Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Ranvir Singh
Espen Eriksen
Jan Ngo
Farhaz Ismail

Incident Response og Incident Response Training

Bacheloroppgave i Digital infrastruktur og cybersikkerhet
Veileder: Erjon Zoto

Mai 2022

NTNU
Kunnskap for en bedre verden

Ranvir Singh
Espen Eriksen
Jan Ngo
Farhaz Ismail

Incident Response og Incident Response Training

Bacheloroppgave i Digital infrastruktur og cybersikkerhet
Veileder: Erjon Zoto
Mai 2022

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

NTNU

Kunnskap for en bedre verden

Incident Response og Incident Response Training

Espen Eriksen, Farhaz Ismail, Jan Ngo og Ranvir Singh

20. mai 2022

Forord

Oppgaven 'Incident Response og Incident Response Training' var et oppdrag av Moelven Industrier ASA til bachelorstudenter i Digital infrastruktur og cybersikkerhet (BDIGSEC) på Norges teknisk-naturvitenskapelige universet (NTNU) i Gjøvik for våren 2022. Som studenter innen informasjonssikkerhet ønsket gruppen primært en oppgave innenfor dette fagområdet. I tillegg har flere gruppemedlemmer erfaring fra hendelseshåndtering gjennom valgfag og relevante deltidsjobber. Oppgaven hadde således høy prioritet.

I oppgaven er det utformet et rammeverk for hendelseshåndtering tilpasset oppdragsgiver. Rammeverket er adskilt i seks faser, og tar sikte på å beskrive hendelseshåndteringsprosessen fra start til slutt. Rammeverket kan benyttes som et referanseverk. Med referanseverk menes et oppslagsverk som inneholder forslag til sikkerhetstiltak, hvilke vurderinger som må ligge til grunn for kritiske avgjørelser og hvordan sikkerhetspersonell fordeler oppgaver seg i mellom. Videre er det utarbeidet et treningsopplegg for å forbedre eksisterende rutiner. Treningsopplegget er rettet mot sikkerhetsteamet, og ikke vanlige sluttbrukere.

Vi ønsker å takke vår veileder Erjon Zoto, universitetslektor ved Norges teknisk-naturvitenskapelige universitet i Gjøvik, for veiledningen gjennom prosjektarbeidet.

En stor takk til Tom Kjølhamar, fagansvarlig for IT-sikkerhet hos Moelven Industrier ASA, for nært samarbeid og oppfølging.

Espen Eriksen

Farhaz Ismail

Jan Ngo

Ranvir Singh

Tittel:

Incident Response og Incident Response Training

Deltaker(e):

Espen Eriksen

Farhaz Ismail

Jan Ngo

Ranvir Singh

Dato:	Emnekode:	Emne:	Publiseringsavtale inngått:
20. mai 2022	DCSG2900	Bacheloroppgave - Bachelor i digital infrastruktur og cybersikkerhet	Åpen

Studium:	Ant. sider / vedlegg:
Digital infrastruktur og cybersikkerhet	221 / 7

Veileder:

Erjon Zoto

Oppdragsgiver:

Moelven Industrier ASA

Kontaktperson(er):

Tom Kjølhamar

Stefan Djupvik

Stikkord:

Hendelseshåndtering, rammeverk, sikkerhetshendelser, trening

Sammendrag:

Prosjektet er gjennomført på oppdrag fra Moelven Industrier ASA. Oppgaven handler om å utforme hendelseshåndteringsrutiner og et treningsopplegg for hendelseshåndtering tiltenkt oppdragsgivers IT-personell.

Hendelseshåndteringsrutinene ble utformet i form av et rammeverk. Rammeverket besto av totalt seks faser som beskriver håndtering av sikkerhetshendelser på en oversiktlig måte. Det ble i tillegg utformet et treningsopplegg i form av tabletop-øvelser.

Utvidet sammendrag

Hendelseshåndtering er et sentralt tema innen informasjonssikkerhet. Det foreligger mye informasjon om beste praksiser og forslag til tiltak, men det er få ressurser som beskriver konkrete fremgangsmåter eller en steg-for-steg-prosess for håndtering av hendelser. Dessuten vil en slik prosess avhenge av størrelsen på virksomheten, hvilken sektor den opererer i, hendelsestype, omfang og alvorlighetsgrad. Gruppen fant derfor denne oppgaven interessant og ønsket å ta oppdraget.

Oppdraget tok utgangspunkt i oppdragsgivers ønsker og ble tilpasset virksomhetens behov. Formålet var å utforme en hendelseshåndteringsprosess virksomheten kunne ta i bruk ved oppdagelse av sikkerhetshendelser, samt et treningsopplegg som kontinuerlig kunne benyttes av IT-personell for å forbedre eksisterende rutiner og prosesser.

Gruppen utformet et rammeverk og et treningsopplegg for oppdragsgiver, basert på deres ønsker og krav. Den største delen av oppdraget var utforming av rammeverket. Rammeverket skulle omfatte hele hendelseshåndteringsprosessen fra start til slutt, og fungere som et referanseverk innen fagområdet. Rammeverket inkluderte blant annet forebyggende tiltak og herding av infrastruktur, policyer og generell informasjon. Den største utfordringen med utformingen av treningsopplegget var å utforme et treningsopplegg som kontinuerlig kunne tas i bruk. Gruppen løste dette ved å utforme et treningsopplegg virksomheten enkelt kan designe og utvide på egen hånd.

For gruppen har bacheloroppgaven vært en svært lærerik prosess med stort læringsutbytte, både faglig, men også knyttet til teamarbeid over en lengre periode.

Extended Abstract

Incident response is an important topic in information security. The greater topic of incident response has been gaining a lot of attention recently, however few businesses have applied proper incident response routines [6]. Incident response seemed like an interesting topic, and for this reason the task was of high priority.

The thesis is based on the needs of the corporation in relation to cybersecurity. The goal is to provide an incident response framework the corporation may utilize in the event of an incident, in addition to training routines for the security team.

To answer this thesis the group developed two documents related to incident response. The largest document contained the framework. The framework targets a wide variety of topics related to incident response, such as routines, measures and tools. The second document pertained to providing training routines for the security team. The document describes tailor-made exercises the corporation can utilize to train their team about incident response.

The group enjoyed the learning process throughout the project period pertaining to the topics of incident response and training, in addition to working as a group on a comprehensive project.

Innhold

Figurer

Tabeller

Forkortelser og ordforklaringer

Forkortelser

- NTNU - Norges teknisk-naturvitenskapelige universitet
- IDS - Intrusion detection system
- CSIRT - Computer Security Incident Response Team
- BDIGSEC - Bachelor i Digital infrastruktur og cybersikkerhet
- IR - Incident response
- NSM - Nasjonal sikkerhetsmyndighet
- SANS - SysAdmin, Audit, Network and Security
- NIST - National Institute of Standards and Technology
- IT - Informasjonsteknologi

Ordforklaringer

- Incident response - Kjent som hendelseshåndtering på norsk. En organisert tilnærming til å identifisere og håndtere hendelser i form av sikkerhetsbrudd eller cyberangrep.
- Scrum - Et prosessrammeverk utviklet for å støtte kompleks produktutvikling.
- Playbook(s) - Håndbok som gir standardprosedyrer for å håndtere sikkerhetshendelser i sanntid.
- Cyberangrep - En ekstern trussel som har som hensikt å forstyrre, skade, eller overbelaste datasystemer [28].

- Løsepengevirus - En type skadevare som krypterer eller låser hele eller deler av innholdet på datamaskinen [25].
- Phishing - Form for sosial manipulering hvor en angriper forsøker å lure et offer til å utføre en handling og gi fra seg personlig informasjon [26].
- Spear phishing - Målrettet forsøk på å innhente spesifikk informasjon [41].
- Smishing - Phishing via SMS [43].
- Inject - En fortsettelse av fortellingen, ofte som et resultat av et negativt utfall for spillerne, som blir presentert av lederen i treningsopplegget.
- Success - 'Success' vil si at en får et terningkast med verdi mellom 1-10 i treningsopplegget. Dette fører til en positiv utvikling i spillet.
- Failure - 'Failure' vil si at en får et terningkast med verdi mellom 11-20 i terningkastet i treningsopplegget. Dette fører til en negativ utvikling i spillet.
- Backdoors and Breaches - Et kortspill for hendelseshåndtering.
- Brute-force - En hackemetode som bruker prøving og feiling for å knekke passord [5].
- Kriminalteknisk image - Kjent som 'Forensic image' på engelsk. En direkte kopi av en fysisk lagringsenhet [42].
- Reconnaissance - Kjent som rekognisering på norsk. Når aktør prøver å samle informasjon som de kan bruke i fremtidige operasjoner [21].
- Initial Access - Kjent som 'initiell aksess' på norsk, er når aktør prøver å komme inn i nettverket [18].
- Execution - Kjent som utførelse på norsk. Når aktør prøver å kjøre ondsinnet kode [16].
- Privilege Escalation - Kjent som 'eskalering av privilegier' på norsk. Når aktør prøver å få privilegier på høyere nivå [20].
- Discovery - Kjent som oppdagelse på norsk. Når aktør prøver å finne ut mer om systemet [14].

- Lateral Movement - Er når aktør prøver å bevege seg i et kompromittert nettverk [19].
- Command and Control - Er når aktør prøver å kommunisere med kompromitterte systemer for å kontrollere dem [13].
- Exfiltration - Kjent som eksfiltrering på norsk. Når aktør prøver å stjele data [17].
- Impact - Er når aktør prøver å manipulere eller ødelegge system og data [18].
- Team - Sikkerhetsgruppe
- Patch - Å reparere et program [23].
- TTP - En metode for å oppdage ondsinnet aktivitet [22].
- Rootkits - Et program som gir en trusselaktør ekstern tilgang og kontroll over et system [40].
- Spoofing - ondsinnet manipulering av data og informasjon for å vinne troverdighet [10].
- Wipe - betyr fullstendig sletting av all data fra et lagringsmedium [44].
- XDR - Et verktøy for trusseldeteksjon og respons som gir en helhetlig beskyttelse mot cyberangrep [46].
- Data Loss Prevention (DLP) - En strategi for å hindre personer i å få tilgang til sensitiv informasjon som de ikke skal opprinnelig ha [36].
- Cyber range - Type treningsøvelse hvor 'brukere og systemer eksponeres for realistiske hendelser i trygge omgivelser' [34].

1 Introduksjon

Dette kapittelet gir en introduksjon til prosjektoppgaven og hvem prosjektet er skrevet for. Kapittelet består av en beskrivelse av oppdragsgiver, en introduksjon til fagområdet hendelseshåndtering, innledning, problemstilling og målgruppe, oppgavens formål, hvilke effektmål og resultatmål som ble satt, avgrensninger, oppgavebeskrivelse, prosjektgruppens bakgrunn, rammer, arbeidsmetode og organisering av rapporten.

1.1 Om Moelven Industrier ASA

Moelven Industrier ASA er en av Skandinavias ledende leverandører av trebaserte byggprodukter. Konsernet leverer produkter og løsninger til industri- og handelskunder, og til bygg- og entreprenørkunder i prosjektmarkedet. Konsernet omfatter totalt 33 produksjonsselskaper fordelt på 41 produksjonssteder i Norge og Sverige. I tillegg har konsernet salgsapparat i Norge, Sverige, Danmark, Storbritannia, Tyskland og Kina. Det er om lag 3300 ansatte totalt.

Moelven Industrier ASA er delt opp i divisjonene Timber, Wood, og Byggsystemer.

Divisjon Timber leverer skurlast og komponenter av lokal gran og furu. Denne divisjonen består av både produksjonsselskaper og salgskontorer. Kundene i denne divisjonen er hovedsakelig industriforetak som kjøper innsatsvarer til egen produksjon av konstruksjonsvirke, panel, gulv, lister, møbler, vinduer og emballasje. Rundt halvparten av denne produksjonen blir solgt i Skandinavia, mens Storbritannia, Tyskland, Nederland, Frankrike, Polen, Spania, Italia, Japan, og Midtøsten & Nord-Afrika utgjør sentrale eksportmarkeder.

Divisjon Wood utvikler og produserer et stort utvalg trebaserte bygg- og interiørprodukter med høy foredlingsgrad. Wood-kunder er hovedsakelig byggvarehandelen og industrikunder i Skandinavia. Divisjonen har produksjonsenheter i Norge og Sverige. Ved flere av Wood sine produksjonsenheter er det både sagbruk, høvleri og impregneringsanlegg. Divisjonen har flere fordelingsenheter som produserer listverk, interiørpaneler, gulv og konstruksjonsvirke av tre.

Divisjon Byggsystemer består av virksomhetsområdene limtre, byggmoduler og systeminnredning. Divisjon Byggsystemer lever systemløsninger til modulbygg, kontorer, og bærende konstruksjoner i limtre til prosjekt- og entreprenørkunder. Disse tre selskapsområdene er markedsledende innenfor sine segmenter og blir hovedsakelig levert i Norge og Sverige.

Moelven Industrier ASA sin eierstruktur ser i dag slik ut:

- Glommen Mjøsen Skog SA: 66,84%
- Viken Skog SA: 32,80%
- Allskog SA: 0,08%
- De resterende 0,28% eies av privatpersoner

1.2 Om hendelseshåndtering

Hendelseshåndtering er en organisert tilnærming til å identifisere og håndtere hendelser i form av sikkerhetsbrudd eller cyberangrep. Målsetningen er å håndtere hendelsen på en slik måte at det begrenser skadeomfanget, reduserer kostnader og gjenopprettingstid. [2]. En sikkerhetshendelse kan oppstå dersom en angrepsaktør får uautorisert tilgang til en virksomhets informasjonssystemer. Hensikten til angrepsaktørene er å skade informasjonssystemer, få tilgang til sensitiv informasjon og/eller endre informasjon med hensyn til konfidensialitet, integritet og/eller tilgjengelighet [24]. I de senere år har det vært en stor vekst av løsepengevirusangrep, med angrepsaktører som krypterer eller eksfiltrerer data med krav om løsepenger for å gjenopprette system(er) til normal drift.

Med en strukturert tilnærming til hendelseshåndteringsprosessen og etablerte rutiner på plass kan virksomheter være i stand til å gjenopprette systemer til normal tilstand etter en sikkerhetshendelse og redusere kostnader.

1.3 Innledning

Prosjektoppgaven gruppen ble tildelt var 'Incident response og incident response training'. Det var en svært åpen oppgave med få begrensninger. Oppgaven måtte omfatte hendelseshåndtering og et treningsopplegg for virksomhetens IT-personell. I samarbeid med oppdragsgiver ble gruppen enig om å utforme et rammeverk for hendelseshåndtering og et treningsopplegg oppdragsgiver kan benytte for å kontinuerlig forbedre sine eksisterende rutiner og kompetanse. Den største utfordringen var knyttet til avgrensning av oppgaven. Ettersom hendelseshåndtering omfatter svært mange ulike hendelser ble oppgavens hovedfokus rettet mot de sikkerhetshendelsene oppdragsgiver fant mest aktuelle, som i dette tilfellet var løsepengevirus- og phishingangrep.

1.4 Problemstilling

Det digitale trusselbildet øker raskt, og det blir stadig mer krevende å beskytte seg mot ondsinnede aktører. Dessuten er balansegangen mellom funksjonalitet og sikkerhet utfordrende. God informasjonssikkerhet krever blant annet gode hendelseshåndteringsrutiner og en strategi for trening av IT-personell.

1.5 Målgruppe

Prosjektoppgaven har hovedsakelig oppdragsgiver som målgruppe. Målgruppen strekker seg videre til studenter, forskere, sensorer og andre som kan dra nytte av prosjektoppgaven. Rammeverket og treningsopplegget er tilpasset oppdragsgivers ønsker og behov, men benytter samtidig mange beste praksiser som kan overføres til andre målgrupper.

1.6 Formål

I prosjektoppgaven var det ønskelig å fremme nytteverdien av et tilpasset rammeverk for hendelseshåndtering. Rammeverket skulle fungere som et referanseverk for aktiviteter innen fagområdet, og tilby virksomheten anledning til å videreutvikle rammeverket selv. Formålet med oppgaven var å øke informasjonssikkerheten i virksomheten og ansatte sin sikkerhetsforståelse. Både rammeverket og treningsopplegget er designet for å tilby virksomheten kontinuerlig læring og forbedring.

1.7 Effektmål

Prosjektoppgaven ble utført med følgende effektmål:

- Gjøre ansatte mer bevisst konsekvensen av å ikke rapportere hendelser
- Øke informasjonssikkerhet i virksomheten
- Kompetanseheving av ansatte gjennom kontinuerlig opplæring
- Redusere antall hendelser som ikke blir varslet om
- Redusere antall hendelser som ikke blir håndtert

1.8 Resultatmål

Prosjektoppgaven ble utført med følgende resultatmål:

- Utforme en sluttrapport som helhetlig beskriver prosjektoppgaven på en tilstrekkelig måte
- Utforme et rammeverk som bistår oppdragsgiver med hendelseshåndtering
- Utforme et treningsopplegg som oppdragsgiver kan bruke for opplæring av sitt IT-personell

Disse resultatmålene var mer generelle:

- Utforme et rammeverk som kan benyttes som et referanseverk for oppdragsgiver
- Engasjerende treningsopplegg som ansatte kan bruke til å lære mer om sikkerhetshendelser og -kultur
- Øke virksomhetens forståelse for hendelseshåndtering

1.9 Avgrensning

Det ble ikke gitt noen begrensninger fra oppdragsgiver i utformingen av rammeverk og treningsopplegg, og det ble uttrykt et ønske om at gruppen selv foretok de avgjørelser de følte var

riktig. For å avgrense oppgaven ble løsepengevirus- og phishingangrep hovedfokuset til rammeverket. I tillegg skulle rammeverket omfatte en generell tilnærming til andre type angrep eller sikkerhetshendelser, og beskrive hvordan sikkerhetsteamet kan gå fram for å håndtere disse på best mulig måte.

I utformingen av treningsopplegget konkluderte gruppen med at det ble for tidkrevende å utforme et treningsopplegg som simulerer reelle cyberangrep som for eksempel kan oppnås i et cyber range-miljø. Følgelig ble treningsopplegget avgrenset til tabletop-øvelser med en leder som også er med på å designe øvelsen underveis. Treningsopplegget tar utgangspunkt i ulike angrepsvektorer og oppdragsgivers egne systemer, slik at det blir svært relevant for reelle hendelseshåndteringsprosesser og kan være med på å avdekke svakheter eller mangler i eksisterende rutiner.

Gruppen ble enig om at rammeverket skulle benyttes som et referanseverk. Som en følge av dette ble det avgjort å utforme playbooks som skulle fungere som nedskalerte versjoner av rammeverket. Playbooks skulle fungere som en strømlinjeformet prosess for hvordan sikkerhetsteamet kan håndtere sikkerhetshendelser med en konkret steg-for-steg-prosess. Det skulle utformes en playbook for løsepengevirusangrep, phishingangrep og en generell for andre type hendelser.

Avgrensningene ble foretatt med hensyn til å få et tilfredsstillende resultat, og samtidig begrense omfanget slik at prosjektoppgaven ble gjennomførbar.

1.10 Oppgavebeskrivelse

Det digitale trusselbildet blir stadig større, og det stiller større krav til hvordan virksomheter sikrer seg mot angrep. Prosjektoppgaven gikk ut på å utforme gode incident response-rutiner, samt en incident response training-strategi for oppdragsgiver.

1.11 Prosjektgruppens bakgrunn

Gruppens medlemmer går tredje og avsluttende år på bachelorstudiet Digital infrastruktur og cybersikkerhet ved Norges teknisk-naturvitenskapelige universet (NTNU) i Gjøvik. Medlemmene har samarbeidet på gruppeprosjekter gjennom hele studieløpet og kjenner hverandre godt fra før. Studiet har omfattet mange fagområder, som blant annet risikostyring, operativsystemer, programmering, etisk hacking, infrastruktur og datamodellering og databasesystemer. To av medlemmene har også hatt relevante emner innen hendelseshåndtering.

Ingen medlemmer hadde tidligere kjennskap til tekstbehandlingssystemet LaTeX, som prosjektgruppen valgte til å utforme produktet og sluttrapporten.

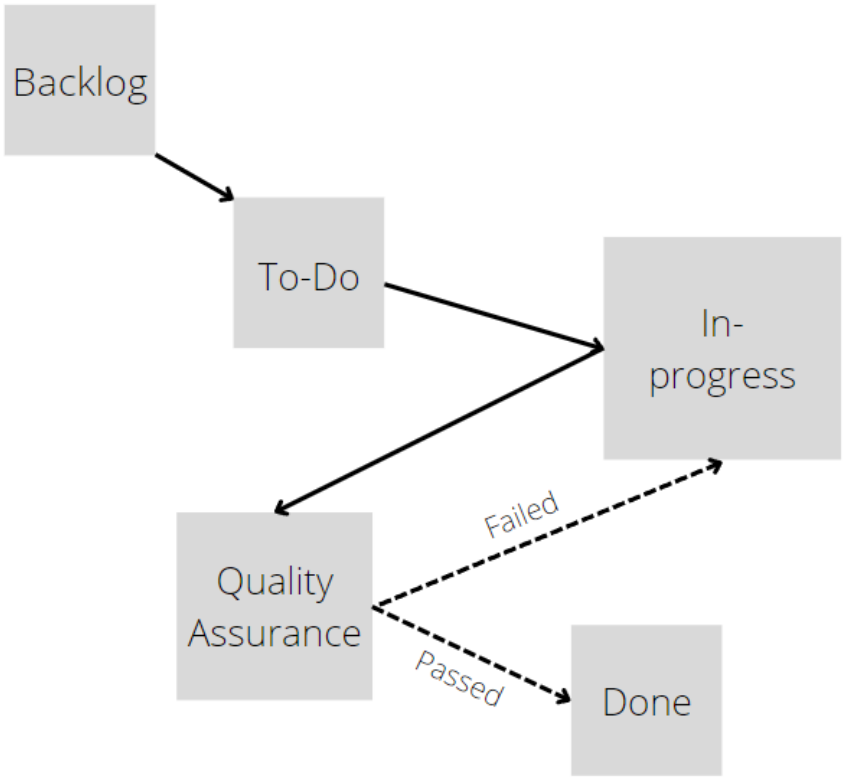
1.12 Rammer

Prosjektet ble utført i tidsrommet 10. januar 2022 til 20. mai 2022. Rapporten er skrevet på norsk og utformet i samskrivningsprogrammet Overleaf som benytter LaTeX. Arbeidsoppgaver i gruppen ble fordelt i et kanban board i Github med en angitt tidsfrist. For møter med oppdragsgiver ble dette hovedsakelig gjennomført via Microsoft Teams. Noen møter ble også avholdt hos oppdragsgivers kontorer.

1.13 Arbeidsmetode

Gruppen la stor vekt på både struktur og organisering ved valg av arbeidsmetode. God planlegging var nødvendig for å holde seg til definert tidsskjema. Valgt prosessrammeverk for gruppen ble et kanban board, dette ga gruppen god fleksibilitet i delegeringen av oppgaver. Ved å følge et kanban board ble det enklere å følge gruppens progresjon underveis. Det tillot dessuten gruppen å holde en god fremdrift og følge med på hvordan arbeidsflyten utviklet seg. Bruk av kanban board var meget nyttig ettersom gruppen samarbeidet digitalt mesteparten av prosjektfasen, der kanban tillot dette på grunn av dets adaptive kvaliteter [11].

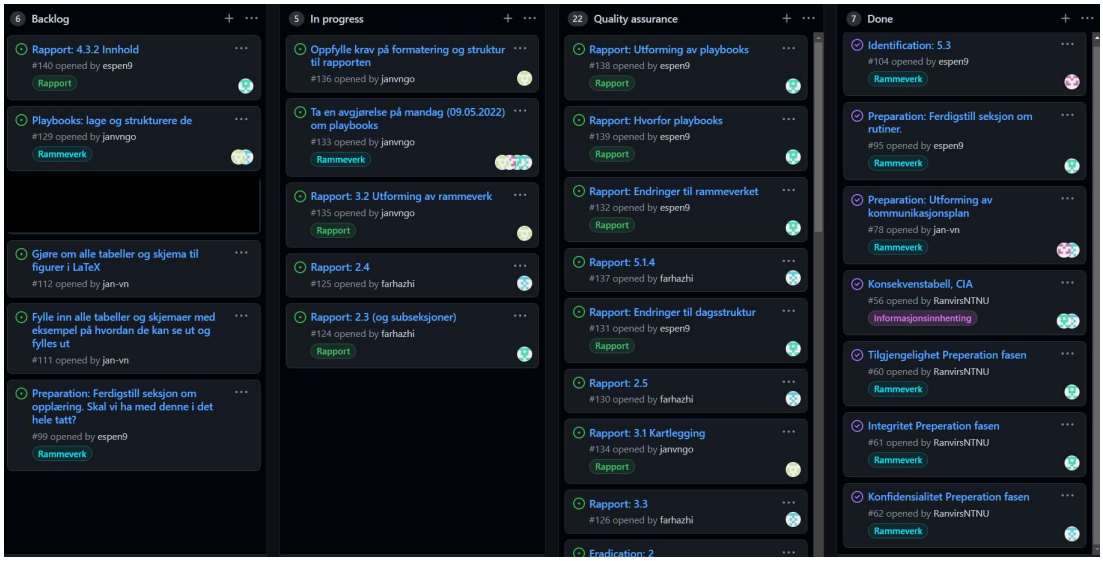
Github ble valgt for bruk av kanban board. Avgjørelsen hadde grunnlag i at prosjektgruppen var kjent med denne plattformen fra tidligere prosjekter, og var fornøyd med dens funksjonalitet.



Figur 1: Kanban prosess

I GitHub delte gruppen kanban opp i fire hovedkolonner som representerte hvilken fase en oppgave tilhørte. 'Backlog' var kolonnen som inneholdt alle oppstående gjøremål. I denne kolonnen ble det satt frister og tildelt ansvarsperson. På denne måten var 'backlog' en samling av gjøremål som ikke var påbegynt. 'In progress' var kolonnen som inneholdt alle oppgaver som ble jobbet med. Fra 'in progress' ble de flyttet til 'quality assurance' når oppgavene var ferdigstilt. I denne kolonnen skulle de være inntil en kvalitetssjekk ble utført, og eventuelle kommentarer ble utbedret. Når kvalitetsikrer var fornøyd med oppgaven ble gjøremålene flyttet til 'done'. Dersom gjøremålet ikke tilfredsstilte 'quality assurance' ble gjøremålet flyttet tilbake til 'in progress'.

Et eksempel på hvordan kanban board så ut underveis var som følger:

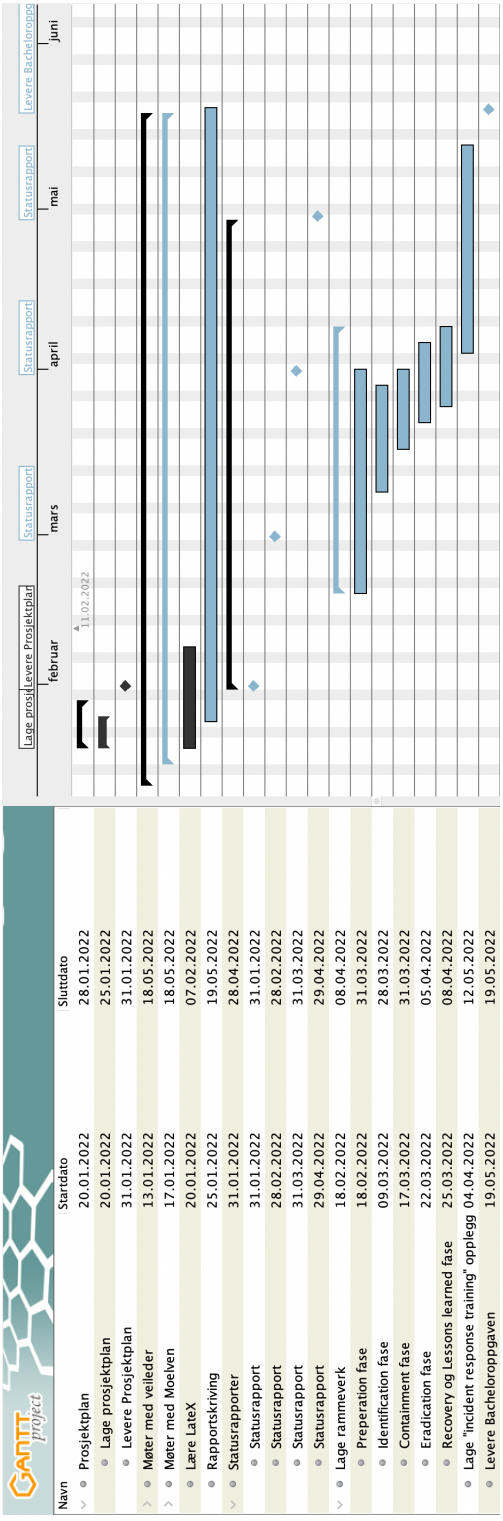


Figur 2: Kanban board i GitHub

Det ble videre utarbeidet et gantt-skjema som et overordnet tidsskjema for hele prosjektfasen. Gantt-skjemaet delte prosjektfasen inn i mindre faser, med angitte delfrister. Skjemaet ble gjennomgått hver torsdag for å sikre at gruppen fulgte tidsskjemaet. Det ble utført endringer på skjemaet etter behov.

Gantt-skjemaet dekker alle arbeidsoppgaver og møter som ble utført under prosjektperioden.

Gantt-skjemaet var som følger:



Figur 3: Gantt-skjema

Jf. vedlegg G for et klarere bilde av gantt-skjemaet.

1.14 Organisering av rapporten

Prosjektrapporten er delt inn i syv hovedkapitler, samt vedlegg. Rapportstrukturen er basert på eldre bachelor- og masteroppgaver, i tillegg til NTNU sin mal for rapporter [33].

1. **Introduksjon**

   Dette kapittelet inneholder grunnleggende informasjon om prosjektoppgaven, prosjektgruppens avgjørelser og arbeidsmetodikk.

2. **Metodikk**

   Dette kapittelet inneholder metodikken som gruppen benyttet for å løse prosjektoppgaven i tillegg til kravene som ble stilt til rammeverket og treningsopplegget.

3. **Utforming av rammeverk**

   Dette kapittelet inneholder gruppens fremgangsmåte for utforming av rammeverket, og oppsummerer dets innhold.

4. **Utforming av treningsopplegg**

   Dette kapittelet inneholder gruppens fremgangsmåte for utforming av treningsopplegget, og oppsummerer dets innhold.

5. **Utforming av playbooks**

   Dette kapittellet inneholder gruppens fremgangsmåte for utforming av playbooks.

6. **Drøfting og diskusjon**

   Dette kapittelet inneholder prosjektgruppens diskusjoner og avgjørelser.

7. **Avslutning**

   Dette kapittelet inneholder gruppens konklusjoner og en avsluttende oppsummering av prosjektoppgaven.

2 Metodikk

Dette kapittelet beskriver metodikken som ble benyttet i utarbeidelsen av prosjektoppgaven. Kapittelet består av kartlegging og problemdefinisjon, valg av rammeverk som grunnlag, analyse av ulike rammeverk og hva gruppen kom fram til, informasjonsinnhenting, utvikling av rammeverk og utvikling av treningsopplegg.

2.1 Kartlegging og problemdefinisjon

Prosjektoppgaven startet med informasjonsinnhenting og kartlegging av oppgavens rammer. I innledningen av prosjektet ble det avholdt møter med oppdragsgiver der gruppen fikk en gjennomgang av konsernet, og anledning til å stille spørsmål relatert til virksomhetens nåværende infrastruktur og sikkerhetsnivå.

Basert på kartleggingen avgjorde gruppen å utforme et rammeverk for hendelseshåndtering for å besvare oppgavens krav om hendelseshåndteringsrutiner. Det var videre ønskelig å utforme et treningsopplegg til virksomhetens IT-personell, som gruppen fant hensiktsmessig å begynne med etter at prosessen med utforming av rammeverket enten var ferdigstilt eller i en avsluttende fase. Årsaken til en slik prioritering var at rammeverket kunne gi gruppen et bedre grunnlag for hva slags trening som kunne være aktuelt, og eventuelt tilpasse treningsopplegget til rammeverkets struktur.

Ettersom rammeverket ble svært omfattende ble gruppen etter hvert enig om å utforme playbooks. Formålet med playbooks var å utforme en nedskalert, steg-for-steg-prosess virksomheten kunne forholde seg til og aktivt følge under sikkerhetshendelser. Rammeverkets formål ble derfor å fungere som et referanseverk innen fagområdet hendelseshåndtering.

2.2 Valg av rammeverk som grunnlag

For å utforme et rammeverk tilpasset oppdragsgiver var det verdifullt å ha et allerede eksisterende og anerkjent rammeverk som grunnlag. Det ble utført en større analyse av relevante rammeverk prosjektgruppen kunne bygge videre på. Elementer som passet best til prosjektoppgaven ble hentet ut. Etter mye kartlegging kom gruppen fram til fire etablerte rammeverk verdt

å analysere. Disse rammeverkene var som følger:

- MITRE ATT&CK
- SANS Incident Handler's Handbook
- NIST Incident Handling Guide
- ISACA Cybersecurity Incident Response

2.2.1 Kravliste til rammeverk

For å være i stand til å vurdere hvorvidt rammeverkene passet som grunnlag til oppgaven valgte gruppen å definere en kravliste. Kravene var med på å avgjøre hvilke rammeverk gruppen mente var best egnet for prosjektoppgaven. Kravlisten bestod av alder på rammeverket, dets struktur, og kredibilitet.

Her følger en beskrivelse av de ulike kravene prosjektgruppen definerte.

Alder

For kravet om alder ble det undersøkt hvor gammelt rammeverket var og hvorvidt det hadde blitt vedlikeholdt med oppdateringer eller endringer. Som en følge av den raske utviklingen innen informasjonssikkerhet var alder en viktig parameter da det ga en pekepinn på hvor oppdatert rammeverket var til dagens trusselbilde.

Struktur

Struktur handlet om hvordan rammeverket var satt opp. Gruppen så etter hvilken struktur som var mest hensiktsmessig for prosjektoppgaven ved å se på om rammeverket samsvarte med avgrensningen som ble definert. Gruppen så også etter hvilken struktur som var enkel å følge, og som ga rom for å formidle innholdet på en enkel måte for oppdragsgiver.

Kredibilitet

Kredibilitet handlet om troverdigheten til rammeverket. Et anerkjent rammeverk med et godt omdømme vil typisk ha en kjent og kredibel utgiver. Et kredibelt rammeverk har dessuten større sannsynlighet for å være i bruk i industrien, som videre gjør den mer troverdig.

2.3 Analyse av rammeverk

Her følger en beskrivelse av analysen som ble utført av de ulike rammeverkene:

2.3.1 Analyse av MITRE ATT&CK

MITRE ATT&CK-rammeverket er en kunnskapsbase og modell for hvordan en skal beskytte seg mot cyberangrep [15]. Rammeverket er utviklet av MITRE, en ideell organisasjon fra USA. MITRE leder 'Federally funded research and development centers', og støtter USAs regjering innen blant annet luftfart, sikkerhet, helsevesen og cybersikkerhet. Rammeverket ble utviklet som svar på spørsmålet 'How well are we doing at detecting documented adversary behavior?'. Rammeverket omfatter de ulike stegene for en hendelse, sett fra angripers perspektiv. Stegene går fra rekognosering til etter-utnyttelse. Det vil si at den omfatter alle fasene i et angrep fra start til slutt.

Alder

Rammeverket ble først utgitt i 2013 og har blitt oppdatert jevnlig siden [12]. Levering av cyberangrep og dens tactics, techniques and procedures (TTP) utvikler seg og trusselbildet endrer seg stadig. Dette fører til at nye sårbarheter og trusler oppstår. ATT&CK-rammeverket blir følgelig kontinuerlig oppdatert i takt med det økende trusselbildet.

Struktur

MITRE ATT&CK-rammeverket viser de ulike stegene av et angrep, fra rekognosering til etter-utnyttelse. Rammeverket tilbyr også veiledning for å identifisere og beskytte seg mot angrep i alle faser av angrepet. I tillegg inkluderer rammeverket en katalog over ulike teknikker og teknologier angriperen kan benytte seg av i de ulike stegene av et angrep.

Følgene er steg i rammeverket:

- Reconnaissance
- Initial Access
- Execution
- Privilege Escalation
- Discovery
- Lateral Movement
- Command and Control
- Exfiltration
- Impact

Kredibilitet

MITRE ATT&CK-rammeverket er utarbeidet av MITRE Corporation. MITRE Corporation er en amerikansk ideell organisasjon og administrerer føderalt finansierte forskningssentere som støtter ulike amerikanske myndighetsorganer innen blant annet forsvar, luftfart, helse, og cybersikkerhet. Dette gir organisasjonen svært god kredibilitet.

2.3.2 Analyse av SANS Incident Handler's Handbook

Akronymet SANS står for 'SysAdmin, Audit, Network and Security'. SANS-rammeverket ble utviklet av SANS Institute, et privat selskap fra USA som ble grunnlagt i 1989. SANS er en svært troverdig og anerkjent leverandør innen cybersikkerhet, og tilbyr blant annet flere kurs innen hendelseshåndtering.

Alder

SANS Incident Handler's Handbook ble utgitt i 2012, og har blitt jevnlig oppdatert. Siste revisjon er fra 2021 [39].

Struktur

SANS-rammeverket er delt opp i seks adskilte, men sammenhengende faser. Fasene er som følger:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons learned

Preparation

Denne fasen tar for seg ulike metoder sikkerhetsteamet kan forberede seg på å håndtere hendelser. Fasen omfatter også forebyggende tiltak som kan herde infrastrukturen og gjøre den mer motstandsdyktig mot cyberangrep.

Identification

Denne fasen tar for seg identifikasjon av hendelser, og hvordan sikkerhetsteam kan gå fram for å kartlegge omfanget av hendelsen.

Containment

Denne fasen tar sikte på å begrense skadeomfanget av hendelsen. SANS deler fasen inn i korttids- og langtidsbegrensende tiltak.

Eradication

Denne fasen tar for seg sletting av spor fra angrepsaktør, og gjenoppretting av berørte systemer.

Recovery

Denne fasen tar for seg hvordan berørte systemer kan gjenopprettes til produksjon, samt testing, overvåkning og verifisering av systemer.

Lessons learned

Denne fasen omfatter hva en kan lære av håndteringen av sikkerhetshendelsen, og setter deretter søkelys på forbedringspunkter. Eksempler kan være knyttet til rutiner, mangelfull dokumentasjon og ressurser. I tillegg tar fasen for seg prosedyren med dokumentasjon av hendelsen.

Kredibilitet

SANS er et amerikansk selskap som spesialiserer seg på informasjonssikkerhet og cybersikkerhetstrening. SANS er en av verdens mest pålitelige kilder for opplæring innen informasjonssikkerhet og sikkerhetssertifisering [38]. SANS er også i dag verdens største forsknings- og opplæringsorganisasjon for cybersikkerhet. Dette gir selskapet svært god kredibilitet.

2.3.3 Analyse av NIST Incident Handling Guide

Akronymet NIST står for 'National Institute of Standards and Technology'. NIST ble grunnlagt i 1901 og er en offentlig, amerikansk etat underlagt Handelsdepartementet. NIST opererer innen fagområder som blant annet fysikk, kjemi, elektronikk og cybersikkerhet.

Alder

NIST-rammeverket ble først utgitt i 2004 og har siden den gang blitt revidert på jevnlig basis. [29].

Struktur

NIST-rammeverket er delt opp i fire faser. Fasene er som følger:

- Preparation
- Detection and analysis
- Containment, Eradication, Recovery
- Post-incident activity

Strukturen ligner SANS sitt rammeverk, men tredje trinn i NIST sitt rammeverk består av Containment, Eradication, Recovery, der de var adskilt i SANS sitt rammeverk. I NIST sitt rammeverk skal en ikke vente til alle trusler er begrenset før en går videre til utryddelse. Ifølge NIST er utryddelse en prosess som bør utføres fortløpende. [29].

Kredibilitet

Rammeverket til NIST er sammen med SANS sitt rammeverk et av de ledende rammeverkene innen hendelseshåndtering. NIST utvikler cybersikkerhetsstandarder og retningslinjer blant annet for å å møte behovene til amerikanske industrier, føderale byråer og den bredere offentligheten [30]. Et av de største datasikkerhetsteknologiselskapene, Crowdstrike, bruker NIST sitt rammeverk i deres hendelseshåndteringsprosess. [3]. Dette gir dem svært god kredibilitet.

2.3.4 Analyse av ISACA Cybersecurity Incident Response

ISACA er et akronym tidligere kjent som 'Information Systems Audit and Control Assocation', men benytter nå kun akronymet sitt. ISACA er et sertifiseringsprogram for operasjonskontroll hos datasystemer og tilbyr et rammeverk for å gi kunnskap til ulike virksomheter om datasikkerhet og hendelseshåndtering. ISACA har dessuten som målsetning å utdanne virksomheter, og ikke kun være begrenset til et rammeverk. Gjennom ulike metoder å utdanne virksomheter på kan virksomheter motta en ISACA-sertifisering.

