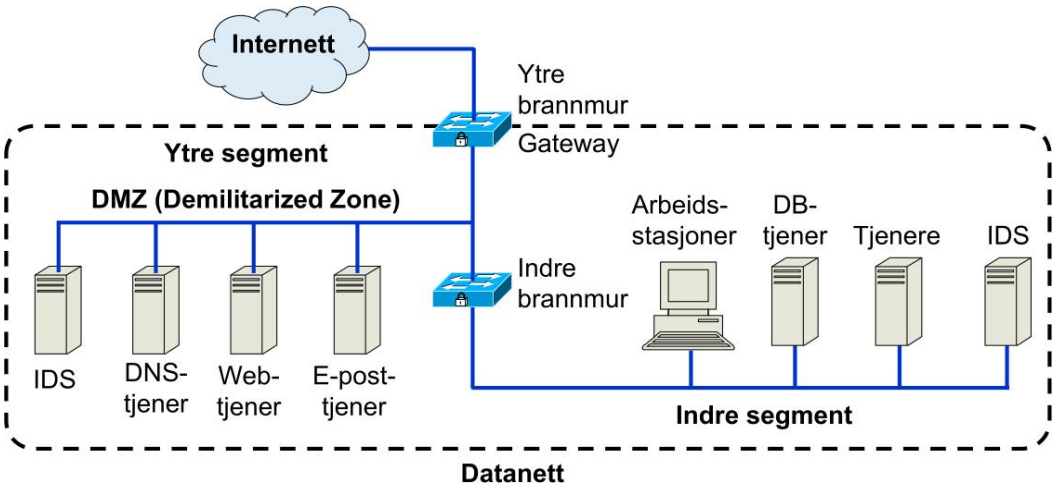
Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2023
Teoretiske oppgaver med løsningsforslag

T9 (Del 10): Datanettsikkerhet og cyberoperasjoner

Oppgave 1: Brannmurer



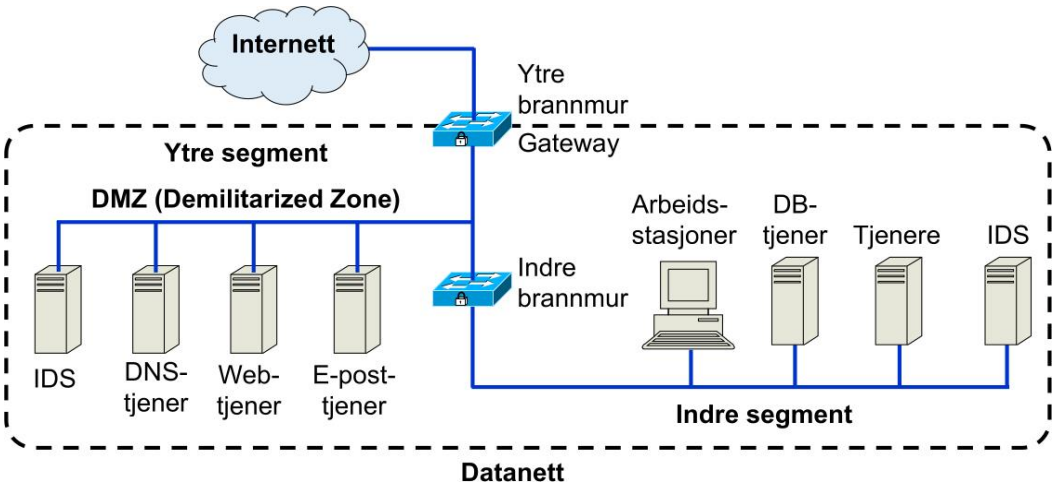
Se på figuren over som viser en enkel nettverksarkitektur med brannmurer.

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

Svarforslag

a) Alle tjenester som skal være tilgjengelige for å motta direkte forespørsler/meldinger fra internett (f.eks. oppslag på nettsider eller mottak av epost), bør plasseres i eget nettverk (DMZ) bak en ytre brannmur som nettopp tillater den type trafikk.
b) Indre brannmurene er konfigurert slik at tilgang fra DMZ videre til indre segmenter er strengt kontrollert med en eller flere indre brannmurer som har mer detaljerte og strengere regler for å kontrollere trafikken. Dette gjør det vanskelig å gjennomføre angrep fra internett via DMZ mot indre segmenter.
c) Pakkefiltre opererer på transportlaget (OSI-lag 4), internettlaget (OSI-lag 3), og delvis på linklaget (OSI-lag 2). Det betyr at regler for filtrering kan baseres på parametere i pakkehodene på disse tre lagene.
d) Applikasjonsbrannmurer kan filtrere trafikk basert på brukerdata. Slike brannmurer kan dermed operere på applikasjonslaget (OSI-lag 7). Det betyr at regler for filtrering kan baseres på brukerdata, i tillegg til parametere fra pakkehoder i de underliggende lagene. Filtrering basert på brukerdata kan gi høy belastning, slik at applikasjonsbrannmurer må ha høy ytelse.

