telenor | cyberdefence

White Paper

TIBER-NO - Trusselbasert penetrasjonstesting i finansielle foretak

v1.0 – 13.02.2025

Digital operasjonell motstandsdyktighet er ikke lenger et ambisjonsnivå, men et regulatorisk krav. Med DORA, tilhørende forskrifter og tekniske standarder er trusselbasert testing formalisert gjennom TLPT, med TIBER-EU som metodisk grunnlag. I denne white paperen tar vi en gjennomgang av det oppdaterte regelverket og belyser hvilke praktiske konsekvenser kravene har for finansforetak som omfattes.

Innholdsfortegnelse

1 Bakgrunn

I 2018 lanserte Den europeiske sentralbanken (ECB) TIBER-EU (Threat Intelligence-based Ethical Red-teaming), et rammeverk for å teste finansforetaks evne til å oppdage, beskytte seg mot og respondere på avanserte cyberangrep. Rammeverket er utviklet for å styrke motstandsdyktigheten i finansforetak og kritisk finansiell infrastruktur gjennom realistiske angrepssimuleringer som er skreddersydd til det enkelte foretaks trusselbilde og driftsmiljø.

I februar 2025 publiserte ECB en oppdatert versjon av TIBER-EU som presiserer kravene til trusselbasert penetrasjonstesting (Threat-Led Penetration Testing – TLPT) i finanssektoren i tråd med DORA (Digital Operational Resilience Act). Samtidig ble det vedtatt utfyllende bestemmelser for gjennomføring av TLPT gjennom Delegert kommisjonsforordning (EU) 2025/1190 av 13. februar 2025. Denne forordningen fungerer som en regulatorisk teknisk standard (RTS) for trusselbasert penetrasjonstesting etter DORA og er utarbeidet i samsvar med det oppdaterte TIBER-EU-rammeverket. Forordningen gjenspeiler rammeverkets struktur, metodikk og prosessbeskrivelse, og innebærer i praksis at TIBER-EU fungerer som en operativ håndbok for gjennomføring av TLPT-tester etter DORA.

TIBER-programmet legger til rette for at finansforetak gjennomfører regelmessige red-teaming-tester basert på de samme taktikker, teknikker og prosedyrer (TTP-er) som benyttes av reelle trusselaktører. Disse identifiseres gjennom grundig trusseletterretningsanalyse, med formål å avdekke og utbedre sårbarheter i kritiske systemer og prosesser før de kan utnyttes av faktiske angripere.

Hver TIBER-test er unik og tilpasses det enkelte foretaks risikoprofil og trusselbilde. Denne tilnærmingen bidrar til å sikre at foretakets cybersikkerhetsforsvar ikke bare er robust på papiret, men også effektivt i praksis mot avanserte og vedvarende trusler (APT).

En TIBER-test gjennomføres i fasene forberedelse, testing og avslutning, med tydelige krav til roller, ansvar og styring for alle involverte parter. Dette omfatter blant annet utarbeidelse av en skreddersydd trusseletterretningsrapport og testplan, gjennomføring av selve testaktivitetene samt dokumentasjon av erfaringer og forbedringstiltak i en samlet "Lessons Learned"-rapport.

1.1 DORA i norsk rett

DORA-loven "Lov om digital operasjonell motstandsdyktighet i finanssektoren" (LOV-2025-05-27-18) trådte i kraft 01.07.2025. Den implementerer EØS-versjonen av EUs Digital Operational Resilience Act (DORA) som norsk lov.

DORA-forskriften "Forskrift om digital operasjonell motstandsdyktighet i finanssektoren" (FOR-2025-06-24-1296) trådte i kraft 01.07.2025 som supplement til loven. Den gir utfyllende bestemmelser til lovens overordnede bestemmelser.

"Forskrift om endring i DORA-forskriften" (FOR-2026-01-26-87) er en endringsforskrift til DORA-forskriften. Den trådte i kraft 26.01.2026, og har som formål å oppdatere og utvide det tekniske regelverket som gjelder som norsk forskrift etter DORA-loven. Hovedinnhold i endringen er innlemmelse av fire nye tekniske reguleringsstandarder (RTS-er) i DORA-forskriftens § 3 bokstav g–j. Disse standardene er knyttet til DORA-forordningen (EU) 2022/2554 og gir detaljerte krav innen blant annet tilsyn, testkrav og krav for tredjeparter.

Særlig sentral er innlemmelsen i DORA-forskriftens § 3 bokstav j av RTS om Threat-Led Penetration Testing (TLPT), fastsatt i Delegert kommisjonsforordning (EU) 2025/1190 av 13.02.2025. Forordningen fastsetter kriterier for hvilke foretak som omfattes av TLPT-kravet, samt detaljerte krav til testmetodikk, omfang, styring og samarbeid med relevante tilsynsmyndigheter. Innlemmelsen markerer et tydelig skifte fra overordnede prinsippkrav til konkrete, målbare og etterprøvbare forventninger til digital operasjonell motstandsdyktighet i finanssektoren. RTS-en fastslår at TLPT under DORA ikke introduserer et nytt testregime, men bygger direkte på og formaliserer TIBER-EU som det metodiske og strukturelle fundamentet for trusselbasert testing i finanssektoren. For finansforetak som omfattes av TLPT-kravet innebærer dette at etablerte TIBER-EU-rammeverk og nasjonale implementeringer kan benyttes direkte, forutsatt at denne er i samsvar med kravene i artikkel 26 og 27 i DORA-forordningen og den tilhørende RTS-en. Regelverket gir dermed både regulatorisk forutsigbarhet og metodisk kontinuitet, samtidig som det gjør avansert trusselbasert testing til et bindende krav snarere enn en frivillig modenhetsøvelse.

1.2 TIBER-EU-tilpasninger

Nasjonale versjoner av TIBER-EU er innført i flere europeiske land. Disse tilpasningene er vanligvis skreddersydd for å møte lokale forhold og regulatoriske krav, samtidig som kjerneprinsippene i TIBER-EU-rammeverket beholdes.