Alder

ISACA ble opprettet i 1967 og er et av de fremste og mest anerkjente sikkerhetsrammeverkene i dag. Det er jevnlig vedlikeholdt og blir kontinuerlig forbedret, i takt med stadig mer sofistikerte og cyberangrep. ISACA blir benyttet over hele verden og er standarden hos over 165 000 medlemmer. [8]

Struktur

ISACA sin forretningsmodell går ut på å tilby tjenester innen sikkerhetshendelser. Det er variasjon i tjenestene de tilbyr; noen eksempler på tjenester er opplæring, sertifisering og rådgivning. ISACA sine tjenester baseres på virksomheters ønsker og hva virksomheten har behov for. ISACA tilbyr også veiledning og vurderinger som kan kartlegge hvilke tjenester som egner seg for virksomhetene. [7]

Kredibilitet

ISACA har et godt omdømme og blir benyttet over hele verden, og i over 180 forskjellige land. Rammeverket er standard hos over 165 000 medlemmer. ISACA tilbyr internasjonale godkjente sertifiseringer innenfor IT og sikkerhet. [9]

2.4 Hva gruppen kom fram til

Det eksisterer et utall rammeverk, og alle har unike trekk som skiller seg fra hverandre. I prosessen med å utforme et eget rammeverk ble det vurdert å enten utforme et helt nytt rammeverk fra bunn, eller å basere seg på elementer fra eksisterende rammeverk. Grunnlaget for vurderingen om å utforme et helt nytt rammeverk var å tilpasse rammeverket fullstendig for oppdragsgiver. På en annen side var fordelen med å basere seg på eksisterende rammeverk at de beviselig er kvalitetssikret gjennom bruk av flere store virksomheter. Etter diskusjon med oppdragsgiver valgte gruppen å utføre analyse av noen anerkjente rammeverk. Analysene ledet til en felles enighet om at SANS var rammeverket som var best egnet til å basere utformingen av rammeverket på. Dessuten hadde oppdragsgiver tidligere erfaring fra SANS sine prinsipper.

SANS sitt rammeverk bestod av seks adskilte, men sammenhengende faser. Gruppens målsetning var å gi oppdragsgiver tydelig adskilte faser, som beskrev håndtering av sikkerhetshendelser på en oversiktlig måte. En stor andel av SANS sine ressurser er ikke åpent tilgjengelig, og følgelig kunne ikke en komplett dybdeanalyse av SANS bli utført. SANS sin Incident Handler's Handbook inneholdt riktignok ulike faser med overordnede fokuspunkter, som ga gruppen et godt grunnlag for oppsett og struktur.

Det ble videre bestemt at MITRE ATT&CK skulle være en sentral referansekilde for sikkerhetshendelser. MITRE ATT&CK ble benyttet til å utforme egne beskrivelser av tegn på sikkerhetshendelser for oppdragsgiver. I motsetning til SANS sitt rammeverk er MITRE ATT&CK betydelig mer detaljert. MITRE ATT&CK tilbyr innholdsrike beskrivelse av ulike sikkerhetshendelser. MITRE ATT&CK har også en svært god oversikt over ofte brukte teknikker av angrepsaktører. Disse teknikkene er videre kategorisert i underteknikker.

2.5 Informasjonsinnhenting

Gruppen benyttet forskjellige metoder for informasjonsinnhenting i prosjektet. Møter med oppdragsgiver bygde grunnlaget vårt for informasjonsinnhenting hos virksomheten. Veileder ga også gode føringer underveis, og kom med forslag til ressurskilder.

2.5.1 Intervjuer og møter

Gruppen avholdt ukentlige møter med oppdragsgiver. Enkelte uker var det ikke behov for møte da det ikke forela noen diskusjonspunkter eller nytt materiale å presentere.

I løpet av hele prosjektperioden samlet gruppen spørsmål i et eget dokument som ble besvart og drøftet under møtene med oppdragsgiver.

De fleste møtene med oppdragsgiver foregikk over Microsoft Teams. Det ble også avholdt et fysisk møte hos oppdragsgivers kontorer i starten av prosjektfasen. Under møtene hadde gruppen alltid en leder som førte samtalen, og et medlem som skrev møtereferat. Øvrige gruppemedlemmer bidro til samtalen ved å stille spørsmål.

Gruppen brukte innhentet informasjon fra møtene i utformingen av rammeverket. Det ble blant annet innhentet informasjon relatert til virksomhetens infrastruktur, oppsett og deres ressurskapasitet tilgjengelig for hendelseshåndteringsprosesser. Dessuten ble det kartlagt hvilke sårbarheter og angrepstyper virksomheten var mest utsatt for, og hvilke sikkerhetstiltak de hadde på plass fra før. Tekniske detaljer ble også innhentet.

2.5.2 Krav til kilder

Det ble sjekket at kildene stammet fra anerkjente og pålitelige utgivere. Et eksempel på en pålitelig utgiver er Nasjonal sikkerhetsmyndighet (NSM). NSM er Norges ekspertorgan for informasjonssikkerhet og er det nasjonale fagmiljøet for IKT-sikkerhet [31]. Dette gjør informasjon fra NSM svært pålitelig. Om det var usikkerhet knyttet til kildens pålitelighet ble det gjort sammenligninger mot andre kilder for å avgjøre om innholdet var av relevans og mulig å ta i bruk. Denne tilnærmingen til kildekritikk skulle bidra til å utforme prosjektoppgaven av tilfredstillende kvalitet.

2.6 Utvikling av rammeverk

Dette kapittelet beskriver hvordan gruppen gikk fram for å utvikle rammeverket for oppdragsgiver. Kapittelet inneholder krav, struktur og kvalitetssikring. I tillegg redegjøres det for hvilke avgjørelser gruppen tok innholdsmessig i utviklingen av rammeverket.

2.6.1 Krav

Rammeverket ble utformet for å gi oppdragsgiver bedre hendelseshåndteringsrutiner. Det var noen krav som ble fulgt i utviklingen av rammeverket for å oppnå det. Kravene var som følger:

- Innholdet skulle være utfyllende og forståelig for oppdragsgiver
- Innholdet måtte være av høy kvalitet
- Innholdet måtte være pålitelig
- Innholdet måtte stamme fra forskningsbasert teori
- Det måtte bli referert til kilder der det var nødvendig
- Fasene måtte følge hverandre kronologisk

2.6.2 Struktur

En av årsakene til at SANS sitt rammeverk ble brukt som inspirasjon var at rammeverket hadde en klart definert struktur adskilt i faser. SANS sitt rammeverk er totalt delt opp i seks faser med sitt eget formål. Gruppen valgte å følge denne strukturen. Fasen inneholdt kun overordnede anbefalinger, og det var opp til gruppen å konkretisere hver enkelt fase med forskjellige seksjoner. De engelske navnene på fasene er beholdt. På den måten blir det enklere for virksomheten å relatere elementer fra de ulike fasene til SANS og andre aktuelle rammeverk.

Jf. seksjon 2.3.2 for mer informasjon om fasene.

2.6.3 Innholdsmessige avgjørelser

I samråd med oppdragsgiver ble det foretatt avgjørelser for å avgrense omfanget av oppgaven. Det ble blant annet besluttet å avgrense omfanget til det oppdragsgiver vurderte til å ha størst risiko for virksomheten. Oppdragsgiver konkluderte med at virksomheten var mest utsatt for løsepengevirus- og phishingangrep, og rammeverket ble således utformet med fokus på disse angrepene. Rammeverket omfattet også mer generelle angrep.

Gruppen avtalte med oppdragsgiver å utelate regulatoriske retningslinjer og håndtering av media da dette ikke var relevant for oppgaven. Oppdragsgiver hadde dessuten noen regulatoriske retningslinjer definert fra før. Prosedyrer for 'kartlegging av sårbarhetsflate' og 'kriminalteknisk image' i rammeverket er ikke utformet da det krever svært tekniske beskrivelser, og faller utenfor prosjektoppgavens omfang.

Det var ikke nødvendig å inkludere alle typer for phishingangrep. De mest utbredte formene for phishingangrep som e-postphishing, smishing og spear phishing er inkludert. Mindre vanlige phishingangrep som for eksempel vishing er ikke tatt med.

2.6.4 Kvalitetssikring

Kvalitetssikring av arbeidet ble utført for å påse at kvaliteten av rammeverket tilfredsstilte kravene. Etter ferdigstillelse av en fase ble det oversendt et utkast til veileder og oppdragsgiver. Veileder og oppdragsgiver kunne dermed gi tilbakemelding på innhold som kunne endres eller fjernes. Tilbakemeldingene bisto i forbedringen av rammeverket, og sørget for god forventningsavklaring underveis. Det ble dessuten utført flere kvalitetssikringsgjennomganger av medlemmer i gruppen.

2.7 Utvikling av treningsopplegg

Dette kapittelet handler om hvordan gruppen gikk fram for å utvikle treningsopplegget for IT-personellet til oppdragsgiver. Kapittelet inneholder krav, hvorfor gruppen valgte et slikt treningsopplegg og kvalitetssikring.

Jf. seksjon 4.1 for mer informasjon om prosessen av denne øvelsen.

2.7.1 Krav

Et krav for øvelsen var at det skulle være lett å forstå og med mulighet for interaktiv læring der alle spillerne deltar aktivt. Det var viktig at øvelsen trente deltakerne i hvordan en kan gå frem for å løse en hendelse. Dessuten skulle deltakerne se nytteverdien av å ha klart definerte prosedyrer på plass før en hendelse oppstår.

Et annet krav for øvelsen var at den ikke skulle ha for lang varighet. En øvelse med for lang varighet kan føre til at deltakere mister motivasjon og fokus, og dermed gi mindre læringsutbytte.

Innholdet i treningsopplegget måtte være av høy kvalitet, og stamme fra forskningsbasert teori. Om innholdet ikke stammet fra forskningsbasert teori måtte gruppen ha gode argumentasjoner for hvorfor det ble inkludert.

2.7.2 Hvorfor gruppen valgte et slikt treningsopplegg

Gruppen ønsket å gi oppdragsgiver et treningsopplegg de kunne bruke kontinuerlig. Gruppen gjorde det videre mulig å utvide treningsopplegget og tilpasse det etter eget behov. Det gjorde det blant annet mulig for oppdragsgiver å oppdatere treningen med nye angrepsaktører eller -vektorer. Det er utformet en mal på hvordan en kan innføre nye angrepsvektorer i øvelsen.

Gruppen ønsket dessuten å utforme et underholdende treningsopplegg for å engasjere deltakerne. Gruppen tok derfor inspirasjon fra et treningsopplegg fra 'Backdoors and Breaches' og andre Dungeons & Dragons-spill [45]. Dungeons & Dragons er et rollespill med deltakere som går frem for å løse problemer og blir vanligvis benyttet til å fortelle fiktive fortellinger. Fortellingen blir presentert av en leder, og resten av deltakerne går frem for å løse problemet. Ved å spillifisere tabletop-øvelsen kan det gjøre læringsopplevelsen mer underholdende og engasjerende, men samtidig lærerik [37].

2.7.3 Kvalitetssikring

Treningsopplegget ble revidert av medlemmene i gruppen og deretter presentert og diskutert med oppdragsgiver. Det ble foretatt en del endringer i revisjonene etter diskusjon. Endringene ble foretatt for å tilpasse treningsopplegget mer for oppdragsgiver og få det til å henge sammen med rammeverket.

3 Utforming av rammeverk

Dette kapittelet handler om utformingen av rammeverket. Kapittelet består av rammeverkets innhold og presenterer rammeverkets faser i kronologisk rekkefølge.

Rammeverket gruppen utformet er inspirert av anerkjente rammeverk som benyttes internasjonalt. Analysen gruppen utførte ledet til SANS som hovedrammeverk å hente inspirasjon fra. MITRE ATT&CK ble benyttet som en database for sikkerhetshendelser, som rammeverket kunne referere til.

Rammeverket er basert på SANS sine seks faser for håndtering av sikkerhetshendelser. Gruppen valgte å sentrere oppgaven rundt SANS på grunn av oppdragsgivers kjennskap til deres prinsipper, og fordi SANS hadde en enkel og oversiktlig struktur.

3.1 Rammeverkets faser

Fasene i rammeverket er som følger:

3.1.1 Preparation

'Preparation' var den første fasen i rammeverket, og tok for seg ulike sikkerhetsmekanismer og andre forbyggende tiltak som kan bidra til å redusere risikoen for at sikkerhetshendelser oppstår. 'Preparation' var den mest omfattende fasen og bestod av til sammen ni kapitler. Kapitlene er som følger:

- Revisjonsplan
- Rutiner
- Policy
- Sikring av infrastruktur
- Kartlegging av sårbarhetsflate
- Definisjon av hendelser

- Klassifisering og prioritering av hendelser
- Kommunikasjonsplan
- Team og roller

Revisjonsplan

Revisjonsplanen ble plassert i 'Preparation', men omfatter rammeverket i sin helhet. Revisjon kan utføres på hele eller deler av rammeverket. Formålet med revisjonsplanen er å sikre at rammeverket blir kontinuerlig oppdatert. Det ble bestemt at rammeverket skal gjennomgå revisjon minst én gang i året, og ellers ved behov. En prosedyre for revisjon av hele rammeverket er ikke definert, og må utformes av virksomheten selv. Det er blant annet beskrevet når revisjon skal utføres for 'kommunikasjonsplan' i 'Preparation'-fasen. Videre bør for eksempel rammeverket revideres dersom virksomheten ser behov for å legge til elementer i 'forhåndsdefinerte handlingsmønstre'. Etter en hendelseshåndteringsprosess skulle teamet benytte 'Lessons learned'-fasen til å avgjøre hvorvidt det var behov for en revisjon av deler av rammeverket.

For selve revisjonsprosessen utformet gruppen en mal som teamet kunne benytte i deres revisjonsprosess:

Malen var som følger, med eksempler:

Hva må forbedres	**Hvordan skal det forbedres**	**Hvem er ansvarlig**	**Når skal tiltaket senest gjennomføres**	**Hvem skal følge opp tiltaket**
Kommunikasjon	Opplæring av ansatte	Kriseleder	03.09.2022	Kriseleder
E-posthåndtering	E-læringskurs	IT-personell	21.04.2022	Kriseleder

Tabell 1: Oversikt over revisjonstiltak

Revisjonsprosessen inkluderte også en mal for å følge opp at tiltakene ble gjennomført. Malen var som følger, med eksempler:

Hvilken hendelse ble revisjonen gjennomgått for (med saksnr.)	**Revisjonsdokument opprettet**	**Er revisjon fulgt opp og lukket**
Phishing (001)	Revisjonsdokument om phishing, 01.04.2022	Ja
Løsepengevirus (002)	Revisjonsdokument om løsepengevirus, 04.08.2021	Nei

Tabell 2: Oppfølging av revisjon

Rutiner

Kapittelet om rutiner tar for seg tre rutiner for informasjonssikkerhet som har som målsetning å redusere sårbare inngangssvektorer. De tre rutinene er som følger:

- Sikkerhetskopiering
- Gjennomgang av åpne og lukkede kilder
- Håndtering av kjente sårbarheter

Sikkerhetskopiering av data er en viktig rutine for å være i stand til å gjenopprette systemer og tjenester etter en hendelse. Det er derfor avgjørende at virksomheten har en godt definert og planlagt prosess. Aktiviteter som bør defineres er hva som skal sikkerhetskopieres, hyppighet på sikkerhetskopieringen, hvilken sikkerhetskopi type som skal kjøres og når, og hvilke instanser som kjører sikkerhetskopiene.

For å få en oversikt over dette ble følgende tabell utformet:

System	CIA-score	Hyppighet på sikkerhetskopi	Type sikkerhetskopi (full, inkrementell, differensiell)	Instanser som kjører kopieringen

Tabell 3: Tabell for oversikt over backup

Kolonnen 'system' refererer til hva som skal sikkerhetskopieres. CIA-score er hentet fra kapittelet 'klassifisering og prioritering av hendelser'. 'Type sikkerhetskopi' kan enten være full, inkrementell eller differensiell. 'Instanser som kjører kopieringen' refererer til de instansene sikkerhetskopiene kjører på.

Det anbefales videre at virksomheten utformer en plan for testing av gjenoppretting. Mal for sikkerhetskopiering kan benyttes som grunnlag, og tilpasses etter behov.

Åpne kilder er offentlig tilgjengelig data om cybertrusseletterretning, og kan brukes av sikkerhetsteamet til å holde seg oppdatert på trusselbildet. Lukkede kilder kan dessuten ofte gi informasjon om kompromitterte brukerdetaljer. Å ha en god rutine på dette er viktig for å kunne respondere hurtig til sikkerhetshendelser. Det ble utformet et forslag til liste over åpne og lukkede virksomheten kan benytte, men denne listen er utelatt fra rapporten av konfidensialitetshensyn.

Den tredje rutinen beskriver håndtering av kjente sårbarheter, ofte forkortet til CVE-[tallkode], som har blitt varslet om i virksomhetens system [27]. Virksomheten bør selv utforme en rutine for oppfølging og håndtering av disse sårbarhetene.

Policy

Kapittelet om policy omfatter retningslinjer IT-personell og vanlige ansatte må forholde seg til for å sikre forsvarlig IT-bruk i virksomheten. Kapittelets underkapitler var som følger:

- Generell informasjon
- Varsling av hendelser
- Brukeradministrasjon (med fire underkapitler)
- Passordhåndtering (med to underkapitler)
- E-posthåndtering
- Nettverk (med to underkapitler)
- Tredjepart (med tre underkapitler)
- Utstyr (med to underkapitler)

Kapittelet trekker frem hovedessensen fra kapittelet da denne delen av rammeverket var så omfattende at gruppen valgte å ikke beskrive den i detalj i sluttrapporten.

'Generell informasjon' listet informasjon brukere må gjøre seg kjent med. Det var informasjon knyttet til blant annet bruk av sosiale medier, kildekritikk, spam, lagring av data og overvåkning. Hensikten med kapittelet var å bevisstgjøre brukere på hvordan en bør opptre i det digitale rom, og for å redusere risikoen for at sluttbrukere blir en inngangsvektor for cyberangrep.

'Varsling av hendelser' var en policy for ansatte og underleverandører knyttet til deres ansvar om å varsle om sikkerhetsrelaterte hendelser. Det beskrives også hvilke kommunikasjonskanaler som kan være hensiktsmessig i ulike typer hendelser.

I 'Brukeradministrasjon' definerte gruppen en policy om å fase ut foreldede brukere. Inaktive brukere tar opp plass og øker kompleksiteten til systemet, og kan i verste fall være en

inngangsvektor til cyberangrep. Det ble videre definert hvordan virksomheten skal håndtere høyprivilegerte brukere, som for eksempel administratorkonti som domeneadministratorer og tjenestebrukere. Tilnærmingen gruppen valgte var prinsippet om 'least privilege', for å sikre at ingen brukere hadde mer rettigheter enn nødvendig.

For 'Passordhåndtering' ble det utarbeidet en policy for IT-personell, og en policy for sluttbrukere.

For IT-personell ble det satt krav til hvordan passord skulle bli distribuert. Passordet skulle bli sendt på SMS eller kryptert e-post. Det måtte også foretas en autentisering av personen før distribusjon av passordet. Videre skulle personen som fikk passordet bekrefte at passord var mottatt.

Multifaktorautentisering var også et krav for alle brukere.

For sluttbrukere ble det definert mer generelle passordkrav. Noen krav var som følger:

- Ikke tillatt med gjenbruk av passord. Samme passord kan ikke benyttes på ulike systemer tilknyttet virksomheten. Det er heller ikke tillatt å benytte passord i bruk på private tjenester.
- Ikke tillatt å oppbevare passord i fysisk form.
- Hyppighet på passordendring,
- Kriterier som må oppfylles for å sette passord. Disse kriteriene er utelatt fra rapporten av konfidensialitetshensyn.
- Kompromittert konto må endre passord umiddelbart. Skal rapporteres til IT-personell.
- Passord skal aldri deles med noen, uansett årsak.

'E-posthåndtering' beskriver viktigheten av å ha tydelige retningslinjer for e-post. Dette grunner i at e-post er en av de største inngangsvektorene for phishingangrep [1].

Noen retningslinjer var som følger:

- E-post skal kun benyttes til arbeidsrelatert arbeid.
- E-post skal ikke benyttes til privat kommunikasjon.
- Ikke tillatt med ppsett av privat e-postkonto.

I 'Nettverk' ble overordnede retningslinjer definert. Noen etningslinjer var som følger:

- Bruk av internett skal i hovedsak benyttes til jobbrelatert arbeid.
- Virksomhetens etiske retningslinjer og policy for sosiale medier skal følges.
- Installasjon av programvare skal gjøres i samråd med IT.
- Kun lisensiert programvare er tillatt.
- Alle endepunktsklienter skal være sikret med antivirusprogram.
- Segmenterte nettverk må være satt opp. Gjestenettverk skal benyttes for eksterne brukere.

I 'Lagring' ble det det bestemt at arbeidsrelatert data kun skal lagres på virksomhetens delte lagringsområder. Ved å følge denne policyen kan en hindre at arbeidsrelatert data går tapt eller havner på avveie. Det vil også sørge for at data er enkelt tilgjengelig via løsninger som VPN.

Videre ble det bestemt at ikke-arbeidsrelatert data ikke skal lagres på virksomhetens delte lagringsområder. Det vil spare virksomheten for lagringsplass, og kan forhindre at private, infiserte filer påvirker nettverket.

Flyttbare medier som minnepenner og eksterne disker er ikke tillatt å koble til nettverket med mindre de er klarert og godkjent av IT-personellet.

I 'Ekstern tilgang' ble retningslinjer knyttet til tilgang fra eksterne nettverk definert.

For bruk av fjernstyringsprogramvare av IT-personell skal kun godkjent programvare benyttes. Programvaren skal sikres med tofaktorautentisering, og det skal være et koblingsbrudd etter en gitt periode med inaktivitet.

For eksterne konsulenter skal de gis tilgang til et segmentert nettverk, og må logge inn ved bruk av tofaktorautentisering. Eksterne konsulenter skal kun gis de rettighetene de behøver, og tilgang skal stenges umiddelbart etter at oppdraget er fullført.

I 'Tredjepart' ble det definert hvordan brukere skal behandle utstyr og enheter, applikasjoner og systemer levert av en tredjepartsleverandør.

For applikasjoner skal virksomheten ha en liste over godkjente applikasjoner. Det er kun disse applikasjonene som er tillatt å installere, og det er IT-personellet som har ansvar for installasjon.

Eksterne brukere må benytte tofaktorautentisering. Eksterne brukere defineres som brukere som ikke er tilknyttet konsernet, men bistår virksomheten. Det betyr at brukere underordnet en av virksomhetens bransjer eller divisjoner vil inngå som en intern bruker. Gjestebrukere skal opprettes via virksomhetens portal, og brukere som ikke lenger er aktive eller behøver tilgang må deaktiveres umiddelbart. Referer til virksomhetens rutine for oppsett av gjestebruker.

Kapittelet om 'Utstyr' tar for seg retningslinjer relatert til utstyr benyttet i virksomhetens nettverk eller i sammenheng med selskapets verdier og/eller tjenester. Kapittelet er delt opp i internt utstyr og eksternt utstyr.

Internt utstyr er definert som alt utstyr godkjent og distribuert av virksomheten til sine brukere. Med distribusjon menes utstyr virksomheten selv har kjøpt inn eller mottatt via godkjent tredjepartsleverandør. Disse enhetene skal klargjøres for bruk i selskapets nettverk og skal primært benyttes til jobbrelatert arbeid. Det er sterkt oppfordret til å unngå oppsett av private e-postkonti, og lagring av private filer på disse enhetene er forbudt.

For endepunktsklienter som ikke kan meldes inn i domenet bør virksomheten utarbeide en kravliste som må være oppfylt for at enhetene kan benyttes i nettverket. Kravlisten kan inneholde krav til blant annet antivirusprogram, tilgangsrettigheter og oppdateringsrutiner.

Eksternt utstyr er definert som utstyr som ikke er eid av virksomheten selv, men er tilknyttet virksomhetens nettverk. Eksempler på eksternt utstyr er enheter tilhørende underleverandører eller kunder på gjestebesøk, eller eksterne konsulenter koblet til via VPN. Eksternt utstyr skal tilkobles gjestenettverk eller et eget, separat nettverk, og skal aldri være tilkoblet samme nettverk som internt utstyr.

Sikring av infrastruktur

Dette kapittelet handler om hvordan virksomheten kan sikre deler av infrastrukturen sin. Kapittelet tar hovedsakelig for seg ulike sikkerhetsmekanismer for e-post ettersom e-post er en svært populær inngangsvektor for angripere. Gruppen gjorde seg derfor kjent med sikkerhetsmekanismene og utformet en kort og forklarende beskrivelse av deres nytteverdi.

Sender Policy Framework (SPF)

Den første sikkerhetsmekanismen for e-post var Sender Policy Framework (SPF). SPF er en standardmetode for e-postautentisering og bidrar til å beskytte domenet mot forfalskning eller såkalt 'spoofing'. SPF spesifiserer e-postservere som har lov til å sende e-post på vegne av domenet. Mottakende e-postservere benytter deretter SPF til å verifisere at innkommende e-poster som ser ut som de kom fra domenet faktisk ble sendt fra e-postservere som er autorisert.

SPF stopper riktignok ikke all uønsket trafikk. En kompromittert e-postkonto som tilhører en virksomhet som benytter SPF kan passere en SPF-sjekk. Uønskede e-poster som blir sendt på vegne av domener som ikke benytter SPF vil dessuten ikke fanges opp i en SPF-sjekk.

DomainKeys Identified Mail (DKIM)

Den andre sikkerhetsmekanismen for e-post var DomainKeys Identified Mail (DKIM). DKIM er en standardmetode for e-postautentisering som legger til en digital signatur til utgående e-poster. Mottakende e-postservere vil kunne verifisere at e-posten faktisk kom fra avsenderen den utgir seg for å være. DKIM sjekker også etter om innholdet i e-posten har blitt endret. Med DKIM vil en kunne forbedre sannsynligheten for at legitime e-poster blir levert til mottakere. Mottakende e-postservere kan verifisere at e-poster faktisk kom fra domenet, og ikke er forfalsket.

Domain based Message Authentication, Reporting and Conformance (DMARC)

Den tredje sikkerhetsmekanismen for e-post for Domain based Message Authentication, Reporting and Conformance (DMARC). DMARC benyttes i kombinasjon med SPF og DKIM. Dersom en benytter DMARC vil andre som mottar e-post enklere kunne avgjøre om den faktisk er sendt fra avsender den utgir seg for å være. En vil også kunne motta rapporter for å avgjøre hvorvidt domenet blir misbrukt.

STARTTLS

Videre anbefalte gruppen å implementere STARTTLS. STARTTLS er en beskyttelsesmekanisme for overføring av e-post mellom e-posttjenere. STARTTLS sørger for autentisering av e-posttjenere og sikrer konfidensialitet [32].

DNS Security Extensions (DNSSEC)

DNSSEC er en sikkerhetsmekanisme som blir lagt inn i domenenavnsystemet. DNSSEC signerer svar på et domeneoppslag slik at en kan kontrollere at de kommer fra riktig kilde og sikre at de var uendret underveis. Svar på domeneoppslag blir signert kryptografisk.

Multifaktorautentisering

Multifaktorautentisering legger til et ekstra beskyttelseslag for innloggingsprosessen. Eksempler på multifaktorautentisering er SMS eller kode via applikasjoner som Google Authenticator. Gruppen anbefalte å innføre multifaktorautentisering på alle systemer i virksomheten. Multifaktorautentisering kan blant annet forhindre uautorisert tilgang dersom passord havner på avveie.

Deaktivering av eldre autentiseringsprotokoller

Eldre autentiseringsprotokoller som POP3, IMAP og IWS støtter ikke multifaktorautentisering. Det anbefales derfor å deaktivere disse protokollene.

Deaktivering av automatisk videresending til eksterne domener

Automatisk videresending til eksterne domener kan føre til at sensitiv informasjon havner utenfor virksomheten. Det anbefales derfor å deaktivere automatisk videresending til eksterne domener.

Kartlegging av sårbarhetsflate

Formålet med dette kapittelet var å utforme en prosess for kartlegging av virksomhetens sårbarhetsflate. Med sårbarhetsflate menes summen av inngangsvektorer en ondsinnet aktør kan utnytte til kompromittering eller forsøk på kompromittering av virksomhetens systemer. Sår-

barhetsflaten er dynamisk og endrer størrelse ettersom nye systemer blir faset inn, oppdatert, endret eller faset ut. Bedre kontroll over virksomhetens sårbarhetsflate vil bidra til å redusere risikoen for angrep da aktørens potensielle inngangsvektorer blir færre eller bedre sikret.

Sårbarhetsflaten vil vokse ettersom virksomheten implementerer flere systemer for å imøtekomme krav knyttet til vekst på antall brukere, nye kundeforhold eller andre krav til den digitale plattformen. For å kunne forstå og behandle sårbarhetsflaten bør virksomheten utforme en kravliste til sine enheter og systemer. Det vil også være hensiktsmessig å utforme en oversikt over systemer, nettverk og integrasjoner i virksomheten. På den måten kan virksomheten systematisk kartlegge hvilke sårbarheter som eksisterer i systemet, og arbeide for å fortløpende minimere sårbarhetsflaten. En detaljert prosess av denne kartleggingen er ikke beskrevet i rammeverket da den falt utenfor gruppens definerte omfang.

Definisjon av hendelser

I dette kapittelet ble det utformet definisjoner for relevante hendelser som kan ramme virksomheten. Virksomheten identifiserte at det var løsepengevirus- og phishingangrep som var mest relevant, og følgelig var hovedfokuset på disse to angrepstypene.

Noen utvalgte definisjoner av inngangsvektorer var som følger:

- E-post(vedlegg)

  Phishingforsøk via e-post er svært utbredt. Angrepsaktør vil gjerne lokke mottaker til å trykke på en ondsinnet lenke. Lenken kan åpne nettsider hvor den ber bruker om å logge inn, som kan føre til blant annet at brukerdetaljer havner på avveie eller at bruker laster ned ondsinnet programvare, som for eksempel løsepengevirus.

- Kompromitterte eller aktørstyrte nettsider

  Det finnes nettsider som utgir seg for å være legitime. Disse nettsidene kan lure sluttbrukere til å tro at de laster ned legitim programvare som i realiteten er skadevare. Nettsidene kan også etterligne påloggingssider som for eksempel Office 365 sin påloggingsportal.

- Skytjenester

  Kompromitterte skytjenester kan inneholde infiserte filer som kan laste ned løsepengevirus på enheten om de åpnes.

- Flyttbare medier

  Flyttbare medier som en USB-minnepenn kan føre til at enheter blir infisert av løsepengevirus.

Klassifisering og prioritering av hendelser

Dette kapittelet beskrev hvordan virksomheten kunne klassifisere og prioritere sikkerhetshendelser. Klassifiseringen vil gi virksomheten innsikt i beskyttelseskravene for sine systemer med hensyn til konfidensialitet, integritet og tilgjengelighet. Denne prosessen vil gi virksomheten bedre oversikt over systemene som blir påvirket under diverse angrep, og vil gi et grunnlag for prioritering av eventuelle hendelser.

Gruppen utformet en tabell for å klassifisere systemer basert på akseptabel nedetid. Akseptabel nedetid ble bestemt i samråd med oppdragsgiver. Systemer vil få en lavere prioritet under en hendelse dersom det er aksept for lengre nedetid.

	Lav	**Middels**	**Høy**	**Kritisk**
Tilgjengelighetsnekt	Over 24 timer	5 timer til 24 timer	30 minutter til 5 timer	0 til 30 minutter

Tabell 4: Klassifisering av tilgjengelighet

Gruppen utformet videre en tabell for å klassifisere konfidensialiteten til systemer. Denne tabellen kan benyttes som en pekepinn til å bestemme hva en skal prioritere under en hendelse. I tabellen ser vi hva som klassifiseres fra lav til kritisk. Lav har ganske åpen tilgjengelighet til informasjon og kritisk har strengt fortrolig informasjon. Tabellen var som følger:

	Lav	**Middels**	**Høy**	**Kritisk**
Konfidens-ialitet	Åpen tilgjengelig-het, altså informasjo-nen er tilgjengelig for alle uten særskilte tilgangsret-tigheter	Informasjonen har beskyttelse til en grad, men både interne og eksterne kan få tilgang til den	Informasjonen har strenge tilgangsret-tigheter og tap av konfi-densialitet kan forårsake skade på virksomhe-ten	Informasjon har strenge tilgangsret-tigheter og tap av konfi-densialitet kan forårsake betydelig skade på virksomhe-ten og andre interesser

Tabell 5: Klassifisering av konfidensialitet

Det ble også utformet en tabell for å klassifisere integriteten til systemer. Denne tabellen brukes for å vurdere systemets krav til integritet. Systemer som har minimal påvirkning og passer beskrivelsen for lav integritet får lav prioritering, mens systemer med høye krav til integritet får høyere prioritering. Tabellen var som følger:

	Lav	**Middels**	**Høy**	**Kritisk**
Integritet	Minimal påvirkning hvis informasjon er unøyaktig eller ufullstendig	Kan bli noe berørt ved tap av integritet, men situasjonen kan enkelt bli oppdaget og gjenopp-rettet	Tap av integritet vil føre til betydelig skade eller forstyrrelser og kan føre til stopp av arbeid. Er også vanskelig å oppdage	Ingen tap av integritet er tolerert og tap av integritet her kan føre til stor skade

Tabell 6: Klassifisering av integritet

Videre ble det benyttet enda en tabell for å gi bedre oversikt over systemene og hvordan de er vurdert på konfidensialitet, integritet og tilgjengelighet. Virksomheten setter inn hvilket system eller verdi som har blitt vurdert inn i kolonnen helt til venstre med navn 'system/verdi', deretter setter en verdiene for konfidensialitet, integritet og tilgjengelighet fra vurderingene en utførte tidligere. Totalscoren er satt lik den høyeste verdien for enten konfidensialitet, integritet eller tilgjengelighet. Scoren er parameteren systemene skal rangeres etter.

Mal for tabellen var som følger:

System/verdi	Konfidensialitet	Integritet	Tilgjengelighet	Score

Tabell 7: CIA-tabell

Det ble også utformet en tabell for å klassifisere selve angrepet og sette en alvorlighetsgrad. Alvorlighetsgraden går fra S1-S4 der S1 har liten påvirkning på virksomheten og S4 har svært høy påvirkning på virksomheten. Tabellen var som følger:

Alvorlighetsgrad	Beskrivelse
S1	Ikke alvorlig, liten effekt på kritiske systemer, ingen kompromittert data. burde være oppmerksom på det og ev. overvåke.
S2	Mindre alvorlig, kan komme seg inn i systemer og kompromittere en liten mengde data, bør planlegge tiltak.
S3	Alvorlig, hendelsen kan levere skadevare som påvirker kritiske systemer i fremtiden, sensitiv data har blitt kompromittert, tiltak burde implementeres snarest.
S4	Svært alvorlig, kritiske systemer er svært utsatt for kompromittering, tiltak må implementeres umiddelbart.

Tabell 8: Klassifisering av angrep

Til slutt ble det utformet en tabell for en helhetlig klassifisering av hendelsen. Nedenfor er en mal med eksempler på hvordan hendelsen i sin helhet kan vurderes. Malen bistår med å visualisere hendelsen og systemene som blir påvirket. Scoren skal regnes ut ved å gange CIA-scoren med alvorlighetsgraden til angrepet. Om alvorlighetsgraden er S1 skal CIA-scoren ganges med 1, om graden er S2 skal det ganges med 2 og så videre.

Følgende er tabellen:

System	**CIA score**	**Angrepstype**	**Alvorlighetsgrad**	**Score**

Tabell 9: Klassifisering av hendelse

Kommunikasjonsplan

I dette kapittelet beskrives prosedyren for kommunikasjon i en hendelse. Det følger også en oversikt over en intern og ekstern varslingsliste, samt rutiner for periodevis revisjon av kommunikasjonsplanen og i andre tilfeller dette må gjennomføres, eksempelvis etter en større hendelse, i etterkant av trening av IT-personell eller ved endring av kontaktpersoner. Avslutningsvis beskrives konkrete tiltak for hendelser av spesifikke klassifiseringstyper.

Kommunikasjonsprosedyren vil avhenge av hvilken klassifisering hendelsen blir tildelt. En hendelse kan bli klassifisert fra S1 til S4, der S1 har lavest alvorlighetsgrad og S4 har høyest alvorlighetsgrad.

Revisjonsplan

Kommunikasjonsplanen skal gjennomgå revisjon etter håndtering av en større hendelse. En større hendelse er definert som S3 eller S4. Dessuten gjennomføres det som et minimum en årlig revisjon av hele rammeverket, hvor kommunikasjonsplan inngår som en del av dette.

Følgende er et eksempel på oversikt over kommunikasjonskanaler:

Kommunik-asjonskanaler	**Tilgjengelig på**	**Lav/middels/ kritisk**	**Beskrivelse**
Portal	URL her	S1	Generelle spørsmål
E-post	E-postadresse her	S1	Phishing
Telefon	Telefonnummer her	S2, S3 og S4	Benyttes for alvorlige hendelser som er tidssensitive
Programvare for distribusjon av informasjon til ansatte	URL her	S2	Benyttes for distribusjon av informasjon til alle ansatte. Det eksisterer ingen alternativ kanal, men det er eventuelt mulig å massesende SMS til alle.
Dedikert fysisk møterom for internkommuni-kasjon	Arbeidsrom / Grupperom	S3 og S4	For intern diskusjon av alvorlige hendelser
Dedikert virtuelt møterom for kontakt med eksterne	Virtuelt møterom	S3 og S4	For diskusjon med eksterne under alvorlige hendelser

Tabell 10: Eksempel på utfylling av kommunikasjonskanaler

Intern varslingsliste

Den interne varslingslisten inneholder en komplett oversikt over tilgjengeliggjort personell i en sikkerhetshendelse. Listen er en oversikt over ulike roller, og er ikke personavhengig. Hvem som besitter hvilken rolle kan endres avhengig av virksomhetens ressurser og behov.

Oversikten omfatter fullt navn, telefonnummer, e-postadresse, rolle og foretrukket kontaktmåte.

Fullt navn	**Telefon**	**E-postadresse**	**Rolle**	**Foretrukket kontakt-måte**
Petter Persen	992 00 102	Petter @gmail.com.	Leder	E-post
Johan Per	921 12 213	johan @gmail.com	Sikkerhets-leder	Telefon
Anna Per	902 12 345	anna @gmail.com	IT utvikler	E-post
Ola Petter	902 11 341	ola @gmail.com	IT utvikler	Telefon

Tabell 11: Eksempel på utfylling av intern varslingsliste

Ekstern varslingsliste

Den eksterne varslingslisten inneholder en komplett oversikt over kontaktpersoner til virksomhetens underleverandører. Kontaktpersonene er knyttet opp mot applikasjoner eller utstyr levert til virksomheten, og kan bistå med systemkompetanse i en hendelse.

Oversikten over fullt navn, telefonnummer, e-postadresse, system og leverandør.

Navn	**Telefon**	**E-post**	**System**	**Leverandør**
Per Pettersen	915 00 123	per @gmail.com	Brannmur	Leverandør A
Ole Nord	932 23 432	ole @gmail.com	Kjerneswitch	Leverandør B
Henrik Petter	902 32 332	henrik @gmail.com	Strøm / Aggregater	Leverandør C
Jesper Nord	915 46 543	jesper @gmail.com	Brannmur	Leverandør D

Tabell 12: Eksempel på utfylling av ekstern varslingsliste

Eskalering av hendelse

Dersom hendelsen faller under klassifisering S3 eller S4 vil den vurderes til å ha en middels til høy alvorlighetsgrad. I dette tilfellet må virksomheten opprette en dedikert kanal for kommunikasjon. Kanalens formål begrenser seg dermed til hendelsen. Opprettelse av dedikert kanal gjøres gjennom virksomhetens foretrukne kommunikasjonsverktøy.

Kapittelet kan seneres utvides til å beskrive konkrete tiltak for andre klassifiseringer. Det kan også suppleres med flere tiltak for S3- eller S4-hendelser isolert, eller i kombinasjon med hverandre.

Team og roller

Dette kapittelet definerte ulike roller virksomheten kan ta i bruk under en sikkerhetshendelse, og rollenes ansvarsområder. I de senere fasene følger et kapittel for 'koordinering av team', og disse kapitlene beskriver i detalj hvilke ansvarsområder de ulike rollene innehar.

Teamet ble delt opp i fire hovedroller. En rolle var ikke begrenset til et antall personer, og flere personer kunne inneha samme rolle. Rollene var som følger:

- Triage-ansvarlig
- Hendelsesleder
- Hendelseshåndterer
- IT- og infrastruktur-ansvarlig

Ansvarsområdet til triage-ansvarlig under 'Preparation'-fasen er å følge med på innkommende varsler og saker som rapporteres inn, for å vurdere hvor kritisk hendelsen er og om det er hensiktsmessig å påbegynne en hendelseshåndteringsprosess. Triage-ansvarlig skal utføre denne analysen basert på vurdering av angrepets alvorlighetsgrad og verdivurderingen til systemet som er utsatt. Dersom hendelsen viser seg å være kritisk nok skal hendelsen tilordnes en alvorlighetsgrad ved bruk av tabellene i 'klassifisering og prioritering av hendelser', og hendelsesleder skal varsles. Et utklipp fra rammeverket av sjekklisten for triage-ansvarlig var som følger:

- Avgjøre hvorvidt hendelsen er kritisk nok til å påbegynne hendelseshåndteringsprosess
- Loggføre hendelsen. Det er viktig at triage-ansvarlig legger til så mye informasjon som mulig. Dette vil forenkle prosessen videre.

