Informasjonssikkerhet: Teori og praksis

Audun Jøsang
2. utgave 2023
Universitetsforlaget

Oppgaver

Kapittel 17: Cyberoperasjoner

Oppgave 1: Offensive og defensive cyberoperasjoner

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

Oppgave 2: CTI

a. Hvorfor er deling av CTI viktig?
b. Hva menes med at CTI kan være kortvarig eller langvarig?
c. Hvorfor er det viktig å kunne (del)automatisere CTI?
d. Nevn utfordringer med å (del)automatisere CTI.

Oppgave 3: Cyberoperasjoner og cybervåpen

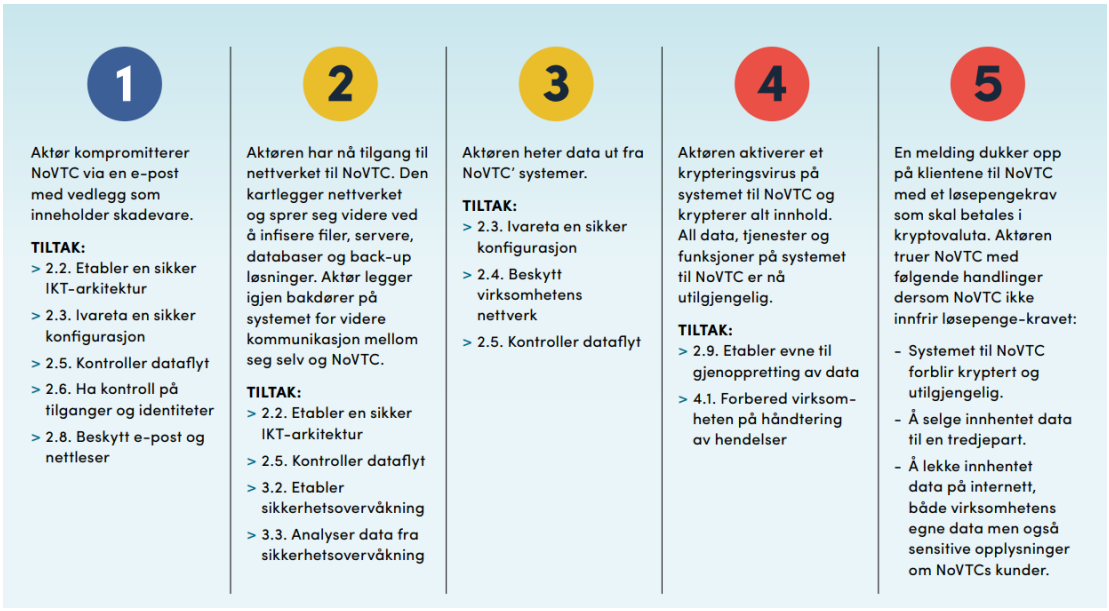
a. Hva er sammenhengen/forskjellen mellom informasjonsoperasjoner og cyberoperasjoner i militær sammenheng?
b. Beskriv nytten av ulike former for militære cyberoperasjoner.
c. Beskriv aspekter og egenskaper ved cybervåpen.
d. Hva er cyberavskrekking, og hvorfor kan det være nyttig?
e. Hvorfor er det vanskelig å få til en internasjonal konvensjon om cyberkrigføring?