1.2.1 TIBER-NO

I 2021 lanserte Norges Bank og Finanstilsynet en norsk tilpasning av rammeverket kalt TIBER-NO. Som følge av ECBs oppdatering av TIBER-EU ble TIBER-NO i 2025 revidert for å sikre samsvar med den oppdaterte metodikken og de harmoniserte kravene til trusselbasert penetrasjonstesting. Rammeverket har som formål å styrke finansiell stabilitet ved å øke motstandsdyktigheten mot cyberangrep mot kritiske funksjoner i det norske finansielle systemet.

TIBER-NO følger de grunnleggende prinsippene i det originale TIBER-EU-rammeverket, som fokuserer på å bruke trusselbasert penetrasjonstesting for å teste og forbedre cyberforsvaret til finansielle institusjoner. Ved å implementere dette rammeverket har Norges Bank som mål å gjøre det mulig for finansforetak i Norge å bedre forberede seg mot sofistikerte cybertrusler ved å simulere realistiske angrepsscenariener som reflekterer de mest relevante risikoene for hvert enkelt foretak.

Under TIBER-NO vil finansforetak typisk gjennomgå en skreddersydd testprosess som inkluderer innsamling av trusseletterretning, definering av kritiske funksjoner og systemer, og gjennomføring av kontrollerte cyberangrep av et uavhengig "Red Team" for å identifisere sårbarheter og teste effektiviteten til foretakets cyberforsvar.

1.2.2 Tilpasning til andre sektorer

Selv om det opprinnelig ble designet for finanssektoren, har TIBER-rammeverket et potensial for tilpasning på tvers av forskjellige andre kritiske sektorer på grunn av sin robuste tilnærming til å øke motstandsdyktigheten i nettverks- og informasjonssystemer til både private og offentlige aktører som opererer i relevante sektorer. Vesentlige samfunnsviktige sektorer fremgår av NIS2-direktivets vedlegg 1. Denne gruppen omfatter utvalgte offentlige eller private tilbydere av samfunnsviktige tjenester som opererer i sektorene energi, transport, bank, finansmarkedsinfrastrukturer, helse, drikkevann, avløpsvann, digital infrastruktur, IKT-tjenester, offentlig forvaltning (sentral og regional) og romvirksomhet.

Her er noen eksempler på bruk av TIBER-rammeverket i andre sektorer:

- **Kraftforsyning**: Denne sektoren er avgjørende for nasjonal og samfunns-sikkerhet. Tilpasning av TIBER kan bidra til å identifisere sårbarheter som kan utnyttes til å forårsake betydelige forstyrrelser.
- **Helsevesen**: Sykehus og helsevesen stoler i økende grad på digitale systemer, noe som gjør dem sårbare for nettangrep som kan få alvorlige konsekvenser for pasientbehandlingen. TIBER-lignende tester kan øke motstandskraften til helsevesenets IT-systemer ved å sikre at de kan motstå sofistikerte cybertrusler.
- **Transport**: Dette inkluderer luft-, sjø- og landtransportsystemer som er avgjørende for både økonomisk stabilitet og nasjonal sikkerhet. TIBER-lignende tester i denne sammenhengen kan bidra til å forhindre forstyrrelser som kan oppstå fra cyberfysiske angrep.
- **Offentlige tjenester**: Offentlige etater, som håndterer sensitive data og kritisk infrastruktur, kan dra nytte av TIBER-lignende tester for å beskytte mot spionasje, datatyveri og sabotasje.
- **Telekommunikasjon**: Som ryggraden i digital kommunikasjon er denne sektoren en kritisk infrastruktur som trenger robuste forsvarsmekanismer mot komplekse cybertrusler, noe som gjør den til en ideell kandidat for TIBER-lignende rammeverk.

2 Organisering og ledelse av et TIBER-engasjement

Foretak som gjennomfører tester under TIBER-rammeverket er selv ansvarlige for å administrere og organisere testen. Dette ansvaret inkluderer å anskaffe tjenester fra eksterne leverandører, implementere kontroller, prosesser og prosedyrer for å sikre at testen overholder kravene i TIBER-rammeverket og overholder beste praksis. I tillegg må foretaket håndtere risikoer for å sikre at de holder seg innenfor akseptable nivåer.

I en TIBER-test spiller flere spesialiserte team avgjørende roller for å sikre effektiviteten og integriteten til testprosessen. Her er en kort beskrivelse av de viktigste teamene:

1. **TIBER Cyber Team (TCT)**: Teamet hos den relevante myndigheten som har ansvar for å føre tilsyn med gjennomføringen av testen og påse at den oppfyller kravene i TIBER-rammeverket. Dette sikrer at testen kan gjensidig anerkjennes av relevante myndigheter.
2. **Control Team (CT)**: Det teamet overvåker hele TIBER-testen for å sikre at den utføres rettferdig, sikkert og i samsvar med de avtalte vilkårene og betingelsene. Dette teamet inkluderer vanligvis medlemmer fra organisasjonens ledelse og noen ganger representanter fra reguleringsorganer. De koordinerer og administrerer samspillet mellom de andre teamene, sørger for overholdelse av testens omfang og håndterer logistikk og administrasjon av testen. Control Team sørger også for at resultatene dokumenteres hensiktsmessig og at det iverksettes oppfølgingstiltak basert på funnene.
3. **Red Team Testers (RTT)**: Dette er en ekstern gruppe, ofte engasjert fra spesialiserte leverandører, som har som oppgave å simulere handlingene til potensielle angripere basert på etterretningen levert av TIP. Målet er å utfordre organisasjonens forsvar ved å utnytte sårbarheter på en kontrollert og avtalt måte. Effektiviteten til Red Team er avgjørende siden det direkte tester robustheten til organisasjonens defensive mekanismer og den generelle sikkerhetstilstanden til organisasjonen.