Oppgavene beskrevet i rammeverket for hendelseslederen er å påbegynne hendelseshåndteringsprosessen etter at hendelsen har blitt definert og rapportert av triage-ansvarlig. Videre skal hendelsesleder ha ansvar for å følge opp og holde oversikt over hendelsens utviklingsløp inntil den er ferdighåndtert. Det gjøres gjennom kommunikasjon internt med sikkerhetsteamet og til

eksterne interessenter. Hendelsesleder må også sørge for at all viktig informasjon, hypoteser og beslutninger blir dokumentert. Hendelsesleder har ansvar for at kritiske hendelser blir rapportert videre til ledelsen, med kritiske hendelser menes hendelser av alvorlighetsgrad S3 og S4.

Jf. tabell 8 for mer informasjon om alvorlighetsgrad.

Et utklipp fra rammeverket av sjekklisten for hendelseslederen var som følger:

- Overordnet ansvar for hendelseshåndteringen fra start til slutt
- Delegere oppgaver til alle roller som inngår i teamet
- Identifisere ressurser
- Dialog med alle involverte parter (bør omfatte for hvem, hvor ofte, hvor dialog skal holdes, hva som skal informeres om)

Ansvarsområdene til hendelseshåndtereren handler om de tekniske aspektene ved hendelsen, og prosessen med gjenoppretting av systemer. Hovedansvaret til hendelseshåndtereren går ut på å analysere hvor feilen stammer fra, utarbeide en strategi for å gjenopprette systemer til normal tilstand og utføre en effektiv implementasjon av løsningen. Hendelseshåndtereren skal bistå hendelsesleder med delegering av oppgaver.

Et utklipp fra rammeverket av sjekklisten for hendelseshåndterer er som følger:

- Ansvar for tekniske aspekter
- Finne ut hva som gikk galt
- Utarbeide gjenopprettingsstrategi
- Implementere løsning

Videre ble rollene for IT- og infrastruktur-ansvarlig beskrevet. IT- og infrastruktur-ansvarlig har ansvar for å de fullføre tekniske aktiviteter for å begrense skadeomfanget og gjenopprette systemer til normaltilstand, samt utføre andre delegerte arbeidsoppgaver fra hendelsesleder.

For å få en oversikt over rollene ble det utformet en tabell. Tabellen er delt opp i tre kolonner: Navn, rolle og ansvar. Kolonnen for 'navn' inneholder navnene til personensom tildeles rollen. Kolonnen for 'rolle' beskriver rollens navn. 'Ansvar' blir beskrevet til slutt i den siste kolonnen. Tabellen var som følger:

Navn	**Rolle**	**Ansvar**
	Hendelsesleder	Holde oversikt over hele hendelsen
	Triage Ansvarlig	Triage-prosess
	Hendelseshåndterer	Håndtering av hendelse
	IT og Infrastruktur	Ansvar over IT infrastruktur

Tabell 13: Oversikt over roller

3.1.2 Identification

Fasen 'Identification' handlet om prosessen virksomheten kan ta i bruk for å identifisere at de har blitt utsatt for en sikkerhetshendelse, og hvordan de kan innhente så mye informasjon som mulig om hendelsen. Fasen inkluderte indikatorer på vellykkede angrep, prosess for rapportering av en sikkerhetshendelse, analyseverktøy og til slutt en prosess for videre håndtering av hendelsen.

Fasen bestod av fem kapitler. Kapitlene var som følger:

- Metoder for å identifisere hendelser
- Rapportering av hendelser
- Analyseverktøy
- Koordinering av team

Metoder for å identifisere hendelser

Dette kapittelet tok for seg ulike metoder for å identifisere hendelser. Kapittelet beskriver indikatorer som kan tyde på vellykkede angrepsforsøk mot virksomheten. Disse indikatorene kan bli benyttet av sikkerhetsteamet for å vurdere hvorvidt en reell sikkerhetshendelse har funnet sted, alvorlighetsgraden til hendelsen og eventuelt hvem angrepsaktøren er. Indikatortypene kapittelet tar for seg er som følger:

- Rekognosering
- Skadevare
- Uautorisert tilgang eller feilede påloggingsforsøk
- Command and Control (C2)
- Fullførelse av angrepet

Rekognosering

Rekognosering er ofte det første steget i et angrep, hvor aktøren innhenter informasjon om endemålet. Dette kan blant annet være informasjon om nettverksinfrastrukturen, systemer, endepunktsklienter og sluttbrukere. En vanlig metode aktører bruker for å oppnå dette er kartlegging av servere og tjenester som står eksponert mot internett, som ofte blir utført med bruk av portskannere. En metode virksomheten kan bruke for å oppdage forsøk på rekognosering er å undersøke om eksponerte servere opplever mange mistenkelige oppslag.

Skadevare

Dette underkapittelet beskriver indikatorer relatert til skadevare. Skadevare er en samlebetegnelse på ulike typer programvare som uten brukerens tillatelse utfører uønskede handlinger. Skadevare er ofte forkledd som ufarlige filer, som for eksempel PDF-filer. Noen indikatorer på infeksjon av skadevare er blant annet løsepengevirus, nedgang på enheters ytelse over kort tid, og programmer som åpnes eller lukkes automatisk.

Det ble skrevet om ulike indikator på vellykket infeksjon av løsepengevirus. En indikator kan være en beskjed, ofte i form av en tekstfil på skrivebordet, som eksplisitt beskriver at en er infisert av virus, med medfølgende instruksjoner for å gjenopprette til normal drift. Andre indikatorer kan være krypterte filer med filendelser som .encrypted, .locked, og .crypto.

Drastisk nedgang på enheters ytelse på kort tid er en annen indikator som ble beskrevet. Nedgang på ytelse kan skyldes skadevare som kjører i bakgrunnen, som for eksempel spionvare eller trojaner.

Uautorisert tilgang eller feilede påloggingsforsøk

Underkapittelet i rammeverket beskriver indikatorer relatert til uautorisert tilgang til sluttbrukeres konti.

Noen eksempler på indikatorer var som følger:

- Varsel fra deteksjonsprogramvare
- Kontoaksess fra ukjent område og/eller enhet
- Endringer i filer som svært sjeldent eller aldri skal endres på
- Låst brukerkonto
- Mistenkelig administrativ brukeratferd (privilege escalation)
- Kompromitterte konto med lekkede brukerdetaljer
- Uvanlig nettverksaktivitet

Command and Control (C2)

Underkapittelet i rammeverket beskriver indikatorer på C2-kommunikasjon. Phishing er en typisk inngangsvektor for å infisere et system og opprette C2-kommunikasjon. En typisk indikator på C2-trafikk kan være uvanlig mengde med nettverkstrafikk. For eksempel vil en liten mengde innkommende trafikk og en større mengde utgående nettverkstrafikk fremstå mistenkelig.

Fullførelse av angrepet

Dette underkapittelet i rammeverket beskriver indikatorer på fullførelse av angrep. De to mest relevante måtene et angrep blir fullført på er gjennom tjenestenektangrep og dataeksfiltrering.

Tjenestenektangrep har som formål å utføre angrep som hindrer at systemer kan opprettholde normal drift. Disse angrepene leder ofte til overbelastede systemer som videre fører til at systemet går ned og blir ikke-funksjonelle. Noen indikatorer på et slikt angrep er uvanlig mengde med nettverkstrafikk, og en uvanlig stor mengde med serverforespørsler over kort tid.

En uvanlig mengde med nettverkstrafikk er den mest vanlige indikatoren for tjenestenektangrep. Dette kan føre til at nettsider går ned og kan gi ulike feilmeldinger. Et høyt antall serverforespørsler over kort tid fra forskjellige IP-adresser kan for eksempel indikere et botnet-angrep. Botnet-angrep bruker et nettverk av infiserte maskiner til å utføre ondsinnede handlinger. Angripere kan beordre maskinene til å utføre spørringer mot nettverk og dermed overbelaste systemene.

Dataeksfiltrering er en svært populær teknikk som benyttes i stadig større grad i forbindelse med løsepengevirusangrep. Ettersom virksomhetene etablerer bedre teknikker for sikkerhetskopier og gjenoppretting av data, utvikler angriperne andre metoder for å skade virksomheters omdømme. Dataeksfiltrering handler om å kopiere ut data før det krypteres. Aktører kan deretter true med å lekke sensitiv data. Dette kan i mange tilfeller skade virksomheters omdømme eller få store økonomiske konsekvenser.

En liste på indikatorer på dataeksfiltrering er som følger:

- Varsel fra overvåkningsystemer som Data Loss Prevention (DLP)
- Ukjente protokolloverføringer. Eksempel kan være at HTTP benyttes istedenfor HTTPS, som strider med virksomhetens nettverksoppsett
- Unormalt store filer med arkiveringsformat som .zip

Rapportering av hendelse:

Dette kapittelet presenterte en mal for rapportering av identifiserte hendelser. Prosessen kan benyttes av alle ansatte i virksomheten. Kapittelets underkapitler var som følger:

- Hendelse identifiseres og varsles om
- Opprettelse av sak

Malen var som følger, med eksempler:

Hvem rapporterte hendelsen (Fullt navn)	Arne Bjertulf
Når ble hendelsen oppdaget (Dato og klokkeslett)	Torsdag, 14.04.2022, kl. 12:34
Hvordan ble hendelsen oppdaget (Én til tre setninger)	Passord fungerte ikke, og ansatt mistenkte derfor kompromittering.
Kort beskrivelse av hendelsen og hvilke systemer og/eller brukere som ble påvirket	Ondsinnet lenke sendt til mottaker, mottaker trykket på lenken og oppga sensitiv brukerinformasjon, en ansatt sin konto er kompromittert.

Tabell 14: Mal for rapportering av hendelse

Det anbefales at malen blir tilgjengeliggjort på virksomhetens intranett.

Analyseverktøy

Dette kapittelet listet utvalgte verktøy sikkerhetsteamet kunne benytte i analysen av sikkerhetshendelsen. Formålet med listen er å gi sikkerhetsteamet en kort beskrivelse av verktøyenes bruksområde. Beskrivelsen kan senere utvides med instruksjoner for hvordan verktøyene kan benyttes. Listen inneholder per dags dato kun forslag til verktøy, og bør oppdateres av virksomheten til å reflektere hvilke verktøy som er i bruk.

Listen var som følger:

- Loggfiler

  Kan innhentes fra brannmur, XDR, Event Viewer eller annen programvare. XDR vil ofte gi en beskrivelse av indikatortrigging eller anomali, som kan gi sikkerhetsteamet verdifull bakgrunnsinformasjon om årsaken til hendelsens opphav.

- Netflow

  Analyse av nettverkstrafikk. Kan gi informasjon om kilde- og destinasjons-IP-adresse, pakker sendt, tidspunkt for trafikk og nettverksprotokoll(er) brukt.

- Feilmeldinger

  Kan innhentes fra brannmur, XDR, Event Viewer eller annen programvare. Feilmeldingskoder eller en beskrivelse av feilen kan gi sikkerhetsteamet mer informasjon om hendelsen.

- Intrusion Detection System (IDS)

  XDR er virksomhetens IDS. XDR vil varsle om anomali i nettverkstrafikken.

- VirusTotal

  Analyserer filer og URL-er. Virksomheten må ta i betraktning at søk vil bli tilgjengeliggjort for brukere med lisens.

- Programvare for sandkasse.

  Muliggjør å kunne kjøre og analysere kode i et kontrollert miljø.

- Programvare for Data Loss Prevention.

  Kan benyttes for å varsle om mistenkelig dataeksfiltrering, eller forhindre utkopiering av data basert på spesielle mønstre i nettverkstrafikken.

Koordinering av team

Dette kapittelet tok for seg hvilke ansvarsområder og aktiviteter som skulle utføres av de ulike rollene i 'Identification'-fasen.

Triage-ansvarlig er ansvarlig for å utforme en hypotese av hendelsen. Triage-ansvarlig kan formulere hypotesen med utgangspunkt i rapporteringsmalen. For å supplere hypotesen skal triage-ansvarlig også utføre en rotårsaksanalyse. Rammeverket beskriver tre vanlige rotårsaker. Disse er som følger:

- Årsaker relatert til systemer. Dette kan være feil på maskinvare som fører til avvik, systemfeil ved oppstart, feilkonfigurasjon av systemer, applikasjoner eller servere
- Menneskelige feil og/eller målrettede angrep. For eksempel sluttbruker som trykker på en phishing-lenke
- Organisatoriske årsaker. Dette kan være uklar kommunikasjon innad i organisasjonen eller med leverandører

Det er også hensiktsmessig å se på hvordan hendelsen kan utvikle seg. Er det for eksempel identifisert et løsepengevirusangrep kan det haste med å stenge ned tilganger eller skru av nettverk for å forhindre videre spredning. I et slikt tilfelle må triage-ansvarlig varsle videre så fort som mulig. Etter at dette er gjort kan triage-ansvarlig videre se på:

- Å utarbeide en hypotese om hvorfor angrepet ble oppdaget, og om kompromitteringen var vellykket.
- Påvirkede systemer, og hvor langt angrepet er kommet

All informasjon skal samles for å kategorisere hendelsen, og årsaken skal dokumenteres. Hvilke systemer og brukere som er påvirket av hendelsen skal dokumenteres i tillegg. Triage-ansvarlig skal varsle hendelsesleder som videre koordinerer teamet og delegerer oppgaver. Dokumentasjon i rotårsaksanalysetabellen skal overleveres hendelseshåndterer for videre analyse.

Informasjonen kan dokumenteres i tabellen under.

Kategori	Beskrivelse
Alvorlighetsgrad	S2
Rotårsak	Phishing
Hypotese	Opportunistisk angrep
Påvirkede systemer/brukere	Bruker A
Er nødvendige varslet?	Nei
Hendelseskategori	Løsepengevirus

Tabell 15: Oppsummerende tabell for hendelsen etter identifikasjon

Etter at triage-ansvarlig har loggført og registrert en ny hendelse har hendelseslederen ansvar for videre koordinering av hendelseshåndteringsprosessen. Første steg er å delegere oppgaver.

Hendelseslederen skal sikre at aktiviteter utført av teamet er av høyt kvalitetsnivå og at alle gjør oppgavene de har blitt tildelt. En del av ansvarsområdet til rollene i sikkerhetsteamet er forhåndsdefinert i 'koordinering av team' i hver fase, men hendelseslederen må supplere med flere oppgaver eller omfordele ved behov. Hvis teammedlemmer blir usikre på hva de skal gjøre skal hendelsesleder tildele oppgaver avhengig av situasjonen.

Hendelseslederen skal sørge for at alle har nødvendig utstyr og verktøy til å komme i gang med hendelseshåndteringen. Mangler det ressurser i form av verktøy, kontaktpersoner eller annet må hendelseslederen drive denne prosessen fremover.

Førsteprioritet er å varsle eventuelle kunder som er påvirket. Dette er hovedsakelig hendelseslederens ansvar. Det kan være vanskelig å ha fullstendig oversikt over alle systemer og brukere påvirket i en tidlig fase. Derfor kan det vurderes å ha en informasjonsside der informasjon om hendelsen publiseres offentlig.

Videre bør det tas kontakt med underleverandører som kan bistå. Det anbefales også å ta kontakt med internettleverandør for videre bistand.

Det er hendelseslederens ansvar å ha et overordnet oversiktsbilde over kommunikasjonsprosessen i hendelsen, avtale møter og sette ressurser i kontakt med hverandre.

Eksempler på informasjon som bør avklares:

- Hvilket type angrep er det?
- Hva har blitt påvirket?
- Hvordan påvirker dette produksjonen?
- Hvor kom angrepet fra eller hvor mistenker dere at den kommer fra?
- Hva har blitt gjort mot hendelsen så langt?
- Hva skal bli gjort videre?
- Hvordan er situasjonen?
- Innspill fra andre

Hendelseshåndtereren er ansvarlig for å samle inn og analysere data som skal støtte etterforskningen av hendelsen. Hendelseshåndtereren kan ta utgangspunkt i informasjon overlevert av triage-ansvarlig for videre analyse.

For hendelseshåndtereren er det utformet en fremgangsmåte for henholdsvis løsepengevirus- og phishingangrep.

Analyser fokusert mot løsepengevirusangrep

Er det oppdaget løsepengevirus i en tidlig fase er det svært sannsynlig at viruset kan spre seg videre. Uavhengig av om det allerede har spredt seg eller er i ferd med å spre seg bør nettverksaksess stenges av så fort som mulig. Dette inkluderer å koble ut nettverksenheter som for eksempel hub, switch og router. Internettaksess inn og ut fra virksomheten bør kuttes. Virksomheten bør selv utarbeide en liste over alle enheter som skal kobles ut, samt utforme en rutine på hvordan dette skal gjøres.

Når en har forhindret videre spredning av angrepet er det viktig å kartlegge hvilke systemer som er rammet. Hendelseshåndtereren bør ha en forhåndsdefinert liste over indikatorer som kan tyde på at enheter er infisert. Denne listen bør virksomheten utforme selv. Listen bør sjekkes opp mot hver enhet for å identifisere hvorvidt enhetene er infisert. Listen må kontinuerlig oppdateres med enheter sjekket og status på disse.

Hendelseshåndtereren bør forsøke å identifisere om data har blitt eksfiltrert av aktøren. Dette er en svært vanlig og populær metode, og kan benyttes til blant annet utpressing i forbindelse med å lekke sensitive data.

For å avgjøre hvorvidt løsepenger skal utbetales, må hendelseshåndtereren ta følgende elementer i betraktning:

- Hva betaler virksomheten løsepenger for? Er det for gjenoppretting av krypterte filer eller å unngå lekkasje av bedriftssensitiv data?
- Hvilken garanti har virksomheten for at aktøren gjør det de hevder? Hva forteller tidligere historikk?
- Hvilke økonomiske konsekvenser har utbetaling av løsepenger for virksomheten? Hvordan påvirkes virksomhetens omdømme? Skal avgjørelsen hvorvidt løsepenger betales offentliggjøres?
- Hvor tidskritisk er det å fatte en avgjørelse? Øker prisen ettersom tiden går?
- Hvem skal fatte den endelige avgjørelsen? Skal det være én eller flere personer? Skal begrunnelsen for avgjørelsen dokumenteres?
- Hvordan skal betalingen utføres? Hva slags valuta er det, for eksempel kryptovaluta? Hvilken enhet skal utføre betalingen?

Det finnes mange angrepsaktører og de kan bli identifisert ved å se på hva slags tactics, techniques and procedures (TTP) som er brukt. Det kan være formålstjenlig både i prosessen med å gjenopprette systemer tilbake til normaltilstand og for potensielle fremtidige hendelser å kart-

legge hvem som står bak cyberangrepet. Ved å identifisere angrepsaktør kan en også søke i åpne kilder om det foreligger offentlig tilgjengelige dekrypteringsnøkler. Det understrekes at slike dekrypteringsnøkler alltid bør benyttes med varsomhet og testes før det benyttes i produksjonsmiljø.

Analyser fokusert mot phishingangrep

Vellykkede phishingangrep kan være en inngangsvektor for mange angrep, blant annet løsepengevirus. Det er derfor vanskelig å konkretisere tiltak mot vellykkede phishingangrep, da det kan føre til svært mange forskjellige utfall.

Vellykkede phishingangrep vil i de aller fleste tilfeller forekomme via e-post. Det er gjerne ondsinnede vedlegg som åpnes eller nettsider som besøkes. Et vellykket phishingangrep kan være vanskelig å oppdage avhengig av hvordan aktøren opererer. Er det for eksempel brukerdetaljer på avveie kan det hende aktøren avventer med å nyttiggjøre seg av denne informasjonen. Derfor vil det være verdifullt om sluttbrukere rapporterer om mistenkelig aktivitet.

Selv om tofaktorautentisering er et av de sikreste tiltakene mot uautorisert tilgang, er en fremdeles sårbar for angrep. Tofaktorautentisering har som regel ingen grense på hvor mange forespørsler en kan få innen en gitt tidsramme. En metode aktører kan bruke er å massesende tofaktorforespørsler slik at bruker til slutt godkjenner forespørselen [4].

3.1.3 Containment

'Containment' handler om hvordan virksomheten kan gå fram for å isolere en hendelse og bekjempe potensialet for spredning til andre systemer. Fasen inkluderer generell informasjon om spredning av skadevare, en prosess for vurdering av hvor mange systemer og endepunkter skadevaren har nådd og hvilke tiltak som må iverksettes for å håndtere hendelsen, om sikkerhetskopiering for kriminalteknisk etterforskning og koordinering av sikkerhetsteamet.

Fasen bestod av fem kapitler. Fasene var som følger:

- Isolering (med to underkapitler)
- Kriminalteknisk Image (med tre underkapitler)

- Forhåndsdefinerte handlingsmønstre
- Koordinering av team

Isolering

I dette kapittelet ble det beskrevet ulike tiltak for å isolere en hendelse.

Før en iverksetter effektive tiltak for en hendelse er det viktig å forstå omfanget av hendelsen. Derfor ble viktigheten av å vurdere et angrep beskrevet.

Det ble beskrevet to ulike metoder for begrensning av angrep: Kortidsbegrensning og langtidsbegrensning. Kortidsbegrensning skal som regel tas i bruk først under en hendelse, men både korttids- og langtidsbegrensningstiltak er vanligvis aktuelle.

Korttidsbegrensing har som formål å begrense skadeomfanget så raskt som mulig. Korttidsbegrensning er tiltak som forhindrer angrepets spredning på kort sikt, med tanke på maskineri og systemer. Eksempler på tiltak til slike situasjoner er blant annet å ta ned eller isolere servere og maskineri, rute trafikk til failover-servere, blokkere eller isolere endepunktsklienter, og deaktivere brukere.

Noen eksempler på korttidsbegrensede tiltak er som følger:

- Isolering av endepunkt med funksjon fra XDR
- Deaktivering av brukerkonti
- Skru av infiserte enheter og benytte failover-servere ved behov
- Opprette nye brannmurregler på kompromittert enhet for å forhindre all utgående trafikk

Langtidsbegrensning har som formål å få produksjons- og hovedenheter tilbake til normal drift. Langtidsbegrensning setter i gang tiltak som kan fortsette å begrense angrepet, men samtidig opprettholde normal drift. Målet med langtidsbegrensning er å identifisere bakdører, kompromitterte brukere og kompromitterte enheter.

Noen eksempler på langtidsbegrensende tiltak er som følger:

- Oppdatering av systemer
- Bytte av passord
- Fjerne kompromitterte brukerkonti
- Legge til brannmur- og filterregler
- Tett overvåkning over systemer ved hjelp av XDR

Kriminalteknisk image

Dette kapittelet beskrev viktigheten av å ta kriminalteknisk image under en hendelse. Et kriminalteknisk image er en bit-for-bit, sektor-for-sektor direktekopi av en fysisk lagringsenhet, inkludert alle filer, mapper og ikke-allokert plass. Et kriminalteknisk image inkluderer også slettede filer [42]. Sikkerhetskopi i form av et kriminalteknisk image er viktig av flere årsaker. Imaget kan benyttes som bevis i rettsaker tiltaker. Samtidig er det egnet for videre analyse og kan benyttes som læringspunkter i 'Lessons learned'. Når en tar kriminalteknisk image anbefales det å benytte dedikert programvare som er designet for dette formålet. Spesialdesignet programvare kopierer identisk status på systemet, slik at hendelsen kan analyseres i et sikkert og kontrollert miljø. Det er ikke beskrevet i detalj hvordan sikkerhetsteamet kan utføre denne prosessen da det i stor grad vil avhenge av hendelsestype og hvilke verktøy virksomheten tar i bruk. Virksomheten må utforme en prosess for å ta kriminalteknisk image selv.

Forhåndsdefinerte handlingsmønstre

Dette kapittelet definerte noen forhåndsdefinerte handlingsmønstre for spesifikke hendelsestyper. Formålet med kapittelet er at sikkerhetsteamet raskere kan fatte avgjørelser og håndtere hendelsen på en mer effektiv måte. Listen bør oppdateres kontinuerlig.

Noen eksempler på forhåndsdefinerte handlingsmønstre var som følger:

Handlingsmønstre:	**Hendelsestype**	**Godkjent (ja/nei/N/A)**
Endre passord	Brukerdetaljer kompromittert	Ja
Isolering av endepunktsklienter	Endepunktsklient infisert av skadevare	Ja
Udefinert	Eksfiltrert data fra virksomhet	N/A

Tabell 16: Forhåndsdefinerte handlingsmønstre

Koordinering av team

For denne fasen går teamets ansvarsområder ut på hvordan de skal begrense skadeomfanget.

Hendelseshåndterer har ansvar for å utarbeide en gjenopprettingsstrategi, som starter med å begrense hendelsen.

Ved løsepengevirusangrep skal hendelseshåndterer begynne med korttidsbegrensning. Ettersom løsepengevirus kan spre seg svært raskt og ofte kryptere store eller hele deler av nettverket, er det svært kritisk å begrense skadeomfanget så fort som mulig. Er det identifisert løsepengevirus i nettverket, bør internettilgangen til virksomheten kuttes umiddelbart. Det kan forhåpentligvis kutte forbindelsen til angriperen. Viruset kan fremdeles spres internt i nettverket, og det er følgelig viktig å ha sikkerhetskopier og segmenterte nettverk for å motvirke dette.

Av kriminaltekniske årsaker anbefales det ikke å slå av identifiserte kompromitterte enheter. Det kan for eksempel være indikatorer lagret i minne som vil forsvinne i et slikt tilfelle. Er det identifisert en kompromittert enhet som ikke har spredd viruset til andre enheter, bør denne enheten isoleres på et eget, segmentert nettverk. Deretter bør hendelseshåndterer ta et image av hele maskinen for senere skadevareanalyse.

Ondsinnet aktivitet fra phishingangrep må bli håndtert så raskt som mulig. Når aktøren først har kommet inn i systemet kan angrepet fort spre seg. Ettersom vellykkede phishingangrep kan være en inngangsvektor til eskalering av mange ulike type angrep, er det vanskelig å lage en

forhåndsdefinert liste over begrensede tiltak. Tiltak må iverksettes basert på hvilke systemer som er påvirket. Om bruker er kompromittert bør passord endres umiddelbart, eller bruker vurderes å midlertidig deaktiveres.

Hendelsesleder skal vurdere om langtidsbegrensning er nødvendig. Om systemer kan tas offline etter utføring av korttidsbegrensning og kriminalteknisk image, kan hendelseslederen vurdere å gå rett til 'Eradication'-fasen. Dersom systemene må forbli i produksjon skal hendelsesleder få i gang langtidsbegrensningen ved å gi beskjed til hendelseshåndterer og IT- og infrastruktur-nsvarlig.

IT- og infrastruktur-ansvarlig skal bistå hendelseshåndterer i å begrense hendelsen og holde tett kontakt med hendelseshåndterer i denne fasen. Under langtidsbegrensning kan oppdatering av systemer være nødvendig om det blir avdekket aktive sårbarheter. Dette er IT- og infrastruktur-ansvarlig sitt ansvarsområde.

3.1.4 Eradication

Dette kapittelet handlet om hvordan virksomheten kan gå fram for å fjerne skadelig program-vare.

Fasen bestod av fem kapitler. Fasene var som følger:

- Kartlegging av utnyttet sårbarhetsflate
- Utryddelse (med to underkapitler)
- Sletting av berørte system(er) og enhet(er)
- Koordinering av team (med fire underkapitler)

Kartlegging av utnyttet sårbarhetsflate

For å være i stand til å fjerne alle spor av angrepsaktøren bør en ha kartlagt inngangsvektoren til hendelsen. Denne analysen bør allerede ha blitt utført i 'Identification'-fasen av triage-ansvarlig, eventuelt i samarbeid med hendelseshåndterer. Avhengig av hva inngangsvektoren var, er det

viktig å herde systemer slik at de blir mer motstandsdyktig mot fremtidige angrep. Er det avdekket utnyttelse av sårbare systemer som kunne ha vært forhindret ved raskere oppdatering bør det sørges for å bedre virksomhetens oppdateringsrutiner. Er inngangsvektoren derimot sosial manipulering i form av et phishingangrep er det ikke mulig å beskytte seg helt for dette, men det bør brukes som et opplæringspunkt i 'Lessons learned'-fasen.

Når en skal utføre utryddelse er det viktig å ha kartlagt hvilke systemer som er berørt, og hva slags angrep det er snakk om. Som et utgangspunkt bør en prøve å sikre inngangsvektoren som ble benyttet for initiell aksess. Videre må teamet ha en oversikt over andre berørte systemer og enheter. Teamet har muligens avdekket ulike artefakter i forbindelse med angrepet, og disse bør håndteres i en slik grad at de slettes fra systemet. I et tilfelle med løsepengevirus bør virksomheten definere ulike strategier basert på angrepets omfang.

- Er endepunktsklienter infisert uten at det er tegn til spredning, anbefales det å wipe hele klienten. Endepunktsklienten skal på dette tidspunktet allerede ha blitt isolert.

- Er delte nettverksområder kryptert kan det være nødvendig med en komplett sletting av nettverksområdet, med gjenoppretting av sikkerhetskopi. Gjenoppretting bør testes i et testmiljø før det kjøres i produksjon, og det krypterte nettverksområdet bør ikke slettes, men heller isoleres inntil gjenoppretting er fullført og vellykket.

- For infeksjon av domenekontroller eller andre kritiske enheter bør det defineres en større plan. Det kan være vanskelig å gjøre en komplett sletting av slike systemer, selv med fungerende sikkerhetskopi, da det kan føre til mye nedetid. Her bør en sjekkliste for ulike tiltak defineres og deretter følges.

En utryddelse tar sikte på å fjerne alle spor av angrepsaktør, men en kan aldri være helt sikker på at det er tilfellet. Det er heller ikke uvanlig at angrepsaktør vil forsøke å angripe kort tid etter initiell angrep, ettersom virksomheten kan være i en sårbar fase og i en prosess med å gjenopprette til normal drift. Følgelig anbefales det å sette opp overvåkning av berørte systemer i en angitt tidsperiode for å eventuelt oppdage anomali i systemet. Beste praksis foreslår overvåkning minst 30 dager etter at et angrep er håndtert.

For løsepengevirus anbefales det å utforme rutine på hvordan en effektivt kan endre passord til alle brukere. For phishingangrep kan det være tilstrekkelig å endre passord til den kompromitterte brukeren.

Sletting av berørte system(er) og enhet(er)

Dette kapittelet tok for seg rutiner en virksomhet burde ha på plass i forbindelse med sletting av program- og maskinvare. Noen eksempler er som følger:

Sikkerhetshendelse	Kategori	Mulige tiltak
Kompromittert brukerkonto pga. phishing	Kompromittert konto	• Passordbytte • Overvåking av brukerkonto • Sletting av brukerkonto
Løsepengevirus låst endepunkt	Endepunktsklient	• Wipe via dedikert verktøy • Gjenoppretting fra sikkerhetskopi •
Servertrafikk kompromittert, eksfiltrering av data	Servere	• Gjenopprett fra sikkerhetskopi • Isolering av server • Overvåking av server • Skru av server • Komplett sletting av server
Domenekontroller infisert og kompromittert	Domenekontroller	• Gjenopprett fra sikkerhetskopi • Skru av domenekontroller • Isolere domenekontroller • Deaktivere domenekontroller • Komplett sletting av domenekontroller

Tabell 17: Mulige tiltak for sletting

Koordinering av team

Siste kapittel i fasen beskrev hvordan sikkerhetsteamet bør organisere seg.

Hendelseshåndterer skal sørge for å fjerne alle spor av angrepsaktør.

Jf. tabell 17 for mulige tiltak som hendelseshåndterer kan utføre for ulike sikkerhetshendelser.

Hendelseslederen skal også sørge for at alle i teamet dokumenterer underveis. I tillegg skal hendelseslederen se vurdere hvorvidt hendelseshåndterer trenger bistand fra triage -ansvarlig og IT- og infrastruktur-ansvarlig.

Triage-ansvarlig skal sørge for å overvåke berørte systemer og gi beskjed til andre i teamet om det er oppstår mistenkelig aktivitet under 'Eradication'-fasen. Overvåkning blir gjort ved bruk av XDR.

IT- og infrastruktur-ansvarlig skal bistå hendelseshåndterer under hele 'Eradication'-fasen.

3.1.5 Recovery

'Recovery' handler om hvordan virksomheten skal gjenopprette berørte data, systemer og/eller enheter tilbake til normal tilstand. Det må bli gjort grundig testing av systemene i denne fasen for å verifisere at systemer er operasjonelle.

Fasen bestod av fire kapitler. Kapitlene var som følger:

- Gjenoppretting til normaltilstand (med tre underkapitler)
- Oppdatering av systemer
- Koordinering av team (med tre underkapitler)

Gjenoppretting til normaltilstand

Gjenoppretting av data må utføres avhengig av virksomhetens behov. Det er svært viktig at integriteten testes og verifiseres i et testmiljø først da det er en mulighet for at sikkerhetskopier har blitt kompromittert.

Etter gjenoppretting av data må det verifiseres at systemet fungerer som det skal.

Prosedyrer for gjenoppretting av data og verifisering er ikke beskrevet i detalj da det avhenger av virksomhetens verktøy for sikkerhetskopiering og gjenoppretting.

Oppdatering av systemer

Basert på analyse og informasjon fra hendelsen skal virksomheten vurdere hvorvidt det er nødvendig å oppdatere sine systemer.

For phishingangrep er det i mange tilfeller ikke like relevant med sikkerhetsoppdateringer da inngangsvektor ofte er via uvitende eller uforsiktig sluttbruker.

Det anbefales at virksomheten selv utformer en rutine for oppdatering av systemer.

Koordinering av team

Dette kapittelet var delt opp i tre hovedroller som koordinerer sikkerhetsteamet sine oppgaver. Rollenes ansvarsområder er ikke like omfattende på grunn av fasens natur. Disse var som følger:

- Hendelseshåndterer
- Hendelsesleder
- IT- og infrastruktur-ansvarlig

Hendelseshåndterer er ansvarlig for gjenoppretting av sikkerhetskopiene. Det må først bli sjekket og verifisert at sikkerhetskopiene ikke er kompromitterte. Hendelseshåndterer skal dermed sørge for at sikkerhetskopiene blir gjenopprettet i et testmiljø før det gjenopprettes i produksjonsmiljø. Etter gjenoppretting må hendelseshåndterer verifisere at alle systemer er operasjonelle og fungerer som forventet.

Om gjenopprettingsfasen er så omfattende at det må gjøres en prioritering, skal hendelseslederen utføre denne vurderingen i samråd med ledelsen.

IT- og Infrastruktur-ansvarlig har ansvar for å gjøre eventuelle sikkerhetsoppdateringer av berørte systemer.

3.1.6 Lessons Learned

I denne fasen skal teamet reflektere over hva de har lært fra hendelsen, og trekke frem aktiviteter som eventuelt kan forbedres. Det blir dessuten avholdt et lærdomsmøte der teamet diskuterer hendelsen i plenum. Avslutningsvis skal det utformes en hendelsesrapport som gir en oversikt over hele hendelsesforløpet, og denne skal overrekkes ledelsen.

Fasen bestod av fem kapitler. Kapitlene var som følger:

- Hendelsesrapport
- Forbedringspunkter
- Lærdomsmøte

Hendelsesrapport

Det skal utformes en hendelsesrapport for håndteringen av hendelsen. Hendelsesrapporten skal bestå av en steg-for-steg-gjennomgang av hele hendelsen. Hendelsesrapporten skal benyttes som grunnlag for revisjon av rammeverket. Hendelsesrapporten skal til slutt distribueres til ledelsen.

Virksomheten må selv utforme en mal for hendelsesrapporten.

Forbedringspunkter

Det skal utføres en individuell refleksjon av teamets medlemmer etter håndtering av hendelsen.

Noen elementer som må besvares under selvrefleksjonen er som følger:

- Hvilke valg under håndteringen var du fornøyd med, og hvorfor?
- Hvilke valg under håndteringen var du misfornøyd med, og hvorfor?
- Hva kunne du ha utført bedre under hendelsen?
- Var prioriteringene underveis riktige?
- Ble alle stegene i hendelseshåndteringen utført? Om ikke, hvorfor?
- Var dokumentasjonen utfyllende? Om ikke, hvorfor?

Listen kan senere utvides med flere elementer.

Lærdomsmøte

Dette kapittelet tok for seg hvordan et lærdomsmøte etter hendelsen skulle foregå. Alle som var involvert i hendelsen skal diskutere hendelsen i møtet og vurdere hvordan de kan forbedre sine rutiner.

Noen elementer som må besvares under lærdomsmøtet er som følger:

- Når ble problemet først oppdaget og av hvem?
- Omfanget av hendelsen
- Hvilke spesifikke ressurser/eiendeler og plattformer ble det målrettet mot?
- Hva slags data ble eksponert?
- Hvordan hendelsen ble begrenset (contained) og utryddet (eradicated)?
- Arbeid utført under Recovery-fasen
- Områder der IR-teamet var effektive
- Hvordan eksisterende sikkerhetstiltak fungerte
- Områder som trenger forbedring

4 Utforming av treningsopplegg

Dette kapittelet beskriver utformingen av treningsopplegget. Kapittelet tar for seg gruppens valg, og beskriver hvordan spillet fungerer.

4.1 Prosess

Grunnidéen med spillet er at deltakerne skal diskutere og finne løsninger sammen for å løse en hendelse. Ut fra en gruppe deltakere skal én deltaker bli valgt ut som leder av øvelsen. Lederen skal trekke et kort som simulerer starten av en hendelse, og dermed starter spillet. Resten av deltakerne vil få en rolle som spillere, også kalt forsvarere. Spillerne får tildelt alle nedskrevne playbooks de kan ta i bruk for å løse hendelsen. Med playbooks menes de ulike fasene i rammeverket. Kortene og playbooks er i utgangspunktet digitale i form av en PDF. Spillet har hovedsakelig fire faser: 'Identification', 'Containment', 'Eradication' og 'Recovery'. Fasene er knyttet opp mot rammeverket, hvor de samme fasene er beskrevet i detalj. Det kan videre oppstå flere 'injects' i fasene fra lederen. Med 'inject' menes en fortsettelse av fortellingen.

Etter at playbooks er tildelt gruppen og lederen har trukket ut et kort, skal lederen utforme og presentere en fortelling som passer kortet. Fortellingen skal ikke være veldig detaljert og lederen bør ikke bruke mer enn to til tre minutter på utformingen. Lederen kan for eksempel presentere følgende fortelling: 'Noen fra IT-personell melder om unormal aktivitet mot webserver'. Deretter skal spillerne diskutere og foreta handlinger. Spillerne bør her ta i bruk playbooks. Spillerne vil følge fasene i kronologisk rekkefølge, som betyr at spillerne først håndterer hendelsen basert på ansvarsområder i 'Identification'-fasen, deretter 'Containment'-, 'Eradication-' og 'Recovery'-fasen. Lederen skal deretter følge diskusjonen. Etter at spillerne er ferdigdiskutert skal en terning bli kastet. Det er ikke satt noen begrensning på hvor lenge en diskusjon kan vare, men det anbefales å holde seg innenfor en tidsramme på fem til ti minutter. Om kastet fører til 'failure' skal lederen presentere en 'inject' og fortelle at spillernes handlinger førte til ytterligere problemer. Om kastet fører til 'success' skal lederen gi spillerne tillatelse til å gå videre til neste fase, dersom lederen konkluderer med at spillernes svar er godt nok. Når spillerne er gjennom siste fase er øvelsen vellykket.

Jf. seksjon 4.6 for mer informasjon om 'injects' og seksjon 4.2 for begrepene 'success' og 'failure'.

Uavhengig av resultatet av øvelsen skal det foretas en gjennomgang av hvordan øvelsen ble håndtert. Denne delen kan ansees som 'Lessons learned'-fasen av rammeverket. I denne fasen skal alle deltakerne i øvelsen diskutere hva som gikk bra og hva som kunne blitt gjort annerledes. Utfallet fra hendelsen er ikke det viktigste i denne øvelsen; det er diskusjonene som kommer som et resultat fra øvelsen som står i sentrum.

Det overordnede målet med øvelsen er hovedsakelig å forbedre rutiner og forsvarsmekanismer. Gjennomgang av øvelsen til slutt kan dessuten brukes av IT-personell til å illustrere for ledelsen viktigheten av å ha definerte og gjennomarbeidede prosedyrer. Tilfeldigheter i form av utfallet fra terningen er en del av øvelsen, og simulerer de ukjente faktorene ved en reell hendelse.

