FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

STOREBRAND LIVSFORSIKRING AS
Postboks 500
1327 LYSAKER

VÅR REFERANSE	DERES REFERANSE		DATO
19/10251	AR395664706		17.03.2021

Tilsynsrapport

Finanstilsynet gjennomførte stedlig tilsyn i Storebrand Livsforsikring AS 18. og 19. november 2019. Tilsynet hadde som formål å foreta en vurdering av hvordan foretaket ivaretar styring og kontroll innen IKT-sikkerhetsområdet internt i foretaket, samt styring og kontroll med relevante leverandører av IKT-tjenester.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige tilsynsrapport datert 15. september 2020 og styrets kommentarer til foreløpig tilsynsrapport i brev av 30. oktober 2020.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

Organisering og ansvarsforhold

Finanstilsynet pekte i foreløpig tilsynsrapport på at leder for konsernsikkerhet (CISO) er organisert i førstelinjen og utfører oppgaver der, samtidig som CISO ivaretar sin rolle i kontrollfunksjonen (andrelinjen) for konsernet (Storebrand ASA). For å sikre selvstendighet og uavhengighet bør disse rollene etter Finanstilsynets vurdering ivaretas av to ulike personer. I foreløpig tilsynsrapport påpekte Finanstilsynet videre at rollen som CISO synes å være innplassert på et for lavt nivå i organisasjonen, og med manglende mulighet for direkte rapportering til administrerende direktør i konsernet.

Av styrets svar har Finanstilsynet notert seg at organisasjonsmessig tilhørighet ble vurdert ifm. ny konsernorganisering 1. juli 2019, samt at kravene til CISO-funksjonens uavhengighet ble presisert og tydeliggjort i konsernets styrende dokumenter ifm. foretakets tilpasning til "EBA Guidelines on internal governance" (EBA/GL/2017/11).

Finanstilsynet forventer at foretaket etablerer en organisering og styringsmodell som legger til rette for at foretaket oppfyller Finanstilsynets anbefalinger til CISO-funksjonen som uavhengig kontrollfunksjon.

Uavhengige kontrollfunksjoner

Compliance

I foreløpig tilsynsrapport vurderte Finanstilsynet kontrollarbeidet som utføres av foretakets compliancefunksjon innen IKT-området som begrenset. Det er Finanstilsynets vurdering at

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Jarleif Lødøen
Dir. tlf 22 93 98 00

foretaket bør fastsette hvilke kontroller førstelinjen skal være pålagt å utføre, samt hvilke av disse som skal overvåkes av compliancefunksjonen. Vurderingene av resultater og kontrollarbeid vil naturlig inngå som en del av underlagsmaterialet til foretakets compliancerapporter.

I styrets svar anser styret at CISO-funksjonens uavhengighet er ivaretatt og at arbeidsdelingen og samarbeidet med compliancefunksjonen sikrer at compliancefunksjonens kontrollporteføljе er hensiktsmessig fastsatt.

Finanstilsynet understreker viktigheten av at hvert enkelt foretak i konsernet fastsetter sine kontroller og kontrollaktiviteter knyttet til IKT-området basert på innspill fra relevante områder og funksjoner i foretaket, dernest at foretaket fastsetter hvilke kontroller som skal overvåkes og rapporteres av foretakets compliancefunksjon.

Risikostyringsfunksjonen

Finanstilsynet pekte i foreløpig tilsynsrapport på at risikostyringsfunksjonen i foretaket ikke synes å ha tilstrekkelig oppmerksomhet om, og oversikt over, risikobildet innen informasjonssikkerhet for foretaket. Etter Finanstilsynets syn bør foretakets risikostyringsfunksjon identifisere og kategorisere risikobildet innen informasjonssikkerhet, og IKT-området for øvrig.

Av styrets svar fremgår det at samarbeidet mellom CISO-funksjonen og risikostyringsfunksjonen er lagt opp etter tilsvarende modell som for compliancefunksjonen, der uavhengigheten etter styrets oppfatning er ivaretatt. Etter styrets vurdering bidrar CISO til kompetansesynergi, slik at risikostyringsfunksjonen kan bygge videre på CISO-funksjonens risikovurdering i sin sammenstilling av det helhetlige risikobilde for foretaket.

