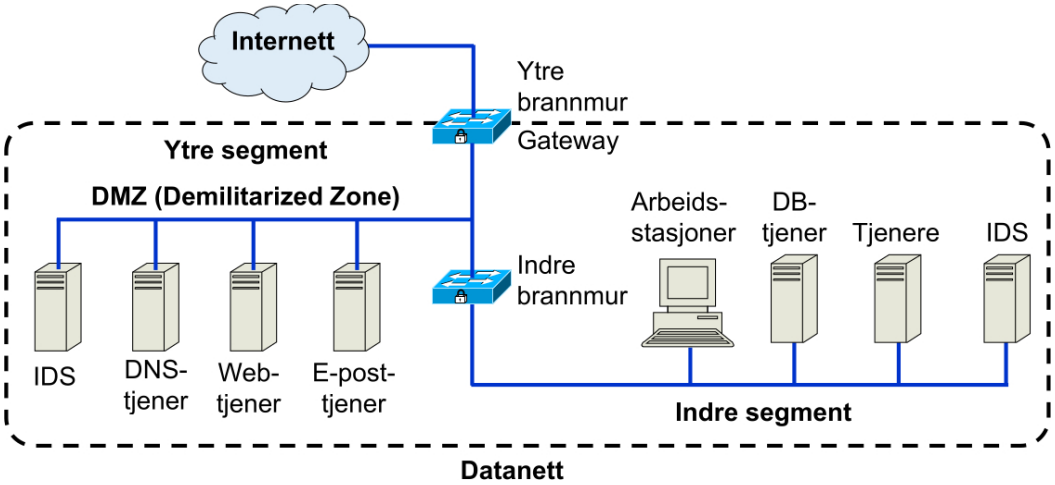
Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2023
Teoretiske oppgaver

T9 (Del 10): Datanettsikkerhet og cyberoperasjoner

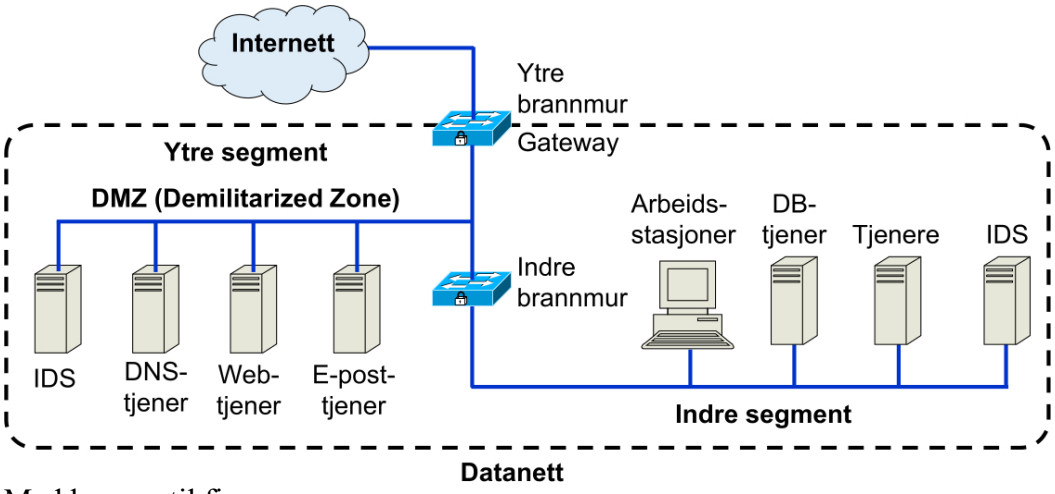
Oppgave 1: Brannmurer



Se på figuren over som viser en enkel nettverksarkitektur med brannmurer.

a) Hva er formålet med DMZ? Hvilke tjenester fins typisk der?
b) På hvilke lag i internettstakken (og OSI-stakken) opererer en brannmur av typen pakkefilter?
c) Hvilken type brannmur kan filtrere trafikk basert på brukerdata i datapakker?

Oppgave 2: Pakkefilter og inntrengingsdeteksjon



Med hensyn til figuren over.

a) Hva er en typisk sikker konfigurasjon (filterregler) for brannmurene?
b) Hvor kan nettverksinntrengingsdeteksjon (NIDS) plasseres?
c) Beskriv konsekvens av å plassere NIDS i de ulike delene
d) Anta at det står en NIDS i det indre segmentet. Anta videre at IP-adressen til webtjeneren er 4.3.2.1 og IP-adressen til DB-tjeneren er 4.3.2.10. På DB-tjeneren kjøres det en SQL tjeneste med port 1444. Skriv en Snort-regel som gir en alarm for TCP-trafikk fra web-tjeneres til denne SQL-tjenesten. Du kan anta at $HOME_NET variablen er satt opp etter ønsket formål.

