Bacheloroppgave

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

Thea Fritzvold Hatlem
Emma Rønningstad
Anett Voldheim Øverstad

Escaperom - et effektivt læringsverktøy?

Bacheloroppgave i Digital infrastruktur og cybersikkerhet
Veileder: Shao-Fang Wen

Mai 2022

NTNU
Norwegian University of
Science and Technology

Thea Fritzvold Hatlem
Emma Rønningstad
Anett Voldheim Øverstad

Escaperom - et effektivt læringsverktøy?

Bacheloroppgave i Digital infrastruktur og cybersikkerhet
Veileder: Shao-Fang Wen
Mai 2022

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

NTNU
Kunnskap for en bedre verden

Abstract

Title:	Escape room - an effective learning tool?
Date:	20.05.2022
Authors:	Thea Fritzvold Hatlem Emma Rønningstad Anett Voldheim Øverstad
Supervisor:	Shao-Fang Wen, researcher, Department of Information Security and Communication Technology
Employer:	Arnt-Helge Nilsen Øyan, Helsetjenestens driftsorganisasjon for nødnett HF (HDO)
Keywords:	Escape room, training, cyber security, HDO
Pages:	83
Attachments:	8
Availability:	Open

Abstract: “Escape room - an effective learning tool?” deals with the issue of whether it is possible to design an escape room - primarily a physical phenomenon, as an effective virtual learning tool for Helsetjenestens driftsorganisasjon for nødnett HF (HDO). The thesis uses relevant theory about e-learning, serious games and existing frameworks for physical escape rooms in order to create a framework designed specifically for virtual escape rooms and HDO. In addition to this, current threat and risk assessments have been used to ensure that the content of the escape rooms is relevant to the cyber security threats facing HDO today. The results suggests that escape rooms can be an effective learning tool, in addition to being something fun. But it is difficult to come to a final conclusion in regards to it being an effective learning tool, without more extensive testing.

Sammendrag

Tittel:	Escaperom - et effektivt læringsverktøy?
Dato:	20.05.2022
Deltakere:	Thea Fritzvold Hatlem Emma Rønningstad. Anett Voldheim Øverstad
Veileder:	Shao-Fang Wen, forsker, Institutt for informasjonssikkerhet. og kommunikasjonsteknologi
Oppdragsgiver:	Arnt-Helge Nilsen Øyan, Helsetjenestens driftsorganisasjon for nødnett HF (HDO)
Nøkkelord:	Escaperom, opplæring, cybersikkerhet, HDO
Antall sider:	83
Antall vedlegg:	8
Tilgjengelighet:	Åpen

Sammendrag: “Escaperom - et effektivt læringsverktøy?” handler om hvorvidt det er mulig å utforme escaperom - et hovedsaklig fysisk fenomen, til å bli et effektiv virtuelt læringsverktøy for Helsetjenestens driftsorganisasjon for nødnett HF (HDO). Oppgaven bruker relevant teori om e-læring, seriøse spill og eksisterende rammeverk for fysiske escaperom, for å lage et rammeverk tilpasset både virtuelle escaperom og HDO. I tillegg er det blitt benyttet dagsaktuelle risiko- og trusselvurderinger, for å sikre at innholdet i escaperommene er relevant for de cybersikkerhetstruslene HDO står ovenfor i dag. Resultatene tyder på at escaperom kan være et effektivt læringsverktøy og at det i tillegg er noe som blir oppfattet som gøy. Men det er vanskelig å konkludere med at det faktisk er effektivt læringsverktøy uten mer omfattende testing.

Forord

I januar 2021 ble Østre Toten kommune utsatt for et løsepengevirus, hvor rundt 1800 filer ble lekket på det mørke nettet. Stortinget har gjentatte ganger blitt utsatt for dataangrep, hvor det også har blitt hentet ut sensitivt innhold. Flere trussel- og risikovurderinger drar frem at trusler som blant annet løsepengevirus, phishing og nulldagssårbarheter blir mer og mer aktuelle for organisasjoner og privatpersoner i tiden fremover. Risikoen for at angripere skal lykkes med disse angrepene kan minimeres ved at personer og organisasjoner har en god sikkerhetsholdning.

Helsetjenestens driftsorganisasjon for nødnett HF - HDO, mener at et viktig aspekt av sikkerhetsholdningen til en organisasjon er det å utføre regelmessig trening og opplæring. Mennesker lærer best på ulike måter, det er derfor vanskelig å finne en opplæringsmetode eller et læringsverktøy som vil treffe de aller fleste.

"Escaperom - et effektivt læringsverktøy?" tar derfor for seg konseptet virtuelle escaperom som et læringsverktøy. I løpet av prosessen har vi undersøkt hvordan man best kan bygge opp et slikt type escaperom, hva innholdet bør være i henhold til dagens trusselbilde og hvordan man kan lære bort på en effektiv måte, for å så bruke denne informasjonen til å lage escaperom. Til slutt har escaperommene blitt testet for å finne ut om de faktisk fungerer som et læringsverktøy.

Oppgaven har gitt oss mulighet til å bli kjent med escaperom på en måte som tidligere var ukjent for oss. Det har vært interessant og lærerikt, men samtidig utfordrende å finne ut av hvordan man best bruker escaperom for å lære opp personer innenfor forskjellige og dagsaktuelle tema innenfor cybersikkerhet.

Tusen takk til Arnt-Helge Nilsen Øyan og HDO for oppdraget og veiledning.
Tusen takk til vår veileder Shao-Fang Wen for veiledning gjennom arbeidet.
Takk til Erik Hjelmås for gjennomlesning og tilbakemeldinger.
Takk til Grethe Østby for verdifull hjelp og veiledning.

Til slutt - takk til alle ansatte i HDO som har satt av litt tid i en hektisk arbeidshverdag til å svare på spørreundersøkelser og til å teste escaperommene. Vi gleder oss til å dele resultatet av bacheloroppgaven med dere.

Innhold

Figurer

Tabeller

Kapittel 1

Introduksjon

1.1 Bakgrunn og formål

"*Stadig flere nordmenn opplever at de får bedre ferdigheter i digital sikkerhet på nett etter å ha gjennomført opplæring. Samtidig er det slik at hele 68% av nordmenn ikke har fått organisert opplæring i digital sikkerhet i løpet av de siste to årene. Nærmere 3 av 10 nordmenn mener de ikke får tilstrekkelig med informasjon til å vurdere de truslene som finnes på nett. 1 av 10 mener de i liten eller svært liten grad selv er i stand til å vurdere risikoene som møter dem på nettet. Dette er et klart signal at selv om flere får bedre ferdigheter i digital sikkerhet, er det fremdeles en stor gruppe nordmenn som ikke har tilstrekkelige digitale ferdigheter. Spesielt norske arbeidsgivere må ta mer ansvar med å få på plass en god digital sikkerhetskultur – det innebærer blant annet god opplæring*" [1].

Helsetjenestenes driftsorganisasjon for nødnett HF, heretter omtalt som HDO, mener at et viktig aspekt av sikkerhetsholdningen til en organisasjon er som NorSIS peker på [1]: "det å utføre regelmessig trening og opplæring". HDO ønsker i denne forbindelsen å få utarbeidet en eller flere opplæringspakker, basert på konseptet "cyberescaperom" - virtuelle escaperom, på tvers av ansvar og roller i organisasjonen. Virtuelle escaperom er - i likhet med vanlige escaperom, et spill hvor deltagerne må løse gåter, finne hint og gjøre oppgaver for å løse en større sluttoppgave, som i dette tilfelle har bakgrunn i informasjon- og cybersikkerhet [2].

HDO ønsker at disse skal skape bevisstgjøring rundt sikkerhetshendelser, samtidig som det gir ansatte mestringsfølelse og en mulighet til å bygge relasjoner med hverandre. Innholdet i escaperommene vil baseres på møter med ansatte i HDO - blant annet CISO, samt trusselvurderinger slik at innholdet blir relevant for HDO, men også dagsaktuelle i henhold til dagens trusselbilde.

1.2 Problemområde

I januar 2021 ble Østre Toten kommune utsatt for et løsepengevirus, hvor rundt 1800 filer ble lekket på det mørke nettet. Cirka 200 av disse filene inneholdt personsensitive opplysninger [3]. Det tok kommunen over et halvt år før alt av systemer og programmer var tilbake til normalen. Stortinget har gjentatte ganger blitt utsatt for dataangrep, hvor det også har blitt hentet ut sensitivt innhold [4, 5]. Både Østre Toten og Stortinget hadde sårbarheter som kunne vært eliminert ved hjelp av opplæring av de ansatte [4, 6].

"*Dreiningen til angrep mot mennesker fremfor virksomhetens IT-systemer gjør det enda viktigere at den enkelte ansatte har kompetanse om hvordan svindlere jobber og hva de skal være på vakt mot. Det er de som blir angrepsvektoren, ikke systemet*"[1].

Sitatet fra NorSIS (Norsk senter for informasjonssikring) hjelper med å illustrere hvor viktig det er at ansatte har kompetanse innenfor informasjonssikkerhet. Den fortsatt økende digitaliseringen gjør at kompetansen til ansatte må øke tilsvarende. Det er derfor viktig at opplæringen ansatte mottar oppdaterer kunnskapen deres i henhold til dagens trusselbilde og skaper en bevisstgjøring hos de ansatte.

Opplæringen skal gjennomføres ved bruk av opplæringspakker eller virtuelle escaperom. Hvordan opplæringspakkene og/eller escaperommene skal utvikles og hva innholdet skal være er ganske fritt. Siden escaperom er nevnt i oppgaveteksten er dette et naturlig utgangspunkt, og sammen med gruppens veileder ser gruppen et potensiale i opplæring i form av et virtuelt spill. Virtuelle escaperom er en form for e-læring kalt seriøse spill (spill med andre hensikter enn underholdning). Gruppen har i liten grad funnet informasjon om opplæringsescaperom innenfor cybersikkerhet og derfor er dette en spennende utfordring.

Escaperommene vil bli laget digitale da pandemien fortsatt er aktiv i Norge når oppgaven starter, og en erfaring som ble gjort tidligere under pandemien er at det kan være lurt å ikke begrense seg ved å holde ting utelukkende fysisk. Mer om dette under 1.5. Avgrensning.

