FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Pressebriefing 28. april 2016

Risiko- og sårbarhetsanalyse (ROS) 2015
Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi

Seksjonssjef Olav Johannessen
Finanstilsynet

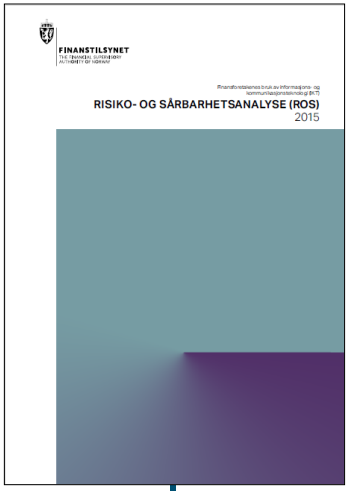
ROS-analysen 2016:

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Innledning
2. Oppsummering
3. Finanstilsynets funn og vurderinger
4. Aktørenes vurdering av risikofaktorer
5. Endringer i reguleringer
6. Finanstilsynets oppsummerende vurdering av risikobildet
7. Finanstilsynets oppfølging
8. Ordliste

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

ANSTILSYNET
ANCIAL SUPERVISORY
RITY OF NORWAY



- Skaffe oversikt
- Analysere
- Foreslå tiltak

Resultater fra tilsyn IT og betalingstjenester

Gjennomførte ROS-intervju og spørre-undersøkelser

Hendelses-håndtering

Data fra hendelsesdatabase

Betalingstjenester

Meldeplikt Betalings-tjenester

Annen relevant Informasjon

Beredskap
- BFI-sekretariatet
- Samarbeid andre myndigheter
- Infrastruktur betalings-systemer

Våre virkemidler
Regelverk, Innrapportering og Tilsyn

3. Finanstilsynets funn og vurderinger

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Rapporterte hendelser 2015
2. Funn, observasjoner og vurderinger
   - Betalingssystemer og utvikling. Tapstall
   - Bank
   - Verdipapirområdet
   - Forsikring
   - Regnskapsførerselskap
   - Forbruker
3. Utviklingstrekk

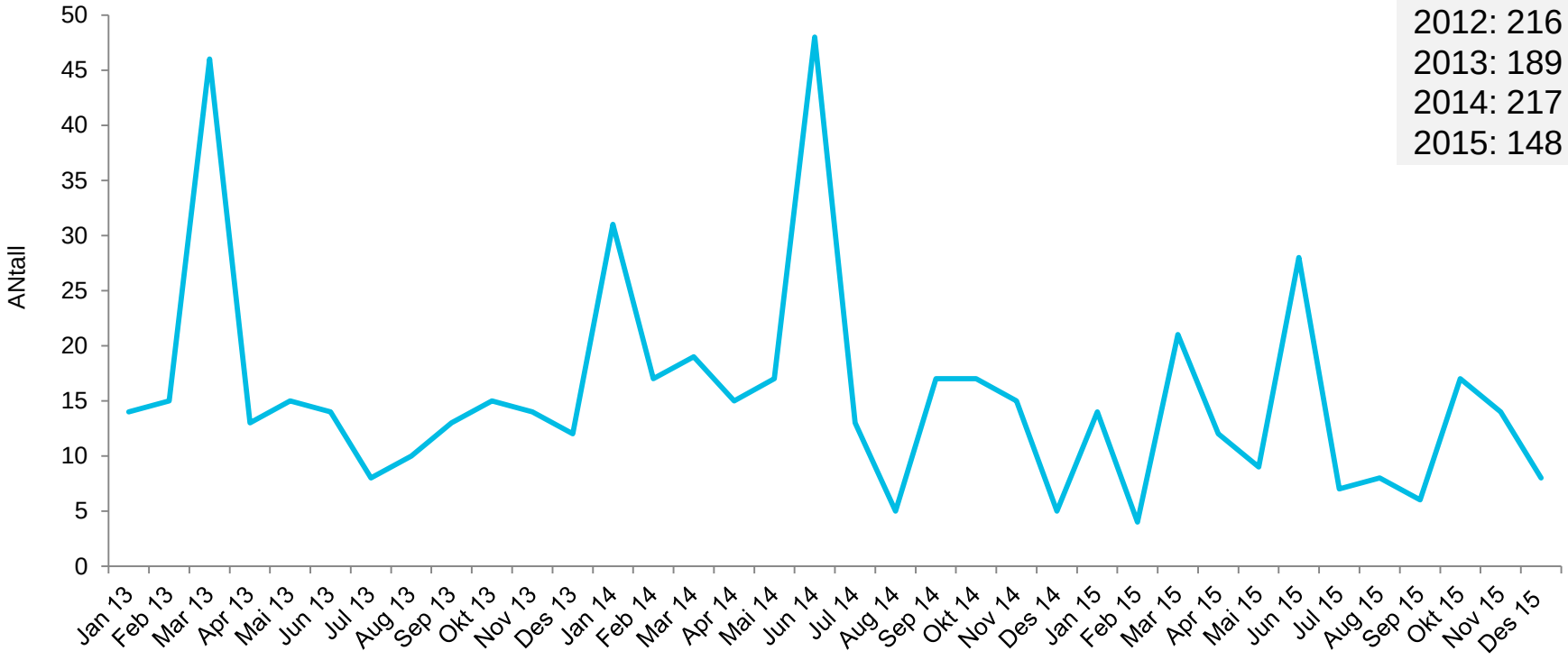
Utviklingen i hendelser er tilbake på den positive trenden fra 2011 etter at den ble brutt i 2014