Finanstilsynet påpeker at risikobildet varierer mellom de ulike foretakene i konsernet og understreker viktigheten av at hvert enkelt foretak i konsernet, basert på innspill fra relevante områder og funksjoner, fastsetter sitt eget helhetlige risikobilde for IKT-området.

Internrevisjonen

Finanstilsynet pekte i foreløpig tilsynsrapport på at de gjennomførte internrevisjonsaktivitetene på IKT-området de siste årene i for liten grad synes å dekke områder med høy operasjonell risiko, herunder leverandørstyring, kontinuitetsledelse og kriseledelse. Videre var Finanstilsynets vurdering at internrevisjonen i for liten grad ble brukt til å innhente uavhengige bekreftelser på styring og kontroll innen IKT-området.

Fra styrets svar noterer Finanstilsynet seg at internrevisjonens arbeid er risikobasert og at det gjennomføres flere revisjoner knyttet til IKT-området hvert år. I tillegg er det de siste årene utført spesifikke internrevisjonsaktiviteter knyttet til operasjonelle enkeltrisikoer. Det fremgår videre at internrevisjonen blir brukt til å kvalitetssikre håndteringen av nye risikoer.

Finanstilsynet ber foretaket vurdere i større grad å innhente uavhengige vurderinger for å bekrefte foretakets styring og kontroll med IKT-området.

I foreløpig tilsynsrapport viste Finanstilsynet til at internrevisjonen i større grad burde deltatt i arbeidet med implementering og vurdering av konsekvensene ved innføring av ny policy for informasjonssikkerhet, "Information Security Management System"(ISMS) og gitt en uavhengig vurdering av om foretaket hadde tilstrekkelig styring og kontroll med det samlede IKT-risikobildet underveis i implementeringen.

Finanstilsynet har fra styrets svar notert seg at det har vært diskusjoner om internrevisjonens rolle i implementeringen av ISMS og at internrevisjonen iht. årsplan for 2020 har foretatt en gjennomgang av «Risiko- og sårbarhetsanalyser» med vurdering av hvordan ISMS er koordinert og hvordan ISMS samspiller med risiko- og sårbarhetsanalyser.

Risikostyring innen IKT-området

I foreløpig tilsynsrapport var Finanstilsynets vurdering at foretakets nivå på cyberrisiko ikke var i tråd med foretakets risikotoleranse. Videre påpekte Finanstilsynet at forretningssiden må eie IKT-risikoer knyttet til sine forretningsprosesser.

Av styrets svar fremgår det at det er arbeidet videre med rammeverk for konsernfelles risikovurderinger og at det er fastsatt en ny risikomatrise. Når risikokategoriene for cyberrisiko scores iht. det justerte rammeverket, er ingen av kategoriene i rød sone.

Finanstilsynet tar til etterretning styrets informasjon om at risikokategoriseringen for cyberrisiko er aggregert opp fra de risikoer som er identifisert i samarbeid med forretningssiden.

Styring og kontroll med utkontraktert virksomhet – leverandørstyring

Oppfølging av sikkerhetskravene hos leverandørene

I foreløpig tilsynsrapport pekte Finanstilsynet på viktigheten av at foretaket følger opp at foretakets retningslinjer for informasjonssikkerhet til enhver tid er kjent for leverandørene, og at retningslinjene etterleves av leverandørene.

Finanstilsynet noterer seg fra styrets svar at foretakets retningslinjer for informasjonssikkerhet er revidert flere ganger og at leverandørenes etterlevelse p.t. er i henhold til ulike versjoner av retningslinjene.

Finanstilsynet understreker viktigheten av at foretaket fortsetter arbeidet med å følge opp leverandørenes etterlevelse av kravene til informasjonssikkerhet, og at leverandørenes etterlevelse blir vurdert i forhold til siste versjon av retningslinjene.