4. **Blue Team (BT)**: Dette teamet er ansvarlig for forsvar av organisasjonens IT-infrastruktur. De er vanligvis det interne sikkerhetsteamet til organisasjonen som testes. Deres rolle i en TIBER-test er å respondere på angrepene simulert av Red Team, implementere defensive strategier og reagere på brudd som de ville gjort i et ekte angrepsscenario. Dette gir innsikt i organisasjonens beredskap og motstandskraft mot faktiske cybertrusler.
5. **Threat Intelligence Provider (TIP)**: Leverandør av trusseletterretning spiller en kritisk rolle i forberedelsesfasen av TIBER-testen. De samler inn og gir detaljert og relevant trusselinformasjon om potensielle trusselaktører som er spesifikke for organisasjonen. Denne etterretningen inkluderer taktikker, teknikker og prosedyrer (TTP-er) som trusselaktører sannsynligvis vil bruke. Kvaliteten og nøyaktigheten til informasjonen levert av TIP er avgjørende for å utforme realistiske angrepsscenarier som Red Team vil utføre.

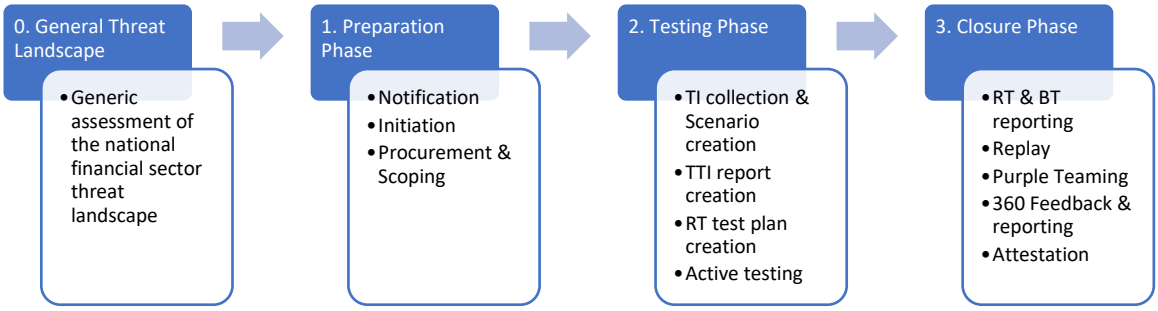
Merk: For TIBER-NO-tester er det et krav at tredjepartsleverandører må brukes til målrettet trusseletterretning og Red Team-testing. Under visse omstendigheter (se TIBER-EU 3.6.3) kan et internt Red Team med de nødvendige ferdighetene og erfaringene benyttes for å utføre testen. Dette skal kun gjøres i unntakstilfeller og krever forhåndsgodkjenning fra TCT.

3 Testprosessen

Testprosessen i et TIBER-engasjement er utformet for å sikre en strukturert, kontrollert og realistisk gjennomføring av målrettede trusselbaserte tester. Prosessen omfatter planlegging, gjennomføring og avslutning av testen i tråd med TIBER-rammeverket, med tydelig definerte roller, ansvar og styringsmekanismer. Den legger til rette for en helhetlig vurdering av foretakets evne til å forebygge, avdekke, håndtere og lære av avanserte cyberangrep mot kritiske funksjoner, og danner grunnlaget for målrettede forbedringstiltak innen operasjonell motstandsdyktighet.

3.1 Overordnet prosessoversikt

Den overordnede prosessoversikten gir et samlet bilde av hovedfasene i et TIBER-engasjement og hvordan disse henger sammen gjennom hele testløpet. Prosessen illustrerer samspillet mellom styring, trusselbasert forberedelse, kontrollert gjennomføring og strukturert oppfølging, og viser hvordan aktiviteter og beslutningspunkter er organisert fra forberedelse til avslutning. Prosesstegningen understøtter forståelsen av rekkefølge, avhengigheter og ansvar, og bidrar til en felles referanseramme for involverte parter.



0. **Generelt trussellandskap (General Threat Landscape - GTL)**

- **GTL-rapport(er)**: GTL-fasen involverer en generisk vurdering av det nasjonale trusselbildet for finanssektoren, skisserer de spesifikke rollene til enhetene, identifiserer relevante avanserte trusselaktører for sektoren og TTP-ene som er rettet mot disse enhetene. Nordiske land som har tatt i bruk TIBER-EU har bestemt at den årlige "Cyber Threat Landscape"-rapporten fra Nordic Financial CERT (NFCERT) skal være generisk trussellandskapsrapport for TIBER-testing og er også valgt for TIBER-NO. Det bør også tas hensyn til de årlige nasjonale trusselrapportene fra Nasjonal sikkerhetsmyndighet (NSM), Politiets sikkerhetstjeneste (PST) og Etterretningstjenesten.

1. **Forberedelse (Preparation Phase)**
   - **Notification process**: Foretaket varsler TIBER-NO om intensjon om å gjennomføre TIBER-test og etablerer konfidensiell dialog.
   - **Initiation process**: Intern beslutning tas, Control Team etableres, og prosjektmandat og overordnede rammer fastsettes.
   - **Scoping process**: Kritiske funksjoner, systemer og leverandører identifiseres, og testomfang avgrenses og godkjennes.
   - **Procurement process**: Uavhengige Threat Intelligence- og Red Team-leverandører anskaffes i tråd med TIBER-krav.
   - **Approval process**: Scope, leverandører og testopplegg godkjennes av ledelsen og TIBER-NO.
   - **Project management process**: Prosjektstyring etableres med plan, roller, eskalering og forberedelse til testfasen.
2. **Testing (Testing Phase)**
   - **Testing phase: Threat Intelligence**
     - **Threat intelligence collection process**: Innsamling og analyse av relevant informasjon om aktører, kapabiliteter og angrepsmetoder rettet mot foretaket.
     - **Scenario creation process**: Utforming av realistiske og målrettede angrepsscenarier basert på identifiserte trusselaktører og kritiske verdier.
     - **TTI Report creation process**: Utarbeidelse av Targeted Threat Intelligence-rapport som dokumenterer trusselbildet og anbefalte testscenarier.
     - **Approval process**: TTI-rapport og scenarier gjennomgås og godkjennes av Control Team og TIBER-NO.
     - **Project management process**: Løpende styring og koordinering av TI-aktivitetene mot tidsplan og kvalitetskrav.
   - **Testing phase: Red-Teaming**
     - **RT test plan creation process**: Utarbeidelse av detaljert Red Team-testplan basert på godkjente TTI-scenarier.
     - **Approval process**: Testplan, metodevalg og sikkerhetsrammer godkjennes av Control Team og TIBER-NO.
     - **Active Testing process**: Kontrollert gjennomføring av realistiske angrep for å teste institusjonens deteksjons- og responskapasitet.
     - **Project management process**: Styring av testgjennomføring, eskalering, fremdrift og samhandling mellom involverte parter.

