



FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Pressebriefing 9. april 2015

Risiko- og sårbarhetsanalyse (ROS) 2014 Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi

Seksjonssjef Olav Johannessen



ROS-analysen 2014:

1. Innledning
2. Oppsummering
3. Finanstilsynets funn
4. Andre observasjoner
5. Utviklingstrekk, Aktuelle trender som kan påvirke risiko
6. Risikoområder
7. Finanstilsynets oppfølging
8. Ordliste

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



- Skaffe oversikt
- Analysere
- Foreslå tiltak



2. Oppsummering

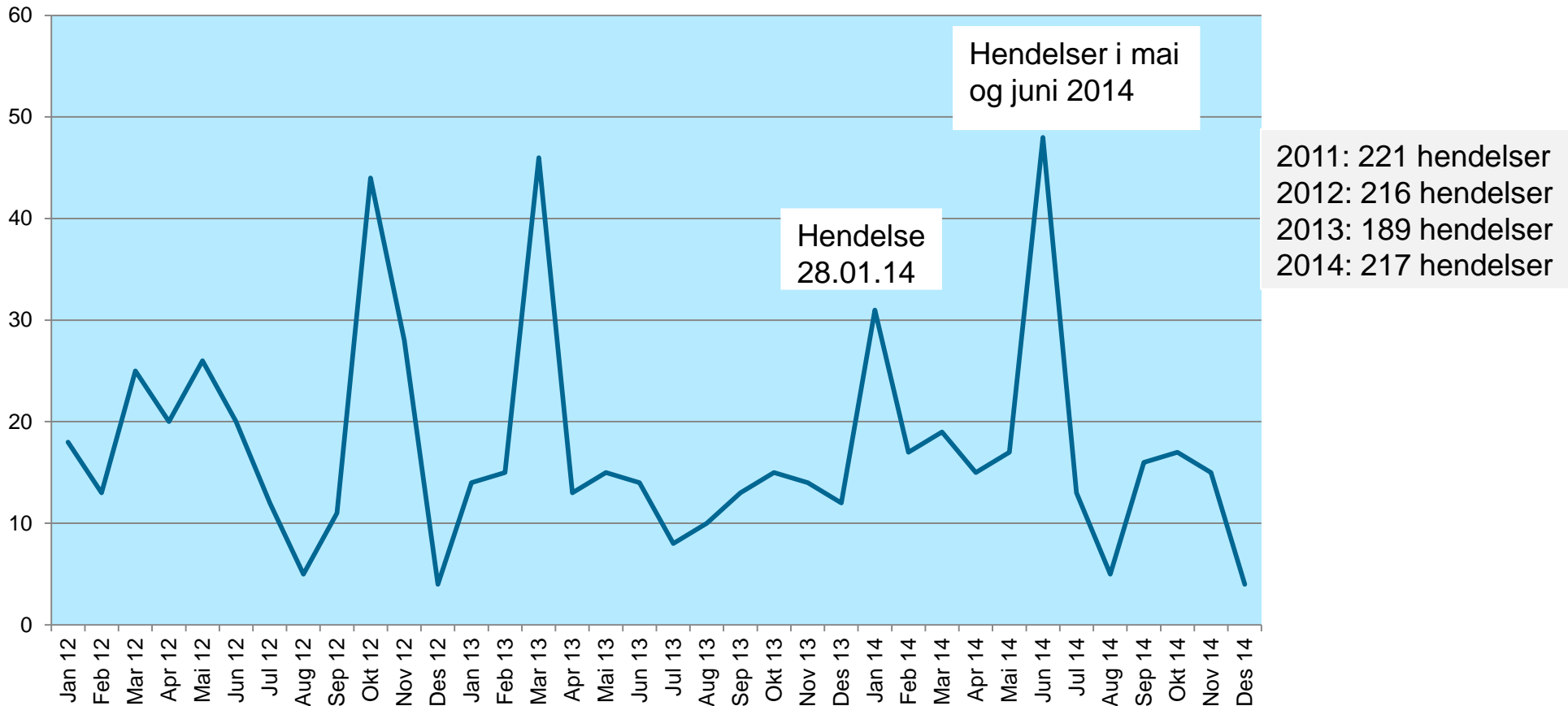
- Betalingstjenestene generelt er stabile og har hovedsakelig en god kvalitet, selv om det i 2014 var en økning i alvorlige hendelser som bidro til å redusere betalingssystemenes tilgjengelighet
- Økt kortsvindel med stjålet kortinformasjon
- Økte tap som skyldes at kundens innloggingsmekanisme er blitt stjålet og misbrukt
- Utviklingen i digital kriminalitet gjør forbrukerne mer sårbare
 - *Det er krevende for forbrukere å forholde seg til trusler og sårbarheter i finansielle tjenester*
- Den alvorligste trusselen er at inntrengere får tilgang til IKT-infrastruktur og applikasjoner gjennom målrettede angrep
- Omfattende endringer i finanssektorens IKT-virksomhet
 - *Endringene kan gi forbedringer, men de kan også skape nye sårbarheter.*

