



**FINANSTILSYNET**

THE FINANCIAL SUPERVISORY  
AUTHORITY OF NORWAY

# Pressebriefing 8. mai 2018

## Risiko- og sårbarhetsanalyse (ROS) 2017 Finanssektorens bruk av informasjons- og kommunikasjonsteknologi

Seksjonssjef Olav Johannessen  
Finanstilsynet



**FINANSTILSYNET**  
THE FINANCIAL SUPERVISORY  
AUTHORITY OF NORWAY

Finansforetakenes bruk av informasjons- og  
kommunikasjonsteknologi (IKT)

**RISIKO- OG SÅRBARHETSANALYSE (ROS)**  
2017

# ROS-analysen 2017:

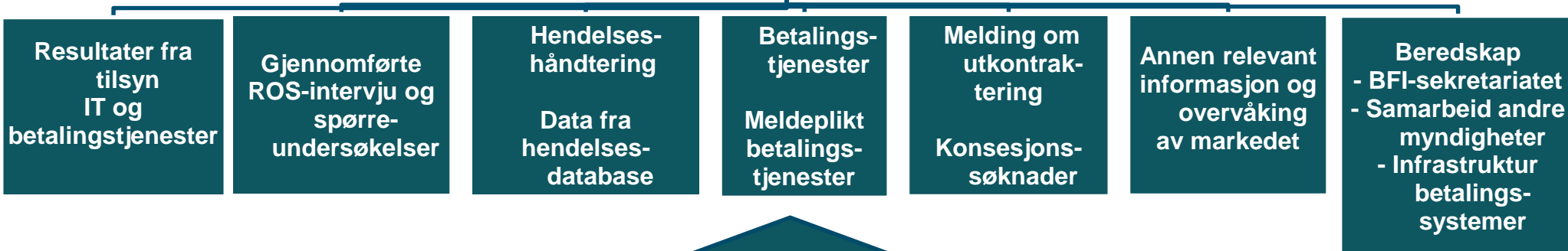
1. Innledning
2. Oppsummering
3. Finanstilsynets funn og vurderinger
4. Aktørenes vurdering av risikofaktorer
5. Finanstilsynets vurdering av risikobildet
6. Finanstilsynets oppfølging

Vedlegg: Ordliste

# Hensikten med den årlige ROS-analysen er å speile risikobildet i finanssektorens bruk av IKT



- Skaffe oversikt
- Analysere
- Foreslå tiltak



**Våre virkemidler**  
**Regelverk, innrapportering og tilsyn**

# 3. Finanstilsynets funn og vurderinger

1. Betalingssystemer og utvikling
2. Bank
3. Verdipapirområdet
4. Forsikring
5. Revisjonsselskaper
6. Tilsyn med etterlevelse av hvitvasking
7. Rapporterte hendelser i 2017
8. Tapstall for betalingsformidlingen
9. Utkontraktering
10. IKT- og informasjonssikkerhet
11. Utviklingstrekk innenfor finansiell teknologi

# Betalingstjenester

- Flere alvorlige hendelser, både i omfang og varighet, for betalingssystemene i 2017.
- Noen av hendelsene førte til at betalingstjenestene var utilgjengelige i opp til et helt døgn for mer enn 30 prosent av bankkundene.
- Det skapte usikkerhet i markedet knyttet til foretakenes evne til kontinuerlig å levere betalingstjenester og gjennomføre betalingsoppdrag.
- Hendelser viste at det for enkelte typer betalingskort ikke er etablert reserveløsninger.
- Betalingssystemene vurderes likevel hovedsakelig som stabile.
- Hendelsene viser at det er rom for forbedringer, særlig innenfor:
  - Kapasitetsovervåking og kapasitetsstyring
  - Kriseløsninger (kontinuitetsløsninger)
  - Styring av operasjonell risiko, særlig ved endringer.
- Bankenes plikt til å sikre kontantdistribusjon i krisesituasjoner er fastsatt.
- Konsolidering i det norske markedet for mobile betalingsløsninger ved etablering av eget betalingsforetak for samarbeid om Vipps, og avvikling av MobilePay og mCASH.
- Foretak og deres leverandører tilpasser virksomheten til det nye betalingstjenestedirektivet PSD 2.
- Utviklingen med bruk av biometriske kjennetegn ifm. autentisering og betaling fortsetter.

- Det er kontinuerlige endringer i trusselbildet for digitale angrep, en risiko som i økende grad utfordrer bankene i arbeidet med å etablere risikoreduserende tiltak.
- Bankene har behov for å forbedre sitt arbeid på IKT-sikkerhetsområdet.
  - Organisering av arbeidet
  - Gjennomføring av risikoanalyser både for egen infrastruktur og for utkontraktert IKT-infrastruktur
  - Ajourføring av sikkerhetsrammeverket
  - Proaktive tiltak for å styrke foretakets forsvarsverk (som patching).
- Risikovurderinger omfatter ikke i tilstrekkelig grad utkontraktert teknisk infrastruktur.
- Styring og kontroll med tilgangsrettigheter, særlige utvidede, må forbedres.
- Kun unntaksvis at avtaler om utkontraktering ikke er i tråd IKT-forskriftens § 12 om utkontraktering.
- Virkelige hendelser har blitt ansett som tilstrekkelig gjennomførte tester av beredskapsløsninger.
- Det er fortsatt behov for forbedringer i bankenes arbeid med å utarbeide forretningsmessige konsekvensanalyser som grunnlag for bankenes krav til kontinuitets- og katastrofeløsninger, selv om det observeres en forbedring.
- Erfaringen fra tilsyn om etterlevelse av bankenes krav til rapportering til Bankenes sikringsfond er at rapporteringen synes å nærme seg en tilfredsstillende kvalitet.

