FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Pressebriefing 9. mai 2019

Risiko- og sårbarhetsanalyse (ROS) 2018
Finanssektorens bruk av informasjons- og kommunikasjonsteknologi

Seksjonssjef Olav Johannessen
Finanstilsynet

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

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Skaffe oversikt
- Analysere
- Foreslå tiltak

- Resultater fra tilsyn IT og betalingstjenester
- Gjennomførte ROS-intervju og spørre-undersøkelser
- Hendelses-håndtering
  Data fra hendelses-database
- Betalings-tjenester
  Meldeplikt betalings-tjenester
- Melding om utkontrak-tering
  Konsesjons-søknader
- Annen relevant informasjon og overvåking av markedet
- 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. Betalingssystemer og utvikling
2. Bank
3. Verdipapirområdet
4. Forsikring
5. Revisjonsselskaper
6. Betalingsforetak
7. Rapporterte hendelser i 2018
8. Tapstall knyttet til betalingsformidling
9. IKT-sikkerhet og digital kriminalitet
10. Utviklingstrekk innenfor finansiell teknologi
11. Utkontraktering
12. Kort om andre tema

Betalingstjenester og utvikling

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Finanstilsynet observerte få alvorlige hendelser i betalingssystemene i 2018, både i omfang og varighet.
- Betalingsområdet var også i 2018 preget av store endringer, blant annet ved fusjon av Vipps AS, BankAxept AS og BankID AS.
- Bankene har forberedt seg til nye regler som følge av (PSD 2). Trådte i kraft i Norge 1. april 2019. → Tilrettelegge for tilgang til konto for tredjeparter
- Flere banker etablerte avtaler med globale foretak om betalingsløsninger.
- Endringene må ses i lys av økt konkurranse som følge av ny teknologi, regulatoriske endringer og kunders forventninger.
- Antall brukersteder som aksepterer kontaktløse betalinger har økt betydelig. Kundenes betalingsvaner endrer seg gradvis.
- Bruk av biometriske kjennetegn i forbindelse med autentisering og betaling øker, bl.a. bruk av fingeravtrykk ("touch") og ansiktsgjenkjenning for innlogging på mobile løsninger.
- Ny forskrift om systemer for betalingstjenester stiller en rekke krav til styring og kontroll med betalingssystemene og gjelder både banker, betalings- og e-pengeforetak.
- Ifm PSD 2 stilles det utvidede krav om styring og kontroll med risiko og sårbarheten i betalingssystemene.
- Nye aktører søker om konsesjon.

Bank

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Mangler avdekket knyttet til foretakenes virksomhetsstyring på IKT-området innenfor
  - hvordan styrings- og kontrollfunksjoner er etablert
  - organisering og klare rapporteringslinjer
  - sikring av tilstrekkelig kompetanse og ressurser.
- Sikkerhetspolicy må utarbeides i tråd med de forretningsmessige mål og regulatoriske krav som stilles.
- Avdekket mangler innen området kontinuitetsledelse og kriseløsninger knyttet til
  - styrende dokumenter
  - opplæring
  - trening, øvelse og test av kriseløsning.
- Forbedring av tilgangsstyringen, særlig gjelder det ved utvidete tilgangsrettigheter, både mhp personell hos foretakene og leverandører.
- Avdekket feil ved uttrekk fra kildesystem til antihvitvaskingssystem.
- Tilsyn med bankenes etterlevelse av krav til rapportering til Bankenes sikringsfond, viser at rapporteringen stadig bedres og nærmer seg en tilfredsstillende kvalitet.

Verdipapirområdet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Det er avdekket svakheter ved foretaks kriseløsninger, der systemer som skal brukes i en krisesituasjon, ikke har hatt tilstrekkelig kapasitet til å kunne overta relevant driftsbelastning.
- Foretakene har fortsatt behov for å forbedre sin dokumentasjon av retningslinjer, rutiner og planer for gjennomføring av sikkerhetstester.
- Testsystemer som ikke er riktig konfigurert eller ikke likt konfigurert som produksjonssystemet har medført feil ved produksjonssetting.
- Oppdeling av ansvar for kritiske systemer bør unngås og at forretningsansvarlige bør ha totalansvaret for viktige løsninger på eget område.
- Sensitiv informasjon på avveie er en reell risiko og bør prioriteres i foretakenes risikovurderinger.
- Foretakene bør styrke tiltak for å redusere risikoen for sensitiv informasjon på avveie, som
  - styrking av foretakets digitale forsvar
  - klassifisering av informasjon
  - tilgangsstyring og
  - kontroll med dokumentasjon som sendes fra foretaket.

Forsikringsområdet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Innrapporterte hendelser viser at forsikringsforetak har svakheter i egne testrammeverk, som har medført konfidensialitetsbrudd ved driftssetting av løsninger.
- Finanstilsynet har gjennom tilsyn avdekket at foretak ikke har en tilstrekkelig oppfølging av adgangs- og tilgangsrettigheter for egne, og i noen tilfeller også leverandørers, personell.
- Utkontraktert IKT-virksomhet følges ikke opp i samme grad som intern IKT-virksomhet.
- Foretakene må sikre at IT-strategier etableres med klar forankring til forretningsstrategien, revideres jevnlig og oppdateres ved endringer i forretningsstrategien.
- Det observeres fortsatt at IKT-hendelser ikke rapporteres.