3. **Avslutning (Closure Phase)**
    - **RT & BT reporting process**: Ferdigstillelse og konsolidering av Red Team- og Blue Team-rapporter med endelige funn og læringspunkter.
    - **Replay process**: Strukturert gjennomgang av testforløpet for å verifisere hendelseskjede, observasjoner og beslutninger.
    - **Purple Teaming process**: Felles analyse mellom Red Team og Blue Team for å validere funn og identifisere konkrete forbedringstiltak.
    - **Approval process**: Endelige rapporter og konklusjoner kvalitetssikres og godkjennes av Control Team og TIBER-NO.
    - **Reporting process**: Formell rapportering til ledelse og relevante styringsorganer i henhold til TIBER-NO-krav.
    - **360° Feedback process**: Systematisk innhenting av tilbakemeldinger om gjennomføring, samhandling og modenhet.
    - **Attestation process**: Formell bekreftelse på at TIBER-testen er fullført i samsvar med metodikk og godkjente rammer.
    - **Project management process**: Avslutning av prosjektet med dokumentasjon, erfaringsoppsummering og formell lukking.

Disse fasene er sykliske, noe som forsterker det faktum at cybersikkerhet er en kontinuerlig prosess med forbedring og tilpasning til trusler i utvikling. Denne strukturerte tilnærmingen sikrer at hver TIBER-test er utformet for å utfordre finansforetakets forsvar så realistisk som mulig, noe som fører til meningsfulle forbedringer for motstandsdyktigheten i nettverks- og informasjonssystemer.

4 Roller og ansvar

Aktivitetene som utføres av de ulike teamene i en TIBER-test er organisert i tråd med testens faser og reflekterer deres roller i planlegging, gjennomføring og oppfølging av trusselbasert penetrasjonstesting. Beskrivelsen belyser hvordan samspillet mellom teamene bidrar til en strukturert og effektiv testgjennomføring, og hvordan de samlede aktivitetene understøtter økt motstandsdyktighet i kritiske funksjoner.

4.1 TIBER Cyber Team (TCT)

TIBER Cyber Team (TCT), i Norge TCT-NO, er et dedikert myndighetsteam med ansvar for å forvalte og sikre korrekt gjennomføring av tester i samsvar med TIBER-rammeverket, slik at resultatene gjensidig kan anerkjennes av relevante myndigheter.

Teamet har ansvar for styring og kvalitetssikring av testløpet, herunder godkjenning av omfang og metode, oppfølging av krav og føringer i rammeverket, samt uavhengig vurdering av gjennomføring og resultater. I tillegg støtter teamet foretak som gjennomfører TIBER-NO-testing med planlegging, koordinering av involverte aktører, risikovurdering, gjennomføring av tester og etterfølgende evaluering.

4.2 Control Team (CT)

For hver TIBER-test skal det etableres et Control Team (CT)[1], ledet av en dedikert Control Team Lead (CTL) fra foretaket. CT skal være organisert slik at teamet har nødvendig innsikt i deteksjoner fra Blue Team (BT) og eventuelle tredjepartsleverandører av IKT-tjenester som foretaket benytter.

Det overordnede ansvaret for planlegging og styring av testen ligger hos foretaket. CTL har ansvar for å fastsette og sluttføre testens omfang, inkludert styregodkjenning, definere scenarier og risikostyringstiltak, samt sikre at disse er validert av testleder (TM). Videre koordinerer CTL all testaktivitet, herunder samhandling med leverandør av trusseletterretning (TIP), Red Team-testere (RTT) og relevante myndigheter, og sørger for at leverandørenes prosjektplaner inngår i foretakets samlede planlegging av TIBER-testen.

Gitt CTLs sentrale rolle anbefales det sterkt å utpeke en stedfortreder. Tett samarbeid mellom CTL og TM er en forutsetning i alle testfaser. CT skal på forespørsel gjøre relevant testinformasjon tilgjengelig for TM.

4.3 Red Team Testers (RTT)

Red Team-testere (RTT) har som mål å vurdere foretakets cybermotstandsdyktighet i lys av de truslene foretaket står overfor. RTT planlegger og gjennomfører angrep mot de systemene og tjenestene som er omfattet av det avtalte testomfanget. I gjennomføringen skal RTT benytte ulike og kreative angrepsalternativer i de ulike fasene av testen, basert på taktikker, teknikker og prosedyrer (TTP-er) som benyttes av avanserte trusselaktører, for å håndtere endrede forutsetninger eller manglende effekt av enkelte angrepsmetoder. RTT dokumenterer funn og observasjoner fra testen i en Red Team Test Report (RTTR).

RTT skal følge en grundig, strukturert og etisk metodikk for trusselbasert penetrasjonstesting, og oppfylle minimumskravene fastsatt i TIBER-rammeverket. Regler for engasjement og spesifikke testkrav skal fastsettes i samarbeid mellom RTT og foretaket.

