FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Pressebriefing 26. april 2017

Risiko- og sårbarhetsanalyse (ROS) 2016
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. Funn, observasjoner og vurderinger
   - Betalingssystemer og utvikling.
   - Bank
   - Verdipapirområdet
   - Forsikring
   - Eiendomsmeglere
2. Rapporterte hendelser 2016
3. Tapstall Betalingsformidlingen
4. Utviklingstrekk

Betalingstjenester

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Betalingssystemene vurderes generelt som solide og stabile i 2016. Det er likevel rom for forbedringer innenfor særlig
  - Kapasitetsovervåkning, kapasitetsstyring og kriseløsninger (kontinuitetsløsninger)
  - Styring av operasjonell risiko
- Rapporterte hendelser i 2016:
  - Viste ved flere tilfeller mangelfull kvalitet på testing hos foretakene
  - Der hendelsen traff betalingsinfrastrukturen eller sentrale underleverandører, rammet hendelsen bredt og mange foretak og medførte raskt betydelige brukerkonsekvenser
  - Flere alvorlige hendelser knyttet til BankID / BankID på mobil rammet betalingsformidlingen
  - Mobilbetalingstjenester rammet av lange tjenestebrudd
  - Endringer er fremdeles en for hyppig årsak til feil og avvik
- Manglende etterlevelse av regelverk, både regulatorisk og bransje regelverk
- Rask utvikling på betalingstjenesteområdet
  - Konsolidering i det norske markedet for mobile betalingsløsninger
- Næringen forbereder seg på at PSD 2 kommer
- Fortsatt vekst i kriminell aktivitet som rammer betalingsformidlingen
  - Phishing, SMS, trojanere, tyveri av kortinformasjon, CEO fraud
- Foreslått å presisere bankenes plikt til å sikre kontantdistribusjon i krisesituasjoner

Bank

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Flere store endringsprosesser – god kontroll på prosessene – hovedsakelig god driftsstabilitet
- Mot slutten av 2016 og inn i 2017 imidlertid negativ utvikling i driftsstabiliteten
- Risikoen for digitale angrep er tiltakende, og arbeidet med IKT-sikkerhet bør intensiveres ytterligere
- Foretakene må sikre konsistent tilgangsstyring, enten det er tilgang via frontsystemer eller direkte tilgang til kjernesystemene, og også ved utkontraktering. Tilgangsstyring er generelt for svak
- Mangler i etterlevelse av retningslinjer for sikkerhet for Internettbetalinger
- Mangler i etterlevelse av regelverk ved utkontraktering, eks. avtaler og risikovurdering
- Svakheter i foretakenes analyser av konsekvenser ved bortfall av applikasjoner vedrørende (etablering av) beredskapsløsninger
- Distribusjon av informasjon med sensitivt innhold gjennom åpen e-post
- Observasjoner viser at de elektroniske overvåkningsscenariene ifm hvitvaskingskontroll er lite treffsikre og medfører mange falske treff. Krever store kontrollressurser for å skille de fra ekte treff
- Gjennomføringen av hvitvaskingsregelverkets krav om oppdatert kontroll av kundene ved endringer i sanksjonslistene er utfordrende
- Flere rapporter hendelser knyttet til feil og driftsproblemer for AML-løsninger

Verdipapirområdet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Fortsatt god kvalitet og høy stabilitet på verdipapirsektorens IKT-systemer
- Flere foretak med utilstrekkelig tilgangskontroll for systemer med sensitiv informasjon
- Flere foretak legger **for** stor vekt på driftsleverandørenes risikoanalyser med fare for at analysen ikke er tilpasset foretakets særskilt sensitive data. Foretakene har selv ansvaret!
- Mangler i etterlevelse av regelverk ved utkontraktering, eks. er foretak som avtalemessig har avskrevet seg retten til å gjennomføre inspeksjoner
- Verdipapirområdets informasjonssystemer inneholder store mengder sensitiv informasjon om foretak, som
  - Skaper utfordringer når det gjelder å beskytte sensitiv informasjon ved økende utkontraktering av IKT-systemer med sensitiv informasjon kombinert med at informasjonen konsentreres hos få driftsselskaper
  - Krever bedre beskyttelse av sensitiv informasjon i takt med det økende trusselbilde fra omverdenen
  - Har medført at ansatte i IKT-driftssentre har handlet verdipapirer i foretak det forestår IKT-driften av i perioder med handelsbegrensninger
  - Gir en økt sårbarhet når også ikke-finansforetak, som behandler store mengder sensitiv foretaksinformasjon, også gjør bruk av samme IKT-driftsleverandører
  - Stiller store krav til foretakets styring og kontroll med tilgangene til informasjon og sin IKT-virksomhet der den er utkontraktert, slik at informasjonslekkasjer kan forebygges.
- Nasdaq selskapers (de svenske) manglende styring og kontroll med risikoen i egen virksomhet

