Notat:

Høringssvar vedr Tiber-NO fra Sparebanken Vest

Bergen 07.05.2021

Generelle betraktninger:

Tiber- NO er omfattende og for mindre og mellomstore banker med begrensede ressurser innenfor sikkerhetsområdet og krav i rammeverket vil kunne gå ut over det daglige operasjonelle sikkerhetsarbeid. Hvordan ser NB for seg at dette skal kunne skaleres til å være tilpasset de forskjellige foretak?

Mange foretak har mange av sine kritiske tjenester hos samme leverandør og sjansen for at leverandør blir en viktig del av flere Tiber tester er stor. Hvordan ser NB for seg at en skal styre antall samtidige Tiber tester for at nøkkel leverandører i den norske infrastruktur ikke skal bli skadelidende?

Kritiske funksjoner og tjenester kan variere fra foretak til foretak. Hvor sterk styring av testcase tenker NB å ha, og hvordan tenker en at styringen skal foregå?

Tiber-NO er bygget på en stor andel av eksterne ressurser. Ressurser som etter vår erfaring kan være en knapphet på. Dette gir ofte de som har de største økonomiske muskler en fordel og som kan gi en usunn prising av sikkerhetstjenester.

Kan ikke finne noe om ønsket hyppighet av Tiber øvelser. Forventet at det skal øves årlig etter Tiber-NO rammeverk? Når en leser erfaringer fra de som har gjennomført tester i henhold til Tiber-EU rammeverket så går det med betydelige ressurser til planlegging og gjennomføring av øvelser. Om dette skal skje årlig må det planlegges for en økt bemanning hos foretakene.

Nesten ingen i Finansforetak i Norge kommer utenom en sentral 3dje part. Bør det være krav til tredjeparter som driver kritisk infrastruktur om at de må ha rutiner og prosesser på plass for å gjennomføre TIBER-NO testing? Blir veldig tungvint om hvert enkelt foretak må gå opp dette med sin 3dje part. Kan ofte være vanskelig nok bare å få gjennomført en pentest mot enkelte 3dje parter.

Samarbeid mellom banker

Vil det kunne godkjennes av TCT-No at det kjøres «felles» Tiber-NO øvelser på tvers av banker med omtrent lik størrelse og infrastruktur?

Roller:

TCT-NO

Skal bemannes og dekkes av personell fra NB. Hvordan ser en for seg at alle deler av finansnæringen skal kunne være med å legge rammene og føringene for TCT teamet?

Pkt. 3.1 foretaket er selv ansvarlig for kjøp av tjenester fra eksterne. Vil det bli laget en liste over foretak som er godkjent for å bruke til Tiber-NO tester? Kan det f.eks. være en ide å lage en «fast time pris» som de ekstern kan forvente å få i forbindelse med gjennomføring av en Tiber-No test? Dette for å få litt kontroll med forventede kostnader samtidig som en holder prisnivå stabilt.

Pkt. 3.1.1 er det mulig å leie inn prosjektledere til White Team? En erfaren konsulent innen WT vil kunne hjelpe betraktelig med gjennomføring

Pkt 3.1.4/3.1.5 kan leverandør av trusselbilde og red team være samme selskap?

Pkt. 3.1.5 må Red Team leverandører være forhåndsgodkjente av TCT eller vil det være en standard de må forholde seg til? Trusselbilde endrer seg så fort at standarder kan være et grunnelement, men bør ikke være en begrensing. Sirkulering av leverandører kan være positiv da de kan ha forskjellige fokuser og kompetanse. Så hvis de skal være forhåndsgodkjente leverandør bør det være en romslig liste og som et minimum nordiske leverandører, ikke bare norske.

Pkt. 4.2.2 TCT-NO bør ha helt klare anbefalinger rundt scoping, foretaket selv har ikke nødvendigvis nok selvinnsikt i hva de bør scope selv

Testing og rapport bør/kan kanskje også inneholde informasjon om det er tegn på aktive eller uaktive "innbrudd/uønsket aktivitet"

Pkt. 4.4.2 Hva med en "åpen" godkjenning for alle medlemmer på enkelte tester/scope hvis man er en underleverandør som andre benytter seg av