4.2 Regler

Spillerne kan bruke all kompetanse de besitter i kombinasjon med playbooks for å løse problemene. Etter at spillerne har diskutert skal de komme fram til en handling de ønsker å utføre. For hver handling spillerne utfører skal en 20-sidet terning kastes. Dersom terningen gir et tall mellom en og ti betyr det 'failure' og lederen skal presentere noe som gikk galt ut ifra spillernes handlinger. Om terningen gir et tall mellom elleve og tjue betyr det 'success' og lederen kan velge å gå videre til neste fase. Det er lederen som vurderer om diskusjonen og svaret fra spillerne er god nok til å gå videre på tross av at terningen gir 'success'. Om spillerne tar i bruk playbooks de fikk tildelt er det en +3-modifikator på terningkastet. Det betyr at om spillerne for eksempel kaster en terning som gir 9, kan terningkastet endres til 12. Hvorvidt spillerne tar i bruk playbooks er basert på om de tar i bruk et tiltak som er beskrevet i playbooken. Modifikatoren er definert for å belyse hvorvidt viktige steg er definert i playbooks, og vil belønne spillerne om det er tilfellet. Er ikke tiltaket definert bør det tas med i gjennomgangen av øvelsen til slutt.

Spillet varer i maksimalt tolv runder. Om antall runder overstiger dette taper spillerne og hendelsen ender uløst. Et kast av en terning signaliserer slutten på en runde.

Det er videre ikke mulig å få 'failure' fra et terningkast mer enn to ganger på rad. Om spillerne får 'failure' to ganger på rad vil neste terningkast automatisk bli 'success'. Begrensningen er satt for å minimere sjansen for at øvelsen drar ut i tid.

4.2.1 Tidsbruk

Et spill kan variere i tiden det tar å fullføre den. Ettersom spillets hensikt er opplæring er tidsbruk essensielt. Om gjennomføringens varighet er for kort får spillerne lite utbytte av spillet. Er varigheten derimot for lang kan det bli vanskelig å fokusere, og deltakerne kan miste motivasjon. Følgelig bestemte gruppen å ha et maksimalt antall med terningkast og runder. Gruppen kom fram til at antall terningkast ikke skulle overstige tolv. Om antall runder overstiger tolv taper spillerne og spillet er over. Det betyr at hendelsen ender uløst. Ut ifra testing av spillet fra medlemmer i gruppen kom gruppen fram til at et spill bør vare om lag 30-40 minutter. Det gir spillerne tid til å lære, men samtidig blir ikke øvelsen så lang at det kan fremstå kjedelig eller tungt.

4.3 Terning

Terningen er med i treningsopplegget for å skape tilfeldigheter. Under en reell hendelse går ikke handlinger alltid som planlagt og det forsøker terningen å illustrere.

Den 20-sidede terningen kan bli hentet digitalt om en ikke har en fysisk 20-sidet terning. Dette kan bli gjort ved å søke opp 'D20' på Google.

4.4 Kort fra treningsopplegg

Kortene skal gi lederen et utgangspunkt å bygge videre på. Et eksempel på et kort lederen kan trekke ut er som følger:

Phishing Angriper sender en ondsinnet e-post til brukere i virksomheten.
Oppdagelse XDR-varsel Varsel fra bruker
Årsak Ukjent

Tabell 18: Kort brukt i treningsopplegg

Kortene består av følgende felter:

Tittel

Tittelen skal være angrepstype som for eksempel phishing.

Oppdagelse

Oppdagelse skal presentere ulike metoder angrepet kan bli identifisert.

Årsak

Årsak skal fortelle noe om årsaken til at angrepet ble utført. Ofte er dette ikke kjent.

4.4.1 Informasjon om kort

Kortene blir hovedsakelig utformet av fagansvarlig for IT-sikkerhet i virksomheten. Utformingen kan også bli gjort i samarbeid med andre som skal delta i treningsopplegget. Det kan bli utformet så mange kort virksomheten selv ønsker, og kan gjøres ved å følge malen. Virksomheten kan også vurdere om enkelte kort skal fases ut dersom relevansen reduseres.

4.5 Roller

Spillet har hovedsakelig to roller: Leder og spillere.

Leder

Det skal være én leder i spillet og denne lederen har ansvar for å holde spillet i gang. Det er kun lederen som skal kjenne til kortet som representerer forskjellig type angrep. Lederen skal utforme små fortellinger som passer kortet som ble valgt og skal forsøke å skape diskusjoner blant spillerne. Denne rollen bør derfor i utgangspunktet bli tildelt en deltaker med inngående kunnskap om hendelseshåndtering. I tillegg har lederen ansvar for at alle som deltar i øvelsen er aktive ved å for eksempel stille spørsmål underveis. Passive spillere vil ta bort mye av hensikten med øvelsen.

Lederen har ansvar for å loggføre alle handlingene spillerne utfører og den tilknyttede verdien av terningkastet. I tillegg skal lederen loggføre antall terningkast gjennom hele øvelsen, og holde oversikt over tidsbruken.

Spiller/forsvarer

Resten av medlemmene som deltar i øvelsen skal være spillere, også kalt forsvarere. Disse spillerne skal til sammen utgjøre teamet og forsøke å løse hendelsen sammen. Det er ingen begrensning på antall spillere som kan delta i øvelsen. Spillerne skal ha playbooks for å bistå med håndtering av hendelsen. I utgangspunktet har spillerne lik rolle, men om ønskelig kan de få mer spesifikke roller. Disse rollene kan bli hentet fra rammeverket.

4.6 Fortellinger/injects

Fortellingene er det som fører spillet framover. Fortellingene skal beskrive hendelsen. Lederen starter med å beskrive starten på en hendelse basert på kortet som ble trukket ut, og bygger videre på fortellingen basert på diskusjonen fra spillerne. Ettersom spillernes diskusjon vil variere har ikke lederen en klart definert måte på hvordan fortellingene skal være. Egne tanker fra lederen vil være viktig for å holde fortellingene i gang. Lederen har en liste med eksempler på spørsmål som kan bli spurt.

Eksempler på spørsmål lederen kan stiller er som følger:

- Hvordan skal dere gå fram for å identifisere dette angrepet?
- Hvor mye ressurser, i form av ansatte og leverandører, kreves for å håndtere dette angrepet?
- Hvor mye nedetid på kritiske systemer kreves for å håndtere hendelsen?
- Hvem har ansvar for hva?
- Hvordan skal dere begrense angrepet etter å ha identifisert det?
- Hvordan skal dere utrydde angrepet?
- Hvordan skal dere gjenopprette systemer etter å ha utryddet angrepet?
- Hva kan virksomheten gjøre annerledes for å forhindre at et liknende angrep oppstår i fremtiden?

5 Utforming av playbooks

Dette kapittelet handler om utformingen av playbooks.

Playbookene skulle utformes i tabellform og bestå av fasene 'Identification', 'Containment', 'Eradication' og 'Recovery'. Fasene i playbooks skulle baseres på tilsvarende faser i rammeverket. Playbooks inneholder ikke første fase i rammeverket, 'Preparation', og heller ikke siste fase, 'Lessons Learned'. Det skyldes at fasene ikke passer formålet til playbooks, ettersom de kun skal inneholde prosedyrer for håndtering av et angrep i sanntid.

5.1 Formål

Formålet med playbooks var at de skulle fungere som en substitutt for rammeverket under kjente angrep som også er tidskritiske å håndtere. Playbooks spiller blant annet inn på effektmålet om å redusere antall hendelser som ikke blir håndtert. Nedskrevne og tydelige prosedyrer vil hjelpe sikkerhetsteamet å effektivt håndtere hendelser når de først inntreffer. Dette er svært viktig siden hendelser som ikke blir håndtert over lengre tid kan føre til store konsekvenser, og det tillater aktøren mer tid til å utføre skade [35].

5.2 Hvorfor playbooks

Det ble bestemt å utforme playbooks for å supplere hendelseshåndteringsrutinene. Ettersom rammeverket ble svært omfattende og inneholdt flere generelle prosedyrer, kunne det bli vanskelig for sikkerhetsteamet å forholde seg til under tidskritiske hendelser. Playbooks forsøkte å løse dette problemet ved å tilby en nedskalert, steg-for-steg-prosess for spesifikke angrepstyper.

6 Drøfting og diskusjon

Dette kapittelet diskuterer og drøfter gruppens arbeidsprosess og erfaringer knyttet til prosjektoppgaven. Kapittelet gjennomgår hvilke endringer gruppen hadde ønsket å gjøre med hensyn til avgrensning av prosjektoppgaven, gruppens arbeidsflyt og en redegjørelse for hvordan gruppen organiserte seg og arbeidet under prosjektperioden.

6.1 Avgrensning av prosjektoppgave

Prosjektoppgaven har vært en tidkrevende prosess, og tidlige beslutninger ledet til en mer omfattende oppgave enn først antatt. Tidlig i prosjektfasen var det diskusjoner med oppdragsgiver om omfanget av oppgaven, og om hva som var gjennomførbart. Oppdragsgiver var åpen for alle forslag, og i diskusjonen ble det tatt små beslutninger som over tid definerte avgrensningene. Gruppen begynte med å avgrense sikkerhetshendelser til å hovedsakelig fokusere på løsepengevirus og phishingangrep. Da gruppen begynte å skrive om policy i fasen 'Preparation' ble det tatt en avgjørelse på å utelate mandater fra ledelsen som IT-personell kan forholde seg til, og policy relatert til mediahåndtering.

Utformingen av treningsopplegget ble tidlig i prosjektfasen diskutert i mindre grad ettersom det var mye usikkerhet knyttet til hvordan det skulle utformes. Hovedutfordringen var at gruppen måtte utforme et treningsopplegg virksomheten kontinuerlig kunne bruke, som igjen satte krav til å lage et opplegg som var reproduserbart.

Underveis i prosjektfasen oppstod det usikkerhet om hvor enkelt det ville bli for oppdragsgiver å forholde seg til og ta i bruk rammeverket under en sikkerhetshendelse. Gruppen konkluderte med at rammeverket ble for omfattende til å effektivt kunne benyttes spesielt i tidskritiske hendelser som for eksempel løsepengevirusangrep. Gruppen bestemte derfor å utforme playbooks som skulle fungere som nedskalerte versjoner av rammeverket, og som kunne rette seg mot spesifikke angrepstyper. Oppdragsgiver støttet denne vurderingen.

Prosjektfasens avslutningsfase ble meget krevende relatert til arbeidsmengde og tidsbruk. Hovedårsaken til økt arbeidsbelastning mot slutten av prosjektfasen var knyttet til en for liten avgrensning av prosjektoppgaven. Dessuten tok det svært mye tid å utforme rammeverket da gruppen ikke hadde noen mal å ta utgangspunkt i, kun fokuspunkter fra SANS. Hvilke kapitler som skulle inkluderes måtte gruppen selv bestemme.

I retroperspektiv skulle gruppen avholdt flere møter med oppdragsgiver som kunne klargjort i større grad hvilket omfang som var overkommelig. I tillegg burde gruppen ha satt av mer tid i innledningen av prosjektfasen til å dele opp oppgaven i mindre deler og satt mye kortere perioder for hver del. Dette hadde hjulpet gruppen til å bedre identifisere hvorvidt gruppen ikke overholdt tidsskjemaet underveis, og anledning til å nedskalere omfanget i et tidligere stadium.

6.2 Arbeidsflyt

En god arbeidsflyt bidrar til strukturerte arbeidsdager. Når en jobber med prosjektoppgaver blir det ofte delt opp i roller, ansvarsfordeling og så videre. Det var derfor viktig for gruppen å definere en god arbeidsflyt for å optimalisere prosjektoppgaven så langt det lot seg gjøre.

6.2.1 Arbeidsdelegering

I prosjektperioden ble det benyttet et kanban board for delegering av arbeidsoppgaver. Kanban board bidro til en oversikt over hvilke arbeidsoppgaver som tilhørte hvilke faser. I utgangspunktet valgte gruppen å benytte scrum, men dette ble endret til kanban board etter noen måneder. Endringen ble gjort fordi gruppen ikke jobbet i sprinter, slik metodikken i scrum benytter seg av. Kanban var en bedre tilnærming fordi gruppen stadig opprettet nye gjøremål som ble løst fortløpende.

6.2.2 Dagsstruktur

Gruppen ble enig om fem dager arbeid i uken fra klokken 09:00 - 15:00. Dette mente gruppen var en nødvendig arbeidsmengde for å oppnå god fremdrift i prosjektoppgaven. Formålet med faste dager var å ha en klar forventning til arbeidsmengde. Gruppen ønsket også å unngå skippertaksarbeid og ville organisere seg på best mulig måte for å gi en lineær progresjon.

Senere i prosjektperioden ble gruppens arbeidstider mer fleksibel. Det var fremdeles faste arbeidsøkter fra 09:00 - 15:00, men arbeid utenfor normal arbeidstid var mulig og gjerne oppfordret. For noen gruppemedlemmer kolliderte noen faste arbeidsøkter med timeplan. Tapt tid skulle tas igjen. Dette var nødvendig for å unngå skjev arbeidsfordeling og for å opprettholde prosjektfremdriften.

Funksjonalitet av dagsstruktur

Dagsstrukturen var ment å simulere en vanlig arbeidsdag. Arbeidet ble på den måten forutsigbart og håndterbart. Faste møtetider økte dessuten tilgjengeligheten og kommunikasjon mellom gruppemedlemmene, og dette førte til enklere samarbeid.

6.2.3 Fordeler og ulemper

Faste arbeidsdager har sine fordeler og ulemper. Her følger noen fordeler gruppen støtte på:

Fordeler

- Enkel kommunikasjon
- Økt tilgjengelighet av gruppemedlemmer
- Økt forutsigbarhet til prosjektframdrift
- Konstant rutine som er lett å forholde seg til

Fordelene med en slik dagsstruktur var mangfoldig. Enkel kommunikasjon var en viktig faktor; dette var et samarbeid som krevde diskusjon og samtaler for å oppnå felles enighet i utformingen av prosjektoppgaven. For en prosjektoppgave som var så omfattende var det også en stor fordel med forutsigbarhet i hverdagen. Prosjektoppgaven krevde langtidsplanlegging, og det var enklere å oppnå med forutsigbare arbeidsdager.

Her følger noen ulemper gruppen støtte på:

Ulemper

- Repetitivt
- Mye tid foran skjermen hver dag
- Monotont arbeid

Ulempene med dagsstrukturen var få, men noen faktorer påvirket arbeidseffektiviteten. De største faktorene var knyttet til monotont og repetitivt arbeid. Dette kunne påvirke mentaliteten negativt som ledet til mindre effektive arbeidsdager enn ønsket.

6.3 Endringer til dagsstruktur

I starten av prosjektoppgaven manglet strukturen fleksibilitet når gruppemedlemmer skulle ta igjen timer som hadde gått tapt. Gruppen valgte å beholde en 09:00 - 15:00-struktur, men ble i tillegg enige om at antall timer utenfor fast arbeidstid skulle loggføres. For å sikre at gruppemedlemmene arbeidet like mye valgte gruppen å sette et ukesmål på minimum 30 arbeidstimer.

Denne strukturen fungerte godt i perioder hvor gruppen måtte øke intensiteten på arbeidet for å fullføre arbeidet med rammeverket.

Gruppen burde ha definert et minimum antall arbeidstimer i uken fra begynnelsen av. Videre kunne gruppen ha definert gjøremål med kortere frister eller arbeidsperioder for mer effektivt arbeid.

6.4 Endringer til rammeverket

Arbeidsprosessen for utviklingen av rammeverket kunne dratt nytte av flere endringer. Med bedre planlegging kunne gruppen hatt tid til å utføre testing av rammeverket ved bruk av gruppens utviklede treningsopplegg. Dette kunne gitt prosjektet mer målbare effekt- og resultatmål.

Videre kunne noen av prosessene i rammeverket knyttes opp mot eksisterende prosesser i virksomheten og programvare som er i bruk. For eksempel kunne gruppen ha utviklet en steg-for-steg-prosess for hvordan XDR kunne blitt benyttet i en konkret hendelseshåndteringsprosess. Det ville konkretisert oppgaven enda mer.

6.5 Endringer til treningsopplegg

Endringer som kunne blitt gjort på det endelige opplegget

Det var noen endringer som kunne blitt gjort på det ferdige treningsopplegget. Øvelsen består alltid av en leder og denne lederen har et stort ansvar og mye å tenke på. Gruppen kunne tenkt ut noen måter å redusere arbeidsbelastningen til lederen i øvelsen. Dette kunne blitt gjort ved å ha en bedre og mer detaljert fremgangsmåte for lederen. Treningsopplegget kunne dessuten hatt flere kort for en type hendelse som kunne veiledet lederen gjennom øvelsen, men samtidig kunne øvelsen blitt mer komplisert som et resultat av det. En annen løsning kunne vært å ha to eller flere ledere til å bistå hverandre.

Gruppen burde videre ha startet på treningsopplegget på et tidligere stadium. Det ble konkludert med at gruppen skulle jobbe med treningsopplegget etter at rammeverket var ferdigstilt. Gruppen forventet ikke at rammeverket skulle være så omfattende som det ble. Dette resulterte i at gruppen ikke fikk like mye tid som ønsket til å jobbe med treningsopplegget. Gruppen kunne vurdert å jobbe med utformingen av treningsopplegget parallelt med rammeverket. Det hadde gitt gruppen mer tid til planlegging og prøving og feiling.

6.6 Utfordringer relatert til playbooks

Det oppstod flere utfordringer med utformingen av playbooks. For det første ble det bestemt ganske langt ut i prosjektperioden at playbooks skulle inkluderes i omfanget av oppgaven. Dette ga gruppen mindre tid til utformingen enn ønskelig. På grunn av arbeid med rammeverk og gruppens sluttrapport var ikke resterende tid tilstrekkelig til å utforme playbooks. Etter diskusjon med oppdragsgiver ble det avtalt at oppdragsgiver kan benytte rammeverket som et grunnlag for utformingen av playbooks selv.

7 Avslutning

Dette kapittelet diskuterer resultatet av oppgaven. Kapittelet tar for seg det gruppen mente kunne forbedres, hva oppdragsgiver kan gjøre videre, en selvevaluering av gruppens arbeid og til slutt en konklusjon av prosjektoppgaven.

7.1 Kritikk av oppgaven

Gruppen har opplevd både mange positive og negative aspekter ved prosjektfasen. Det har vært en del utfordringer, men gruppen er for det meste fornøyd med oppgaven. Gruppen er ikke helt fornøyd med noen av de siste fasene i rammeverket, da disse fasene ikke ble like utfyllende som gruppen hadde planlagt. Det gjelder i særdeleshet 'Eradication'-fasen. Det er avtalt med oppdragsgiver at disse fasene ferdigstilles av gruppen så fort som mulig.

Oppgaven var utfordrende ettersom det var første gang medlemmene var en del av en så omfattende oppgave. Gruppen opplevde til tider at oppgaven var overveldende, og at medlemmer i noen tilfeller gikk utenfor omfanget av oppgaven. Det var ikke bevisst, og kom som et resultat av at prosjektoppgaven var vanskelig å definere og avgrense. Dette fratok gruppen en del tid.

Alle resultatmålene gruppen hadde oppgitt i starten av prosjektfasen ble oppnådd. Rapporten beskriver prosjektoppgaven i sin helhet, og gruppen har utformet et rammeverk som bistår oppdragsgiver i deres hendelseshåndteringsrutiner. Gruppen har videre utformet et treningsopplegg som oppdragsgiver kan bruke for opplæring av sitt IT-personell. Dette var de viktigste resultatmålene. De generelle resultatmålene ble også oppnådd. Rammeverket kan benyttes som et referanseverk for oppdragsgiver, og treningsopplegget er designet for å engasjere ansatte i fagområdet om hendelseshåndtering.

7.2 Videre arbeid

Trusselbildet endrer seg stadig og følgelig må virksomheter oppdatere sine rutiner. Både rammeverket og treningsopplegget er designet for å kontinuerlig oppdateres og endres.

Treningsopplegget er ikke helt komplett da det eksisterer flere angrepstyper som ikke er inkludert. Malen for å legge til angrepstyper er satt opp med eksempler og oppdragsgiver kan selv legge til angrepstyper de mener er relevante. Treningsopplegget kan senere brukes som grunnlag til utvikling av et cyber range-miljø, der deltakerne kan teste sine ferdigheter i et virtuelt testmiljø med mulighet for mer tekniske utfordringer.

Oppdragsgiver kan utforme egne playbooks med rammeverket som grunnlag. Ettersom playbooks skal være en nedskalert versjon av rammeverket skal mye informasjon allerede foreligge i rammeverket.

Videre kan prosjektoppgaven legge til rette for en analyse av hvorvidt effekten til rammeverket og treningsopplegget reduserer tiden det tar for sikkerhetsteam å håndtere en sikkerhetshendelse, ved å sammenligne opp mot tidligere håndterte hendelser.

7.3 Evaluering av gruppens arbeid

Gruppedynamikken har fungert godt, og alle gruppemedlemmer har ferdigstilt delegerte arbeidsoppgaver. Gruppen har tidligere jobbet sammen på andre prosjekter, og det var en fordel for denne prosjektoppgaven. Gruppearbeidet har i stor grad foregått over kommunikasjonsplattformen Discord i hele prosjektperioden. Fysisk oppmøte ble forsøkt, men gruppen følte at det ikke fungerte optimalt. Gruppen jobbet aldri mindre enn fem dager i uken, men mot slutten av prosjektperioden ble arbeidstid økt betraktelig med mye kvelds- og helgejobbing i tillegg.

Det har ikke vært noen store konflikter innad i gruppen. I starten av prosjektperioden oppstod det et problem med at noen gruppemedlemmer ikke alltid kunne delta på de normale arbeidsøktene. Problemet ble raskt løst i fellesskap, og løsningen fungerte uten behov for endringer. Det var også noe sykdom i gruppen, men det begrenset seg til noen få dager og påvirket ikke arbeidet i stor grad.

Rollene i gruppen har fungert som forventet. Lederrollen var rullerende mellom gruppemedlemmene og formålet med en slik ordning var at alle medlemmer skulle ta eierskap til prosjektet og

føle på hvordan det var å ha et overordnet ansvar for oppgaven. Mot slutten av perioden mente gruppen at det var ett medlem som egnet seg best til rollen. Dette var mye basert på erfaringer fra tidligere prosjekter og medlemmets evne til å drive prosjektoppgaven fremover. Alle på gruppen var enig i denne beslutningen.

Gruppen forsøkte å holde arbeidsmengden jevn gjennom hele prosjektperioden, men det gikk ikke helt som planlagt. Hovedårsaken til dette var at omfanget av oppgaven ble mye større enn forventet. Det førte til at playbooks ikke ble utformet, og de siste fasene av rammeverket ikke ble helt ferdigstilt før utforming av rapporten måtte prioriteres.

Oppdragsgiver har vært svært hjelpsom og fremstått som veldig imøtekommende for gruppens ønsker gjennom hele prosjektperioden. Spørsmål ble besvart fortløpende, og møter ble avholdt jevnlig. Dette førte til at oppdragsgiver ble en viktig bidragsyter i utformingen av oppgaven, og ikke en hemsko gruppen måtte vente på tilbakemelding fra.

Oppdragsgivers tilbakemelding til gruppen var som følger:

> *Oppstart*
>
> Vi får en gruppe studenter som viser stor interesse for faget og som kommuniserer godt med oss som oppdragsgiver. Vi føler litt på hvordan oppgaven skal scopes for å holde oppgaven innenfor tidsrammen samt treffe godt på et rammeverk vi kan bygge videre på. Gruppen stiller gode spørsmål og samler masse informasjon som gir oppgaven en god start.
>
> *Mellomfase*
>
> I denne fasen så jobber gruppen veldig selvstendig og former oppgaven i stor grad på egenhånd. Vi syntes vurderingene til gruppen er fornuftige og blander oss lite inn i oppgaven utenom det å svare opp spørsmål gruppen har. Vi forsøker å holde fornuftige arbeidsmøter for å forsikre oss om at gruppen ikke må vente på oss for svar.

Sluttfase

Vi innser at scopet kanskje er litt stort i forhold til tiden oppgaven er berammet til. Gruppen tar kloke valg for nytt scope som gjør at Moelven er i stand til å benytte rammeverk og treningsplan i videre arbeid. Dette treffer meget godt innenfor vårt ønske for oppgaven. (Tom Kjølhamar, 2022)

7.4 Konklusjon

Gruppen er fornøyd med å ha gjennomført bacheloroppgaven. Det har vært en svært lærerik prosess med stort læringsutbytte, både faglig, men også knyttet til det å jobbe i et team over en lengre periode. Å gjennomføre en oppgave for en ekstern oppdragsgiver har gitt gruppemedlemmene en stor ansvarsfølelse, og har vært givende og motiverende.

Gruppen fikk ikke bruk for så mange tekniske ferdigheter som har blitt lært i løpet av studieløpet da oppgaven ikke krevde det. For å løse oppgaven hadde gruppen stor nytte av emnene 'Risikostyring' og 'Introduksjon til hendelseshåndtering'.

I løpet av prosjektperioden har gruppen lært mye om hendelseshåndtering. Gruppen fikk mulighet til å lære om hvordan et stort skandinavisk industrikonsern håndterer hendelseshåndtering og generell informasjonssikkerhet. Gruppen fikk utformet et rammeverk og et treningsopplegg for oppdragsgiver. Rammeverket gir også oppdragsgiver et grunnlag til å utforme playbooks. Gruppen har utformet oppgaven med den hensikt at oppdragsgiver kan ta i bruk rammeverket og treningsopplegget og kontinuerlig forbedre disse slik at hendelseshåndteringen i virksomheten stadig styrkes.

Litteraturliste

[1] Akashdeep Bhardwaj mfl. «Why is phishing still successful?» I: *Computer Fraud & Security* 2020.9 (2020), s. 15–19.

[2] Wesley Chai. *incident response*. Tekn. rapp. 2020. URL: https://www.techtarget.com/searchsecurity/definition/incident-response.

[3] Crowdstrike. *INCIDENT RESPONSE STEPS*. Tekn. rapp. 2021. URL: https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/.

[4] Erlend Andreas Gjære. *Er du et "ja"-menneske?* Tekn. rapp. 2022. URL: https://securepractice.co/bulletins/nb-no/er-du-et-ja-menneske/78.

[5] Katie Terrell Hanna. *brute-force attack*. Tekn. rapp. 2021. URL: https://www.techtarget.com/searchsecurity/definition/brute-force-cracking.

[6] Alexander Harsch, Steffen Idler og Simon Thurner. «Assuming a state of compromise: A best practise approach for SMEs on incident response management». I: *2014 Eighth International Conference on IT Security Incident Management & IT Forensics*. IEEE. 2014, s. 76–84.

[7] ISACA. *Building a Better Digital World for All*. Tekn. rapp. 2022. URL: https://www.isaca.org/.

[8] ISACA. *HISTORY*. Tekn. rapp. 2022. URL: https://www.isaca.org/why-isaca/about-us/history.

[9] ISACA. *ISACA Certifications*. Tekn. rapp. 2022. URL: https://apmg-international.com/isaca-certification.

[10] Kaspersky. *What is Spoofing – Definition and Explanation*. Tekn. rapp. N.d. URL: https://www.kaspersky.com/resource-center/definitions/spoofing.

[11] Henrik Kniberg. «Kanban vs scrum». I: *Crisp AB. Viitattu* 1 (2009), s. 1–41.

[12] Ben Lutkevich. *MITRE ATT&CK framework*. Tekn. rapp. 2020. URL: https://www.techtarget.com/searchsecurity/definition/MITRE-ATTCK-framework.

[13] MITRE. *Command and Control*. Tekn. rapp. 2019. URL: https://attack.mitre.org/tactics/TA0011/.

[14] MITRE. *Discovery*. Tekn. rapp. 2019. URL: https://attack.mitre.org/tactics/TA0007/.

[15] MITRE. *Enterprise Matrix*. Tekn. rapp. 2022. URL: https://attack.mitre.org/matrices/enterprise/.

[16] MITRE. *Execution*. Tekn. rapp. 2019. URL: https://attack.mitre.org/tactics/TA0002/.

[17] MITRE. *Exfiltration*. Tekn. rapp. 2019. URL: https://attack.mitre.org/tactics/TA0010/.

[18] MITRE. *Initial Access*. Tekn. rapp. 2020. URL: https://attack.mitre.org/tactics/TA0001/.

[19] MITRE. *Lateral Movement*. Tekn. rapp. 2019. URL: https://attack.mitre.org/tactics/TA0008/.

[20] MITRE. *Privilege Escalation*. Tekn. rapp. 2021. URL: https://attack.mitre.org/tactics/TA0004/.

[21] MITRE. *Reconnaissance*. Tekn. rapp. 2020. URL: https://attack.mitre.org/tactics/TA0043/.

[22] MITRE. *TTP-BASED HUNTING*. Tekn. rapp. 2020. URL: https://www.mitre.org/publications/technical-papers/ttp-based-hunting.

[23] NAOB. *patche*. Tekn. rapp. 2022. URL: https://naob.no/ordbok/patche.

[24] Netsecurity. *Hendelseshåndtering*. Tekn. rapp. 2022. URL: https://www.netsecurity.no/tjenester/hendelseshandtering.

[25] Nettvett. *Løsepengevirus*. Tekn. rapp. 2021. URL: https://nettvett.no/losepengevirus/.

[26] Nettvett. *Phishing*. Tekn. rapp. 2019. URL: https://nettvett.no/phishing/.

[27] Stephan Neuhaus og Thomas Zimmermann. «Security trend analysis with cve topic models». I: *2010 IEEE 21st International Symposium on Software Reliability Engineering*. IEEE. 2010, s. 111–120.

[28] NHO. *Hva er et cyberangrep?* Tekn. rapp. 2022. URL: https://arbinn.nho.no/Medlemsfordeler/medlemsfordeler-nho/nho-forsikring/sporsmal-og-svar/hva-er-et-cyberangrep/.

[29] NIST. *Computer Security Incident Handling Guide*. Tekn. rapp. 2012. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

[30] NIST. *Overview*. Tekn. rapp. 2022. URL: https://www.nist.gov/cybersecurity.

[31] NSM. *DIGITAL SIKKERHET*. Tekn. rapp. 2022. URL: https://nsm.no/fagomrader/digital-sikkerhet/.

[32] NSM. *GRUNNLEGGENDE TILTAK FOR SIKRING AV E-POST*. Tekn. rapp. 2022. URL: https://nsm.no/getfile.php/133663-1592828388/Filer/Dokumenter/u-02-grunnleggende-tiltak-for-sikring-av-e-post---endelig.pdf.

[33] NTNU. *Hvordan strukturere teksten? Oppgavens struktur*. Tekn. rapp. n.d. URL: https://www.ntnu.no/sekom/oppgavens-struktur.

[34] NTNU. *Norwegian Cyber Range*. Tekn. rapp. N.d. URL: https://www.ntnu.no/ncr.

[35] Cyril Onwubiko og Karim Ouazzane. «SOTER: A playbook for cybersecurity incident management». I: *IEEE Transactions on Engineering Management* (2020).

[36] Andy Patrizio. *data loss prevention (DLP)*. Tekn. rapp. 2021. URL: https://www.techtarget.com/whatis/definition/data-loss-prevention-DLP.

[37] Iris Rieff. «Systematically Applying Gamification to Cyber Security Awareness Trainings: A framework and case study approach». I: (2018).

[38] SANS. *Expertise Matters*. Tekn. rapp. 2022. URL: https://www.sans.org/security-awareness-training/why-sans/.

[39] SANS. *Incident Handler´s handbook*. Tekn. rapp. 2021. URL: https://sansorg.egnyte.com/dl/6Btqoa63at.

[40] Mary E. Shacklett. *rootkit*. Tekn. rapp. 2021. URL: https://www.techtarget.com/searchsecurity/definition/rootkit.

[41] Mary E. Shacklett. *spear phishing*. Tekn. rapp. 2020. URL: https://www.techtarget.com/searchsecurity/definition/spear-phishing.

[42] TechTarget. *forensic image*. Tekn. rapp. 2017. URL: https://www.techtarget.com/whatis/definition/forensic-image.

[43] TechTarget. *SMiShing (SMS phishing)*. Tekn. rapp. 2007. URL: https://www.techtarget.com/searchmobilecomputing/definition/SMiShing.

[44] TechTarget. *Wipe*. Tekn. rapp. 2012. URL: https://www.techtarget.com/whatis/definition/wipe.

[45] Jacob Young og Sahar Farshadkhah. «Backdoors & Breaches: Using a Tabletop Exercise Game to Teach Cybersecurity Incident Response». I: *Proceedings of the EDSIG Conference ISSN*. Bd. 2473. 2021, s. 4901.

[46] Anne Aarnes. *url*. Tekn. rapp. 2022. URL: https://www.crowdstrike.com/cybersecurity-101/what-is-xdr/.

A Vedlegg: Rammeverk

Preparation

Espen Eriksen, Jan Ngo, Farhaz Ismail, Ranvir Singh

May 19, 2022

Contents

1 Om denne fasen

Formålet med denne fasen er å sikre at virksomheten er best mulig forberedt på sikkerhetshendelser eller cyberangrep. Fasen tar for seg ulike sikkerhetsmekanismer og andre forebyggende tiltak som kan bidra til å redusere risikoen for at hendelser oppstår, men også beskytte virksomheten når en hendelse først har inntruffet. Fasen inkluderer både retningslinjer og prosedyrer for å forberede seg mot potensielle hendelser.

2 Revisjonsplan

2.1 Revisjonplanens formål

Hendelseshåndtering er et relativt ferskt fagområde og er i stadig utvikling. Det oppstår kontinuerlig nye sikkerhetshendelser og metoder for å utføre cyberangrep, og dermed også metoder for å beskytte seg. Det er helt essensielt å regelmessig oppdatere seg på hendelseshåndteringsprosessen. Revisjonsplanen skal danne et beslutningsgrunnlag for vurdering av revisjonsaktiviteter, og eventuelt implementere disse i rammeverket.

Revisjonplanen skal gjennomgås i sin helhet minst én gang i intervaller på ett år, men kan gjennomgås oftere ved behov.

2.2 Revisjonsprosess

I forkant av en revisjonsprosess må en kartlegge hva og hvorfor det skal revideres. Tiltak skal skje på grunnlag av at elementer i rammeverket må endres for en mer effektiv og optimalisert prosess.

Overblikk

Behov for revisjonstiltak oppstår gjerne i løpet av en hendelseshåndteringsprosess. Fasen "Lessons learned" skal avdekke hvilke mangler en oppdaget under denne prosessen. For phishingangrep kan det blant annet gjelde kommunikasjon, kultur, informasjon, kunnskap og opplæring. Et løsepengevirusangrep vil muligens avdekke mangler i overvåkning, urapporterte hendelser, uvitende ansatte og så videre. "Lessons learned" er en fase som må følges opp og er tett tilknyttet revisjon av rammeverket.

Revisjon

Revisjonen gjennomføres når det er konsensus om hva som trenger endring eller optimalisering.

Følgende er en tabell en kan følge for å danne en oversikt over revisjonstiltak:

NB! Dette er kun et eksempel.

Hva må forbedres	**Hvordan skal det forbedres**	**Hvem er ansvarlig**	**Når skal tiltaket gjennomføres**	**Hvem skal oppfølge tiltaket**
Kommunikasjon	Oppfordring og opplæring av ansatte	Kriseleder	03.09.2022	Kriseleder
E-posthåndtering	Opplæring	IT	21.04.2022	Kriseleder

Følgende er en tabell en kan følge for oppfølging av revisjonen:

NB! Dette er kun et eksempel.

Hvilken hendelse/årsak ble revisjonen gjennomgått for	**Revisjonsdokument opprettet**	**Er revisjon oppfulgt og lukket**
Phishing	Revisjonsdokument om phishing, 01.04.2022	Ja
Løsepengevirus	Revisjonsdokument om løsepengevirus, 04.08.2021	Nei

Det anbefales å ta utgangspunkt i denne malen, og eventuelt supplere med mer informasjon ved behov, og fylle ut denne fortløpende. Det er den ansvarlige sitt ansvar å følge opp at tiltakene blir implementert og at revisjonen ferdigstilles og lukkes. Alle revisjoner bør lagres på et fast, definert lagringsområde som kun nødvendige personer har tilgang til.

Disse tabellene skal benyttes for å gi en ryddig oversikt på alle revisjoner og revisjonstiltak.

3 Rutiner

Gode rutiner for informasjonssikkerhet kan eliminere og redusere mange angrepsvektorer, og blir derfor en viktig praksis å følge. Tre relevante rutiner for virksomheten er sikkerhetskopiering, kartlegging av sårbarheter ved bruk av åpne kilder, og oppdatering av systemer.

Rutine 1: Sikkerhetskopiering

Jevnlig sikkerhetskopiering av data og systemer er en viktig rutine for å raskt hente systemer tilbake til produksjon etter en hendelse. Det er derfor avgjørende at virksomheten har en godt definert og planlagt prosess. Elementer som bør defineres er en liste over hva som sikkerhetskopieres, hyppighet på sikkerhetskopiering og hvilken type (full, inkrementell) og hvilke instanser som kjører sikkerhetskopier.

Her må det lages en tabell eller rutine på testing av gjenoppretting.

Det anbefales at det er implementert både offline- og offsite-sikkerhetskopi for virksomhetskritisk data.

Periodevis test av gjenoppretting av data bør gjøres. Intervaller på dette kan variere, men bør være definert og gjennomføres.

For å få en oversikt over dette kan sikkerhetsteamet føre inn i tabellen under. Systemkolonnen er navnet til systemet, CIA-score er hentet fra vurderingen av systemet, hvor ofte kopi skal tas føres inn i hyppighet på sikkerhetskopi, type kopi som tas av systemet føres inn deretter, og til slutt de serverene som utfører selve kopieringen.

System	**CIA-score**	**Hyppighet på sikkerhetskopi**	**Type sikkerhetskopi (full, inkrementell)**	**Instanser som kjører kopieringen**

Rutine 2: Gjennomgang av åpne kilder

Gjennomgang av åpne kilder vil holde sikkerhetsteamet oppdatert på trusselbildet og hvordan det utvikler seg. Å ha en god rutine for dette er viktig for å kunne respondere raskt til nye trusler. Åpne kilder er offentlig tilgjengelig data om cybertrusseletterretning, som bør brukes av sikkerhetsteamet for å holde seg oppdatert på den nyeste informasjonen og vil hjelpe med oppdagelse av potensielle sikkerhetshull. Dersom sikkerhetsteamet mener de ikke er rustet for angrep bør det undersøkes om systemer har aktuelle sårbarheter og deretter håndtere dette.

Foreslått liste til OSINT:

- Random
- CrowdStrike Intelligence
- CISA sårbarhetsliste
- Mandiant News Analysis
- Dark web (URL?) for sjekk av lekkede brukerdetaljer

Rutine 3: Oppdatering og patching av systemer

En tredje rutine er håndtering av kjente sårbarheter, ofte forkortet CVE-[tallkode], som har blitt oppdaget i systemene. CVE gir en indikasjon på hvilke systemer som kan utsettes for nedetid eller kompromittering.

4 Policy

Følgende retningslinjer skal være et grunnlag for rutiner og opptreden som representant av en virksomhet. Formålet er å sette tydelige forventninger og krav til ansatte hos virksomheten om oppførsel og behandling av data, og samtidig gi riktig kunnskap om hvordan en opptrer under en hendelse.

4.1 Generell informasjon

Her listes en del nyttig informasjon alle brukere bør gjøre seg kjent med.

- Du er selv ansvarlig for å bruke IT-systemer i henhold til virksomhetens rutiner. En skal bruke IT-systemer til å utføre oppgaver som dere har ansvar for på en ansvarlig og profesjonell måte. Ikke bruk IT-systemene til å tilegne deg informasjon du ikke er ment å ha tilgang til.
- Bruk av sosiale medier er lov, men vær klar over det som publiseres. Det skal ikke bli publisert opplysninger som kan føre til skade på virksomhetens omdømme og virksomhetens interessenter. Publisering av skadelige opplysninger kan innebære brudd på lojalitetsplikten i arbeidsforholdet.
- Vær kritisk til bruk av kilder. Sørg for at kildene du bruker er troverdige og ikke bruk en kilde ukritisk. For nettkilder kan en se på nettadressen, domenenavnet, og oppsettet til nettsiden for å finne ut om det er legitimt.
- Vær ansvarlig og bruk sunn fornuft. Spør om hjelp ved usikkerhet.
- En skal ikke svare eller trykke på spam. Blokkér avsender og slett meldingen.
- Vær obs og bruk sunn fornuft når du trykker på lenker, åpner dokumenter eller nettsider. Vær oppmerksom på nettsider med merkelig nettadresse og oppsett.
- Unngå lagring av unødvendig informasjon lokalt på maskinen, og heller ikke på virksomhetens lagringssteder.
- IT loggfører aktiviteter for å administrere og overvåke sikkerheten i IT-systemene.
- Bærbare PC-er er klargjort for bruk fra hotell- og hjemmenettverk.
- Avsenderadresse i e-postkommunikasjon er ikke pålitelig. Personer med teknisk kompetanse kan forfalske avsenderadresse. Det er viktig å være klar over at en e-post kan være sendt av hvem som helst, selv om det ikke ser slik ut.