Forsikring

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Flere forsikringsforetak har fremdeles behov for å bedre sitt arbeid med risikoanalyser for å skaffe seg et riktig bilde av den samlede risikoen ved foretakets bruk av IKT
- IT-risikoene knyttet til utkontraktert virksomhet er ofte ikke i tilstrekkelig grad vurdert, og inngår ikke alltid i de årlige risikogjennomgangene av den samlede IT-risikoen
- Der regneark brukes som grunnlag for forretningsmessig rapportering og beslutning bør det etableres felles prosesser og rutiner for dette, da slik bruk ofte utgjør en «skjult» form for IKT-virksomhet med tilhørende risikoer

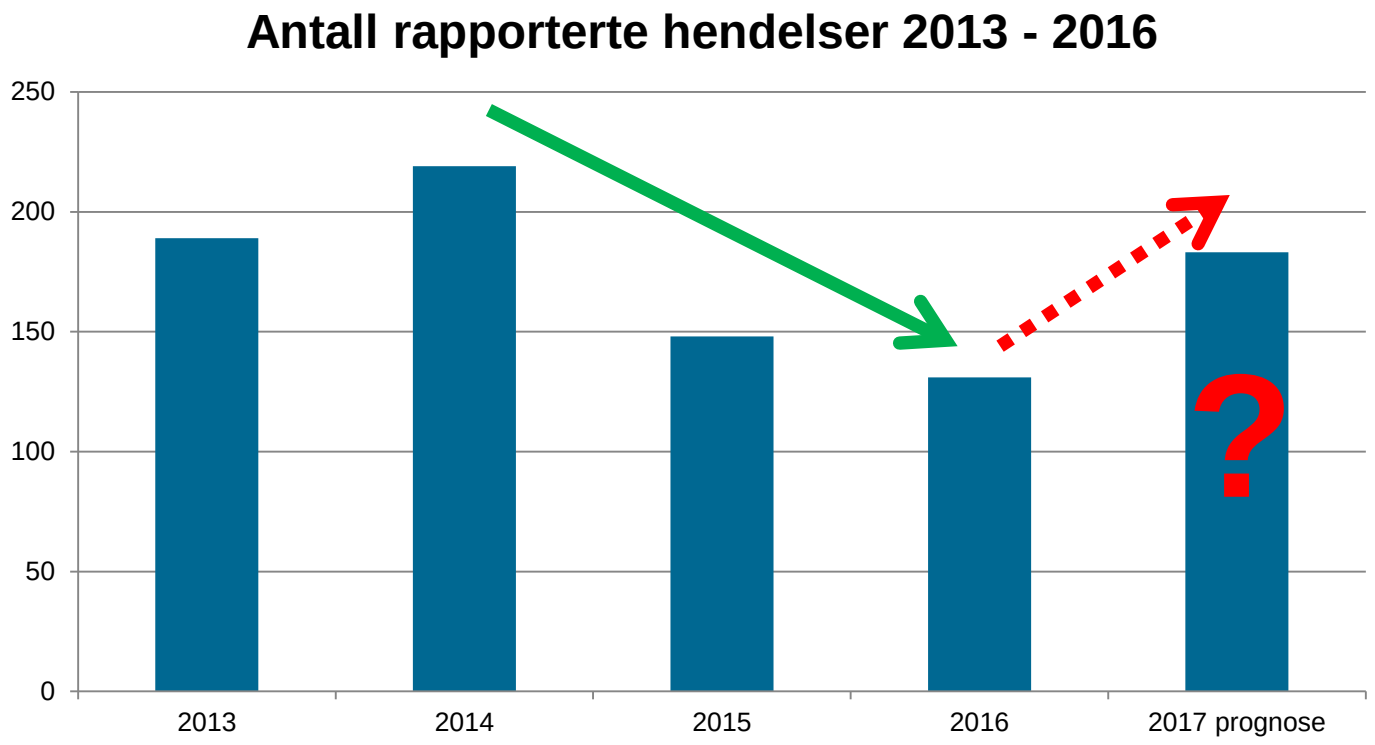
Eiendomsmeglerselskap

- Foretakene må sikre at utbetalingsfiler som genereres fra oppgjørssystemet kontrolleres mot filene med betalings-data levert til nettbanken