Revisjonsselskaper

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Det er avdekket mangel på skriftlige avtaler ved som i tilstrekkelig grad sikrer selskapets styring, innsyn og kontroll med utkontraktert IKT-virksomhet.
- Det er avdekket manglende retningslinjer for testing av forsvaret mot digital kriminalitet, herunder angrep rettet mot selskapets systemer

Betalingsforetak

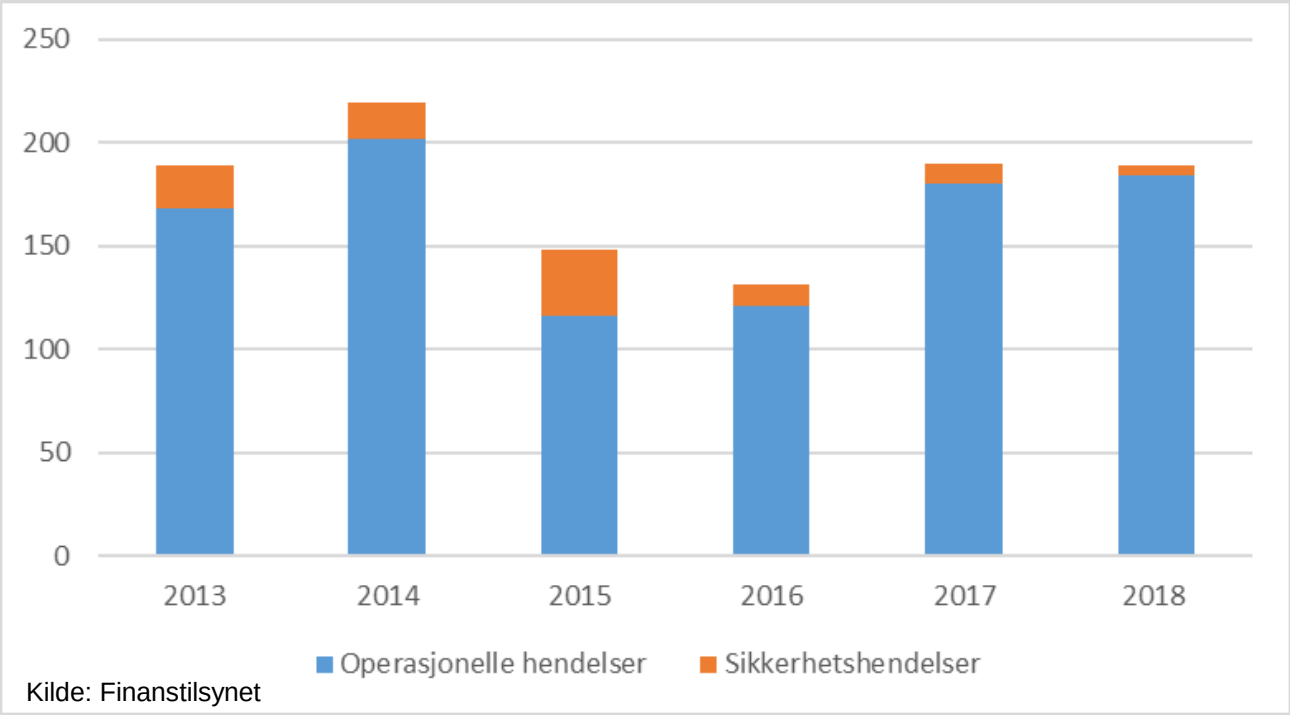
- Mangelfull informasjon om funksjoner i betalingstjenesten
- Mangler i betalingstjenesters funksjonalitet
- Det er avdekket svakheter i betalingsforetaks kundekontroll av brukersteder. Risikoen for hvitvasking og behov for forsterkede kundetiltak er ofte størst på brukerstedssiden.

