FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Protector Forsikring ASA
Ved styret
Postboks 1351 Vika
0113 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
23/9223			04.09.2024

Tilsynsrapport

Finanstilsynet gjennomførte stedlig IKT-tilsyn i Protector Forsikring ASA (Protector eller foretaket) 8. oktober 2023.

Hensikten med tilsynet var å gjøre en vurdering av hvordan foretaket administrerer, utvikler, drifter, vedlikeholder og sikrer IKT-systemer og -tjenester. For dette området ble tilsynet avgrenset til elektronisk forsvar og tilhørende emner innen IKT-sikkerhet og styring og kontroll med IKT-virksomheten. Videre ønsket Finanstilsynet å gjøre en vurdering av foretakets beredskapsarbeid relevant for IKT-området, herunder vurdere beredskapen i foretaket og for utkontrakterte IKT-tjenester, samt at regulatoriske krav på dette området overholdes.

Til grunn for tilsynsrapporten ligger Finanstilsynets foreløpige rapport datert 23. april 2024 og styrets kommentarer til rapporten i brev av 13. juni 2024.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

Organisering

Det framgår av finansforetaksloven § 8-6 første ledd at styret skal sørge for forsvarlig organisering av virksomheten. Videre stilles det krav til at et finansforetak skal ha uavhengige kontrollfunksjoner med ansvar for risikostyring, etterlevelse, aktuarfaglig oppgaver og internrevisjon, jf. § 13-5 andre ledd.

Finanstilsynet pekte i foreløpig rapport på at det for Finanstilsynet var uklart hvor i foretakets organisasjon ansvaret for informasjonssikkerhet er plassert. Det ble videre pekt på at dersom informasjonssikkerhetsansvarlig er organisert i foretakets første forsvarslinje, vil denne ikke ha en uavhengig rolle i forhold til foretakets førstelinje. Foretaket må av den grunn sikre at andre forsvarslinje bemannes med ressurser og kompetanse som kan kontrollere og se til at foretakets IKT-sikkerhetspolicy er operasjonalisert i foretaket, og at de samme kravene også gjelder for IKT-tjenesteleverandører og underleverandører.

Styret har i sitt svarbrev opplyst at informasjonssikkerhetsansvarlig er organisert under IT og at andrelinjen vil bli styrket.

Finanstilsynet tar styrets svar til orientering og legger til grunn at foretakets andrelinje skal styrkes tilstrekkelig for å ivareta kontroller på IKT-sikkerhets området.

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Stig Ulstein
Dir. tlf. 22 93 99 66

Overvåking og rapportering av IKT-risiko
Finansforetaksloven § 13-5 stiller krav til forsvarlig virksomhet og god forretningsskikk. Foretaket skal ha klare og hensiktsmessige styrings- og kontrollsystemer samt hensiktsmessige retningslinjer og rutiner for å styre, overvåke, og rapportere risiko foretaket er eller kan bli eksponert for, jf. finansforetaksloven § 13-5 første ledd. Videre stiller IKT-forskriften § 2 første ledd krav til at foretaket skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten.

Finanstilsynet forventer at styregodkjente styringsdokumenter som strategier og policyer følges opp for å sikre at foretakets drift og planer utføres i henhold til disse. I foreløpig rapport pekte Finanstilsynet på at det ikke i tilstrekkelig grad gjennomføres egne andrelinje-kontroller eller revisjonsgjennomganger fra tredjelinjen av IKT-virksomheten for å kunne vurdere etterlevelse av foretakets overordnede målsetting om å ha effektiv styring og overvåkning av operasjonell risiko.

Styret har i sitt svarbrev opplyst om at styret mottar rapporter fra selskapets interne- og eksterne revisorer, samt rapporter fra internkontrollprosessen. Videre tar styret til etterretning at Finanstilsynet mener at IKT-virksomhetens kontroller og revisjoner bør ha ett utvidet omfang i forhold til dagens revisjoner.

Finanstilsynet tar styrets svar til orientering og legger til grunn at en styrket andrelinje vil utvide omfanget av andrelinjekontroller på IKT-området.

Virksomhetens konsekvensanalyse
Foretaket har ansvar for at nødvendig forretningsmessig kontinuitet og beredskap er sikret, jf. IKT-forskriften § 11. EIOPAs retningslinjer for IKT-sikkerhet og virksomhetsstyring[1], gir en utdyping av IKT-forskriftens bestemmelse for hvordan foretaket skal sikre forretningsmessig kontinuitet basert på virksomhetens konsekvensanalyser (BIA).

I foreløpig rapport pekte Finanstilsynet på at det ikke var gjennomført en virksomhetsmessig konsekvensanalyse. Finanstilsynet påpekte videre viktigheten av at foretaket utarbeider virksomhetsmessige konsekvensanalyser ledet av forretningssiden, der resultatet av konsekvensanalysen blant annet vil gi oversikt over foretakets systemporteføljе og angi kritikaliteten systemene har for foretakets virksomhet.