# Verdipapirområdet

- Det har ikke vært kritiske eller svært alvorlige IKT-hendelser på verdipapirområdet i 2017, til tross for at foretakenes systemporteføljer generelt har vært preget av mange og til dels store endringer.
- Systemendringene førte imidlertid til hendelser og avdekket svakheter i foretakenes IKT-systemer, inkludert testsystemer.
- Flere hendelser i verdipapirforetak ble ikke rapportert til Finanstilsynet slik IKT-forskriften krever.
- Ustabilitet i noen banker og verdipapirforetaks e-handelsløsninger for aksjehandel førte til at kunder ikke fikk endret sine porteføljer.
- I forbindelse med etableringen av det nye produktet aksjesparekonto, var det enkelte foretak som etablerte løsninger uten nødvendig funksjonalitet.
- Flere av foretakene har behov for å forbedre sin dokumentasjon av retningslinjer, rutiner og planer for gjennomføring av sikkerhetstester, særlig ved bruk av tredjeparter.
- Ved gjennomgang av meldinger om utkontraktering av IKT-tjenester fra verdipapirforetak og ved stedlige tilsyn er det avdekket mangler i risikovurderinger og i utkontrakteringsavtalene.

- Finanstilsynet erfarer at de fleste forsikringsforetakene har god risikostyring, men at det også er foretak hvor situasjonen ikke er tilfredsstillende.
- Finanstilsynet observerer bruk av løsninger (bl.a. regneark og åpne analyseverktøy) ifm. avsetnings- og lønnsomhetsberegninger som har dårlig eller manglende integrasjonskontroll, dårlige tilgangskontroller og svak endringskontroll.
- Det synes fortsatt å være en underreportering av hendelser fra forsikringsforetak. Dette vil bli fulgt opp gjennom tilsynsarbeidet.
- Ny teknologi tas i bruk ved nye forsikringsprodukter, og dette stiller økte krav til både bruk av og kontroll med innsamlede data og krav til risikovurderinger som identifiserer relevant risiko. Dette gjelder for eksempel ved bruk av sensorteknologi og overvåking av kundeatferd.



- Det er avdekket mangel på skriftlige avtaler om utkontraktering som sikrer tilstrekkelig innsyn og kontroll i den utkontrakterte virksomheten ved konsernintern utkontraktering.

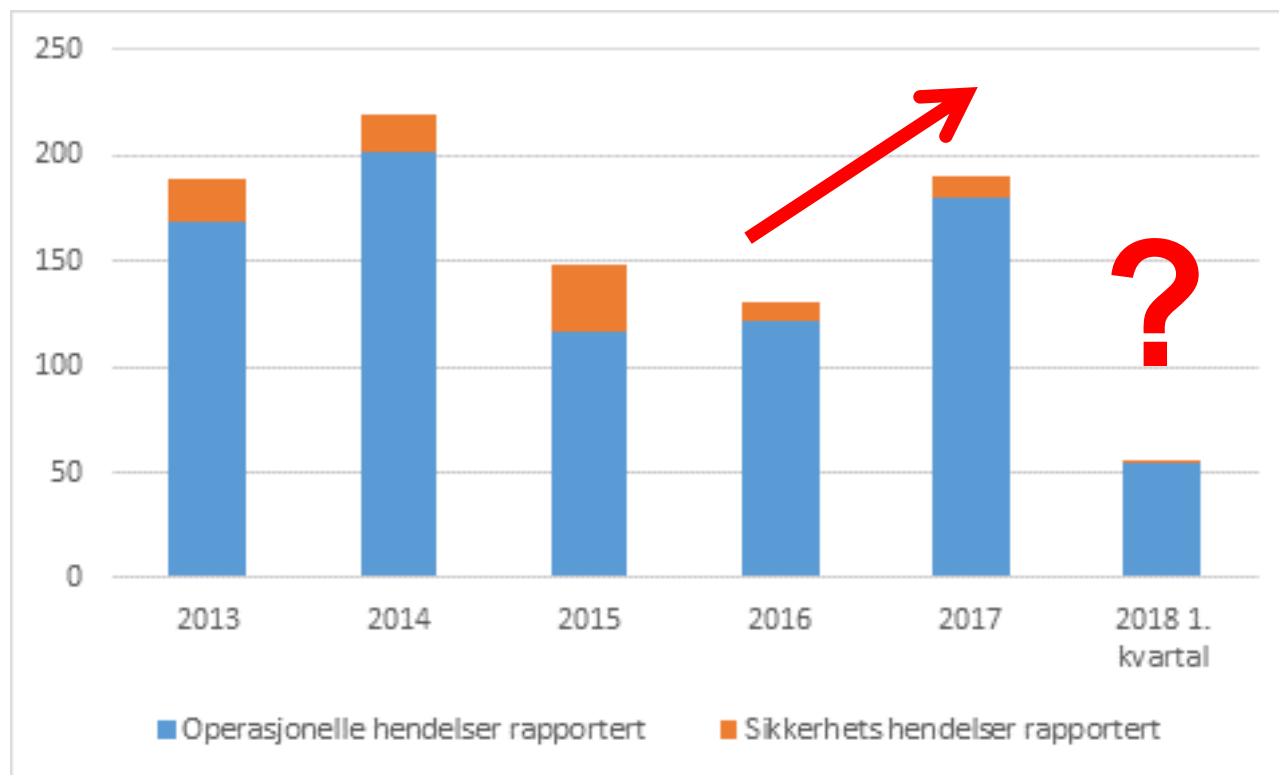
## Tiltak mot hvitvasking

- Det er observert mangelfull dokumentasjon av risikovurderingene som ligger til grunn for de elektroniske kunde- og transaksjonskontrollene.
- Det er påpekt at rutiner for å beslutte en ny elektronisk kontroll, og for å evaluere og følge opp nye/endrede kontroller, skal være formaliserte og dokumenterte for å sikre at kontrollene har rimelig grad av treffsikkerhet.
- Det er påpekt mangler i screening der den til enhver tid sist oppdaterte sanksjonslisten ikke er brukt.