Utviklingen i hendelser fortsatte i 2016 den positive trenden fra 2015, men mot slutten av 2016 og inn i 2017 var det imidlertid en negativ utvikling

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Antall hendelser i 2016 er lavere enn foregående år

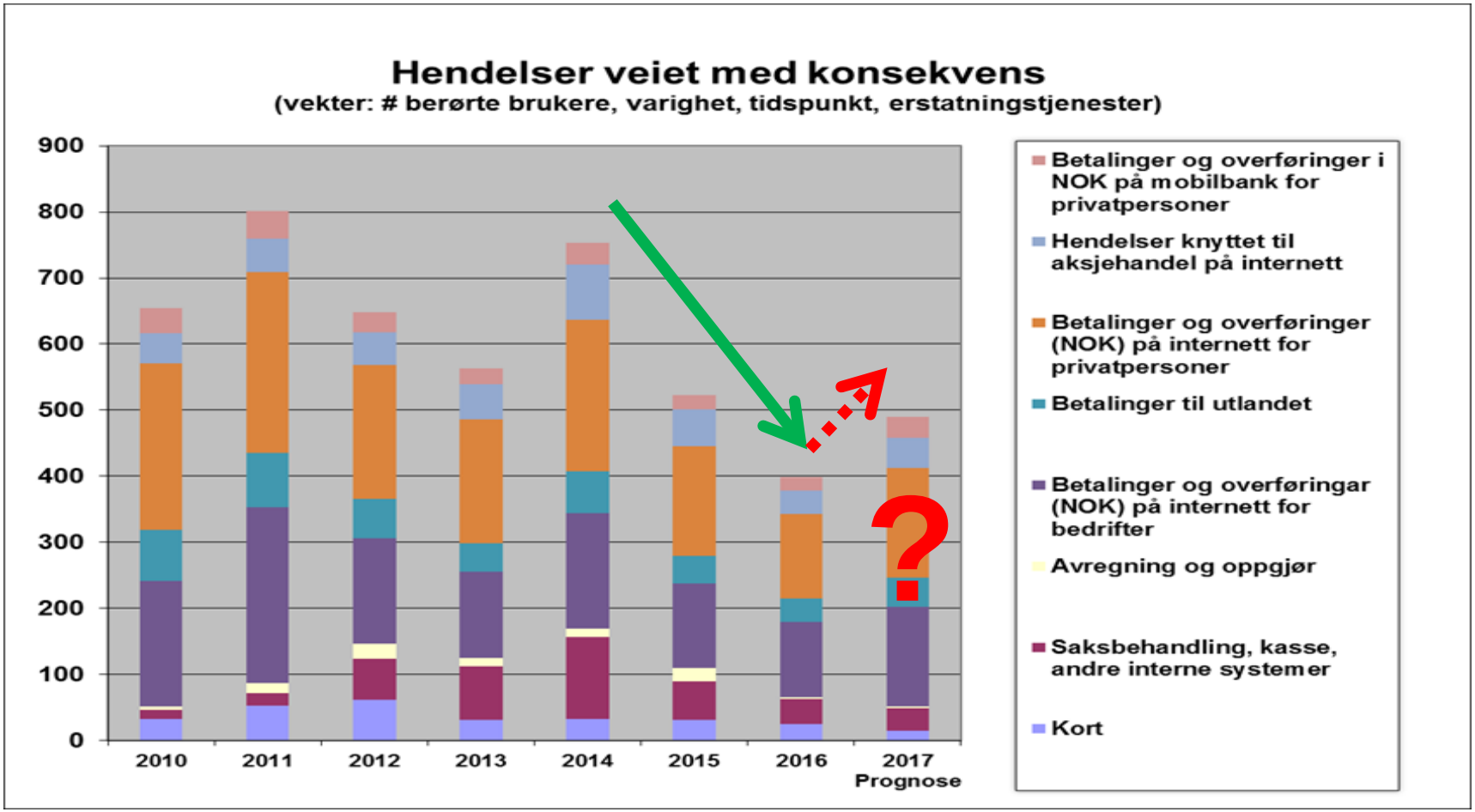


Kilde: Finanstilsynet

2011: 221 hendelser
2012: 216 hendelser
2013: 189 hendelser
2014: 217 hendelser
2015: 148 hendelser
2016: 131 hendelser
- 121 operasjonelle
- 10 sikkerhets