4.2 Varsling av hendelser

Alle ansatte i virksomheten er pliktet å rapportere og varsle om sikkerhetsrelaterte hendelser. I tillegg skal underleverandører rapportere sikkerhetsavvik. Informasjonen de rapporterer om er avhengig av hvilket system de leverer til virksomheten. Ansatte skal ikke varsle gjennom andre ansatte; dette for å oppnå en direktekobling mellom sikkerhetsteamet og vedkommende hendelsen gjelder for.

Når ansatte og underleverandører skal rapportere om en hendelse skal riktig kommunikasjonskanal brukes, avhengig av alvorlighetsgraden til hendelsen. Underleverandører bør ringe dersom avviket har middels til høy alvorlighetsgrad. Dersom en ansatt opplever at kontoen har blitt kompromittert, er hovedregelen at telefon skal benyttes for varsling. Det bør ringes når en er usikker på alvorlighetsgraden til hendelsen. Om ansatte mener at det gjelder en mindre alvorlig hendelse skal det kontaktes gjennom e-post.

Mal på hva som bør inkluderes i avviksrapporter befinner seg i fase 02 identifikasjon.

4.3 Brukeradministrasjon

Brukeradministrasjon spiller en sentral rolle for å styrke informasjonssikkerheten og unngå misbruk av systemer. Her følger noen retningslinjer for håndtering av brukere.

4.3.1 Aktivering av brukere

Før aktivering av nye brukere må de fullføre et sikkerhetskurs.

4.3.2 Sletting av brukere

For å unngå at foreldede brukerkontoer blir værende i systemet skal det kjøres regelmessig kontroll av inaktive brukere, og deretter sletting av disse. Inaktive brukere defineres som brukere som ikke har logget inn for eksempel de siste tolv månedene. Det anbefales å kjøre kontrollsjekk minst én gang i måneden. Se her for ytterligere informasjon: `https://docs.microsoft.com/nb-no/services-hub/health/remediation-steps-ad/regularly-check-for-and-remove-inactive-user-accounts-in-active-directory`

Ved ansettelsesforholdets opphør skal brukerkonto deaktiveres umiddelbart. Den ansatte plikter før arbeidstidens slutt å overlevere data tilhørende bedriften til sin nærmeste leder. Alt utstyr som tilhører arbeidsgiver skal enten reinstalleres og klargjøres for ny bruker, eller wipes og sendes til gjenvinning. Som standard er det bestemt at PC-er eldre enn fire år sendes til gjenvinning. Det er viktig at e-postkonto og privatområder slettes, helst umiddelbart og senest seks måneder etter brukerens fratreden.

4.3.3 Høyprivilegerte brukere

Det skal eksistere egne administratorkontoer med kun begrenset, nødvendige administratorrettigheter for IT-personell. Ved bruk av personlige administratorkontoer unngår en problematikk med passordbytte ved en ansatt sin fratreden i virksomheten.

Tjenestebrukere skal benyttes på applikasjoner hvor det er nødvendig og kun ha begrenset, nødvendige administratorrettigheter.

4.3.4 Annet

For mange mislykkede påloggingsforsøk mot domenet vil medføre låst brukerkonto.

4.4 Passordhåndtering

Denne seksjonen tar for seg hvordan en skal håndtere passord innad i organisasjonen.

4.4.1 For IT

Ved passordendring skal det settes et førstegangspassord som brukeren kan benytte til å sette et personlig passord. Førstegangspassord skal bli sendt på SMS eller kryptert e-post og bør aldri bli sendt i klartekst. Det skal også bli gjort en autentisering av personen før distribusjonen for å sikre at riktig person får passordet. Dette kan bli autentisert muntlig med personen, enten over telefon eller i person. Brukeren som fikk passordet skal gi beskjed om at de har fått og endret passordet til IT.

Multifaktorautentisering skal aktiveres for alle brukere.

4.4.2 For sluttbrukere

Passord skal bestå av minst 8 tegn. Lange passord pleier å være sterkere enn korte og derfor skal en ha minst 8 tegn og gjerne mer. En skal ikke bruke passord som lett kan gjettes av folk som kjenner deg, for eksempel passord som inneholder personlig informasjon som fødselsdato eller gateadresse. Gode passord inneholder en blanding av både store og små bokstaver, tall, og ikke-alfabetiske symboler som ”@” eller ”*”. Passord skal endres hver 90. dag. Det er kun lov med 3 påloggingsforsøk i timen for å hindre potensielle brute-force forsøk.

Ved endring av policy eller implementasjon av nye systemer, er det viktig at passordpolicy oppfyller følgende kriterier:

Krav til passord:

- Minst 8 tegn
- Alfabetiske tegn
- Store bokstaver (A-Z)
- Små bokstaver (a-z)
- Ikke-alfabetiske tegn
- Skal skiftes hver 90.(?) dag
- Tillatte påloggingsforsøk innenfor en gitt tidsperiode: 3

Det er ikke tillatt med gjenbruk av passord. Det medfører at samme passord ikke kan brukes på ulike jobbsystemer. Det er heller ikke tillatt å benytte passord som benyttes på private tjenester.

Det er ikke tillatt å oppbevare passord i fysisk form, for eksempel ved å skrive ned passord på en lapp. Fysisk oppbevaring av passord kan føre til at passordet kommer på avveie. En skal heller aldri dele passordet sitt med noen, uansett årsak.

4.5 E-posthåndtering

E-post er et arbeidsverktøy de aller fleste bruker til daglig, og benyttes til kommunikasjon både internt og eksternt. Dessverre er e-post en svært populær angrepsvektor, og kan anvendes av ondsinnede aktører til å få uautorisert tilgang til systemer. Av den grunn er det viktig at brukere utviser varsom håndtering av e-post. Her følger noen viktige retningslinjer for behandling av e-post.

E-postkontoen din skal kun brukes til jobbrelatert arbeid. Ikke bruk denne e-postkontoen til privat kommunikasjon. Din private e-postkonto skal heller ikke brukes til jobbrelatert arbeid.

Mistenkelige e-poster skal bli rapportert via e-post og en skal melde avvik dersom en oppdager eller mistenker at en er kompromittert.

4.6 Nettverk

Bruk av internett eksponerer virksomheten for potensielle angrepsvektorer, og det er viktig at brukere er varsomme og bevisst sin internettaktivitet for å redusere muligheten for kompromittering. Bruk av internett skal i hovedsak benyttes til jobbrelaterte aktiviteter, og usikre nettsider bør unngås. Virksomhetens etiske retningslinjer og policy for sosiale medier skal følges.

Ved behov for installasjon av programvare skal dette avklares og gjøres i samråd med IT. Det understrekes at kun lisensiert programvare er tillatt, og eventuell bruk av piratkopiert materiell kan få konsekvenser for den enkelte.

Det er et krav at alle endepunktsklienter er sikret med antivirus.

Det er viktig å ha segmenterte nettverk for å minimere risikoen for spredning av virus, og begrense tilganger til brukere. Som et minimumskrav skal det være et gjestenettverk eksterne brukere kan koble seg til.

4.6.1 Lagring

For å sikre god informasjonsflyt og redusere risiko for at data kommer på avveie eller går tapt skal arbeidsrelatert data kun lagres på tildelte lagringsområder.

En skal ikke lagre ikke-arbeidsrelatert data på disse områdene.

For flyttbare medier som minnepenner eller eksterne disker er det ikke lov å koble disse til nettverket med mindre det er klarert og godkjent av IT.

4.6.2 Ekstern tilgang

Det skal kun benyttes godkjent fjernstyringsprogramvare. Denne skal sikres med multifaktorautentisering og det skal være ett koblingsbrudd etter en viss periode med inaktivitet.

Bærebare PC-er

Bærbare PC-er levert av virksomheten skal være klargjort for bruk fra hotell og hjemmenettverk. På disse skal det installeres VPN som skal være i bruk til alle tider på offentlige områder, inkludert hjemmenettverk om det trengs aksess til virksomhetens nettverk. Antivirus eller form for XDR burde være installert for overvåking av hendelser som skulle oppstå.

Behandling av sensitiv data

Ved behandling av sensitiv data utenfor virksomheten, skal det ikke oppbevares noen steder enn tildelte lagringsområder hos virksomheten inne i deres nettverk. Skal en sende informasjonen til en person som f.eks. en kollega skal det skje via krypterte kanaler fra innsiden av virksomheten og aldri eksternt.

Fjernstyringsprogramvare

Kun godkjent fjernstyringsprogramvare skal tas i bruk. Tilgangene skal også sikres med mutlifaktorautentisering før det etableres en kobling. All fjernstyring skal ha koblingsbrudd ved inaktivitet. Det kan variere på hvor lenge før koblingsbruddet skjer, men aldri lengre enn ett døgn.

Eksterne konsulenter

Eksterne konsulenter som trenger tilgang til virksomheten skal holdes segmentert fra hovednettverket og skal inn i virksomheten med multifaktorautentisering. De skal kun få rettigheter til områder de trenger.

4.7 Opplæring

TBD

4.8 Tredjepart

Denne seksjonen omhandler hvordan brukere skal behandle utstyr, applikasjoner, enheter og systemer levert av tredjeparter.

4.8.1 Underleverandører

TBD

4.8.2 Applikasjoner

Virksomhetens IT skal ha en liste over godkjente applikasjoner. Ikke-godkjente applikasjoner er ikke tillatt å installere. Virksomhetens IT har ansvar for installasjon av programvare. Installasjon av programvare som trenger administratorrettigheter gjøres i samråd med IT.

4.8.3 Eksterne brukere

Eksterne brukere defineres som brukere som ikke er en del av virksomheten, slik at alle bransjer og divisjoner vil inngå som intern bruker. Ekstern bruker defineres som personer og/eller selskaper som bistår virksomheten, men tilhører et annet selskap.

Det er viktig at eksterne brukere som får tilgang på riktig sikkerhetsnivå. Alle som får tilgang må bruke multifaktorautentisering.

4.9 Utstyr

Denne seksjonen tar for seg retningslinjer relatert til utstyr benyttet i virksomhetens nettverk eller i sammenheng med virksomhetens verdier og/eller tjenester.

4.9.1 Internt utstyr

Internt utstyr er definert som alt utstyr godkjent og distribuert av virksomheten til sine brukere. Med distribusjon menes utstyr virksomheten selv har kjøpt inn eller fått via godkjent tredjepartsleverandør. Disse enhetene skal klargjøres for bruk i virksomhetens nettverk, og skal primært benyttes til jobbrelatert arbeid. Det er sterkt oppfordret til å unngå oppsett av private e-postkontoer og lagring av private filer på disse enhetene.

4.9.2 Eksternt utstyr

Eksternt utstyr er definert som utstyr som ikke er eid av virksomheten selv, men er tilknyttet virksomhetens nettverk. Eksempler kan være underleverandører eller kunder på gjestebesøk, eller eksterne konsulenter koblet til via VPN. Eksternt utstyr skal tilkobles gjestenettverk eller et eget, separat nettverk.

5 Sikring av infrastruktur

Denne seksjonen handler om hvordan man skal sikre ulike deler av infrastrukturen. Dette gjelder deler av infrastrukturen som applikasjoner og e-post.

5.1 Programvareoversikt

Det er viktig at denne oversikten har jevnlige revisjoner, da applikasjoner sannsynligvis vil fases ut og nye vil bli implementert. Det er også viktig slik at systemer som ikke lenger er i bruk kan fases ut og ikke ligger nedlagte (deprecated) i systemet som en mulig sårbar inngangsvektor. I tillegg er det viktig at utdaterte applikasjoner faktisk blir oppdatert eller patchet.

5.2 Sikring av e-post

Denne seksjonen består av ulike beskyttelsesmekanismer en kan implementere for e-post for å beskytte mot misbruk av egne e-posttjenere.

- SPF

  Kun autoriserte e-postservere kan sende e-post fra angitt domene. SPF er en standardmetode for e-postautentisering og bidrar til å beskytte domenet mot forfalskning (spoofing). SPF spesifiserer e-postserverne som har lov til å sende e-post på vegne av ditt domene. Mottakende e-postservere bruker da SPF til å verifisere at innkommende e-poster som ser ut til at den kom fra ditt domene faktisk ble sendt fra servere som er autorisert av deg[**SPF**]. Det er riktignok viktig å understreke at SPF stopper ikke all uønsket trafikk. En kompromittert e-postkonto som tilhører en virksomhet som benytter SPF kan passere en SPF-sjekk. Uønskede e-poster som blir sendt på vegne av domener som ikke bruker SPF vil dessuten ikke fanges opp i en SPF-sjekk.

- DKIM

  DKIM er en standardmetode for e-postautentisering som legger til en digital signatur til utgående e-poster. Mottakende e-postservere som får e-posten vil da kunne verifisere at e-posten faktisk kom fra avsenderen og ikke noen som prøver å utgi seg som avsenderen. DKIM sjekker også etter om innholdet i e-posten har blitt endret. Med

DKIM vil en kunne forbedre sannsynligheten for at legitime e-poster blir levert til mottakere. Mottakende servere kan verifisere at e-poster faktisk kom fra ditt domene, og ikke er forfalsket. [**DKIM**]

- DMARC

  1. Må enten være i kombinasjon med SPF, DKIM eller begge.
  2. Vil enklere kunne finne ut om e-posten faktisk er sendt fra deg.
  3. Kan motta rapporter for å finne ut om domenet misbrukes. Rapporter som forklarer hvor utgående e-poster har sitt opphav.
  4. Domain based Message Authentication, Reporting and Conformance.
  5. Kan ta i bruk DMARC ved å legge det inn i DNS-oppføringen for domenet.

- STARTTLS

  STARTTLS er en beskyttelsesmekanisme for overføring av e-post mellom e-posttjenere. Den sørger for autentisering av e-posttjenere og den sikrer konfidensialitet.

- Sikring av DNS bør sikres med DNSSEC

  DNSSEC er en sikkerhetsmekanisme som blir lagt inn i domenenavnsystemet. DNSSEC signerer svar på et domeneoppslag slik at en kan kontrollere at de kommer fra riktig kilde og sikre at de er uendret underveis. Svar på domeneoppslag blir altså signert kryptografisk.

- Multifaktorautentisering

  Multifaktorautentisering vil legge tt beskyttelseslag for innloggingsprosessen. Det vil si at brukere må gjennom ekstra identitetsbekreftelser for å få tilgang til brukerkontoer. Dette vil sikre brukerkontoene selv om en av identitetsbekreftelsene som for eksempel passord kommer på avveie.

- Deaktiver eldre autentiseringsprotokoller (Redigert innhold)

  Støtter ikke multifaktorautentisering så slike protokoller burde bli deaktivert.

- Deaktiver automatisk videresending til eksterne domener der det er aktuelt

  Automatisk videresending til eksterne domener kan føre til at viktig informasjon havner utenfor organisasjonen. En bør heller ha en unntaksliste for tilfeller der automatisk videresending er nødvendig.

5.3 Tjenester fra underleverandører

Denne seksjonen ble ikke inkludert i vedlegget pga. konfidensialitetsavtale.

6 Prosess for kartlegging av sårbarhetsflate

Denne seksjonen er en kartlegging over virksomhetens sårbarhetsflate. Sårbarhetsflaten er summen av angrepsvektorer en ondsinnet aktør kan utnytte til kompromittering eller forsøk

på kompromittering av systemer. Sårbarhetsflaten er dynamisk og endrer størrelse ettersom nye systemer blir faset inn, oppdatert, endret eller faset ut. En bedre kontroll over sårbarhetsflaten vil bidra til å redusere risiko for angrep da aktørens potensielle angrepsvektorer blir mindre eller bedre sikret.

Som regel vil sårbarhetsflaten vokse ettersom virksomheten implementerer flere systemer i takt med vekst på brukere, nye kundeforhold eller andre krav til den digitale plattformen. For å kunne forstå og behandle sårbarhetsflaten bør en stegvis gå gjennom en identifikasjonsprosess.

Første steg er å kartlegge angrepsflaten. Dette kan gjøres ved å kartlegge systemer, nettverk og koblinger eller integreringer mellom disse. En kan for eksempel visualisere angrepsflaten. Et angrepskart kan inneholde, men er ikke begrenset til:

- Servere
  - Applikasjonsservere, herunder bl.a. webserver,
- Endepunkter
  - Stasjonære datamaskiner
  - Bærbare datamaskiner
  - Andre mobile enheter
- Nettverk
  - Segmenterte nettverk
  - Private skytjenester
  - Offentlige skytjenester
- Nettverksenheter
  - Rutere
  - Switcher
  - Lastbalanserere

Neste steg er å identifisere hvilken risiko disse systemene utgjør. Noen parametre kan være hvor eksponert de er til internett, svakheter, systemkonfigurasjon, hvem som har tilgang, om systemet er i bruk m.m.

Deretter kan en se etter tegn på kompromittering ved å undersøke om sårbarheter har blitt utnyttet.

6.1 Aktive sårbarheter

Dette kapittelet ble ikke inkludert i vedlegget pga. konfidensialitetsavtale.

7 Definisjon av hendelser

Dette kapittelet inneholder definisjoner for ulike hendelser.

7.1 Inngangsvektorer

- SQL injection

  SQL injection er en type angrepsvektor som bruker ondsinnet SQL-kode for å få aksess til informasjon som ikke skal være ment å bli vist. Dette kan føre til tap av konfidensiell informasjon.

- Innsidetrusler

  Innsidertrusler er trusler fra personer som er en del av organisasjonen. Dette kan være nåværende ansatte og andre interessenter for organisasjonen. Disse personene kan misbruke tilgang til nettverk og andre enheter til å bevisst eller ubevisst skade organisasjonen. Å ubevisst skade organisasjonen gjennom phishing-angrep er relativt utbredt. [**InsideThreat**]

- E-post(vedlegg)

- Phishing gjennom e-post er det mest brukte angrepet mot virksomheter. Her vil den vanligvis be deg trykke på en lenke og skrive inn detaljer som kan gi angriperen tilgang til kontoen din. Lenke kan også føre til at du laster ned ondsinnet programvare som kan føre til løsepengevirus.

- Nettsider

  Ondsinnede nettsider er nettsider som prøver å installere skadevare på maskinen din. Hvis en trykker på en lenke på en slik nettside så kan det føre til at en laster ned en fil eller programvare som starter et løsepengevirusangrep. I noen tilfeller kan programvare bli lastet ned i bakgrunnen ved å bare besøke en slik nettside.

- Skytjenester

  Kompromitterte skytjenester kan ha ondsinnede filer som kan laste ned løsepengevirus på enheten din om du laster ned filen.

- Flyttbare medier

  Flyttbare medier som en USB-minnepenn kan føre til at enheter blir infisert av løsepengevirus. Slike minnepinner kan ligge hvor som helst for å friste noen til å putte det inn i enheten sin.

7.2 Phishing

Phishing er en kjent form for sosial manipulering hvor en angriper forfalsker sin identitet. Angrepet har vanligvis formål i å få uthentet informasjon [**MitreAttck**]. Forfalskningen kan være i form av en reell virksomhet, eksempler på dette er banker, butikker og andre

ulike firma. En annen form er forfalskning av personer som tar kontakt på grunn av en spesiell årsak, og spiller på medfølelsene til offeret.

Phishing i seg selv oppstår i mange ulike former, de mest relevante for virksomheten er vanlig phishing og spearphishing. Vanlig phishing er simpel form, hvor det blir sendt en stor mengde epost og sms til mange personer, uten en spesifikk målgruppe. Formålet er at ett eller flere offer tilfeldigvis trykker på lenkene i phishing medium-et og oppgir informasjon.

7.2.1 Hensikt

Phishing er ikke kun brukt for å få tak i penger eller å kjøre ondsinnet kode. Ofte kan en se at phishing-hendelser i etterkant var relatert til statssponset aktivitet for å uthente viktig data og informasjon om spesifikke myndigheter fra andre land eller firma [**governmentPhishing**]. Dette kalles "Phishing for informasjon". Denne typen phishing har sin hensikt i at den ondsinnede aktøren sender meldinger for å "phishe" for sensitiv informasjon. Aktøren er vellykket når offeret avslører sensitiv data, innloggingsinformasjon, eller annen informasjon den ondsinnede aktøren kan utnytte.

7.2.2 Spear phishing

Spear phishing er et målrettet forsøk på å innhente spesifikk informasjon. Målet varierer, men kan bestå av en gruppe personer eller et firma som angriperen har en interesse for. Formålet med disse type cybersikkerhetsangrep er ofte å anskaffe finansiell verdi eller sensitive dokumenter. Utgangspunktet er å få tak i informasjon for å bruke det til utpressing av penger.

7.2.3 Whaling

Målrettet angrep som går etter ansatte med viktige stillinger, for eksempel CEO, CFO og så videre. Typiske former for whaling kan være falske selvangivelser som blir sendt til deg gjennom e-post. Selvangivelser inneholder verdifull informasjon som navn, adresse, personnummer og bankinformasjon. En whaling-e-post kan for eksempel inneholde informasjon om juridiske konsekvenser mot virksomheten og at en må trykke på lenken for å få mer informasjon. Deretter blir en tatt til en nettside som spør om kritisk data som informasjon i en selvangivelse.

7.2.4 Smishing

Smishing benytter seg av SMS for å utføre angrep. En typisk smishing-teknikk er å sende en SMS til en mobil med en klikkbar lenke eller et returtelefonnumer. Et typisk smishing-angrep er en SMS som forteller at den kommer fra banken din. SMS-en forteller deg at bankkontoen din har blitt kompromittert og at du må svare raskt. Etter å ha trykket på lenken ber den

deg skrive inn personling informasjon som bankkontonummer og personnummer. Dette gir dem tilgang til den informasjonen og kan føre til at de får kontroll over kontoen din.

7.2.5 E-postphishing

E-postphishing er den mest vanlige formen for phishing. Hackere sender en mail der de sier at kontoen din har blitt kompromittert og at du må svare umiddelbart ved å trykke på den oppgitte linken. Deretter ber de deg skrive inn personlig informasjon som de kan få tilgang til. (En annen type for e-post phishing oppstår når en hacker sender en e-post som ser ut til å ha kommet fra deg. Hackeren hevder å ha tilgang til kontoen din og ofte at de har en video av deg. Deretter utpresser de deg til å betale deg i bitcoin for å ikke legge ut videoen.)? Se zombie phishing: `https://cofense.com/zombie-phish-back-vengeance/`

7.3 Løsepengevirus

Løsepengevirus har som formål å utpresse eiere av stjålet data og informasjon for løsepenger. Løsepengevirus kommer vanligvis i form av skadelig programvare slik som datavirus. Datavirus kan spre seg raskt og infisere flere maskiner. Dette kan kryptere deler av innhold og gjøre utilgjengelig for eier. Dette blir brukt som utpressingsvare. Løsepengevirus er ofte resultatet av suksessfult phishingforsøk. Derfor er det viktig å være obs og bli opplært i hvordan en kan oppdage phishing i en tidlig fase.

Løsepengevirus leder fort til uforventede, store skader. Det er derfor viktig å ha segmentert nettverk og gruppere innhold, brukere, data og så videre i forskjellige deler, slik at de ikke får tilgang til alt på en gang.

7.4 Hendelsesprogresjon

Phishing-angrepet inntreffer vanligvis offeret gjennom et sosialt medium som SMS, telefon, eller e-post. Herfra er det opp til offeret å styre angrepets progresjon. Selve angrepet i hendelsen kan være en ondsinnet lenke, noen som utnytter en falsk identitet for å tilegne informasjon, eller en innloggingsside som bruker såkalt "input-capture" (forklar hva dette er).

Høsting av innloggingsinformasjon (input capture) kan forekomme på flere forskjellige måter, blant annet logging av tastetrykk, høsting gjennom grafiske elementer i en nettside, kode som er installert på portaler som peker ut av det interne nettverket og tilkobling til Windows API-funksjoner som inkluderer parametere som innloggingsinformasjon. All informasjon aktøren henter ut nå kan brukes til å phishe videre innad i organisasjonen gjennom en kompromittert bruker, og installering av ondsinnede applikasjoner som løsepengevirus.

Når et phishingangrep er vellykket, må en umiddelbart finne ut hva som har blitt kompromittert. Dette er avgjørende for å finne risikonivået som må innstilles, og hvordan videre handlinger burde utføres. Ofte har det vært vellykket å tilegne seg brukernavn og passord;

dette er mye enklere å håndtere enn når viktige dokumenter og filer har blitt kryptert. Er brukernavn og passord kompromittert, må en bytte brukerdetaljer og overvåke hvor trafikken prøver seg med identifikasjonen. Sjekk at de ikke kommer seg inn på systemet, og at alle nødvendige endringer er gjort. Er det virus som har kryptert dokumenter og filer, burde dette området segmenteres og holdes vekk fra andre systemer.

7.4.1 Vanlige metoder

De tre mest vanlige metodene å utføre phishing på er gjennom tredepartstjenester, vedlegg og lenker. For tredepartstjenester vil den ondsinnete aktøren utgi seg som en legitim person, for eksempel fra et jobbbyrå. De vil etterspørre informasjon relatert til personen de utgir seg for å representere/jobbe for.

For vedlegg kan de utgi seg for å være noen relatert til firmaet offeret jobber i, og be offeret fylle ut et vedlegg, for deretter å sende utfylt vedlegg tilbake til aktøren.

Vedrørende lenker er det flere forskjellige metoder aktøren kan ta det i bruk. Lenker kan være geofenced. Dette går ut på at vanlig eller simpel phishing blir brukt, men kun den målgruppen aktøren vil rette angrepet mot blir kompromittert. I rapporten "Ugg Boots 4 Sale: A Tale of Palestinian-Aligned Espionage" ble nettopp denne metoden brukt. Her brukte en aktør lenker til nyhetssider. Om offeret var utenfor geofence-området ville lenken videresendt personen til nyhetssiden, men om offeret var innenfor aktuelt område ville lenken videresende offeret først til en side som automatisk lastet ned en ".rar"-fil som inneholdt ondsinnet programvare.

8 Klassifisering og prioritering av hendelser

8.1 Prioritering av systemer

I forberedelsesfasen er det viktig at systemer blir klassifisert slik at en vet hvor alvorlig konsekvensene er ved en sikkerhetshendelse og hvor kritisk responsen må være. Dette vil hjelpe med å prioritere hvilke hendelser som må håndteres først. Klassifisering vil også gi oss mer innsikt for beskyttelseskravene for systemene. Dette vil hjelpe til med å opprettholde konfidensialiteten, integriteten og tilgjengeligheten til systemene.

8.1.1 Tilgjengelighet

Å kartlegge oppetidskravene til systemene som blir påvirket ved en hendelse er nødvendig for å måle skadeomfanget. Noen tjenester og systemer er nødvendige for at virksomheten skal kunne fortsette. Oversikten over viktige systemer vil redusere MTTR (Mean Time To Repair)[**barabady2007availability**]. Reduksjon i MTTR øker påliteligheten av systemene.

For å kunne vurdere tilgjengeligheten til systemene kan en dele opp større systemer og atomisere det til mindre deler. De mindre delene vil til sammen utgjøre kritiske systemer som avhenger av høy oppetid.

Det er ikke nødvendigvis kun maskineri eller datasystemer som klassifiseres som systemer, men også brukere som er ansvarlige for deler eller hele prosesser. Når en tar med alle underprosessene vil det gi et mer komplett bilde over systemer som blir påvirket.

	Lav	**Middels**	**Høy**	**Kritisk**
Tilgjengelig-hetsnekt	Over 24 timer	5 timer til 24 timer	30 minutter til 5 timer	0 til 30 minutter

Tabellen brukes for å klassifisere systemet basert på akseptabel nedetid. Systemet vil få en lavere prioritet under en hendelse dersom det er større aksept for lengre nedetid. Klassifisering av applikasjoner og systemer i tabellen vil gi et spektrum av hvor lenge tilgjengelighetsnekt ikke har store følger.

8.1.2 Konfidensialitet

Å bestemme konfidensialiteten til system er viktig for å vite hvor alvorlig det er om uvedkommende får tilgang til informasjonen. Det er viktig at informasjon kun er tilgjengelig for de som skal ha tilgang til det. Om for eksempel strategidokumenter kommer på avveie kan det få monetære konsekvenser for virksomheten. Dette er et eksempel på en hendelse som går under "høy" i tabellen under.

I tabellen ser vi hva som klassifiseres fra lav til kritisk. Lav har ganske åpen tilgjengelighet

til informasjon og kritisk har strengt fortrolig informasjon. Denne oversikten kan brukes som en pekepinn til å bestemme hva en skal prioritere under en hendelse. En må vurdere hvor viktig informasjonen en håndterer er og angi hvilket nivå den skal være på. En vurderer slik informasjon ved å se på konsekvensene den kan ha dersom informasjonen blir sett av uvedkommende. [**unit2020**]

	Lav	**Middels**	**Høy**	**Kritisk**
Konfidensialitet	Åpen tilgjengelighet, altså informasjonen er tilgjengelig for alle uten særskilte tilgangsrettigheter	Informasjonen har beskyttelse til en grad, men både interne og eksterne kan få tilgang til den	Informasjonen har strenge tilgangsrettigheter og tap av konfidensialitet kan forårsake skade på virksomheten	Informasjon har strenge tilgangsrettigheter og tap av konfidensialitet kan forårsake betydelig skade på virksomheten og andre interesser

8.1.3 Integritet

Integriteten til systemer er viktig for å kunne stole på at data er reell og ikke endret på av uvedkommende. En sikrer et systems integritet ved å ha sikkerhetskontroller. Disse sikkerhetskontrollene skal forhindre endring av informasjon fra uautoriserte parter. Tiltak en kan utføre for å sikre informasjonen er kryptering, tilgangskontroll, sikkerhetskopier, versjonskontroll og iverksetting av programvare som kan oppdage feil. Angrep som kompromitterer integritet i databaserte systemer er en økende faktor innen cybersikkerhetshendelser [**sridhar2010data**].

Alle systemene som behandler informasjon er relevante for integritetsvurderingen. Det er viktig at en verifiserer integriteten til informasjonen som kommer inn til bedriften, som strømmer inne i bedriften, og informasjonen som bedriften sender ut.

	Lav	Middels	Høy	Kritisk
Integritet	Minimal påvirkning hvis informasjon er unøyaktig eller ufullstendig	Kan bli noe berørt ved tap av integritet, men situasjonen kan enkelt bli oppdaget og gjenopprettet	Tap av integritet vil føre til betydelig skade eller forstyrrelser og kan føre til stopp av arbeid. Er også vanskelig å oppdage	Ingen tap av integritet er tolerert og tap av integritet her kan føre til stor skade

Tabellen brukes for å vurdere systemets eller komponentens krav til integritet. De som har minimal påvirkning og passer beskrivelsen for lav integritet får lav prioritering, mens det med høye krav til integritet får høyere prioritering.

8.1.4 CIA-tabell

For å få en bedre oversikt over systemene og hvordan de er vurdert på konfidensialitet, integritet og tilgjengelighet kan en bruke tabellen under. En setter inn hvilket system eller verdi som har blitt vurdert inn i kolonnen helt til venstre som heter "system/verdi", deretter setter en verdiene for konfidensialitet, integritet og tilgjengelighet fra vurderingene en gjorde tidligere. Totalscoren er satt lik den høyeste verdien for enten konfidensialitet, integritet eller tilgjengelighet. Scoren er parameteren systemene skal rangeres etter.

System/verdi	Konfidensialitet	Integritet	Tilgjengelighet	Score

8.2 Klassifisering av angrep

For å kunne klassifisere hendelsene riktig må en også se på selve angrepet og vurdere alvorlighetsgraden. Tabellen under brukes for å vurdere alvorlighetsgraden til angrepet i hendelsen.

Alvorlighetsgrad	Beskrivelse
S1	Ikke alvorlig, lite effekt på viktige systemer, ingen kompromittert data. burde være oppmerksom over det og ev. overvåke.
S2	Mindre alvorlig, kan komme seg inn i systemer og kompromittere en liten mengde data, burde planlegge tiltak.
S3	Alvorlig, virkninger på kritiske systemer kan medfølge hendelsen i fremtiden, data med medium krav på konfidensialitet, integritet og tilgjengelighet har blitt kompromittert, tiltak burde implementeres raskt.
S4	Svært alvorlig, kritiske systemer er under risiko for å bli kompromittert, tiltak må implementeres med en gang.

Tabellen brukes for å rangere angrep fra S1-lav til S4-høy. S1 betyr at angrepet har lav eller ingen påvirkning på kjørende systemer og for framtiden av organisasjonen. Noen eksempler på type angrep som hadde blitt rangert som lav basert på alvorlighetsskalaen er tjenestenekt på systemer med lav krav på tilgjengelighet, portskanning på systemer som ligger utenfor det interne nettverket eller som er tilgjengelig offentlig, veldig åpenbar phishing på ansatte og spam.

S2 betyr at aktøren muligens har fått tilgang til systemer som har blitt klassifisert med lav CIA-score og kompromittert uviktig data eller i liten skala. Angrep som hadde blitt vurdert med middels alvorlighetsgrad kan være vellykkede angrep som uthenter data som har middels krav på konfidensialitet, men vil ha lavere skadeomfang for virksomheten ved lekkasje, vellykket phishing på brukere med få rettigheter.

For S3 har den ondsinnete aktøren fått tilgang og utført angrep som kan få alvorlige virkninger på systemer eller data med høyere krav på tilgjengelighet, konfidensialitet og integritet. Angrep som hadde blitt vurdert med middels alvorlighetsgrad kan være vellykkede angrep som uthenter data som har middels krav på konfidensialitet, men vil ha lavere skadeomfang for virksomheten ved lekkasje, vellykket phishing på brukere med få rettigheter.

S4 betyr at angrepet for tilgang var vellykket og er nå inne med et angrep som kan kompromittere store deler av nettverk og systemer. Dette er en svært alvorlig hendelse og tiltak må implementeres med en gang. Angrep klassifisert som kritiske er målrettede, de sikter på infrastruktur og systemer som er viktige for normal drift. Disse angrepene kan føre til store lekkasjer av sensitiv data og kompromittering av brukere med større mengder rettigheter.

8.3 Eksempler på angrep

Spam er et bredt ordtak for alle typer eposter, SMS, nettsider og sprettoppvinduer som forsøker å få brukeren til å trykke på av ren interesse, og deretter utgi informasjon om deg. Denne typen angrep er tilfeldig og har ingen spesiell formål.

Bruk av portskannere, nettverksskannere o.l. er ofte tegn på at aktør prøver å kartlegge sikkerhetshull som kan utnyttes. I dag er det mange tjenester med innebygd deteksjon av dette. Denne typen angrep er ikke et tegn kompromittering, men et tegn på at angrep eller forsøk på angrep kan være nært forestående.

Phishing er et kjent fenomen som ofte har som mål å få tak i sensitiv informasjon. Phishingangrep er ikke like opportunistisk som spa. Noen eksempler på interessant informasjon er brukernavn og passord, kontonummer og lignende. Det finnes målrettet phishing som sikter på personer med viktige roller eller personer med større roller. Denne type angrep kan by på en betydelig risiko dersom angrep er vellykket.

Skadevare er programvare som har som formål å finne måter å uthente informasjon til bruk som gisselvare, løsepengevirus eller installere rootkits, backdoors, virus og trojanere for å kompromittere systemer. Hvis initielle steg av angrepet er vellykket, i type form av phishing, er skadevare en vanlig hendelse som følger etter. Skadevare kan potensielt få store konsekvenser.

Tjenestenekt er angrep i form av massetrafikk som fører til at systemer overbelastes og ikke klarer å opprettholde normal drift. Mest kjente form av dette angrepet er DDoS som sender store mengder med trafikk til samme destinasjon til det overbelastes. Dette kangi store konsekvenser og kostnader for organisasjonen som påvirkes om de ikke har failover-servere eller andre midler for å opprettholde normal drift under angrepet.

Bruk av opphavsrettet innhold er ikke et angrep, men mer unødvendig bruk av ressurser fordi det ble tatt i bruk og publisert opphavsrettet innhold. I verste fall kan sanksjoner oppstå.

Informasjonslekkasje er ikke et angrep i seg selv, men en sårbarhet som leder til store konsekvenser om det skulle skje. Informasjonslekkasje kan lede til gisselvare og tap av omdømme. Dette skal være veletablerte retningslinjer, lover og regler som motbyr dette.

8.4 Helhetlig klassifisering av hendelsen

Hendelser skal klassifiseres basert på prioriteringen av systemene og hvor alvorlig angrepet i hendelsen er. Denne vurderingen skal gjøres når en sikkerhetsrelatert hendelse oppstår for å kunne delegere ressurser optimalt. Under ligger det en mal med par eksempler på hvordan hendelsen i sin helhet kan vurderes. Malen hjelper med å visualisere hendelsen og systemene som blir påvirket, hvor dataene fra malen kan brukes videre i hendelseslogging for eksempel. Scoren skal regnes ut med å gange CIA-scoren med alvorlighetsgraden til angrepet, om alvorlighetsgraden er S1 skal CIA scoren ganges med 1, om graden er S2 så skal det ganges med 2, og så videre.

System	CIA score	Angrepstype	Alvorlighetsgrad	Score

9 Kommunikasjonsplan

I denne seksjonen beskrives prosedyren for kommunikasjon i en hendelse fra start til slutt. Det følger også en oversikt over en intern og ekstern varslingsliste, samt rutiner for periodevis revisjon av planen og i andre tilfeller dette må gjennomføres, eksempelvis etter en større hendelse, trening av IT-personell eller endring av kontaktpersoner.

Kommunikasjonsprosedyren vil avhenge av hvilken klassifisering hendelsen blir tildelt. En hendelse kan bli klassifisert fra S1 opp til S4, der S1 har lavest alvorlighetsgrad og S4 har høyest alvorlighetsgrad.

9.1 Revisjonsplan

Det er bestemt at kommunikasjonsplanen skal gjennomgå revisjon etter håndtering av en større hendelse (større er definert som S3 / S4), endring av kontaktperson o.l. Dessuten gjennomføres det som et minimum en årlig revisjon av hele rammeverket, hvor kommunikasjonsplan inngår som en del av dette.

9.2 Kommunikasjonskanaler

Dette kapittelet ble ikke inkludert i vedlegget pga. konfidensialitetsavtale.

9.3 Intern varslingsliste

Dette kapittelet ble ikke inkludert i vedlegget pga. konfidensialitetsavtale.

9.4 Ekstern varslingsliste

Dette kapittelet ble ikke inkludert i vedlegget pga. konfidensialitetsavtale.

9.5 Eskalering av hendelse

Basert på en helhetlig vurdering av hendelsen, blir hendelsen tilordnet en klassifisering.

9.5.1 S1 / S2

Dersom hendelsen faller under klassifisering S1 eller S2, vil den vurderes til å ha en mindre/lav alvorlighetsgrad.

9.5.2 S3 / S4

Dersom hendelsen faller under klassifisering S3 eller S4, vil den vurderes til å ha en middels/høy alvorlighetsgrad.

10 Team og roller

Dette kapittelet ble ikke inkludert i vedlegget pga. konfidensialitetsavtale.

10.1 Roller

Triage-ansvarlig Den triage-ansvarlige har det overordnede ansvaret for å følge med på ulike innkommende varsler eller saker som legges inn.

Den triage-ansvarlige må avgjøre hvorvidt hendelsen er kritisk nok til å begynne hendelseshåndteringsprosessen. Dersom hendelsen viser seg å være kritisk nok, skal hendelsen tilordnes en prioriterings- og alvorlighetsgrad, og hendelsesleder varsles.

Sjekkliste for triage-ansvarlig:

- Avgjøre hvorvidt hendelsen er kritisk nok til å påbegynne hendelseshåndteringsprosess
- Logg hendelsen. Dette kan skje automatisk, men det er viktig at triage-ansvarlig legger til så mye informasjon som mulig. Dette vil forenkle prosessen videre.

Hendelsesleder

Ansvaret til en hendelsesleder starter etter at en hendelse er definert fra triage-ansvarlig. Hendelseslederen er ansvarlig for å holde oversikt over hele hendelsen fra start til slutt. Det skal være oppdateringer både internt til teamet og ut til den bredere virksomheten etter behov, samt eksterne interessenter. Hendelseslederen skal sørge for at all viktig informasjon, hypoteser og beslutninger blir dokumentert. Hendelseslederen skal også sørge for at svært alvorlige hendelser blir brakt fram til ledelsen og håndtert deretter. [**IrPlan**]

Sjekkliste for hendelseslederen:

- Overordnet ansvar for hendelseshåndteringen fra start til slutt
- Delegere oppgaver til alle roller som inngår i teamet (f.eks. dokumentasjon)
- Identifisere ressurser
- Dialog med alle involverte parter (bør omfatte for hvem, hvor ofte, hvor det skal holdes, hva som skal informeres om)

Denne delen skal omfatte "hvem", "hva", "hvor", "hvorfor" og "hvordan".

Her følger et eksempel på loggføring i en hendelse. I slutten av dokumentasjonsfasen bør det opprettes et "lessons learned"-dokument som bearbeides og følges opp.