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.

Svarforslag

a) Ekstern brannmur:
   - Utgående forbindelser: tillat alle
   - Innkommende forbindelser: tillat port 80, 443 til webserver, port 53 til DNS-serveren, port 25 (kanskje også 143, 993) til e-postserver; forby alt annet

   Intern brannmur:
   - Utgående forbindelser: tillat alle
   - Innkommende forbindelser: forby alle; kanskje tillat tilkobling fra webserver til DB-server

b) NIDS kan plasseres både i DMZ og i det interne nettverket (og i prinsippet på utsiden av brannmuren)
c) Konsekvens av plassering er hvilken trafikk de ulike NIDS vil se og kan alarmere på. Hvis NIDS plasseres i DMZ vil den ikke se intern trafikk i det indre segment, og (lignende) hvis NIDS plasseres i det indre segment vil den ikke trafikk i det inde segment. Plasseres den på utsiden av ytre brannmur vil den se all trafikk mot virksomheten (også trafikk som stoppes av ytre brannmur), men vil ikke se noe intern trafikk.
d) alert tcp $HOME_NET 4.3.2.1 -> 4.3.2.10 1444 (msg “web til sql trafikk“)

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?

Svarforslag

a. En virksomhet kan vurdere det som en stor trussel at angrep og skadevare kan nå inn til virksomhetens datanett gjennom en kryptert HTTPS-forbindelse. Dette kan gjøre at virksomheten vurderer det som nødvendig å kunne filtrere/inspisere kryptert trafikk ved bruk av TLS-inspeksjon.
b. TLS-inspeksjon er en svært invaderende teknologi som kan dekryptere trafikk på en måte som gjør det vanskelig for brukeren å oppdage. Det er legitimt når en virksomhet informerer ansatte om at TLS-inspeksjon benyttes og hvorfor. Imidlertid kan angripere benytte TLS-inspeksjon uten at brukere forstår at det skjer. Hvis en bruker er koblet til internett gjennom en offentlig wifi kan de som administrerer wifi-nettet gjennomføre TLS-inspeksjon. Nettleseren vil typisk informere brukeren om at den har mottatt et ukjent sertifikat, men mange brukere er kondisjonert til å ikke bry seg om slike advarsler, og godta sertifikatet.
c. Brukeren må vite forskjellen mellom det eksterne PKI-rotsertifikatet og det interne proxy-rotsertifikatet som brukes til å validere det mottatte serversertifikatet. Brukeren kan sjekke sertifiseringsstien/signaturstien fra serversertifikatet til rotsertifikatet. Rotsertifikatet øverst i sertifiseringsstien angir om det mottatte serversertifikatet er ekte eller falskt. Hvis rotsertifikatet er et ekte eksternt PKI-rotsertifikat, er det mottatte serversertifikatet ekte, og den krypterte trafikken er ende-til-ende. Hvis rotsertifikatet er proxy-roten, tilhører det mottatte serversertifikatet proxyen, noe som betyr at trafikken dekrypteres og leses på proxyen. Imidlertid er det teknisk mulig at tilogmed proxy rotsertifikatet er spoofet, og at organisasjonen gir rotsertifikatet et spoofet navn som f.eks. "VeriSign.com". Selv om det unike navnet på rotsertifikatet sier "VeriSign.com" er det ikke nødvendigvis "VeriSign.com". Organisasjonen som drifter proxy-serveren, bestemmer hva de de ulike attributtene til proxy-root-sertifikatet skal være. Hvis brukeren ikke vil stole på noen av attributtene i rotsertifikatet, må hun være i stand til å skille mellom det ekte eksterne rotsertifikatet og proxy-rotsertifikatet basert på den offentlige nøkkelen. En offentlig nøkkel er omtrent 2000 bit lang, som er noen få linjer med HEX-sifre. Siden proxyen kan kopiere alle attributtene fra det ekte eksterne rotsertifikatet til proxy rotsertifikatet, med unntak av den offentlige nøkkelen, kan den offentlige nøkkelen brukes til å bestemme om rotsertifikatet er falsk eller ekte, men det ville kreve at brukeren har en autentisk kopi av den offentlige nøkkelen for det eksterne rotsertifikatet, og sammenligner denne med den offentlige nøkkelen i rotsertifikatet på den interne hosten.