# Det var i 2017 en negativ utvikling i antall hendelser ift. de to foregående årene.

## Plikten til å rapportere hendelser følger av IKT-forskriftens § 9.

- Alvorlige eller kritiske avvik som medfører vesentlig reduksjon i funksjonalitet.
- Avvik der spesielle sårbarheter i applikasjon, arkitektur, infrastruktur eller forsvarsverk avdekkes.



|      | Operasjonelle hendelser rapportert | Sikkerhets hendelser rapportert |
|------|------------------------------------|---------------------------------|
| 2013 | 168                                | 21                              |
| 2014 | 202                                | 17                              |
| 2015 | 116                                | 32                              |
| 2016 | 121                                | 10                              |
| 2017 | 180                                | 10                              |

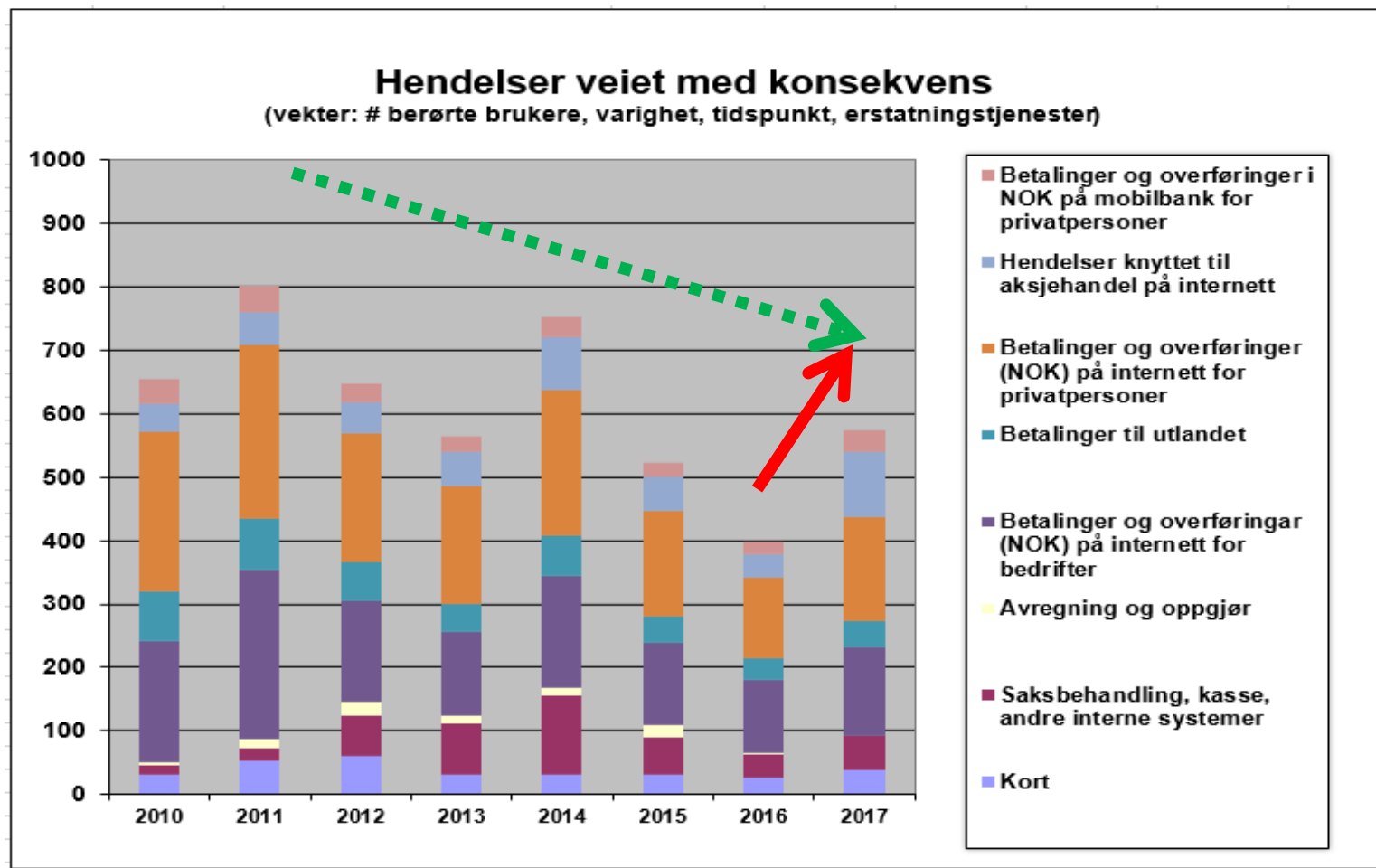
Kilde: Finanstilsynet

# Alvorlige driftshendelser i 2017

| Dato           | Konsekvens  | Varighet | Årsak   |
|----------------|---|----------|---|
| 16.03.17       | Betalingstjenester, kundeløsninger og interne systemer ikke tilgjengelige.  | 15 timer | Feil i styringssystem til lagringsenhet.  |
| 15.06.17       | Betalingstjenester, kundeløsninger og interne systemer ikke tilgjengelige.  | 10 timer | Feil i styringssystem til lagringsenhet oppsto i forbindelse med oppgraderinger.  |
| 04.08.17       | Betalinger mellom personer, og mellom personer og bedrifter fungerte ikke. Kunder opplevde at transaksjoner ble trukket flere ganger. | 18 timer | Feil oppsto i forbindelse med planlagt endring.   |
| 06. - 07.09.17 | Betalingstjenester, kundeløsninger og interne systemer ikke tilgjengelige.  | 23 timer | Feil i forbindelse med UPS-batteri løsninger ved endringer. Da sekundær-løsningen skulle ta over, virket ikke batteriene da sikringene var dimensjonert for lavt. |
| 06.10.17       | Betalingstjenester, kundeløsninger og interne systemer ikke tilgjengelige.  | 24 timer | Feil i styringssystem til lagringsenhet.  |
| 03.11.17       | Nettbank og mobilbank ikke tilgjengelig.  | 20 timer | Feil oppstår etter en endring på kabler i nettverket.   |

Det var også en rekke hendelser gjennom året knyttet til banklagret BankID og BankID på mobil, spesielt på dager med stor belastning på tjenesten.