Hva,	Tidspunkt	Beskrivelse	Utført av
	22:15	Oppdaget [hendelse] i form av [aktivitet]	Sikkerhetsleder
	22:18	Sendte melding til [noen i Team] for videre undersøkelse/assistanse	Sikkerhetsleder
	22:20	Overvåker bruker mens vi undersøker	Sikkerhetsleder og annen random
	23:13	Mistenkelig aktivitet forsøkes	Ukjent
	23:17	Skrur av server/isolerer system	Sikkerhetsleder
	23:20	Varsler påvirkede (av at server er skrudd av)	Random dude
	23:45	Avdekker false positive i samarbeid med DEQ	Sikkerhetsleder og DEQ
	00:30	Skrur på server igjen/gjenoppretter til normaltilstand, følger opp og avslutter sak, legger til oppfølgingspunkter og "lessons learned" til neste gang	Sikkerhetsleder

Hvor skjedde hendelsen?

Hvem rapporterte hendelsen?

Hvordan ble hendelsen oppdaget?

Hvilke områder er påvirket/kompromittert av hendelsen? (Scope)

Hva er forretnignseffekten?

Har kilden til hendelsen blitt oppdaget?

Loggføring av hendelsen?

Hendelseshåndterer

Hendelseshåndterer har ansvar for de tekniske aspektene ved respons og gjenoppretting. Dette gir hendelseslederen mulighet til å primært fokusere på å koordinere hendelsesresponsen. Hovedansvaret til den tekniske lederen er å finne ut av hva som gikk galt, utarbeide en gjenopprettingsstrategi og implementere en løsning så effektivt som mulig. Hendelseshåndterer utfører også analyser under hendelsen og hjelper til med gjenoppretting etter hendelsen. De skal også hjelpe hendelsesleder med tildelte handlinger under hendelsen.

Sjekkliste for Hendelseshåndterer:

- Ansvar for tekniske aspekter
- Finne ut hva som gikk galt
- Utarbeide gjenopprettingsstrategi
- Implementere løsning

IT og infrastruktur

IT og infrastruktur ansvarlige har ansvar for å fullføre tekniske aktiviteter for å begrense og gjenopprette problemer i infrastrukturen. De skal også hjelpe hendelsesleder med tildelte handlinger under hendelsen.

Senior Management (Ledelse)

Ledelsen skal være tilgjengelige til å støtte og å ta kritiske beslutninger under en hendelse. Et eksempel på det er å ta et viktig system offline. Ledelsen skal også bestemme når de skal gjenoppta virksomheten som normalt etter en hendelse ut ifra tilbakemeldinger fra andre i teamet. [**IrPlan**]

Her følger en tabell over ulike roller i en hendelseshåndteringsprosess, og hvem som besitter disse rollene.

Navn	Rolle	Ansvar
	Senior Manager	Støtte kritiske beslutninger
	Triage Manager	Triage prosess
	Incident Manager	Holde oversikt over hele hendelsen
	Technical Lead	
	Investigators/Analysts	
	IT and Infrastructure	

11 Trening

DENNE SEKSJONEN ER UFERDIG.

Ref trening.tex

iProsess/Rapportskriv/referanser.bib

Identifikasjon

Ranvir Singh, Farhaz Ismail, Jan Ngo, Espen Eriksen

May 19, 2022

Contents

1 Om denne fasen

Denne fasen handler om å identifisere hvorvidt virksomheten har blitt utsatt for et cyberangrep, og eventuelt innhente så mye informasjon som mulig. Dette kan gjøres ved å identifisere avvik fra normal drift, og vurdere om avviket representerer en sikkerhetshendelse.

Fasen vil inkludere indikatorer på vellykkede angrep, hvordan overvåkning og logging av tjenester bistår med kartlegging og analyse, koordinering av sikkerhetsteamet og en prosess for videre håndtering av hendelsen.

2 Metoder for å identifisere hendelser

2.1 Indikatorer

Indikatorer er artefakter som kan tyde på vellykkede angrep eller forsøk på angrep, og består av taktikk, teknikk og prosedyrer (TTP) aktørene bruker for å tilegne seg uautorisert tilgang til beskyttede systemer eller brukere. Indikatorer kan brukes av sikkerhetsteamet til å bestemme om en reell hendelse har funnet sted, alvorlighetsgraden og eventuelt hvem aktøren er.

2.2 Cyber kill chain

Lockheed Martin sin Cyber Kill Chain beskriver en struktur angrepsaktører ofte går gjennom i sine angrepsforsøk. Sikkerhetsteamet bør ta sikte på å hindre angrepet i en så tidlig fase som mulig. Ved å dele inn angrepet i ulike faser kan det fortelle sikkerhetsteamet noe om hvor langt i prosessen angrepet har kommet. Det er for eksempel vanskelig å forhindre rekognosering av virksomheten, men kan gi en indikasjon på at et angrepsforsøk kan være nært forestående. Ved å benytte indikatorlisten kan den sees i sammenheng med cyber kill chain for å få en bedre forståelse om hvilket steg angrepet befinner seg i, og håndtere hendelsen deretter.

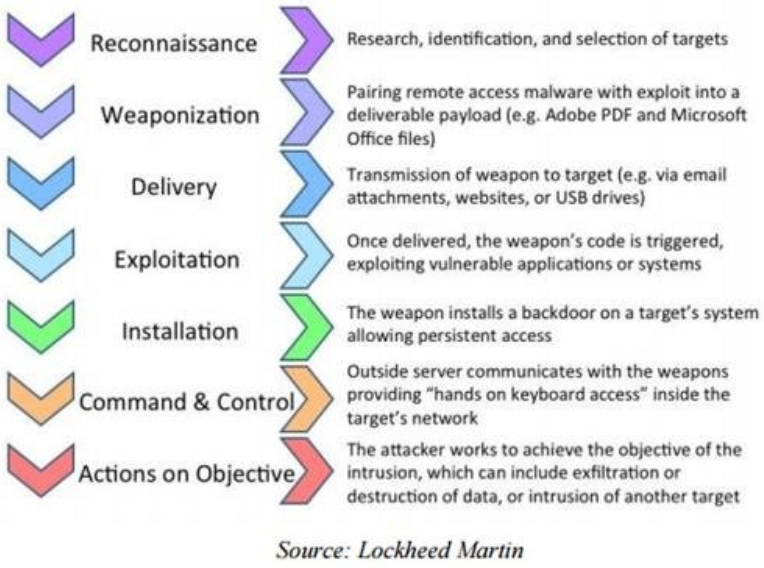


Figure 1: Cyber Kill Chain

2.3 Liste over indikatorer

Det finnes ulike indikatorer på at system har blitt kompromittert eller at det har vært forsøk på ondsinnet aktivitet. Å ha en oversikt over vanlige indikatorer øker sikkerhetsforståelsen til teamet og forenkler prosessen med å identifisere hendelser. Slike indikatorer er ofte omtalt som "Indicators of compromise" (IoC). I dette kapittelet listes noen eksempler på slike indikatorer.

2.3.1 Rekognosering

Rekognosering er en vanlig metode aktører benytter seg av i den initielle fasen av angrepet. Denne fasen handler om å innhente så mye informasjon om nettverksinfrastrukturen som mulig. Den vanligste metoden er skanning av nettverket for å kartlegge hvilke servere eller tjenester som er eksponert mot internett.

- Bruk av portskannere.

  Nmap er et eksempel på bruk av portskanner. Ved å undersøke netflow kan man observere at det er gjort skanning av nettverksinfrastrukturen. Er det gjort mange oppslag mot diverse høye porter fra samme IP-adresse kan det tyde på skanning.

2.3.2 Skadevare

Skadevare er en samlebetegnelse på programvare og -kode som uten brukerens tillatelse utfører uønskede handlinger eller henter ut sensitiv informasjon. Skadevare forkleder seg ofte som ufarlige filer, som PDF-er og Microsoft Office filer. Dette kalles "Weaponization" i cyber-kill-chain. Skadevare omfatter blant annet løsepengevirus, trojanere, spredningsteknikker, bakdører, annonsevare, spionvare og lignende. Her følger noen indikatorer på infeksjon av skadevare.

Løsepengevirus

Et typisk tegn på vellykket infeksjon av løsepengevirus er en beskjed, ofte i form av en tekstfil på skrivebordet, hvor det eksplisitt står beskrevet at en er infisert av virus, samt medfølgende instruksjoner for å gjenopprette normal drift.

Filer blir ofte kryptert, og filendelser kan endres til blant annet ".LOL!, .OMG!, .encrypted, .locked, .crypto" og så videre. Filnavn kan også få nye kryptiske eller autogenererte navn.

Dramatisk nedgang på enheters ytelse over kort tid

Ytelsen på endepunktsklienter får svært nedsatt ytelse over kort tid. Det kan være skadevare som kjører i bakgrunnen, slik som spionvare, trojanere eller former for spredningsteknikker.

Programmer som åpnes eller lukkes automatisk

Om programmer åpnes automatisk, for eksempel ved oppstart av klient, eller programmer lukkes uten brukerinteraksjon kan det indikere at klient er eksternt kontrollert. Det kan riktignok hende at programmer slutter å virke, spesielt dersom programmet er utdatert. Det vil i så henseende ikke være ondsinnet.

2.3.3 Uautorisert tilgang eller feilede påloggingsforsøk

Det er ikke uvanlig at en sluttbruker har glemt passord eller logger på fra en ny lokasjon. For varsling om slike hendelser kan det følgelig være vanskelig å skille mellom legitim og ondsinnet aktivitet. Angrepet er vanligvis innen "Delivery", "Exploitation" og "Installation" fasen i cyber-kill-chain. Det finnes riktignok noen indikatorer på at ondsinnet aktivitet har forekommet.

Varsel i XDR

Redigert innhold

XDR logger når påloggingsforsøk forekom, fra hvilken lokasjon og antall forsøk. Det er mulig å tilpasse triggers slik at varsling sendes på e-post eller mobil når et antall ikke-vellykkede forsøk innenfor en viss tidsperiode har forekommet.

Kontoaksess fra ukjent område og enhet

Redigert innhold

Låste brukerkontoer

Låste brukerkontoer er ofte et resultat av for mange feilede påloggingsforsøk. Det kan være hensiktsmessig å ta kontakt med brukeren for å bekrefte at det var vedkommende som forsøkte å logge på.

Uvanlige filendringer

Logging av filer som svært sjeldent eller aldri skal endres på kan trigge varsling dersom det er oppdaget en nylig filendring. Er det gjort en filendring kan det være et tegn på uautorisert tilgang.

Filer kan også benyttes som såkalte honeypots. Honeypots er filer som fremstår verdifulle fra utsiden, slik at angriper prøver å nå disse filene. Angriperen havner i et kontrollert miljø, hvor det er satt opp sikkerhetsmekanismer for å kontrollere, bekjempe, loggføre og bli kvitt angrepet.

Mistenkelig administrativ brukeratferd

Varsling om at brukere prøver å få tilgang til systemer eller eksekvere filer de ikke har tilgang til kan tyde på ondsinnet aktivitet eller forsøk på å forhøye sine rettigheter.

Kompromittert konto med lekkede brukerdetaljer (credential stuffing)

Det finnes mange åpne kilder som støtter deteksjon av kompromitterte brukerdetaljer. Det bør også sjekkes opp mot det mørke nettet, hvor eksempelvis løsepengevirusaktører ofte opplyser om vellykkede angrep.

(Eksempel: haveibeenpwned.com)

Uvanlig nettverksaktivitet

Ved å definere et normalnivå av nettverkstrafikk, kan en identifisere anomali i trafikkmengden. Konstant høy nedlastingaktivitet kan være tegn på angrepsaktør som laster ned store filer slik som virus eller trojanere.

2.3.4 Command and control (C2)

Phishingangrep kan være en inngangsvektor til blant annet etablering av C2-kommunikasjon. Her følger noen indikatorer på at et slikt angrep har funnet sted.

- Uvanlig mengde nettverkstrafikk.

  Lik mengde utgående nettverkstrafikk over lengre tid kan tyde på C2-kommunikasjon. Dette er en form for anomali. Vanligvis trafikkmengde varierer mye mer.

- Liten mengde innkommende nettverkstrafikk, og større nettverkstrafikk ut.

  Kan tyde på at kommandoer blir sendt fra C2-kontrollert server, og at kommandoer eksekveres fra infisert klient.

- Nettverkskommunikasjon med kjent ondsinnet indikator (gjerne IP-adresse eller domener).

2.3.5 Fullførelse av angrepet

De to mest relevante måter angrepet blir fullført er ved tjenestenektangrep og dataeksfiltrering. Disse to typene har særegne indikatorer.

Tjenestenektangrep

Tjenestenektangrep (også kjent som "denial of service" (DoS) eller "distributed denial of service" (DDoS)") har som formål å utføre angrep som hindrer at systemer kan opprettholde normal drift. Disse angrepene leder ofte til overbelastede systemer som videre fører til at systemet går ned og blir ikke-funksjonelle. Indikatorer på tjenestenektangrep er som regel eksplisitte i form av at en direkte ser at nettsider går ned.

- **Uvanlig mengde nettverkstrafikk**
  - Uvanlig mengde nettverkstrafikk er en av de vanligste typene av tjenestenektangrep. Ofte er det større bulker av trafikk som sendes inn samtidig. Nettsider kan få feilmeldinger som HTTP 503 som indikerer at nettsiden fungerer, men ikke

får kontakt med innhold i bakgrunnen, som databaser, servere og så videre. Via nettverksovervåkning kan en identifisere om slike tilfeller oppstår.

- **Stort antall serverforespørsler over kort tid**
  - Et høyt antall serverforespørsler over kort tid kan indikere et botnet-angrep. Botnet-angrep bruker et nettverk av infiserte maskiner med virus og trojaner for å utføre handlinger. Da kan angriper beordre maskinene til å utføre spørringer mot det interne nettverket og overbelaste systemene. Dette leder til ytelsesnedgang og muligens ikke-funksjonell tilstand.

Dataeksfiltrering

Dataeksfiltrering er en svært populær teknikk som benyttes i stadig større grad i forbindelse med løsepengevirusangrep. Ettersom selskapene etablerer bedre teknikker for sikkerhetskopier og gjenoppretting av data, utvikler angriperne andre metoder for å skade virksomheters omdømme. Dataeksfiltrering handler om å kopiere ut data før det krypteres. Aktører kan deretter true med å lekke sensitiv data. Dette kan i mange tilfeller skade virksomheters omdømme eller få store økonomiske konsekvenser.

- Unaturlig størrelse på HTML-trafikk. Kan indikere SQL injection.
- Økt databaseaktivitet. Massehenting av data (dumps).
- Store mengder utgående nettverkstrafikk.

  Kan indikere at data enten er eller har blitt utkopiert.
- Ukjente protokolloverføringer.

  Eksempel kan være at HTTP benyttes istedenfor HTTPS, og at dette strider med virksomhetens nettverksoppsett.
- Unormalt store filer med arkiveringsformat som .zip.
- Varsel fra overvåkningssystemer som DLP.

3 Rapportering av hendelser

3.1 Omfang

Denne seksjonen gir en konkret fremgangsmåte for innrapportering av hendelser.

3.2 Hendelse identifiseres og varsles om

XDR er et overvåkningssystem som varsler ved ulike hendelser, men klarer dessverre ikke å fange opp alt. Ansatte må varsle dersom det oppdages at en hendelse har oppstått. Rapporteringen kan gjøres via helpdesk-portalen, e-post til IT eller telefonoppringning. Om hendelsen fremstår kritisk oppfordres det å ringe.

Ved innrapportering vil det spare mye tid og ressurser for sikkerhetsteamet om de får så mye informasjon som mulig. Følgende mal kan benyttes ved innrapportering:

NB! Dette er kun et eksempel:

Hvem rapporterte hendelsen (Fullt navn)	Redigert innhold
Når ble hendelsen oppdaget (Dato og klokkeslett)	Torsdag, 14.04.2022, kl. 12:34
Hvordan ble hendelsen oppdaget (En til tre setninger)	Ansatt trykket på en lenke som spurte etter brukernavn og passord, uvitende ble det skrevet inn og sendt, ble oppdaget i etterkant innloggingen var irrelevant til det vedkommende jobbet med.
Kort beskrivelse av hendelsen og hvilke systemer og/eller brukere som ble påvirket	Ondsinnet lenke sendt til mottaker, mottaker trykket på og oppga sensitiv brukerinformasjon, en ansatt (Arne Bjertulf) sin konto er kompromittert.

3.3 Opprettelse av sak

Virksomheten benytter en helpdesk-portal hvor hendelser kan innrapporteres av hvem som helst. Portalen fungerer som et saksbehandlingssystem og gir en ryddig oversikt over alle hendelser for sikkerhetsteamet.

4 Flerkildeanalyse

Kombinering av data fra flere kilder kan gi et mer nøyaktig trusselbilde. Analysering av disse dataene .....

- Loggfiler

  Må beskrive konkret hvordan loggfiler kan benyttes i analyse av hendelsen. Hvilke loggfiler skal sjekkes, hvordan skal det sjekkes, hva skal det sjekkes for og så videre.

- Netflow

  Netflow er analyse av nettverkstrafikk. Source IP/destination IP, pakker sendt, tidspunkt, nettverksprotokoll brukt, .pcap-filer og så videre. Usikker på om Moelven har dette. Kan være et veldig nyttig verktøy. Må forklare hvordan det skal brukes i analyse.

- Feilmeldinger

  Hvor skal man se etter feilmeldinger? Hva skal gjøres med feilmeldingene? Må konkretisere.

- IDS ( )

  IDS er en enhet som overvåker nettverk eller systemer for ondsinnet aktivitet eller brudd av policyer. Må forklare hvordan de skal bruke dette for analyse.

- Brannmur

  Konkretiser hvordan det skal brukes i analyse.

- VirusTotal

  Noe random

- Joe Sandbox

  Noe random

- Programvare for DLP

  Noe random

5 Koordinering av team

Etter at saken er registrert er det hendelseslederens ansvar å følge opp saken til den er ferdighåndtert og avsluttet. Hendelseslederen skal delegere arbeidsoppgaver til sikkerhetsteamet. Mye av ansvarsområdet til de ulike rollene er forhåndsdefinert, men hendelseslederen må vurdere hver enkelt hendelse og eventuelt supplere med flere oppgaver ved behov.

5.1 Triage-ansvarlig

Triage-ansvarlig skal overvåke innkommende saker og avgjøre om saken er kritisk nok til å begynne en hendelseshåndteringsprosess. Beslutningen skal tas på bakgrunn av "klassifisering av angrep" fra Preparation. Etter at angrepet er klassifisert må triage-ansvarlig vurdere om S1- eller S2-type angrep er kritisk nok til å eskaleres til hendelseshåndteringsprosessen. For S3- og S4-type angrep bør hendelseshåndteringrutinen påbegynnes uansett.

5.1.1 Rotårsaksanalyse

Triage-ansvarlig må utføre en rotårsaksanalyse. En rotårsaksanalyse er årsaken til at hendelsen har funnet sted. Det kan for eksempel være målrettet eller opportunistiske angrep eller driftsfeil. Triage-ansvarlig kan ta utgangspunkt i innrapporteringsskjemaet, som enten er fylt ut av sluttbruker eller triage-ansvarlig selv i samråd med sluttbrukeren, for å danne en hypotese.

Tre vanlige typer rotårsaker er:

- Årsaker relatert til systemer. Dette kan være feil på maskinvare som fører til avvik, systemfeil ved oppstart, feilkonfigurasjon av systemer, applikasjoner eller servere.
- Menneskelige feil og/eller målrettede angrep. For eksempel sluttbruker som trykker på en phishing-lenke.
- Organisatoriske årsaker. Dette kan være uklar kommunikasjon innad i organisasjonen eller med leverandører.

Det er også hensiktsmessig å se på hvordan hendelsen kan utvikle seg. Er det for eksempel identifisert et løsepengevirus-angrep, kan det haste med å stenge ned tilganger eller skru av nettverk for å forhindre videre spredning. I et slikt tilfelle må triage-ansvarlig varsle videre så fort som mulig. Etter at dette er gjort kan triage-ansvarlig videre se på:

- Å utarbeide hypotese på hvorfor angrepet ble oppdaget, og om kompromitteringen var vellykket.
- Påvirkede systemer, og hvor langt angrepet er kommet inn i "cyber killchain".

All informasjon skal samles for å kategorisere hendelsen, og årsaken skal dokumenteres. Hvilke systemer og brukere som er kjent at er påvirket av hendelsen skal dokumenteres

i tillegg. Triage-ansvarlig skal varsle hendelsesleder som videre koordinerer teamet og delegerer oppgaver. Initiell dokumentasjon i rotårsaksanalysetabellen skal overleveres hendelseshåndterer for videre analyse.

Informasjonen kan dokumenteres i tabellen under.

Kategori	**Beskrivelse**
Alvorlighetsgrad	
Rotårsak	
Hypotese	
Påvirkede systemer/brukere	
Er nødvendige varslet? Hvem	
Hendelseskategori	

5.2 Hendelsesleder

Etter at triage-ansvarlig har loggført og registrert en ny hendelse, har hendelseslederen ansvar for videre koordinering av hendelseshåndteringsprosessen. Første steg er å delegere oppgaver.

5.2.1 Delegere oppgaver

Hendelseslederen skal sikre at aktiviteter utført av teamet er av høyt kvalitetnivå og at alle gjør oppgavene de har blitt tildelt. Noe av ansvarsområdet til de forskjellige medlemmene i teamet er forhåndsdefinert i "koordinering av team" i hver fase, men hendelseslederen må supplere med flere oppgaver eller omfordele ved behov. Hvis teammedlemmer blir usikre på hva de skal gjøre, skal hendelsesleder tildele oppgaver avhengig av situasjonen.

5.2.2 Identifisere ressurser

Hendelseslederen skal sørge for at alle har nødvendig utstyr og verktøy til å komme i gang med hendelseshåndteringen. Mangler det ressurser i form av verktøy, kontaktpersoner eller annet må hendelseslederen drive denne prosessen fremover.

5.2.3 Dialog med alle involverte parter

Førsteprioritet er å varsle eventuelle kunder som er påvirket. Dette er hovedsakelig hendelseslederens ansvar. Det kan være vanskelig å ha fullstendig oversikt over alle systemer

og brukere påvirket i en tidlig fase. Derfor kan det vurderes å ha en informasjonsside der informasjon om hendelsen publiseres offentlig.

Videre bør det tas kontakt med underleverandører som kan bistå. Dette inkluderer blant annet Redigert Innhold ettersom de spiller en sentral rolle knyttet til informasjonssikkerheten i virksomheten. Det anbefales også å ta kontakt med internettleverandør for videre bistand.

Det er hendelseslederens ansvar å ha et overordnet oversiktsbilde over kommunikasjonsprosessen i hendelsen, avtale møter og sette ressurser i kontakt med hverandre.

Eksempler på informasjon som bør avklares:

- Hvilket type angrep er det?
- Hva har blitt påvirket?
- Hvordan påvirker dette produksjonen?
- Hvor kom angrepet fra eller hvor mistenker dere at den kommer fra?
- Hva har blitt gjort mot hendelsen så langt?
- Hva skal bli gjort videre?
- Hvordan er situasjonen?
- Innspill fra andre

5.3 Hendelseshåndterer

Hendelseshåndtereren er ansvarlig for å samle inn og analysere data som skal støtte etterforskningen av hendelsen. Hendelseshåndtereren kan ta utgangspunkt i informasjon overlevert av triage-ansvarlig for videre analyse.

5.3.1 Analyser fokusert mot løsepengevirus

Forhindre videre spredning:

Er det oppdaget løsepengevirus i en tidlig fase er det svært sannsynlig at viruset kan spre seg videre. Uavhengig av om det allerede har spredt seg eller er i ferd med å gjøre det bør nettverksaksess stenges så fort som mulig. Dette inkluderer å koble ut nettverksenheter som hub, switch og router. Internettaksess inn og ut fra virksomheten bør kuttes. Det bør utarbeides en liste over alle enheter som skal kobles ut, samt en rutine på hvordan dette skal gjøres.

Når en har forhindret videre spredning av angrepet er det viktig å kartlegge hvilke systemer som er rammet. Hendelseshåndtereren bør ha en forhåndsdefinert liste over indikatorer som kan tyde på at enheter er infisert. Listen bør sjekkes opp mot hver enhet for å identifisere hvorvidt enhetene er infisert. Listen må kontinuerlig oppdateres med enheter sjekket og status på disse.

Kommunikasjon til involverte parter:

Hendelseshåndteres har tett dialog med triage-ansvarlig og hendelsesleder under Identification-fasen. De skal sørge for at verdifull informasjon blir utvekslet.

Identifisere mulig dataeksfiltrering og/eller -kryptering:

Hendelseshåndtereren bør forsøke å identifisere om data har blitt eksfiltrert av aktøren. Dette er en svært vanlig og populær metode, og kan benyttes til blant annet utpressing i forbindelse med å lekke sensitive data.

Avgjøre hvorvidt løsepenger skal betales:

Noen elementer å ta i betraktning i vurderingen:

- Hva betaler en løsepenger for? Er det for gjenoppretting av krypterte filer, unngå lekkasje av bedriftssensitiv data, noe annet?
- Hvilken garanti eller sannsynlighet har man for at aktøren gjør det de sier? Kan en se på tidligere historikk?
- Hvilke økonomiske konsekvenser har dette for virksomheten? Hva gjør det med deres omdømmet? Skal avgjørelsen hvorvidt løsepenger betales offentliggjøres?
- Hvor tidskritisk er det å fatte en avgjørelse? Øker prisen ettersom tiden går?

- Hvem skal fatte den endelige avgjørelsen? Skal det være én eller flere personer? Skal begrunnelsen for avgjørelsen dokumenteres?
- Hvordan skal betalingen utføres? Hva slags valuta er det? Kryptovaluta? Hvilken enhet skal utføre betalingen?
- Mer ting...

Identifisere angrepsaktør:

Det finnes mange angrepsaktører og de kan ofte bli identifisert ved å se på hva slags TTP som er brukt. Det kan være formålstjenlig både i prosessen med å gjenopprette systemer tilbake til normaltilstand og for potensielle fremtidige hendelser å kartlegge hvem som står bak. Hendelseshåndtereren bør basert på informasjon om angrepet gjøre seg opp en mening om hvorvidt det er et opportunistisk angrep eller fra an avansert aktør (APT). Ved å identifisere angrepsaktør kan en også sjekke i åpne kilder om det foreligger offentlig tilgjengelige dekrypteringsnøkler. Merk at slike dekrypteringsnøkler alltid bør benyttes med varsomhet og gjerne testes før det benyttes i produksjonsmiljø.

Hvorvidt en skal betale løsepenger:

5.3.2 Analyser fokusert mot phishing

Phishing (på norsk kjent som "nettfisking") har som formål å "fiske" ut sensitiv informasjon fra brukere. Phishing kommer i mange former og er et bredt begrep som omtaler mange ulike former for angrep. Vellykkede phishingangrep kan være en inngangsvektor for mange angrep, blant annet løsepengevirus.

Identifisere angrepsvektor

Vellykkede phishingangrep vil i de aller fleste tilfeller forekomme via e-post. Det er gjerne ondsinnede vedlegg som åpnes eller nettsider som besøkes. Et vellykket phishingangrep kan være vanskelig å oppdage avhengig av hvordan aktøren opererer. Er det for eksempel brukerdetaljer på avveie kan det hende aktøren avventer med å nyttiggjøre seg av denne informasjonen. Derfor vil det være verdifullt om brukere rapporterer mistenkelig aktivitet.

SMS er en mulig angrepsvektor. Aktør kan for eksempel utgi seg for å være et selskap eller noen som ønsker å gjennomføre en legitim spørreundersøkelse, eller påstå at en har vunnet en premie.

Selv om tofaktorautentisering er et av de sikreste tiltakene mot uautorisert tilgang, er en fortsatt sårbar for angrep. Tofaktorautentisering har som regel ingen grense på hvor mange forespørsler en kan få. En metode aktører kan bruke er å massesende tofaktorforespørsler slik at bruker til slutt godkjenner forespørselen.

(Kilde: `https://securepractice.co/bulletins/nb-no/er-du-et-ja-menneske/78`)

6 Kilder

https://www.upguard.com/blog/indicators-of-compromise
https://www.rapid7.com/blog/post/2017/02/13/detection-and-analysis-phase-of-incident-response-li
https://www.domaintools.com/resources/blog/tools-to-quickly-extract-indicators-of-compromise
https://www.makeuseof.com/what-does-indicators-of-compromise-mean/
https://www.cynet.com/incident-response/incident-response-sans-the-6-steps-in-depth/
https://digitalguardian.com/blog/creating-incident-response-classification-framework
https://www.empowerit.com.au/blog/cybersecurity/data-accessed-unauthorised-users/
https://www.baculasystems.com/wp-content/uploads/2021/01/ransomware-prevention-checklist.
pdf

Containment

Espen Eriksen, Jan Ngo, Farhaz Ismail, Ranvir Singh

May 19, 2022

Contents

1 Om denne fasen

Denne fasen i rammeverket omhandler hvordan et sikkerhetsteam kan gå frem for å isolere en hendelse og bekjempe potensialet for spredning til andre systemer. Målet med denne fasen er å begrense skade og hindre ytterlig skade i en hendelse. Fasen inneholder generell informasjon om spredning av skadevare, en vurdering av hvor mange systemer og endepunkter skadevaren har nådd, vurdering av hvilke tiltak som passer best til hendelsen, om sikkerhetskopiering av hendelsene for etterforskning og til slutt om hvordan en skal holde kontroll etter hendelsen har blitt begrenset.

2 Isolering

Formålet med isolering er å begrense skadeomfanget og få kontroll på angrepet. Det er flere grunner til hvorfor en skal isolere et angrep, men noen av de viktigste er å begrense nåværende skade i det angrepet skjer, og begrense spredning av angrepet i fremtiden.

2.1 Vurdering av angrep

For å forstå omfanget til angrepet, må angrepet vurderes for å finne effektivt tiltak. Det skal ses på indikatorlisten, men også alvorlighetsklassifiseringen (jamfør Identification). Dette brukes for å se om angrepet har beveget seg videre i cyber kill chain. Dersom angrepet har beveget seg videre i cyber kill chain bør det vurderes om flere ressurser skal allokeres til hendelsen.

2.2 Isoleringsformat

Isolering av angrep kan kategoriseres til to forskjellige metoder; korttidsbegrensning og langtidsbegrensning. Det er som regel alltid kortidsbegrensninger som skal tas i bruk først, men det presiseres at både korttids- og langtidsbegrensningstiltak er nødvendig. Det må foretas en skjønnsmessig helhetsvurdering av hvilke tiltak det er mest hensiktsmessig å begynne med.

2.2.1 Korttidsbegrensning

Korttidsbegrensing har som formål å begrense skadeomfanget så raskt som mulig. Korttidsbegrensning er tiltak som forhindrer angrepet i å spre seg videre på kort sikt, med tanke på maskineri og systemer. Vanlige tiltak til slike situasjoner er blant å ta ned eller isolere servere og maskineri, rute trafikk til failover-servere, blokkere eller isolere endepunktsklienter og deaktivere brukere.

Det finnes flere ulike tiltak en kan vurdere å ta i bruk. Her følger noen eksempler:

Isolere endepunkt med XDR

XDR har en funksjon som tillater å isolere en endepunktsklienter. Isolasjonen begrenser nettverksaksess til påvirket endepunkt, og vil kun rute trafikk mellom XDR og seg selv. Dette forhindrer kompromitterte enheter å kommunisere med andre endepunkter og vil redusere angrepsflaten.

Deaktivere brukere

Å deaktivere brukere er et tiltak hovedsakelig rettet mot phishing. Vellykket phishing er ikke lett å oppdage. Ofte er et passordskifte et godt tiltak, men en vet aldri om bakdører er satt opp slik at de kan få tilgang igjen, og her kommer deaktivering av hele brukeren

som et alternativ tiltak. Dette er en vurderingssak og må vurderes på grunnlag av hva kompromittert bruker har rettigheter til. Er det en bruker med administratortilgang så er deaktivering et sikrere tiltak.

Skru av enheter

I utgangspunktet frarådes det å skru av infiserte enheter da dette kan føre til tapt analysedata. Er det ikke satt opp en infrastruktur som tillater effektiv isolering av enheten kan dette være et mulig tiltak. Det er spesielt relevant i forbindelse med løsepengevirus der viruset kan spre seg svært raskt til andre enheter.

Failover

Failover-servere eksisterer for de tilfellene hvor produksjonsenheter eller andre viktige enheter går ned, kompromittert eller av en annen grunn ikke kan opprettholde normal drift. Disse enhetene skrus derfor av eller blir flyttet ut av produksjon, og trafikken rutes til failover-servere inntil det er kontroll over situasjonen.

Brannmur

Et mulig tiltak er å opprette nye brannmurregler på kompromittert enhet som hindrer all utgående trafikk, slik at dette forhindrer at angriper kan eksfiltrere data, og ev. regler som hindrer all inngående trafikk også. Slike regler bør optimalt sett eksistere fra før som preventive tiltak.

2.2.2 Langtidsbegrensning

Langtidsbegrensning har som formål å få produksjons- og hovedenheter tilbake til normal drift. Langtidsbegrensning setter i gang tiltak som kan fortsette å begrense angrepet, men samtidig opprettholder normal drift. Hovedfokuset i denne fasen av angrepet er å finne bakdører, kompromitterte brukere, kompromitterte enheter og så videre. Det skal utføres tiltak som fjerner disse sikkerhetshullene og skal til slutt finne roten av problemet slik at alle spor av angrepet blir fjernet.

Oppdatere systemer

Er det avdekket utdaterte systemer bør disse oppdateres i henhold til rutine. Det er svært viktig å holde et oppdatert oversiktsbilde over nye sårbarheter og påse at systemer fortløpende oppdateres for å beskytte seg mot potensielle angrep.

Bytte av passord

Er det oppdaget spor av løsepengevirus bør en anta at alle i virksomheten kan ha blitt kompromittert. Da kan det være hensiktsmessig å benytte f.eks. Powershell for å masseendre passord. Er hendelsen relatert til phishing kan det være nok å endre passord til den aktuelle brukeren.

Fjerne kompromitterte brukerkontoer

Det finnes bakdører inn til systemer via brukerkontoer. Brukerkontoer som blir kompromitterte burde alltid skiftes passord på, men det må vurderes opp mot hva angriper har klart å gjøre med kontoen. Bakdører inn via brukerkontoer eksister, og derfor må det vurderes om brukerkonto burde bli fullstendig fjernet fra systemene, hvorpå det opprettes en ny brukerkonto.

Brannmur- og filterregler

I korttidsbegrensningen ble det nevnt bruk av brannmur og filtre for å isolere endepunkt fra trafikk. Disse filtrene kan også brukes for å lokke frem bakdører og angrep i dvale. Denne trafikken fungerer som en "honeypot", og må ikke inneholde reell data. Det er kjent at angripere kan legge igjen bakdører og angrep som lytter etter trafikk, slik at når enheter er oppe og gående igjen, aktiveres angrep eller angriper blir varslet. Dette kan være en nyttig måte å få informasjonen som hjelper med å finne tiltak på angrepet.

Bakdører

Bakdører er en kjent metode benyttet av aktører for å gi seg selv tilbakevendende tilgang til systemene. Bakdører er utfordrende å oppdage fordi de gjerne blir skjult innad i systemene, for eksempel ved bruk av skjulte prosesser, oppgaver i Task Scheduler, oppføringer i registry og så videre. Ved vellykket angrep bør en analyse av systemer, enheter og kode utføres. Disse bakdørene må fjernes før komplett gjenoppretting av systemet utføres.

Intrusion prevention- og intrusion detection system

Det eksisterer programvarer som hjelper overvåkningen og varsler når noe avviker fra normaldrift. Slik programvarene er hovedsakelig i bruk før et angrep skjer, men kan også benyttes for å overvåke angrep som ligger i dvale, lagt igjen av angriper. Slike angrep er vanskelig å oppdage, og oftest fremkalles når systemer er tilbake på plass i sin normale operasjon. Med IDS og IPS kan dette bli oppdaget.

XDR

Redigert er en hovedprogramvare brukt av Moelven for å overvåke og detektere hendelser, angrep, mistenkelig oppførsel og så videre. Er det enheter på nettverket som ikke har Redigert, må dette installeres umiddelbart.

3 Kriminalteknisk image

3.1 Sikkerhetskopi og dens formål

Sikkerhetskopi i form av et kriminalteknisk image er viktig fordi den spiller to hovedroller. Imaget kan benyttes som bevis i rettsaker eller eventuelt ved tiltaler. Samtidig er det egnet for videre analyse og kan benyttes som læringspunkter i "Lessons learned". Når en tar kriminalteknisk image anbefales det å benytte programvare som er designet for dette formålet. Spesialdesignet programvare opprettholder identisk status på systemet som da det ble kompromittert, slik at hendelsen kan analyseres i et sikkert og kontrollert miljø.

3.2 Tiltale og sanksjoner

Et kriminalteknisk image gjenspeiler hendelsen slik den var. Kriminalteknisk image tillater en å se tilbake på hvordan angrepet ble utført og progresjonen av angrepet. Den gjør det ved å ta opp hvordan de berørte systemene er under hendelsen. Dette blir fungerende som bevis på angrepet og hva angriper var ute etter, eventuelt hva angriper fikk tak i. Alle disse faktorene tas i betraktning når det skal dømmes, og det er derfor meget viktig å ha reelle bevis.

3.3 Analyse

Et kriminalteknisk image kan bistå med å få ytterliggere kunnskap om hendelsen og bidra til å unngå en slik hendelse i fremtiden. Kriminalteknisk images inneholder all data fra kildedisken og dette kan blant annet bistå med å finne rotårsaken til hendelsen. Relevante kriminaltekniske artefakter som slettede filer, slettede filfragmenter og gjemt data kan bli funnet i slack og uallokert plass. [**Forensic**]

4 Forhåndsdefinerte(/-godkjente) handlingsmønstre

5 Koordinering av team

Denne seksjonen innebærer hvordan teamet skal koordineres under Containment-fasen.

5.1 Hendelseshåndterer

Hendelseshåndterer har ansvar for å utarbeide en gjenopprettingsstrategi, og dette starter med å begrense hendelsen.

5.1.1 For løsepengevirus

Ved løsepengevirusangrep skal hendelseshåndterer begynne med korttidsbegrensning. Jamfør seksjon 2.2.1 for mer informasjon.

Begrense skadeomfanget:

Ettersom løsepengevirus kan spre seg svært raskt og ofte kryptere store eller hele deler av nettverket, er det svært kritisk å begrense skadeomfanget så fort som mulig. Er det identifisert løsepengevirus i nettverket, bør internettilgangen til virksomheten kuttes umiddelbart. Det kan forhåpentligvis kutte forbindelsen til angriperen. Viruset kan fremdeles spres internt i nettverket, og det er følgelig viktig å ha sikkerhetskopier og segmenterte nettverk for å motvirke dette.

Hendelseshåndterer kan også isolere endepunkter ved hjelp av XDR:

Av kriminaltekniske årsaker anbefales det ikke å slå av identifiserte kompromitterte enheter. Det kan for eksempel være indikatorer lagret i minne som vil forsvinne i et slikt tilfelle. Er det identifisert en kompromittert enhet som ikke har spredd viruset til andre enheter, bør denne enheten isoleres på et eget, segmentert nettverk. Deretter bør det tas et image av hele maskinen for senere skadevareanalyse.

Videre skal det bli tatt sikkerhetskopi i form av kriminaltekniske images.

Framgangmåte på hvordan en isolerer endepunkter på XDR:

Redigert innhold

Etter at kortidsbegrensningen har blitt utført sammen med sikkerhetskopi, skal det bli vurdert av hendelseslederen hvorvidt det skal utføres en langtidsbegrensning. For løsepengevirus må langtidsbegrensning alltid utføres. Jamfør seksjon 2.2.2 for mer informasjon.

5.1.2 For phishing

Ondsinnet aktivitet fra phishing-angrep må bli håndtert så raskt som mulig. Når aktøren først har kommet inn i systemet kan angrepet fort spre seg. Ettersom vellykkede phishingangrep kan være en inngangsvektor til eskalering av mange ulike type angrep, er det vanskelig å lage en forhåndsdefinert liste over begrensede tiltak. Tiltak må iverksettes basert på hvilke systemer som er påvirket. Om bruker er kompromittert bør passord endres umiddelbart, eller bruker vurderes å midlertidig deaktiveres.

Phishing kan dessuten være en inngangsvektor til løsepengevirus. Om et phishing-angrep fører til en eskalering til løsepengevirus, må rutinen for løsepengevirus bli følges (Seksjon 4.1.1).

5.2 Hendelsesleder

Hendelsesleder skal vurdere om langtidsbegrensning er nødvendig. Om systemer kan tas offline etter utføring av korttidsbegrensning og kriminalteknisk image, kan hendelseslederen vurdere å gå rett til Eradication-fasen. Dersom systemene må forbli i produksjon skal langtidsbegrensning bli utført. Jamfør seksjon 2.2.2 for mer informasjon om langtidsbegrensning.

Hendelsesleder skal også vurdere om triage-ansvarlig må bistå hendelseshåndterer. Om triage-ansvarlige ikke må bistå leder, skal triage-ansvarlig fortsette med nøye overvåkning av systemer i Redigert.

5.3 IT og infrastruktur

IT- og infrastruktur-ansvarlig skal bistå hendelseshåndterer med å begrense hendelsen og holde tett kontakt med hendelseshåndterer i denne fasen. Under langtidsbegrensning kan oppdatering av sikkerhetshull være nødvendig om sikkerhetshull bli oppdaget. IT- og infrastruktur-ansvarlig skal legge til sikkerhetsoppdateringer for sikkerhetshull som kan ha blitt utnyttet av angripere.