3. Finanstilsynets funn

1. Rapporterte hendelser 2014
2. Funn, observasjoner og vurderinger
 - Betalingssystemer og utvikling. Tapstall
 - Verdipapirområdet
 - Bank
 - Forsikring
 - Funn i andre foretak
3. Forbrukerområdet

Antall rapporterte hendelser i perioden 2012–2014

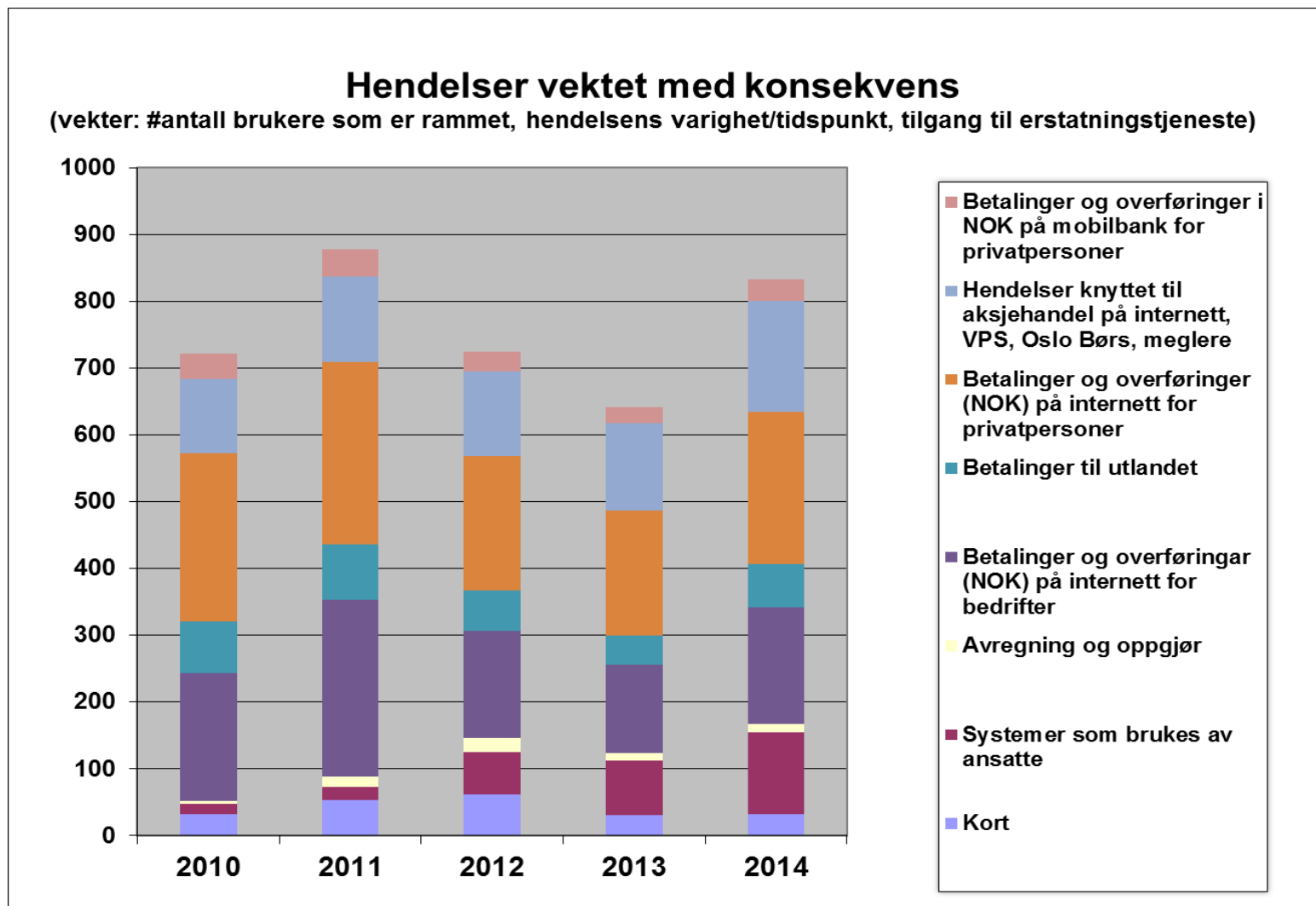
Figur 2: Antall rapporterte hendelser i perioden 2012–2014



