Sikt

Øvelse Morris 2022

Tor Gjerde
Cybersikkerhetssenter for forskning og utdanning (eduCSC)
Sikt – Kunnskapssektorens tjenesteleverandør

Sikt

Om meg

- Opprinnelig utdannet som fysiker, men har jobbet i det som nå er Sikt siden forrige årtusen
- Delt rolle mellom **operativt sikkerhetsarbeid i CERT-funksjonen** og **proaktivt arbeid innenfor informasjonssikkerhet**

På informasjonssikkerhetsområde har fokuset vært:

- veiledning i innføring og videreutvikling av **ledelsessystem** for informasjonssikkerhet
- fasilitering av og kursing i **risikovurderinger**
- bistand til å arrangere **sikkerhetsøvelser**

Sikt

Sikts øvelsesteam

Etter å ha styrket cybersikkerhetssenteret med flere nyansatte hadde vi i 2021 tre personer med sterk interesse for øvelser, men med ganske ulik innfallsvinkel:

- Jeg har lenge jobbet med etablering og videreutvikling av ledelsessystem for informasjonssikkerhet i akademisk sektor, hvor øvelser ofte har fokusert på avdekke mangler i rutiner og beredskap; **Øyvind Eilertsen** har lignende bakgrunn men var ikke med å arrangere Øvelse Morris 2022

- **Made Ziius** kom fra kommersielle internasjonale selskaper som jobbet med økonomi og helsedata, og var vant med øvelser som skulle avdekke om strenge retningslinjer ble korrekt etterfulgt

- **Ingrid Moen** har bakgrunn fra politi og heimevern, hvor øvelser i større grad handler om å gjøre personell mer rutinert i å utøve tjenesten i en «varm» situasjon

Forskjellen skyldes i stor grad fagområdenes modenhet, men alle ytterpunktene kan være verdifulle satt i riktig kontekst. Imidlertid vurderte vi det slik at virksomhetene i vår sektor trenger å komme seg opp på et høyere modenhetsnivå, og at vi ved øvelsesdesign burde fokusere på de områdene hvor det foreligger rutiner, og at evalueringen burde dekke både om disse ble fulgt og om de var formålstjenlige.

Etter å ha arrangert noen øvelser for enkeltkunder så vi at ressursbruken per øvelse gjorde at vi ikke hadde kapasitet til å dekke sektorens ønske om bistand til øvelsesarrangering på denne måten. Vi inngikk derfor et samarbeid med Norwegian Cyber Range ved NTNU Gjøvik om å arrangere en felles «sektorøvelse» for et tverrsnitt av virksomhetene i vår sektor, og fikk med 17 virksomheter av varierende størrelse.

Øvelsen fikk navnet «Øvelse Morris» etter en hendelse i 1988 som regnes som det første skadevareangrepet på internett, og som var årsaken til at man begynte å jobbe systematisk med nettsikkerhet.

Sikt

NTNU

ØVELSE MORRIS 2022

Sikt

Sentrale valg for utformingen av øvelsen

- Riggen til NCR bygger en teknisk spillverden med simulerte tjenester og dataflyt. Dette gjorde det naturlig å gjøre **operativt teknisk personell** til de sentrale aktørene på deltakersiden. Dette passer også med at vi gjennom de senere årene har fått opprettet hendelseshåndteringsteam (IRTer) hos mange av kundene våre, og gjerne vil bidra til å styrke disse.

- Siden en fellesøvelse gir en unik mulighet til å **samarbeide på tvers av virksomhetene** var det åpenbart at vi burde vektlegge dette.

- Et av de viktigste verktøyene til cybersikkerhetssenteret er en **spesielt sikret chat-løsning** for IRTene i sektoren. Vi har allerede tatt ut store gevinster fra denne, men ikke alle virksomhetene er like aktive der. I lys av de foregående punktene var det viktig for oss å inkludere en kopi av dette systemet i øvelsen.

Sikt

Etablering av hovedmål

- Anbefalt beste praksis er å definere overordnede mål for øvelsen tidlig i planleggingsprosessen, og i lys av det foregående ble hovedmål 1 **IRT skal øve på samhandling på tvers av virksomheter i sektoren** og hovedmål 2 **IRT skal øve på analyseferdigheter og responsferdigheter**.

- For å imøtekomme sektorens ønske om å involvere også andre enn IRT var det naturlig å understøtte dette med hovedmål 3 **Virksomheten skal øve på intern kommunikasjon under en sikkerhetshendelse**.