I-prosess/Rapportskriv/referanser.bib

Eradication

Espen Eriksen, Jan Ngo, Farhaz Ismail, Ranvir Singh

May 19, 2022

Contents

1 Om denne fasen

Denne fasen handler om å fjerne skadelig programvare som ble introdusert under angrepet på systemene, og gjenopprette til normal drift. Det er viktig å forstå hva som forårsaket sikkerhetsbruddet slik at en er i stand til å fjerne den skadelige programvaren for godt, og oppdatere systemene for å motvirke angrep i fremtiden.

2 Kartlegging av utnyttet sårbarhetsflate

For å være i stand til å fjerne alle spor av angrepsaktøren bør en ha kartlagt inngangsvektoren til hendelsen. Denne analysen bør allerede ha blitt utført i Identification-fasen av triage-ansvarlig, eventuelt i samarbeid med hendelseshåndterer. Avhengig av hva inngangsvektoren var, er det viktig å hardne systemer slik at de blir mer motstandsdyktig mot fremtidige angrep. Er det avdekket utnyttelse av sårbare systemer som kunne ha vært forhindret ved raskere oppdatering bør det sørges for å bedre virksomhetens oppdateringsrutiner. Er inngangsvektoren derimot sosial manipulering i form av et phishingangrep er det ikke mulig å beskytte seg helt for dette, men det bør brukes som et opplæringspunkt i "Lessons learned"-fasen.

Følgende er et skjema for inngangsvektor (denne er uferdig):

- Inngangsvektor:
- Dato for initiell infeksjon:
- Årsak til infeksjon:

3 Utryddelse

3.1 Vurderingsgrunnlag for sletting av spor av angrepsaktør

Når en skal utføre utryddelse er det viktig å ha kartlagt hvilke systemer som er berørt, og hva slags angrep det er snakk om. Som et utgangspunkt bør en prøve å sikre inngangsvektoren som ble benyttet for initiell aksess. Videre må teamet ha en oversikt over andre berørte systemer og enheter. Teamet har muligens avdekket ulike artefakter i forbindelse med angrepet, og disse bør håndteres i en slik grad at de slettes fra systemet. I et tilfelle med løsepengevirus bør en definere ulike strategier basert på dekningsgrad.

- Er endepunktsklienter infisert uten at det er tegn til spredning, anbefales det å wipe hele klienten. Endepunktsklienten skal på dette tidspunktet allerede ha blitt isolert.
- Er delte nettverksområder kryptert kan det være nødvendig med en komplett sletting av nettverksområdet, med gjenoppretting av sikkerhetskopi. Gjenoppretting bør testes i et testmiljø før det kjøres i produksjon, og det krypterte nettverksområdet bør ikke slettes, men heller isoleres inntil gjenoppretting er fullført og vellykket.
- For infeksjon av domenekontroller eller andre kritiske enheter bør det defineres en større plan. Det kan være vanskelig å gjøre en komplett wipe av slike systemer, selv med fungerende sikkerhetskopi, da det kan føre til mye nedetid. Her bør en sjekkliste for ulike eradication-tiltak defineres og deretter følges.

3.1.1 Beste praksiser

Forklar hva beste praksiser er. Formålet med beste praksiser..

Formålet med beste praksis er å sørge for at valg som blir tatt er mest mulig effektiv.

Her følger noen eksempler på beste praksiser.

En utryddelse tar sikte på å fjerne alle spor av angrepsaktør, men en kan aldri være helt sikker på at det er tilfelle. Det er heller ikke uvanlig at angrepsaktør vil forsøke å angripe kort tid etter første angrep, ettersom virksomheten kan være i en sårbar fase og i en prosess med å gjenopprette til normal drift. Følgelig anbefales det å sette opp overvåkning av berørte systemer i en angitt tidsperiode for å eventuelt oppdage anomali i systemet. En beste praksis er å sette opp overvåkning de neste 30 dager etter at et angrep er håndtert.

For løsepengevirus anbefales det å ha en rutine på hvordan en effektivt kan endre passord til alle brukere. Er tilfellet et vellykket phishing-angrep kan det være tilstrekkelig å endre passord til den kompromitterte brukeren. Jamfør seksjon 2.2.2 i Containment-fasen for mer informasjon.

3.1.2

4 Wipe av berørte system(er) og enhet(er)

Denne seksjonen tar for seg rutiner virksomheten må ha på plass i forbindelse med sletting/wipe av program- eller maskinvare. Sletting er tett knyttet sammen med reimaging. For mer informasjon om reimaging refereres til seksjon xx i Recovery-fasen.

Sletting kan deles inn i følgende kategorier:

- Kompromitterte kontoer på programvare som for eksempel e-postkonto.
- Endepunktsklienter.
- Servere.
- Spesielt kritiske servere, som for eksempel domenekontrollere eller produksjonsservere.

Er det oppdaget kompromittert konto, for eksempel på en brukers e-postkonto, uten tegn til videre spredning kan det i første omgang være nok å bytte passord på brukeren. Deretter bør brukeren og andre systemer overvåkes i en begrenset periode for å se etter tegn til angrepsaktør.

For wiping av endepunktsklienter bør virksomheten benytte dedikerte verktøy for dette for å sikre sikker og robust sletting av disk.

For servere kan wiping være en mer omfattende prosess, og i de fleste tilfeller anbefales det å sikre server basert på inngangsvektor og beste praksiser istedenfor å bygge opp serveren på nytt fra bunn.

For spesielt kritiske servere må virksomheten utarbeide en dedikert plan for sletting. På disse enhetene vil en komplett sletting i nesten alle tilfeller frarådes, da det kan føre til lang nedetid og mulighet for feil eller korrupsjon i filer og/eller systemer ved gjenoppretting. Virksomheten bør opprette en sjekkliste, samt sikre inngangsvektor og benytte beste praksiser for å best mulig slette alle spor av angrepsaktør. På tross av dette kan det i verste tilfelle likevel være behov for en komplett sletting, for eksempel i et omfattende løsepengevirusangrep. Følgelig anbefales det at virksomheten også tar sikte på å utarbeide en plan for dette, som kan testes regelmessig i et testmiljø.

5 Koordinering av team

5.1 Hendelseshåndterer

Hendelseshåndterer skal videre gjøre sårbarhetsanalysen. Dette kan først gjøres ved å bruke Redigert Innhold.

Fremgangsmåte: Redigert innhold

Videre skal det bli gjort en nettverkssårbarhetsanalyse. Dette kan bli gjort med en port skanner som NMAP.

Bruk av NMAP:

5.2 Hendelsesleder

Hendelsesleder skal sørge for at beste praksiser (seksjon 3.1.1) blir fulgt av alle i teamet. Hendelseslederen skal også sørge for at alt blir dokumentert av alle i teamet. I tillegg skal hendelseslederen se over og vurdere om hendelseshåndterer trenger hjelp fra triage asvarlig og It og infrastruktur ansvarlig.

5.3 Triage-ansvarlig

Triage-ansvarlig skal sørge for å tett overvåke berørte systemer og gi beskjed til andre i teamet om det er noe mistenkelig aktivitet under hele eradication fasen.

5.4 IT og infrastruktur

IT og infrastruktur ansvarlig skal hjelpe hendelseshåndterer med "wipe og reimage" av berørte systemer. En kan se nærmere på dette i seksjon 4 og instruksjoner til hvordan dette blir gjort i seksjon 6.1.

Recovery

Espen Eriksen, Jan Ngo, Farhaz Ismail, Ranvir Singh

May 19, 2022

Contents

1 Om denne fasen

Denne fasen handler om å gjenopprette berørte data, systemer og/eller enheter tilbake til normal tilstand, altså tilstanden før hendelsen oppsto. Det er viktig å få systemene og forretningsdriften i gang igjen uten frykt for enda et angrep. Det er også viktig å ha en plan på tidspunkt for gjenoppretting. Tidspunktet vil avhenge av hvor lang tid gjenopprettingen tar, hva som skal gjenopprettes m.m. Det skal bli gjort grundig tester av systemene for å verifisere at alt er klart for å gå tilbake til normal drift.

2 Gjenoppretting til normaltilstand

2.1 Prioritering av gjenoppretting

Skriv rundt dette:

- Tid for gjenoppretting. Tar det av ressurser?
- Hva er mest virksomhetskritisk?
- Noe annet?

Virksomheten må vurdere prioriteringen av hva som skal bli gjenopprettet etter hvor kritisk det er for virksomheten. Dette skal bli vurdert av hendelsesleder sammen med ledelsen. Ut ifra prioriteringen skal det bli definert tid og dato for når gjenopprettingen skal foregå.

2.2 Typer gjenoppretting

Skriv litt om hvordan en gjenoppretter følgende:

- Tjenester som f.eks. Redigert Innhold.
- Endepunktsklienter.
- Servere.

2.3 Før gjenoppretting

Sikkerhetskopier skal bli gjenopprettet avhengig av hva som trengs. Det blir ikke alltid nødvendig med gjenopprettelse av alle sikkerhetskopier etter en hendelse. Integriteten til disse sikkerhetskopiene skal bli verifisert da det er mulig at sikkerhetskopiene også ble kompromittert under hendelsen. Hvis kompromitterte sikkerhetskopier blir brukt i gjenopprettingen så kan angrepet spre seg i virksomheten. Selve gjenopprettingen av sikkerhetskopier bør derfor bli testet i et testmiljø før en gjør det i produksjonsmiljøet. Hvis mulig skal gjenopprettingen skje før en fjerner det som ble isolert under hendelsen.

Det skal være definerte rutiner for både testing og verifisering som kan bli brukt i denne fasen. (Disse skal bli laget av Moelven.)

2.3.1 Etter gjenoppretting

Etter å ha gjenopprettet all data skal det bli verifisert at alt fungerer som det skal. Her kan det bli brukt en type for normalnivå som kan brukes for sammenligning med nivået før

hendelsen oppsto og den nåværende situasjonen. Utenom det skal IR teamet sjekke opp at de gjenopprettede systemene er klar til bruk i produksjon.

Med dette så kan virksomheten få tilbake drift av systemer og begynne med å komme tilbake til normal stand. Det er fortsatt viktig med overvåkning over systemer mens de er i normal drift for å se etter potensielle skjulte elementer fra angrepsaktører.

3 Oppdatering av systemer

Ut ifra analyse og informasjonen en har fått fra hendelsen, skal en se om det er mulig å patche/oppdatere systemer for å styrke sikkerheten. En burde ha oppdaget rotårsaken til angrepet hvis en er i denne fasen og det skal bli satt tiltak for å unngå det i fremtiden. Svakheter og sikkerhetshull som blir oppdaget skal bli patchet av IT og Infrastruktur ansvarlige.

For phishing angrep blir det ikke like relevant med sikkerhetsoppdateringer da det er mest sannsynlig at angrepet kom gjennom en kompromittert konto. Mer bevissthetstrening rundt phishing blir viktig om en blir utsatt for phsihing angrep.

Virksomheten kan bli utsatt for løsepengevirus gjennom bruk av bakdører. Bakdører er en vei inn i et system som er åpnet av uvedkommende og som ikke er kjent av system eier. Dette kan oppstå om det er svakheter i systemene eller gjennom en åpen port i nettverket for eksempel. Ved å se nærmere på og undersøke berørte systemer fra angrepet kan en muligens finne slike svakheter.

4 Koordinering av team

(Hele denne seksjonen må forbindes med "Kommunikasjonskanaler" og "Team og roller" i Preparation.)

4.1 Hendelseshåndterer

Hendelseshåndterer har ansvar for å gjenopprette sikkerhetskopier. Det skal først bli sjekket opp og verifisert om sikkerhetskopiene ikke er kompromitterte. Disse sikkerhetskopiene skal først bli gjenopprettet i et testmiljø og deretter i det faktiske produksjonsmiljøet.

4.2 Hendelsesleder

Hendelsesleder skal sammen med ledelsen ta en vurdering over hva som skal bli prioritert under gjenopprettingen. Videre skal hendelseslederen kommunisere med hendelseshåndterer og IT og infrastruktur ansvarlig om dette. Hendelsesleder sørger for at alt blir dokumentert.

4.3 IT og Infrastruktur

IT og infrastruktur ansvarlig har ansvar for å gjøre sikkerhetsoppdateringer om nødvendig. I tillegg skal de hjelpe hendelseshåndterer med gjenopprettingen om nødvendig. IT og infrastruktur ansvarlig skal undersøke berørte systemer og se om det er noen sikkerhetshull eller svakheter som må bli håndtert.

Lessons Learned

Espen Eriksen, Jan Ngo, Farhaz Ismail, Ranvir Singh

May 19, 2022

Contents

1 Om denne fasen

I denne fasen skal en se over hva en har lært fra hendelsen og hva som kan gjøres bedre neste gang. Hensikten er å gjennomføre all dokumentasjon som ikke ble utformet under hendelsen, og i tillegg dokumentere det som kan være av bruk til fremtidige hendelser. Videre skal det lages en hendelsesrapport som gir oversikt over hele hendelsen, og til slutt ha et lærdomsmøte der det diskuteres om hendelsen, og hvordan implementere lærdommen fra hendelsen.

2 Dokumentasjon

Det skal ha vært dokumentering under hele hendelsen, men om det ikke ble utført på noen steg så skal det bli utført her. Dokumentasjon gir data som kan analyseres. Noen hendelser kan være små i forhold til andre og hyppigheten kan variere, men det er viktig å få dokumentert disse hendelsene, ettersom det utgir mer data for analyse. Dette vil gi mer informasjon om menneskelig feil, regulatoriske feil, systemfeil og mer som kan hjelpe med å forebygge mot fremtidige angrep.

Dokumentasjonen kan bli brukt som et referansepunkt for sammenligning for fremtidige hendelser, og i tillegg også bli brukt for treningsmaterial for fremtidig nye medlemmer av teamet.

3 Hendelsesrapport

Hendelsesrapporten skal bestå av en "play-by-play" gjennomgang av hele hendelsen. Det betyr at hver detalj under hendelsen skal bli beskrevet. Informasjon fra denne rapporten kan være av hjelp for fremtidige hendelser som et referansepunkt for sammenligning.

Ved slutten av denne rapporten skal det skrives en oppsummering som skal sendes til ledelsen.

4 Måter å forberede seg på

En skal selvstendig reflektere over hva som kunne vært utført bedre under hendelsen. Dette skal være en forberedelse før lærdomsmøte. Følgende er spørsmål en kan spørre seg selv:

- Hva var bra?
- Hva var greit?
- Hva var dårlig?
- Hva kunne jeg ha utført bedre?
- Hva ble mest prioritert under hendelsen?
- Var prioritetslisten korrekt?
- Ble alle stegene i hendelseshåndteringen utført? Om ikke, hvorfor?
- Var dokumentasjonen utfyllende? Om ikke, hvorfor?

5 Lærdomsmøte

Det skal være møter med IR-team og andre interessenter for å diskutere hendelsene, og hvordan de kan implementere lærdom fra hendelsen. Videre skal hendelsesrapporten gjennomgås felles. Dette møtet er anbefalt å holde så tidlig som mulig etter hendelsen.

En kan ha presentasjon som blir ført av hendelsesleder, hvor blant annet følgende blir tatt opp:

- Når ble problemet først oppdaget og av hvem?
- Omfanget av hendelsen
- Hvilke spesifikke ressurser/eiendeler og platformer ble det målrettet mot?
- Hva slags data ble eksponert?
- Hvordan hendelsen ble begrenset (contained) og utryddet (eradicated)?
- Arbeid utført under recovery fasen
- Områder der IR-teamet var effektive
- Hvordan eksisterende sikkerhetstiltak fungerte
- Områder som trenger forbedring
- Annet relevant fra alle som deltar i møtet

B Vedlegg: Prosjektplan

Prosjektplan

Ranvir Singh, Farhaz Ismail, Jan Ngo, Espen Eriksen

31. Januar 2022

Innholdsfortegnelse

Figurer

1 Mål og rammer

Denne delen av prosjektplanen inneholder en kort beskrivelse av bakgrunnen til oppgaven, hvilke målsetninger som er satt og hva rammene rundt oppgaven er.

1.1 Bakgrunn

Vi har fått tildelt oppgaven "Incident Response og Incident Response Training" som bacheloroppgave. Denne bacheloroppgaven er en avsluttende oppgave for bachelorstudiet Digital infrastruktur og cybersikkerhet. Oppgaven skal gjennomføres for oppdragsgiver Moelven Industrier ASA. Moelven Industrier ASA er et skandinavisk industrikonsern med hovedkontor i Moelv og har omlag 3200 ansatte. Hovedmarkedet til Moelven er Skandinavia og alle produksjonsenhetene til Moelven ligger også i Skandinavia. Moelven-konsernet omfatter totalt 33 produksjonsselskaper fordelt på 41 produksjonssteder i Sverige og Norge. De har i tillegg salgsapparater i Norge, Sverige, Storbritannia, Danmark, Tyskland og Kina.

Oppgaven går ut på å utforme gode og tilpassede incident response-rutiner og incident response training-strategier for Moelven. Dette skal hjelpe Moelven med å være bedre rustet ved ulike sikkerhetshendelser. Moelven skal bruke disse rutinene basert på alvorlighetsgrad og type hendelse.

1.2 Prosjektmål

1.2.1 Effektmål

Effektmål for oppgaven inkluderer å redusere tiden fra en sikkerhetshendelse oppstår til ansvarlige blir varslet, samt redusere antall hendelser som ikke blir varslet om og at ansatte tar lærdom av sikkerhetshendelser til å forbedre sine rutiner.

1.2.2 Resultatmål

Resultatmål for oppgaven inkluderer å utarbeide en rapport som kan bistå oppdragsgiver med incident response-rutiner og utarbeide incident response training-strategier som kan trene personell i hendelseshåndtering.

1.3 Rammer

Rapporten blir skrevet i Overleaf. Arbeidsoppgaver legges inn i GitHub, hvor de blir tildelt, og tidsfrister for gjøremålene blir satt. Prosjektet skal være ferdig og levert innen 20. mai 2022.

1.3.1 Kontaktpersoner

Kontaktpersoner hos Moelven er:

- Stefan Djupvik, leder IT-utvikling, e-post: stefan.djupvik@moelven.com
- Tom Kjølhamar, fagansvarlig IT-Sikkerhet, e-post: tom.kjolhamar@moelven.com

Veileder fra NTNU Gjøvik er:

- Erjon Zoto, veileder og universitetslektor, e-post: erjon.zoto@ntnu.no

Andre kontaktpersoner fra NTNU Gjøvik:

- Tom Røise, emneansvarlig (for PROG) og universitetslektor, e-post: tom.roise@ntnu.no
- Erik Hjelmås, emneansvarlig (for DIGSEC) og førsteamanuensis, e-post: erik.hjelmas@ntnu.no

1.3.2 Tidsfrister

Rapportens innleveringsfrist er satt av NTNU Gjøvik, og skal leveres senest den 20. mai 2022.

1.3.3 Arbeidsmiljø

Vi skal benytte oss av LaTeX for å skrive og utforme rapporten i Overleaf.

2 Omfang

Denne delen av planen tar for seg en generell beskrivelse av det overordnede problemområdet for oppgaven, en avgrensning av dette og til slutt en problemstilling rapporten skal svare på.

2.1 Problemområde

Hendelseshåndtering går ut på å oppdage og respondere på IKT-sikkerhetshendelser. En sikkerhetshendelse er en situasjon eller aktivitet som truer personell, informasjon og andre verdier. En slik hendelse kan oppstå når en aktør får tilgang til ett eller flere informasjonssystemer. Hendelseshåndteringsprosessen går ut på blant annet å identifisere og klassifisere hendelsen, kartlegge hvordan tilgangen ble kompromittert, begrense og hindre videre uønsket

aktivitet, sikre bevis, returnere til normaltilstand, lage læringspunkter fra hendelsen og lage tiltak for videre sikkerhet, og til slutt rapportere hendelsen. [**NSM**]

2.2 Problemavgrensning

Oppgaven vil hovedsakelig fokusere på å utarbeide et incident response-rammeverk for phishing- og ransomwareangrep. Den vil ta utgangspunkt i disse angrepsvektorene hver for seg, men også se på hvordan phishingangrep eller forsøk på phishing kan være en inngangsvektor for ransomware.

Oppgaven vil også utarbeide en opplæringsmodell for de ansatte som tar sikte på å øke kompetanse og bevissthet rundt typiske angrepsscenarier, og trene dem i hvordan de skal håndtere slike hendelser.

2.3 Problemstilling

Det digitale trusselbildet blir større og større, og det blir stadig vanskeligere å beskytte seg. Samtidig er balansegangen mellom funksjonalitet og sikkerhet utfordrende. Oppgaven tar for seg disse problemstillingene ved å utforme et incident response-rammeverk, slik at ansatte tar bevisste og riktige valg etter at en sikkerhetshendelse har oppstått.

3 Prosjektorganisering

Denne delen av prosjektplanen handler om hvordan vi skal organisere gruppen, hvilke roller og ansvar hver person har, hvor vi skal arbeide, når vi skal arbeide og hvordan vi skal sikre at arbeid blir levert i tide med planlagt kvalitetsnivå.

3.1 Roller og ansvarsforhold

3.1.1 Roller

- Felles

  Fordele arbeidsoppgaver.

- Leder

  Lederrollen er en rullerende rolle, med to ukers varighet. Leder er ansvarlig for kontinuerlig fremdrift i prosjektet og at det er laget ukesplan (at det er planlagt hva som skal gjøres hvilke dager). Merk at ukesplan bør lages i samarbeid med gruppen. Har hovedansvaret for å bestemme hva som skal jobbes med hvilke dager og fordele arbeidsoppgaver fortløpende. Dette for å unngå at dager ikke er uplanlagte og at det oppstår dødtid. Leder har dessuten ansvar for å føre brudd på arbeidskontrakt og eventuelt bøtelegge.

- Kundekontakt (Ranvir)

  Ansvarlig for møteinnkalling til ekstern m/ agenda og holde eksterne møter.

- Dokumentansvarlig (Farhaz)

  Ansvar for å gjøre alle dokumenter tilgjengelige for gruppemedlemmer og opprette ressursliste og holde den oppdatert.

- Møteansvarlig (Jan)

  Ansvarlig for møteinnkalling intern med agenda og holde møtet. Skal skrive møtereferat og følge opp det som ble gjennomgått på møtet. Hva skal gjøres og hvem skal gjøre det? Ansvar for å booke grupperom.

- Kvalitetssikring (Primær: Espen, (evt. sekundær: Farhaz))

  Gå gjennom arbeid som er gjort og markere det som ferdig, samtidig korrekturlese skrevet innhold og komme med forslag til endringer.

3.2 Arbeidssted

Hovedsakelig på skolen i et grupperom, må endres etter koronatiltak og NTNUs situasjon. Sekundært blir hjemme på Discord/Teams/Zoom, bruk av program etter behov.

3.3 Arbeidstid

Fast arbeidstid kl. 09.00 til kl. 15.00. Pause fra kl. 12.45 til 13.00. Det er mulig å ta flere pauser etter behov. Arbeidstid er i utgangspunktet mandag-torsdag, fredag er 3 av 4 opptatt og man må selv disponere tapt tid.

3.4 Arbeidsflyt

- Frister
  - Alle gruppemedlemmer har ansvar for å legge til gjøremål med frister.
  - Frister skal overholdes, og bør helst være ferdig så fort som mulig.
- Arbeidsfordeling
  - For oppgaver som ikke skal tas felles, jobbes det i grupper på to og to. Det rulleres på hvem som jobber sammen.
- Timeplan for prosjektet.
  - Se gantt-skjema lengre ned.
- Forventet innsats:
  - Gruppemedlemmet må jobbe like mye som den man jobber sammen med.

  - Arbeidsoppgaver blir gjort innen satt delfrist.
  - Dersom man ikke rekker å gjøre arbeidsoppgaver i tide, må man si ifra så fort som mulig slik at andre kan hjelpe til eller at arbeidsoppgaven endres.
  - Det er lov å sjekke sosiale medier, men arbeidsøkten skal hovedsakelig gå til relevant arbeid og man bør ikke bruke mer enn fem minutter+- på andre ting. Det kan gjøres i pauser.
  - Om det ikke er noe å gjøre, bør det diskuteres i gruppa. Man kan eventuelt hjelpe andre gruppemedlemmer eller avslutte økten dersom det ikke er noe som helst å gjøre (men dette bør ikke skje).

- Kildehenvisning
  - Kildehenvisning med Harvard-stil.
  - Legg til alle kilder som brukes med en gang. Skal refereres fortløpende.
  - Legg til forkortelser i en ordliste fortløpende.

- Plikter
  - Møte opp til avtalt tid.
  - Man må ha en grunn til forsinkelser. Gi beskjed.
  - Forsovelse er gyldig grunn, men man må fortsatt betale bot. Om det skjer gjentatte ganger, for eksempel fire ganger, er det ikke greit og gruppen må diskutere hva konsekvensen blir.
  - Man bør være til stede gjennom hele møtet.

- Advarsler og bøter
  - Om man ikke møter opp til tide eller gir beskjed med gyldig grunn:
    * 45 kr bot.
  - Om man ikke møter opp til tide eller gir beskjed med gyldig grunn fem ganger:
    * Gruppen kan beslutte å kaste ut gruppemedlem.

4 Planlegging, oppfølging, rapportering

Denne delen inneholder valg av prosessrammeverk og argumentasjon for valget, og en plan for møter og beslutninger.

4.1 Hovedinndeling av prosjektet

For valg av prosessrammeverk har gruppen vår valgt å bruke et scrum board som prosessrammeverk å følge. Å bruke scrum board fremmer interaksjon mellom gruppemedlemmene. Alle i gruppen vil kunne se hva som må gjøres og hvor langt vi har kommet. Vi kan da diskutere progresjonen vår og se på hvordan ulike oppgaver utvikler seg. Det gjør det også

enkelt å visualisere prosjektfremdriften slik at vi kan være sikre på at framgangen til prosjektet går som planlagt. Ettersom alle kan se hva som jobbes med i et scrum board, minker det sjansen på at flere feilaktig jobber med samme gjøremål.

Vi har valgt å inkludere kvalitetssikring som en egen fase i vårt scrum board. Kvalitetssikringsfasen kommer etter gjøremålsfasen, og skal sikre at arbeidet er av tilfredsstillende kvalitet. I kvalitetssikringsfasen vil oppgavene som er håndtert gjennomgås for feil og/eller mangler, og nødvendige korreksjoner vil eventuelt bli gjort.

Vi valgte GitHub til vårt scrum board for dette prosjektet. Vi er allerede kjent med GitHub fra tidligere prosjekter og er fornøyde med hvordan det har fungert. Gruppen sin måte å følge modellen på er illustrert ved figur 1:

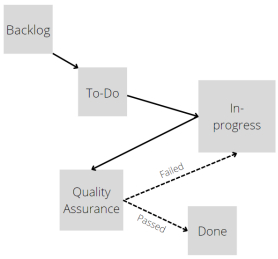


Figure 1: Hvordan gruppa følger modellen

Vi starter med å lage “issues” som forskjellige gjøremål. Gjøremålene legges inn i backlog-tabellen i brettet. Etter at vi har utformet overordnet gjøremål, kalt stories, markerer vi issues i henhold til hvilken story de tilhører. Deretter flyttes de markerte issues inn til to-do-tabellen. Her blir forskjellige issues tildelt gruppemedlemmene. Tildelingen, samt sprintens varighet, bestemmes felles i gruppen på starten av en sprint. Når man begynner på en oppgave flyttes den til “in-progress”-tabellen. Når oppgaven er håndtert, vil den flyttes videre til en kvalitetssikringsfase. I denne fasen vil gruppemedlemmene med rollen ”kvalitetssikring” gjennomgå oppgaven og komme med innspill eller forslag til endringer ved behov. Veileder er vår primære kontaktperson for tilbakemeldinger, og vi vil forhøre oss med veileder om nødvendig. For enkelte oppgaver kan oppdragsgiver bli kontaktet for å forsikre oss om at vi er på riktig vei og at arbeidet blir gjort i henhold til oppdragsgivers ønsker.

Når man er ferdig med oppgaven flyttes issues til ”done”-tabellen, hvor man kan velge å avslutte issues med en kommentar. Når sprinten er ferdig, vil gruppa samles og kunne diskutere om det som ble gjort tilfredsstiller arbeidsmengden oppgaven krever. Dersom kravene ikke er tilfredsstilt, vil en ny iterasjon av samme oppgave gjennomføres basert på de tilbakemeldingene og konklusjonene som ble gjort.

4.2 Plan for statusmøter og beslutningsmøter i perioden

Det skal være to interne statusmøter i uka. Et møte i starten av uka, og et møte i slutten. Varighet på 45 min, men kan forlenges ved behov. Vi skal forsøke å holde ukentlig kontakt med både oppdragsgiver og veileder.

Vedrørende plan for beslutningspunkter, skal gruppen ta en diskusjon om videreføring av prosjektet etter at prosjektplan er levert. Det vil bli avholdt jevnlige statusmøter for å holde orden på fremdriften i prosjektet. Siste møte før levering av endelig rapport er 18. mai.

5 Organisering av kvalitetssikring

Denne delen inneholder hvilke verktøy vi har planlagt å bruke, en plan for testing, og en risikoanalyse av prosjektet.

- Arbeidsverktøy
  - Tekstbehandler: LaTeX i Overleaf
  - Privat GitHub-repo for scrum board
  - Discord for interne møter og arbeidsøkter
  - Teams for dokumenter og møter med oppdragsgiver
- Plan for inspeksjoner og testing
  - Test av vår "incident response training"-rapport.

5.1 Risikoanalyse på prosjektnivå

5.1.1 Teknologisk:

R4	Tap av pågående arbeid
R6	Tap av tilgang på fullført arbeid
R7	Tap av tilgjengelighet av ressurser fra oppdragsgiver

5.1.2 Forretningsmessig:

R2	Lekkasje av sensitive detaljer
R3	Moelven slutter med kommunikasjonen

5.1.3 Prosjektgruppemessig:

R1	Gruppemedlem blir syk
R5	Oppgaven går ikke som planlagt

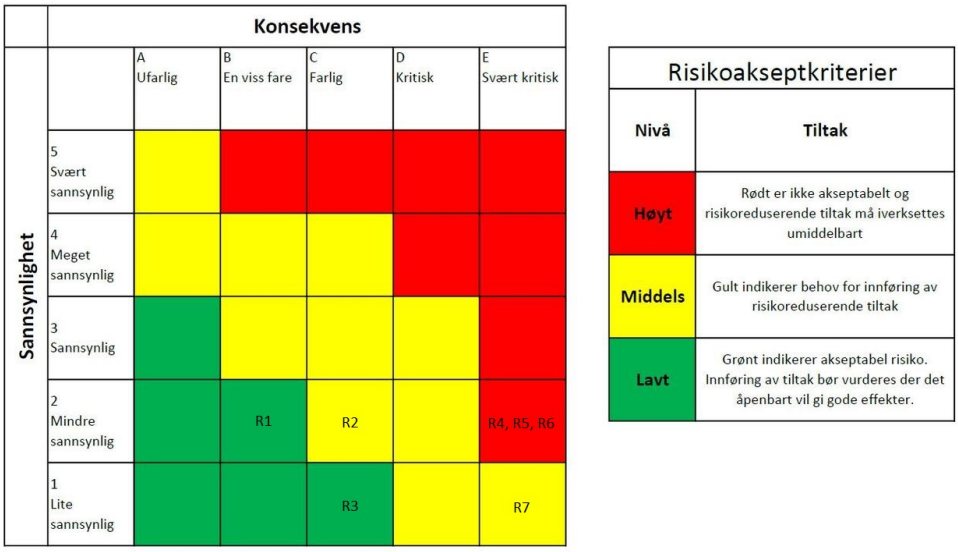


Figure 2: Risikomatrise før tiltak

5.2 Tiltak

- Gruppemedlem blir syk - R1

  Utenfor vår kontroll, men å ha en plan klar kan hjelpe. Vi kan for eksempel fordele arbeidet mellom de som ikke er syke, helt til den syke kommer tilbake. Den syke skal da ta igjen arbeidet som den har mistet. Hvis den syke ikke klarer å komme tilbake, blir det flere konsekvenser og mer arbeid for de andre gruppemedlemmene.

- Lekkasje av sensitive detaljer - R2

  Ha tilgangskontroll og holde dokumentene våre private.

- Moelven slutter med kommunikasjonen - R3

  Vi må være være tydelig med vår kommunikasjon med Moelven. Hvis det faktisk skjer må vi jobbe med andre ting som ikke er avhengig av svar fra Moelven.

- Tap av pågående arbeid - R4

  Ta backup av alle dokumenter slik at vi alltid er sikre på at dokumentene ikke kommer til å forsvinne. Vi har også en plan for hvor dokumenter skal ligge (avtalt at dokumenter skal ligge i teams og ikke lokalt på sin pc).

- Oppgaven går ikke som planlagt - R5

  Å ha en klar plan fra starten kan hjelpe med å unngå dette. Ukentlig møter med veileder og oppdragsgiver for å se om alt er i orden er også viktig for å unngå at oppgaver ikke går som planlagt.

- Tap av fullført arbeid - R6

  Jevnlig oppdatere dokumentene og sjekke tilgjengeligheten av alle dokumenter som blir skrevet i og opplastet til Teams og Overleaf. Ettersom det også må kvalitetssikres, blir det dobbeltsjekk og trippeltsjekk på at alt er tilgjengelig og fungerer som det skal.

- Tap av tilgjengelighet av ressurser fra oppdragsgiver - R7

  Alt gruppen får tilsendt fra oppdragsgiver skal bli lagret i gruppens interne Teams kanal. Vi kan også etterspørre ressurser dersom de blir utilgjengelige.

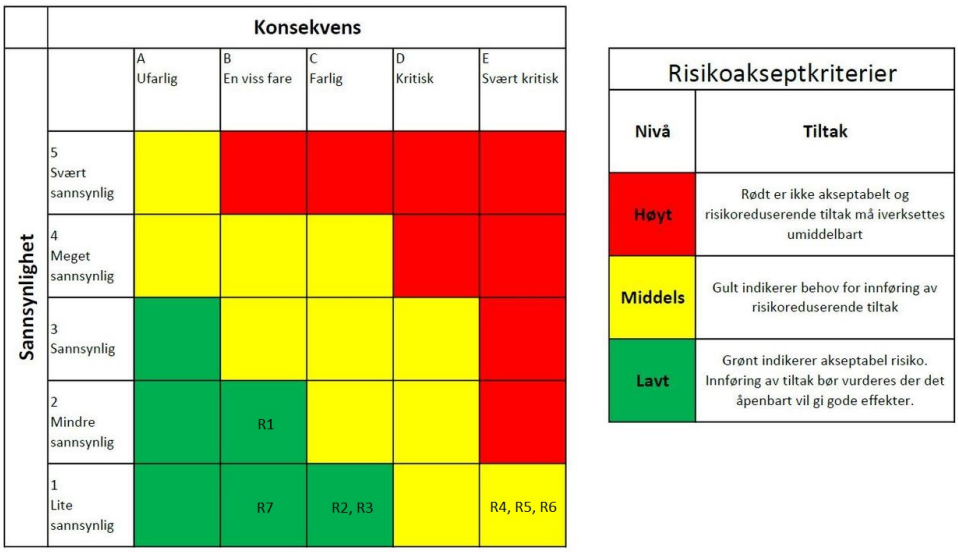


Figure 3: Risikomatrise etter tiltak

6 Plan for gjennomføring

Under er en overordnet plan for hele prosjektet innført i et Gantt-skjema, og diverse milepæler vi har planlagt.

6.1 Milepæler

Våre milepæler er:

Å få godkjent prosjektplanen med innleveringsfrist 31.01.2022.

Få presentert rammeverket for oppdragsgiver før sluttdato av prosjektet 10. Mai 2022.

Levert ferdig prosjektrapport til NTNU 20.Mai 2022.

References

[1] Søknads-og kravdokument, NSMs kvalitetsordning for Hendelseshåndtering. (n.d.). [online] Available at: https://nsm.no/getfile.php/134175-1600072772/Filer/Dokumenter/NSMs%20kvalitetsordning_HH_S%C3%B8knads-%20og%20kravdokument%20Ver%202_0.docx.pdf [Accessed 24 Jan. 2022].

Navn	Startdato	Sluttdato
Lage prosjektplan	20.01.2022	25.01.2022
Definere omfang	20.01.2022	25.01.2022
Informasjonsinnhenting fra Moelven	17.01.2022	29.04.2022
Informasjonsinnhenting	18.01.2022	11.02.2022
Finne kilder	18.01.2022	11.02.2022
Vurdere kilder	28.01.2022	11.02.2022
Lære LateX	20.01.2022	07.02.2022
Kartlegging av viktige detaljer	25.01.2022	29.04.2022
Rapportskriving	25.01.2022	13.05.2022
Levere Prosjektplan	31.01.2022	31.01.2022
Literaturstudie	31.01.2022	28.02.2022
Statusrapport	31.01.2022	31.01.2022
Lage rammeverk	02.02.2022	15.04.2022
Lage "incident response" rutiner	18.02.2022	24.05.2022
Statusrapport	28.02.2022	28.02.2022
Lage "incident response training" opplegg	23.03.2022	20.04.2022
Statusrapport	31.03.2022	31.03.2022
Test av "incident response training" opplegg	01.04.2022	07.04.2022
Statusrapport	29.04.2022	29.04.2022
Levere Bacheloroppgaven	19.05.2022	19.05.2022
Refleksjonsnotat	13.05.2022	20.05.2022
Presentasjonsforberedelser	23.05.2022	01.06.2022
Presentasjon	01.06.2022	01.06.2022

Figure 4: Gantt-skjema

C Vedlegg: Standardavtale

NTNU

Norges teknisk-naturvitenskapelige universitet

Fastsatt av prorektor for utdanning 10.12.2020

STANDARDAVTALE

om utføring av studentoppgave i samarbeid med ekstern virksomhet

Avtalen er ufravikelig for studentoppgaver (heretter oppgave) ved NTNU som utføres i samarbeid med ekstern virksomhet.

Forklaring av begrep

Opphavsrett
Er den rett som den som skaper et åndsverk har til å fremstille eksemplar av åndsverket og gjøre det tilgjengelig for allmennheten. Et åndsverk kan være et litterært, vitenskapelig eller kunstnerisk verk. En studentoppgave vil være et åndsverk.

Eiendomsrett til resultater
Betyr at den som eier resultatene bestemmer over disse. Utgangspunktet er at studenten eier resultatene fra sitt studentarbeid. Studenten kan også overføre eiendomsretten til den eksterne virksomheten.

Bruksrett til resultater
Den som eier resultatene kan gi andre en rett til å bruke resultatene, f.eks. at studenten gir NTNU og den eksterne virksomheten rett til å bruke resultatene fra studentoppgaven i deres virksomhet.

Prosjektbakgrunn
Det partene i avtalen har med seg inn i prosjektet, dvs. som vedkommende eier eller har rettigheter til fra før og som brukes i det videre arbeidet med studentoppgaven. Dette kan også være materiale som tredjepersoner (som ikke er part i avtalen) har rettigheter til.

Utsatt offentliggjøring
Betyr at oppgaven ikke blir tilgjengelig for allmennheten før etter en viss tid, f.eks. før etter tre år. Da vil det kun være veileder ved NTNU, sensorene og den eksterne virksomheten som har tilgang til studentarbeidet de tre første årene etter at studentarbeidet er innlevert.

1. Avtaleparter

Norges teknisk-naturvitenskapelige universitet (NTNU) Institutt: Institutt for informasjonsteknologi og kommunikasjonsteknologi
Veileder ved NTNU: Erjon Zoto e-post og tlf. erjon.zoto@ntnu.no, 984 33 097
Ekstern virksomhet: Moelven Industrier Ekstern virksomhet sin kontaktperson, e-post og tlf.: Stefan Djupvik, stefan.djupvik@moelven.com, 976 63 776
Student: Espen Eriksen Fødselsdato: 11.10.1996
Student: Farhaz Ismail Fødselsdato: 06.07.2000
Student: Jan Ngo Fødselsdato: 08.12.2000
Student: Ranvir Singh Fødselsdato: 07.01.2000
Ev. flere studenter[1]

Partene har ansvar for å klarere eventuelle immaterielle rettigheter som studenten, NTNU, den eksterne eller tredjeperson (som ikke er part i avtalen) har til prosjektbakgrunn før bruk i forbindelse med utførelse av oppgaven. Eierskap til prosjektbakgrunn skal fremgå av eget vedlegg til avtalen der dette kan ha betydning for utførelse av oppgaven.

2. Utførelse av oppgave

Studenten skal utføre: (sett kryss)

Masteroppgave	
Bacheloroppgave	X
Prosjektoppgave	
Annen oppgave	

Startdato: 06.01.2022
Sluttdato: 20.05.2022

Oppgavens arbeidstittel er: «Incident Response og Incident Response Training»

[1] Dersom flere studenter skriver oppgave i fellesskap, kan alle føres opp her. Rettigheter ligger da i fellesskap mellom studentene. Dersom ekstern virksomhet i stedet ønsker at det skal inngås egen avtale med hver enkelt student, gjøres dette.