Betalingssystemene og kunderettede tjenester var mer tilgjengelige i 2016 enn i de foregående årene. Så langt i 2017 viser utviklingen en negativ trend

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY



Kilde: Finanstilsynet

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	2012	2013	2014	2015	2016
Misbruk av kortinformasjon, Card-Not-Present (CNP) (Internett-handel m.m.)	35 701	51 954	72 056	98 410	**137 015**
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort i Norge	2 308	762	524	2 670	1 360
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort utenfor Norge	55 869	51 534	51 685	48 447	41 762
Originalkort tapt eller stjålet, misbrukt med PIN i Norge	28 128	21 274	21 266	18 875	12 857
Originalkort tapt eller stjålet, misbrukt med PIN utenfor Norge	8 544	9 570	13 071	14 224	10 223
Originalkort tapt eller stjålet, misbrukt uten PIN	4 603	4 9 49	5 510	6 033	3 286
TOTALT	**135 153**	**140 043**	**164 113**	**188 660**	**206 503**

Antall betalingskort rammet av misbruk

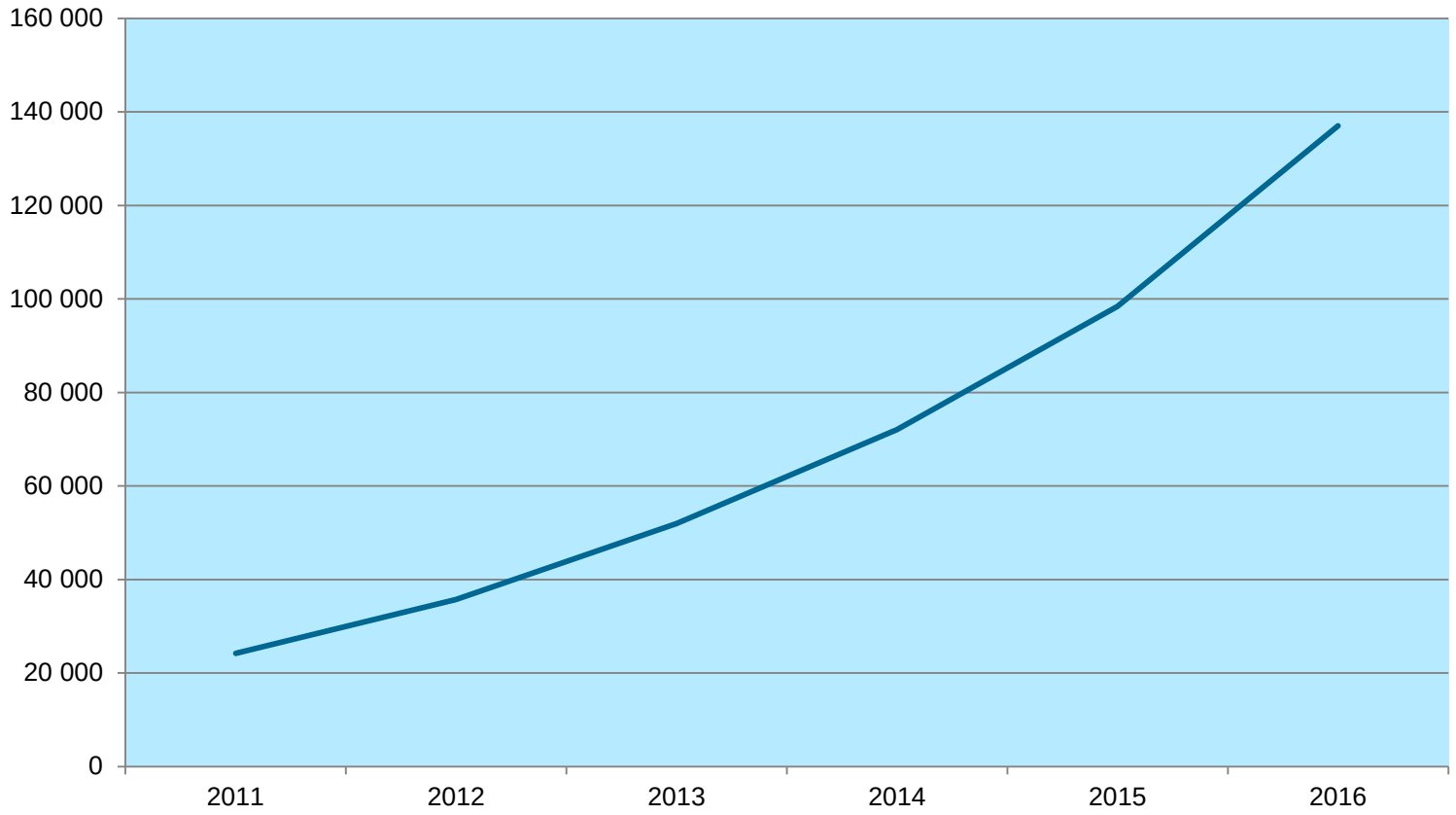
	2012	2013	2014	2015	2016
Antall kort rammet av misbruk	20 332	22 531	38 541	44 900	**68 162**