1.3 Problemstilling

1.3.1 Introduksjon

Som nevnt i 1.1 og 1.2 er målet til oppgaven å utarbeide flere escaperom som skaper en bevisstgjøring rundt sikkerhetshendelser, mens de samtidig gir de ansatte en mestringsfølelse og at de kan ha det litt gøy. Oppgavebeskrivelsen sier følgende: "Det er ingen hemmelighet at personer lærer best på forskjellige måte. For å kunne sikre en god effekt er det behov for å forstå hvordan man kan lære og best mulig effekt av treningen". En viktig del av oppgaven er derfor å kunne måle effekten av læringsobjektet for å se om escaperom kan være et passende læringsverktøy.

1.3.2 Problemstilling

Oppgaven skal derfor ta for seg følgende problemstilling: *Kan virtuelle escaperom være et effektivt virkemiddel for å lære om dagens trusler innen cybersikkerhet?*

Effektivt i denne sammenhengen defineres av Bokmålsordboka. Et effektivt virkemiddel er et virkemiddel "som har god eller tilsiktet virkning", og "som raskt oppnår et godt resultat" [7]. For at escaperom skal være et effektivt virkemiddel må det kunne brukes til å få et læringsutbytte om dagens trusler innen cybersikkerhet, og læringsutbyttet må også raskt kunne oppnås. Hva som menes med *raskt* her er at man bruker relativt kort tid (20-40 min) på å gjennomføre escaperommet.

1.3.3 Hypotese

Gruppens hypoteser er som følger:

Hypotese 1: Escaperom kan være et effektivt virkemiddel for å lære om dagens trusler innen cybersikkerhet.

Hypotese 2: Ansatte føler at de lærer mer om cybersikkerhet ved bruk av escaperom enn ved tradisjonell opplæring.

1.3.4 Forskningsspørsmål

Oppgaven skal forsøke å svare på disse forskningspørsmålene:

- **F1:** Hvordan kan et escaperom utformes for å være et effektivt virkemiddel i opplæring?
- **F2:** Hva er dagens trusler innen cybersikkerhet?

1.4 Prosjektmål

Det overordnende målet for prosjektet er å lage minimum ett escaperom som er tilpasset HDO, og som de kan bruke for å øke de ansattes kunnskaper om cybersikkerhet.

I tillegg til det overordnede målet, har oppgaven også undermål i form av effekt- og resultatmål. Effektmål er de langsiktige målene som ønskes og oppnås basert på sluttproduktet som leveres. Resultatmål er det oppgaven konkret ønsker å levere ved prosjektslutt.

1.4.1 Effektmål

- **E1:** Øke sikkerheten ved å øke kompetansen hos de ansatte i bedriften.
- **E2:** Øke interessen for sikkerhet hos alle ansatte, også hos de som ikke jobber med sikkerhet.
- **E3:** Redusere risikoen for uønskede hendelser relatert til innholdet i escaperommene.

1.4.2 Resultatmål

- **R1:** Lage opplæringsmateriell som er dagsaktuelt og legger til rette for effektiv læring.
- **R2:** Utarbeide 3 opplæringspakker, hvorav én er skreddersydd til HDO sin tjenesteportefølje.
- **R3:** Måle effekten av escaperommene.

1.5 Avgrensning

Oppgaven fokuserer på preventiv opplæring innenfor informasjonssikkerhet ved hjelp av virtuelle escaperom. Målet med opplæringen er å gi de ansatte i HDO innsikt i hva de kan gjøre for å forhindre sikkerhetshendelser. For å identifisere relevante trusler og potensielle sikkerhetshendelser hos HDO vil det være ukentlige møter med gruppens kontaktperson, møter med sikkerhetsledelsen og jevnlig kommunikasjon over e-post.

Det vil også leses relevante trusselvurderinger for å sikre at escaperommene er relevante for dagens trusselbilde. Noen av de ansatte vil i tillegg måtte svare på en pre-test for å finne ut hva slags opplæring og kunnskap de allerede har fått innenfor informasjonssikkerhet, og hva de og HDO gjør for å opprettholde denne kunnskapen. Basert på denne informasjon vil innholdet i escaperommene legges på et nivå som alle vil forstå, og som vil tilrettelegge for samarbeid på tvers av rollene og inngående kunnskap om informasjonssikkerhet i organisasjonen.

Escaperommene vil være satt opp som virtuelle escaperom i Google Forms og ikke som fysiske spill, da det gjør det mulig å gjennomføre dem hvor som helst og når som helst. Google Forms ble valgt over å utvikle rommene ved programmering da gruppen ikke har den spesifikke typen programmeringskunnskap som kreves eller mulighet til å opparbeide dette i løpet av tiden som er til rådighet. Rommene vil måtte jobbes med og utvikles mer senere hvis det er et ønske om å lage det til et tredimensjonalt rom eller et fysisk rom.

Oppgaveteksten ber om minst ett escaperom skreddersydd til HDO og gruppen vil derfor lage to skreddersydde escaperom med temaene nulldagssårbarhet og løsepengevirus. Gåtene og historien i disse escaperommene vil bygge på HDO sin hendelseshåndteringsplan. Denne hendelseshåndteringsplanen er underlagt taushetsplikt og oppbygningen og resultatene fra rommene som bygger på denne kan derfor ikke deles i detalj. Det vil også bli utviklet et tredje escaperom basert på en fiktiv bedrift - dette rommet vil derfor ikke inneholde sensitiv informasjon. Mye av innholdet i kapitlene om metodikk, testing og påfølgende analyse vil være basert på dette escaperommet.

Det må presiseres at rommene kun vil bli testet på et utvalg av de litt over 70 ansatte i HDO, så alle konklusjoner i oppgaven vil være basert på en forholdsvis liten gruppe med personer.

1.6 Målgruppe

Målgruppen for escaperommene er alle ansatte i HDO, uavhengig av stilling og teknisk kompetanse. Dette er både etter oppdragsgiver og gruppens eget ønske – oppdragsgiver ønsker at escaperommene skal få alle opp på et nivå som skaper økt forståelse og tilrettelegger for samarbeid, til tross for ulik kompetanse. Prosjektgruppen anser det som viktig at alle ansatte, uavhengig av organisasjon, har en viss kompetanse innenfor informasjonssikkerhet, slik at man forhindrer uønskede sikkerhetshendelser.

1.7 Prosjektgruppens bakgrunn

Prosjektgruppen går på det tredje og siste året på en bachelor i *Digital infrastruktur og cybersikkerhet* ved Norges-teknisk naturvitenskapelige universitet, campus Gjøvik. I løpet av studiet har gruppen vært gjennom emner og fagområder som: cybersikkerhet og teamarbeid, risikostyring, brukersentrert design, programvareutvikling og hendelseshåndtering. Dette er alle emner og fagområder som er høyst relevante for denne oppgaven, både for å lage gode escaperom med relevant innhold for HDO, men også for å formidle informasjon på en best mulig måte.

1.8 Rammer

1.8.1 Tidsmessige rammer

Bacheloroppgaven skal leveres innen 20. mai 2022.

1.8.2 Språkrammer

Selve rapporten og prosjektplanen blir skrevet på norsk, da det ses som mest naturlig siden oppdragsgiver er et norsk foretak og alle testobjektene er norske.

1.8.3 Andre rammer

Rapporten vil bli skrevet i Overleaf – et nettbasert LaTeX-verktøy. På grunn av den pågående koronapandemien vil møter og intervjuer bli gjennomført både digitalt via Microsoft Teams og fysisk, avhengig av den lokale smittesituasjonen.

1.9 Arbeidsmetode

Prosjektet deles inn i tre hovedfaser der de første to er noe overlappende, mens den tredje og siste skjer etter de to første er ferdig. Prosjektet starter med en utredning hvor det innhentes informasjon som senere skal gjøres om til escaperommenes læringsmateriell og design. Dette fører videre til fase to som omhandler implementasjonen av escaperommene. Disse to fasene kan som nevnt overlappe noe da nye ideer til rommene kan komme fortløpende imens de blir utformet. Tredje og siste fase er testing og evaluering. I denne fasen blir escaperommene sendt ut til HDOs ansatte og svarene vil bli evaluert.

1.10 Rapportstruktur

I kapittel 2 beskrives teorien som har blitt brukt under implementasjonen av escaperommene, læring og testing. Videre beskrives metodikken som har blitt brukt under datainnsamling, testing, og så videre i kapittel 3. Selve testingen av escaperommene, pre-testen og post-testen blir beskrevet i kapittel 4. Analysen av escaperommene og testene beskrives i kapittel 5. I kapittel 6 blir resultatene diskutert og reflektert. I kapittel 7 kommer konklusjonen, der problemstillingen, hypotese og forskningspørsmål blir besvart. Til slutt er det vedlagt flere relevante vedlegg, herunder prosjektavtalen, prosjektplanen og møtereferat.

Kapittel 2

Teori

2.1 Introduksjon

Teorikapitlet består av flere deler, hvorav hver del beskriver relevant teori for oppgaven. Først er det beskrevet flere definisjoner for å sikre en felles forståelse av begrepene som blir brukt. Videre vil det gås inn på relevant teori om e-læring, spillbasert opplæring og seriøse spill, samt aktuelle rammeverk for escaperom for å underbygge utviklingen av escaperommene. For å sikre at innholdet i escaperommene er relevant, er det innhentet flere artikler og rapporter for å identifisere dagens cybersikkerhetstrusler. Til slutt er det innhentet teori om testing av escaperom for å sikre at problemstillingen blir besvart, samt at hypotesene blir bekreftet eller avkreftet.

2.2 Definisjoner

EscapED Rammeverk for fysiske escaperom [8].

SERF Snyder Escape Room Framework, et rammeverk for virtuelle escaperom [9].

Escaperom Et spill der en spiller er låst i et rom og må løse oppgaver for å komme seg ut [2]. Kan også være digitalt.

Spillere Brukerne av escaperommet.

E-læring Læring via teknologiske hjelpemidler [10].

Spillbasert opplæring Bruken av spill, både fysiske og digitale, for å nå læringsmål.

Seriøse spill Spill utviklet med andre hensikter enn underholdning, ofte utdanning [11].

Kinestetisk læring Lære ved å gjøre, oppleve og føle [12].

2.3 E-læring og seriøse spill

E-læring refererer til læring via teknologiske hjelpemidler og blir ofte sett på som mer effektivt enn fysisk læring [10]. En attraktiv side ved e-læring er hvordan en stor gruppe mennesker kan få samme opplæring på tidspunkt som passer hver enkelt, men også hvorhen de vil enten om det er hjemme eller på kontoret. Brukerne får også muligheten til å ta pauser i opplæringen ettersom det passer den enkelte, noe som gjør det mer gjennomførbart for folk med en travel hverdag. I tillegg kan de som overser opplæringen se at alle deltagerne gjennomfører det de skal. Med e-læring kommer det også utfordringer, spesielt knyttet til motivasjon, og det er nettopp motivasjonen og brukerens engasjement som er nødvendig for effektiv e-læring [13].

