FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Rundskriv

Økte krav til bankene i lys av driftsproblemene i påsken 2011

RUNDSKRIV:
20/2011

DATO:
15.06.2011

RUNDSKRIVET GJELDER FOR:
Banker

FINANSTILSYNET
Postboks 1187 Sentrum
0107 Oslo

1 Innledning

Finanstilsynet har vurdert hendelsene i påsken 2011 som rammet bankenes betalingstjenester på kortområdet med påfølgende alvorlige konsekvenser for bankenes kunder. Basert på rapporter fra bankene og deres leverandører har Finanstilsynet fått oversikt over feilårsak, følgefeil og konsekvenser av hendelsene. 140 000 kunder ble på ulike måter rammet av driftsproblemene, enten ved bruk av kort i bankenes minibanker eller på bankenes EFT/POS-løsninger på brukersteder. I perioden fra onsdag 20. april 2011 og frem til alle rettelser var foretatt onsdag 27. april, ble over 200 000 transaksjoner avvist og 240 000 reservasjoner måtte slettes.

I tillegg til en beskrivelse av hendelsene, gir rundskrivet informasjon om hvilke tiltak Finanstilsynet anser nødvendige som ledd i å hindre at slike situasjoner skal gjenta seg.

2 Nærmere om hendelsene i påsken 2011

Hovedårsaken til hendelsene beror på en gjennomført endring hos EDB ErgoGroup ASA (EDB) høsten 2010. En beredskapstest avdekket behov for oppgradering av en sentral komponent (IssuerGatewayServer) i kortsystemløsningen. Løsningen var satt opp som et redundant system med en primær- og en sekundærserver. Ved gjennomføring av endringen ble kun primærserveren oppgradert grunnet manglende tilgang til oppgraderingsutstyr for sekundærserveren. Det er konstatert alvorlige feil, både ved håndtering av endringen og i fagansvarlig enhet hos EDB som ikke fulgte opp mangelen på korrekt måte. Da det oppsto en feil på primærserveren (hardware) onsdag 20. april 2011, viste det seg at sekundærserveren ikke hadde tilstrekkelig kapasitet til å håndtere trafikkvolumet.

Feilen medførte en rekke følgefeil ved bruk av kort i minibank og butikker:

- Kort ble avvist i minibanker. Det grunnet i manglende svar på forespørsel om aksept fra minibanksystemet på uttak, som skyldtes treghet på IGWS-løsningen.
- Kort ble avvist på brukersted, grunnet manglende svar på forespørsel om aksept av betalingen på brukerstedet, som skyldtes treghet på IGWS-løsningen.
- Kort (samme betalingstransaksjon) ble forsøkt benyttet igjen av kunden med den følge at det enten skjedde oppdatering av kapitaltransaksjonen to ganger, eller det skjedde generering av “advice-melding” (grunnlag for oppdatering av disponert beløp til pseudo-systemet (reservasjon av beløp)) to ganger.
- Et stort volum advice-meldinger ble på grunn av problemene hos EDB liggende i en ventekø hos Nets Norway AS (Nets). Da disse senere ble oppdatert hos EDB, var kapitaltransaksjonene (EFT-delen) allerede oppdatert, og senere reservering av beløpene skulle ikke ha skjedd. For bankenes kunder oppfattes dette som dobbelt postering/reduksjon av tilgjengelig saldo.

Problemer på brukersteder og minibanker startet onsdag 20. april 2011 kl. 10.00, og varte frem til kl. 17.00 samme dag. Konsekvenser av feilen overfor bankenes kunder og rettelser av følgefeil pågikk i praksis frem til onsdag 27. april, da de siste korreksjonene ble gjennomført.

EDBs kriseteam ble hurtig etablert for å håndtere avviket. I første omgang ble arbeidet i hovedsak konsentrert om å løse feilen på den aktuelle IGWS-serveren. IGWS-løsningen er en komponent som inngår i en lengre transaksjonskjede. EDBs kriseteam hadde ikke nødvendig innsikt i tjenesteområdene og alle elementer som inngår i transaksjonskjeden. De var dermed ikke i stand til å avverge omfanget av følgefeil. Feilhåndteringen viser at beredskapsorganisasjonen også må bestå av representanter fra bankene og fra andre samarbeidende leverandører, i dette tilfellet Nets.

En beredskapsorganisasjon med deltakelse fra banker og Nets kunne ha begrenset konsekvensene av feilen som oppsto. Etablering av et beredskapsopplegg som også omfatter banker og samhandlingspartnere er et ansvar som påligger bankene.

Nets ivaretar viktige funksjonsområder for bankenes kortsystemer. Siden EDB ivaretar viktige funksjonsområder på de samme områdene, er det nødvendig med en bedre samhandling mellom EDB, Nets og bankene. Konsekvenser av feilen som oppsto hos EDB, ble synliggjort både på brukerstedene og hos Nets som ivaretar oppgaver knyttet til nettverk, innsamling og avregning. Nets fulgte de fastlagte prosedyrene som forvaltes av Finansnæringens Fellesorganisasjon (FNO) og Bankenes Standardiseringskontor (BSK) på vegne av bankene. Nets fulgte transaksjonstrafikken gjennom sine overvåkings- og oppfølgingssystemer og hadde dermed informasjon om problemene som akkumulerte seg. På dette grunnlaget kunne Nets ha gitt et mer tydelig varsel både til bankene og til EDB om omfanget av problemet og risikoen ved at advice-meldinger ville nå frem til EDB først etter at kapitaltransaksjonene var avregnet. Dette betyr at det også hos Nets er behov for å ha en beredskapsorganisasjon som omfatter representanter fra bankene og viktige leverandører som Nets må samhandle med. Etter det Finanstilsynet kjenner til, vil FNO gå gjennom gjeldende regelverk for BankAxept (“Blåboka”) slik at dette kan tilpasses en krisesituasjon på en bedre måte enn nåværende regelverk.