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Antall hendelser i 2015 er lavere enn i foregående år

Figur 4: Antall rapporterte hendelser i perioden 2013–2015

2011: 221 hendelser
2012: 216 hendelser
2013: 189 hendelser
2014: 217 hendelser
2015: 148 hendelser

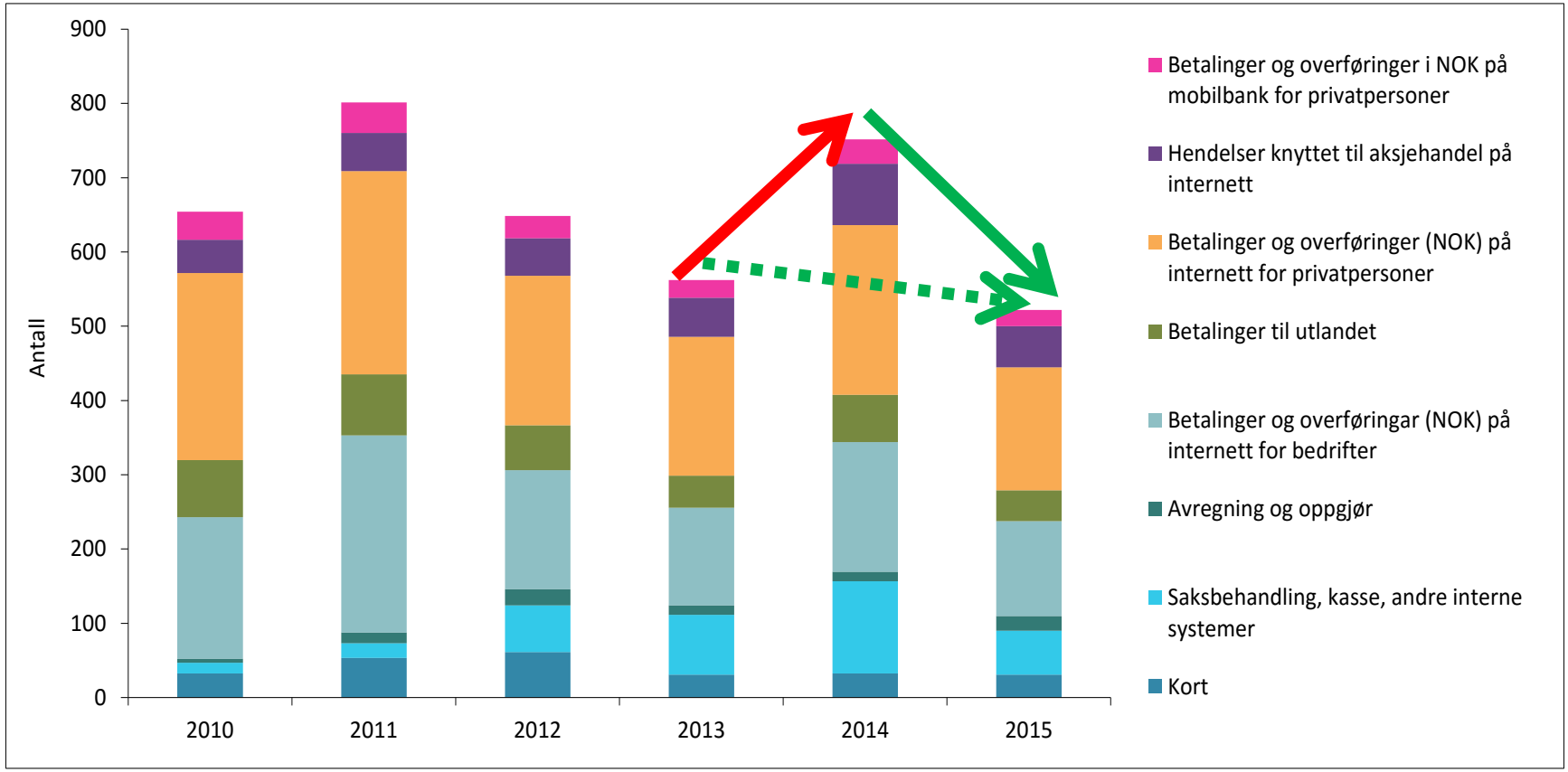


Kilde: Finanstilsynet

Betalingssystemene og kunderettede tjenester var mer tilgjengelige i 2015 enn i året før.

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Figur 6: Hendelser vektet med konsekvens (vekter: berørte kunder, varighet, tidspunkt, erstatningstjenester)



Kilde: Finanstilsynet

Betalingstjenester

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Betalingssystemene er generelt solide og stabile. På enkelte områder er det likevel rom for forbedringer.
   - Blant annet kriseløsninger, styring av operasjonell risiko og styring av tilganger kan bli bedre.
2. Manglende risikovurderinger i forkant av endringer i utkontrakteringsforhold
3. Hendelser viser mangelfull kvalitet på testing
4. Hendelser som oppstår i, eller treffer betalingsinfrastrukturen, rammer bredt og medfører raskt store konsekvenser
5. Noen alvorlige hendelser rammet betalingsformidlingen, bla. BankID (mai/juni)
6. Registrert flere nettverkshendelser som påvirket mobile tjenester
7. Endringer hyppig årsak til feil og avvik og det er derfor knyttet betydelig risiko knytte til dette
8. Enkelte foretak har mangler i sine avtaler, bl.a. IKT-forskriftens regler om utkontraktering