- Å sette hovedmål tidlig og å bevisst bruke disse som retningsgivende i hele prosessen viste seg å være nyttig i alle senere steg, inkludert scenarioutvikling, gjennomføring og evaluering.

Sikt

Men hva skal vi øve på?

For å finne et relevant, interessant og realistisk scenario tok vi utgangspunkt i de ulike **offentlige trusselrapportene**, og kombinerte disse med observasjoner og erfaringer fra vårt **eget løpende sikkerhetsarbeid** i rollen som sektorvist responsmiljø (sektor-CERT) for forskning og høyere utdanning.

Valget vi tok ble også farget av at planprosessen startet samtidig med Russlands fullskalainvasjon av Ukraina. For å kunne ta opp tematikk herfra uten å blande øvelse og virkelighet for tett fulgte vi tradisjonen fra militære øvelser om å la fremmede land i øvelsen være fiktive. Det gjorde de naturlig å også la deltakervirksomhetene spille fiktive universiteter.

For å styrke **fokuset på samarbeid på tvers** av virksomhetene innførte vi et siste fiktivt hovedkonsept: et banebrytende felles forskningsprosjekt som ved hjelp av kunstig intelligens korrelerer data fra satellitter, landbaserte antennesystemer, sensorer på sjøkabler, radar- og sonardata fra sivil skipstrafikk i nordområdene.

Sikt

Spillverdenen – politisk-geografisk

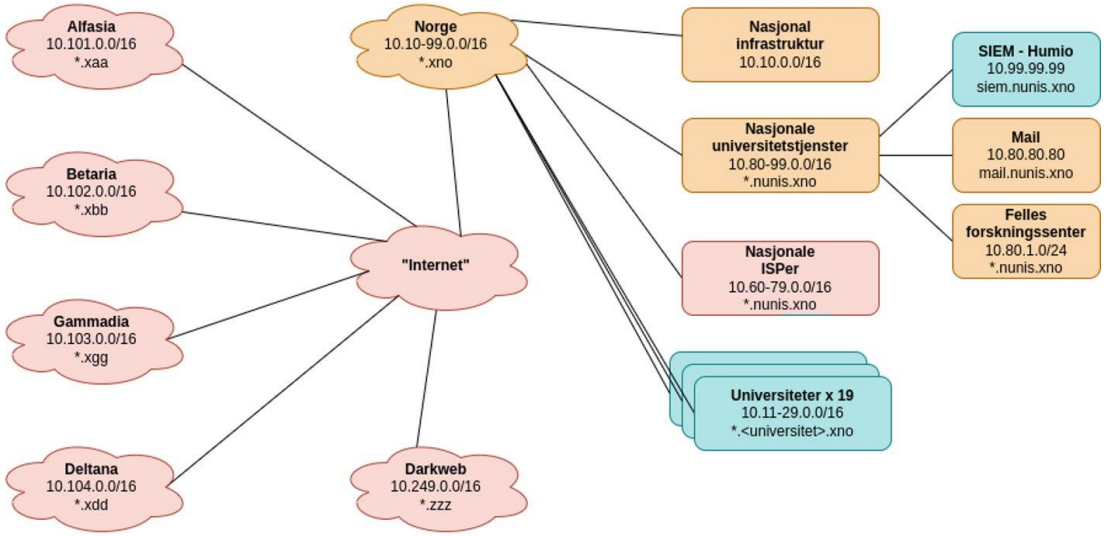
- Alfasia .xaa
- Betaria .xbb
- Gammadia .xgg
- Deltana .xdd
- Norway .xno

Sikt

Spillverdenen – simulert interne

Den tekniske riggen bestod av:

- 473 virtuelle maskiner
- 121 subnett
- En global adresseplan
- Lokale adresseplaner for deltakerne
- Domenenavnssystem for spillverdenen
- Sentral loggtjener for virksomhetene
  - IRTene hadde ikke direkte tilgang til sine systemer, kun loggene fra disse, samt fra det felles forskningsanlegget



