fortsatt anses sårbarheter knyttet til foretaks forsvarsverk mot digital kriminalitet og informasjons-lekkasje, samt IKT-drift, som de mest sentrale truslene knyttet til foretakenes bruk av IKT

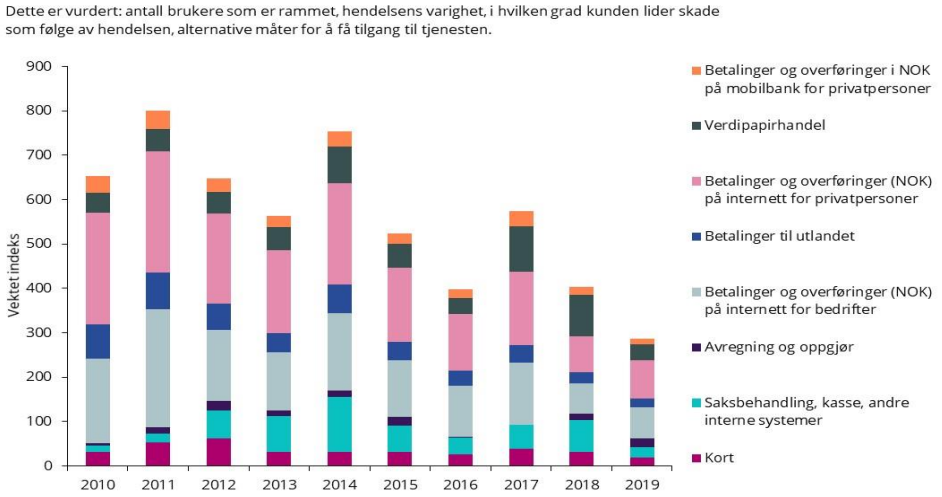
Rapporterte hendelser

Foretakene rapporterte 206 IKT-hendelser i 2019, som er 17 flere enn året før

- Antall rapporteringspliktige foretak økte fra 2018 til 2019
- Flere av de rapportert hendelsene gjaldt samme hendelse hos foretakenes felles leverandør
- Tilgjengeligheten til betalingstjenestene og øvrige kunderettede tjenester noe bedre i 2019 enn i 2018



Kilde: Finanstilsynet



Kilde: Finanstilsynet

Tap som følge av svindel og angrep mot betalingstjenester

(tall i hele tusen)	2014	2015	2016	2017	2018	2019H1	2019H2
TOTAL SVINDEL BETALINGSKORT	164 112	188 659	206 503	145 591	148 732	94 466	94 681 189 047
HERAV SVINDEL MED KORT VED NETTHANDEL	72 056	98 410	137 015	102 980	114 932	76 546	49 282 125 828
TOTAL SVINDEL NETTBANKER (antall)	11 200	12 548	18 631	7 587	20 187	3 637	
TOTAL SVINDEL KONTOBETALINGER							46 500 301 629
ANTALL KORT RAMMET AV MISBRUK H1	38 541	44 900	68 162	65 024	34 999	39 918	
ANTALL TRANSAKSJONEER MED MISBRUK H2							110 580
TAP VED SOSIAL MANIPULERING					300 000		*500 000*