Kilde: Finanstilsynet og Bits

Fortsatt sterk negativ utvikling i svindel med misbruk av kortinformasjon ved Card-Not-Present (kort ikke er til stede), selv om de direkte tapene ikke er store.

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

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



Kilde: Finanstilsynet og Bits

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 ved svindel med betalingskort	2012	2013	2014	2015	2016
Antall kort rammet av misbruk (antall)	20 332	22 531	38 541	44 900	68 162
Samlede direkte tap, jf. tabell 1	135 153	140 043	164 113	188 660	206 503
Saksbehandlerkostnader hos kortutsteder (2.250 kroner per kort)	45 747	50 695	86 717	101 025	153 365
Forbrukerkostnader, 1.000 kroner per kort	20 332	22 531	38 541	44 900	68 162
Samlet beregnet kostnad	**201 232**	**213 269**	**289 371**	**334 585**	**428 030**

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

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

Kilde: Finanstilsynet og Bits

Tap ved CEO-fraud
(tall i hele tusen kroner)

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Tabell 4: Tap ved CEO-fraud (beløp i hele tusen kroner)

Tap ved CEO-fraud	2016
Antall saker	214
Gjennomsnittlig tap per sak	1 374
TOTALT	294 061

Kilde: Finanstilsynet og Bits

Utviklingstrekk

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Den digitale kriminaliteten fortsetter å øke og endrer trusselbildet for finansnæringen
  - Phishing, sosial manipulering og trojanere
  - DDoS-angrep og krypteringsvirus
  - Angrep rettet mot foretaks applikasjoner som skaper transaksjoner for overførsel gjennom Swift-nettverket
  - "Vannhull"-angrep
- Teknologisk utvikling har stor innvirkning på tjenesteutviklingen i finansnæringen
  - FinTech, både ny teknologi, nye selskaper og nye samarbeidsformer
  - Finanstilsynet er bedt av Finansdepartementet å vurdere hvordan et lavterskel kontaktpunkt for veiledning av innovative virksomhet kan etableres
  - Open Banking / API-banking vil skape nye distribusjons- og samarbeidsformer
  - Distributed Ledger Technology forventes **på sikt** å bidra til videre digitalisering og effektivisering av prosesser i finanssektoren
  - Mobilens funksjoner og mobile betalingsløsninger
- Endringer i reguleringer, som PSD 2, åpner for nye aktører og løsninger - utfordrer etablerte forretningsmodeller
- Endringer i regelverk både nasjonalt og fra EU → påvirker foretakenes IKT-løsninger
- Bits, finansnæringens infrastrukturselskap, pådriver i utvikling av felles løsninger for næringen