For å øke motivasjon i e-læring har det blitt sett på å bruke spill til opplæring, og dette kalles spillbasert opplæring. Spillbasert opplæring defineres som bruken av spill, enten allerede-eksisterende eller spesialutviklede, for å nå spesifikke læringsmål. Det blir og sett på som en effektiv metode for å øke motivasjon, samt at det introduserer noe gøy i læringssituasjonen [14]. Spillbasert opplæring er altså en metode for opplæring, og ved å bruke denne metoden kan man for eksempel utvikle seriøse spill. Seriøse spill defineres som spill med andre hensikter enn underholdning [11], for eksempel utdanning. Escaperom med utdannings- og opplæringsformål er dermed et eksempel på et seriøst spill.

E-læring kan vise til mye positive resultater, men Noesgaard og Ørngreen [13] påpeker at "det er merkelig at kun 10% av studiene de har tatt for seg klassifiserer e-læring som *ikke-effektivt*". De stiller derfor spørsmål om hvorvidt resultatene av studiene er gyldige eller om de er påvirket av forskerens egeninteresse, da flere av forskerene tilsynelatende har en andel i e-læring sin suksess. Dette gjør at man ikke kan være sikker på at studiene med positive resultater knyttet til e-læring er gyldige, eller om forskerne har hatt et bias.

Motivasjon blir nevnt som en utfordring for e-læring, og selv om seriøse spill ønsker å løse denne utfordringen, introduserer det også andre problemer. Et seriøst spill kan utformes på mange måter, og selv om det øker spillerens engasjement er det også viktig at læringen har en effekt. En undersøkelse for å sjekke effektiviteten til et seriøst spill kalt "It´s A Deal!" [15] antar at "balansen mellom designet av spillet er nøkkelen til læringseffektiviteten". Et annet problem med seriøse spill er hvordan spillerens fokus blir på spillet og ikke læringen, og at læringsobjektet dermed ikke får ønsket effekt [16]. En annen undersøkelse kartla hvilke elementer i seriøse spill som øker læringseffekt [17], og selv om læringsresultatene av spillopplevelsen var positive, kunne de ikke konkludere med hvilke elementer som var viktigst. Seriøse spill viser positive resultater, men akkurat hva som gjør læringen effektiv kan ikke konkluderes med, og dette kan gjøre utviklingen og kvaliteten av seriøse spill inkonsekvent.

2.4 Escaperom

2.4.1 Teori om escaperom

Escaperom er i følge Nicholson [2] "live-action team-baserte spill der spillerene leter etter hint, løser gåter og fullfører oppgaver i et eller flere rom for å oppnå et mål (ofte å komme seg ut fra rommet) i løpet av en begrenset tidsperiode". Tradisjonelt er escaperom for underholdning i fysiske rom med fysiske rekvisitter, men ettersom escaperom har blitt benyttet til utdanning har virtuelle versjoner blitt utviklet.

Fordelen med escaperom i utdanning er at det er et spill og dermed holder spillerene motiverte og engasjerte slik at de kommer seg gjennom læringsmålene. Ved å løse gåter vil spillerne "lære ved å gjøre", en anerkjent utdanningsteori som hevder at man lærer bedre av å sette seg inn i noe praktisk [18]. En annen fordel er at selv om spill, hovedsakelig dataspill, typisk blir sett på som en interesse for menn, og menn ofte blir mer motiverte av konkurranse enn kvinner [9], viser en undersøkelse fra Nicholson [2] at escaperom blir brukt jevnt av alle kjønn. Dette kan være fordi escaperom kan benytte flere motivasjonselementer som appellerer til alle kjønn. I følge videospilldesigneren Jesse Schell [9] er menn mer motiverte av konkurranse og prøving og feiling, mens kvinner motiveres mer av dialog, verbale gåter, den virkelige verden og følelser. Disse nevnte elementene er naturlige deler av escaperom, og selv om det legges vekt på at motivasjon knyttet til kjønn er meget generaliserende, er det også en positiv indikator som tyder på at utdanningsobjektet vil bli likt av flere, uavhengig av kjønn.

Et annet positivt element ved escaperom er historien den forteller. "I enhver gruppe vil omtrent 40 prosent være visuelle lærere som lærer best fra videoer, diagrammer eller illustrasjoner. 40 prosent til vil være auditive og lære best fra forelesinger og diskusjoner. De resterende 20 prosentene er kinestetiske lærere, som lærer best fra å gjøre, oppleve og føle. Historiefortelling har aspekter som fungerer for alle disse tre typene. Visuelle lærere setter pris på de mentale bildene historien frambringer. Auditive lærere fokuserer på ordene og narratoren sin stemme. Kinestetiske lærere husker de emosjonelle sammenkoblingene og følelsene fra fortellingen" [12]. Et virtuelt escaperom vil ikke nødvendigvis ha en fortellerstemme, men auditive lærere vil få utbytte av diskusjonene som vil oppstå hvis det skal løses av et team. Escaperom vil dermed kunne være et godt læringsvirkemiddel for en større gruppe mennesker hvis det har en god fortelling, da dette naturlig gir rom for auditiv, visuell og kinestetisk læring.

2.4.2 Rammeverk

2.4.2.1 EscapED

EscapED [8] er et prosjekt under Game Change initiativet fra Coventry University. Det er et rammeverk for å lage interaktive escaperom-opplevelser med utdanningsformål og for å utvikle ikke-digitale læringsplatformer. Med dette rammeverket kan man inkludere tema knyttet til læring og læringsformål. EscapED består av de seks hovedkategoriene deltagere, objektiv, tema, gåter, utstyr og evaluering. Under disse er det flere underpunkter.

Figur 2.1: EscapED Framework gjengitt fra Clarke m.fl. [8]

Deltagere
EscapeED-rammeverket starter med en analyse av escaperommets potensielle spillere. For å utføre analysen blir det sett på fem hovedkategorier. Den første er brukertype som inkluderer demografi og spillerenes læringsbehov. Deretter kommer kategorien tid, altså tiden escaperommet bør ta å fullføre. Den tredje er vanskelighetsgrad som bør tilpasses alder og utdanning. Modus, som omhandler hvordan escaperommet skal utføres; skal det være samarbeid? Skal det være konkurransebasert? Den siste kategorien er skala, altså hvor mange brukere spillet skal lages for.

Objektiv
Med objektiver menes hensikten til escaperommet og siden EscapED er for utdanningsformål er dette gjerne myke ferdigheter som kommunikasjon og ledelse, læringsmål, disiplin og problemløsing. Escaperommet bør designes rundt dets formål slik at opplæringen blir en naturlig del av spillet.

Tema
Tema er en stor og viktig del av escaperommet da det er med på å lage en spennende historie. I tradisjonelle escaperom, med underholdningsformål er noen vanlige temaer å flykte fra noe - for eksempel et fengsel eller en ubåt, å hindre noe - ofte noe kriminelt fra å skje eller å løse et mysterium. For en troverdig historie bør escaperommet reflektere historien, for eksempel ved å simulere en ubåt, da dette vil øke engasjement fra spillerne.

I EscapED deles temakategorien i fire deler som det bør tas hensyn til. Først hvordan modus rommet skal ha, enten flyktmodus der målet er å komme seg ut av et låst rom innen en viss tid eller mysteriemodus der målet er å løse et mysterium innen en viss tid. Deretter må man tenke på designet av historien til rommet. Dette er en viktig faktor for å holde spillerne interessert. Utviklerene bør og tenke på om spillet skal være en del av flere spill, eller kun ett alenestående spill.

Gåter
Det som bygger opp escaperommet er oppgavene, altså gåtene. Dette inkluderer design av gåtene, at læringsobjektivene bør reflekteres i oppgavene, instruksjon til brukerne om hvordan ting gjøres og hint til oppgavene da escaperommet ofte kan være utfordrende.

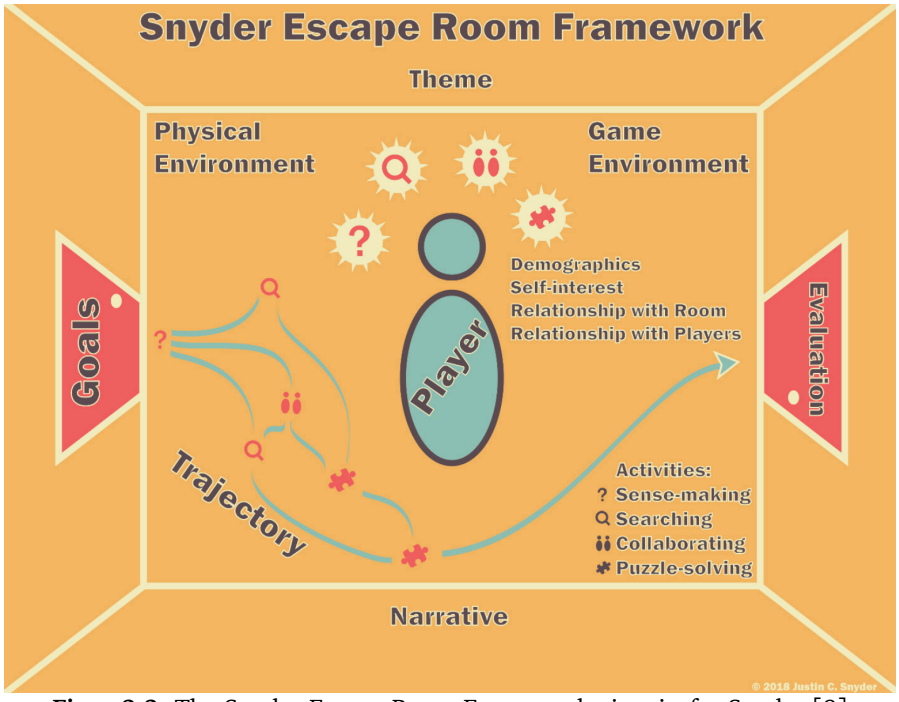
Utstyr
Når man utvikler et escaperom må man tenke på lokasjon og/eller hvis noe utstyr trengs. Denne kategorien inkluderer dermed lokasjon og designet av escaperommet, fysiske rekvisitter, teknologiske rekvisitter og eventuelle skuespillere. Utstyr er viktig og vil være med på å forsterke historien.

Evaluering
Evaluering er et viktig steg for å sjekke om escaperommet har hatt en effekt og om læringsmålene har blitt lært bort til spillerene. Utviklerene må også kunne sjekke om escaperommet møter målene de har satt til rommets kvalitet og effekt.