Antall IKT-hendelser i 2018 på nivå med 2017

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

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

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



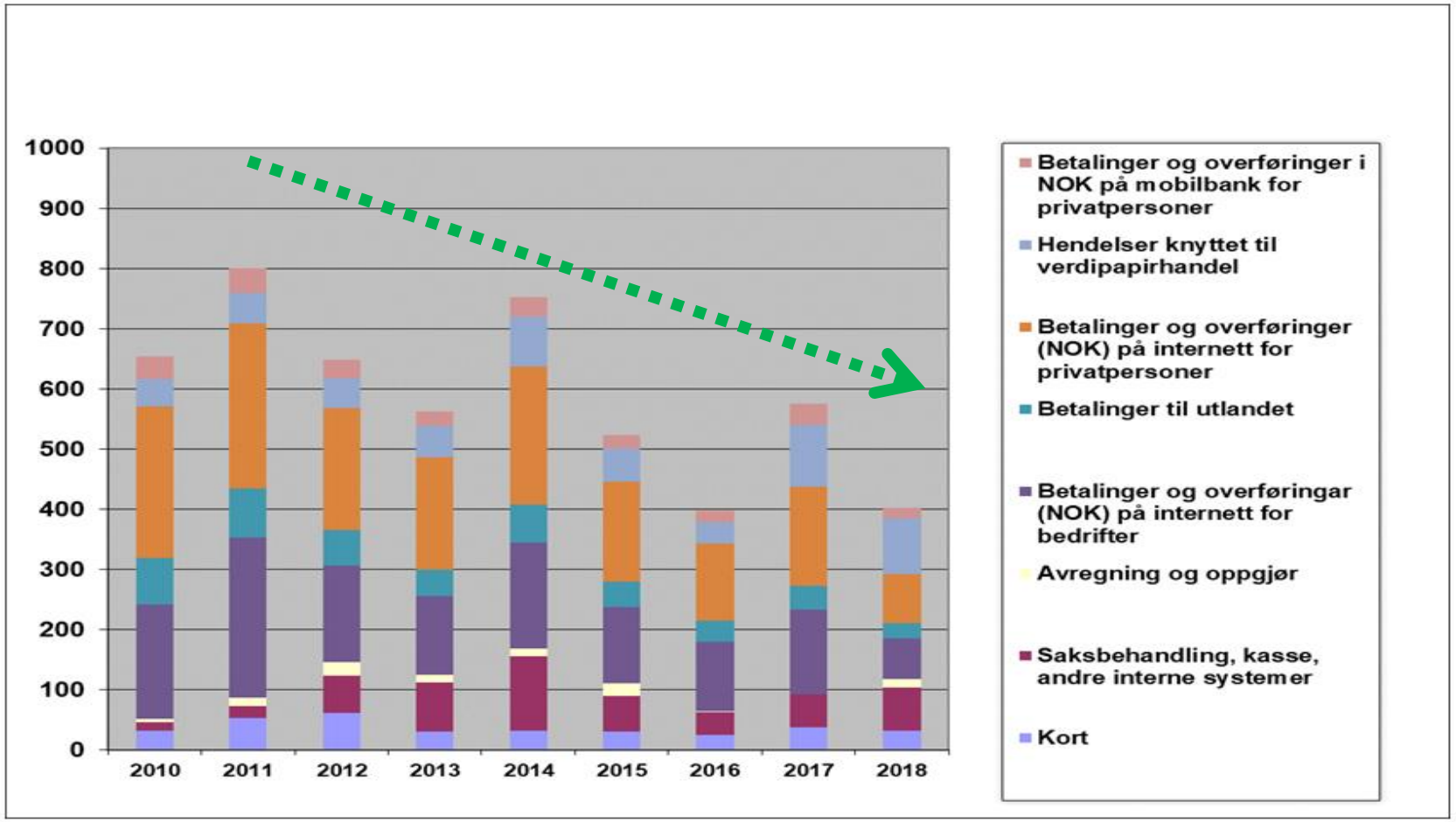
Kilde: Finanstilsynet

	Operasjonelle hendelser rapportert	Sikkerhets hendelser rapportert
2013	168	21
2014	202	17
2015	116	32
2016	121	10
2017	180	10
2018	184	5

→ Alvorlige avvik følges opp løpende

Betalingssystemet og kunderettede løsninger var mer tilgjengelig i 2018 enn i 2017 tross like mye hendelser som i 2017.

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY



Kilde: Finanstilsynet

Rapporterte IKT-hendelser i 2018

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Mest oppmerksomhet fikk hendelsen ved tilløp brann i datasenteret til Nasdaq, der platelager i lagringsenheter havarerte på grunn av akustikk eller økt lufttrykk.
- Flere hendelser rammet Vipps i første halvår av 2018.
  - Sammensatt infrastruktur og ofte bare deler av tjenesten som rammes.
- Det ble rapportert tre hendelser med DDoS-angrep mot banker i 2018.
  - Begrensede konsekvenser til tross for angrep med relativ høy intensitet.
- Enkelte foretak rapporterte om avdekkede sikkerhetshull, uten at disse nødvendigvis hadde blitt utnyttet i ondsinnet hensikt.
- I 2018 var det flere hendelser som skyldes for dårlig styring og kontroll med brukeridentiteter. Ført til gjenbruk av brukeridentiteter og feilkoblinger.
  - Alvorlig brudd på konfidensialitet og
  - Brudd på tilgjengelighet.
- Finanstilsynet mottok for første gang i 2018 rapportering av en hendelse grunnet bruk av robot.
  - Brev ble sendt til feil kunder.

Fortsatt nedgang i 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	2017	2018
Misbruk av kortinformasjon, Card-Not-Present (CNP) (Internett-handel m.m.)	35 701	51 954	72 056	98 410	137 015	102 908	72 909
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort i Norge	2 308	762	524	2 670	1 360	483	3 098
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort utenfor Norge	55 869	51 534	51 685	48 447	41 762	17 452	6 308
Originalkort tapt eller stjålet, misbrukt med PIN i Norge	28 128	21 274	21 266	18 875	12 857	10 194	4 972
Originalkort tapt eller stjålet, misbrukt med PIN utenfor Norge	8 544	9 570	13 071	14 224	10 223	9 663	4 699
Originalkort tapt eller stjålet, misbrukt uten PIN	4 603	4 949	5 510	6 033	3 286	4 891	618
TOTALT	**135 153**	**140 043**	**164 113**	**188 660**	**206 503**	**145 591**	**92 604**