Utkontraktering

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Meldeplikten om utkontraktering av foretaks IKT-virksomhet er et viktig verktøy for Finanstilsynet i oppfølgingen av at foretakene både etterlever regelverk og gjennomfører utkontrakteringen på en forsvarlig måte
- Meldeplikten gir tilsynet god oversikt over markedet for utkontraktering
- Det ble også i 2016 behandlet et betydelig antall meldinger om utkontraktering av IKT
- Flere av avtalene oppfylte ikke kravene i IKT-forskriften
- Etter påtrykk fra Finanstilsynet og finansnæringen, har nye tjenesteleverandører som tradisjonelt ikke har levert driftstjenester til finansnæringen tilpasset sine kontrakter, slik at de følger regelverket finansforetakene er pålagt å etterleve

- Rundskriv 14/2010 Utflytting av bankenes IKT-oppgaver er planlagt revidert ut i fra
  - Vurdering utkontraktering av oppgaver fra aktører innenfor betalingsformidling og annen finansiell infrastruktur
  - EBAs kommende retningslinjer om utkontraktering og skytjenester

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:
  - BankID – særlig på mobil – forårsaket problemer
  - Manglende sikkerhetstenking ved design av løsninger
  - Mangel på kvalifiserte ressurser for både stormaskin, tradisjonell programmering og sikkerhetskompetanse
  - Kunnskap om bruk, arkitektur og oppfølging av skyløsninger
  - Sikkerhet og tilgangsstyring – beskyttelse av foretaksinformasjon
  - Time to market
  - Kriminelle organisasjoner benytter kunstig intelligens
  - Phishing

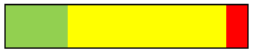
Spørreundersøkelser med foretakene 1

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

Eksempel på tabell fra rapporten

Tabell 7: Data er ikke tilstrekkelig beskyttet

	Sårbarhet	Foretakenes svar	Trend 2016	Trend 2015
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	Mulig inntrenging i våre systemer		→	→
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

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. Utkontraktering, off-shoring og midlertidig, innleid kompetanse skaper utfordringer
   - Inntrenging i systemene anses fortsatt som betydelig en trussel.
4. ID-tyveri
   - Skadevare og misbruk av rettigheter i forbindelse med ID-tyveri utgjør fortsatt en trussel
   - Trussel fra "skimming-" og "Card-not-present"-svindel fortsatt betydelig
5. Misbruk av tilgang til datasystemene
   - Trusselbildet uendret fra foregående år
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

Samlet sett synes foretakenes syn på risikobildet å være svakt økende i 2016, noe det også var i 2015.

Risikoområder påpekt fra andre kilder med særlig relevans for finansnæringen

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Både NSM sin publikasjon "Helhetlig IKT-risikobilde 2016", PST sin trusselvurdering for 2017 og Militære E-tjenestens analyse "Fokus 2017" peker på trusselen knyttet til tilgang til sensitiv informasjon og hvordan både statlige og kriminelle aktører arbeider aktivt for å få tilgang til personer i virksomheter som behandler sensitiv informasjon og teknologi

- Den sensitive informasjonen det siktes til i rapportene, er informasjon om norske foretaks strategi, teknologi og finansielle situasjon. Finanstilsynet vurderer derfor at tyngden av informasjon som rammes av disse truslene vil finnes på verdipapirområdet og i verdipapirforetakene spesielt, men at slik informasjon også finnes andre steder som hos bankenes corporate-funksjoner og i foretakenes økonomienheter

5. Endringer i reguleringer

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- En av de mest sentrale regelendringene er EUs nye betalingstjenestedirektivet (PSD 2) og de ti anbefalinger eller utfyllende bestemmelser som er tillagt EBA å utforme
  - Det åpner for at nye aktører kan tilby betalingstjenester og gis rett til tilgang til betalingskonto.
- Andre større regelendringer i EU er
  - Ny personvernsforordning som trer i kraft i EU i 2018
  - EUs direktiv for nettverks- og informasjonssikkerhet
  - Ny avtale om overføring av data mellom EU/EØS og USA – Privacy Shield
  - Retningslinjer for vurdering av foretakenes operasjonelle IT-risiko
- Større norske regelendringer basert på endringer i EU regelverk
  - MiFID II - Markets in Financial Instruments Directive og MiFIR - Markets in Financial Instruments Regulation
  - EMIR - The European Market Infrastructure Regulation
  - Ny lov og forskrift om tiltak mot hvitvasking og terrorfinansiering
  - Forskrift om formidlingsgebyr i kortordninger
- Norske regelendringer
  - Forslag til ny sikkerhetslov