Kilde: Finanstilsynet

Hendelser vektet med konsekvens

Figur 4: Hendelser vektet med konsekvens



Kilde: Finanstilsynet

Betalingstjenester

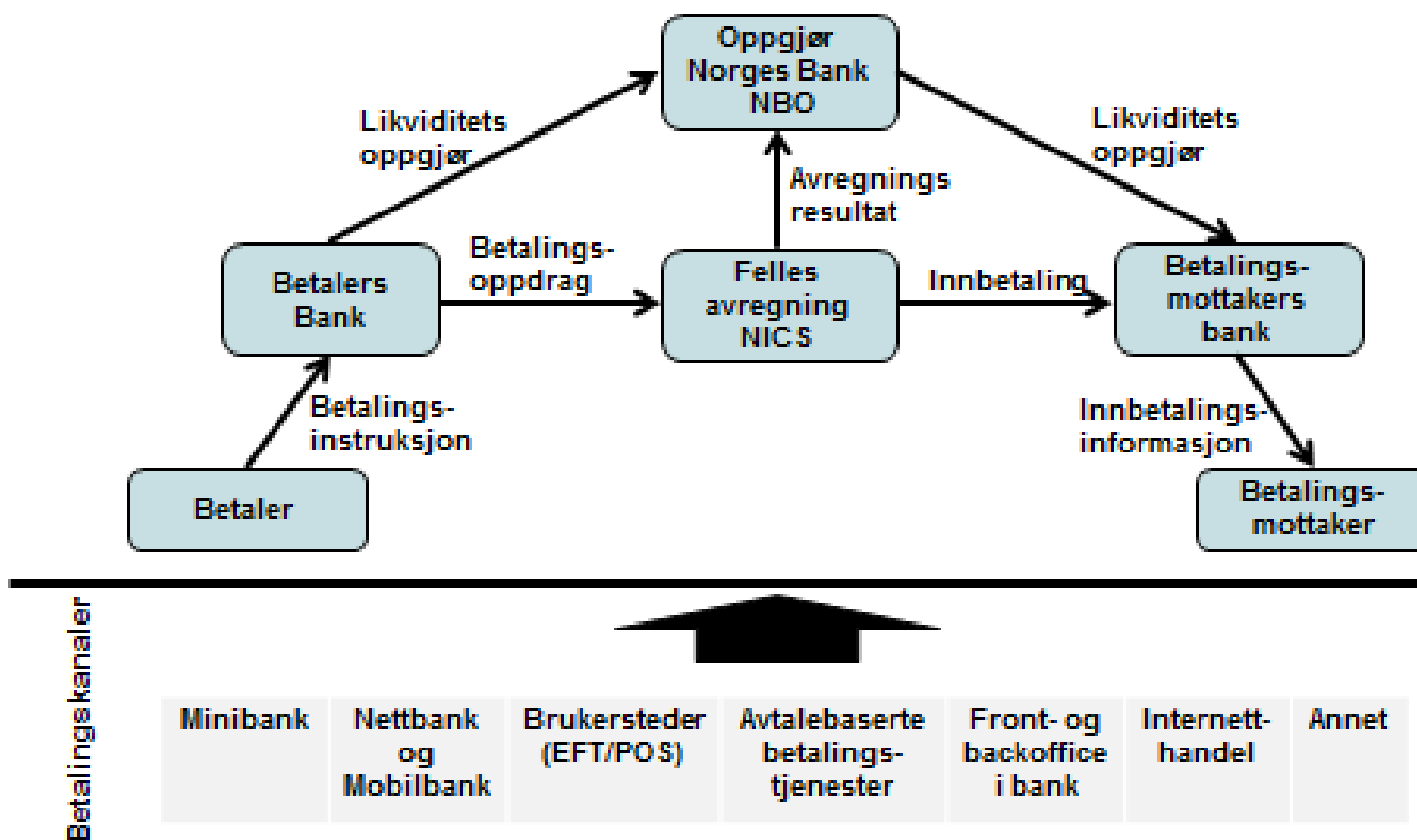
1. Flere alvorlige hendelser rammet betalingsformidlingen
2. Hendelser som oppstår i, eller treffer betalingsinfrastrukturen, rammer bredt og medfører raskt store konsekvenser
3. Endringer hyppig årsak til feil og avvik og det er derfor knyttet betydelig risiko knytte til dette
4. Robustheten i løsninger samsvarer i enkelte sammenhenger ikke med betalingsformidlingens sentrale rolle
5. Svakheter i driftsløsninger som skal sikre kontinuitet for betalingsformidlingen
6. Enkelte foretak har mangler i sine avtaler, bl.a. IKT-forskriftens regler om utkontraktering
7. Rask utvikling innen mobile betalingsløsninger, nasjonalt og internasjonalt
8. Finanstilsynet har gjort sårbarhetsvurderinger knyttet til mobilbaserte betalingsløsninger