# Betalingsystemet og kunderettede løsninger var mindre tilgjengelige i 2017 sammenlignet med de to foregående årene.



Kilde: Finanstilsynet

# Tap ved bruk av betalingskort

(tall i hele tusen kroner)

Tabell 1: Tap ved bruk av betalingskort (tall i hele tusen kroner)

| Svindeltype betalingskort   | 2012    | 2013    | 2014    | 2015    | 2016    | 2017    |
|---|---------|---------|---------|---------|---------|---------|
| Misbruk av kortinformasjon, Card-Not-Present (CNP) (Internett-handel m.m.)            | 35 701  | 51 954  | 72 056  | 98 410  | 137 015 | 102 908 |
| Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort i Norge.       | 2 308   | 762     | 524     | 2 670   | 1 360   | 483     |
| Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort utenfor Norge. | 55 869  | 51 534  | 51 685  | 48 447  | 41 762  | 17 452  |
| Originalkort tapt eller stjålet, misbrukt med PIN i Norge.                            | 28 128  | 21 274  | 21 266  | 18 875  | 12 857  | 10 194  |
| Originalkort tapt eller stjålet, misbrukt med PIN utenfor Norge.                      | 8 544   | 9 570   | 13 071  | 14 224  | 10 223  | 9 663   |
| Originalkort tapt eller stjålet, misbrukt uten PIN                                    | 4 603   | 4 949   | 5 510   | 6 033   | 3 286   | 4 891   |
| <b>TOTALT</b>   | 135 153 | 140 043 | 164 113 | 188 660 | 206 503 | 145 591 |

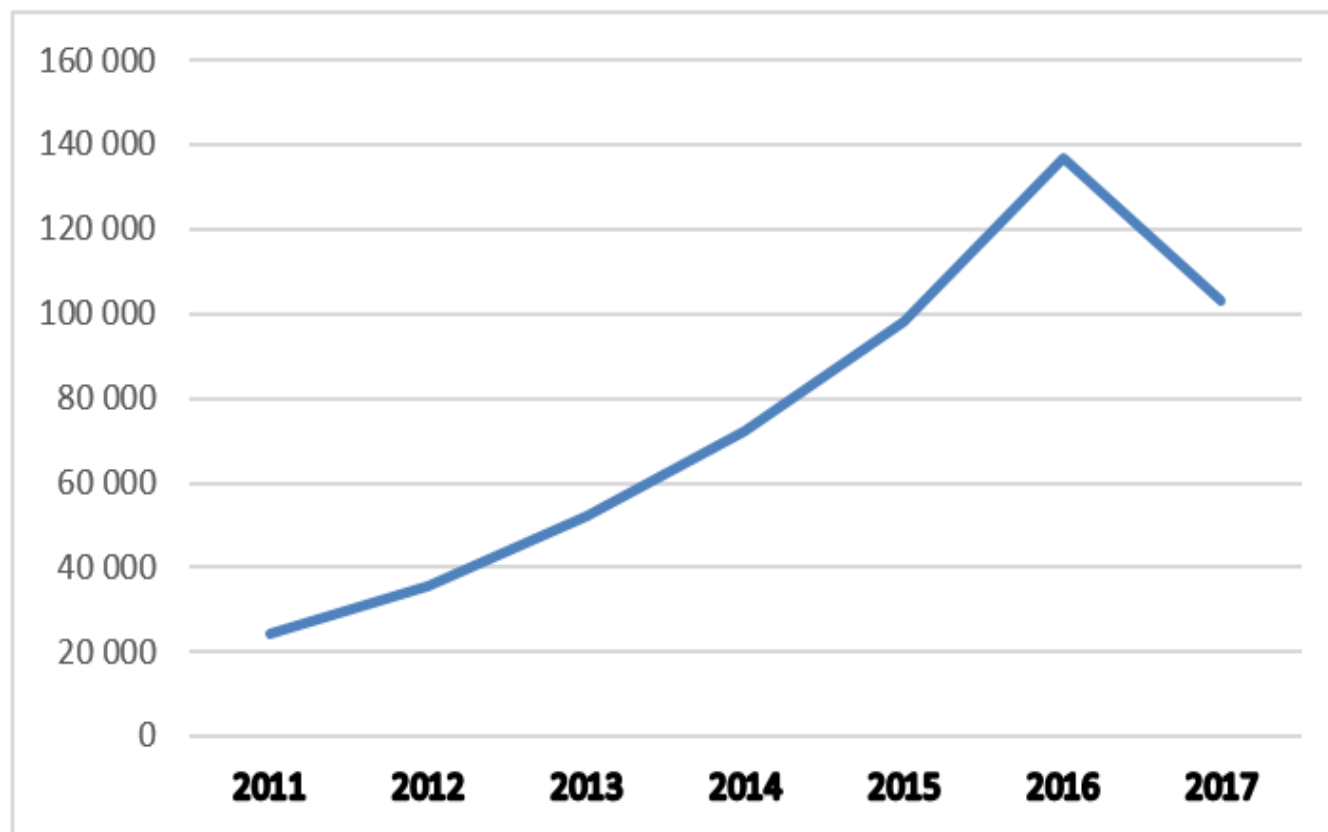
## Antall betalingskort rammet av misbruk

|  | 2012   | 2013   | 2014   | 2015   | 2016   | 2017   |
|--|--------|--------|--------|--------|--------|--------|
| Antall kort rammet av misbruk (antall) | 20 332 | 22 531 | 38 541 | 44 900 | 68 162 | 65 024 |

Kilde: Finanstilsynet og Bits

# De siste års negative utvikling i svindel med misbruk av kortinformasjon ved Card-Not-Present (kort ikke er til stede), ble i 2017 brutt

**Figur1: Utvikling i svindel med misbruk av kortinformasjon der kort ikke er til stede (CNP)**



Svindel med misbruk av kortinformasjon der kort ikke er til stede (CNP) utgjør nær 60% av nedgangen i tap ved bruk av betalingskort .