Oppgave 3: TLS-Inspeksjon

a. Beskriv legitime grunner for å benytte TLS-inspeksjon.
b. Beskriv trusselscenarioer for misbruk av TLS-inspeksjon.
c. Hvordan kan en bruker finne ut om TLS-inspeksjon brukes i en HTTPS nettforbindelse?

Oppgave 4: Offensive og defensive cyberoperasjoner

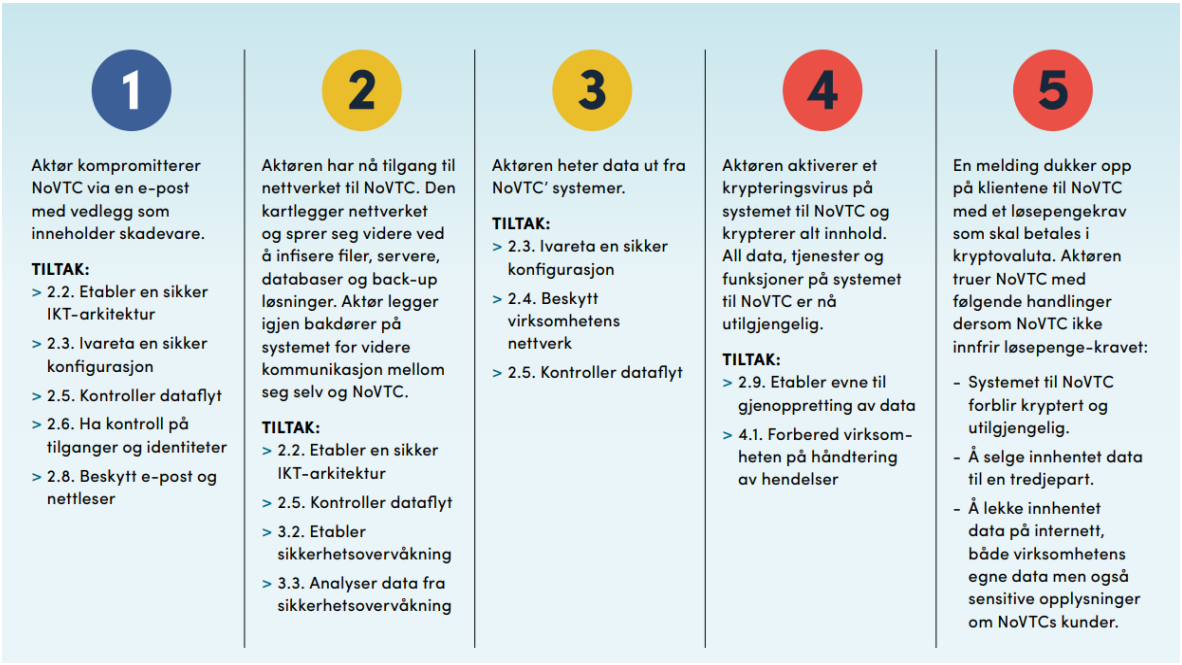
Gi et eksempel på en offensiv cyberoperasjon og et eksempel på en defensiv cyberoperasjon fra en virkelig hendelse.