Oppgave 4: NSMs rapport om nasjonalt digitalt risikobilde 2021

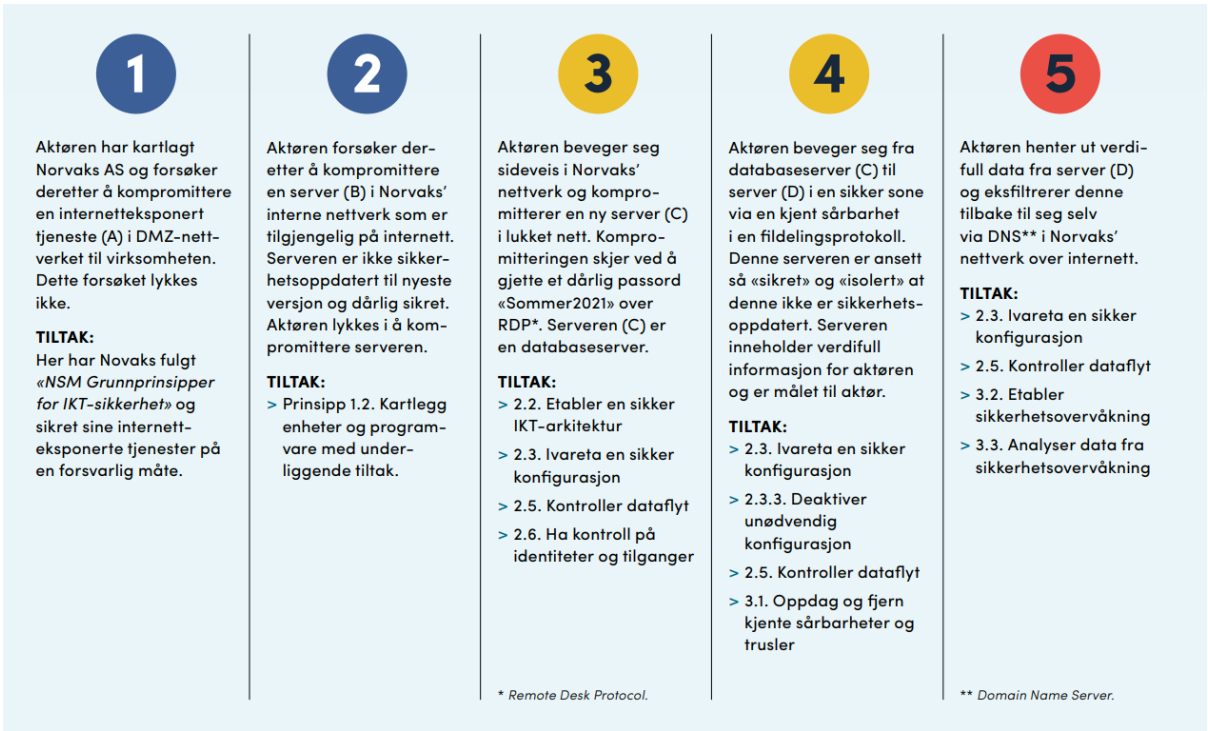
I NSMs rapport «Nasjonalt digitalt risikobilde 2021»
[https://nsm.no/aktuelt/nasjonalt-digitalt-risikobilde-2021]
er to cyberoperasjoner mot norske mål beskrevet. De er

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 5: Cyber Kill Chain og Mitre ATT&CK

Det er både likheter og ulikheter mellom Cyber Kill Chain og taktikkene i Mitre ATT&CK. Dette vil utforskes i denne oppgaven.

Velg deg en APT-gruppe fra gruppene registrert hos Mitre ATT&CK (https://attack.mitre.org/groups), og bruk Mitre ATT&CK til å sette deg inn i de ulike teknikkene og taktikkene denne gruppen har blitt observert å bruke. Her kan du for eksempel bruke ATT&CK Navigator Layers, som ble illustrert i forelesningen.

Bruk dette til å illustrere mulige teknikker fra Mitre ATT&CK for hver av de 7 stegene i Cyber Kill Chain. Dersom du ikke finner observerte teknikker for et gitt steg, kan du finne en du mener er kan være passende eventuelt forklare hvorfor det ikke er aktuelt.

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).

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

Oppgave 7: Info- og cyberoperasjoner

Hva er sammenhengen/forskjellen mellom informasjonsoperasjoner og cyberoperasjoner?

Oppgave 8: Nytte av cyberoperasjoner

Beskriv nytten av ulike former for cyberoperasjoner.

Oppgave 9: Cyberavskrekking

a. Hva er cyberavskrekking og hvorfor kan det være nyttig?
b. Hvilke land praktiserer cyberavskrekking?

Oppgave 10: Cybervåpen

a. Hva er cybervåpen?
b. Nevn viktige aspekter ved cybervåpen.

Oppgave 11: Leveransekjedeangrep

a. Hva er et leveransekjedeangrep?
b. Hvorfor er det typisk en ubalanse mellom en virksomhet og en IT-underleverandør med hensyn til deres nivå for risikoaksept?