Kilde: Finanstilsynet og Bits

# Kostnader forbundet med kortsvindel (tall i hele tusen kroner)

Tabell 2: Kostnader forbundet med kortsvindel (beløp i hele tusen kroner)

| Kostnader ved svindel med betalingskort                        | 2012    | 2013    | 2014    | 2015    | 2016    | 2017    |
|--|---------|---------|---------|---------|---------|---------|
| Antall kort rammet av misbruk (antall)                         | 20 332  | 22 531  | 38 541  | 44 900  | 68 162  | 65 024  |
| Samlede direkte tap, jf. tabell 1                              | 135 153 | 140 043 | 164 113 | 188 660 | 206 503 | 145 591 |
| Saksbehandlerkostnader hos kortutsteder (2250 kroner per kort) | 45 747  | 50 695  | 86 717  | 101 025 | 153 365 | 146 304 |
| Forbrukerkostnader (1000 kroner per kort)                      | 20 332  | 22 531  | 38 541  | 44 900  | 68 162  | 65 024  |
| Samlet beregnet kostnad  | 201 232 | 213 269 | 289 371 | 334 585 | 428 030 | 356 919 |

Kilde: Finanstilsynet

- Ytterligere kostnader forbundet med kortsvindel,
  - Kostnader knyttet til saksbehandling hos kortinnløser
  - Brukersteder
  - Hos Finansklagenemda
  - Kostnader knyttet til advokathonorarer og rettskostnader

# Tap ved bruk av nettbank (tall i hele tusen kroner)

Tabell 3: Tap ved bruk av nettbank (tall i hele tusen kroner)

| Svindeltype – nettbank   | 2012         | 2013         | 2014          | 2015          | 2016          | 2017         |
|--|--------------|--------------|---------------|---------------|---------------|--------------|
| Angrep ved bruk av ondartet programkode på kundens PC eller sikkerhetsmekanisme (trojaner) | 5 064        | 1 327        | 552           | 3 055         | 2             | 727          |
| Tapt/stjålet sikkerhetsmekanisme   | 3 367        | 1 285        | 6 655         | 963           | 8 758         | 1 892        |
| Phishing og falske BankID-brukersteder   | 10           |              | 539           | 5815          | 2 428         | 2 057        |
| Annet/ukjent   | 358          | 779          | 3 474         | 2 715         | 7 444         | 2 911        |
| <b>TOTALT</b>  | <b>8 799</b> | <b>3 391</b> | <b>11 220</b> | <b>12 548</b> | <b>18 632</b> | <b>7 587</b> |

Kilde: Finanstilsynet og Bits



# Utkontraktering

- Finanstilsynet mottok nærmere 50 meldinger om utkontraktering av IKT-virksomhet i 2017.
- Risikovurderinger som skal danne grunnlag for styrebeslutninger om utkontraktering, er i noen tilfeller mangelfulle.
- Ved gjennomgang av avtalene er det kun unntaksvis at IKT-forskriftens krav om rett til revisjon og tilsyn ikke er oppfylt.
- Bestemmelser som skal gjelde ved overføring av tjenesten til annen leverandør (exit-bestemmelser), er ofte for lite spesifisert.
- Et stadig økende antall underleverandører benyttes. Dette stiller økte krav til samhandling med underleverandørene og mellom underleverandørene. Særlig er dette viktig ved håndtering av alvorlige hendelser.
- Det er erfart at skyleverandører ikke har hatt tilstrekkelig modenhet når det gjelder håndtering av hendelser som berører tidskritiske tjenester.
- Utkontrakteres driftstjenester av vesentlig betydning for betalingsformidling eller annen finansiell infrastruktur til utenlandske aktører, kan det bli stilt særskilte krav til etablering av beredskapsløsninger.
- EBAs retningslinjer for utkontraktering er under revidering.

# IKT- og informasjonssikkerhet

- Digital kriminalitet utgjør en økende trussel og har stor oppmerksomhet.
- Omfanget av uønsket aktivitet mot foretakene øker vesentlig – kun et fåtall resulterer i en sikkerhetshendelse.
- Fortsatt økning i kriminell aktivitet som kan ramme foretakene
  - Phishing, SMS, trojanere, tyveri av kortinformasjon, løspengevirus, CEO fraud.
- Finanssektoren i Norge ble ikke rammet ved de store cyber-angrepene, hhv. skadevaren WannaCry i mai og NotPetya i juni, noe som trolig skyldes at finanssektoren er bedre beskyttet og har lengre erfaring i å sikre seg mot angrep.
- Det er registrert organisatoriske, operasjonelle og tekniske svakheter som medfører betydelige sårbarheter for tilsiktede angrep og utilsiktede feil.
- Det skal settes mål for foretakets organisering og arbeid med IKT-sikkerhet.
- Ansvar for henholdsvis styring av IKT-sikkerheten, kontroll med IKT-sikkerheten og det operative IKT-sikkerhetsarbeid skal være klart adskilt.
- Finanstilsynet anser sikkerhetstesting ved bruk av kvalifiserte eksterne ressurser som et viktig verktøy i arbeidet med å avdekke sårbarheter i foretakets infrastruktur og elektroniske forsvar.
- Et annet viktig risikoreduserende tiltak er foretakenes forebyggende arbeid med å bevisstgjøre foretakets ansatte om de ulike metodene som kriminelle benytter.