Betalingstjenester - 2

9. Fortsatt angrep som rammer betalingsformidlingen
 - *DDoS, phishing, trojanere, tyveri av kortinformasjon*
10. Ikke kjent med svindelforsøk via mobiltelefon i Norge
11. Finanstilsynets erfaring er at foretakene har god beredskap, at de har etablert godt forsvarsverk og at de iverksetter effektive tiltak som reduserer både skadeomfang og kunders tapsomfang

Transaksjonsflyten i det norske betalingssystemet

Forenklet bilde av transaksjonsflyten fra der betalingen oppstår, innsamling, avregning og oppgjør.



Stabil
sentral
betalings-
infrastruktur

Flere
hendelser hos
foretakene
som rammer
betalings-
tjenestene

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

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

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

Kilde: Finanstilsynet

Antall betalingskort rammet av misbruk

Tabell 2: Antall betalingskort rammet av misbruk

Svindeltype betalingskort	2011	2012	2013	2014
Antall kort rammet av misbruk	16 784	20 332	22 531	38 541

Kilde: Finanstilsynet

Totaltaper på kortsvindel økte også i 2014. Det var også i 2014 en betydelig økning i svindel av typen «card-not-present» (CNP), mens det var en reduksjon i tapene knyttet til andre typer kortsvindel.

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

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

Svindeltype nettbank	2011	2012	2013	2014
Angrep ved bruk av ondartet programkode på kundens PC (trojaner)	664	5 064	1 327	552
Tapt/stålet sikkerhetsmekanisme	3 321	3 367	1 321	6 655
TOTALT	3 985	8 431	2 648	7 207