Denne kategorien inkluderer derfor testing av escaperom i utviklingsperioden, refleksjon fra spillerne for å lære om deres opplevelse av læringen, en formell evaluering av læringsmålene og eventuelle endringer ettersom man får tilbakemeldinger fra spillerne. Et annet viktig poeng er å nullstille escaperommet etter det har blitt brukt eller testes, altså sette ting tilbake slik det originalt var, slik at alle spillerne får likt utgangspunkt og får løst oppgavene selv.

2.4.2.2 The Snyder Escape Room Framework

The Snyder Escape Room Framework (SERF) [9] er et design-orientert rammeverk utviklet av Justin Charles Snyder. Det består av retningslinjer for designprosessen av escaperom med utdanningsformål. Det er basert på elementer fra rammeverkene EscapED og Ask Why [19]. SERF foreslår å strukturere designprosessen i seks kategorier; mål og objektiv, spillere, aktiviteter, kontekst, hendelsesforløp og evaluering.



Figur 2.2: The Snyder Escape Room Framework gjengitt fra Snyder [9]

Mål og objektiv
For å lage et escaperom er det viktig å designe med et konkret mål i fokus. Dette bør settes i startsfasen av prosjektet og vil være viktig når man skal evaluere escaperommet senere. Objektivene er direkte oppgaver som til sammen skal gjøre at escaperommet når målet. Man må tenke på hva spillerne i escaperommet skal lære av opplevelsen når man utformer objektivene eller oppgavene.

Spillere
Spillere omhandler escaperommets brukere. Man må kartlegge hvem som skal bruke escaperommet for å designe noe som er tilpasset dem. Dette inkluderer å undersøke demografi, spillerenes forhold med hverandre, egeninteresser og kunnskap om læringsobjektivet. Hvis spillerene ikke har et forhold med hverandre, eller hvis spillerne ikke har kjennskap med escaperommet bør det være en introduksjon før spillet begynner. Spillerenes egeninteresser kan kartlegges da dette kan brukes for å øke motivasjon, for eksempel ved premier hvis spillerene

har høyt konkurranseinstinkt, eller ved at rommets utforming er tilpasset deres interesser.

Aktiviteter
Aktiviteter er det som utgjør oppgavene i escaperommet og bør være varierte for en unik opplevelse. SERF beskriver fire kjerneoppgaver kalt meningsskaping, leting, samarbeid og gåteløsing. Meningsskaping er å tenke eller å prosessere informasjon for å finne en løsning. Leting er prosessen der spillerne prøver å finne hint i miljøet. Samarbeid er en aktivitet som det kan legges opp til i designet av oppgaven da escaperommet ofte er laget for å bli løst av en gruppe. Gåteløsning kan være en form eller en kombinasjon av de nevnte aktivitetene, men i SERF blir det sett på som en egen aktivitet da dette er essensen av escaperommet. Disse aktivitetene bør inkluderes og kombineres.

Kontekst
Kategorien kontekst fokuserer på at escaperommet skal ha en fortelling og et tema, samt at oppgavene skal ha en sammenheng. Et godt escaperom følger en historie, og escaperommet spillerne er i skal reflektere denne.

Hendelsesforløp
Hendelsesforløpet er hvordan alle oppgavene henger sammen. Man må lage en historie der man kan følge en vei av oppgaver som gir mening og har sammenheng. Det bør være flere mulige veier, og det bør på en naturlig måte være mulig å gå videre en annen vei.

Evaluering
Den siste kategorien er evaluering. Man skal kunne måle escaperommet mot målene og læringsobjektivene man lagde i den første kategorien mål og objektiver. Testing med spilletester vil være en god måte å adressere problemer på slik at escaperommet kan forbedres og møte målene bedre.

I tillegg refererer SERF til et rammeverk kalt "Ask Why" [19], der poenget er å se på elementene i escaperommet og reflektere over hvorfor de er der. Hvis en del av escaperommet ikke møter målene bør det fjernes.

2.4.3 Plattform

Ved utviklingen av et virtuelt escaperom er det flere plattformer og nettsider man kan benytte seg av. Av de forskjellige plattformene er det Mozilla Hubs og Google Forms som har vært mest aktuelle for oppgaven, da begge disse er plattformer som fremstår som lette å navigere i for de ansatte i HDO.

2.4.3.1 Mozilla Hubs

Mozilla Hubs [20] er en virtuell plattform utviklet av Mozilla. I Mozilla Hubs har man mulighet til å lage virtuelle 3D-rom hvor brukeren kan navigere seg rundt i form av en avatar og samhandle med forskjellig objekter. Det er også mulig å linke til andre nettsider, for eksempel Google Slides, når brukeren plukker opp eller tar på ett objekt. Kombinerer man Mozilla Hubs med andre tredjeparter, har man derfor mulighet til å både gi brukeren et faktisk rom å navigere i, samtidig som man kan gi de oppgaver å løse.

2.4.3.2 Google Forms

Google Forms [21] er en programvare fra Google for å lage spørreundersøkelser og skjemaer. Det har også blitt brukt til å lage escaperom. I Google Forms kan man ha spørsmål med svar i form av avmerkingsbokser, flervalg, rullgardingmeny eller tekstsvar. I tillegg kan skjemaene bygges opp av flere deler, slik at man må svare riktig før man kan gå videre til neste del. Dette gir gode muligheter til å utvikle et escaperom da spørsmålene kan være gåter som må løses før man kan gå videre til neste del, akkurat som et fysisk escaperom. For hint til gåtene kan bilder og tekst benyttes.

2.5 Trusselbilde og sikkerhetskultur

2.5.1 Introduksjon

Rapportene nedenfor gir en oversikt over truslene og trusselaktørene Norge står ovenfor i dag. Det er mest fokus på digitale trusler, da dette blir en mer og mer utsatt angrepsflate. Rapportene peker på flere sektorer som er utsatt for digitale angrep, herunder blant annet helsesektoren. I tillegg til å illustrere dagens trusselbilde, viser noen av rapportene også til tidligere sikkerhetshendelser og hvilke holdninger nordmenn har til digital sikkerhet. Denne informasjonen er nyttig for å identifisere potensielt innhold til escaperommene, slik at innholdet blir relevant i henhold til dagens trusler innen cybersikkerhet.

2.5.2 Fokus 2022

Fokus 2022 [22] er Etterretningstjenestens årlige trussel- og risikovurdering. Rapporten fokuserer på stormaktsrivalisering mellom USA og Russland/Kina og trusselbildet mot Norge. Når det gjelder det digitale trusselbildet kommer det frem i rapporten at "en rekke offentlige og private virksomheter har vært gjenstand for nettverksoperasjoner det siste året." Og at "i all hovedsak er det etterretningsaktivitet i form av kartlegging og innhenting som preger trusselbildet mot norske aktører i det digitale rom." Det er også nevnt at helsesektoren er utsatt for angrep, og nulldagsårbarheter og brute-force blir spesielt lagt vekt på av nettverksoperasjoner i rapporten.

2.5.3 Nasjonal trusselvurdering 2022

Nasjonal trusselvurdering 2022 [23] er Politiets sikkerhetstjenestes årlige trussel- og risikovurdering. Den er delt opp i tre deler; statlig etterretningsvirksomhet, politisk motivert vold - ekstremisme og trusselen mot myndighetspersoner. Det nevnes at antall nettverksoperasjoner og alvorlige cyberhendelser øker mot virksomheter i Norge, blant annet vil selskaper innen helse være utsatt.

2.5.4 Mørketallsundersøkelsen 2020

Mørketallsundersøkelsen 2020 [24] er en rapport fra Næringslivets sikkerhetsråd. Rapporten ser på den digitale sikkerhetstilstanden - herunder årsak til sikkerhetsbrudd, konsekvenser og rapportering av sikkerhetshendelser og forebyggende tiltak som er gjort med mer, både i det private og offentlige næringsliv. Rapporten viser blant annet til at 39% av bedriftene mener at manglende sikkerhetsbevissthet hos ansatte er årsaken til sikkerhetsbrudd, og at de vanligste hendelsene bedriftene er utsatt for er forsøk på hacking, phishing og virus. I tillegg nevner rapporten at 77% av bedriftene har gjennomført aktiviteter som har som mål å øke ansattes sikkerhetsbevissthet - hvorav 39% har oppgitt at de bruker en form for e-læring, men det er ikke spesifisert hva slag type e-læring de har brukt.

2.5.5 Nordmenn og digital sikkerhetskultur 2021

Nordmenn og digital sikkerhetskultur 2021 [1] er NorSIS sin årlige rapport om status på den digitale sikkerhetskulturen i den norske befolkningen. Rapporten nevner at det er tegn til både en økt bevissthet og en forbedring rundt temaet digital sikkerhet. Samtidig nevnes det at 3 av 4 nordmenn ikke har fått organisert opplæring i digital sikkerhet i løpet av de siste to årene, og 28% "mener de ikke får tilstrekkelig med informasjon til å vurdere de truslene som finnes på nett".

2.5.6 Risiko 2022

Risiko 2022 [25] er Nasjonal sikkerhetsmyndighets årlige trussel- og risikovurdering. Denne rapporten fokuserer på risikobildet i det norske samfunnet og for norske virksomheter. Cyberdomenet er godt beskrevet i rapporten og NSM ser økende trusselaktivitet på nett og det nevnes også at "trusselaktørene viser stor kapasitet til å gjennomføre cyberangrep." Mange ulike angrepsmetoder blir vist til i rapporten, blant annet phishing og digital utpressing og sabotasje (løsepengevirus) som trusselaktørene bruker for å "få tilgang til systemer og sensitiv informasjon" slik at "de kan endre innhold eller gjøre tjenester utilgjengelige". Det legges også vekt på at ledelsen i virksomheter bør ha "en årlig gjennomgang av de nasjonale trussel- og risikovurderingene".

2.5.7 Trusler og trender 2021

Trusler og trender 2021 [26] er en årlig rapport fra NorSIS som fokuserer på å skissere de viktigste truslene små og mellomstore bedrifter kan bli utsatt for, og tiltakene bedrifter kan ta for å minimere risiko. Rapporten går inn på trusler som løsepengevirus, kontokapring, verdikjedeangrep og svindel, enten i form av phishing, fakturasvindel og/eller falske nettsider med mer. Det dras fram i rapporten at løsepengevirus er "Europas største digitale trussel mot virksomheter i alle størrelser".