# Utviklingstrekk finansiell teknologi

- Utviklingen innen finansiell teknologi (Fintech) er knyttet både til nyetablerte og eksisterende foretaks tjenester.
- Finanstilsynet følger utviklingen, og ser blant annet på hvordan foretakene og nye aktører innretter seg etter lover og regler. Finanstilsynet legger vekt på at hensynet til finansiell stabilitet, trygge tjenester og god kundebeskyttelse blir ivaretatt. For å oppnå dette, bør lik risiko behandles likt, uavhengig av forretningsmodell.
- Finanstilsynet har etablert en informasjonsside for FinTech-foretak.
- EU og de europeiske finanstilsynene følger utviklingen og vurderer behov for tiltak.
- Teknologi for foretakets oppfølging og etterlevelse av regulatorisk regelverk tas i bruk for å bidra til mer effektive og automatiserte tilsynsprosesser.
- Kunstig intelligens og robotisering tas i bruk av foretakene for å effektivisere og forenkle virksomhetens prosesser. Også blokkjede-teknologiens potensiale vurderes av foretakene.
- Ved innføring av ny teknologi og alternativ anvendelse av eksisterende teknologi forutsetter Finanstilsynet at det gjennomføres risikovurderinger som identifiserer relevant risiko.
- ICO-er faller i hovedsak utenfor eksisterende regelverk på verdipapiriområdet. Dersom en ICO faller utenfor regelverket, kan investorer ikke forvente investorbeskyttelse. Finanstilsynet har publisert advarsler.
- De europeiske finanstilsynene er bekymret for at et økende antall forbrukere kjøper virtuell valuta uvitende om risikoen dette innebærer. Finanstilsynet har publisert advarsler.

# 4. Aktørenes vurdering av risikofaktorer

1. Foretakenes vurdering av risiko
  - Intervjuer
  - Spørreundersøkelse

# Aktørenes vurdering av risikofaktorer

- Foretakene vurderer de mest fremtredende truslene gjennom intervjuene til å være:
  - feil i systemer og svekket stabilitet som følge av økt omfang av og hyppighet på endringer i foretakets systemer
  - dataangrep, herunder mer avanserte og lettere tilgjengelige angrepsmetoder og -verktøy
  - manglende IKT-kompetanse og -kapasitet i foretaket
  - mangelfull styring og kontroll av tilganger for beskyttelse av informasjon og systemer
  - (sensitiv) informasjon på avveie
  - BankID ikke fungerer eller ikke fungerer tilfredsstillende
  - redusert mulighet for å sikre tjenester fra ende-til-ende ved utkontraktering
  - utkontrakterte tjenester ikke tilfredsstiller foretakets krav til sikkerhet og krav som følger av lov og forskrift

# Spørreundersøkelser med foretakene

1. Støtte for strategiske beslutninger
2. Avvik i driften
3. Data er ikke tilstrekkelig beskyttet
4. ID-tyveri
5. Misbruk av tilgang til datasystemene
6. Hvitvasking

## Eksempel på tabell fra rapporten

Tabell 7: Data er ikke tilstrekkelig beskyttet

|   | Sårbarhet   | Foretakenes svar | Trend 2017 | Trend 2016 |
|---|---|------------------|------------|------------|
| 1   | Våre retningslinjer for klassifisering av strukturert (databaser) og ustrukturert (word, e-post) informasjon og beskyttelse av informasjonen  |                  | →          | →          |
| 2   | Tilgangskontroller – ansatte, konsulenter, leverandører, applikasjoner, software  |                  | →          | →          |
| 3   | Våre systemer for logging og evne til å reagere på innholdet i loggene  |                  | →          | ↘          |
| 4   | Nettverkssegmentering, perimetersikring, kryptering   |                  | →          | →          |
| 5   | Sikring av data på bærbart utstyr   |                  | →          | →          |
| 6   | Ved terminering av avtaler om datalagring, må leverandøren dokumentere at data er fullstendig slettet?  |                  | →          | →          |
| 7   | Ustrukturerte data (dvs. data der brukeren selv vurderer behovet for å beskytte dataene) som epost, presentasjoner, tekst-dokumenter blir gjennomgått regelmessig med tanke på beskyttelse, eventuelt sletting? |                  | →          | →          |
| Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet. Hvit: Ikke vurdert. |   |                  |            |            |

# Spørreundersøkelser med foretakene 2

## - Avvik i driften

|    | Sårbarhet  | Foretakenes svar | Trend 2017 | Trend 2016 |
|----|--|------------------|------------|------------|
| 7  | Logger og vår evne til å reagere på innholdet i loggene  |                  | ↘          | →          |
| 8  | "Tikkende miner", dvs. komponenter som gradvis slites eller verdier som gradvis når nivåer som krever inngrep, og vi oppdager det ikke, for eksempel minnelekkasje, sertifikater som går ut på dato, elektroniske komponenter som slites, energiforsyning som "slites" (batterier, brennstoff til nødstrømagregat) |                  | →          | →          |
| 9  | Vår evne til å avdekke avvik i datatrafikken (unormal belastning, unormale porter/ protokoller, avvikende svarider) i driftsmønsteret og ta aksjon før skade   |                  | →          | →          |
| 10 | Vår beskyttelse mot dataangrep (Advanced persistence threat, trojaner, ransomware, DDoS)   |                  | →          | →          |
| 11 | Kvaliteten på kontinuitet- og katastrofeløsningene våre, jf. IKT-forskriften § 11  |                  | →          | ↘          |
| 12 | Samarbeidsrutiner med leverandører   |                  | →          | →          |
| 13 | Leveransepresset vi er utsatt for i markedet gjør kvaliteten i løsningene ikke alltid er god nok   |                  | ↗          | ↗          |
| 14 | Tilgang på kompetanse, herunder kompetanse til å stille krav til leverandører og følge opp leveransene   |                  | ↗          | ↗          |
| 15 | Omfanget av endringer  |                  | ↗          | ↗          |
| 16 | Nye regulatoriske krav som gjør at vi må endre systemene våre  |                  | ↗          | ↗          |
| 17 | Vår kunnskap om hvor datalinjene går og redundans når det gjelder datalinjer   |                  | →          | →          |
| 18 | Tilgangskontroll, adgangskontroll og dual kontroll   |                  | →          | →          |
| 19 | Medarbeidernes årvåkenhet når det gjelder trusler og angrep  |                  | →          | I/A        |