4.3.1 Simulerte angrep

I en TIBER-test gjennomfører Red Team-testerne en rekke målrettede angrep som simulerer handlingene til trusselaktører i den virkelige verden. Disse testene er designet basert på informasjonen som er gitt om sannsynlige trusler og er skreddersydd for å utfordre foretakets kritiske funksjoner og defensive evner. Målet er å avdekke sårbarheter og teste effektiviteten til foretakets deteksjons- og responsmekanismer. Her er noen typiske tester som kan være inkludert i en TIBER-test:

1. **Phishing og spear-phishing-angrep**: Disse testene innebærer å sende villedende e-poster til ansatte for å lure dem til å avsløre sensitiv informasjon, klikke på skadelige lenker eller laste ned infiserte vedlegg. Spear-phishing er mer målrettet, rettet mot spesifikke individer eller grupper i foretaket.
2. **Sosial manipulering**: Utover phishing kan sosial manipuleringstest innebære vishing (voice phishing), lokking eller påskudd, der angripere manipulerer enkeltpersoner til å bryte sikkerhetsprosedyrer. Disse testene evaluerer ansattes bevissthet og effektiviteten av sikkerhetsopplæring.

[1] Control Team er omtalt som White Team i tidligere TIBER-EU-versjoner.

3. **Penetrasjonstesting av nettverk og applikasjoner**: Dette innebærer systematiske forsøk på å bryte de ulike lagene av forsvar ved å bruke verktøy og teknikker som er tilgjengelige for trusselaktør. Det inkluderer forsøk på å utnytte kjente sårbarheter i programvare og maskinvare som ikke er riktig oppdatering eller konfigurert.
4. **Advanced Persistent Threat (APT)-simulering**: Denne testen simulerer et vedvarende angrep der en uautorisert bruker får tilgang til et nettverk og forblir uoppdaget i en lengre periode for å stjele sensitive data. Den tester foretakets evne til å oppdage og reagere på skjulte, kontinuerlige hacking-prosesser.
5. **Fysiske sikkerhetsbrudd**: Tester kan omfatte forsøk på å få uautorisert adgang til sikre steder gjennom "tailgating", låsdirking eller andre midler. Dette aspektet kontrollerer de fysiske sikkerhetstiltakene og ansattes årvåkenhet.
6. **Simulering av forsyningskjedeangrep**: Dette innebærer testing av sårbarheter som kan oppstå fra tredjepartsleverandører eller programvareleverandører. Testen kan simulere scenarier der angripere kompromitterer en leverandørs systemer for å få tilgang til foretakets nettverk.
7. **Denial of Service (DoS) og distribuert Denial of Service (DDoS)-tester**: Disse testene sjekker hvor godt foretaket kan håndtere massive økninger i trafikk designet for å overvelde systemer og forstyrre tjenester.
8. **Dataeksfiltrering**: Denne typen tester innebærer simulering av uautorisert overføring av data utenfor foretaket for å teste både evnen til å oppdage og respondere på datainnbrudd.
9. **Insider-trusselsimulering**: Simulere handlinger fra ondsinnede innsidere for å se hvor godt foretaket kan oppdage og redusere trusler innenfra, inkludert feil tilgang til sensitiv informasjon og sabotasje.

Hver av disse testene utføres i et kontrollert miljø der hovedmålet ikke bare er å finne sårbarheter, men også å se hvor godt foretaket kan oppdage, respondere og komme seg etter angrepene. Resultatene gir verdifull innsikt i områder der foretaket trenger å styrke sitt forsvar.

4.4 Blue Team (BT)

For hver TIBER-test omfatter Blue Team (BT) alle ansatte i foretaket, relevante tredjepartsleverandører og andre aktører innenfor testens omfang som ikke inngår i Control Team (CT) og som ikke er kjent med at testen gjennomføres. BT har ansvar for å beskytte foretakets bruk av nettverks- og informasjonssystemer ved å opprettholde et forsvarlig sikkerhetsnivå mot simulerte eller reelle angrep.

Det er avgjørende at BT holdes fullstendig adskilt fra forberedelse og gjennomføring av TIBER-testen. I avslutningsfasen, når BT informeres om testen, bør relevante og egnede medlemmer av BT delta i Replay-, Purple Teaming- og utbedringsaktiviteter, inkludert tilhørende oppfølging, for å sikre læring og forbedring av sikkerhetsnivået.

4.5 Threat Intelligence Provider (TIP)

Leverandør av trusseletterretning skal levere trusseletterretning til foretaket i form av en målrettet trusseletterretningsrapport (Targeted Threat Intelligence Report – TTIR), som ved behov kan videreutvikles og berikes av Red Team-testerne (RTT). TIP skal benytte flere etterretningskilder for å sikre at vurderingene er mest mulig presise, relevante og oppdaterte. Trusseletterretningsrapporten beskriver trusselscenarier som, i samarbeid med RTT, videreutvikles til konkrete angrepsscenarier.

TIP skal samarbeide tett med RTT gjennom resten av TIBER-testen, herunder bidra til utvikling av angrepsscenarier for red team-testen og håndtere eventuelle nye etterretningsbehov som oppstår underveis i testforløpet. TIP forventes også å bidra med innspill til den endelige Red Team Test Report (RTTR) som utarbeides og oversendes foretaket.

