Netsecurity

Red Team-øvelser

Basert på TIBER-NO

Bakgrunn

I forbindelse med at Finanstilsynet og Norges Bank innfører TIBER-NO, tilbyr Netsecurity en ny tjeneste for trusselbaserte Red-Team øvelser rettet mot finansiell sektor.

Finanstilsynet og Norges Bank har gått sammen om å utarbeide et nytt rammeverk kalt TIBER-NO. Dette er det første nasjonale rammeverket som legger retningslinjer for hvordan man kan teste finansielle institusjoners evne til å forebygge, beskytte seg mot og håndtere cyberangrep.

TIBER er en forkortelse for "Threat-Intelligence-based Ethical Red Teaming", og TIBER-NO bygger på rammeverket TIBER-EU som er utviklet av den Europeiske Sentralbanken.

Hva er TIBER-NO test?

En Red Team-test etter TIBER-NO retningslinjene er beskrevet på følgende måte i Norges Banks implementeringsveiledning:

> ***«En TIBER-NO-test imiterer et potensielt angrep fra relevante trusselaktører for å teste om tiltakene foretakene har iverksatt er tilstrekkelige. Testingen er et supplement til foretakenes periodiske sikkerhetsrevisjoner, penetrasjonstester og sårbarhetsskanninger, og kan bidra til å gi et mer reelt bilde av motstandsdyktighet overfor cyberangrep.»***

Red Team-øvelser har, til forskjell fra ordinære penetrasjonstester, som formål å teste virksomhetens motstands, deteksjons- og responsevne på et angrep.

TIBER-NO/EU-baserte tester har følgende mål:

- Forbedre sikkerheten til virksomhetene, og finansbransjen generelt

- Standardisere og harmonisere måten virksomheter gjennomfører etterretningsdrevet Red Team-tester på tvers av EU

- Støtte etterretningsdrevet Red Team-tester på tvers av landegrenser for multinasjonale selskaper

- Etablering av et offentlig godkjenningsorgan av tester, slik at resultatene kan vises til på tvers av EU

Etterretningsbaserte Red Team-tester skiller seg fra ordinære Red Team-tester ved at man baserer testaktiviteter på reell kunnskap om hva slags angripere som er sannsynlige at er interessert i kundens virksomhet, og hvilke metoder disse bruker.

Som et eksempel så kan trusseletterretning vise at de aktuelle angriperne ikke benytter fysisk inntrenging som en del av sine operasjoner.
Man kan da nedprioritere fysiske angrepsmetoder, og fokusere mer på digitale angrep. Dette gir en mer effektiv og realistisk test, sammenlignet med en generisk Red Team-test basert på kundens og Red Team sine antagelser om hva man kan bli utsatt for.

Hvem trenger en slik test?

TIBER-NO er ment for foretak i finansiell sektor med funksjoner som er kritiske for det norske finansielle systemet. Myndighetene har likevel valgt at også ikke-kritiske funksjoner kan inkluderes.

Vi i Netsecurity mener at testmetodikken i en TIBER-NO-test vil være effektiv for andre næringer enn finansnæringen. Alle virksomheter med høye sikkerhetskrav vil ha nytte av slik testing, men virksomheter innen offshore, energi og kommunikasjon kan ha særlig behov for en slik vurdering av sin egen sikkerhet.

Hvis man føler at virksomheten har oppnådd en modenhet innen sikkerhet som gjør at man bør klare å oppdage og motstå et angrep, er tiden riktig for å gjennomføre en TIBER-NO basert Red Team-test for å få en uavhengig vurdering av om man er så godt forberedt som man tror.

Hvordan gjennomføres en TIBER-test?

Tiber-tester gjennomføres overordnet i fire faser:

I. White Team (kunden) beslutter omfang og gjennomføring av testing
II. Leverandør av trusseletterretning, for eksempel Netsecurity, stiller med spesifikk trussel- og scenariorapport om virksomheten.
III. Red Team planlegger og gjennomfører en TIBER-NO-test av virksomhetens infrastruktur basert på scenariene utviklet av trusseletterretningsleverandøren
IV. Avslutning, rapportering og godkjenning av TIBER Cyber Team (TCT-NO).

Red Team-tjenester

Dette er en ekstern tjenesteleverandør som planlegger og gjennomfører en TIBER-NO-test basert på scenariene i rapporten fra leverandøren av målrettet trusseletterretning. Etter testen skal Red Team levere en rapport som beskriver funnene hos virksomheten.

Netsecurity Red Team er et av Norges sterkeste fagmiljøer innen penetrasjonstesting og Red Team-øvelser. Vårt fokus er på å hjelpe kundene våre oppdage reell forretningsrisiko i deres virksomhet ved å bruke samme teknikker, taktikker og prosedyrer som det en ekte angriper ville gjort, uten å gjøre skade. Red Team sine medlemmer har lang erfaring med testing av all slags infrastruktur, og har særlig søkelys på etikk og kundekonfidensialitet. Samtlige har gjennomgått bakgrunnssjekker, og flere har aktive sikkerhetsklareringer i forbindelse med tidligere oppdrag.