9. Rask utvikling innen mobile betalingsløsninger, nasjonalt og internasjonalt
10. Fortsatt angrep som rammer betalingsformidlingen
    - *DDoS, phishing, SMS, trojanere, tyveri av kortinformasjon, CEO fraud*

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

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

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

Svindeltype betalingskort	2011	2012	2013	2014	2015
Misbruk av kortinformasjon, Card-Not-Present (CNP) (internetthandel m.m.)	24 190	35 701	51 954	72 056	**98 410**
Stjålet kortinformasjon (inkl. skimming), misbrukt med falske kort i Norge	468	2 308	762	524	**2 670**
Stjålet kortinformasjon (inkl. skimming), misbrukt med falske kort utenfor Norge	57 340	55 869	51 534	51 685	**48 447**
Originalkort tapt eller stjålet, misbrukt med PIN i Norge	32 224	28 128	21 274	21 266	**18 875**
Originalkort tapt eller stjålet, misbrukt med PIN utenfor Norge	7 008	8 544	9 570	13 071	**14 224**
Originalkort tapt eller stjålet, misbrukt uten PIN	4 488	4 603	4 949	5 510	**6 033**
TOTALT	125 718	135 153	140 043	164 113	**188 660**

Tabell 2: Antall betalingskort rammet av misbruk

	2011	2012	2013	2014	2015
Antall kort rammet av misbruk	16 784	20 332	22 531	38 541	**44 900**

Kilde: Finanstilsynet

Kostnader forbundet med kortsvindel
(tall i hele tusen kroner)

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Tabell 3: Kostnader forbundet med kortsvindel (beløp i hele tusen kroner)