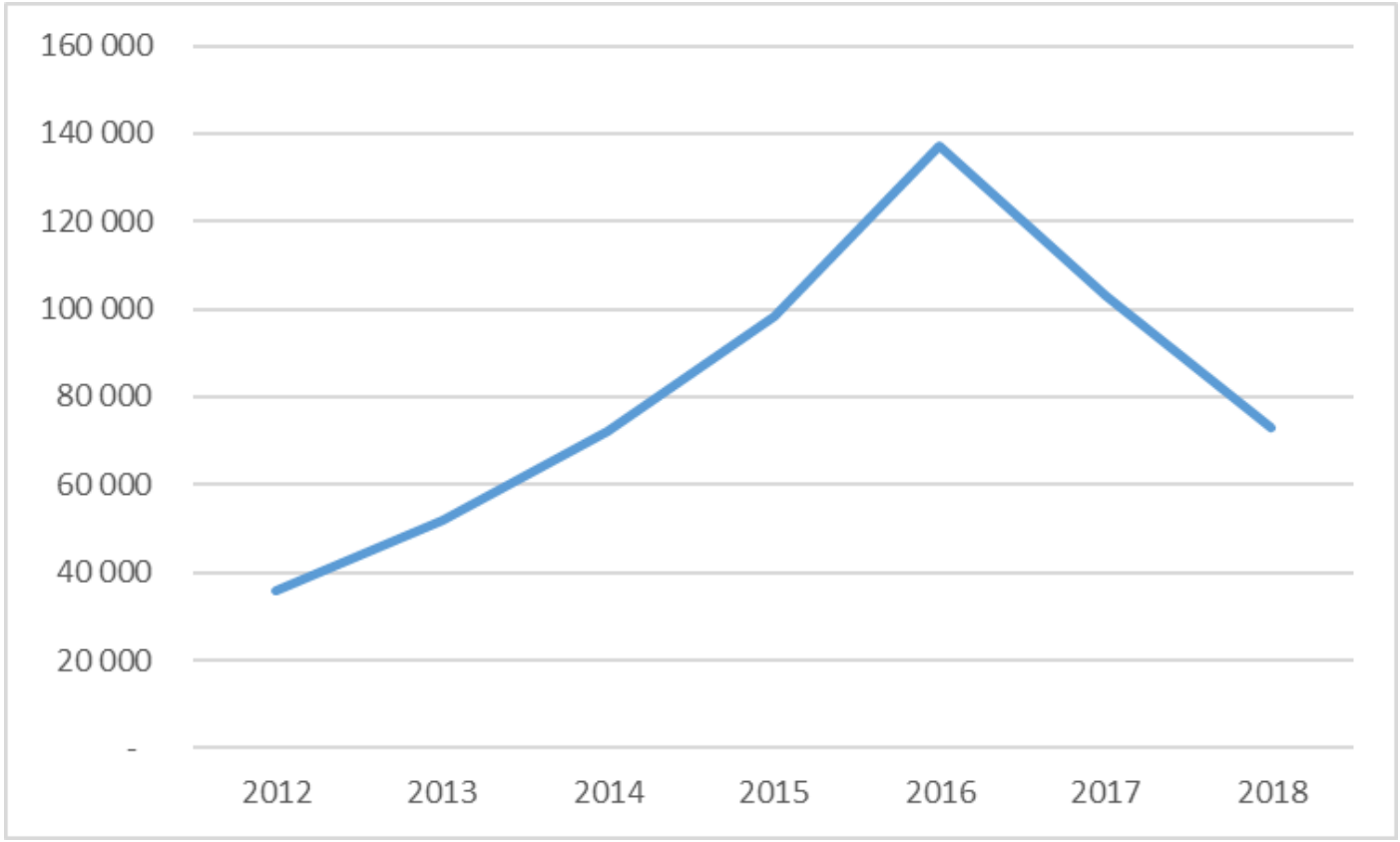
	2012	2013	2014	2015	2016	2017	2018
Antall kort rammet av misbruk (antall)	20 332	22 531	38 541	44 900	68 162	65 024	34 999

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 (tall i hele tusen kroner)

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Figur1: Utvikling i svindel med misbruk av kortinformasjon der kort ikke er til stede (CNP), (tall i hele tusen kroner)



Svindel med misbruk av kortinformasjon der kort ikke er til stede (CNP) utgjør nær 80% av det samlede tapstallet, mens nedgangen utgjør ca 43 av den samlede nedgangen i tap ved bruk av betalingskort .

Kilde: Finanstilsynet og Bits

Beregnede kostnadene forbundet med kortsvindel er halvert siste 2 år
(tall i hele tusen kroner)

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

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

Kostnader ved svindel med betalingskort	2012	2013	2014	2015	2016	2017	2018
Antall kort rammet av misbruk (antall)	20 332	22 531	38 541	44 900	68 162	65 024	34 999
Samlede direkte tap, jf. tabell 1	135 153	140 043	164 113	188 660	206 503	145 591	92 604
Saksbehandlerkostnader hos kortutsteder (2 250 kroner per kort)	45 747	50 695	86 717	101 025	153 365	146 304	78 748
Forbrukerkostnader (1 000 kroner per kort)	20 332	22 531	38 541	44 900	68 162	65 024	34 999
Samlet beregnet kostnad	**201 232**	**213 269**	**289 371**	**334 585**	**428 030**	**356 919**	**206 351**

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	2017	2018
Angrep ved bruk av ondartet programkode på kundens PC eller sikkerhetsmekanisme (trojaner)	5 064	1 327	552	3 055	2	727	1 304
Tapt/stjålet sikkerhetsmekanisme	3 367	1 285	6 655	963	8 758	1 892	874
Phishing og falske BankID-brukersteder	10		539	5815	2 428	2 057	16 384
Annet/ukjent	358	779	3 474	2 715	7 444	2 911	1 624
TOTALT	**8 799**	**3 391**	**11 220**	**12 548**	**18 632**	**7 587**	**20 186**

Kilde: Finanstilsynet og Bits

Rapporterte tap ved svindel gjennom sosial manipulering

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Type svindel i 2018	Antall
Betaling for å leie et objekt mottager av pengene ikke eier	948
Innskudd etter løfter om store utbetalinger senere	9 091
Kjærlighet	88 191
Investeringer i falske selskaper	92 073
Betaling for varer som ikke leveres	11 972
Endret mottakerkonto	8 606
Direktørsvindel	33 913
Falsk faktura	32 982
Andre/nye typer	19 593
TOTALT	**297 369**

Kilde: Finanstilsynet og Bits

IKT-sikkerhet og digital kriminalitet - I

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Angrep, dvs. digital kriminalitet, mot finansforetakene systemer øker betydelig fra år til år.
- Økende grad av oppmerksomhet på et trusselbilde som er i kontinuerlig endring.
- Foretakenes systemer for overvåking stadig bedre, og angrepene avverges som oftest før de får konsekvenser for foretaket. Men, etablering av et tilstrekkelig digitalt forsvar er krevende.
- Ingen sikkerhetshendelser innen norsk finansnæring som kan kategoriseres som alvorlig eller med konsekvenser for finansiell stabilitet.
- Økonomisk vinning så langt hovedmotiv ved målrettede angrep mot finansforetak i andre land.
- Manipulering av betaleren gjennom en kombinasjon av digital og sosial manipulering lykkes i størst grad, og øker derfor i omfang.
- Angrep rettes i større grad mot grunnleggende infrastruktur og manipulering av data som styrer infrastrukturen
- Det er usikkert hvordan foretak vil takle og håndtere en alvorlig situasjon der angripere har etablert fotfeste på innsiden av IT-systemene, og iverksatt sine handlinger. Foretakene ikke er tilstrekkelig forberedt på slike situasjoner, og de kan derfor ha utfordringer med å håndtere alvorlige cyber-hendelser.