6. Finanstilsynets oppsummerende vurdering av risikobildet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Finansiell infrastruktur
2. Foretakene
3. Forbrukere

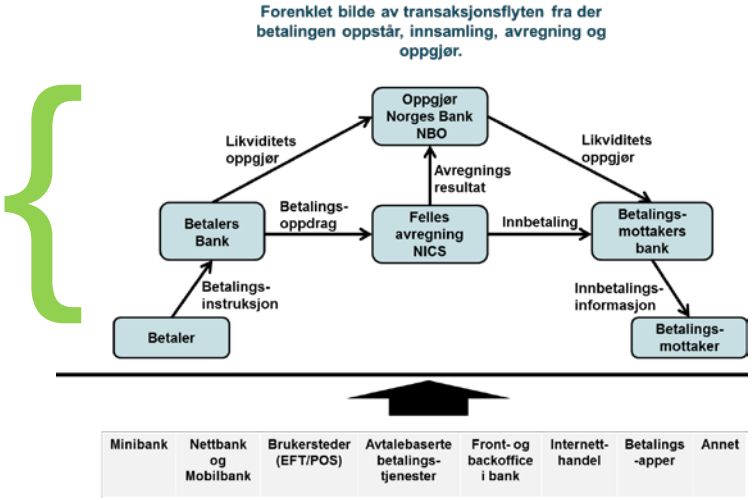
Finansiell infrastruktur

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- **Stabiliteten i den finansielle infrastrukturen var i 2016 god og på linje med 2015 og den ble rammet av færre operasjonelle hendelser.**

- 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 betalingsløsningene utilgjengelige i kortere perioder, vurderer Finanstilsynet den norske finansielle infrastrukturen som solid og stabil.**