2.6 Teori om testing

For å kunne validere om problemstillinger og hypoteser stemmer eller ikke, er det nødvendig å få testet en behandling på en relevant testgruppe. Det finnes mange måter å teste en persons kunnskap på, men i følge Leedy og Ormrod [27] er et eksperimentelt design den beste måten å finne årsakssammenhenger på. Et eksperimentelt design er en måte å utføre testing hvor man systematisk manipulerer situasjonen man undersøker, for eksempel et læringsobjekt.

Det finnes flere måter å implementere et slikt design på, men hovedsakelig kan det deles inn i tre hovedtyper: pre-eksperimentelle design, kvasi-eksperimentelle design og ekte eksperimentelle design. Designene blir fremstilt slik de gjør hos Leedy og Ormrod; i tabeller med grupper nedover i første kolonne, og aktiviteter i riktig rekkefølge tidsmessig bortover hver rad for hver gruppe. Aktivitetene er enten en behandling (treatment) forkortet til Tx eller en observasjon forkortet til Obs i tabellene. Det er også mulig å ikke ha en aktivitet i en periode og det indikeres ved en "-".

2.6.1 Pre-eksperimentelle design

2.6.1.1 Design 1

Design 1 er det enkleste designet der en behandling blir introdusert til en gruppe og deretter blir gruppens resultater av behandlingen observert igjennom for eksempel en test:

Gruppe 1	Tx	Obs

Tabell 2.1: Design 1

Design 1 gir ingen klar årsak-sammenheng. Siden det kun blir gjort en observasjon etter behandlingen er det ingen klar måte å bekrefte at det faktisk har skjedd en endring i situasjonen til gruppen gjennom behandlingen.

2.6.1.2 Design 2

I design 2 legges en observasjon til før behandlingen, slik at situasjonen kan sammenlignes før og etter, slik at det kan verifiseres om en endring har skjedd eller ikke. Det er fortsatt ikke mulig å være sikker på om det er behandlingen som er årsaken til endringen eller om det kan være andre grunner.

Gruppe 1	Obs	Tx	Obs

Tabell 2.2: Design 2

2.6.1.3 Design 3

Her introduseres en kontrollgruppe (gruppe 2) som bør være like stor som test-gruppen for et godt sammenligningsgrunnlag. Kontrollgruppen får ikke behandlingen som gruppe 1 får. Gruppe 1 og gruppe 2 sine resultater kan nå sammenlignes etter behandlingen. Likevel er det ikke lagt til rette for å sammenligne gruppene før behandlingen, og derfor er det heller ikke mulig å garantere at gruppene er tilsvarende hverandre. Tilsvarende vil her si at gruppene er likeverdige, gjerne med tanke på alder, kjønn, yrke og lignende.

Gruppe 1	Tx	Obs
Gruppe 2	-	Obs

Tabell 2.3: Design 3

2.6.2 Ekte eksperimentelle design

I enhver eksperimentell studie blir det stilt spørsmål ved den interne gyldigheten. Intern gyldighet betyr i den grad designet og dataene i studiet lar forskeren trekke legitime konklusjoner om årsak-virknings effekten og andre forhold i studiet [27]. Uten intern gyldighet kan ikke slike konklusjoner trekkes, og den interne gyldigheten er dermed helt essensiell. For å maksimere den interne gyldigheten er man nødt til å kontrollere forvirrende variabler som kan tolkes som mulige årsaker. Det er flere ulike måter å gjøre dette på; i design 2 er det med en pre-test for å vurdere ekvivalens før behandlingen og i design 3 ble en kontrollgruppe introdusert. I ekte eksperimentelle design blir også folk tilfeldig tilordnet til gruppene, slik at de ses på som tilsvarende.

2.6.2.1 Design 4

I design 4 blir begge gruppene tilfeldig valgt ut og test-gruppen (gruppe 1) går igjennom to observasjoner og en behandling, mens kontrollgruppen bare går igjennom observasjonene.

Tilfeldig tildelt	Gruppe 1	Obs	Tx	Obs
Tilfeldig tildelt	Gruppe 2	Obs	-	Obs

Tabell 2.4: Design 4

Dette designet gir en god mulighet til å kunne finne en årsak-sammenheng siden det kan verifiseres om det skjer en endring etter behandlingen ved bruk av to observasjoner. I tillegg er også andre årsaker til endringen eliminert ved å inkludere kontrollgruppe og tilfeldig valgte grupper.

2.6.2.2 Design 5

For å kunne fastslå at ikke pre-testen (den første observasjonen) kan påvirke hvordan gruppene gjennomfører behandlingen, kan design 4 utvikles til design 5:

Tilfeldig tildelt	Gruppe 1	Obs	Tx	Obs
Tilfeldig tildelt	Gruppe 2	Obs	-	Obs
Tilfeldig tildelt	Gruppe 3	-	Tx	Obs
Tilfeldig tildelt	Gruppe 4	-	-	Obs

Tabell 2.5: Design 5

Design 5 består av fire tilsvarende grupper som går igjennom ulike aktiviteter. Gruppe 1 går igjennom to observasjoner, en før og en etter de får behandlingen. Gruppe 2 går også igjennom to observasjoner, men ingen behandling. Gruppe 3 tar behandling og observasjon etter, mens gruppe 4 kun tar den siste observasjonen. Dette gjør at man får kontrollert for forvirrende variabler ved å ha to kontrollgrupper, gruppe 2 til gruppe 1 som tar pre-test og gruppe 4 til gruppe 3 som ikke tar pre-test. Hvis gruppe 3 og 4 avviker i samme grad som gruppe 1 og 2 gjør, kan man si at pre-testen ikke har effekt på læringsutbyttet.

2.6.2.3 Design 6 og 7

Design 6 og 7 er også ekte eksperimentelle design. Design 6 er brukt der en pre-test ikke er mulig å gjennomføre, og dette designet kan derfor ses på som bare de to siste gruppene av design 5. I design 7 gjennomgår en gruppe to ulike behandlinger på samme tid og også to ulike observasjoner på samme tid.

Gruppe 1	Tx-a	Obs-a
Gruppe 1	Tx-b	Obs-b

Tabell 2.6: Design 7

2.6.3 Kvasi-eksperimentelle design

Kvasi-eksperimentelle design brukes i situasjoner der det å velge ut tilfeldige grupper enten er umulig eller upraktisk.

2.6.3.1 Design 8

Dette designet er en blanding av design 3 og 4. Designet består av to grupper som har to observasjoner hver, men kun gruppe 1 har behandlingen. Gruppene er ikke tilfeldig valgt ut da dette da enten er umulig eller upraktisk, og det er derfor ikke mulig å garantere at gruppene er likeverdige.

Gruppe 1	Obs	Tx	Obs
Gruppe 2	Obs	-	Obs

Tabell 2.7: Design 8

2.6.3.2 Design 9-13

Disse designene inneholder flere observasjoner enn to per gruppe i testingen, gjerne mellom 4 og 8. I løpet av at prosjekttiden er det ikke tid til å gjennomføre dette, og designene er derfor ikke forklart nærmere.

Kapittel 3

Metode

3.1 Introduksjon

Metodekapitlet består av flere deler, hvorav hver del beskriver prosessene og valgene gjort i løpet av oppgaven. Først er det beskrevet hvilke metoder som er valgt for datainnsamling. Videre utdypes det hvilke metoder som er valgt for å teste rommene og hvilken kunnskap testobjektene forhåpentligvis opparbeider seg etter å ha testet et escaperom. Til slutt går teksten igjennom hvordan hvert enkelt escaperom er bygget opp - herunder hvilken plattform som er brukt, hvilke tema de enkelte rommene omhandler, basert på aktuelle artikler og rapporter, samt HDO sitt opplæringsbehov og metoder brukt i oppbygging av rommene.

3.2 Datainnsamling

For å kunne avgjøre datainnsamlingsmetode er det viktig å identifisere hva slags type data som er nødvendig for å kunne bekrefte og/eller avkrefte hypotesene definert i kapittel 1.3 Problemstilling, samt for å svare på selve problemstillingen: "kan virtuelle escaperom være et effektivt virkemiddel for å lære om dagens trusler innen cybersikkerhet?". Problemstillingen og hypotesene legger til rette for bruk av tallfestet data da disse er ja eller nei spørsmål. Samtidig er det også nødvendig å gå ned på detaljnivå for å identifisere hvilke områder som det er viktig at HDO får opplæring innenfor når det gjelder dagsaktuelle trusler og risikoer.

For å samle inn dataene som kan tallfestes, er det naturlig å først vurdere en kvantitativ metode. En kvantitativ metode brukes i de tilfellene der man ønsker å samle inn data som enkelt kan tallfestes, for eksempel alder. Siden oppgaven har et behov for å gå i dybden, kan ikke kun en kvantitiv innsamlingsmetode benyttes. Det blir derfor benyttet en blanding av kvantitativ og kvalitativ metode. En kvalitativ metode legger opp til man kan gå i dybden på et smalt felt, i dette tilfelle opplæring innenfor cybersikkerhet, ved bruk av intervjuer, artikler,

rapporter, observasjoner med mer. En kombinasjon av disse sørger derfor for at gruppen kan innhente data som kan tallfestes, samtidig som det er mulig å gå mer i dybden der det er behov [28].

På grunn av den pågående pandemien falt valget på en digital spørreundersøkelse bestående av innledende spørsmål som alder, flervalgsspørsmål, men også fritekstspørsmål som går i dybden på de ansattes faktiske kunnskap om cybersikkerhet. Dette gir en god kombinasjon av både kvantitativ og kvalitativ metode, samtidig som det sørger for gruppen får dataene som er nødvendig.

3.3 Testing

3.3.1 Introduksjon

Ved bruk av pre-eksperimentelle design eller kvasi-eksperimentelle design er det ikke mulig å være sikker på at det er behandlingen som har effekt på læringsutbyttet og ikke noe annet. Ved bruk av pre-eksperimentelle design er det ikke mulig å fastslå årsak-virkning. Enten fordi den uavhengige variabelen, for eksempel behandlingen, ikke endrer seg, eller fordi de som blir testet ikke er tilfeldig valgt ut. Som nevnt i 2.6.3 er det ved bruk av kvasi-eksperimentelle design ikke mulig å ha tilfeldig utvalgte grupper, enten fordi det er upraktisk eller fordi det er umulig. Dette gjør at det ikke er mulig å utelukke at det er andre faktorer som har påvirket resultatet man får. Et ekte eksperimentelt design er med andre ord en god måte å sikre at det er behandlingen som har effekt og ikke andre faktorer.

3.3.2 Valg av design

Design 5 velges som testdesign for testene på HDOs ansatte.