Finanstilsynet pekte i foreløpig tilsynsrapport på at det synes som om foretaket ikke får tilstrekkelig dokumentasjon av teknisk infrastruktur hos leverandørene til å kunne å følge opp etterlevelsen av sikkerhetskravene.

Finanstilsynet har merket seg styrets svar på hvordan slik informasjon innhentes.

Uavhengige erklæringer og uttalelser fra leverandører

I foreløpig tilsynsrapport pekte Finanstilsynet på at uavhengige revisjonserklæringer fra leverandører er en viktig del av foretakets internkontroll, men at aktiv bruk av denne typen bekreftelser forutsetter at foretaket er innforstått med i hvilken grad erklæringen og bekreftelsen omfatter de utkontrakterte tjenestene. Eksempelvis er formålet med leverandørens ISAE 3402 rapportering å redusere behovet for at foretakets eksterne revisor selv må utføre revisjonshandliger for å vurdere dataintegriteten i systemer som behandler finansielle data som kan påvirke foretaket sitt regnskap.

Finanstilsynet har notert seg styrets svar om at foretaket er bevisst i hvilken grad erklæringen og bekreftelsen omfatter de utkontrakterte tjenestene, og prosessene som leverandørene benytter for leveransene til foretaket. Av svaret fremgår det videre at foretaket med utgangspunkt i risikovurderinger vil ta initiativ til testing dersom det er uklart om internkontrollen hos leverandører er tilfredsstillende.

Sårbarheter knyttet til egne ansatte og personell hos leverandører

I foreløpig tilsynsrapport anbefalte Finanstilsynet at foretaket styrket kontrollen ved ansettelse av personell som skal ha administrative tilgangsrettigheter til kritisk infrastruktur.

Finanstilsynet har fra styrets svar merket seg tiltak foretaket har iverksatt.

Finanstilsynet pekte videre på at det er uklart om foretaket, som del av leverandøroppfølgingen, kontrollerer om leverandørene har etablert rutiner for utvidet bakgrunnssjekk og periodisk risikovurdering av personell med administrative tilgangsrettigheter, og om leverandørens etterlevelse av slike krav blir fulgt opp.

Fra styrets svar har Finanstilsynet merket seg at de største leverandøravtalene har bestemmelser om bakgrunnssjekk, og at leverandørens etterlevelse av kravene blir fulgt opp gjennom mottak av ISAE 3402-rapporter og at dette er på agendaen ved sikkerhetsrevisjoner hos leverandører. Finanstilsynet har videre merket seg at foretaket på ny vil gjennomgå rutinene på dette området.

Forsvarsverk

Sikkerhetstest

I foreløpig tilsynsrapport ba Finanstilsynet foretaket om å redegjøre for rutiner og planer for periodisk sikkerhetstesting, og hvordan foretaket sikrer at all kritisk infrastruktur er omfattet av testingen.

Av styrets svar fremgår det at foretaket har en risikobasert tilnærming, der testingen tilpasses relevante scenarioer for det aktuelle trusselbilde, de relevante sårbarhetene og de berørte verdiene på tidspunktet for testing.

Etter Finanstilsynets vurdering bør foretaket sørge for at alt relevant teknisk utstyr og systemer i foretakets infrastruktur over tid omfattes av testingen (jf. også avsnittet "Konfigurasjonsstyring" nedenfor), slik at også eventuelt utdatert og usanksjonert utstyr og systemer som ikke omfattes av de utvalgte scenarioene blir avdekket.

Overvåkning og analyse

I foreløpig tilsynsrapport understreket Finanstilsynet viktigheten av å få på plass overvåkningsløsninger som tilfredsstiller foretakets behov og krav, og at arbeidet med dette gis nødvendig prioritet.

Finanstilsynet har fra styrets svar merket seg at foretaket har styrket systemovervåkingen, herunder at ny overvåkningsløsning ble satt i produksjon våren 2020.