Oppgave 4: Offensive og defensive cyberoperasjoner

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

Løsningsforslag

Cyberoperasjoner involverer typisk en offensiv og en defensiv part. Nedenfor er noen eksempler.

IT-angrepet mot Stortinget i august 2020

- *Offensiv cyberoperasjon.* I august 2020 ble det kjent at Stortinget hadde vært utsatt for et cyberangrep. Antagelig hadde ansatte og stortingsrepresentanter blitt utsatt for phishingangrep, og blitt lurt til å gi fra seg passord for innlogging. Alternativt hadde noen brukere svake passord som ble cracket. Forut for angrepet var det gjort en risikovurdering der det ble anbefalt å innføre 2FA (tofaktor-autentisering). Denne anbefalingen ble ikke fulgt opp, noe som gjorde at hackere med enkle stjålne brukerpassord fikk tilgang til de respektive brukerkontoene. I desember 2020 konkluderte

PST med at angrepet ble utført av cyberaktøren Fancy Bear som knyttes til Russlands militære etterretningstjeneste GRU.

- *Defensiv cyberoperasjon*. Stortinget har ikke beskrevet arbeidet med opprydding etter angrepet. Antagelig ble alle kontoer stengt, strengere passordpolicy ble innført, og ansatte måtte bytte passord før de igjen kunne få tilgang. Samtidig ble 2FA innført. Logger ble antagelig undersøkt for å kartlegge angripernes aktiviteter på kompromitterte kontoer, og for å fjerne skadevare og bakdører som eventuelt hadde blitt installert. Stortinget rapporterte at en begrenset mengde med data hadde blitt lekket og at liten skade var blitt gjort. Stortinget ble ilagt et gebyr på NOK 2 millioner av Datatilsynet for manglende oppfølging av risikovurderingen og brudd på GDPR art. 32 nr.1.b, noe som førte til at Stortingets IT-direktør måtte fratre sin stilling.

Microsoft Exchange-tjener datainnbrudd i 2021

Offensiv cyberoperasjon. I begynnelsen av 2021 ble en sårbarhet i Microsoft Exchange Server utnyttet til å begå datainnbrudd i stor skala globalt. Per 9. mars 2021 ble det anslått at rundt 250 000 Exchange-tjenere hadde blitt kompromittert globalt. I februar/mars 2021 ble Stortinget utsatt for angrep som del av samme angrepsbølge. Angrepet utnyttet en nulldags-sårbarhet som Microsoft først ble klar over etter at de første angrepene ble rapportert, slik at trusselaktører kunne utnytte sårbarheten i perioden frem til alle systemer var blitt patchet. Stortinget hadde ikke mulighet til å patche sin Exchange-tjener raskt nok, slik at de var sårbare da angrepet skjedde. Exchange-tjenere som SaaS i Microsoft sine Azure-installasjoner hadde ikke sårbarheten, og ble derfor ikke angrepet. Stortinget vurderte i utgangspunktet at det var sikrere å selv drifte Exchange on-prem, som ironisk nok gjorde at Stortingets Exchange-tjener var usikker. Microsoft fant ut at angrepet opprinnelig ble utført av Hafnium, en kinesisk statsstøttet APT-hackergruppe (avansert vedvarende trussel).

Defensiv cyberoperasjon. Angrep som utnyttet sårbarheten i Exchange var svært alvorlig. Angripere kunne stjele data og installere skadevare. Den 5. januar 2021 sendte sikkerhetstestselskapet DEVCORE den tidligste kjente rapporten om sårbarheten til Microsoft, som Microsoft bekreftet 8. januar. Det første bruddet på en Microsoft Exchange-tjener ble observert av nettsikkerhetsselskapet Volexity 6. januar 2021. Den 2. mars 2021 informerte Microsoft alle kunder av Exchange om sårbarheten, og oppfordret kundene til å patche Exchange-tjenerene deres. Den 3. mars ble sikkerhetsoppdateringen gjort tilgjengelig, og systemene på Stortinget ble oppdatert samme dag. Imidlertid ble Stortinget antageligvis kompromittert gjennom automatiserte massivt angrep allerede den 2. mars 2021, som kompromitterte tusenvis av Exchange-tjenere i hele verden, og installerte bakdører. Som sagt ble ikke Exchange i Azure-skyen angrepet. Det er mulig at Stortinget ble angrepet enda tidligere enn 2. mars 2021, men i så fall ikke gjennom automatiserte angrep. Den 5. mars fikk Stortinget varsel fra NSM om uvanlig trafikk inn mot Stortingets systemer, og NSM orienterte offentlig om sårbarheten ved Microsoft Exchange. Den 8. mars fikk Stortinget bekreftet at angripere hadde hentet ut data. Det er plausibelt at store menger data og eposter fra Stortinget ble stjålet. Antagelig ble Stortingets Exchange-tjener stengt ned for en periode for å fjerne sårbarheten. Muligens ble også andre IT-funksjoner stengt ned. Det ble gjort undersøkelser for å avdekke om det var installert skadevare og bakdører som ble fjernet. Igjen ble antagelig alle brukere bedt om å endre passord. Stortinget hadde i

