FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Styret i Gjensidige Forsikring ASA
Postboks 700 Sentrum
0106 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
18/4504			10.12.2018

Merknader - endelig rapport

Finanstilsynet gjennomførte stedlig tilsyn i Gjensidige Forsikring ASA 21. juni 2018. Formålet med tilsynet var å vurdere Gjensidige Forsikring ASAs arbeid med cybersikkerhet som relatert til dette tilsynet var definert som proaktive og reaktive tiltak mot tilsiktedet angrep over internett. Tilsynet var begrenset til Gjensidige Forsikring ASAs skadeforsikringsvirksomhet i Norge.

Til grunn for disse merknadene ligger Finanstilsynets foreløpige rapport datert 30. august 2018 og styrets kommentarer til rapporten i brev av 30. september 2018.

Finanstilsynet har følgende merknader etter det stedlige tilsynet:

Forhold knyttet til styring og kontroll av cybersikkerhet.

Styring og kontoll med forretningssidens involvering på IKT-sikkerhetsområde.
Gjennom tilsynet fremkom det at forretningssiden ikke er representert i sikkerhetsforum og ikke innehar noen rolle som sikkerhetskoordinator. Finanstilsynet pekte i foreløpig rapport på at forretningssiden bør ha en bredere involvering og tydeliggjøre sitt eierskap og ansvar for å stille krav til sikkerhet for systemer i verdikjeder som understøtter deres forretningsprosesser. Finanstilsynet har merket seg styrets svar der det fremgår at Gjensidige Forsikring ASA vil påse at administrasjonen tydeliggjør forretningssidens ansvar gjennom å revidere instrukser, utnevne sikkerhetskoordinatorer for relevante forretningsområder og sørge for at forretningssiden blir tydeligere representert i sikkerhetsforum.

Styring og kontroll med krav i styrende dokumenter i sikkerhetsrammeverket.
Finanstilsynet merket seg gjennom tilsynet at en del av de operative instruksene og rutinene i sikkerhetsrammeverket manglet konkrete krav til når eller hvor ofte aktiviteter skal gjennomføres. Finanstilsynet pekte i foreløpig rapport på at styret må sikre at instrukser, standarder og rutiner for IKT-sikkerhetsområdet utformes slik at konkrete krav til gjennomføring av aktivitetene fremkommer og ved det, gjør det mulig å kontrollere at kravene etterleves. Finanstilsynet ba også styret redegjørde for status og struktur på styrende dokumenter på IKT-sikkerhetsområdet.

FINANSTILSYNET
Revierstredet 3
Postboks 1187 Sentrum
0107 Oslo

Telefon 22 93 98 00
Telefaks 22 63 02 26

post@finanstilsynet.no
www.finanstilsynet.no

Saksbehandler
Åshild Johnsen
Dir. tlf 22 93 97 02

Det fremgår av styrets svar at styrende dokumenter, rutiner og standarder for å understøtte intern operasjonalisering på IT-sikkerhetsområdet er under kontinuerlig utvikling bl.a. som følge av nye og detaljerte sikkerhetskrav til foretakets leverandører. Finanstilsynet har merket seg styrets beskrivelse av organiseringen av arbeidet med den styrende dokumentasjonen. Finanstilsynet har notert seg at styret vil påse at forpliktende krav tas inn i rutiner og relevante styrende dokumenter i tråd med Finanstilsynets anbefaling.

Styring og kontroll med adgangsstyring for tilgang til å utføre driftsoperasjoner.
Ansatte med utvidete rettigheter og adgang til å utføre driftsoperasjoner kan ved feil bruk eller misbruk av sine rettigheter påføre selskapet stor skade, enten dette skjer fra innsiden eller utsiden. Administrasjonen av slike rettigheter må derfor være underlagt ekstra kontroll. Finanstilsynet ble gjennom tilsynet informert om at Gjensidige Forsikring ASA har laget en ny strategi for tilgangsstyring med spesifiserte krav til ny løsning for styring og kontroll med utvidete tilgangsrettigheter. Finanstilsynet ba i foreløpig rapport Gjensidige Forsikring ASA prioritere styringen med utvidete tilgangsrettigheter for egne ansatte, ansatte hos leverandøren og ansatte hos underleverandøren slik at disse er i henhold til tjenstlig behov, samt at bruken av utvidete tilgangsrettigheter overvåkes og kontrolleres spesielt. Finanstilsynet har merket seg styrets svar om at det i ny tjenesteavtale med leverandør er inntatt krav til løsning for styring og kontroll med utvidete tilgangsrettigheter, og at leverandøren vil sikre at dette blir implementert fortløpende gjennom 2019.

Styring og kontroll av tredjepartsleverandører av relevant infrastruktur.
Gjensidige Forsikring ASA har etablert et program for oppfølging av leverandørene med omfattende kontroller som etter Finanstilsynets oppfatning bidrar til at foretaket får et mere relevant bilde av sikkerhetsnivået hos leverandøren og gjør Gjensidige Forsikring ASA i stand til å stille spesifiserte krav til leverandøren som foretaket ellers ikke ville kunne gjort. Til tross for dette kan det være vanskelig å sikre seg at leverandørene på alle punkter etterlever sikkerhetskravene på en tilfredsstillende måte. Finanstilsynet ba i foreløpig rapport Gjensidige Forsikring ASA fortsette den grundige oppfølgingen av leverandørene og bruke ressurser på dette. Styrets svar bekrefter at det er en prioritert oppgave for Gjensidige Forsikring ASA å følge opp nye og eksiterende leverandørers etterlevelse av sikkerhetskravene.

Styring og kontroll - sikring mot kjente sårbarheter.
Finanstilsynet observerte under tilsynet at Gjensidige Forsikring ASA ikke mottar rapporter på sikring mot kjente sårbarheter for alle relevante plattformer samt mangler knyttet til egen drift på området. Finanstilsynet har merket seg styrets svar om at foretaket vil tilpasse rutiner og styringsmodell for leverandøroppfølging- og rapportering slik at det sikrer mottak av alle relevante rapporter samt at administrasjonen vil påse at relevante rutiner for systemutvikling og -forvaltning på dette området oppdateres og operasjonaliseres.

Styring og kontroll – sikring av e-post.
Finanstilsynet stilte i foreløpig rapport spørsmål om Gjensidige Forsikring ASA har etablert tilstrekkelige tiltak for å sikre e-post. Finantilsynet har merket seg styrets svar om at krav til nye

sikkerhetsløsninger for e-post er fremmet i ny tjenesteavtale med leverandør som vil bli implementert i 2019.

Styring og kontroll – beredskap for elektroniske angrep.
Finanstilsynet pekte i foreløpig rapport på at i Gjensidige Forsikring ASA's instruks for håndtering av sikkerhetshendelser bør det tydeligere refereres til konkrete og forhåndsbestemte tiltak som skal igangsettes for ulike typer angrep eller trusler om slike. Styret bekrefter i sitt svar at Gjensidige Forsikring ASA vil utarbeide relevante instrukser som ledd i implementeringen av en ny modell for samarbeid om incidenthåndteringen mellom foretaket og aktuelle leverandører.

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

Finanstilsynet ber om status for gjennomføringen av tiltakene som er omtalt i styrets brev innen 20. desember 2019.

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

For Finanstilsynet

Olav Johannessen
seksjonssjef

Åshild Johnsen
tilsynsrådgiver

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.