Kostnader svindel med betalingskort	2011	2012	2013	2014	2015
Antall kort rammet av misbruk, jf. tabell 2 (antall)	16 784	20 332	22 531	38 541	**44 900**
Samlede direkte tap, jf. tabell 1	125 718	135 153	140 043	164 113	**188 660**
Saksbehandlerkostnader kortutsteder (2 250 kroner per kort)	37 764	45 747	50 695	86 717	**101 025**
Forbrukerkostnader, 1 000 kroner per kort	16 784	20 332	22 531	38 541	**44 900**
Samlet beregnet kostnad	180 266	201 232	213 269	289 371	**334 585**

Kilde: Finanstilsynet

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

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

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Tabell 4: Tap ved bruk av nettbank (tall i hele tusen kroner)

Svindeltype nettbank	2011	2012	2013	2014	2015
Angrep ved bruk av ondartet programkode på kundens PC (trojaner)	664	5 064	1327	552	**3055**
Tapt/stjålet sikkerhetsmekanisme	3 321	3 367	1 285	6 655	**963**
Phishing og falske BankID-brukersteder		10		539	**5815**
Annet/ukjent		358	779	3474	**2715**
TOTALT	3 985	8 799	3 391	11 220	**12 548**

Kilde: Finanstilsynet

Bank

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Flere store endringsprosser – god kontroll på prosessene – god driftsstabilitet
2. Oppfølgingen av ISP-leverandører (internett service providere) kan være mangelfull
3. Foretakene må sikre styring og kontroll av tilganger også ved utkontraktering og det er behov for å forbedre kvaliteten på tilgangslister
4. Mangelfulle produksjonslike testmiljøer
5. Bedret etterlevelse krav til rapportering til Bankenes sikringsfond ved fallent
6. Risikoen for digitale angrep tiltar. Arbeidet med IKT-sikkerhet bør intensiveres ytterligere
7. Mangelfull oppfølging av internrevisjonsrapporter og dokumentering av tiltak
8. Endringer på driftsleverandørsiden, både eierskifter og bytte av leverandører kan øke risikoen spesielt i endringsperioden
9. Enkelte foretak har mangler i sine avtaler, bl.a. IKT-forskriftens regler om utkontraktering
10. Kan bli utfordrende for foretakene å skaffe tilstrekkelig kompetanse på IKT-sikkerhetsområdet
11. Utsatt for ransomware angrep (kryptering)

Verdipapirområdet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Høy stabilitet og god kvalitet kjennetegner verdipapirområdet
2. Manglende retningslinjer ved bruk av tredjepartssystemer for informasjonsutveksling
3. Foretakene kan bedre kvaliteten på tilgangsstyringen
   - Verdipapirforetakene må bli bedre på å sikre at sensitiv informasjon ikke kommer på avveie
   - Observert utkontraktering av IKT-systemer med kurssensitive data hvor foretaket har hatt manglende kontroll med leverandørens driftsoperatører
4. Manglende klassifisering av sensitiv informasjon
5. Behov for bedre sikring av informasjon ifm epostutveksling
6. Flere hendelser innen verdipapirområdet med manglende lydopptak av samtaler med kunder mv. grunnet teknisk svikt i opptaksutstyret
7. Mangelfulle avtaler mellom verdipapirforetak og leverandører av utkontrakterte ordresystemer
8. Risiko for leveringskapasitet av komponenter hos leverandører i kritiske situasjoner
9. Utsatt for ransomware angrep (kryptering)

Forsikring

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Flere forsikringsforetak fremdeles behov for å utarbeide bedre og mer helhetlige risikoanalyser som viser samlet risiko ved foretaket bruk av IKT.
2. Komplekse forsikringssystemer med sensitiv informasjon krever sikker og betryggende forvaltning og etablerte reserveløsninger.
3. Mye regelverksendringer som medfører endringer i forsikringssystemene.
4. Få rapporterte hendelser. Mulig manglende rapportering iht IKT-forskriftens krav.

Regnskapsførerselskaper

1. Dokumentbasert tilsyn med regnskapsførerselskapenes bruk av IKT viser at en del selskaper har behov for å iverksette risikoreduserende tiltak knyttet til IKT-systemene i virksomheten.