Ansvarlig veileder ved NTNU har det overordnede faglige ansvaret for utforming og godkjenning av prosjektbeskrivelse og studentens læring.

3. Ekstern virksomhet sine plikter

Ekstern virksomhet skal stille med en kontaktperson som har nødvendig faglig kompetanse til å gi studenten tilstrekkelig veiledning i samarbeid med veileder ved NTNU. Ekstern kontaktperson fremgår i punkt 1.

Formålet med oppgaven er studentarbeid. Oppgaven utføres som ledd i studiet. Studenten skal ikke motta lønn eller lignende godtgjørelse fra den eksterne for studentarbeidet. Utgifter knyttet til gjennomføring av oppgaven skal dekkes av den eksterne. Aktuelle utgifter kan for eksempel være reiser, materialer for bygging av prototyp, innkjøp av prøver, tester på lab, kjemikalier. Studenten skal klarere dekning av utgifter med ekstern virksomhet på forhånd.

Ekstern virksomhet skal dekke følgende utgifter til utførelse av oppgaven: Reise til Moelven kontoret i forbindelse med møter eller arbeidsdager.

Dekning av utgifter til annet enn det som er oppført her avgjøres av den eksterne underveis i arbeidet.

4. Studentens rettigheter

Studenten har opphavsrett til oppgaven[2]. Alle resultater av oppgaven, skapt av studenten alene gjennom arbeidet med oppgaven, eies av studenten med de begrensninger som følger av punkt 5, 6 og 7 nedenfor. Eiendomsretten til resultatene overføres til ekstern virksomhet hvis punkt 5 b er avkrysset eller for tilfelle som i punkt 6 (overføring ved patenterbare oppfinnelser).

I henhold til lov om opphavsrett til åndsverk beholder alltid studenten de ideelle rettigheter til eget åndsverk, dvs. retten til navngivelse og vern mot krenkende bruk.

Studenten har rett til å inngå egen avtale med NTNU om publisering av sin oppgave i NTNUs institusjonelle arkiv på Internett (NTNU Open). Studenten har også rett til å publisere oppgaven eller deler av den i andre sammenhenger dersom det ikke i denne avtalen er avtalt begrensninger i adgangen til å publisere, jf. punkt 8.

5. Den eksterne virksomheten sine rettigheter

[2] Jf. Lov om opphavsrett til åndsverk mv. av 15.06.2018 § 1

Der oppgaven bygger på, eller videreutvikler materiale og/eller metoder (prosjektbakgrunn) som eies av den eksterne, eies prosjektbakgrunnen fortsatt av den eksterne. Hvis studenten skal utnytte resultater som inkluderer den eksterne sin prosjektbakgrunn, forutsetter dette at det er inngått egen avtale om dette mellom studenten og den eksterne virksomheten.

Alternativ a) (sett kryss) Hovedregel

X	Ekstern virksomhet skal ha bruksrett til resultatene av oppgaven

Dette innebærer at ekstern virksomhet skal ha rett til å benytte resultatene av oppgaven i egen virksomhet. Retten er ikke-eksklusiv.

Alternativ b) (sett kryss) Unntak

	Ekstern virksomhet skal ha eiendomsretten til resultatene av oppgaven og studentens bidrag i ekstern virksomhet sitt prosjekt

Begrunnelse for at ekstern virksomhet har behov for å få overført eiendomsrett til resultatene:

6. Godtgjøring ved patenterbare oppfinnelser

Dersom studenten i forbindelse med utførelsen av oppgaven har nådd frem til en patenterbar oppfinnelse, enten alene eller sammen med andre, kan den eksterne kreve retten til oppfinnelsen overført til seg. Dette forutsetter at utnyttelsen av oppfinnelsen faller inn under den eksterne sitt virksomhetsområde. I så fall har studenten krav på rimelig godtgjøring. Godtgjøringen skal fastsettes i samsvar med arbeidstakeroppfinnelsesloven § 7. Fristbestemmelsene i § 7 gis tilsvarende anvendelse.

7. NTNU sine rettigheter

De innleverte filer av oppgaven med vedlegg, som er nødvendig for sensur og arkivering ved NTNU, tilhører NTNU. NTNU får en vederlagsfri bruksrett til resultatene av oppgaven, inkludert vedlegg til denne, og kan benytte dette til undervisnings- og forskningsformål med de eventuelle begrensninger som fremgår i punkt 8.

8. Utsatt offentliggjøring

Hovedregelen er at studentoppgaver skal være offentlige.

Sett kryss

X	Oppgaven skal være offentlig

I særlige tilfeller kan partene bli enige om at hele eller deler av oppgaven skal være undergitt utsatt offentliggjøring i maksimalt tre år. Hvis oppgaven unntas fra offentliggjøring, vil den kun være tilgjengelig for student, ekstern virksomhet og veileder i denne perioden. Sensurkomiteen vil ha tilgang til oppgaven i forbindelse med sensur. Student, veileder og sensorer har taushetsplikt om innhold som er unntatt offentliggjøring.

Oppgaven skal være underlagt utsatt offentliggjøring i (sett kryss hvis dette er aktuelt):

Sett kryss		Sett dato
	ett år	
	to år	
	tre år	

Behovet for utsatt offentliggjøring er begrunnet ut fra følgende:

Dersom partene, etter at oppgaven er ferdig, blir enig om at det ikke er behov for utsatt offentliggjøring, kan dette endres. I så fall skal dette avtales skriftlig.

Vedlegg til oppgaven kan unntas ut over tre år etter forespørsel fra ekstern virksomhet. NTNU (ved instituttet) og student skal godta dette hvis den eksterne har saklig grunn for å be om at et eller flere vedlegg unntas. Ekstern virksomhet må sende forespørsel før oppgaven leveres.

De delene av oppgaven som ikke er undergitt utsatt offentliggjøring, kan publiseres i NTNUs institusjonelle arkiv, jf. punkt 4, siste avsnitt. Selv om oppgaven er undergitt utsatt offentliggjøring, skal ekstern virksomhet legge til rette for at studenten kan benytte hele eller deler av oppgaven i forbindelse med jobbsøknader samt videreføring i et master- eller doktorgradsarbeid.

9. Generelt

Denne avtalen skal ha gyldighet foran andre avtaler som er eller blir opprettet mellom to av partene som er nevnt ovenfor. Dersom student og ekstern virksomhet skal inngå avtale om konfidensialitet om det som studenten får kjennskap til i eller gjennom den eksterne virksomheten, kan NTNUs standardmal for konfidensialitetsavtale benyttes.

Den eksterne sin egen konfidensialitetsavtale, eventuell konfidensialitetsavtale den eksterne har inngått i samarbeidprosjekter, kan også brukes forutsatt at den ikke inneholder punkter i motstrid med denne avtalen (om rettigheter, offentliggjøring mm). Dersom det likevel viser seg at det er motstrid, skal NTNUs standardavtale om utføring av studentoppgave gå foran. Eventuell avtale om konfidensialitet skal vedlegges denne avtalen.

Eventuell uenighet som følge av denne avtalen skal søkes løst ved forhandlinger. Hvis dette ikke fører frem, er partene enige om at tvisten avgjøres ved voldgift i henhold til norsk lov. Tvisten avgjøres av sorenskriveren ved Sør-Trøndelag tingrett eller den han/hun oppnevner.

Denne avtale er signert i fire eksemplarer hvor partene skal ha hvert sitt eksemplar. Avtalen er gyldig når den er underskrevet av NTNU v/instituttleder.

Signaturer:

Instituttleder: Dato:
Veileder ved NTNU: Dato:
Ekstern virksomhet: Tom Kjølhamar Dato: 28.01.2022
Student: Ranvir Singh Dato: 29.01.2022
Student: Dato:
Student: Farhaz Dato: 30.01.2022
Student: Espen Eriksen Dato: 31.01.2022

D Vedlegg: Statusrapporter

Statusrapporter

Ranvir Singh, Farhaz Ismail, Jan Ngo, Espen Eriksen

January 2022

1 Statusrapport 02.02.2022

1.1 Utført denne måneden

Denne perioden, som varte fra prosjektstart til idag, har vi arbeidet på og levert inn prosjektplanen. Vi har kommet igang med informasjonsinnhenting fra Moelven (oppdragsgiver) og har hatt tre møter med dem hittil. Arbeidet med generell informasjonsinnhenting for å øke gruppens kompetanse innenfor IR og relaterte rammeverk. I tillegg har gruppa økt kompetansen innenfor LaTeX, i samsvar med planen.

1.2 Avvik fra planen

Ifølge Gannt-skjemaet ligger vi bak når det kommer til å kartlegge og trekke ut viktige detaljer basert på informasjon Moelven har sendt. Årsaken til dette er at vi har lagt mer fokus på å tilegne oss mer kunnskap. Vi oppdaget at rapportskriving manglet fra Gannt-skjemaet i prosjektplanen.

1.3 Forbedringsplan

Vi har hatt møter med veileder om vår framgang i perioden, hvor vi fikk gode innspill på hva vi burde undersøke i Moelven, dette bør vi fortsette med. Vi bør begynne å kategorisere og kartlegge situasjonen i Moelven, slik at det blir enklere å arbeide i samsvar med det oppdragsgiver ønsker.

1.4 Konklusjon

Vi ligger nå litt bak i forhold til Gantt-skjemaet, men er godt i gang. Videre skal vi jobbe med å lage et rammeverk for "incident response" og lage "incident response" rutiner for Moelven. I tillegg skal vi fortsette med informasjonsinnhentingen og vurdere kilder.

2 Statusrapport 07.03.2022

2.1 Utført denne måneden

Denne perioden, som varte fra 02.02.2022 til idag, har vi endret en del på måten vi har jobbet på. Vi lagde en discord server, der vi har grupperom, hvor vi jobber, og møterom for å kunne fordele arbeid og jobbe bedre sammen. Vi har begynt med å skrive rammeverket og har kommet godt igang. Spesielt med preperation fasen i rammeverket vårt. Vi har også fått mer oversikt over hvor mange timer vi skal per uke for å kunne bli ferdig med prosjektet. Hver av medlemmene skal jobbe minst 30 timer i uka og vi loggfører det i et excel dokument. Vi har også hatt noen møter med Moelven for videre informasjonsinnhenting.

2.2 Avvik fra planen

Denne statusrapporten skulle ha blitt utført forrige uke, men på grunn av mye arbeid glemte vi å skrive den. Vi hadde planer om å ha ett fysisk møte med Moelven for et par uker siden, men måtte ta det online på grunn av sykdom i gruppen. Det var også planlagt å jobbe fysisk sammen på campus, men etter å ha prøvd det ut par ganger fant vi ut at det ikke ga en meningfull verdi. Vi hadde heller ikke lagt planer basert på Gannt skjemaet, som gjorde det vanskeligere å følge med på fremgangen vår.

2.3 Forbedringsplan

Vi har hatt ett internt møte der vi ble enige om å bruke gantt skjemaet vårt mer. Vi skal gå gjennom gantt skjemaet hver torsdag og se gjennom både det vi har gjort for den uken og hva som skal gjøres neste uke.

2.4 Konklusjon

Vi har kommet godt igang med rammeverket vårt og skal prøve å bli ferdig med den denne måneden. Videre vil vi starte med å jobbe med "incident training" opplegget vårt og faktisk begynen å skrive på hovedrapporten.

3 Statusrapport 06.04.2022

3.1 Utført denne måneden

Denne perioden, som varte fra 07.03.2022 til idag, har vi fokusert på å bli ferdig med fase 1 (Preparation) i rammeverket. Tiltaket vi introduserte i forrige statusrapport, om oppsjekk av gantt-skjema, har vi fulgt, og har hjulpet oss med å holde oss til planen. Vi har levert et utkast av preparation fasen til både oppdragsgiver og veileder for tilbakemelding. Vi har fått gjort klar en struktur på alle fasene i rammeverket, og vi har også kommet godt i gang med de andre fasene. Vi har også fått startet med å skrive på rapporten i slutten av denne perioden.

3.2 Avvik fra planen

Planen vår var å bli ferdig med hele rammeverket i denne perioden, men vi fant ut at det ikke var oppnåelig. Vi måtte justere på gantt-skjemaet litt.

3.3 Forbedringsplan

Ut ifra interne møter har vi kommet fram til at vi skal bruke mer tid på selve rapporten.

3.4 konklusjon

Videre skal vi ha fokus på rapporten og prøve å bli ferdig med rammeverket ved siden av. I tillegg skal vi begynne med trening opplegget vårt og forhåpentligvis bli ferdig med den også i den neste perioden.

E Vedlegg: Arbeidslogg

Navn:	Dato:	Timer:	Hva ble gjort:
Farhaz	06.01.2022	1	Internt møte - avtaler
	12.01.2022	2	Internt møte - avtaler/forarbeid + møte med veileder
	16.01.2022	1	Internt møte for møte med oppdragsgiver
	17.01.2022	5	arbeidsøkt + møte med oppdragsgiver
	18.01.2022	5	arbeidsøkt (prosjektplanlegging)
	19.01.2022	5	arbeidsøkt (prosjektplanlegging + gantt skjema)
	20.01.2022	5	internt møte - lesing av tidligere bacheloroppgaver
	21.01.2022	4	selvarbeid - læring av LateX og prosjektplanlegging
	24.01.2022	5	Læring av LateX + prosjektplanlegging
	25.01.2022	6	Møte med oppdragsgiver + prosjektplanlegging
	26.01.2022	6	Arbeidsøkt + møte med veileder
	27.01.2022	6	Literature review
	28.01.2022	5	literature review
	31.01.2022	6	Literature review
	01.02.2022	6	Literature review + ir rammeverk
	02.02.2022	6	Literature review + ir rammeverk
	03.02.2022	6	Literature review + ir rammeverk
	04.02.2022	6	Literature review + lete etter kilder
	07.02.2022	6	literature review + møte med veileder
	08.02.2022	6	literature review + skrive på rapport (metodikk)
	09.02.2022	6	rammeverkanalyse
	10.02.2022	6	rammeverkanalyse
	11.02.2022	5	rammeverkanalyse
	14.02.2022	4	Fysisk møte med oppdragsgiver
	15.02.2022	3	Start av kartlegging av applikasjon
	17.02.2022	3	Kartlegging av applikasjoner
	18.02.2022	6	Kartlegging av applikasjoner
	21.02.2022	6	Kartlegging av applikasjoner
	22.02.2022	4	starte med å klassifisere systemer
	23.02.2022	6	klassifisere systemer
	24.02.2022	6	klassifisere systemer og hendelser
	25.02.2022	6	policy arbeid
	28.02.2022	6	policy arbeid
	01.03.2022	6	Kommunikasjonsplan
	02.03.2022	4	Kommunikasjonsplan
	03.03.2022	4	Team - definere roller
	04.03.2022	6	Team - definere roller
	07.03.2022	6	Se på training i preparation
	08.03.2022	6	Se på training i preparation + hendelser
	09.03.2022	6	Starte med identifikasjon fase
	10.03.2022	6	Identifikasjonsfase + møte med oppdragsgiver
	11.03.2022	6	Identifikasjonsfase
	14.03.2022	6	Identifikasjonsfase + møte med veileder
	15.03.2022	5	Identifikasjonsfase + starte med struktur på recovery
	16.03.2022	6	struktur på recovery og lessons learned
	17.03.2022	6	struktur rammeverk
	18.03.2022	6	preparation fase
	20.03.2022	7	preparation fase
	21.03.2022	6	preparation fase
	22.03.2022	6	preparation fase
	23.03.2022	6	Identifikasjonsfase

	24.03.2022	6	Identifikasjonsfase
	25.03.2022	7	Identifikasjonsfase
	28.03.2022	6	ulike deler av rammeverk
	30.03.2022	6	ulike deler av rammeverk
	31.03.2022	6	ulike deler av rammeverk
	01.04.2022	6	rammeverk
	04.04.2022	8	rapportskriving
	05.04.2022	7	rapportskriving
	06.04.2022	6	rapport og identifikasjon
	07.04.2022	6	fylle inn containment fase + møte med oppdragsgiver
	08.04.2022	6	fylle inn containment, eradication.
	11.04.2022	6	containment fase
	12.04.2022	6	gjøre ferdig identification
	13.04.2022	6	gjøre ferdig identification
	14.04.2022	6	gjøre ferdig identification
	15.04.2022	6	gjøre ferdig identification, containment
	18.04.2022	6	containment fase og eradication
	19.04.2022	6	Eradication of recovery
	20.04.2022	4	rammeverk
	21.04.2022	5	rapport
	22.04.2022	6	Begynne med trening
	25.04.2022	6	Trening
	26.04.2022	6	Trening og eradication
	27.04.2022	6	Recovery og lessons learned
	28.04.2022	6	trening + rapport
	29.04.2022	6	rapport + møte med oppdragsgiver
	02.05.2022	7	rapport
	03.05.2022	8	rapport
	04.05.2022	8	rapport
	05.05.2022	8	start på playbook + rapport
	06.05.2022	7	rapport
	07.05.2022	6	rapport
	08.05.2022	6	rapport
	09.05.2022	8	rapport
	10.05.2022	8	rapport
	11.05.2022	8	rapport
	12.05.2022	8	rapoort
	13.05.2022	8	rapport
	15.05.2022	8	rapport
	16.05.2022	9	rapport
	17.05.2022	10	rapport
	18.05.2022	11	rapport
	19.05.2022	8	rapport
Farhaz	Totalt antall timer:	562	

Navn:	Dato:	Timer:	Hva ble gjort:
Ranvir	06.01.2022	1	Internt møte - avtaler
	12.01.2022	2	internt møte - avtaler/forarbeid + møte med veileder
	16.01.2022	1	Internt møte for møte med oppdragsgiver
	17.01.2022	5	arbeidsøkt + møte med oppdragsgiver

	18.01.2022	5	arbeidsøkt (prosjektplanlegging)
	19.01.2022	5	arbeidsøkt (gannt + prosjektplanlegging)
	20.01.2022	5	Inspirasjonsarbeid (lesing av bacheloroppgaver)
	21.01.2022	2	Overføring av prosjektplan til Overleaf og omskriving til LaTeX
	24.01.2022	5	Skriving av forprosjekt til overleaf + planlegging av møte
	25.01.2022	6	Møte med oppdragsgiver + skriving av prosjektplan
	26.01.2022	6	Arbeidsøkt + møte med veileder
	27.01.2022	7	Selvarbeid (literature review) + finpuss av rapporten
	28.01.2022	6	Selvarbeid (literature review)
	31.01.2022	6	Selvarbeid / gruppe organisering
	01.02.2022	8	notater og selvarbeid/lesing
	02.02.2022	5	Selvarbeid/planlegging av møte
	03.02.2022	4	Møte med oppdragsgiver + selvlesing
	07.02.2022	6	Literature review
	08.02.2022	6	Selvarbeid, finne kilder
	09.02.2022	6	Kartlegging av rammeverk
	10.02.2022	5	Kartlegging av rammeverk
	11.02.2022	1	Oppsummering av rammeverkanalyse
	14.02.2022	4	Fysisk møte med oppdragsgiver + planlegging av kommende uke
	15.02.2022	2	Start av kartlegging av applikasjoner
	17.02.2022	3	Fortsetting av kartlegging av applikasjoner
	18.02.2022	6	Fortsetting av kartlegging av applikasjoner
	21.02.2022	6	Arbeid med klassifisering av systemer
	22.02.2022	3	Arbeid med klassifisering av systemer
	23.02.2022	6	Arbeid med klassifisering av systemer
	24.02.2022	6	Arbeid med klassifisering av hendelser
	25.02.2022	6	Arbeidet med policies
	28.02.2022	6	Arbeid med policies
	01.03.2022	6	Møte med oppdragsgiver + veileder
	02.03.2022	2	Fortsettelse med omskriving av policies til tekst
	03.03.2022	3	Fortsettelse med omskriving av policies til tekst
	04.03.2022	6	Skriving av hendelser
	07.03.2022	6	Skriving av hendelser
	08.03.2022	6	Skriving av hendelser
	09.03.2022	6	Vurdering av hendelser
	10.03.2022	6	Skriving av hendelser
	11.03.2022	6	Skriving av hendelser
	14.03.2022	6	Rammeverk
	15.03.2022	6	Rammeverk
	16.03.2022	6	Rammeverk
	17.03.2022	6	Rammeverk
	18.03.2022	6	Rammeverk
	21.03.2022	6	Rammeverk
	22.03.2022	6	Rammeverk
	23.03.2022	7	Rammeverk
	24.03.2022	6	Rammeverk
	25.03.2022	6	Rammeverk
	26.03.2022	2	Rammeverk
	27.03.2022	1,5	Rammeverk
	28.03.2022	6	Rammeverk
	29.03.2022	6	Rammeverk
	30.03.2022	6	Rammeverk

	31.03.2022	6	Rammeverk
	01.04.2022	6	Rammeverk
	02.04.2022	2	Rammeverk
	03.04.2022	2	Rammeverk
	04.04.2022	6	Rammeverk
	05.04.2022	6	Rammeverk
	06.04.2022	6	Rammeverk
	07.04.2022	6	Rammeverk
	08.04.2022	6	Rapport
	09.04.2022	1	Rapport
	10.04.2022	3	Rapport
	11.04.2022	6	Rapport
	12.04.2022	6	Rapport
	13.04.2022	6,5	Rapport
	14.04.2022	8	Rapport
	15.04.2022	6,5	Rapport
	18.04.2022	7	Rapport
	19.04.2022	6	Rapport
	20.04.2022	7	Rapport
	21.04.2022	8	Rapport
	22.04.2022	6	Rapport
	25.04.2022	0	Grunnet sykdom
	26.04.2022	0	Sykdom
	27.04.2022	0	Sykdom
	28.04.2022	6	Rapport
	29.04.2022	6	Rapport
	30.04.2022	1	Rapport
	01.05.2022	2	Rapport
	02.05.2022	6	Rapport
	03.05.2022	6	Rapport
	04.05.2022	7,5	Rapport
	05.05.2022	8	Rapport
	06.05.2022	7	Rapport
	07.05.2022	2	Rapport
	08.05.2022	3	Rapport
	09.05.2022	9	Rapport
	10.05.2022	10	Rapport
	11.05.2022	10	Rapport
	12.05.2022	8	Rapport
	13.05.2022	10	Rapport
	14.05.2022	5	Rapport
	15.05.2022	4	Rapport
	16.05.2022	8	Rapport
	17.05.2022	3	Rapport
	18.05.2022	11	Rapport
	19.05.2022	12	Rapport
Ranvir	Totalt antall timer:	542	

Navn:	Dato:	Timer:	Hva ble gjort:
Espen	06.01.2022	1	Internt møte - avtaler

	12.01.2022	2	Internt møte - avtaler/forarbeid + møte med veileder
	16.01.2022	1	Internt møte - planlegging av uke
	17.01.2022	1	Intern arbeidsøkt, eksternmøte
	18.01.2022	4	Intern arbeidsøkt
	19.01.2022	4	Intern arbeidsøkt
	20.01.2022	5	Intern arbeidsøkt
	25.01.2022	6	Intern arbeidsøkt
	26.01.2022	6	Intern arbeidsøkt
	27.01.2022	6	Intern arbeidsøkt
	31.01.2022	6	Literature review
	01.02.2022	6	Literature review
	02.02.2022	6	Literature review
	03.02.2022	6	Literature review
	07.02.2022	6	Literature review, møte med veileder
	08.02.2022	6	Literature review
	09.02.2022	6	Rammeverksanalyse, honeypots
	10.02.2022	6	Rammeverksanalyse
	14.02.2022	4	Fysisk møte med oppdragsgiver
	15.02.2022	2	Rammeverksanalyse
	17.02.2022	3	Rammeverksanalyse
	18.02.2022	6	Rammeverksanalyse
	21.02.2022	6	Påbegynt første fase av rammeverk
	22.02.2022	3	Arbeidet med policy
	23.02.2022	6	Arbeidet med policy
	25.02.2022	6	Arbeidet med policy
	28.02.2022	6	Arbeidet med policy
	01.03.2022	6	Kommunikasjonsplan
	02.03.2022	2	Kommunikasjonsplan
	03.03.2022	3	Team
	04.03.2022	6	Team
	05.03.2022	5	Sett på phishing
	06.03.2022	4	Sett på phishing
	07.03.2022	6	Påbegynt identikasjonsfase
	08.03.2022	6	Identifikasjonsfase
	09.03.2022	6	Identifikasjonsfase
	10.03.2022	6	Identifikasjonsfase. Laget struktur
	11.03.2022	6	Rapportskriving, identifikasjonsfase.
	14.03.2022	6	Gjennomgang og opprydding av interne dokumenter
	15.03.2022	6	Identifikasjonsfase, recovery
	16.03.2022	6	Identifikasjonsfase, recovery
	17.03.2022	6	Recovery, lessons learned
	18.03.2022	6	Påbegynt ferdigstille seksjoner i Preparation
	21.03.2022	6	Påbegynt ferdigstille seksjoner i Preparation
	22.03.2022	6	Påbegynt ferdigstille seksjoner i Preparation
	23.03.2022	4	QA av Preparation
	24.03.2022	6	QA av Preparation
	28.03.2022	6	QA av Preparation
	29.03.2022	6	QA av Preparation
	30.03.2022	6	Ulike deler av rammeverk
	31.03.2022	6	Ulike deler av rammeverk
	01.04.2022	6	Rammeverk
	04.04.2022	6	Rapportskriving

	05.04.2022	6	Rapportskriving
	06.04.2022	6	Rapport og identifikasjon
	07.04.2022	6	Containment, møte med oppdragsgiver
	08.04.2022	6	Containment, eradication
	11.04.2022	6	Containment
	12.04.2022	6	Identification
	13.04.2022	6	Identification
	14.04.2022	6	Identification
	15.04.2022	6	Identification, containment
	17.04.2022	8	Rammeverk
	18.04.2022	6	Containment, eradication
	19.04.2022	6	Eradication, recovery
	20.04.2022	4	Rammeverk
	21.04.2022	4	Rapportskriving
	22.04.2022	6	Trening
	23.04.2022	7	Rapportskriving
	24.04.2022	9	Rapportskriving
	25.04.2022	6	Trening
	26.04.2022	6	Trening, eradication
	27.04.2022	6	Recovery, lessons learned
	28.04.2022	6	Trening, rapport
	29.04.2022	6	Rapportskriving, møte med oppdragsgiver
	30.04.2022	9	Rapportskriving
	01.05.2022	10	Rapportskriving
	02.05.2022	7	Rapportskriving
	03.05.2022	7	Rapportskriving
	04.05.2022	8	Rapportskriving
	05.05.2022	8	Playbook, rapportskriving
	06.05.2022	7	Rapportskriving
	07.05.2022	6	Rapportskriving
	08.05.2022	6	Rapportskriving
	09.05.2022	8	Rapportskriving
	10.05.2022	8	Rapportskriving
	11.05.2022	8	Rapportskriving
	12.05.2022	8	Rapportskriving
	13.05.2022	8	Rapportskriving
	14.05.2022	10	Rapportskriving
	15.05.2022	7	Rapportskriving
	16.05.2022	8	Rapportskriving
	17.05.2022	10	Rapportskriving
	18.05.2022	11	Rapportskriving
	19.05.2022	8	Rapportskriving
Espen	Totalt antall timer:	566	

Navn:	Dato:	Timer:	Hva ble gjort:
Jan	12.01.2022	2	Internt møte - avtaler/forarbeid + møte med veileder
	16.01.2022	1	Internt møte - planlegging av arbeid forover
	17.01.2022	5	Internt møte + eksterntmøte - arbeidsøkt
	19.01.2022	5	Internt møte - prosjektplan ++
	20.01.2022	5	Internt møte - lesing av tidligere bacheloroppgaver

	21.01.2022	2	Selvarbeid - Læring av LaTeX
	24.01.2022	5	Omskriving av prosjektplan til LaTeX
	26.01.2022	6	Arbeidsøkt + møte med veileder
	27.01.2022	5	Literature review + finpuss av prosjektplan
	28.01.2022	2	Literature review
	31.01.2022	6	Gruppe organisering + lesing om DataEquipment, Atea, Evry
	02.02.2022	6	IR-rammeverk research
	03.02.2022	4	Internt møte og eksternt møte
	04.02.2022	3	Selvarbeid - IR rammeverk/plan + literature review
	07.02.2022	6	Literature review + møte med veileder
	09.02.2022	6	Rammeverksanalyse
	10.02.2022	3	Rammeverksanalyse
	14.02.2022	6	Fysisk møte hos Moelven
	17.02.2022	3	Rammeverksanalyse
	21.02.2022	6	Start på rammeverk
	23.02.2022	6	Ekstern møte + policy
	24.02.2022	6	Policyarbeid
	25.02.2022	6	Organisering av informasjon + policy
	28.02.2022	6	Arbeid med policies
	01.03.2022	6	Møter med veileder og arbeidsgiver
	02.03.2022	2	Policyarbeid
	03.03.2022	3	Definering av hendelser + lesing av hendelser
	04.03.2022	6	Lesing og skriving om phishing og ransomware
	07.03.2022	6	Mer lesing om phishing og ransomware
	08.03.2022	6	Skriving om hendelser
	09.03.2022	6	Skriving om hendelser og klassifisering
	10.03.2022	6	Start på containment
	11.03.2022	6	Containment
	14.03.2022	6	Containment
	15.03.2022	6	Containment + eradication
	16.03.2022	6	Containment
	17.03.2022	6	Eradication
	18.03.2022	6	Eradication + finskriving av preparation
	21.03.2022	6	Finskriving av preparation
	22.03.2022	6	Finskriving av preparation
	23.03.2022	6	Finskriving av preparation
	24.03.2022	6	Påbegynt skriving av identification
	25.03.2022	6	Research på identifcation
	28.03.2022	6	Research og skriving på identification
	29.03.2022	6	Skriving på identification
	30.03.2022	6	Finskriving av preparation
	31.03.2022	6	Finskriving av preparation
	01.04.2022	6	Rammeverkskriving
	04.04.2022	6	Rammeverkskriving + rapportskriving
	05.04.2022	6	Rapportskriving
	06.04.2022	6	Rapportskriving
	07.04.2022	6	Rammeverkskriving + statusmøte
	08.04.2022	6	Containment + eradication
	11.04.2022	6	Containment + eradication
	12.04.2022	6	Containment + eradication
	13.04.2022	6	Eradication
	14.04.2022	6	Eradication

	15.04.2022	6	Eradication
	17.04.2022	6	Eradication
	18.04.2022	6	Rapportskriving
	20.04.2022	8	Rapportskriving
	21.04.2022	6	Rapportskriving
	22.04.2022	6	Rapportskriving
	23.04.2022	6	Rapportskriving
	24.04.2022	6	Rapportskriving
	25.04.2022	6	Rapportskriving
	26.04.2022	8	Rapportskriving
	27.04.2022	8	Rapportskriving
	28.04.2022	8	Rapportskriving
	29.04.2022	8	Rapportskriving
	30.04.2022	6	Rapportskriving
	01.05.2022	6	Rapportskriving
	02.05.2022	8	Rapportskriving
	03.05.2022	7	Rapportskriving
	04.05.2022	8	Rapportskriving
	05.05.2022	8	Rapportskriving
	06.05.2022	8	Rapportskriving
	07.05.2022	6	Rapportskriving
	08.05.2022	6	Rapportskriving
	09.05.2022	8	Rapportskriving
	10.05.2022	8	Rapportskriving
	11.05.2022	8	Rapportskriving
	12.05.2022	8	Rapportskriving
	13.05.2022	9	Rapportskriving
	14.05.2022	6	Rapportskriving
	15.05.2022	6	Rapportskriving
	16.05.2022	9	Rapportskriving
	17.05.2022	11	Rapportskriving
	18.05.2022	11	Rapportskriving + møte med oppdragsgiver og veileder
	19.05.2022	10	Rapportskriving
Jan	Totalt antall timer:	547	

F Vedlegg: Tilbakemelding fra oppdragsgiver

Evaluering bachelor oppgave IT Sikkerhet NTNU

Forord

Moelven fikk forespørsel om å lage en bachelor oppgave innenfor IT sikkerhet til NTNU Gjøvik. Siden Moelven nettopp hadde økt fokus på dette området tenkte vi at vi kunne utforme en oppgave som går på incident response rammeverk samt incident response training. Dette ville kunne hjelpe oss å bli bedre på dette området samtidig som vi fokuserte på modenhetsanalyse og retningslinjer å jobbe etter. Dette førte til en ganske åpen oppgave som studentene i stor grad kunne være med å utforme. Vi ble veldig glad for interessen rundt vår oppgave på Campus samt alle gode spørsmål.

Oppstart

Vi får en gruppe studenter som viser stor interesse for faget og som kommuniserer godt med oss som oppdragsgiver. Vi føler litt på hvordan oppgaven skal scopes for å holde oppgaven innenfor tidsrammen samt treffe godt på et rammeverk vi kan bygge videre på. Gruppen stiller gode spørsmål og samler masse informasjon som gir oppgaven en god start.

Mellomfase

I denne fasen så jobber gruppen veldig selvstendig og former oppgaven i stor grad på egenhånd. Vi syntes vurderingene til gruppen er fornuftige og blander oss lite inn i oppgaven utenom det å svare opp spørsmål gruppen har. Vi forsøker å holde fornuftige arbeidsmøter for å forsikre oss om at gruppen ikke må vente på oss for svar.

Sluttfase

Vi innser at scopet kanskje er litt stort i forhold til tiden oppgaven er berammet til. Gruppen tar kloke valg for nytt scope som gjør at Moelven er i stand til å benytte rammeverk og treningsplan i videre arbeid. Dette treffer meget godt innenfor vårt ønske for oppgaven.

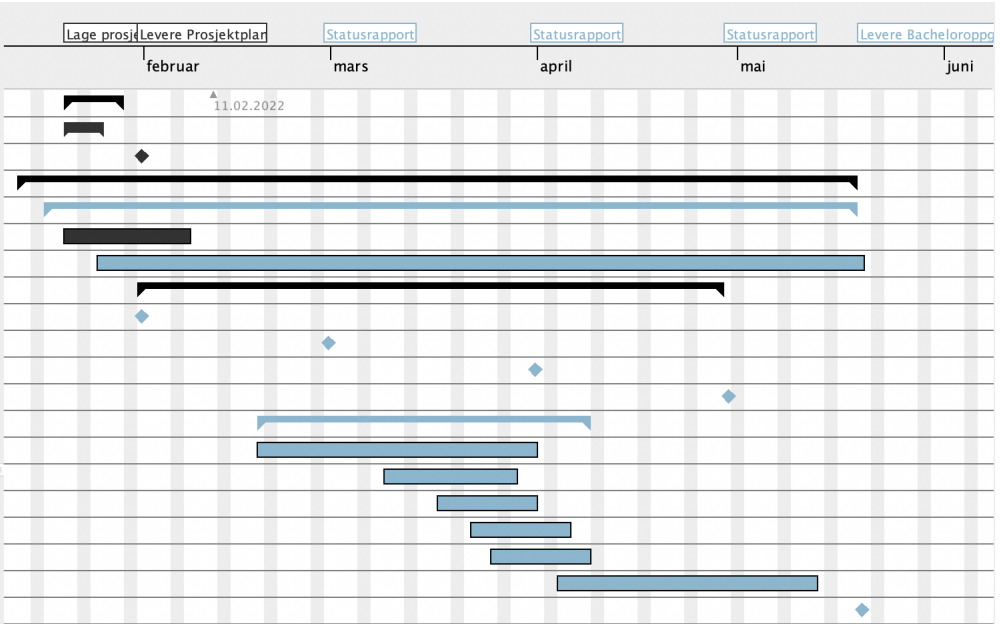
Konklusjon

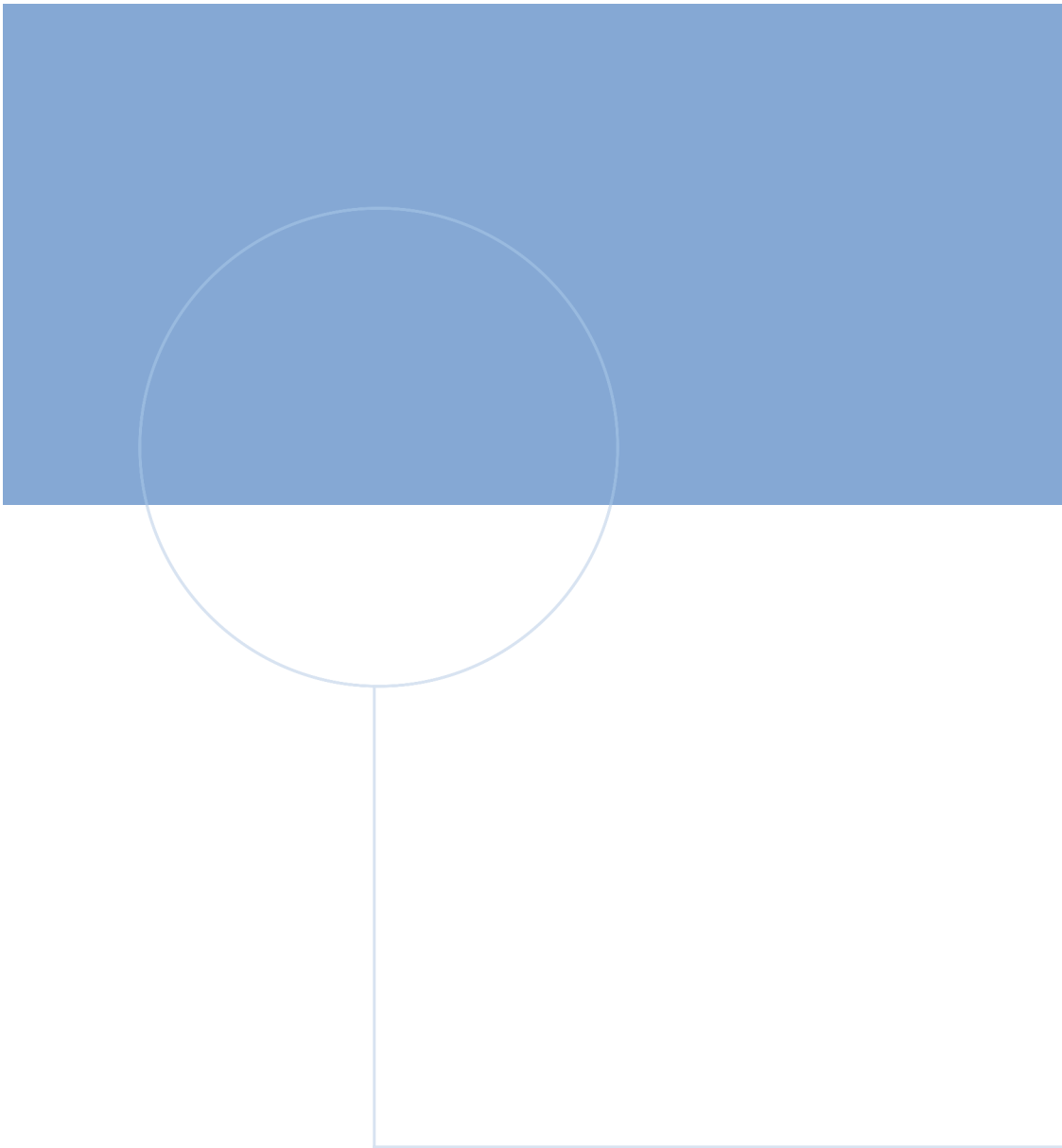
Personlig synes jeg det var veldig spennende å få være med å utforme en slik oppgave samt bistå studentene underveis. Jeg er glad for at NTNU lot oppgaven være såpass åpen da vi ikke hadde kommet særlig langt på området selv da oppgaven skulle utformes. Jeg er veldig glad for interessen studentene viste for oppgaven og veldig imponert over gruppen som fikk tildelt vår oppgave. De jobbet veldig selvstendig under tiden. De viste interesse for faget samt god forståelse. Jeg syntes også vurderingene og endring av scope underveis er fornuftige og riktige.

Tom Kjølhamar

G Vedlegg: Gantt-skjema forstørret

Navn	Startdato	Sluttdato
Prosjektplan	20.01.2022	28.01.2022
Lage prosjektplan	20.01.2022	25.01.2022
Levere Prosjektplan	31.01.2022	31.01.2022
Møter med veileder	13.01.2022	18.05.2022
Møter med Moelven	17.01.2022	18.05.2022
Lære LateX	20.01.2022	07.02.2022
Rapportskriving	25.01.2022	19.05.2022
Statusrapporter	31.01.2022	28.04.2022
Statusrapport	31.01.2022	31.01.2022
Statusrapport	28.02.2022	28.02.2022
Statusrapport	31.03.2022	31.03.2022
Statusrapport	29.04.2022	29.04.2022
Lage rammeverk	18.02.2022	08.04.2022
Preperation fase	18.02.2022	31.03.2022
Identification fase	09.03.2022	28.03.2022
Containment fase	17.03.2022	31.03.2022
Eradication fase	22.03.2022	05.04.2022
Recovery og Lessons learned fase	25.03.2022	08.04.2022
Lage "incident response training" opplegg	04.04.2022	12.05.2022
Levere Bacheloroppgaven	19.05.2022	19.05.2022





NTNU

Kunnskap for en bedre verden