IKT-sikkerhet og digital kriminalitet - II

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Evne til å oppdage og fjerne uønskede aktører på innsiden må også vies oppmerksomhet, ikke bare sikring av nettverk mot angrep utenfra.
- Manglende klassifisering av informasjon medfører risiko for at informasjon ikke omfattes av beskyttende tiltak. Konfidensiell informasjon kan derfor komme på avveie.
- Forretningssiden må i større grad involveres i foretakets sikkerhetsarbeid
- Foretakene må rette mer oppmerksomhet mot alle former for innsidetrusler i sitt sikkerhetsarbeid.
- Backup-strategi som tar høyde for å sikre data ved angrep er viktige tiltak. Kartlegging viser at banker i all hovedsak har etablert kontroller som sikrer at korrumperte data ikke blir lagt til backup.
- Foretakene må ha tiltak for å redusere sårbarheter knyttet til maskinvare og fastvare.
- EU-kommisjonen og EBA, ESMA og EIOPA
  - Mål å harmonisere og etablere minimumskrav for IKT-sikkerhet for finansnæringen.
  - Samordne regelverk og testrammeverk for å teste robustheten i foretakenes digitale forsvarsverk.

Utviklingstrekk finansiell teknologi

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Utviklingen innenfor finansiell teknologi drives av både nye og eksisterende foretak.
- Foretakene søker kontinuerlig å forenkle og forbedre sine IKT-løsninger.
- Kompleksiteten og sårbarheten i den samlede tekniske infrastrukturen øker som følge av flere aktører, ny teknologi, flere tjenester, samt en generelt høy endringstakt.
- Behov for å ha et kritisk blikk på hvilke interessenter som skaper forventinger og behov for en raskere og økt digital transformasjon. Det må unngås at beslutninger tas på feil grunnlag og medfører kostbare endringsprosjekter
- Tredjeparter etablerer tjenester mellom banker og bankers kunder.
  - PSD 2 regulerer tilgang til bankenes infrastruktur og betalingskonto, og stiller en rekke krav til foretakene
  - På andre områder må foretakene selv sikre seg avtalemessig og sikkerhetsmessig
- Foretak som tar i bruk kunstig intelligens (AI) bør etablere en styringsmodell som legger nødvendige føringer for bruk, og som forankres og godkjennes av foretakets ledelse og styre.
- Foretak og deres leverandører bruker vesentlige ressurser i arbeidet med å fornye sin infrastruktur, og i arbeidet med å etablere tjenester på nye teknologiske plattformer.

Utkontraktering av IKT-virksomhet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Finanstilsynet mottok i 2018 161 meldinger om ny eller endret utkontraktering av IKT, nær en dobling fra 2017.
- Meldingene vurderes opp mot regelverket, at det har vært en forsvarlig beslutningsprosess i foretaket og at nødvendige risikovurderinger er gjennomført og eventuelle risikoreduserende tiltak iverksatt.
- Meldingene viser en klar tendens til økt bruk av skytjenester.
- Finanstilsynets vurdering er at foretak, som tar i bruk skytjenester foretar nødvendige risikovurderinger, at sikkerhetskrav søkes ivaretatt, og at foretakene har den nødvendige oppmerksomhet knyttet til oppfølging av driften og sikkerheten i den utkontrakterte virksomheten.
- Mangler i meldinger er blant annet
  - Unntaksvis er krav om rett til innsyn og tilsyn ikke oppfylt
  - Mangler i risikovurderinger
  - Mangelfulle bestemmelser vedrørende terminering.
- Kompleksiteten i samhandlingen mellom flere aktører utgjør en risiko, spesielt dersom alvorlige hendelser inntreffer.
- Foretakene må sikre at kontrollhandlingene ved utkontraktert virksomhet er minst like gode som ved egen intern virksomhet. Foretakene må ha evne og kompetanse til å ivareta dette kravet.

Andre tema

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Foretakets styringsmodell og forsvarslinjer

- Foretakene må etablere en fungerende styringsmodell for IKT-virksomheten i tråd med prinsippet om tre forsvarslinjer; Operasjonell ledelse, Risikostyring og compliance, og Internrevisjon.

Risikostyring

- Foretakene må etablere god risikostyring innen IKT-virksomheten, med bred involvering i foretaket og en god risikoforståelse.

Kompetanse

- Tilstrekkelig IKT-kompetanse er en utfordring for foretakene.
- Avhengigheten av utenlandske leverandører kan øke ytterligere i årene som kommer, og gi nye sårbarheter og økt risiko.
- Ved utkontraktering til utlandet må det etablere beredskap som innebærer at kritiske IKT-tjenester kan overtas og utføres av personell i Norge / andre land.

Geopolitiske forhold

- Geopolitisk usikkerhet må tas hensyn til i risikovurderinger og beslutningsprosesser.
- IKT-kompetanse som ikke lenger forvaltes og utvikles i Norge, kan utgjøre en vesentlig risiko.

4. Aktørenes vurdering av risikofaktorer

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Foretakenes vurdering av risiko
   - Intervjuer
   - Spørreundersøkelse

Aktørenes vurdering av risikofaktorer

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Foretakene vurderer følgende trusler som de viktigste:

- sosial manipulering der angriperen kan få uautoriserte tilganger og misbruker disse
- svindel foretatt av familiemedlemmer, eksempelvis ved bruk av BankID
- leveransepress, både på grunn av mange nye reguleringer og kundekrav
- økt kompleksitet i systemporteføljene
- mange leverandører involvert i tjenesteleveranser
- bytte og flytting av driftssted
- digitale angrep
- mangel på kompetanse på viktige IKT-områder.