4.5.1 Kilder til trusseletterretning

Trusseletterretningsleverandører (TIP) samler detaljert og relevant trusseletterretning om potensielle trusselaktører fra en rekke kilder. Disse kildene gir omfattende innsikt i taktikkene, teknikkene og prosedyrene (TTP-er) som brukes av trusselaktørene. Her er noen vanlige kilder for trusseletterretning:

1. **Open-Source etterretningskilder (OSINT)**:
   - **Beskrivelse**: Informasjon samlet inn fra offentlig tilgjengelige kilder.
   - **Eksempler**: Nyhetsnettsteder, blogger, sosiale medier, fora, offentlige rapporter og datalager.
   - **Fordeler**: Gir en bred oversikt over nye trusler og generelt trussellandskap.
2. **Lukket kildeinformasjon**:
   - **Beskrivelse**: Informasjon hentet fra proprietære eller begrensede kilder.
   - **Eksempler**: Abonnementsbaserte trusseletterretningsplattformer, private fora og grupper for deling av trusseletterretning.
   - **Fordeler**: Inkluderer ofte mer detaljert og spesifikk etterretning som ikke er tilgjengelig i offentlige kilder.
3. **Menneskelig etterretning (HUMINT)**:
   - **Beskrivelse**: Informasjon samlet inn gjennom direkte menneskelig interaksjon.
   - **Eksempler**: Innsideinformasjon, ekspertintervjuer og hemmelige operasjoner.
   - **Fordeler**: Kan gi dyp innsikt i trusselaktørers motiver og evner som ikke kan erverves fra digitale kilder alene.
4. **Teknisk etterretning (TECHINT)**:
   - **Beskrivelse**: Informasjon hentet fra teknisk analyse av data.
   - **Eksempler**: Malwareanalyse, nettverkstrafikkanalyse og elektroniske bevis.
   - **Fordeler**: Tilbyr presise detaljer om verktøy, metoder og sårbarheter utnyttet av trusselaktører.
5. **Feeds for Cyber Threat Intelligence (CTI)**:
   - **Beskrivelse**: Sanntidsdatastrømmer som gir informasjon om aktuelle cybertrusler.
   - **Eksempler**: Indikatorer for kompromittering (IOC), trusselaktørprofiler og angrepsmønstre.
   - **Fordeler**: Gir mulighet for raske oppdateringer og rettidig respons på nye trusler.
6. **Fellesskap for deling av trusselinformasjon**:
   - **Beskrivelse**: Samarbeidsgrupper som deler trusseletterretning blant medlemmene.
   - **Eksempler**: Informasjonsdelings- og analysesentre (ISAC), bransjespesifikke trusseletterretningsgrupper og regjeringsledede initiativer.
   - **Fordeler**: Forenkler deling av verdifull, sektorspesifikk trusseletterretning og beste praksis.
7. **Dark Web Intelligence**:
   - **Beskrivelse**: Informasjon samlet fra skjulte deler av internett.

- **Eksempler**: Dark web-markedsplasser, hackerfora og krypterte kommunikasjonskanaler.
- **Fordeler**: Gir tidlige advarselstegn på planlagte angrep eller datainnbrudd.

8. **Hendelsesrapporter og historiske data**:
   - **Beskrivelse**: Analyse av tidligere hendelser og sikkerhetsbrudd.
   - **Eksempler**: Rapporter etter hendelsen, sikkerhetsbrudddatabaser og historiske angrepsmønstre.
   - **Fordeler**: Hjelper med å forstå tilbakevendende trusler og forberede seg på lignende fremtidige angrep.
9. **Kommersielle trusseletterretningstjenester**:
   - **Beskrivelse**: Tjenester levert av spesialiserte selskaper.
   - **Eksempler**: FireEye, CrowdStrike, Recorded Future og andre cybersikkerhetsfirmaer.
   - **Fordeler**: Gir strukturert, verifisert og kontekstualisert trusseletterretning basert på observasjoner av trusselaktører, TTP-er og kampanjer, med støtte for både operativ deteksjon og strategisk risikovurdering.
10. **Interne sikkerhetsdata**:
    - **Beskrivelse**: Informasjon samlet inn fra organisasjonens egne systemer og nettverk.
    - **Eksempler**: Logger fra inntrengningsdeteksjonssystemer (IDS), sikkerhetsinformasjons- og hendelsesstyringssystemer (SIEM) og hendelsesresponsrapporter.
    - **Fordeler**: Tilbyr spesifikk innsikt i trusler som direkte påvirker foretaket.

4.5.2 Trusselaktører

For TIBER-tester bidrar en systematisk vurdering av relevante trusselaktører til å sikre at organisasjonen er forberedt ikke bare på de mest sofistikerte og sannsynlige truslene, som statsstøttede aktører og organisert kriminalitet, men også på mindre forutsigbare og opportunistiske angrep som kan utnytte uforutsette sårbarheter. En slik helhetlig tilnærming til trusselmodellering er avgjørende for å utvikle robust motstandsdyktighet i nettverks- og informasjonssystemer.

Den årlige CTL-rapporten fra NFCERT viser at det nordiske trussellandskapet omfatter et bredt spekter av trusselaktører og trusselkategorier. For finanssektoren utgjør særlig organisert kriminalitet (OCG), nasjonale aktører, ondsinnede innsidere, hackere og hacktivister de mest sentrale truslene. I tillegg finnes det andre typer trusselaktører som, selv om de ikke nødvendigvis er like relevante for finanssektoren, likevel kan være nyttige å ha kjennskap til i et helhetlig risikoperspektiv.

Nedenfor beskrives de ulike trusselaktørene nærmere.

1. **Statlige aktører**: Disse aktørene er statlige enheter som opererer direkte under myndighetenes kontroll og instruksjon og utfører cyberoperasjoner for å oppfylle nasjonale sikkerhetsmål, økonomiske fordeler eller for å påvirke utenrikspolitikken. Deres aktiviteter er godt koordinert og finansiert, ofte rettet mot kritisk infrastruktur, finansielle systemer og statlige nettverk. Russland, Kina, Nord-Korea og Iran har over tid, i både nasjonale og internasjonale trusselvurderinger, blitt identifisert som de mest fremtredende statlige trusselaktørene.
   - **Mål**: Å gjennomføre cyberoperasjoner som støtter nasjonale sikkerhetsmål og geopolitiske mål.