Kilde: Finanstilsynet

Verdipapirområdet

1. Høy stabilitet og god kvalitet kjennetegner verdipapirområdet
2. Betydelig endringsomfang på regelverksområdet (EU) vil påvirke infrastrukturen og innebærer endringsrisiko med behov for kvalitetssikring
3. Gamle såkalte legacy-systemer representerer en utfordring, og en fornyelse innebærer risiko under gjennomføringen
4. Bruk av skybaserte tjenester kan gi nye utfordringer ved at forretningsansvarlige i foretak går til «innkjøp» av IKT-tjenester uten å gå via egen IT-avdeling
5. Mangelfulle tilgangskontroller til sensitiv informasjon
6. Bruk av samme nettverksinfrastrukturer representerer en konsentrasjonsrisiko

1. Endringer på driftsleverandørsiden, både eierskifter og bytte av leverandører kan øke risikoen spesielt i endringsperioden
2. Reetablering av IKT-tjenester i en katastrofesituasjon vil kunne ta lenger tid enn antatt
3. Foretakene må sikre egen styring og kontroll av IKT-virksomheten, også ved utkontraktering
4. Manglende etterlevelse om krav til datasystemer og rapportering til Bankenes sikringsfond dersom foretaket blir satt under offentlig administrasjon
5. Mangelfull gjennomgang og kontroll av ansattes tilganger til systemer og applikasjoner
6. Utfordrende å styre og kontrollere klassifiseringsregler, spesielt mht. tilganger til graderte data og systemer

1. Komplekse forsikringssystemer med sensitiv informasjon krever sikker og betryggende forvaltning og etablerte reserveløsninger
2. Få rapporterte hendelser tyder på god endringskontroll
3. De fleste hendelsene er knyttet til konfidensialitetsbrudd
4. Mangler i etterlevelse av forskriftenes krav ved utkontraktering
 - *Kan medføre mangelfull oversikt over, og kontroll med, IKT-virksomhet og IKT-risikoer*
5. Risikoanalyser ofte fragmenterte, mangelfulle og dekker ikke selskapets samlede IKT-virksomhet
6. Testing av kontinuitets- og katastrofeplaner synes å være et forbedringsområde
7. Sensitiv informasjon, kan være av interesse for inntrengere

- Finanstilsynet gjør enkelte stedlige IT-tilsyn i inkassoselskaper og eiendomsmeglingsforetak. I tillegg må eiendomsmeglingsforetakene og inkassoselskapene svare på et forenklet egnevalueringsskjema med spørsmål om IT-virksomheten ved ordinære fagtilsyn.
- Finanstilsynet hadde i 2014 merknader til
 - Manglende beredskapsløsninger
 - Sikring av konfidensiell informasjon
 - Manglende rutiner for å håndtere sikkerhetshendelser
 - At foretaket peker på IT-leverandøren som ansvarlig for IT-prosessene.

1. Mangelfull ID-sjekk ved utlevering av BankID kan få store konsekvenser for den rammende forbruker
 - *Gjaldt 15 av 150000 utleveringer i 2014*
2. Forbrukere kan bli svindlet ved netthandel mellom private parter dersom de ikke gjør bruk av handelssteders betalingstjenester
3. Forbruker må forsikre seg om at nettstedet har den nødvendige sikkerhet, som f.eks. kryptering (hengelås i adressefeltet)

4. Andre observasjoner

1. Foretakenes vurdering av risiko
 - Intervjuer
 - Spørreundersøkelse
2. Risikoområder påpekt fra andre kilder
 - Intervju med sikkerhetselskaper og internettjenesteleverandører
 - Rapporter fra internasjonale sikkerhetsorganisasjoner

Intervjuer og spørreundersøkelser med foretakene

1. De mest fremtredende truslene synes å være at inntrengere får tilgang til IKT-infrastruktur og applikasjoner gjennom målrettede angrep.
2. Andre trusselområder som representerer betydelig risiko er:
 - økningen i IKT- og cyberkriminalitet
 - sikkerhetshull i programvare som kan utnyttes av kriminelle
 - den sterke avhengigheten til Internett
 - ansattes bruk av sosiale medier
 - informasjon som kommer på avveie
 - ✓ Utlevering av BankID kodebrikke, Personopplysninger
3. Kompleksitet i IKT-løsninger utgjør også en høy risiko for datakvalitet og stabil drift, og kan hindre nyutvikling.