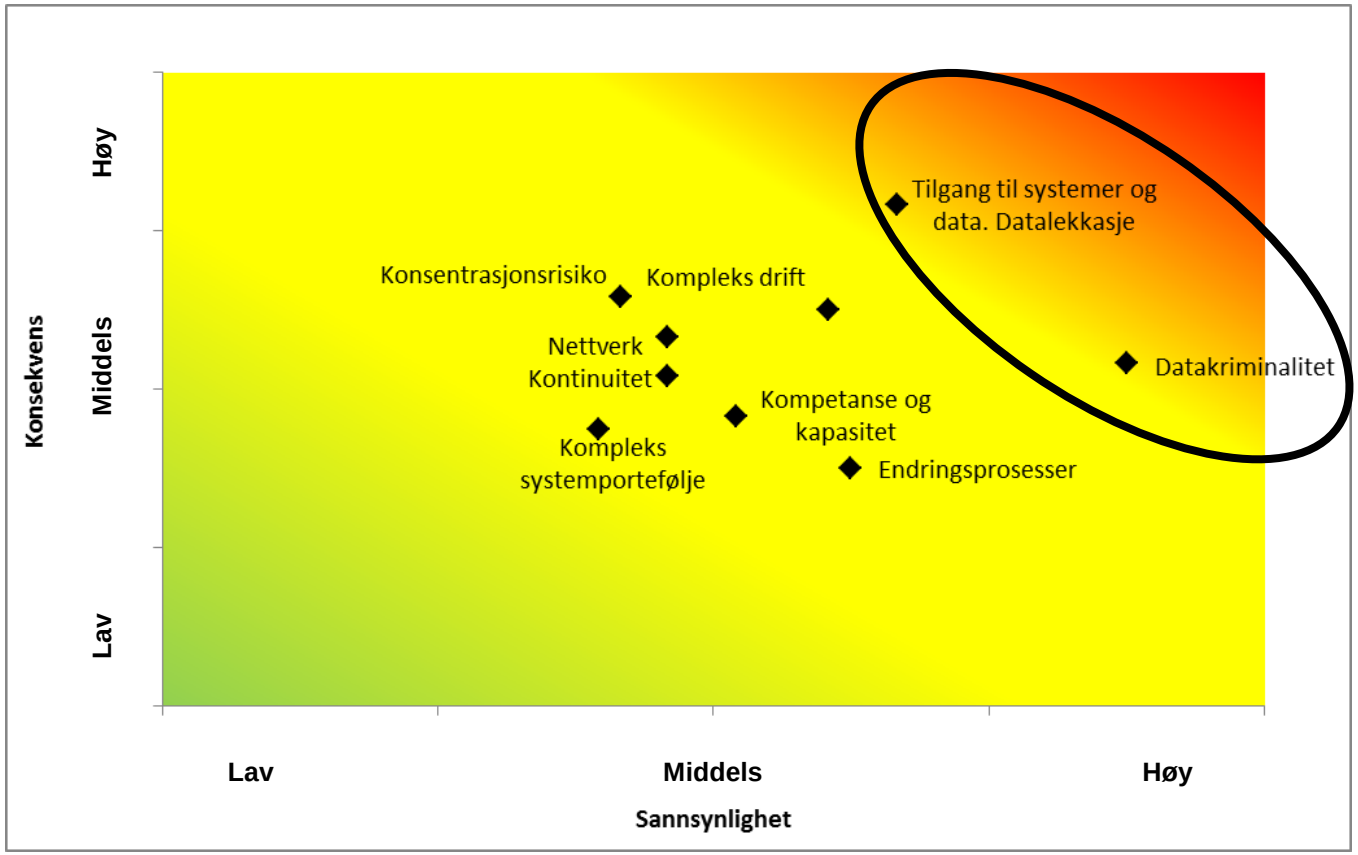


- Funn fra tilsynsvirksomheten viste imidlertid svakheter når det gjelder styring og kontroll med tilganger til systemer som kan inneholde markedssensitiv informasjon

Foretakene -

Finanstilsynets vurdering av de mest sentrale truslene mot og sårbarhetene i foretakenes systemer

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY



Finanstilsynets vurderer

- Tilganger til systemer og data og datalekkasje
- Datakriminalitet

som de mest sentrale truslene mot og sårbarhetene i foretakenes systemer

- Kompleks drift
- Konsentrasjonsrisiko
- Feil i nettverk

utgjør også sentrale trusler og sårbarheter

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

- Risiko ved bruk av e-handelssystemer for verdipapirhandel
  - Forbrukere som handler aktivt gjennom e-handelssystemer for verdipapirhandel er sårbare for bortfall av tilgang til systemet, mens profesjonelle aktører ofte har tilgang til alternative e-handelssystemer for gjennomføring av handler
- Brukergrupper blir stengt ute
  - Enkelte grupper av forbrukere, blant annet eldre, får problemer når digitaliseringen medfører bortfall av eller vanskeliggjør bruk av manuelle betalingstjenester
- Brukerne påføres risiko
  - Manglende etterlevelse av retningslinjer for sikkerhet i Internett-betalinger hos betalingstjenesteytere reduserer forbrukerens muligheter til å beskytte seg mot svindel

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. Oppfølging av trusselbildet knyttet til digital kriminalitet
6. Forbrukervern

Oppsummering

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Den finansielle infrastrukturen i Norge er robust og det var ingen alvorlige IKT-hendelser med konsekvenser for finansiell stabilitet
- Operasjonelle hendelser utgjorde 121 av de 131 rapporterte hendelsene, resterende 10 var sikkerhetshendelser
- Betalingssystemene er generelt solide og stabile, selv om det inntraff enkelte hendelser som medførte utilgjengelige i kortere perioder. På enkelte områder likevel rom for forbedringer
  - Blant annet kapasitetsovervåkning, kapasitetsstyring og kriseløsninger og styring av operasjonell risiko kan bli bedre.
- Nedgang i antall hendelser med konsekvens for hhv. enkeltforetak og forbrukerne
- Betalingssystemene og kunderettede tjenester mer tilgjengelige i 2016 enn året før
- Vurdering av IT-risikoer kan bli bedre, også ved utkontraktering
- Samlede tap ved bruk av nettbank økte betydelig fra 2015 til 2016, men er likevel små
- Fortsatt økning i tap ved kortsvindel med stjålet kortinformasjon, særlig Card-Not-Present
- Samlede kostnader forbundet med kortsvindel er betydelige
- Digital kriminalitet, urettmessig tilgang til systemer og data og datalekkasje vurderes som de største truslene mot og sårbarhetene i foretakenes systemer
  - Digital kriminalitet øker i omfang og kompleksitet og gjør at risikoen er høyere enn i 2015
  - Det er betydelige mangler når det gjelder kontroll med tilgang til systemer og data, og risikoen har tiltatt siden 2015
  - Det økende trusselbildet krever bedre beskyttelse av sensitiv informasjon

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