Forbrukerområdet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Sperring av kort mot betalinger av handel på Internett

- Retningslinjer for sikkerhet i Internett-betalinger trådte i kraft 1. august 2015. Retningslinjene sier blant annet at forbruker i større grad skal kunne sette effektive grenser for hva betalingskort kan benyttes til. Blant annet skal kunden kunne sperre kortet for bruk på Internett.

- Finanstilsynet har merket seg at ikke alle kortutstedere har implementert retningslinjene i sine løsninger. Finanstilsynet vil følge opp dette i 2016.

Utviklingstrekk

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Den digitale kriminaliteten øker og endrer trusselbildet for finansnæringen
  - Ransomware og DDoS med utpressing
  - CEO Fraud
  - Trojanere
  - Målrettede politiaksjoner hjelper
- Den teknologiske utviklingen har stor innvirkning på tjenesteutviklingen i finansnæringen
  - FinTech, både ny teknologi og nye selskaper
  - Blockchain er en teknologi næringen vier stor interesse
  - Mobilens funksjoner og mobile betalingsløsninger
- Deregulering åpner for nye aktører og løsninger - utfordrer etablerte forretningsmodeller
- Endringer i regelverk både nasjonalt og fra EU → påvirker foretakenes IKT-løsninger
- Finansnæringen vedtok i 2015 å samle arbeidet innen betalingsformidling i et nytt og styrket infrastrukturselskap – Bits
- Det er endringer i tjenesteleverandørmarkedet, organisering og eierskap og utkontrakteringslandskapet

Utkontraktering

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Det ble behandlet over 100 meldinger om utkontraktering av IKT i 2015
- Gjennom behandling av utkontrakteringsmeldingene har tilsynet erfart svakheter både når det gjelder gjennomførte
  - risikoanalyser
  - foretakets selvstendige vurderinger av utkontrakteringen
  - etterlevelse av gjeldende lover og forskrifter.
- Bl.a. meldinger der avtalene ikke tar tilstrekkelig hensyn til reguleringskrav som IKT-forskriftens eller internkontrollforskriftens krav om at foretak under tilsyn skal gis rett til å kontrollere, herunder revidere, de av leverandørens aktiviteter som er knyttet til avtalen.

4. Aktørenes vurdering av risikofaktorer

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Foretakenes vurdering av risiko
   - Intervjuer
   - Spørreundersøkelse
2. Risikoområder påpekt fra andre kilder

Aktørenes vurdering av risikofaktorer

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Foretakene vurdere de mest fremtredende truslene til å være:
  - Forstyrrelser i infrastruktur
  - Kompleksitet i IKT-systemer og leveransekjeder
  - Digital kriminalitet og inntrenging i systemer
  - Brudd på konfidensialitet
- Andre trusselsområder som foretakene trekker frem er:
  - Knapphet på kompetanse
  - Ukritisk bruk av fildelingstjenester og manglende styring og kontroll med bruk av skytjenester
  - Manglende kvalitet eller mangel på penetrasjonstesting
  - Omfanget av endringer
  - At IKT-systemene ikke gir tilfredsstillende støtte til beslutninger, kundebehandling eller saksbehandling
- Foretakene peker også på:
  - Samfunnsendringene, hvor betalingssystemene i økende grad kan bli brukt til flytting av ulovlige midler, som en trussel
  - Risiko for at de ikke klarer å lage systemer som har høy nok presisjon når det gjelder å flagge mistenkelige transaksjoner (hvitvasking/terrorfiansiering)

Spørreundersøkelser med foretakene 1

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

Tabell 7: Data ikke tilstrekkelig beskyttet

	Sårbarhet	Foretakenes svar	Trend 2014	Trend 2015
1	Våre retningslinjer for klassifisering av informasjon og beskyttelse av informasjonen		→	→
2	Kvaliteten på våre tilgangskontroller		→	→
3	Våre systemer for logging og evne til å reagere på innholdet i loggene		→	→
4	Mulig inntrenging i våre systemer		→	→
5	Sikring av data på bærbart utstyr (fjernsletting av mobildata osv.)		→	→
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.			