Støtte for strategiske beslutninger

	Sårbarhet	Foretakenes svar	Trend
1	Systemenes evne til å innhente og sammenstiller all relevant informasjon fra interne og eksterne kilder for beslutningsformål		↘
2	Systemer for beslutningsstøtte og rapportering henter relevant informasjon fra foretakets produksjonssystemer og sammenstiller og synkroniserer informasjonen til et bilde av foretakets risiko til bruk i styringsøyemed og til myndighetsrapportering.		↘
3	Systemene gir automatisk et totalbilde av risikoen, for eksempel slik at hvis en hjemstedsbedrift går konkurs, så varsler systemet automatisk om lån til ansatte i bedriften og lån til leverandører til bedriften, slik at vi kan vurdere å tapsavskrive på disse.		↘
4	Systemene identifiserer automatisk muligheter for mersalg.		↘
5	Datakvalitet		↘
6	Integrasjon og synkronisering mellom systemene		↘
7	Når nye IT-løsninger skal utvikles, tar vi i betraktning behovene og løsningene til alle relevante avdelinger. Dette for å unngå utfordringer forbundet med "silo-løsninger" slik som omfattende vedlikehold av programmer, komplisert drift og utfordringer med synkronisering av data.		↘
8	Grad av kompleksitet i IT-systemene		→
9	Grad av mangler og feil i systemene		→

Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet.

Avvik i driften

Sårbarhet		Foretakenes svar	Trend
1	Organisering, rutiner, stillingsbeskrivelse, rapportering og kontroll		✓
2	Grad av kompleksitet i driften		→
3	Test-systemene er "produksjonslike", dvs. at systemene har testdata, applikasjoner, programvare, styresystemer (SW) og annet som sikrer mot "overraskelser" når nye applikasjoner skal i produksjon.		✓
4	Vi gjør endringer i infrastrukturen ("ikke- funksjonelle" endringer) i trafikkstille perioder, og kan reversere endringen og rulle tilbake på kort tid hvis nødvendig.		→
5	Vår evne til å avdekke alle svakheter		✓
6	Kontroller som skal sikre at alle maskiner og programmer er inkludert i IDS/IDP, brannmur og virus og andre tiltak for å sikre stabil drift		→
7	"Tikkende miner", dvs. komponenter som gradvis slites eller verdier som gradvis når terskelverdien uten at vi er oppmerksom på det, for eksempel minnelekkasje, elektroniske komponenter som slites, energiforsyning som "slites" (batterier eller annet)		→
8	Logger og vår evne til å reagere på loggene		✓
9	Vår evne til å avdekke avvik i driftsmønsteret og ta aksjon før skade (avvik når det gjelder trafikkmønster, porter, protokoller, avvikende svarstider osv.)		✓
10	Dataangrep (Advanced persistence threat, trojaner, ransomware, DDoS)		→
11	Kvaliteten på kontinuitet- og katastrofeløsningene våre		✓
12	Samarbeidsrutiner med leverandører		→
13	Leveransepress		→
14	Kompetansen vi besitter		✓
15	Mengden av endringer (ny leverandør, nye grunnsystemer)		→
16	Vår kunnskap om hvor datalinjene går og redundans når det gjelder datalinjer		→
17	Tilgangskontroll, adgangskontroll og tjenstedeling ("segregation of duty")		→

Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet.

Data er ikke tilstrekkelig beskyttet

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

Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet.

ID-tyveri




Sårbarhet		Foretakenes svar	Trend
1	Skadevare som infiserer en bruker og misbruker den infiserte brukeren sine rettigheter		→
2	Kontroll når det gjelder utlevering og bruk av logon-id og passord til kunder og medarbeidere (BankID, ansatte-id, systembrukere, admin-brukere)		→
3	Innsyn i kundedata		→
4	Kort ("Card not present, skimming")		→

Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet.

Misbruk av tilgang til datasystemene

Sårbarhet		Foretakenes svar	Trend
1	Tilgangskontroll		→
2	Tjenestedeling		→
3	Logging		→
4	Markedsovervåking		→
5	Analyse av "mistenkelige" transaksjoner som tilbakevaluering, bevegelser på interne kontoer, overføring fra kunde til ansatt og tilbake		→
Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet.			