28% økning

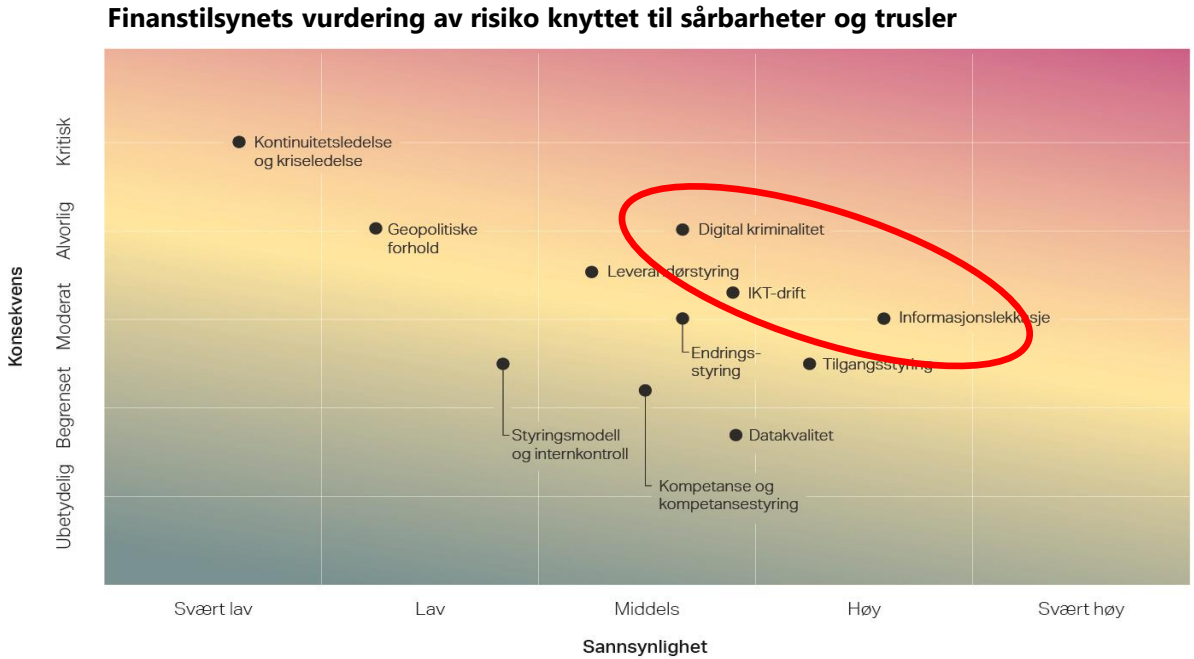
2016-nivå

(tall i prosent)	2019H2
SVINDEL BETALINGSKORT AV TOTAL TRANSAKSJONSVERDI	0,02
SVINDEL BETALINGSKORT VED NETTHANDEL AV TOTAL TRANSAKSJONSVERDI	0,09
SVINDEL BETALINGKORT AV TOTALT ANTALL TRANSAKSJONER	0,007
SVINDEL KONTOBETALINGER AV TOTAL TRANSAKSJONSVERDI (1)	0,000147
(1) SVINDEL KONTOBETALINGER OMFATTER OGSÅ TAP VED SOSIAL MANIPULERING	

Enkelte funn fra tilsynsvirksomheten, alle tilsynsområder

- Mangler ved styring og kontroll med foretakets IKT-virksomhet og utkontraktert virksomhet
- Utilstrekkelig oppfølging av leverandører, spesielt etterlevelse av foretakets sikkerhetskrav
- Mangler i oppdatering og forbedring av sikkerhetsdokumentasjon. Manglende kontroll med at egne sikkerhetskrav etterleves
- Mangelfulle rutiner for informasjonsklassifisering og beskyttelse
- Risikoanalyser av IKT-virksomheten avdekker ikke reell risiko
- Svakheter i organisering av sikkerhetsarbeidet
- Svakheter i kontinuitets- og kriseledelse, og kriseløsninger
- Behov for å bedre forberedelsene på å håndtere en evt. alvorlig cyber-hendelse
- Mangler ved rutinene for sikkerhetstesting
- Svakheter i kontrollen med uttrekk til AML-systemene

Oppsummerende vurdering av risikobildet knyttet til sårbarheter og trusler i foretakenes IKT-virksomhet



Foretakenes egne vurderinger av risiko

- Økende kompleksitet i systemporteføljen medfører risiko og innebærer bl.a. følgende utfordringer:
  - Arbeidet med å utforme gode kriseløsninger kompliseres
  - Logger fra ulike systemer kan være vanskelig å sammenholde og svekker muligheten for å utnytte informasjonen i loggene
  - Etablere et helhetlig forsvar mot elektroniske angrep
  - Komplisert og tidkrevende feilsøking
  - Komplisert, omfattende og krevende arbeid med risikoanalyser
  - Manglende datakvalitet

  Risikoen vurderes likevel som minkende
- Digitale angrep anses som en alvorlig og aktuell risiko
- Manglende sikkerhetsbevissthet øker faren for at angrep lykkes
- Leveransepresset anses som en risiko, men risikoen antas å bli dempet
- Omfanget av regulatoriske krav, herunder nye krav med kort frist for gjennomføring, som en betydelig utfordring og risiko


Foto: Colourbox

Noen andre forhold fra årets rapport

Digital kriminalitet

- Fortsatt betydelig økning i digitale angrep mot foretakene
- Systemer for overvåking stadig bedre og angrepene avverges før de får konsekvenser
- Skillet mellom trusselen fra organiserte kriminelle og fremmed etterretning viskes stadig mer ut
- Etablering av rammeverk for sikkerhetstesting