Styret opplyser i sitt svarbrev at foretaket har gjennomført analyser av konsekvensene av ulike driftsavbrudd, som har ført til krav til tidsgrenser for gjenoppretting. Disse kravene skal videre differensieres for ulike scenarier, og oppdateres jevnlig. Styret vil påse at virksomhetsmessige konsekvensanalyser inngår i foretakets ordinære drift og blir formidlet til relevante leverandører innen første kvartal 2025.

Finanstilsynet tar styrets svar til orientering.

IKT-sikkerhetshendelser
IKT-forskriften § 5 stiller krav om at foretaket skal ha prosedyrer for å sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Videre skal operasjonelle hendelser som medfører vesentlig reduksjon i funksjonalitet som følge av brudd på konfidensialitet, integritet eller tilgjengelighet til IKT-systemer og/eller data uten ugrunnet opphold rapporteres til Finanstilsynet, jf. IKT-forskriften

[1] EIOPA "Guidelines on information and communication technology security and governance" av 12. oktober 2020.

§ 9 tredje ledd. Foretaket skal rapportere hendelser som foretaket selv kategoriserer som alvorlig eller kritisk, jf. § 9 tredje ledd annet punkt. Foretaket kan videre rapportere andre avvik dersom disse avdekker spesielle sårbarheter i applikasjon, arkitektur, infrastruktur eller forsvarsverk. EIOPAs retningslinjer for IKT-sikkerhet og virksomhetsstyring beskriver nærmere hvilke krav som stilles til deteksjonsløsninger og hendelseshåndtering.

Finanstilsynet påpekte i foreløpig rapport at foretaket bør sikre at policyer og rutiner dokumenteres i tilstrekkelig grad, både for egne, interne systemer og for systemer levert av tjenesteleverandører, både i og utenfor normal arbeidstid.

Styret skriver i sitt svar at det forutsettes at nye konsekvensanalyser og forretningsstyrte planer for beredskap og gjenoppretting danner grunnlag for policyer og rutiner knyttet til hendelseshåndtering.

Finanstilsynet tar styrets svar til orientering og legger til grunn at nye konsekvensanalyser skal utarbeides og rutiner for hendelseshåndtering skal oppdateres i henhold til disse.

Utkontraktering

I henhold til IKT-forskriften § 2 skal foretaket ha retningslinjer for å sikre at utkontraktert IKT-virksomhet oppfyller kravene i § 12. Dette gjelder blant annet krav til skriftlig avtale, der avtalen skal sikre foretakets rett til å kontrollere, herunder revidere leverandørens aktiviteter, samt Finanstilsynets tilgang til opplysninger og mulighet for å føre tilsyn hos IKT-leverandøren.

I foreløpig rapport pekte Finanstilsynet på at foretaket har utkontrakteringsavtaler med begrensninger som strider med IKT-forskriftens bestemmelser. Finanstilsynet pekte videre på at det er foretaket som har ansvaret for at foretakets IKT-virksomhet oppfyller kravene i IKT-forskriften, herunder det å sikre at avtaler oppfyller forskriftens bestemmelser.

Styret har i sitt svarbrev opplyst om at samtlige utkontrakteringsavtaler er gjennomgått i sammenheng med implementering av [redacted]. Videre skriver styret at [redacted] avtalen skal gjennomgås, og eventuelle andre avtaler som faller under meldepliktforskriften skal snarest meldes til Finanstilsynet.

Finanstilsynet tar styrets svar til orientering.

Kriseberedskap

I IKT-forskriftens § 11 framgår kravene om at foretaket skal ha en dokumentert kriseplan som skal kunne iverksettes dersom IKT-driften ikke kan opprettholdes som følge av en krise, og at det minst årlig skal gjennomføres opplæring, øvelse og testing, med dokumentasjon av testresultater, som viser at kriseløsningen virker som forutsatt.

I foreløpig rapport pekte Finanstilsynet på at foretaket bør se på omfanget av beredskapstester som involverer foretakets hovedleverandør, for å sikre at områder foretaket har definert som kritiske blir ivaretatt i testutvalget. Videre pekte Finanstilsynet på at foretaket har satt et mål for gjenopprettingstid[2] som ikke tar utgangspunkt i virksomhetens konsekvensanalyse.

Styret skriver i sitt svar at det har tatt initiativ ovenfor IKT-tjenesteleverandør for å sikre at områder foretaket har definert som kritiske blir ivaretatt i testutvalget. Videre skriver styret at å gjennomføre

[2] Recovery time objective – RTO.

konsekvensanalyser og sette mål for gjenopprettingstid er en del av arbeidet framover, et arbeid som vil sluttføres i løpet av 2024.

Finanstilsynet tar styrets svar til orientering og legger til grunn at arbeidet med konsekvensanalyser vil ferdigstilles i løpet av 2024.

Kopi av dette brevet bes sendt til valgt revisor.

For Finanstilsynet

Olav Johannessen
seksjonssjef

Stig Ulstein
senior tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.