- Motivasjon: Politiske, økonomiske eller militære fordeler fremfor andre nasjoner eller enheter.
- **Kapabilitet**: Svært høy; tilgang til avanserte verktøy og teknikker utviklet eller anskaffet gjennom betydelige statlige ressurser.
- **Kapasitet**: Høy; i stand til å opprettholde langsiktige, komplekse cyberoperasjoner globalt.
- **Relevans for TIBER**: Disse aktørene representerer et høyt nivå av sofistikering og potensiell innvirkning på grunn av deres evner til å utnytte avanserte sårbarheter og gjennomføre vedvarende kampanjer.

2. **Statsstøttede aktører**: Dette er ikke-formelle aktører som får støtte, beskyttelse eller oppdrag fra en stat, men uten å være en offisiell del av statsapparatet. De kan inkludere private grupper, enkeltpersoner eller selskaper som har inngått kontrakt med eller er støttet av myndighetene for å drive med nettspionasje, sabotasje eller forstyrrelser. Disse aktørene forfølger typisk mål i samsvar med nasjonale interesser og er utstyrt med betydelige ressurser og avanserte verktøy. Når de opptrer som stedfortredere, lar statsstøttede aktører nasjonalstater utvide sin rekkevidde og utføre cyberoperasjoner indirekte. Dette kan gi plausibel benektelse, da den direkte koblingen mellom cyberaktiviteten og myndighetene kan være tilslørt eller skjult. Eksempler på statsstøttede trusselaktører som reflekterer avanserte, vedvarende og målrettede angrep mot kritiske funksjoner er russiske APT29/28, Turla, kinesiske APT10/41/40, nordkoreanske Lazarus/APT38 og iranske APT35, APT34, MuddyWater, APT33.
   - **Mål**: Å utføre cyberaktiviteter på vegne av sin sponsornasjon, rettet mot utenlandske myndigheter, kritisk infrastruktur, selskaper eller dissidenter.
   - **Motivasjon**: Å utvide sponsorens politiske, økonomiske og militære rekkevidde.
   - **Kapabilitet**: Høy; ofte lik nasjonalstatsaktører, ved å bruke sofistikerte cyberverktøy.
   - **Kapasitet**: Høy; støttet av nasjonalstater, kan de delta i omfattende, ressurskrevende cyberoperasjoner.
   - **Relevans for TIBER**: Trusselen fra statsstøttede aktører er kritisk på grunn av deres støtte fra nasjonalstater, noe som kan gjøre attribusjon og forsvar utfordrende.
3. **Organiserte kriminelle grupper**: Disse aktørene engasjerer seg i nettkriminalitet for økonomisk vinning. De er involvert i et bredt spekter av ondsinnede aktiviteter inkludert, men ikke begrenset til datainnbrudd, økonomisk svindel, løsepenge-angrep og identitetstyveri. Eksempler på slike grupper er FIN7, LockBit, REvil (Sodinokibi), Conti, DarkSide og Evil Corp, som alle er kjent for økonomisk motivert nettkriminalitet og høy evne til rask teknologisk og operasjonell tilpasning.
   - **Mål**: Økonomisk gevinst gjennom ulike former for nettkriminalitet, inkludert løsepengevare, datatyveri, økonomisk svindel og utpressing.
   - **Motivasjon**: Profittorientert, utnytter cyberevner for økonomiske fordeler.
   - **Kapabilitet**: Middels til høy; har ferdigheter og verktøy for å utføre storskala nettkriminelle aktiviteter.
   - **Kapasitet**: Middels til høy; opererer ofte som bedrifter for å maksimere profitt, med fokus på å skalere driften effektivt.

- **Relevans for TIBER**: Det er viktig å vurdere trusselen fra disse gruppene, siden de ofte retter seg mot finansielle institusjoner for å maksimere inntjeningen.

4. **Hacktivister**: Hacktivister er motivert av politiske eller sosiale agendaer og bruker cyberangrep for å trekke oppmerksomhet til saken sin, protestere mot organisasjoner eller gjennomføre hevnaksjoner. Eksempler på slike grupper er Anonymous, LulzSec, Killnet, GhostSec og CyberBerkut, som benytter politisk eller ideologisk motiverte cyberangrep som tjenestenekt, nettstedødeleggelse og informasjonslekkasjer for å skape oppmerksomhet og påvirkning.
   - **Mål**: Å fremme politisk eller sosial endring gjennom forstyrrelser, datalekkasjer eller offentlig eksponering av spesifikke organisasjoner.
   - **Motivasjon**: Drevet av ideologiske overbevisninger eller spørsmål om sosial rettferdighet.
   - **Kapabilitet**: Lav til middels; evner kan variere mye mellom grupper eller enkeltpersoner.
   - **Kapasitet**: Lav til middels; begrensede ressurser, men sikter ofte mot synlige mål med høy effekt for å forsterke budskapet deres.
   - **Relevans for TIBER**: Selv om deres tekniske evner kan variere mye, må uforutsigbarheten og potensialet for skade på omdømme vurderes under trusselvurderingen.
5. **Terroristgrupper**: Disse aktørene bruker cybermidler for å fremme terror, destabilisere regjeringer eller tvinge enkeltpersoner eller myndigheter. Eksempler på slike grupper er Islamic State (IS / ISIS), Al-Qaeda, Hamas, Hezbollah og Hayat Tahrir al-Sham (HTS), som benytter cybermidler til propaganda, påvirkning, forstyrrelse og i enkelte tilfeller forsøk på cyberstøttede eller cyberfysiske angrep for å fremme terrorrelaterte mål.
   - **Mål**: Å skape frykt, tvinge regjeringer eller sosialt manipulere grupper for politiske eller religiøse årsaker.
   - **Motivasjon**: Ideologisk, søker å fremme sine politiske, religiøse eller sosiale mål.
   - **Kapabilitet**: Generelt lav til middels; cyberoperasjoner er mindre sofistikerte sammenlignet med statlige aktører.
   - **Kapasitet**: Lav til middels; cyberevner dukker opp blant terrorgrupper, men er fortsatt mindre utviklet enn andre aspekter av deres operasjoner.
   - **Relevans** for TIBER: Selv om de generelt er mindre sofistikert teknologisk, utgjør utviklingen av cyberevner blant terrorgrupper en økende bekymring i TIBER-sammenheng, spesielt for sektorer som energi, transport og offentlig sikkerhet.
6. **Spenningssøkere**: Ofte amatørhackere eller yngre individer. Drevet av ønsket om anerkjennelse, spenning eller utfordring, kan spenningssøkere engasjere seg i hacking på lavt nivå som forfalskning av nettsider, enkle tjenestenektangrep eller uautorisert systemtilgang.
   - **Mål**: Å bryte seg inn i systemer eller skape forstyrrelser for utfordringen, spenningen eller å bevise sine ferdigheter.
   - **Motivasjon**: Personlig tilfredsstillelse, nysgjerrighet eller spenningen ved å hacke seg inn i sikre nettverk.
   - **Kapabilitet**: Lav til middels; ofte selvlært og opportunistisk.
   - **Kapasitet**: Lav; aktiviteter har en tendens til å være sporadiske og ikke en del av en vedvarende kampanje.