Oppgave 5: NSMs rapport om nasjonalt digitalt risikobilde 2021

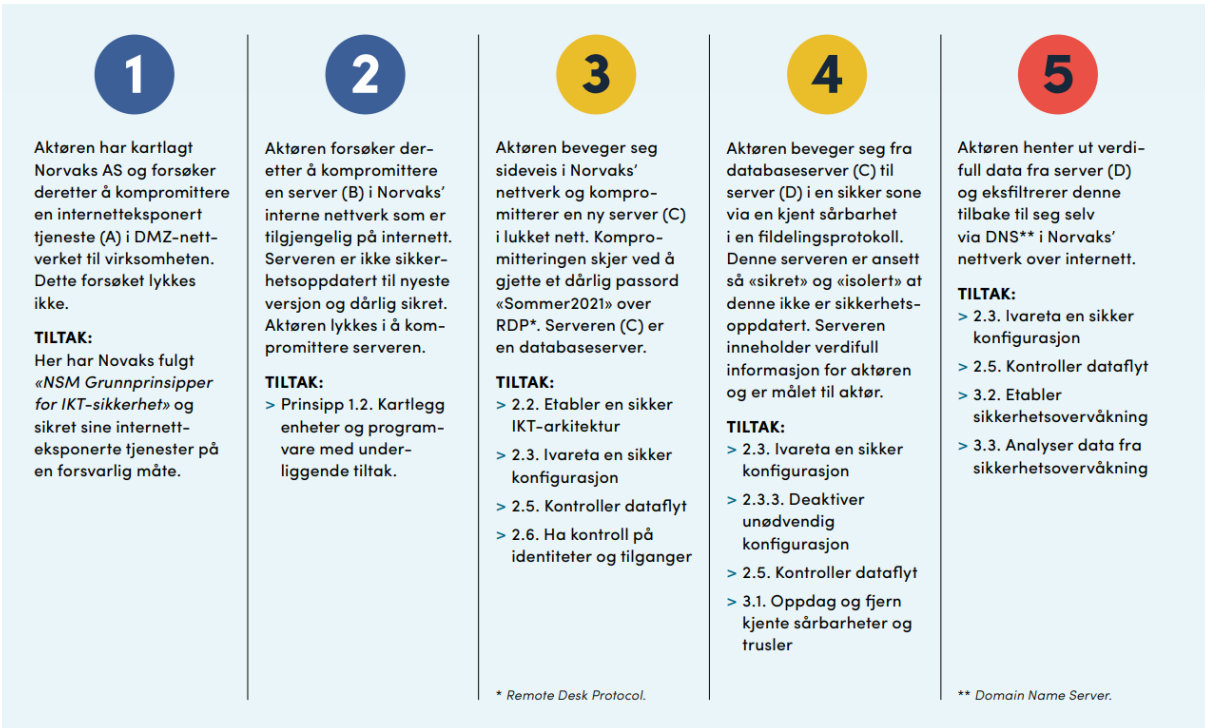
I NSMs rapport «Nasjonalt digitalt risikobilde 2021»
[https://nsm.no/aktuelt/nasjonalt-digitalt-risikobilde-2021]
er to cyberoperasjoner mot norske mål beskrevet. De er

a) Mot bedriften Norske VTC-tjenester
b) Mot bedriften Norsk Vaksine AS

Gå gjennom stegene beskrevet der, og kartlegg dem mot stegene i Cyber Kill Chain og argumenter for løsningen. Disse stegene er gjengitt i figur 1 og figur 2 nedenfor for oppgave a og b respektivt. Merk at det ikke nødvendigvis er en 1:1 relasjon mellom stegene i rapporten og stegene i Cyber Kill Chain.



Figur 1 – steg i angrep mot Norske VTC-tjenester for oppgave 1a
[Kilde: https://nsm.no/aktuelt/nasjonalt-digitalt-risikobilde-2021]



Figur 2 – steg i angrep mot Norsk Vaksine AS for oppgave 1b
[Kilde: https://nsm.no/aktuelt/nasjonalt-digitalt-risikobilde-2021]

Oppgave 6: Trinn i Cyber Kill Chain

Et angrep mot en virksomhet (som for øyeblikket jobbet med et anbud for et oppdrag) skjedde som følger:

i. Angriper fant en ansatt i bedriften og brukte LinkedIn og Facebook for å finne mer detaljer om personen og hva den jobbet med
ii. En (veldig troverdig) SMS med link til en falsk side ble sendt til denne ansatte der den ansatte trodde at linken (som hen logget seg inn på) var for et av bedriftens systemer.
iii. Dette gav angriper brukernavn og passord som den brukte for å logge inn i det faktiske systemet og plantet en skadevare.
iv. Skadevaren søkte gjennom systemet til virksomheten og fant informasjonen om anbudet som den søkte etter. (Personen som hadde blitt angrepet hadde fulle/admin rettigheter på systemene)
v. Rett etter fristen endret skadevare på innholdet i dokumentene for anbudet som medførte at bedriften ikke fikk tilslag. Skadevaren slettet deretter alle spor av angrepet (inkludert seg selv).

Kartlegg hver aktivitet ovenfor til riktig trinn i cyber kill chain. Hvilket KIT-mål ble brutt?