Hvitvasking

	Sårbarhet	Foretakenes svar	Trend
1	Markedsovervåking		→
2	IT-systemenes evne til å samle informasjon om kunde, kunderelasjoner og kundedferd (KYC- Know Your Customer)		→
3	Elektronisk overvåking av transaksjoner – presisjon i flagging av mistenkelig transaksjoner		→

Grønt: lav sårbarhet. Gult: middels sårbarhet. Rødt: høy sårbarhet.

Risikoområder påpekt fra andre kilder

- Norge et av de minst infiserte land når det gjelder PC-virus
- Foretakene bør sørge for at ISP-er tar en mer aktiv rolle i bekjempelse av DDoS og spam
- Advanced Persistent Threat (APT) - den største trusselen fra nettet
 - *Brukermedvirkning finnes i nesten 50 prosent av APT-inntrenginger*
- Foretakene må sikre at informasjon ikke kommer på avveie
- Sikkerhetsatferd viktig. 80–20-regelen kan benyttes i fordeling mellom menneskelige og teknologiske svakheter
- Datainnbrudd globalt økt i frekvens med 25 prosent siste året.
 - *Manglende sikkerhet i sluttbrugerleddet årsak til mer enn 50 prosent av innbruddene*
- Viktig å holde oppe forsvaret mot ondsinnede angrep fra nettet, feil kan medføre alvorlige konsekvenser både for foretaket og kundene.

Finanstilsynets oppsummering av IKT- og internettbasert kriminalitet

- Trusselen fra cyberangrep øker ved at verktøyene som benyttes, blir mer sofistikerte og at metodene som benyttes, blir mer varierte
- Angrepene som gjøres, er målrettede og utføres ofte av organisasjoner som baserer forretningsdriften sin på kriminell virksomhet
- Denne typen organisasjoner har gjerne tilgang til ressurser med stor kunnskap innenfor IKT-området, nødvendig datakapasitet og god tilgang på finansiering av virksomheten

5. Utviklingstrekk

1. Økende digital kriminalitet. Myndighetene vier dette større oppmerksomhet
2. Endringer i tjenesteleverandørmarkedet, organisering og eierskap og utkontrakteringslandskapet
3. Utviklingen i teknologi åpner for utvikling av mer effektive og brukervennlige tjenester. Høy endringstakt innenfor mobilbaserte betalingstjenester og utviklingen i sikkerhetsløsninger
4. Endringer i regelverk både
 - Nasjonalt
 - EU
5. Fellestiltak fra finansnæringen
6. Virtuelle valutaer

6. Finanstilsynets oppsummerende vurdering av risikobildet

1. Aktuelle risikoområder er vurdert ut fra kontrollmålene integritet, konfidensialitet, tilgjengelighet og at IT fungerer tilfredsstillende som støtte for forretningsdriften.
2. Risikoen knyttet til integritet er høy og økende, risikoen knyttet til konfidensialitet er middels og stabil, risikoen knyttet til tilgjengelighet er middels og økende og risikoen knyttet til at IT fungerer tilfredsstillende som støtte for forretningsdriften er middels og stabil.
3. Finansforetak var under angrep i 2014. Virkningen har vært dempet som følge av tiltak fra foretakene. Digitale angrep mot finanssektoren kan føre til at markedene og finansiell stabilitet kan bli truet.
4. Endringer i systemer og omgivelser hyppigste feilårsaken hos foretakene, og de må fortsatt ha særlig oppmerksomhet rettet mot dette området.
5. Det er krevende for forbrukere å forholde seg til trusler og sårbarheter i finansielle tjenester på en kvalifisert måte, og finansnæringen har et stort ansvar for å bygge inn tilstrekkelig sikkerhet i løsningene.

7. Finanstilsynets oppfølging

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

Takk for oppmerksomheten!

Olav Johannessen
Seksjonssjef seksjon for tilsyn med IT og betalingstjenester
E-post: ola@finanstilsynet.no

FINANSTILSYNET

Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

www.finanstilsynet.no