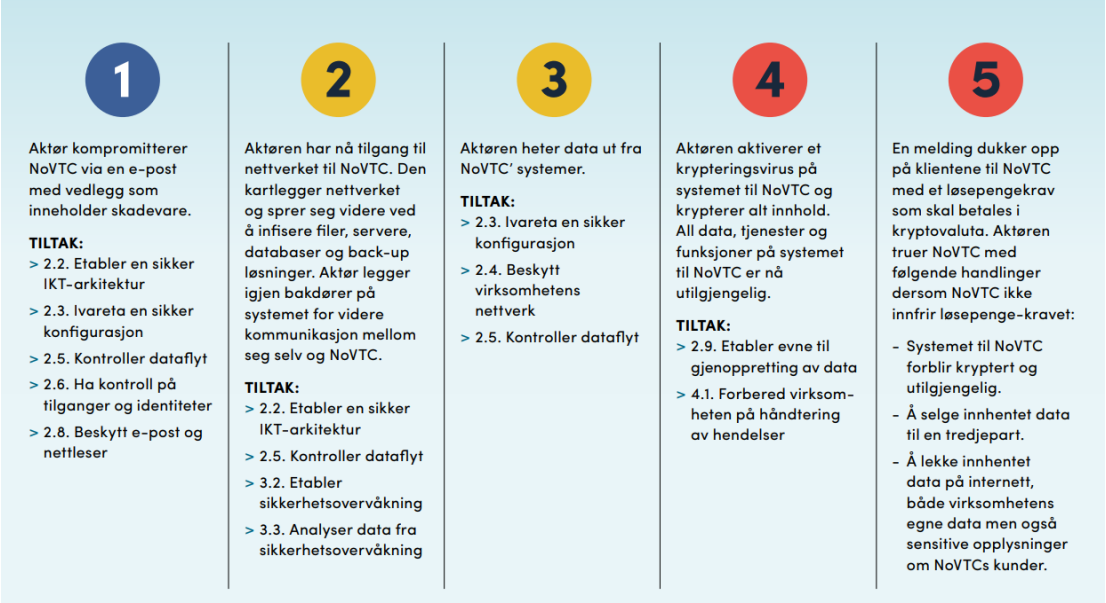
prinsippet gjort det de kunne for å opprettholde god sikkerhet, men ble likevel kompromittert. Om Stortinget fremdeles kjører Exchange on-prem er uvisst for offentligheten, det er en avveining mellom risikoer som en skyløsning medfører, og risikoer som en on-prem-løsning medfører.

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]

Løsningsforslag

Formålet her er å sette seg litt inn i cyber kill chain samtidig som man jobber med en reell hendelse og kan sette seg inn i rapporten til NSM.

Husk at cyber kill chain har følgende steg:

1. Rekognisering
2. Bevæpning
3. Overlevering
4. Utførelse av exploit
5. Innstallering
6. Kommando og kontroll
7. Måloppnåelse

a)

1: Dette tilsvarer (3) overlevering (gjennom epost). Siden det står at den kompromitteres innebærer det også (4) utførelse (og muligens (5) installering).

2: Dette er kommando og kontroll stadiet (6)

3,4,5: Dette er siste stadiet av cyber kill chain (aksjon (7)).

b)

1: Kartlegging innbærer rekognisering (1), og kompromittering vil nok her også innebære at noe må (2) bevæpnes og (3) overleveres, men siden den mislykkes vil nok ikke (4) utførelse blitt gjennomført.

2: Her lykkes det men det er ikke no rekognisering så vil nok innebære 3, 4 og trolig 5 (installing)

3: Dette tilsvarer kommando og kontroll stadiet (6)

4: Dette tilsvarer også kommando og kontroll stadiet (6)

5: Det tilsvarer aksjon (7).

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?

Løsningsforslag

Integritet er i hvert fall brutt (muligens også konfidensialitet hvis informasjon også ble uthentet, men dette var ikke beskrevet i caset). De ulike stegene kan mappes som følger:

i. Dette er rekognosering (trinn1) da info blir samlet om målet
ii. Dette vil være overlevering (trinn 3) og utførelse (trinn 4) av exploit
iii. Installasjon av skadevare (trinn 5)
iv. Kommando og kontroll (trinn 6)
v. Aksjon (trinn 7)