Utkontraktering IKT-virksomhet

- 135 meldinger + ifm. konsesjonsbehandling
- Meldingene blitt mer omfattende og kompleksiteten i utkontrakteringsforholdene økt
- Bedre håndtering av utkontrakteringsavtalene
- Fortsatt klar tendens til økt bruk av skytjenester
- Økende kompleksitet i foretakenes løsninger pga. multi-sourcing

Meldinger betalingstjenester

- 21 meldinger om endrede / nye betalingstjenester
- 30 søknader knyttet til reautorisering og/eller konsesjon til å yte betalingstjenester
  - Flere foretak manglende forståelse av regelverket og behov for å vesentlig forbedre sine rutiner
- Fritak for reserveløsning iht PSD 2
- Utsatt frist for SKA ved bruk av betalingskort v/netthandel

Risiko knyttet til kundenes tilgang til digitale tjenester

- BankID "universalnøkkel"
- BankID brukes på mange forskjellige tjenester, og ofte uten ytterligere kontroller for å forhindre misbruk
- De fleste finansielle tjenestene er basert på selvbetjening
  - Stiller store krav til IKT-drift og informasjonssikkerhet
  - Krav til god oppfølging av kunder ved avvik i bruk av tjenestene
- Digitaliseringen gitt enkelte kundegrupper utfordringer

Nytt på reguleringsfronten for betalingsformidling

Regelverk

- EU kommisjonen vedtatt sin "Digital Finance Package"
  - "Digital Finance Strategy" og "Retail Payment Strategy"
  - PSD2 og EMD2
- EBAs Retningslinjer om utkontraktering og FTs Rundskriv om Utkontraktering
- EBAs Retningslinjer om IKT-sikkerhet
  - ~~EBAs retningslinjer for operasjonell og sikkerhetsrisiko under PSD2~~
- EBAs Retningslinjer for autorisering under PSD2
- EBAs Retningslinjer om rapportering av hendelser under PSD2
- Retningslinjer for begrenset nettverk under PSD2
- Forskrift om formidlingsgebyrer
- Forordning om gebyrlikhet nasjonale og grensekryssende betalinger
- AMLD4
- Antatt oppstart revidering av direktivet om endelig avregning i Q4 2020

"Retail Payment Strategy"

Bygger på 4 hovedpilarer

- Flere digitale løsninger og straksbetalingsløsninger
  - Sikre et bredt utvalg av sikre, billige, raske og sømløse betalingsløsninger
  - Støtte/utvikle europeiske/paneuropeiske betalingsløsninger
  - Paneuropeisk kortordning (card scheme)
- Innovative og konkurranse dyktige betalingsmarkeder
  - Revidering av PSD2
  - Utnytte potensialet i open banking
- Effektive og interoperatible betalingsløsninger og støttende infrastruktur
  - Innta betalings- og e-pengeforetak i finalitetsdirektivet
- Effektive internasjonale betalingstjenester
  - Forbedre betalinger over landegrensene med land utenfor EU

PSD2 → "PSD3"

- Vil bli revidert ila 2021, antakelig bli publisert Q1 2022
- Vil ta hensyn til erfaringene fra implementeringen av PSD2
- Justeres der det er nødvendig
  - ✓ Forbrukerbeskyttelse
  - ✓ Virkningen av gebyrer
  - ✓ Maksimumsgrenser ved NFC
- Vurdere om nye, uregulerte, aktører bør bli omfattet
  - ✓ PSD2 gjør unntak for tekniske tjenesteytere
- Forhold holdt utenfor PSD2 vil bli vurdert inntatt ifm revideringen
- Ta med erfaringene fra Wirecard-skandalen
- Inkludere e-pengeutstedelse (e-pengedirektivet) som del av revideringen
- Sikre et høy sikkerhetsnivå, sterk kundeautentisering kanskje ikke tilstrekkelig
- Forbedret bruk av eID-løsninger
- Økt gjennomsiktighet

"Digital Finance Strategy"

- Finanstjenestene skal bli mere digitale, fragmenteringen av finansielle tjenesteytelser skal reduseres og adgang til grensekryssende tjenester skal sikres
- Lovgivningen skal stimulere til innovasjon og konkurranse mellom finansielle tjenesteleverandører og sikre markedseffektivitet
- Fremme datadeling og datadreven innovasjon iht datastrategien og stimulere til open finance
- Nye utfordringer og risikoer som er forbundet med den digitale omstillingen skal håndteres