# Spørreundersøkelser med foretakene 3

1. Støtte for strategiske beslutninger
  - Kompleksitet i IT-systemene anses å være en økende risiko. Nye tjenester kombinert med til dels gammel arkitektur gir kompleksitet og risiko for mangelfullt informasjonsgrunnlag.
2. Avvik i driften
  - Dataangrep er en vedvarende trussel
  - Omfanget av endringer i systemer og leverandører, samt leveransepress likeså
  - Også nye regulatoriske krav som medfører behov for endringer i systemene utgjør en trussel
3. Data er ikke tilstrekkelig beskyttet
  - Tilgangskontroller er stadig en utfordring.
  - Sårbarhet knyttet til nettverkssegmentering, perimetersikring og kryptering utgjør fortsatt en trussel.
  - økt teknisk kompleksitet og tjenesteomfang øker risikoen for at sikkerhetstiltakene ikke fanger opp angrep
  - profesjonelle angripere og flere angrep krever økt ressursbruk og strengere kontroll
4. ID-tyveri
  - Skadevare og misbruk av rettigheter i forbindelse med ID-tyveri utgjør fortsatt en trussel
5. Misbruk av tilgang til datasystemene
  - Trusselbildet synes å ha gått noe ned fra 2016
6. Hvitvasking
  - Foretakene synes fortsatt det er utfordrende å lage systemer som har høy presisjon når det gjelder å flagge mistenkelige transaksjoner, noe som utgjør en risiko for at transaksjoner ikke blir flagget

**Gjennom besvarelse av spørreundersøkelsen synes foretakenes samlede syn på risikobildet svakt økende i 2017, noe det også var i 2015 og 2016.**

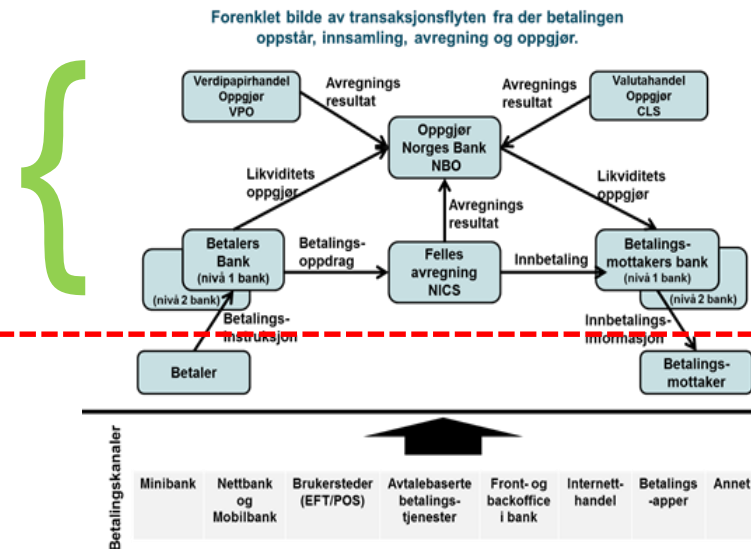


# 5. Finanstilsynets oppsummerende vurdering av risikobildet

1. Finansiell infrastruktur
2. Foretakene
3. Forbrukere

# Finansiell infrastruktur

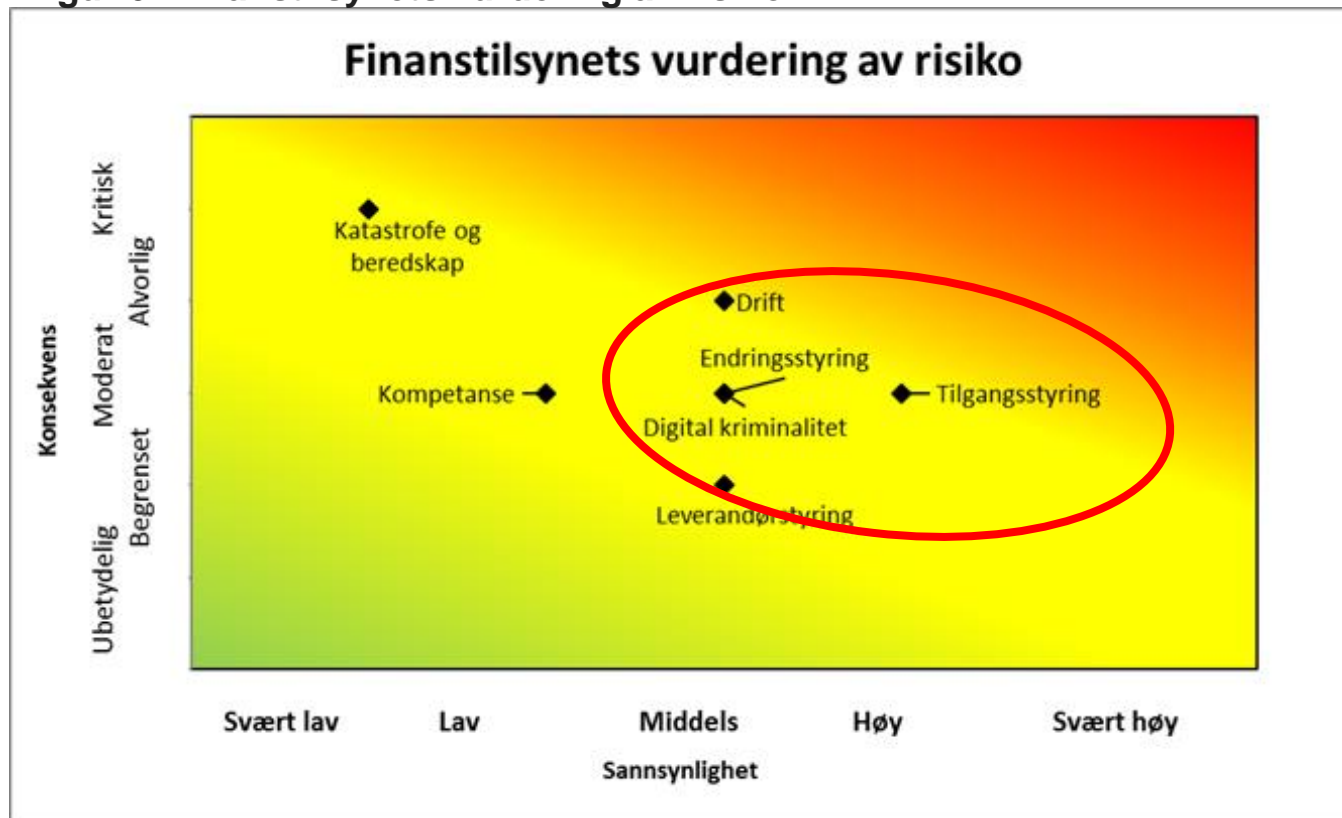
- Den finansielle infrastrukturen består av betalingsystemet og verdipapiroppgjørssystemet samt verdipapirregisteret (VPS), markedsplasser og sentrale motparter. Infrastrukturen skal sørge for at pengebetalinger og transaksjoner i finansielle instrumenter blir registrert, avregnet og gjort opp.
- Det var god regularitet på avregnings- og oppgjørssystemene og kommunikasjonen mot det internasjonale betalingsystemet SWIFT og det internasjonale oppgjørssystemet CLS.
- **Selv om det var hendelser som gjorde betalingsløsninger utilgjengelige i lengre perioder og tilgjengeligheten til betalingssystemer var noe svakere enn i 2016, vurderer Finanstilsynet likevel den norske finansielle infrastrukturen som hovedsakelig robust.**