Spørreundersøkelser med foretakene

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Foretakene bes vurdere i hvilken grad de anser seg sårbare for aktuelle trusler.

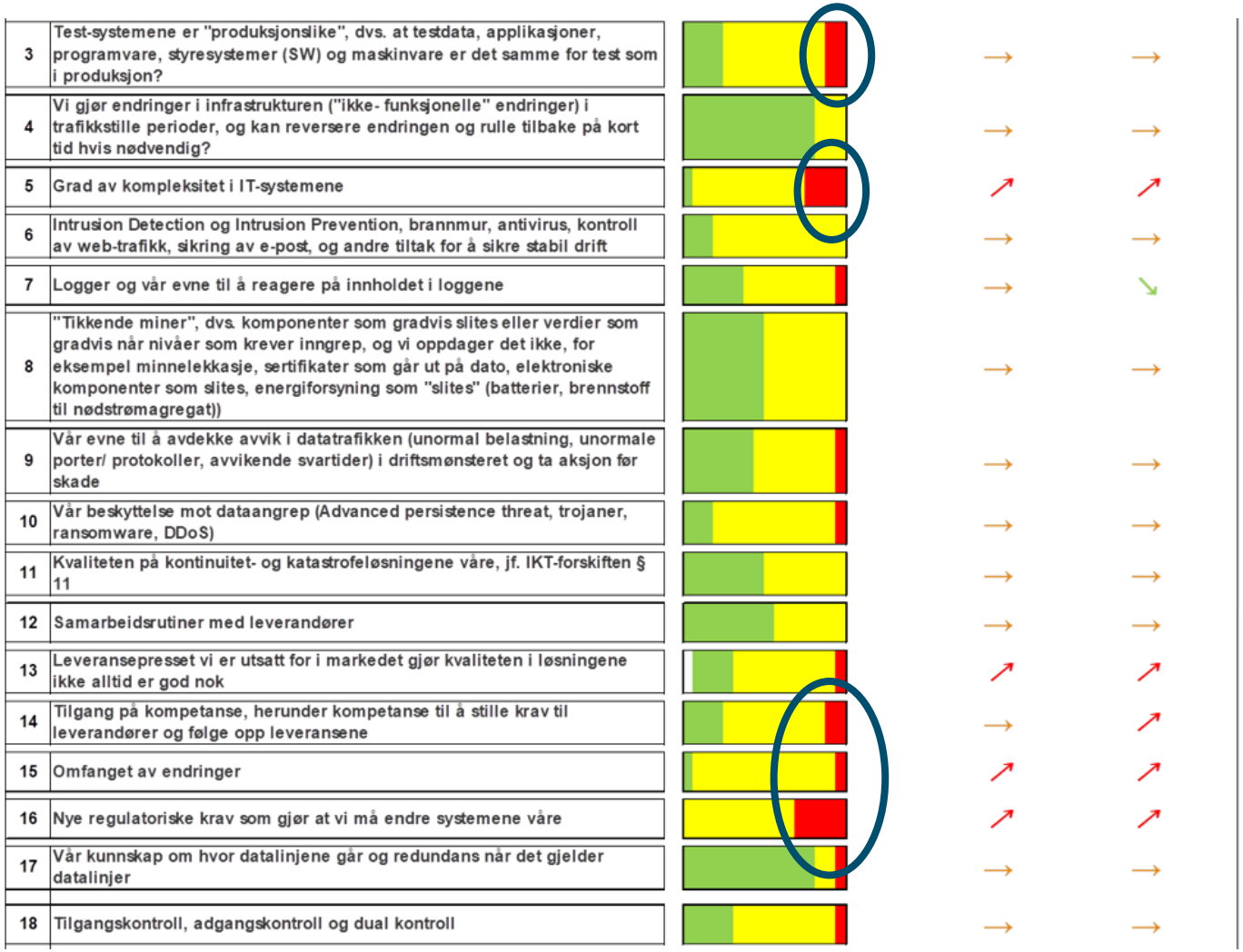
1. Støtte for strategiske beslutninger
2. Avvik i driften
3. Data er ikke tilstrekkelig beskyttet
4. ID-tyveri
5. Misbruk av tilgang til datasystemene
6. Hvitvasking

Eksempel på tabell fra rapporten

	Sårbarhet	Foretakenes svar	Trend 2018	Trend 2017
1	Systemes evne til å hente informasjon fra eksterne og interne kilder og sammenstille og synkronisere informasjonen til et bilde av foretakets risiko til bruk i styringsøyemed og til myndighetsrapportering		→	→
2	Systemenes evne til automatisk å gi et totalbilde av risikoen, for eksempel slik at hvis en hjørnestensbedrift 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		→	→

Spørreundersøkelser med foretakene 2 - Avvik i driften

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY



Spørreundersøkelser med foretakene 3

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Støtte for strategiske beslutninger
   - Risikoen knyttet til dårlig datakvalitet og manglende beskyttelse av ustrukturerte data vurderes som nedadgående. Kan ha sammenheng med arbeidet gjort i forbindelse med implementeringen av datalagringsdirektivet (GDPR).
2. Avvik i driften
   - Økende antall leverandører, og underleverandører, i verdikjedene utgjør en risiko som følge av mer kompleks infrastruktur og samhandling.
   - Omfanget av endringer og nye regulatoriske krav kan redusere foretakenes evne til å levere på tid og med nødvendig kvalitet.
   - Tendensen til avtakende risiko knyttet til mangler i organisering, stillingsbeskrivelser, rapportering og kontroll, har stoppet opp.
3. Data er ikke tilstrekkelig beskyttet
   - Foretakenes vurdering av risiko knyttet til beskyttelse av sensitive data viser omtrent det samme bildet som i 2017.
4. ID-tyveri
   - Bedre kontroll med utlevering av brukeridentitet og passord til kunder og medarbeidere.
   - Risikoen for at en angriper tar over en brukeridentitet og misbruker denne, anses dermed noe mindre enn tidligere.
5. Misbruk av tilgang til datasystemene
   - Trusselbildet knyttet til interne misligheter synes lite endret fra 2017 til 2018
6. Hvitvasking
   - Risikoen for hvitvasking er redusert som følge av forbedringer i IT-systemenes evne til å samle relevant informasjon om kunder, kunderelasjoner og kundeadferd som grunnlag for kontroller.

