FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Risiko- og sårbarhetsanalyse (ROS) 2017

Finanssektorens bruk av informasjons- og kommunikasjonsteknologi

Seminar 29. mai 2018

Olav Johannessen
seksjonssjef
for tilsyn med IT og betalingstjenester

ROS-analysen 2017:

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Finanstilsynets funn og vurderinger
2. Aktørenes vurdering av risikofaktorer
3. Finanstilsynets vurdering av risikobildet
4. Oppsummering

Finanstilsynets funn og vurderinger
- Betalingstjenester

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- 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.
- 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.

Finanstilsynets funn og vurderinger - Bank

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Kontinuerlige endringer i trusselbildet for digitale angrep utfordrer i økende grad 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.
- Fortsatt behov for forbedringer i bankenes arbeid med å utarbeide forretningsmessige konsekvensanalyser som grunnlag for krav til kontinuitets- og katastrofeløsninger, selv om det observeres en forbedring.

Finanstilsynets funn og vurderinger
- Verdipapirområdet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- 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.
- Det er avdekket mangler i risikovurderinger og utkontrakteringsavtaler for verdipapirforetak.

Finanstilsynets funn og vurderinger
- Forsikringsområdet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Finanstilsynet erfarer fortsatt at risikostyringen hos enkelte foretak 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.
- Der ny teknologi tas i bruk ved nye forsikringsprodukter stilles det økte krav til både bruk av og kontroll med innsamlede data og krav til risikovurderinger som identifiserer relevant risiko.
  - Eksempelvis ved bruk av sensorteknologi og overvåking av kundeatferd.

Finanstilsynets funn og vurderinger
- Revisjonsselskaper

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

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

Finanstilsynets funn og vurderinger
- Tiltak mot hvitvasking

- Det er observert mangelfull dokumentasjon av risikovurderingene som ligger til grunn for de elektroniske kunde- og transaksjonskontrollene.
- Det er påpekt at beslutning om ny elektronisk kontroll eller endret kontroll ikke er tilstrekkelig formalisert og dokumentert.
- Der den til enhver tid sist oppdaterte sanksjonslisten ikke er brukt i screeningen, er påpekt.