- Hendelser og funn fra tilsynsvirksomheten viste imidlertid sårbarheter når det gjelder
  - Styring og kontroll med tilganger til systemer og data, særlig utvidete administrasjonsrettigheter
  - Kapasitetsovervåkning og kapasitetsstyring
  - Kriseløsninger (kontinuitetsløsninger)
  - Styring av operasjonell risiko, særlig ved endinger

# Finanstilsynets oppsummerende vurdering av risikobildet – foretakene

Figur 6: Finanstilsynets vurdering av risiko



Kilde: Finanstilsynet

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

Finanstilsynets vurderer sårbarheter i

- Driftsløsninger og
- Mangelfull tilgangsstyring

som de mest dominerende risikoene i foretakene .

Sårbarheter knyttet til

- Mangelfull endringsstyring og
- Svakheter i forsvarsverk, som kan føre til skade som følge av digital kriminalitet

er også dominerende risikoer.

- Digitale løsninger blir stadig mer dominerende.
- Spor som legges igjen ved bruk av digitale tjenester kan misbrukes av tjenesteleverandører. Slike spor kan, dersom de kommer uvedkommende i hende, utgjøre en betydelig risiko for å bli brukt i kriminell vinning.
- Økt digitalisering innebærer at bankkunder, som av forskjellige grunner ikke selv benytter bankenes digitale tjenester, ser seg nødt til å la familiemedlemmer eller andre betrodde få tilgang til sine digitale signaturer for bruk av digitale tjenester. Finanstilsynet vurderer at dette utgjør en risiko for at identiteter kan bli misbrukt, spesielt der kundens innlogging i nettbank opereres av den betrodde.
- Bankene har på sin side fokusert på å hjelpe denne kundegruppen over fra analoge til digitale løsninger gjennom informasjon og kurs. Finanstilsynet har inntrykk av dette er initiativ som har bidratt til at flere tar steget over i den digitale verden.
- Samtidig er det fortsatt kunder som vil forbli analoge fordi de digitale løsningene er for kompliserte, de ønsker anonymitet eller fordi de rett og slett ikke vil være digitale.

# 6. Finanstilsynets oppfølging

1. Sentrale områder for Finanstilsynets IKT-tilsyn
2. Arbeid med betalingssystemer
3. Oppfølging av hendelser
4. Beredskapsarbeid
5. Oppfølging av trusselbildet knyttet til digital kriminalitet
6. Forbrukervern

# Oppsummering

- Den finansielle infrastrukturen i Norge er hovedsakelig robust.
- Økning i antall IKT- hendelser med konsekvens for hhv. enkeltforetak og forbrukerne, men ingen med konsekvenser for finansiell stabilitet.
- Betalingssystemene og kunderettede tjenester var mindre tilgjengelige i 2017 enn året før
- Flere alvorlige hendelser medførte at betalingstjenestene var utilgjengelige i opp til et helt døgn for mer enn 30 prosent av bankkundene. Det skapte usikkerhet i markedet om foretakenes evne til kontinuerlig å levere betalingstjenester og gjennomføre betalingsoppdrag
- Det er rom for forbedringer
  - Kriseløsninger (kontinuitetsløsninger), styring av operasjonell risiko, særlig endringer og kapasitetsovervåkning og -styring
- 180 av de 190 rapporterte hendelsen var forårsaket av operasjonelle avvik, resterende 10 var sikkerhetshendelser.
- Tap ved kortsvindel sank med ca. 25 prosent fra 2016 til 2017, tap med stjålet kortinformasjon (Card-Not-Present) utgjorde 60 prosent av nedgangen.
- Samlede tap ved bruk av nettbank sank betydelig i 2017 i forhold til 2016.
- Finanstilsynet vurderer sårbarheter i driftsløsninger og mangelfull tilgangsstyring som de mest dominerende risikoene i foretakene. Sårbarheter knyttet til mangelfull endringsstyring og svakheter i forsvarsverk, som kan føre til skade som følge av digital kriminalitet, er også dominerende risikoer.
- Styring og kontroll med utvidete tilgangsrettigheter må forbedres.
- Teknologisk utvikling har stor innvirkning på tjenesteutviklingen i finansnæringen. Hensynet til finansiell stabilitet, trygge tjenester og god kundebeskyttelse må ivaretas. Lik risiko bør behandles likt, uavhengig av forretningsmodell.

# Takk for oppmerksomheten!

**Olav Johannessen**  
**seksjonssjef – seksjon for tilsyn med IT og**  
**betalingstjenester**

**E-post: [ola@finanstilsynet.no](mailto:ola@finanstilsynet.no)**