I foreløpig tilsynsrapport pekte Finanstilsynet på at det er behov for styrking av overvåking og kontroll for å avdekke og forhindre at infrastruktur og systemer infiseres av skadevare, og at arbeidet med forbedringstiltak gis prioritet og sluttføres.

Fra styrets svar har Finanstilsynet notert seg at dette er et område som foretaket tar svært alvorlig og at det er implementert ny antivirusløsning, ny løsning for overvåkning av endepunkt og ny løsning for sikring av e-post. Finanstilsynet tar videre foretakets opplysning om at ytterligere sikkerhetstiltak knyttet til blant annet datalekkasje og overvåkning er til vurdering i forbindelse med ny fremtidig infrastrukturplattform til etterretning.

I foreløpig tilsynsrapport ba Finanstilsynet foretaket kort redegjøre for hva sikkerhetspartneren overvåker og hvilken tilnærming som benyttes for å identifisere unormale aktiviteter utført av egne ansatte, eller av personell hos leverandører, inkludert konsulenter, med tilgang til foretakets infrastruktur og/eller systemer.
Av styrets svar fremgår det at sikkerhetspartneren skal overvåke konkrete forsøk på innbrudd og tyveri av informasjon, men at eventuelt misbruk av rettigheter i systemene utført av egne medarbeidere eller ansatte hos leverandører ikke blir overvåket. Videre fremgår det av styrets svar at foretaket vil ta Finanstilsynets innspill om overvåkning og analyse av unormal brukeraktivitet i foretakets infrastruktur og systemer med i det videre arbeidet med overvåkningsløsninger.

Konfigurasjonsstyring

I foreløpig tilsynsrapport ba Finanstilsynet foretaket redegjøre for om det er etablert en konfigurasjonsdatabase (CMDB), som til enhver tid viser oversikt over komponenter i teknisk infrastruktur med status på programvare, herunder versjoner, patch-status, og status på herding, inkludert utkontraktert virksomhet.

Fra styrets svar har Finanstilsynet merket seg at foretaket har et eget verktøy for styring av patcher og at foretaket forbereder migrering til ny infrastrukturplattform. På den nye plattformen vil det etableres en mer komplett oversikt over utstyr, og konfigurasjonsstyringen vil bli forsterket.

Kontroll og overvåking av konfigurasjonsendringer i brannmurer

Finanstilsynet anbefalte i foreløpig tilsynsrapport bruk av proaktive kontroller, som gjennom alarmer i sanntid kan avdekke uautoriserte endringer på sikkerhetskomponenter.

Fra styrets svar har Finanstilsynet merket seg at foretaket løser behovet for kontroller ved at sikkerhetspartneren aktivt overvåker definerte høyrisikoområder. Videre fremgår det av styrets svar at foretaket kontrollerer at prosedyrer for endring og godkjenning følges, og at foretaket kontrollerer at utførte endringer på sikkerhetskomponenter er i samsvar med de endringer som er godkjent. Som verifikasjon på sikkerhetsstatus og motstandsevne mot sårbarheter fremgår det av styrets svar at det gjøres bruk av sporadiske penetrasjonstester.

Informasjonslekkasje

Finanstilsynet viste i foreløpig tilsynsrapport til at foretaket hadde svakheter som utgjør risiko for informasjonslekkasje, og at Finanstilsynet ikke var kjent med at foretaket hadde rutiner og kontroller for klassifisering av informasjon og for å avdekke uautoriserte forsendelser av informasjon via e-post.

Fra styrets svar har Finanstilsynet merket seg at foretaket i etterkant av tilsynet har etablert rutiner for klassifisering av informasjon og for sikker e-post-utveksling. Det fremgår videre av styrets svar at foretaket er i prosess med å etablere forbedrede rutiner og løsninger for å redusere risiko for informasjonslekkasjer.

Tilgangsstyring

Finanstilsynet pekte i foreløpig tilsynsrapport på at foretaket så ut til å mangle uavhengig kontroll av lederes godkjenning av tilganger som gis til ansatte og konsulenter. Finanstilsynets vurderte at foretaket burde styrke kontrolltiltak som reduserer risikoen for at ansatte, konsulenter og personell hos leverandører har tilganger og autorisasjonsnivåer som går utover deres ordinære rolle og fullmakter.