Tilfeldig tildelt	Gruppe 1	Pre-test	Escaperom	Post-test
Tilfeldig tildelt	Gruppe 2	Pre-test	-	Post-test
Tilfeldig tildelt	Gruppe 3	-	Escaperom	Post-test
Tilfeldig tildelt	Gruppe 4	-	-	Post-test

Tabell 3.1: Design 5

Dette er fordi det er ønskelig å finne en årsak-virkning-sammenheng i resultatene, som er kontrollert for forvirrende variabler. For å kunne svare på problemstillingen er det satt to hovedmål:

- Finne ut om escaperom fører til at deltagerne lærer noe om cybersikkerhet
    - Pre-test
    - Post-test

- Utelukke andre mulige årsaker til en eventuell endring i kunnskap
    - Flere grupper
    - Kontrollgruppe
    - Tilfeldig valgte grupper
    - Halvparten tar ikke pre-test
    - Noe som holdes konstant

Ved bruk av design fem kan man kontrollere at endringen som finner sted skjer som følge av at test-gruppen tar escaperommene og ikke på grunn av andre variabler. For å få et stort nok sett med resultater til å kunne svare på problemstillingen med et godt grunnlag, blir det lagt opp til at hver gruppe skal bestå av 10 personer. Da vil det være 20 personer som svarer på pre-testen, 20 personer som tar escaperom og alle 40 tar post-testen. I utgangspunktet tenker gruppen at 20 stykker til å ta escaperom er for lite, men siden HDO bare er litt over 70 ansatte, konkluderes det med at det vil være en grei størrelse på utvalget.

Design fem legger, i likhet med de andre ekte eksperimentelle designene, vekt på tilfeldige og likeverdig utvalgte grupper. Alle de ulike avdelingene i HDO skal representeres, men siden noen avdelinger er større enn andre, er det naturlig at ansatte fra disse avdelingene står for en større andel av gruppene. Siden gruppen ikke har tilgang til lister over HDOs ansatte, får gruppens kontaktperson i HDO oppgaven med å trekke ut et tilfeldig utvalg som får tilsendt pre-test, escaperom og post-test.

3.3.3 Pre-test og post-test

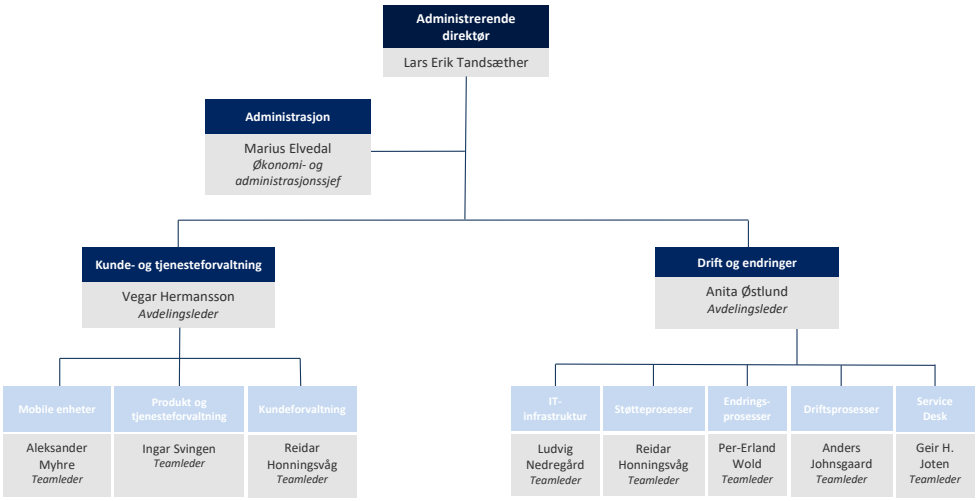
Pre-testen og post-testen lages som digitale spørreundersøkelser på grunn av den pågående pandemien. Spørreundersøkelsene lages i Nettskjema [29] da gruppen er godt kjent med plattformen og dette er en sikker plattform. De fleste ansatte i HDO har vært på hjemmekontor i store deler av prosjektperioden slik at det er vanskelig å få til fysiske intervjuer. Samtidig er det ønskelig å få flest mulig responser i den tilgjengelige tiden. På grunn av dette brukes spørreundersøkelser og ikke digitale intervjuer.

Pre-testen og post-testen er bygd opp likt med rundt 20 spørsmål hver. Testene starter med innledende spørsmål for å kartlegge alder og avdeling, samt tidligere erfaring med escaperom. Dermed kan resultatene deles inn i aldersgruppe og avdeling, slik at det blir et sammenligningsgrunnlag for mindre grupper innad i HDO. Videre består testene av selvvurderingsspørsmål som spør om testdeltagerne sine subjektive mening rundt deres digitale sikkerhet. Eksempelvis kommer spørsmålet "i hvilken grad opplever du selv at du behersker informasjonssikkerhet?" for å se hva de selv mener deres nivå ligger på. Til slutt inkluderes faglige spørsmål der de ansattes faglige kunnskap om temaer innen digital sikkerhet

vil bli testet. Dette gir et sammenligningsgrunnlag på hva testdeltagerne faktisk lærer mot hvor godt de selv mener de behersker digital sikkerhet.

På pre-testen er målet å få 20 responser, og den sendes derfor ut til 20 stykker i første omgang. Post-testen sendes ut til de 20 som tar pre-testen, til 10 stykker som tar escaperommene, men ikke pre-test, og til 10 som hverken har tatt pre-test eller escaperom slik at det blir 40 svar på post-testen tilsammen.

3.3.4 Testobjekter

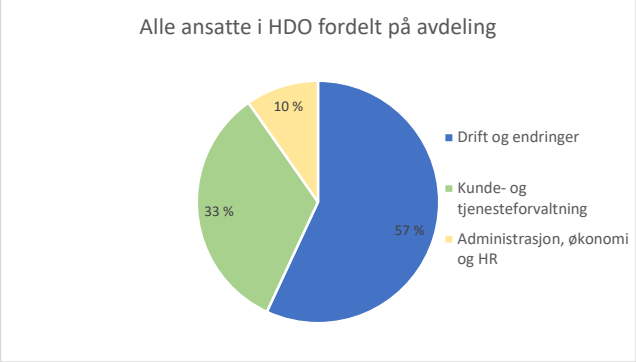


Figur 3.1: Organisering HDO

Som illustrert i figur 3.1 ser man at de ansatte i HDO er fordelt over flere ulike avdelinger, alt fra IT, til kundestøtte og til administrasjon. Dette gjør at det er svært variert innad i HDO hvor mye de jobber med cybersikkerhet i det daglige. Basert på de tre hovedavdelingene i HDO: drift og endringer, kunde- og tjenesteforvaltning og økonomi, administrasjon og HR er de ansatte fordelt slik:

- **41 stk** drift og endringer
- **24 stk** kunde- og tjenesteforvaltning
- **7 stk** økonomi, Administrasjon og HR

Det resulterer i prosentvis fordeling som ser slik ut:



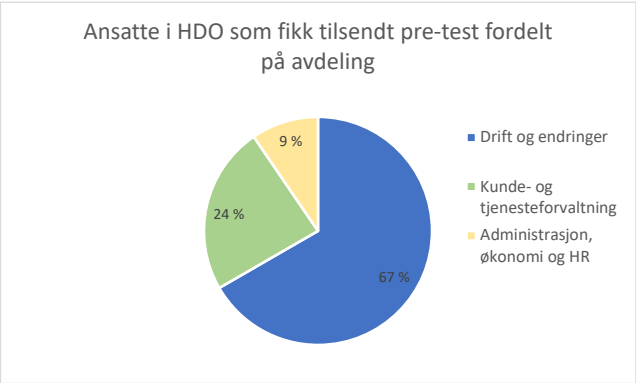
Figur 3.2: Alle ansatte i HDO fordelt på avdeling

Oppdragsgiver anslår at snittalderen på de ansatte ligger mellom 35-45 år, og at majoriteten av de er menn. For gruppen er det viktig å lage noe som alle ansatte kan dra nytte av, uavhengig av avdeling, alder og kjønn. Dette er fordi uavhengig av de ansattes kompetanse innen cybersikkerhet, er alle ansatte like mye utsatt for digitale trusler og enhver ansatt er en vei inn i systemet. Det er derfor svært viktig at alle ansatte innad i en bedrift har en viss grunnleggende kompetanse.

For å sørge for at testene når ut til alle ansatte, tar oppdragsgiver et uttrekk av 20 tilfeldige ansatte. Det tilfeldige uttrekket resulterer i en fordeling som ser slik ut:

- **14 stk** drift og endringer
- **5 stk** kunde- og tjenesteforvaltning
- **2 stk** stk økonomi, administrasjon og HR

Den prosentvise fordelingen vil bli seende slik ut:



Figur 3.3: Ansatte som fikk tilsendt pre-test fordelt på avdeling

Som grafen viser er avdelingsfordelingen så å si lik i uttrekket som ble gjort til pre-testen, men med en liten økning på avdelingen drift og endringer og en reduksjon i kunde- og tjenesteforvaltning.

3.4 Escaperom

3.4.1 Valg av plattform

Den første tanken var å bruke en kombinasjon av Mozilla Hubs og Google Forms. Dette gir en mulighet til å designe escaperom hvor ansatte i HDO kan føle at de navigerte i et faktisk rom, samtidig som de må løse gåter og gjøre andre oppgaver. Utfordringen med et virtuelt rom via Mozilla Hubs er at det ikke er mulig å ha kontroll over hvilken rekkefølge de ansatte tar spørsmålene i, og det vil derfor ikke være mulig å kontrollere at de følger historien det er tenkt at de skal følge. I tillegg vil utformingen og utviklingen av rommet være tidskrevende, i stedet for å fokusere på innholdet i oppgavene.

Valget falt derfor på Google Forms. Her har man mulighet til, som nevnt i 2.4.3, å legge inn spørsmål og/eller gåter som kan svares på blant annet via tekstsvar og/eller flervalg. Man kan i tillegg validere svarene til de som tar rommet og gi de hint hvis de ikke klarer å løse oppgaven(-e). I tillegg til hintene som kan gis når svarene valideres, er det mulig å gi hint i form av bilder eller tekst.

Til slutt gir Google Forms muligheten til å forplikte de som tar escaperommet til å følge historien og gjøre oppgavene i riktig rekkefølge. På denne måten sørger man for at de ansatte får med seg alle komponentene som ligger i rommet, og at de samtidig får det ønskelige læringsutbyttet.