Besvarelsene viser at samlet sett synes foretakenes vurdering av risikoen å være svakt økende i 2018, slik den også var i 2017 og 2016.

5. Finanstilsynets oppsummerende vurdering av risikobildet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. Finansiell infrastruktur
2. Foretakene
3. Foretakenes kunder

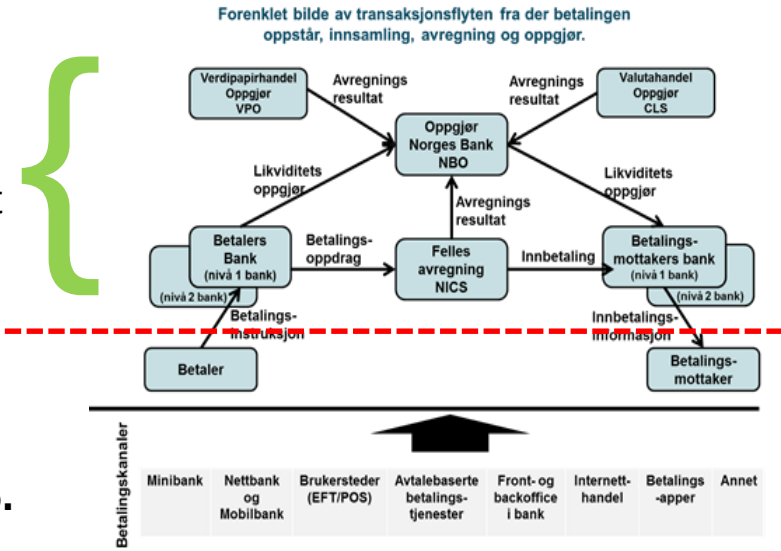
Finansiell infrastruktur

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 en kritisk hendelse som medførte feil i betalingssystemet og hendelser som gjorde betalingsløsninger utilgjengelige i perioder, var tilgjengeligheten bedre enn i 2017 og på nivå med 2016. Finanstilsynet vurderer på den bakgrunn den norske finansielle infrastrukturen som robust.**

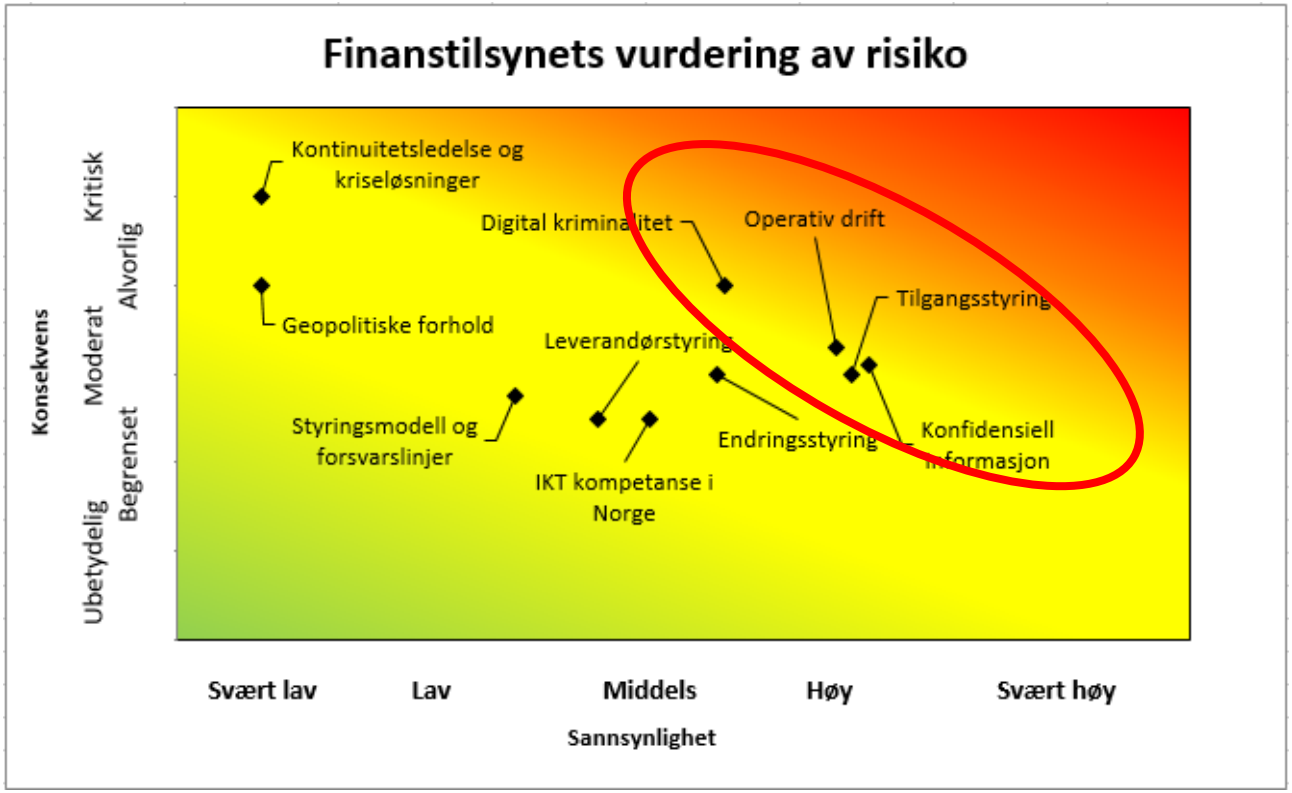


- Hendelser og funn fra tilsynsvirksomheten viste imidlertid sårbarheter når det gjelder
  - Feil etter endringer
  - Mangelfull kapasitetsplanlegging
  - Svikt i overvåking av parametere som utløpsdatoer, fyllingsgrader og terskelverdier.