Red Team kan gjennomføre testing av alle scenarier en reell angriper vil kunne utføre, som for eksempel:

/ Rekognosering
/ Sosial manipulering
/ Fysisk inntrenging
/ Inntrengning via eksterne og interne nettverk
/ Antivirus bypass
/ Angrep mot skybaserte miljøer
/ Phishing

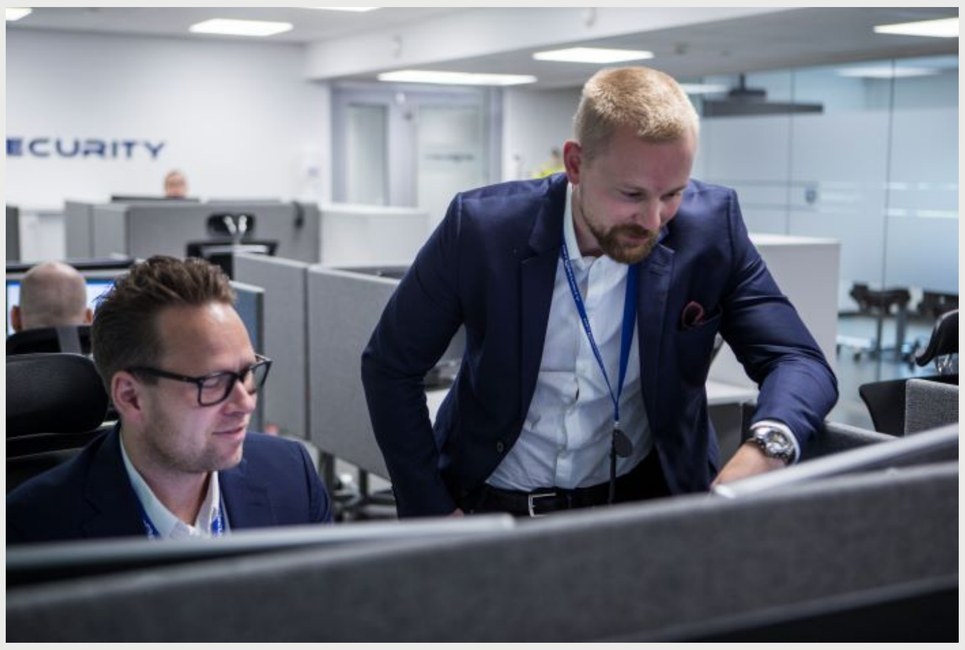
Oppsummering

Netsecurity AS stiller seg helhjertet bak Finanstilsynet og Norges Banks innføring av TIBER-NO. Dette vil være et viktig løft for sikkerheten for kritiske finansvirksomheter i Norge, og gir et godt utgangspunkt for andre sektorer til også kunne gjennomføre tester over samme lest. Vi oppfordrer tilsynsmyndighetene i andre sektorer til å følge Finanstilsynets eksempel i dette og opprettet tilsvarende ordninger.

Med vår lansering av trusseletterretningsbasert Red Team-testing har markedet fått en leverandør som står sterkt rustet til å utfordre sikkerheten hos enhver virksomhet, ved hjelp av avanserte, strukturerte og etterprøvbare metoder.

Trenger du bistand til gjennomføring av en TIBER-test eller er bekymret for tilstanden til sikkerheten i virksomheten din, så ta gjerne kontakt for en uforpliktende prat!

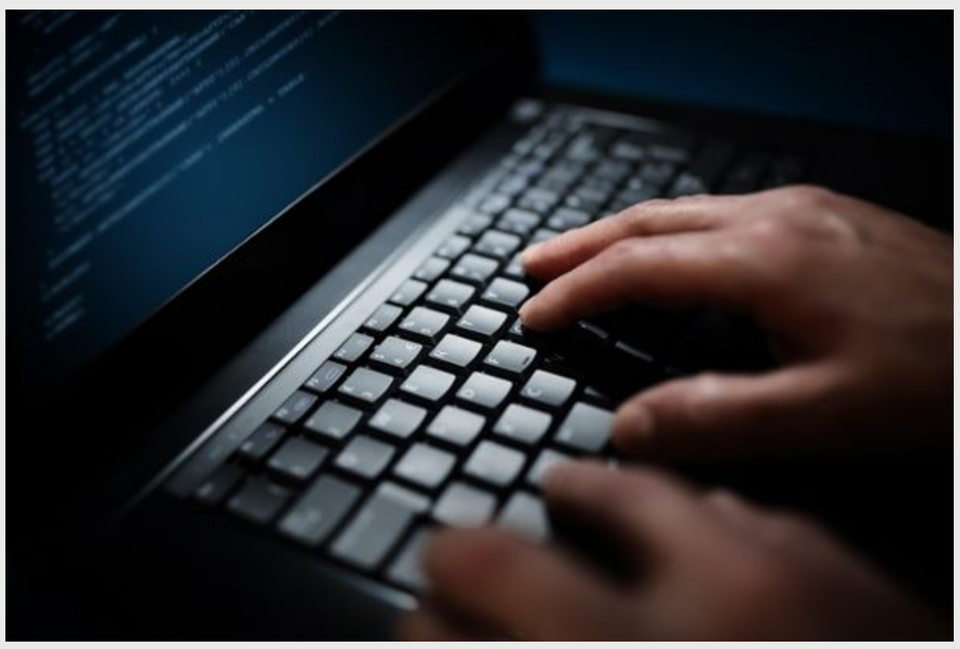
Relaterte tjenester fra Netsecurity



Hendelseshåndtering

De fleste bedrifter og organisasjoner må forholde seg til og forberede seg på sikkerhetshendelser. Dette kan være alt fra hacking, datainnbrudd og distribuert tjenestenekt til løsepengevirus, skadevare og ulike typer virusutbrudd.

LES MER



Penetrasjonstesting

Vi simulerer hvordan en målrettet angriper vil angripe dine systemer og din organisasjon. Dette gir et godt bilde av hvilken forretningsrisiko som eksisterer i organisasjonen, og tillater deg å rette opp i problemene før de blir utnyttet av andre.

LES MER

Vil du ha råd om hvordan du kan ta vare på IT-sikkerheten i din bedrift?

Vegard Vaage
Leder Red Team

vegard@netsecurity.no / +47 4114 2323