3.4.2 Oppbygging av escaperom

For å lage escaperommene har rammeverkene nevnt i 2.4.2 Rammeverk blitt benyttet. Disse rammeneverkene sørger for at alle elementene som kreves for et godt escaperom inkluderes. For denne oppgaven har rammeverkene EscapED og SERF blitt kombinert til et eget rammeverk mer ideelt for oppgaven. Dette er blant annet fordi begge rammeverkene er ment for fysiske escaperom, og noen av kategoriene, som “utstyr”, ikke er relevante for virtuelle escaperom. Rammeverket er illustrert i følgende tabell:

Kategori	**Forklaring**
Mål	Hva skal spillerne lære seg gjennom rommet?
Tema	Hva er det overordnede temaet?
Spillere	
Antall	Hvor mange spillere per spill?
Kunnskap fra før	Hvilken kunnskap har spillerene om tema?
Alder	Hvor gamle er spillerne?
Avdeling	Hvilken avdeling er de fra?
Organisering	
Vanskelighetsgrad	Lett/Middels/Vanskelig/Svært vanskelig
Tid	Antall minutter
Samarbeid	Ja/Nei/Noe
Historie	Hva er konteksten og historien gjennom rommet?
Oppgaver	Hva er det spillerne testes på? Det kan være gåter, puzzels, quiz, mm.
Hendelsesforløp	Hvordan henger oppgavene sammen? Er det flere veier for å komme seg "ut"?
Evaluering	Skjer gjennom en post-test. Se at de faktisk klarer oppgavene og kommer seg igjennom rommet.

Tabell 3.2: Endelig rammeverk

Rammeverket starter med å definere målet og temaet for escaperommet. Her kommer hensikten med rommet fram. Spillerne er beskrevet med antall, alder, avdeling og hvilken kunnskap de har om temaet fra før. Disse punktene er tatt med for å beskrive demografien av spillerne som skal teste rommene. Organiseringen handler om hvor enkelt eller vanskelig rommet er, hvor lang tid det tar og om det er lagt opp til samarbeid eller ikke. Konteksten til rommet kommer fram i historien. Historien skal knyttes opp mot målet og bør ha en sammenheng med hensikten bak rommet. Oppgavene lages også med tanke på målet og hensikten av rommet. Disse er gjerne gåter man må løse for å komme frem til en kode slik at man kan gå videre i rommet. Hendelsesforløpet beskriver hvordan oppgavene og valgene man tar henger sammen. Det kan gjerne være flere hendelsesforløp i rommene, som enten er parallelle eller som går inn i hverandre på veien. Til slutt er det en evaluering av rommene som skjer igjennom en post-test. Denne brukes for å se om spillerne har lært noe av escaperommene. I tillegg er tilbakemeldinger fra spillerne ønskelig for å se hvor vanskelig det er å løse de ulike oppgavene og å komme seg igjennom rommene.

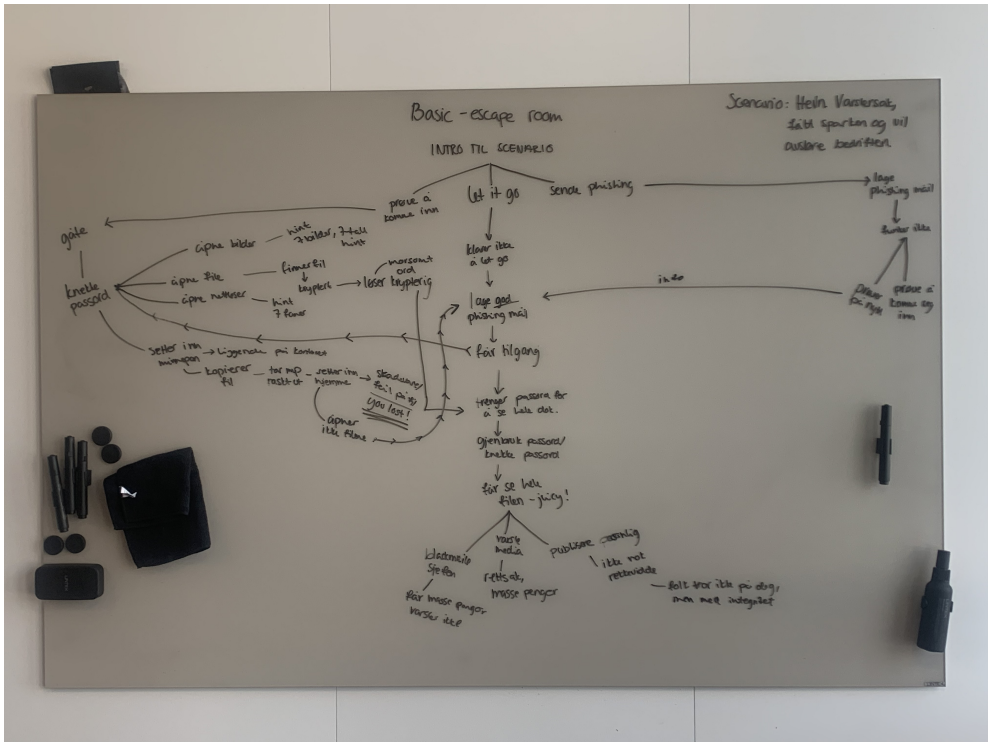
En mer detaljert beskrivelse med bilder av basisrommet sin oppbygning og dets oppgaver finnes i neste del. Dette escaperommet handler om generell cybersikkerhet og historien omhandler en fiktiv bedrift og inkluderer dermed ikke informasjon om HDO. Escaperommene nulldagssårbarhet og løsepengevirus er ikke like nøye beskrevet da de er skreddersydd for HDO og dermed inneholder sensitiv

informasjon som ikke kan inkluderes i teksten.

3.4.2.1 Basis

Det var et ønske fra HDO å få en opplæringspakke som alle ansatte kunne ha nytte av, både teknisk personell og ledelsen. I tillegg ønsket gruppen å lage en opplæringspakke om grunnleggende cybersikkerhet da rapporter om dagens trusselbilde [24, 26] viser at flere bedrifter mener at manglende sikkerhetsbevissthet hos ansatte er årsaken til sikkerhetsbrudd og at løsepengevirus og phishing er et problem. Det ble derfor valgt å lage et escaperom for å dekke temaer som passordsikkerhet, phishing, kryptering og adgangssikkerhet.

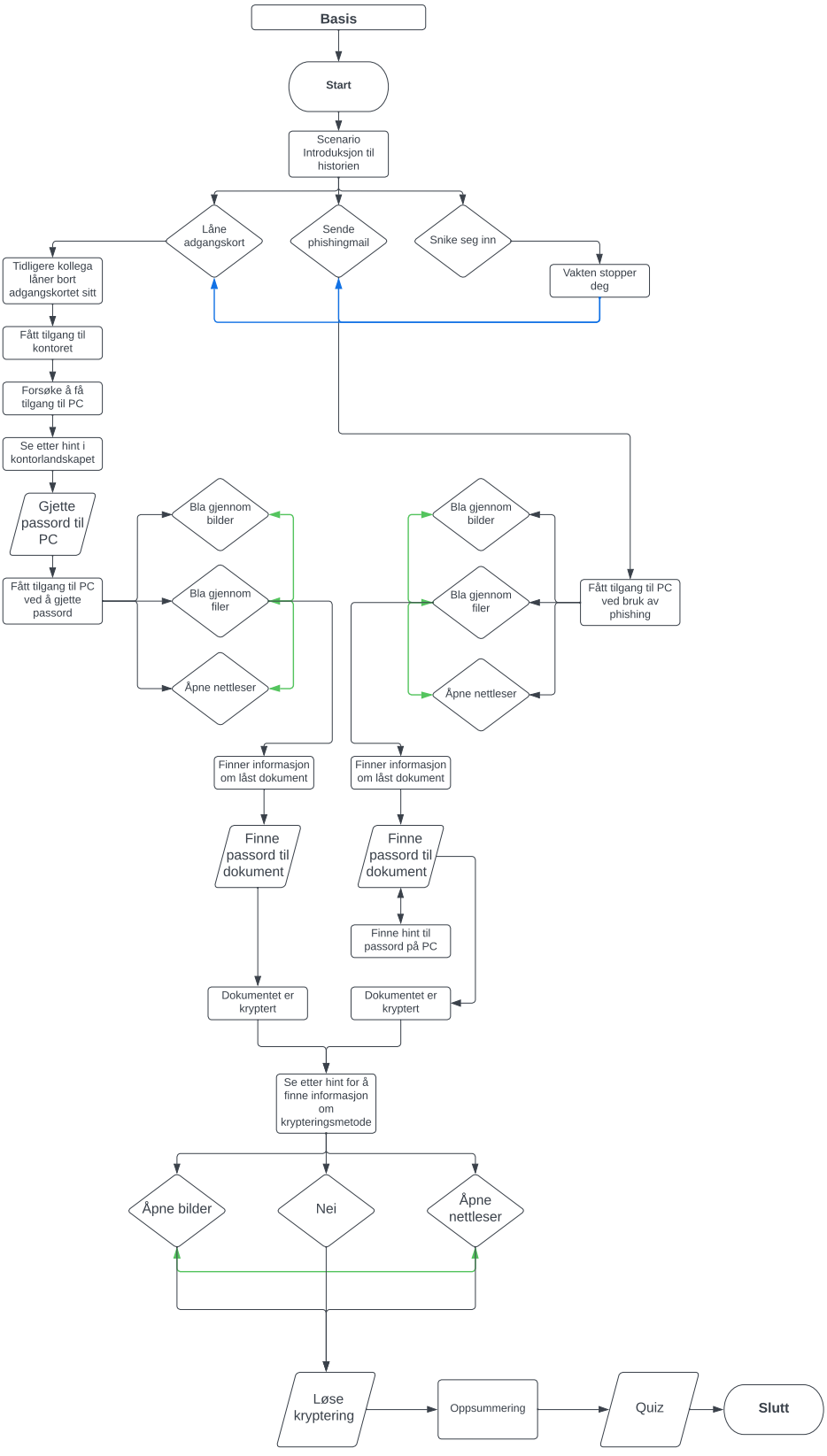
Figuren under viser førsteutkastet av basisrommet sitt hendelsesforløp. Under selve utviklingen av escaperommet ble dette endret på. Det er flere temaer som gjerne skulle blitt inkludert som gåter, blant annet håndtering av ukjente minnepenner og sikkerhetsforhåndsregler utenfor kontoret. Dette ble ikke prioritert da det var vanskelig å implementere i praksis.



Figur 3.4: Førsteutkast av basisrommet sitt hendelsesforløp.