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.

Finanstilsynet vurderer risikoen knyttet til sårbarheter i

- **Operativ drift**
- **Digital kriminalitet**
- **Konfidensiell informasjon**
- **Tilgangsstyring**

som de mest sentrale truslene knyttet til foretakenes bruk av IKT

Finanstilsynets oppsummerende vurdering av risikobildet – foretakene

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Den samlede risikoen knyttet til sårbarheter ved **operativ drift** vurderes som **middels** til **høy**.
- Sannsynligheten for uønskede hendelser vurderes som ***høy*** og konsekvensen **som *moderat*.**
- Følgende vurderinger er lagt til grunn:
  - Sannsynligheten for redusert datakvalitet som følge av kompleks integrasjon mellom tjenesteleverandører vurderes som ***middels*** og med ***moderat*** konsekvens.
  - Sannsynligheten for ustabile og /eller utilgjengelige tjenester som følge av økt grad av integrasjon mellom ulike tjenesteleverandører vurderes som ***middels*** og med ***alvorlig*** konsekvens.
  - Sannsynligheten for driftsproblemer som rammer felles operasjonell infrastruktur vurderes som ***middels*** og med ***alvorlig*** konsekvens.
  - Sannsynligheten for utilgjengelige tjenester som følge av mangelfull kapasitetsstyring vurderes som ***middels*** og med ***alvorlig*** konsekvens.
  - Sannsynligheten for at systemkomponenter i redundante løsninger feiler, som følge av mangelfull overvåking og test, vurderes som ***lav*** og med ***alvorlig*** konsekvens.
  - Sannsynligheten for driftsproblemer (nettverk og tjenester) som følge av ugyldige digitale sertifikater eller ugyldige lisenser vurderes som ***middels*** og med ***moderat*** konsekvens.
  - Sannsynligheten for driftsproblemer, som følge av mangelfull kompetanse innen driftstøtte for stormaskin, vurderes som ***middels*** og med ***moderat*** konsekvens.

Foretakenes kunder

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- ***Påloggingsinformasjon på avveie, misbruk av BankID og Identitetstyveri***
  - Digitale identifiserings- og autoriseringsløsninger kan være en utfordring for mange
    - passord ofte blir skrevet ned
    - passord og koder blir delt eller stjålet

    utgjør en betydelig risiko for misbruk, med i verste fall store økonomiske konsekvenser for den skadelidende.
  - Det er knyttet en konsentrasjonsrisiko til BankID ved misbruk grunnet bredt bruksområde
- ***Svindel ved sosial manipulering***
  - Kjærlighetssvindel, investeringssvindel, falske fakturaer og kunder som blir forledet til å gi fra seg sensitiv informasjon
  - Utgjør en vesentlig større risiko for den enkelte kunde, enn digital kriminalitet rettet mot foretakene i finanssektoren eller bruken av foretakenes løsninger
- ***Kundegrensesnitt gjennom nye aktører***
  - Stadig nye kundegrensesnitt kan skape usikkerhet hos kundene
- ***Foretakenes integritet som følge av digital kriminalitet***
  - Kunder er redd for at deres midler skal gå tap som følge av digital kriminalitet
  - Ved alvorlige hendelser forsterkes usikkerhet blant foretakets kunder

6. Finanstilsynets oppfølging

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

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

Finanstilsynets oppsummering

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Den norske finansielle infrastrukturen er robust.
- Samme omfang av hendelser i 2018 som i 2017, alvorlighetsgraden lavere, og betalingssystemet og kunderettede løsninger mer tilgjengelige i 2018 enn i 2017.
- 184 av 189 rapporterte hendelser forårsaket av operasjonelle avvik, 5 var sikkerhetshendelser.
- Angrep (digital kriminalitet) mot foretakenes systemer øker betydelig fra år til år. Angrepene avverges som oftest før de får konsekvenser for foretaket. Ingen med konsekvens for finansiell stabilitet.
- Foretakene bør fortsatt styrke arbeidet innen IKT-sikkerhetsområdet, samt arbeide for å redusere sannsynligheten for alvorlige avvik. Bedre arbeidet knyttet til endringer, kapasitetsplanlegging og overvåking.
- Omfanget av kortsvindel avtok ytterligere i 2018, både målt i kroner og i antall misbrukte kort.
- Tapene som følge av svindel mot nettbank er lave selv om de økte noe i 2018.
- Kunders tap ved sosial manipulering viser at det er her de kriminelle har størst utbytte.
- Vesentlig økning i antall meldinger om utkontraktering av IKT. Klar tendens til økt bruk av skytjenester.
- Betalingsområdet var også i 2018 preget av store endringer. Endringene må ses i lys av økt konkurranse som følge av ny teknologi, regulatoriske endringer og kunders forventninger.
- Kompleksiteten i den tekniske infrastrukturen øker og gir en økende risiko som følge av at det blir flere aktører, bruk av ny teknologi og teknologi på nye områder, samt en fortsatt høy endringstakt. Hensynet til finansiell stabilitet, trygge tjenester og god kundebeskyttelse må ivaretas.
- Sårbarheter knyttet til foretakenes operative drift, digital kriminalitet, skjerming av konfidensiell informasjon og tilgangsstyring anses som de mest sentrale truslene knyttet til foretakenes bruk av IKT.

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