3 Tiltak og oppfølging

3.1 Bankenes ansvar

Driftsproblemene synliggjør sårbarheter i transaksjonskjeden, og viser nødvendigheten av at bankene tar tydeligere ansvar for den delen av transaksjonskjeden som driftes av eksterne leverandører.

Bankene har ansvar for alle aktiviteter som utgjør bankens virksomhet. Dette er særlig tydeliggjort i Forskrift om risikostyring og internkontroll og i IKT-forskriften som vektlegger bankenes ansvar også for oppgaver som er utkontraktert. Dette ansvaret gjelder uavkortet også om feilen reelt har oppstått hos leverandøren. Det er et spørsmål om feil, slik som i dette aktuelle tilfellet, kunne vært begrenset ved at bankene i større grad og på en mer aktiv måte utøvde sitt ansvar.

Nødvendige tiltak:
Bankene må sette konkrete krav til leverandørene og deres arbeid, og forsikre seg om at arbeidet utføres i henhold til avtale, aktuelle retningslinjer og gjeldende regelverk, gjennom utøvelsen av en aktiv styring og kontroll med leveransene.

3.2 Kartlegging av kritiske komponenter

Det er av vesentlig betydning for bankenes virksomhet at bankene har identifisert komponentene i sin IKT-infrastruktur som representerer kritiske funksjoner slik at betalingssystemer og kundereskontrovirksomheten har tilstrekkelig tilgjengelighet. Det vises til IKT-forskriftens § 3 (Risikoanalyse), § 10 (Krav til kontinuitet) og § 11 (Driftsavbrudd og katastrofeberedskap) som stiller krav på dette området.

Nødvendige tiltak:

- Bankene må kartlegge og dokumentere kritiske komponenter i sin IKT-infrastruktur og øvrige nødvendige elementer som inngår i transaksjonskjeden, inkludert de komponenter som befinner seg hos eksterne leverandører. Dokumentasjonen skal inneholde en vurdering av risiko, sikring av kontinuitet og hvordan beredskap er sikret.

- Bankens internrevisjon[1] skal bekrefte at kartleggingen og dokumentasjonen er foretatt på en forsvarlig måte.

- Dokumentasjonen, sammen med internrevisjonens bekreftelse, skal forelegges bankens styre. Finanstilsynet legger til grunn at risikovurderingen knyttet til kritiske komponenter i IKT-infrastrukturen inngår som del av den årlige vurderingen av risikosituasjonen, jf. forskrift om risikostyring og internkontroll § 8.

- Kopi av dokumentasjonen etter gjennomgangen i 2011 og internrevisjonens bekreftelse skal sendes Finanstilsynet innen 31.12.2011.

3.3 Samordnet beredskap

Det er ikke tilfredsstillende at banker og viktige leverandører ikke har en samordnet beredskap. Hendelsene i påsken 2011 viser at den enkelte leverandør ikke har tilstrekkelig innsikt til å begrense konsekvensene av en alvorlig hendelse. Presis og rettidig informasjon i aktuelle kanaler kan være avgjørende for håndtering av et problem. Når det gjelder krav til beredskapsopplegg vises det til IKT-forskriftens § 11 (Driftsavbrudd og katastrofeberedskap).

Bankene må sikre at beredskapen er samordnet med leverandørenes beredskapsorganisasjoner der dette vurderes som hensiktsmessig (leverandør som har betydning for bankens virksomhet), og at det gjennomføres øvelser som sikrer at den totale beredskapsorganisasjonen fungerer.

Den enkelte bank gir Finanstilsynet en redegjørelse for hvordan dette er løst innen 31.12.2011.

[1] Gjelder for de bankene som har internrevisjon.

3.4 Endringskontroll

Nødvendige tiltak:
Bankene må vurdere hvordan de på en hensiktsmessig måte og i større grad enn i dag kan delta i endringshåndteringen hos leverandører. Dette gjelder der bankenes løsninger er direkte berørt i endringene, og for kritiske komponenter som direkte kan berøre bankenes betalingssystemer og/eller kunde-/reskontroområdet. Det vises her til IKT-forskriftens § 9 (Avviks- og endringshåndtering).

En redegjørelse for hvordan den enkelte bank vil sikre seg en mer direkte deltakelse i endringshåndteringen sendes Finanstilsynet innen 31.12.2011.

Emil R. Steffensen

Anne Merethe Bellamy

Kontaktpersoner:
Seksjonssjef Frank Robert Berg, tlf. 22 93 98 47, e-post: frank.robert.berg@finanstilsynet.no
Tilsynsrådgiver Stig Ulstein, tlf. 22 93 99 66, e-post: stig.ulstein@finanstilsynet.no


SYNET
entrum
7 Oslo
ET.NO
ET.NO