Spørreundersøkelser med foretakene 2

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Støtte for strategiske beslutninger
   - Risiko for at IKT ikke fungerer tilfredsstillende som støtte for virksomheten
   - Seks av truslene har gått fra å være minkende i 2014 til å være stabile i 2015
2. Avvik i driften
   - Dataangrep er en vedvarende trussel
   - Omfanget av endringer i systemer og leverandører likeså
   - Flere foretak enn i fjor anser at testsystemene kunne vært bedre. Kan henge sammen med økt leveransepress, omfanget av endringer og endringer fra nye regulatoriske krav
3. Data er ikke tilstrekkelig beskyttet
   - Tilgangskontroller er stadig en utfordring. Utkontraktering, off-shoring og midlertidig, innleid kompetanse skaper utfordringer
   - Inntrenging i systemene anses som en trussel. Økning i ransomware i 2015
4. ID-tyveri
   - Skadevare og misbruk av rettigheter i forbindelse med ID-tyveri fortsatt betydelig trussel
   - I 2015 ble trusselen fra CNP-svindel ansett å være økende
5. Misbruk av tilgang til datasystemene
   - Trusselbildet uendret fra foregående år
6. Hvitvasking
   - Utfordrende å lage systemer som har høy presisjon når det gjelder å flagge mistenkelig transaksjoner

Tre av sårbarhetene har gått fra å være stabile i 2014 til å være økende i 2015.

Risikoområder påpekt fra andre kilder - ENISA

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Offentlige myndigheter og deres leverandører har blitt mer effektive i kampen mot digital kriminalitet ved:
  - Mere samstemte/organiserte tiltak for å stanse cyberangrep
  - Økt kompetanse og kjennskap til cyberkriminalitet, økte budsjetter og mer samarbeid over landegrenser
  - Øvelser, økt etterretning og informasjonsdeling mellom nasjoner
  - Økt fokus på forskning og utvikling for å utvikle løsninger som beskytter mot cyberkriminalitet

- Utviklingen fortsetter. De kriminelle krefter demonstrerer at de rår over betydelige ressurser ved:
  - Stadig forbedrede applikasjoner for kriminelle handlinger, og som tilbys som tjenester over Internett
  - Forbedrede løsninger for avdekking og utnytting av svakheter i eksisterende systemer
  - Å i stor grad å lykkes med å utvikle ulike innbringende ransomware-tjenester
  - Å utvide fokusområdet for kriminalitet til å omfatte alle Internett-tilkoblede enheter
  - Å gjennomføre angrep som ikke registreres av vanlige forsvarsløsninger

5. Endringer i reguleringer

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Den mest sentrale regelendringen er EUs nye betalingstjenestedirektivet (PSD2).
  - Det åpner for at nye aktører kan tilby betalingstjenester og gis rett til tilgang til betalingskonto.

- Andre større regelendringer er
  - EUs forordning om behandling av personopplysninger
  - EUs direktiv for nettverks- og informasjonssikkerhet
  - Ny avtale om overføring av data mellom EU/EØS og USA
  - Norsk forskrift om systemer for betalingstjenester
  - Retningslinjer for sikkerhet i Internett-betalinger
  - Norsk forskrift om innføring av forordning om interbankgebyrer

- I tillegg endringer i IKT-forskriften
  - Krav om at avtaler om utkontraktering av IKT skal behandles av foretakets styre

6. Finanstilsynets oppsummerende vurdering av risikobildet

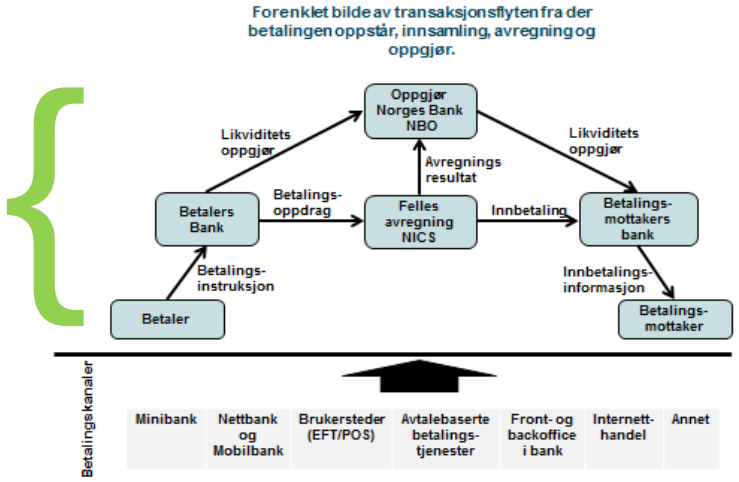
FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Finansiell infrastruktur
2. Foretakene
3. Forbrukere
4. IMFs vurdering av finansiell infrastruktur

