Norges Bank
Per E-post

Dato: 11.05.2021
Vår ref.: 2021 - 403
Deres ref.: Høringssvar TIBER NO

Høringssvar TIBER-NO

Finans Norge og Bits har behandlet forslaget og sender samlet høringssvar. Vi støtter forslaget til rammeverk TIBER-NO med følgende kommentarer til hovedpunktene i Høringsnotatet:

Generelle prinsipper

«Målsettingen for TIBER-NO er å bidra til finansiell stabilitet gjennom økt motstandsdyktighet mot cyberangrep for kritiske funksjoner i det norske finansielle systemet. TIBER-NO er ikke ment som et verktøy for tilsyn og overvåking av foretak og enkeltsystemer.»

Kommentar: Det er i foretakenes egeninteresse å sikre at virksomheten og systemene er motstandsdyktige mot cyberangrep. Kommersielle interesser har ofte et produkt eller tjenestespesifikt syn på saken, og det er derfor velkomment at myndighetene fastsetter et beste-praksis rammeverk som gjelder for alle. Implementert riktig, vil dette fungere som veiledning for å øke motstandsdyktigheten mot angrep for virksomheter av alle størrelser.

På bakgrunn av dette er vi enige i vurderingen fra myndighetene om at TIBER-NO ikke skal benyttes som et verktøy for tilsyn og overvåking av foretak og enkeltsystemer.

Frivillig eller obligatorisk deltakelse

På bakgrunn av ovenstående foreslås det at det er frivillig å delta i TIBER-NO.

Kommentar: I vårt høringssvar fra 2019, konkret for spørsmål 3 svarte Bits at vi mener at «… et norsk rammeverk må tilpasses variasjonen i størrelse og kapasitet for virksomheter i den norske finansnæringen». Vi kommenterte også at «… en eventuell implementering bør skje gradvis for å unngå at tester basert på rammeverket går på bekostning av andre sikkerhetsoppgaver».

Finans Norge og Bits mener fortsatt at disse kommentarene er gyldige, og at – dersom de hensyntas i implementeringen i Norge, vil bidra til økt deltakelse – gitt prinsippet om frivillighet.

Enkelte av våre medlemmer har også stilt spørsmål om det er mulig å komme med en tydeligere definisjon av «Sentrale aktører». Vil en sentral aktør være en bank-allianse eller større enkeltbanker i eller utenfor en allianse. Eventuelt om definisjonen også omfatter felles leverandører til alliansebanker eller banker i en løsere organisering.

Hansteens gt. 2 ● Telefon 23 28 42 00 ● firmapost@finansnorge.no ● PB 2473, 0202 Oslo ● Org.nr. 994 970 925 ● finansnorge.no

Målgruppe

«TIBER-NO er ment for foretak i finansiell sektor som har funksjoner som er kritiske for det norske finansielle systemet. For TIBER-NO er det likevel valgt at ikke-kritiske funksjoner også kan inkluderes i tester. Videre er det åpnet for at foretak i finansiell sektor som ikke har kritiske funksjoner kan delta i TIBER-NO og gjennomføre TIBER-tester»

Kommentar: Enkelt av våre medlemmer understreker at det er viktig at «kritiske funksjoner» defineres tydelig fra myndighetenes side. Se også kommentar vedrørende behovet for definisjon av «sentrale aktører». Det er viktig at disse definisjonene ses i sammenheng.

Andre medlemmer med nordisk eller europeisk nedslagsfelt understreker at hvis disse har sin hovedaktivitet i en annen EU-region så skal de følge prinsippene for den regionen, men da dele sine resultater med TIBER-NO.

Testprosessen

Kommentarer er tatt inn under hvert av punktene nedenfor.

Generic Threat Landscape Report

På bakgrunn av ovenstående foreslås det at GTL-rapport er obligatorisk for TIBER-NO og at GTL-rapporten fra NFCERT med vedlegg om norsk finansiell infrastruktur benyttes.

Kommentar: Finans Norge og Bits støtter dette. Så vidt næringen er informert om så er det allerede utarbeidet en norsk GTP-rapport. Enkelte medlemmer med nordisk nedslagsfelt kommenterer også at en GTL-rapport utarbeidet for et av de andre nordiske landene også bør kunne aksepteres.

Involvering av nasjonal trusseletterretning og sikkerhetstjenester

På bakgrunn av ovenstående foreslås det at involvering av nasjonale etterretnings- og sikkerhetstjenester er frivillig ved testing etter TIBER-NO, både for TCT-NO og foretakene som gjennomfører testing.

Kommentar: Finans Norge og Bits støtter dette. Etter som vi allerede har en god involvering fra NFCERT synes våre medlemmer ikke det er nødvendig med obligatorisk involvering av nasjonal trusseletterretning og sikkerhetstjenester.

Involvering av andre myndigheter i testing

På bakgrunn av ovenstående foreslås det at TCT-NO og foretaket som testes kan involvere andre myndigheter i testingen, men at dette ikke er obligatorisk etter TIBER-NO.

Kommentar: Finans Norge og Bits støtter dette, men vil understreke at dette ikke må endre testprosessen eller testaktivitetene på noen måte. Næringen støtter at dette ikke bør være obligatorisk.

Oppdatering av etterretning

Det foreslås at oppdatering av etterretning gjennom testperioden er frivillig etter TIBER-NO.

Kommentar: Finans Norge og Bits støtter dette, og vil understreke at det kan være nyttig med deltakelse fra trusseletterretning (TI) under 'red-team' testfasen siden de kan bidra med inspirasjon

og innsyn. Våre medlemmer har ingen motforestillinger mot at dette skal være en frivillig aktivitet, men understreker at det må avtales på forhånd siden dette kan påvirke kostnader og kapasitet.

Bruk av fysiske gjenstander i testingen

På bakgrunn av ovenstående foreslås det at bruk av fysiske gjenstander (minnepinner mv.) tillates etter TIBER-NO. Foretakets «White Team» må sørge for at det gjøres en grundig risikovurdering forut for hver test. Eventuelle tiltak for å redusere testrisiko må gjennomføres før testing igangsettes.

Kommentar: Finans Norge og Bits støtter dette og har ingen ytterligere merknader.

Utvide enkelttester til å inkludere funksjoner som ikke er kritiske

På bakgrunn av ovenstående foreslås det at testing etter TIBER-NO kan inkludere ikke-kritiske funksjoner hos foretaket som testes.

Kommentar: Finans Norge og Bits støtter dette. Enkelte av våre medlemmer understreker at de vil lage en prioritert liste over ulike funksjoner og vil inkludere ikke-kritiske funksjoner etter kapasitet og en god grunn for å inkludere de.

Scenarier som ikke er avtalt på forhånd

På bakgrunn av ovenstående foreslås det at TIBER-NO tillater Scenario X-testing. «White Team» i foretaket som testes har ansvar for å godkjenne Scenario X-testing.

Kommentar: Finans Norge og Bits støtter dette. Godkjenning av Scenario X bør være basert på en risikovurdering av de foreslåtte test-scenariene.

«Purple Teaming»

På bakgrunn av ovenstående foreslås det at «Purple Teaming» er valgfritt etter TIBER-NO.

Kommentar: Finans Norge og Bits støtter dette og har ingen ytterligere merknader.

Med vennlig hilsen
Finans Norge

Tom Høiberg
Fagdirektør Betaling og Digitalisering