Felles universitetstjenester

SIEM
10.99.99.99 / siem.nunis.xno

Epost
10.80.80.80 / mail.nunis.xno

Felles forskningssenter
10.80.1.0/24 / *.rsd.nunis.xno

Nasjonal infrastruktur

DNS
10.10.10.10

ISPOne
10.61.0.0/16 / *.ispone.xno

ISPTwo
10.62.0.0/16 / *.isptwo.xno

ISPThree
10.63.0.0/16 / *.ispthree.xno

Campusnettverket

Administrative systemer
10.29.1.0/24
*.adm.granuni.xno

Ansatte
10.29.2.0/24
*.emp.granuni.xno

Studentsystemer
10.29.3.0/24
*.sas.granuni.xno

Studenter og gjester
10.29.4.0/24
*.sag.granuni.xno

Sensitiv forskningslab
10.29.5.0/24
*.srl.granuni.xno

HUMIO

Sikt

Spillverdenen – liv og røre

De 135 individuelle spilldeltakerne befant seg på sitt vanlige arbeidssted, og koblet seg opp mot spillverdenen via VPN-løsning. For å gjøre spillverdenen mer levende brukte vi også:

- Kopi av sektorens reelle sikre chatløsning
- Ni personer med hver sin telefon som spilte ulike roller:
  - Brukere ved virksomheten
  - Uhjelpsom driftstekniker ved fellesanlegget
  - Gravende journalist
- Nettaviser med relevante og irrelevante nyheter, inkludert hendelsene i øvelsen belyst av deltakernes svar til journalist
- Forespørsler om rapportering til virksomhetens kriseledelse og pressebrief
- Seks utdypende dilemmaer for kriseledelsen

Sikt

Gjennomføring

- Øvelsen ble gjennomført på én dag, uten pauser
- Spillstaben på 15 personer var samlet i NCRs lokaler i Gjøvik
- Fem observatører fulgte med fra Sikts lokaler i Trondheim

- Tre tiltakskort var utarbeidet på forhånd til bruk for virksomheter uten slike fra før
- Logger ble generert fortløpende i den virtuelle verdenen med ulikt innhold for hver virksomhet
- 21 spillmeldinger ble posjonert ut gjennom dagen
- Medieportalen ble kontinuerlig fylt på med nytt innhold, både forhåndsprodusert og ad hoc

- Debriefing/«hot wash up» ble avholdt hos hver enkelt virksomhet fasilitert av lokal øvingsleder

Sikt

Evaluering

- Evalueringsskjema ble sendt ut kort etter øvelsen med kort svarfrist for å sikre at svarene kom mens opplevelsen var friskt i minne

- Evalueringen skulle både gi tilleggsverdi til deltakervirksomhetene og til oss selv som arrangør; spørsmålene var derfor basert på læringsmålene for øvelsen pluss de momentene vi som arrangør fant mest relevante

- For å muliggjøre aggregering hadde de fleste spørsmålene et lukket sett med alternativer, men med et felt for «usikker/ikke relevant for meg» for å unngå vilkårlige valg, samt fritekstfelt for å fange opp tilbakemeldinger som ikke passet inn i skjemaet

Sikt

Nyttige lærdommer

- Fokus på læringsmål fra starten av hadde stor verdi
- Bruk av klonet chat-tjeneste var i tillegg til å være viktig i selve øvelsen et svært nyttig verktøy for å kommunisere innad i arrangørstaben, og da spesielt med de lokale øvingsansvarlige hos deltakervirksomhetene
- At eduCSC «spilte seg selv» gjorde det mulig for deltakerne å dele informasjon anonymt i forhold til andre deltakere – dette senker terskelen for å dele, men vi observerte at øvelseskonteksten medførte «overdeling»

- Man kan alltid informere bedre i forkant, for eksempel hvorvidt alle får samme informasjon eller om det er variasjon mellom virksomhetene
- Det er viktigere at alle som trenger det har enkel tilgang på informasjonen de trenger under øvelsen enn at ingen kan komme til å få vite litt for mye
- Deltakerne vil ha et ønske om å få vite «hva som egentlig skjedde» og om deres handlinger var «bra/riktig»

- Spilløvelser lar seg godt kombinere med andre øvelsesformer
  - Her utvidet vi omfanget med å forelegge et sett dilemmaer som sprang ut fra scenariets hendelsesforløp, som kunne brukes som diskusjonsøvelse for kriseledelsen enten i parallell med øvelsen eller neste dag
  - Hadde vi hatt tid til å forberede det ville vi hatt en teknisk funksjonsøvelse i forkant hvor deltakerne samtidig kunne gjøre seg kjent med verktøyene


Sikt