Finansiell infrastruktur

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

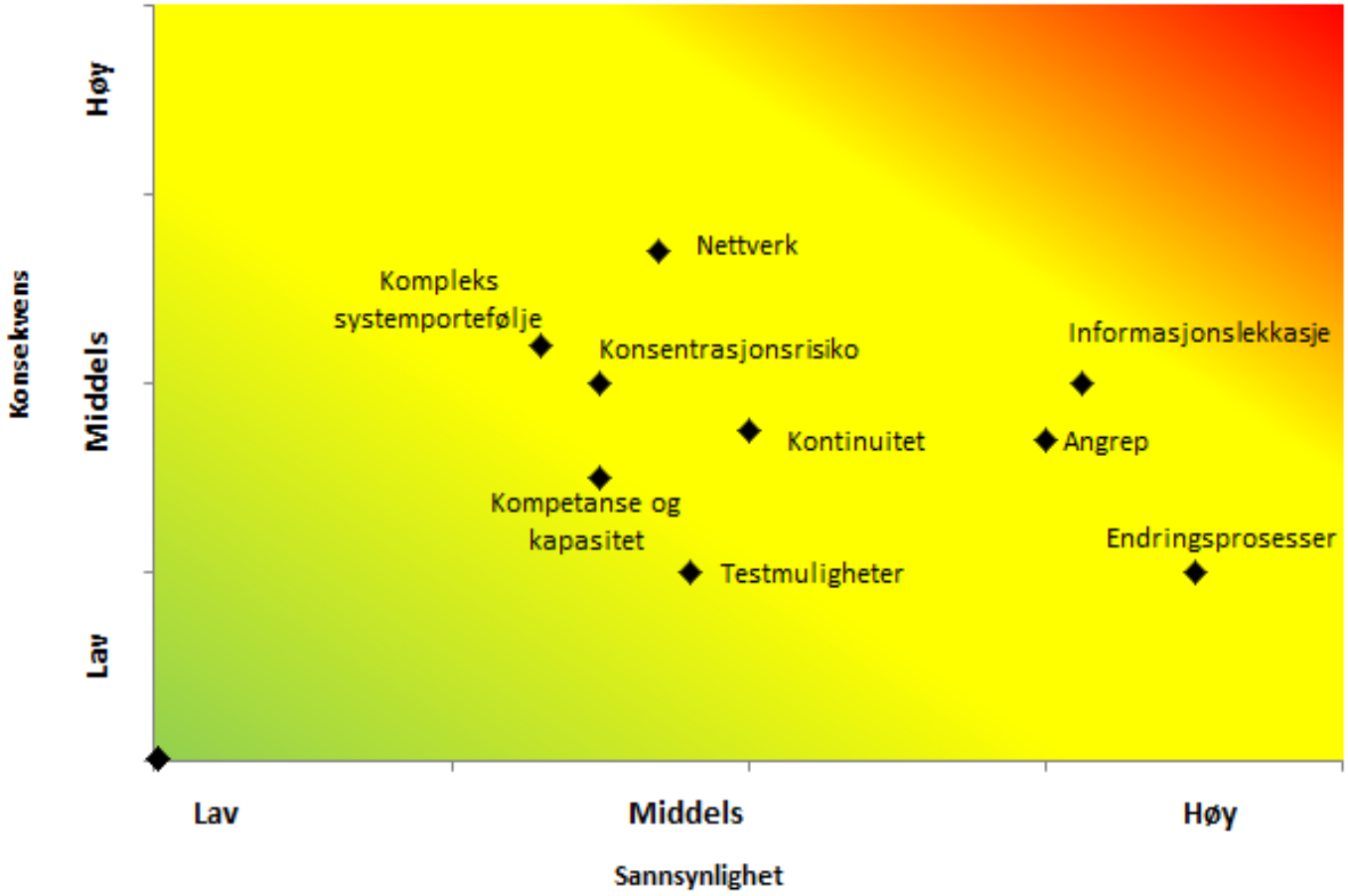
- **Stabiliteten i den finansielle infrastrukturen var bedre i 2015 enn i 2014 og den ble rammet av færre operasjonelle hendelser.**
- God regularitet på avregnings- og oppgjørssystemene og kommunikasjonen mot det internasjonale betalingssystemet SWIFT og det internasjonale oppgjørssystemet CLS.
- **Finanstilsynet vurderer på den bakgrunn den norske finansielle infrastrukturen som solid og stabil, men at det på enkelte områder er rom for forbedringer.**
  - Dette gjelder blant annet kriseløsninger og styring av operasjonell risiko