Av styrets svar fremgår det at compliancefunksjonen og personvernombudet har utført selvstendig kontrollarbeid knyttet til tilgangsstyring, og at det er etablert prosess for revidering av tilganger i førstelinje, der resultater rapporteres til compliancefunksjonen og styret. Finanstilsynet noterer seg at foretaket vil vurdere styrking av kontrolltiltak i forbindelse med etablering CISO-funksjonens rolle og ansvar som kontrollfunksjon i andre linje.

Finanstilsynet har videre fra styrets svar merket seg at det for 2021 er satt av ekstra midler øremerket tilgangsstyring for å skifte ut/modernisere deler av de tekniske løsningene, og at foretaket i forbindelse med overgang til ny infrastrukturplattform forutsetter at brukeradministrasjonen vil bli forenklet og mer intuitiv.

Utvidede tilgangsrettigheter hos leverandører

I foreløpig tilsynsrapport påpekte Finanstilsynet at det var uklart om foretaket til enhver tid har oversikt over hvem, både ansatte og personell hos leverandører, som har utvidede tilgangsrettigheter.

Finanstilsynet har fra styrets svar merket seg at forbedringer på dette området vil bli tatt høyde for i governance og compliance knyttet til ny infrastrukturplattform.

Finanstilsynet forventer at foretaket sikrer tilstrekkelig overvåking av og kontroll med aktivitetene til personell med utvidete tilgangsrettigheter, slik at uautoriserte handlinger, som kan påføre foretaket stor skade, blir avdekket.

Kontinuitetsledelse

Forretningsmessige konsekvensanalyser

I foreløpig tilsynsrapport pekte Finanstilsynet på at det for noen forretningsprosesser så ut til å mangle forretningsmessige konsekvensanalyser, og stilte også spørsmål ved kvaliteten på selve analysene.

Styret har i sitt svar kun redegjort for eksempler på forretningsmessige konsekvensanalyser.

Etter Finanstilsynets vurdering bør de forretningsmessige konsekvensanalysene ta utgangspunkt i forretningsenhetens evne til å utføre kritiske forretningsprosesser. Konsekvensanalyse på enkeltprosesser vil avdekke hvilke infrastrukturelementer og systemer som må være tilgjengelig for at enkeltprosessene skal kunne utføres.

Finanstilsynet understeker viktigheten av at styret sikrer at forretnings- og stabsområdene tar tydelig eierskap og selv utfører de forretningsmessige konsekvensanalysene, med utgangspunkt i de forretningsprosessene som defineres som kritiske.

Forvaltning av forretningsmessige konsekvensanalyser

Finanstilsynet pekte i foreløpig tilsynsrapport på at det er viktig at foretaket sikrer at det etableres rutiner for at kontinuitetsplaner oppdateres der endringer i forretningsprosesser kan påvirke kravene til kontinuitet og reserveløsninger.

Finanstilsynet har merket seg styrets orientering om at oppdatering av kontinuitetsplaner i dag primært ivaretas i prosjektstyringen, der endrede krav til driftsoppsett og kontinuitetshensyn vil bli ivaretatt.

Scenarioer

I foreløpig tilsynsrapport stilte Finanstilsynet spørsmål til om foretaket hadde tilstrekkelige scenarioer for alvorlige cyberangrep og tilstrekkelig trening i å håndtere slike scenarier.

Finanstilsynet har merket seg styrets svar som beskriver foretakets tidligere og pågående aktiviteter på området.

Finanstilsynet vurderer det som viktig å inkludere scenarier og øvingsaktiviteter som innbefatter leverandørene, samt scenarier der inntrengere har fått fotfeste på innsiden av foretakets infrastruktur.

Finanstilsynet ber om å motta kopi av protokollen fra styremøtet hvor Finanstilsynets merknader blir behandlet.

Kopi av dette brevet bes sendt til ekstern og intern revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Jarleif Lødøen
tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.