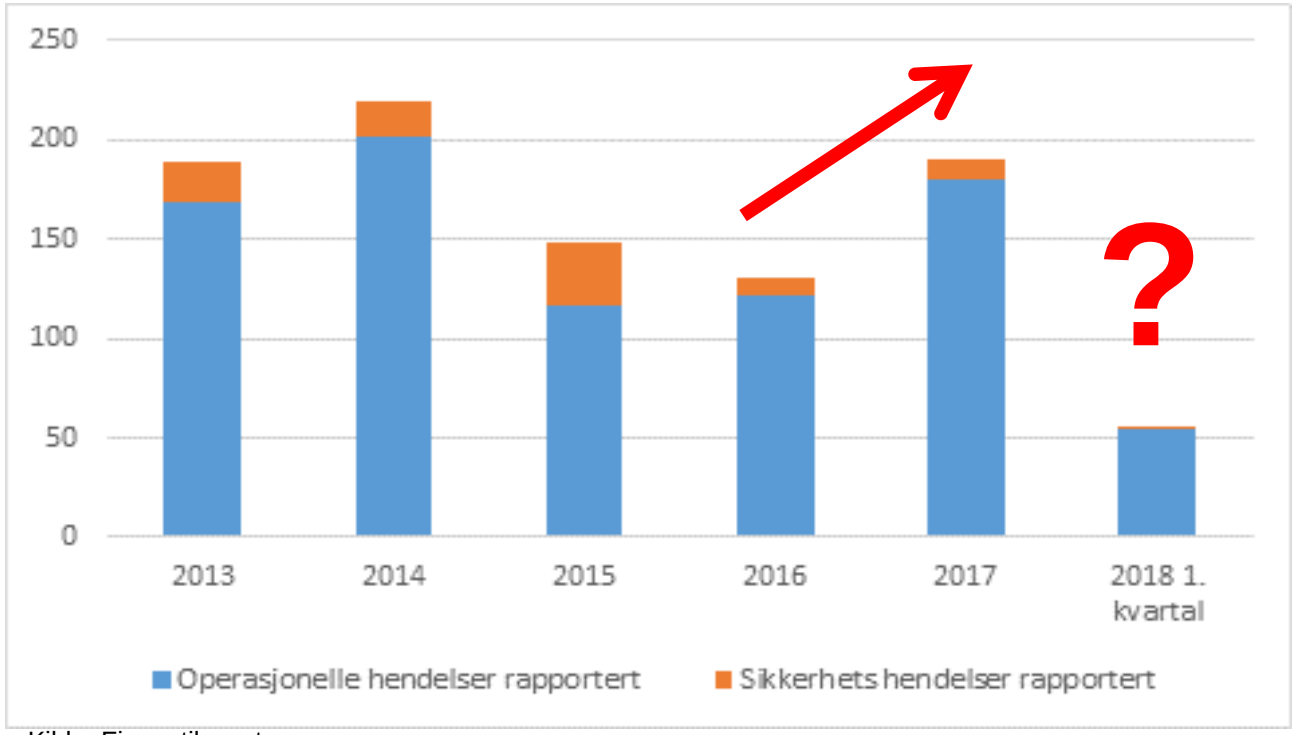
Finanstilsynets funn og vurderinger

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

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

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.



Kilde: Finanstilsynet

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

Finanstilsynets funn og vurderinger
- Alvorlige driftshendelser i 2017

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

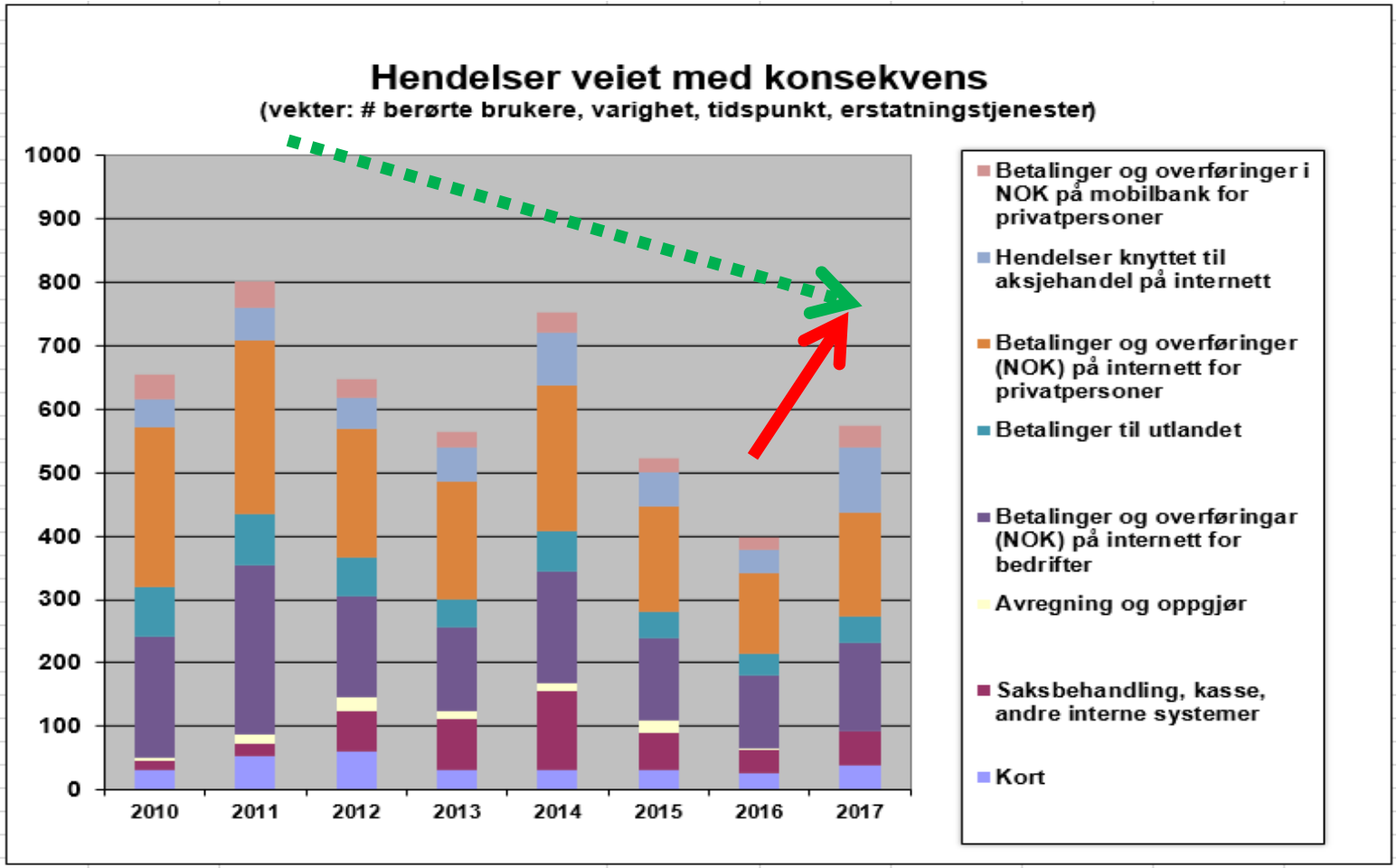
Dato	Konsekvens	Varighet	Årsak
16.03.17	Betalingstjenester, kundeløsninger og interne systemer ikke tilgjengelige.	15 timer	Feil i styringssystem til lagringsenhet.
15.06.17	Betalingstjenester, kundeløsninger og interne systemer ikke tilgjengelige.	10 timer	Feil i styringssystem til lagringsenhet oppsto 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.

Finanstilsynets funn og vurderinger

- **Betalingssystemet og kunderettede løsninger var mindre tilgjengelige i 2017 sammenlignet med de to foregående årene.**

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY



Kilde: Finanstilsynet

2018

?

Finanstilsynets funn og vurderinger

- Tap ved svindel og angrep mot betalingstjenester

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

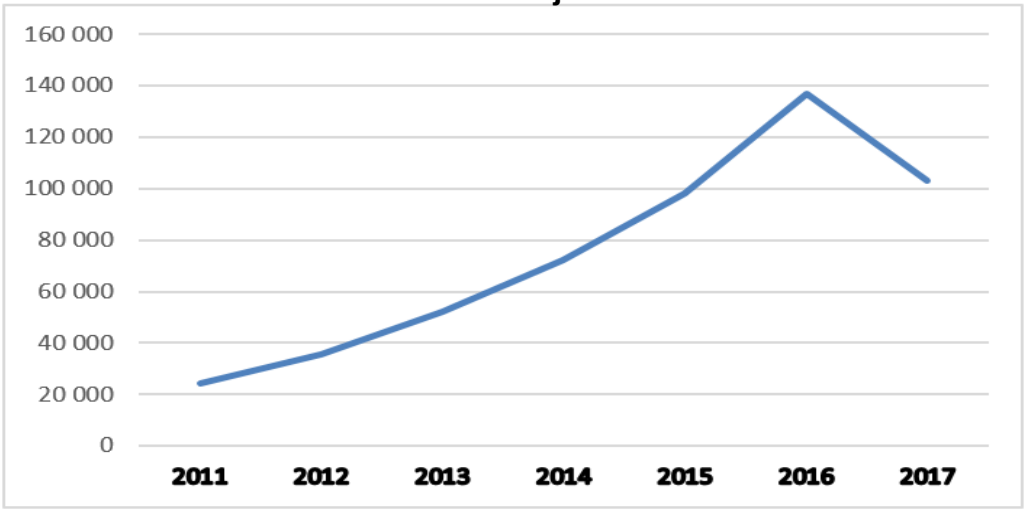
Finanstilsynet har for første gang siden registreringen startet i 2010, observert en nedgang i kortsvindel.

(tall i hele tusen kr.)	2012	2013	2014	2015	2016	2017
TOTAL SVINDEL BETALINGSKORT	135 153	140 043	164 113	188 660	206 503	145 591
TOTAL SVINDEL NETTBANKER	8 799	3 391	11 220	12 548	18 632	7 587

ANTALL KORT RAMMET AV MISBRUK (ANTALL)	20 332	22 531	38 541	44 900	68 162	65 024

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

Svindel med misbrukt kortinformasjon ikke tilstede. Tall i hele tusen kr.



Finanstilsynets funn og vurderinger
- Utkontraktering

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- 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.

Finanstilsynets funn og vurderinger
- IKT- og informasjonssikkerhet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- 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.
- Ansvaret 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.

Finanstilsynets funn og vurderinger
- Utviklingstrekk finansiell teknologi

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- 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 verdipapirområdet. 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.

Aktørenes vurdering av risikofaktorer - Intervjuer

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- 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

Aktørenes vurdering av risikofaktorer
- Spørreundersøkelser med foretakene

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

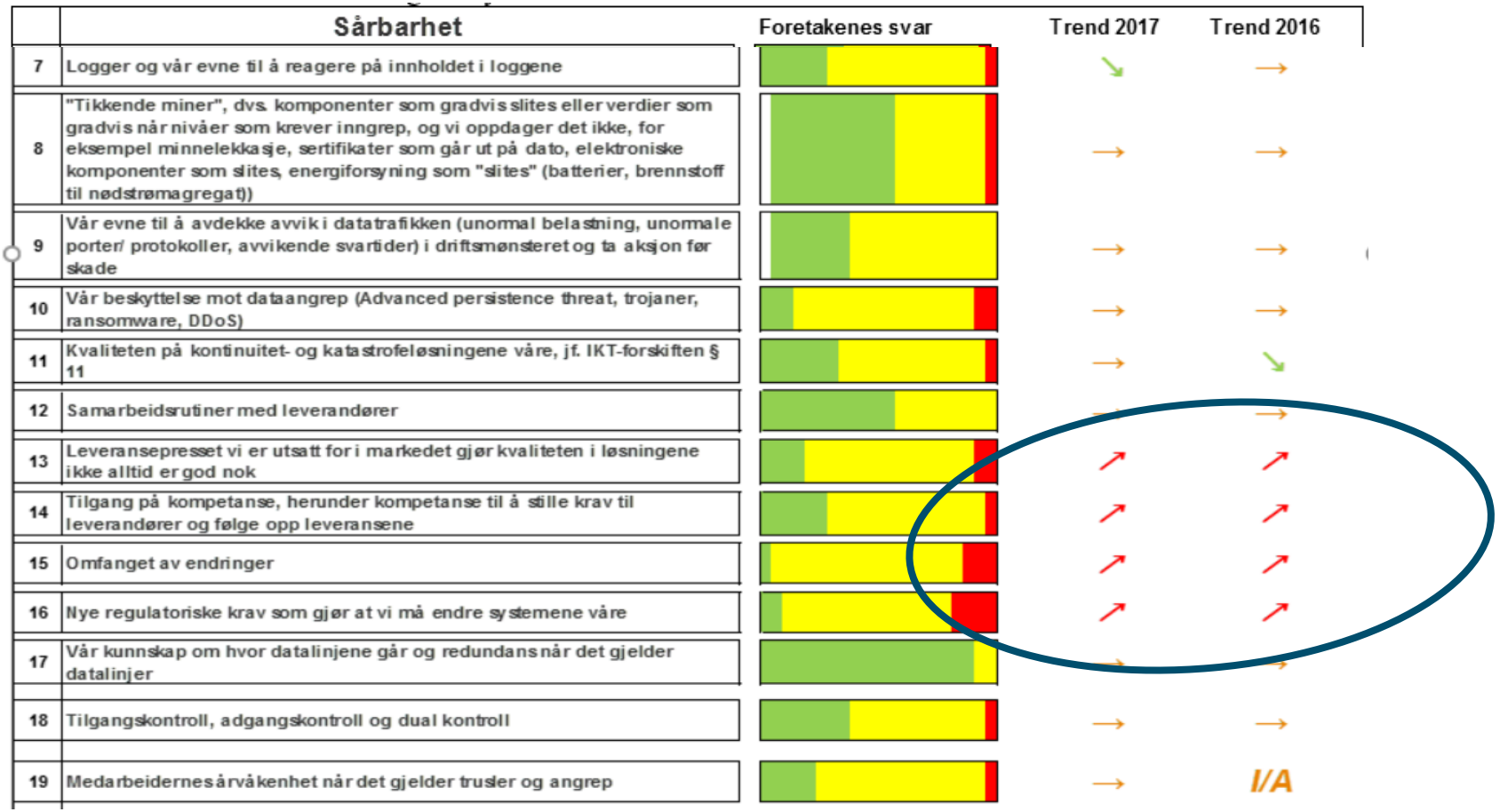
1. Støtte for strategiske beslutninger
2. Avvik i driften
3. Data er ikke tilstrekkelig beskyttet
4. ID-tyveri
5. Misbruk av tilgang til datasystemene
6. Hvitvasking

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

Aktørenes vurdering av risikofaktorer
- Spørreundersøkelser med foretakene 2

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

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 svartider) 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-forskiften § 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

Aktørenes vurdering av risikofaktorer - Spørreundersøkelser med foretakene 3

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

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 mistenkelig transaksjoner, noe som utgjør en risiko for at transaksjoner ikke blir flagget

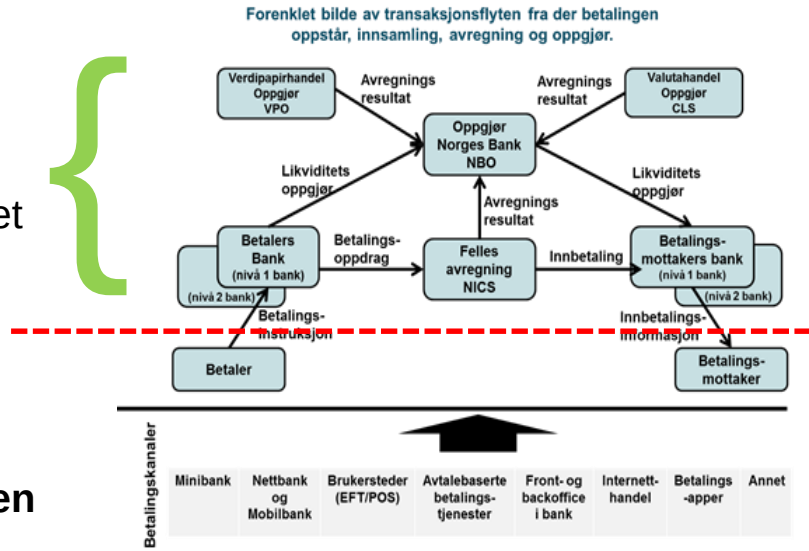
Finanstilsynets oppsummerende vurdering av risikobildet - Finansiell infrastruktur

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Den finansielle infrastrukturen består av betalingssystemet 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 betalingssystemet 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.**

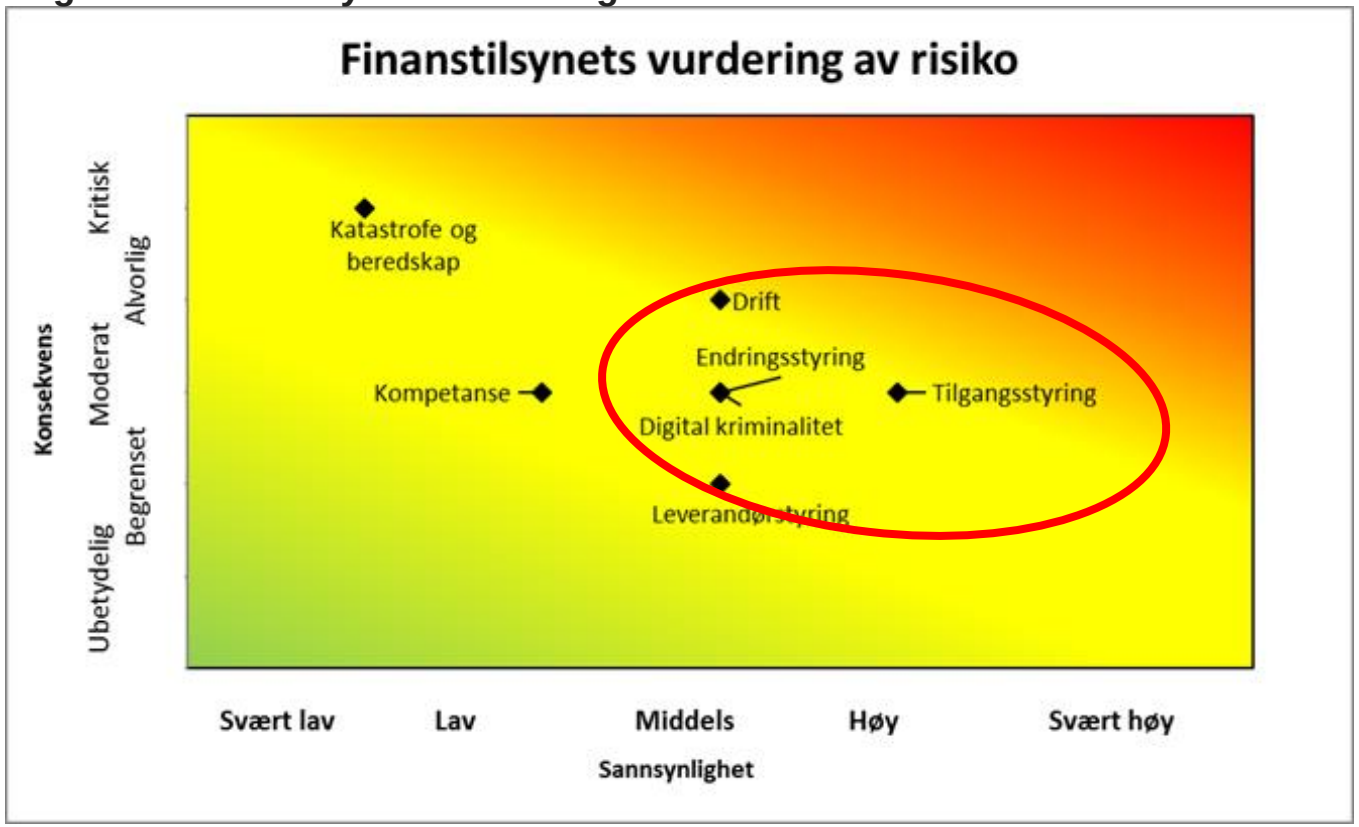


- Hendelser og funn fra tilsynsvirksomheten viste imidlertid sårbarheter når det gjelder
  - Styring og kontroll med tilganger til systemer og data, særlig utvidete administrasjonsrettigheter
  - Kapasitetsovervåkning og kapasitetsstyring
  - Kriseløsninger (kontinuitetsløsninger)
  - Styring av operasjonell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

Finanstilsynets oppsummerende vurdering av risikobildet – Foretakene

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

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.

Finanstilsynets oppsummerende vurdering av risikobildet - Forbrukere

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Digitale løsninger blir stadig mer dominerende.
- Finanstilsynet erfarer at bankene har fokusert på å hjelpe analoge kundegrupper over på digitale løsninger.
- Der kunder synes digitale løsninger er for kompliserte, er det en risiko for at identiteter kan bli misbrukt, når de overlater digitale signaturer til familiemedlemmer eller andre betrodde.

- Analoge kunder løper en risiko for dårlige tjenestetilbud

- 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.

Oppsummering

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- 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.

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Takk for oppmerksomheten!

Olav Johannessen
Seksjonssjef – seksjon for tilsyn med IT og betalingstjenester

E-post: ola@finanstilsynet.no