Foretakene -

Vurdering av de mest sentrale truslene mot og sårbarhetene i foretakenes systemer

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY



Finanstilsynets vurderer

- Feil i nettverk
- Informasjonslekkasjer
- Digitale angrep
- Komplekse systemporteføljer
- Feil ved endringsprosser

som de mest sentrale truslene mot og sårbarhetene i foretakenes systemer

De ulike risikoområdene er klassifisert etter sannsynlighet for at en negativ hendelse oppstår (lav, middels, høy) og konsekvensene dersom hendelsen oppstår (lav, middels, høy).

Forbrukere

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Økt digitalisering:
  - Gjør forbrukerne mer sårbar for svikt i foretakenes elektroniske tjenester
  - Kan gjøre det vanskelig for forbrukerne å forstå alle konsekvenser av sine digitale handlinger
  - Gjør forbrukerne i økende grad eksponert for svindel ved bruk av digitale løsninger.
  - Beskyttelse av informasjon og å forhindre ID-tyveri er stadig aktuelle utfordringer.

- I arbeidet med regelverksendringer står hensynet til forbrukerne og forbrukernes sikkerhet og rettigheter sentralt

IMFs vurdering av finansiell infrastruktur

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Norges finansielle infrastruktur (FMI) omtales som moderne og stabil.
- IMF gir uttrykk for at tilsyns- og overvåkingsfunksjonene med FMI-foretakene virker å være effektive.
- IMF gir imidlertid også uttrykk for at det finnes et potensiale for å styrke samarbeidet på myndighetsnivå for å adressere risikoene som enkelte av FMI-foretakene har når det gjelder avhengighet av kritiske leverandører.

- IMFs peker i tillegg på en del konkrete tiltak for bl.a. å minske den operasjonelle risikoen for FMI-foretakene som utgjør kjernekomponentene i landets finansielle infrastruktur.

7. Finanstilsynets oppfølging

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. IT-tilsyn og annen kontakt med foretakene
2. Arbeid med betalingssystemer
3. Oppfølging av hendelser
4. Beredskapsarbeid
5. Videreutvikling av tilsynsverktøy
6. Oppfølging av trusselbildet knyttet til digital kriminalitet
7. Forbrukervern

Oppsummering

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Ingen alvorlige IKT-hendelser med konsekvenser for finansiell stabilitet.
- Nedgang i antall hendelser med konsekvens for hhv. enkeltforetak og forbrukerne.
- Betalingssystemene og kunderettede tjenester mer tilgjengelige i 2015 enn året før.
- Betalingssystemene er generelt solide og stabile. På enkelte områder er det likevel rom for forbedringer.
  - Blant annet kriseløsninger, styring av operasjonell risiko og styring av tilganger kan bli bedre.
- Antall svindelangrep er økende.
- Samlede tap ved bruk av nettbank endret seg lite fra 2014 til 2015.
  - Tapene i 2015 var i stor grad knyttet til svindel via bedriftsnettbanker.
- Fortsatt økning i tap ved kortsvindel med stjålet kortinformasjon, særlig card-not-present.
- Samlede kostnader forbundet med kortsvindel er betydelige
- Krypteringsvirus forårsaket at foretak ble utestengt fra arbeidsverktøy og data
- Svakheter avdekket ved behandling av foretakenes meldinger om utkontraktering av IKT.
  - Gjennomførte risikoanalyser, selvstendige vurderinger av utkontrakteringsforholdet og etterlevelse av gjeldende lover og forskrifter.

Takk for oppmerksomheten!

FINANSTILSYNET

Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

www.finanstilsynet.no

Olav Johannessen
Seksjonssjef seksjon for tilsyn med IT og betalingstjenester

E-post: ola@finanstilsynet.no