- **Relevans for TIBER**: Selv om deres innvirkning kan være lavere sammenlignet med andre kategorier, kan deres uforutsigbare natur utgjøre unike risikoer, spesielt for mindre sikre systemer.

7. **Script Kiddies**: Dette er amatør-cyberangripere som mangler tekniske ferdigheter og ofte er avhengige av forhåndsskrevne skript, verktøy eller programvare utviklet av andre for å utføre angrep. De er typisk preget av deres minimale forståelse av de underliggende prinsippene eller konsekvensene av angrepene de utfører.
   - **Mål**: Å bryte seg inn i systemer eller nettverk, ofte for nysgjerrighetens skyld eller for å skryte av sine evner overfor jevnaldrende.
   - **Motivasjon**: Å få anerkjennelse og rykte blant sine jevnaldrende, drevet av et ønske om oppmerksomhet.
   - **Kapabilitet**: Lav; stoler på eksisterende verktøy, skript og metoder utviklet av andre.
   - **Kapasitet**: Lav; deres lavere ferdighetsnivåer og avhengighet av offentlig tilgjengelige verktøy.
   - **Relevans for TIBER**: Trusselen fra Script Kiddies anses vanligvis som lavere risiko. Imidlertid kan de fortsatt forårsake forstyrrelser eller avsløre sårbarheter i en organisasjons systemer, spesielt hvis disse systemene ikke er ordentlig sikret mot vanlige utnyttelser.
8. **Insidere**: Disse kan være nåværende eller tidligere ansatte, kontraktører eller forretningspartnere som har eller har hatt autorisert tilgang til organisasjonens systemer. Innsidere kan utføre ondsinnede aktiviteter på grunn av misnøye, økonomiske insentiver eller tvang fra eksterne aktører.
   - **Mål**: Å utnytte deres tilgang til sensitiv informasjon eller systemer for personlig vinning, for å forårsake skade eller på grunn av tvang.
   - **Motivasjon**: Økonomisk vinning, hevn mot sin arbeidsgiver, tvang fra eksterne parter, eller ideologiske grunner.
   - **Kapabilitet**: Høy når det gjelder tilgang; innsidere kan utnytte sin legitime tilgang til systemer og data, og omgå mange eksterne sikkerhetstiltak.
   - **Kapasitet**: Varierer; virkningen og omfanget av handlinger avhenger av innsiderens posisjon og tilgangsnivå.
   - **Relevans for TIBER**: Innsidetrusler er svært betydelige på grunn av deres tilgang til og kunnskap om interne prosesser, noe som kan føre til betydelig skade eller datainnbrudd.

5 Oppsummering og konklusjon

Denne white paperen har gitt en gjennomgang av TIBER-NO og TIBER-engasjementer, med vekt på formål, struktur og roller i testløpet. TIBER er utformet for å styrke motstandsdyktigheten i finansielle institusjoners nettverks- og informasjonssystemer gjennom realistisk simulering av avanserte cyberangrep basert på trusseletterretning fra den virkelige verden. Prosessen er strukturert i tydelige faser – fra forberedelse og etterretningsinnhenting, via testing og rapportering, til oppfølging og forbedringstiltak.

TIBER-engasjementer utgjør et sentralt og effektivt virkemiddel for å proaktivt forbedre foretakenes evne til å forebygge, avdekke og håndtere sofistikerte cybertrusler. Bruken av realistiske

angrepsscenarier og uavhengige tredjepartsleverandører gir en helhetlig og troverdig vurdering av både tekniske, prosessuelle og menneskelige sikkerhetsmekanismer. Samspillet mellom Red Team, Blue Team, Threat Intelligence Provider og Control Team sikrer en kontrollert, konsistent og kvalitetssikret gjennomføring.

Erfaringene og innsikten som oppnås gjennom TIBER-engasjementer er avgjørende for å identifisere sårbarheter, styrke deteksjons- og responskapasiteter og forbedre den samlede sikkerhetsmodenheten. I et trusselbilde i kontinuerlig utvikling bør regelmessig TIBER-testing inngå som en integrert del av en robust og langsiktig cybersikkerhetsstrategi, og bidra til at finansielle foretak står bedre rustet til å håndtere og begrense konsekvensene av fremtidige cyberangrep.

6 Referanser

- TIBER-EU: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html
- TIBER-NO: https://www.norges-bank.no/tema/finansiell-stabilitet/Forebygging/tiber/
- Lovdata - DORA-loven: https://lovdata.no/dokument/NL/lov/2025-05-27-18
- Lovdata - DORA-forskriften: https://lovdata.no/dokument/SF/forskrift/2025-06-24-1296
- Lovdata - Delegert kommisjonsforordning (EU) 2025/1190: https://lovdata.no/static/NLX3/32025r1190.pdf
- Nordic Financial CERT: https://www.nfcert.org/