- Sikre like vilkår for leverandører av finansielle tjenester, det være seg tradisjonelle banker eller teknologiselskaper: samme aktivitet, samme risiko, samme regler

- Forslag til lov om krypto-eiendeler (MiCA)
  - Utnytte muligheter og redusere risiko
- Forslag til lov om digital operasjonell motstandsdyktighet (DORA)
  - Redusere (konsekvensen av) digitale angrep og andre risikoer
  - Håndtere alle typer driftsforstyrrelser

MiCA – Markets in Crypto-Assets

- Omfatter regulering av
  - Krypto-aktiva – utility tokens
    - ✓ Digital representasjon av en verdi eller rett som kan overføres og lagret elektronisk
  - Aktiva-baserte tokens
    - ✓ Krypto-aktiva basert på en eller flere fiat valutaer eller varer eller krypto-aktive eller kombo
  - E-penge tokens (inkluderer e-penger)
    - ✓ For bruk til veksling/betaling basert på en fiat valuta
- Omfatter ikke krypto-aktiva klassifisert som finansielle instrumenter (MiFiD)

- Skal adressere
  - Risiko knyttet til forbrukerbeskyttelse, investorbeskyttelse og markedets integritet
  - Særskilte risikoer knyttet til finansiell stabilitet og pengepolitikk mhp stable coins
- Skal bidra til innovasjon og juridisk klarhet
- Virkeområdet er uregulerte krypto aktiva (aktører)

- Regler for pilotregime (sandkasse) for markeds infrastrukturer basert på DLT

DORA – Digital Operational Recilience Act

- Governance
- Styring av IKT-risiko
- Rapportering av større IKT-relaterte hendelser
- Testing av digital operasjonell motstandsdyktighet
- Utkontraktering, tredjeparts IKT-risiko og overvåkningsrammeverk
- Deling av informasjon og etterretning ift cybertrusler og sårbarheter

IKT-forskiften

- ✓ § 2 Organisering
- ✓ § 3 Risikoanalyse
- ✓ § 9 Avviks- og endringshåndtering
- ✓ § 11 Driftsavbrudd og kriseberedskap
- ✓ § 12 Utkontraktering
- ✓ NFCERT

- *Bestemmelser for myndighetene, bl.a. sektorovergripende beredskapstesting og sanksjoner*

Testrammeverk

TIBER-NO

Testing av digital operasjonell motstandsdyktighet (DORA)

- Mangel på felles regelverk
- Felles regelverk viktig for grensekryssende virksomheter
- Alle skal teste regelmessig, jf. krav i IKT-forskriftens § 11 Driftsavbrudd og kriseberedskap
- Testkravene høyere for "signifikante" foretak
- Kun "signifikante" foretak vil bli krevd å gjennomføre såkalt avansert testing (TLPT) etter foreslått regelverk
  - Noen områder viktigere enn andre: Eks. Betaling, banker, avregning og oppgjør
  - Minimum hvert tredje år
  - Minimum kritiske funksjoner og tjenester
  - Scope skal valideres av tilsynsmyndigheten(e)
  - Resultat skal forelegges tilsynsmyndigheten(e), valideres og utstede attest
- Det skal utarbeides nærmere regelverk for TLPT av ESAene
  - Skal ses hen til eksisterende relevante rammeverk for TLPT
- Tre i kraft først 36 mnd etter fastsettelse → Flere år frem i tid

TIBER-NO

- Norges Bank og Finanstilsynet igangsatte høsten 2019 er arbeid med TIBER-NO, ble satt noe på hold pga. Korona-pandemien
- Flere foretak og enkelte leverandører ble invitert til å gi innspill, som ble oppsummert i eget informasjonsmøte januar 2020
- Gjenopptatt – antatt ferdigstillelse H1 2020
- Skal utarbeides basert på TIBER-EU og hensynta EUs forslag i DORA om testing av digital operasjonell motstandsdyktighet
- Skal utformes sammen med næringen og relevante myndigheter
- Hensynta at norske finansforetak er små i europeisk målestokk
- Skal inneholde retningslinjer for testing av finansielle institusjoners evne til å oppdage, beskytte seg mot og håndtere avanserte cyberangrep
- Vil styrke cybersikkerheten i finansiell sektor, i påvente av kommende regelverk

FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY