FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i SPAREBANK 1 SR-BANK ASA
Postboks 250
4068 STAVANGER

| VÅR REFERANSE | DERES REFERANSE | | DATO |
|---|---|---|---|
| 19/5056 | | | 06.03.2020 |

## Tilsynsrapport

Finanstilsynet gjennomførte stedlig tilsyn i SpareBank 1 SR-Bank ASA (SR-Bank) 20. juni 2019. Tema for tilsynet var cybersikkerhet, som i relasjon til dette tilsynet var definert som proaktive og reaktive tiltak mot tilsiktede elektroniske angrep.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige rapport datert 27. september 2019 og styrets kommentarer til rapporten i brev av 30. oktober 2019.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

**Forhold knyttet til styring og kontroll med styrende sikkerhetsdokumentasjon.**

Dokumenthierarki.
Finanstilsynet viste i foreløpig rapport til uklarheter knyttet til innholdet i sikkerhets-policyer, -standarder og -rutiner, og et behov for å definere hva de ulike dokumenttypene skal beskrive i bankens vedtatte dokumenthierarki.

Finanstilsynet har fra styrets svar merket seg at banken har iverksatt en gjennomgang av styrende sikkerhetsdokumentasjon, herunder krav til innhold og format, som skal være ferdigstilt i Q1 2020.

Tydeliggjøring av SR-Bank og Sparebank1 Banksamarbeidets styrende dokumentasjon.
Finanstilsynet viste også i foreløpig rapport til at det for en del av den styrende sikkerhetsdokumentasjonen er vanskelig å se koblingen mellom bankens og SpareBank 1 Banksamarbeidets dokumentasjon. Finanstilsynet pekte på at der bankens standarder bygger på SpareBank 1 Banksamarbeidets standarder, må dette tydelig fremgå og innholdet forankres i banken.

Finanstilsynet har fra styrets svar merket seg at gjennomgang av referanser og koblinger til SpareBank 1 Banksamarbeidets dokumentasjon inngår i den gjennomgangen banken har iverksatt av styrende sikkerhetsdokumentasjon.

**Forhold knyttet til styring og kontroll med etterlevelse av sikkerhetskrav.**

Kontroll av tilganger.
Finanstilsynet etterspurte i foreløpig rapport en nærmere redegjørelse for hvordan tilganger til driftsoperasjoner kontrolleres og resultatet dokumenteres.

**FINANSTILSYNET**
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

**Saksbehandler**
Åshild Johnsen
Dir. tlf 22 93 97 02

Finanstilsynet har fra dokumentasjon vedlagt styrets svar, merket seg SpareBank 1 Banksamarbeidets rutine for, og dokumentasjon av, gjennomførte tilgangskontroller. Finanstilsynet har videre merket seg fra styrets svar at banken har dokumentert eksisterende prosess for gjennomføring av tilgangsrevisjoner i en formell rutine.

Avdekke avvik i henhold til egne rutiner.
I bankens sikkerhetsrutiner fremgår det hvordan avvik fra den aktuelle rutinen skal behandles. Finanstilsynet stilte i foreløpig rapport spørsmål til kontroller for å avdekke slike avvik.

Finanstilsynet har fra styrets svar merket seg at avvik fra rutinene registreres som hendelser i bankens hendelsesdatabase. Finanstilsynet har notert seg at banken vil styrke gjennomføringen av kontrollaktiviteter gjennom egne kontrollplaner på IT-sikkerhetsområdet, som skal være ferdige i Q1 2020.

Kontroll av leverandørens etterlevelse av bankens sikkerhetskrav.
Finanstilsynet ba i foreløpig rapport banken redegjøre for kontroller for å påse at SpareBank 1 Banksamarbeidet og leverandører til SpareBank 1 Banksamarbeidet etterlever kravene i bankens sikkerhetsstandarder.

Finanstilsynet har fra styrets svar merket seg at banken vil styrke leverandøroppfølgingen og at banken vil oppdatere sine rutiner slik at det tydelig fremgår hvordan den operative oppfølgingen av leverandørene skal foregå. Finanstilsynet har merket seg at oppdatert prosess skal være på plass innen 31. desember 2019.

**Sikkerhetsoppdateringer.**

Finanstilsynet påpekte i foreløpig rapport at sikkerhetsrutinene ikke hadde tilstrekkelig beskrivelse av håndteringen av nylig avdekkede kritiske sårbarheter.

Finanstilsynet har fra styrets svar merket seg at sikkerhetsrutinene vil bli oppdatert innen Q1 2020 slik at dette tydelig fremkommer.

**Hendelsesrapportering til Finanstilsynet.**

Finanstilsynet pekte i foreløpig rapport på at i henhold til IKT-forskriftens § 9 skal alvorlige og kritiske IKT-hendelser rapporteres til Finanstilsynet. For banker i Banksamarbeidet gjelder dette også hendelser som kun rammer en enkelt bank og ikke alle bankene i Banksamarbeidet.

Finanstilsynet har notert seg fra styrets svar at banken vil vektlegge dette ved vurdering av fremtidige hendelser banken rammes av.

**Adressering av sikkerhetshendelser i katastrofeplanen.**

For å sikre en mest mulig effektiv hendelseshåndtering i en krisesituasjon anbefalte Finanstilsynet i foreløpig rapport at banken i sin katastrofeplan har et rutinemessig sjekkpunkt for om årsaken til hendelsen kan være en tilsiktet hendelse.

Finanstilsynet har fra styrets svar merket seg at banken har oppdatert katastrofeplanen med dette.

**Forhold knyttet til styring og kontroll med bruk av AdminControl.**

Mange foretak benytter AdminControl til styre- og ledelsesarbeid. Basert på den totale mengden konfidensiell styre- og ledelsesinformasjon som kan komme på avveie ved kompromittering, vurderer Finanstilsynet AdminControl som et kritisk system.

Finanstilsynet har fra styrets svar merket seg at identifiserte risikoer i risikoanalysen av systemet vil bli fulgt opp i henhold til gjeldende rutine.

Kopi av merknadene bes sendt intern og ekstern revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Åshild Johnsen
senior tilsynsrådgiver

*Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.*