Flytdiagrammet nedenfor viser hvordan basisrommet faktisk er utformet. Ovalene viser hvor rommet begynner og slutter. De avrundede firkantene illustrerer informasjon spillerne får og/eller kan velge å få. Rombene illustrerer valg spillerne må ta og parallellogrammene illustrerer de konkrete oppgavene spillerne går igjennom i løpet av rommet. Blå piler vises der hvor et hendelsesforløp tar slutt og spilleren må gå til et annet hendelsesforløp. Til slutt, grønne piler vises der hvor spilleren kan gå frem og tilbake flere ganger før den tar et valg.

Figur 3.5: Oversikt over figurer brukt i flytdiagram

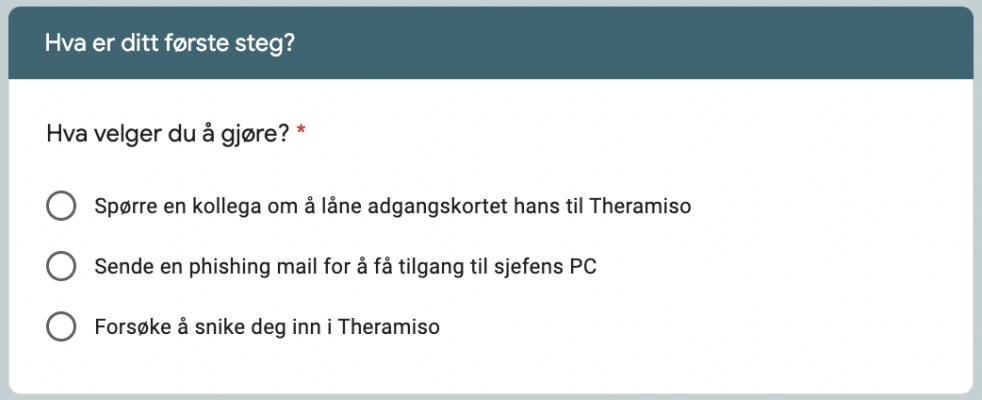


Figur 3.6: Flytdiagram som viser hvordan basisrommet er bygd opp

Kategori	**Forklaring**
Mål	Lære grunnleggende cybersikkerhet, spesielt knyttet til passordsikkerhet og phishing
Tema	Hva er det overordnede temaet?
Spillere	
Antall	1-4
Kunnskap fra før	Liten til ingen
Alder	18-79
Avdeling	Alle
Organisering	
Vanskelighetsgrad	Lett til middels
Tid	20-40 minutter
Samarbeid	Ja, men kan også utføres alene
Historie	Historien er en bedriftshemmelighet der deg-personen må komme seg inn i systemet til en bedrift ved valg og gåteløsning for å finne ut av hemmeligheten. Settingen foregår i bedriftens kontor.
Oppgaver	Gåter om passord, kryptering og phishing da målet er å lære om grunnleggende cybersikkerhet. De skal testes på HDO.
Hendelsesforløp	Flere ulike hendelsesforløp som fører til samme slutt.
Evaluering	Post-test brukes for å evaluere rommet

Tabell 3.3: Rammeverk basis

Escaperommets historie går ut på å eksponere bedriftshemmeligheten til en fiktiv bedrift. Deg-personen har oppdaget noe rart på jobben, og etter å ha spurt sjefen om det blir du sparket. Du får dermed lyst til å etterforske dette videre da hele situasjonen er merkelig, og målet blir å finne ut av hemmeligheten og forhåpentlighvis renvaske deg selv. For å gjøre dette må du inn i bedriftens systemer, og for å finne bevis må du ta valg og løse gåter. Rommet gir spilleren flere valgmuligheter med forskjellig utfall, men alle hendelsesforløpene vil gi samme utfall til slutt. Hovedsakelig er det tre hendelsesforløp; sende phishing mail for å kompromittere systemet, få tak i et adgangskort for å ta seg inn i bedriften eller å snike seg inn. Disse hendelsesforløpene illustreres i flytdiagrammet over, og vil påvirke resten av historien. Hvordan dette valget ble implementert i Google Forms vises i figuren under.



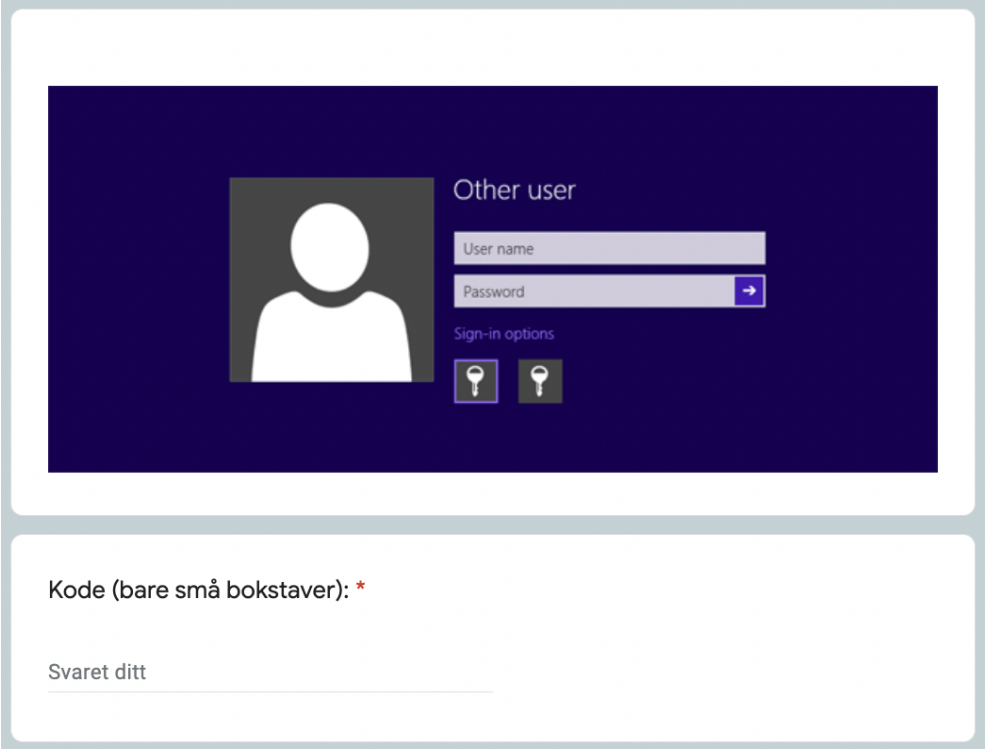
Figur 3.7: Figur som viser første valgmulighet i basis-escaperommet.

Rommet er lagt opp til å ha lett til middels vanskelighetsgrad og vil ta mellom 20-40 minutter. Dette vil variere ut ifra spillerne sin tidligere erfaring med gåteløsning og eventuelt CTF [30], spesielt siden det er en krypteringsoppgave som kan være lettere å skjønne hvis man er kjent med kryptografi. Det kan spilles alene eller i grupper på maks fire ettersom hvordan det passer de enkelte. Gruppearbeid vil ha flere fordeler; det vil være mindre sannsynlighet å stå fast, gi mer refleksjon rundt læringsmålene og det kan rett og slett være morsommere. Basisrommet er ikke spesifikt tilpasset HDO da oppgavene er om generell cybersikkerhet. Derfor kan det også passe til andre bedrifter som ønsker opplæring i cybersikkerhet, siden settingen er på et kontor og historien omhandler et kontor og en bedrift. Da vanskelighetsnivået er relativt lavt vil det passe for IT-ansatte, men også ledelse og andre ledd i bedriften.

Den ene oppgaven er som nevnt en krypteringsoppgave hvor krypteringen brukt er cæsarschiffering, også kjent som Cæsars kode [31]. Kryptering er viktig for informasjonssikkerhet da det gjør lesbar tekst, klartekst, om til kryptert tekst. Man vil trenge en nøkkel for å gjøre den krypterte teksten til klartekst, og dermed beskytter det teksten sin konfidensialitet. Selv om man med dagens teknologi sjeldent trenger å kryptere noe manuelt, er det essensielt for sikkerhet, og det lager en morsom oppgave i escaperommet. En annen gåte omhandler passord, der man skal kunne gjette seg til et enkelt passord med hint fra eieren til pc-en sin kalender og notatbok. Dette demonstrerer hvorfor svake, personlige passord er et problem, da man kan "brute-force" seg inn. I en senere gåte som ber om et passord, er svaret passordet fra den forrige oppgaven. Dette demonstrerer hvorfor man ikke skal gjenbruke passord. Escaperommet viser også en phishingmail med mål om å vise hvor overbevisende phishingmailer kan være. Rommet avrundes med en liten quiz som oppsummerer læringsmålene.

Figur 3.8 nedenfor viser en oppgave hvor spillerne må finne en kode/passord som deretter skal skrives inn her. Ordet "kode" brukes siden Google Forms fjerner skjemaet hvis ordet "passord" blir nevnt, da de tror det er et legitimt svindelforsøk.

For å gjette passordet er det hint i en kalender og en notatblokk i figur 3.9.



Figur 3.8: Eksempel på oppgave.

Figur 3.9: Kalender og notatbok som viser hint til passordet for figuren over.

3.4.2.2 Løsepengevirus

Kategori	**Forklaring**
Mål	Lære om gangen i hendelseshåndteringsplanen i HDO og løsepengevirus som angrepsmetode
Tema	Hendelseshåndteringsplan og løsepengevirus
Spillere	
Antall	1-4
Kunnskap fra før	Fra noe til en del
Alder	18-79
Avdeling	Alle
Organisering	
Vanskelighetsgrad	Middels
Tid	20-40 minutter
Samarbeid	Ja, men kan også utføres alene
Historie	Historien starter med at en ansatt fra HDO som får opp en README-fil på PC-skjermen på jobben. Videre følger vi den ansatte og CISO/ledere gjennom håndteringen av avviket.
Oppgaver	Labyrint, gåter, lete etter hint, valg, fylle inn avviksrapport, krypteringsoppgave.
Hendelsesforløp	Ulike hendelsesforløp flere steder i rommet. Velger man "riktig" valg hver gang vil veien "ut" være enklere og raskere.
Evaluering	Post-testen brukes for å evaluere rommet

Tabell 3.4: Rammeverk løsepengevirus

Målet med løsepengevirus escaperommet er å lære å bruke hendelseshåndteringsplanen som HDO har for sikkerhetshendelser. CISO ønsket at denne skulle være fokuset i noe av opplæringen. Som sikkerhetshendelse i rommet ble løsepengevirus-angrep valgt da dette er en av de mest dagsaktuelle metodene for cyberangrep (se 2.5 Trusselbilde og sikkerhetskultur) og også en metode som bruker enkle angrepsvektorer som alle i HDO kan bli utsatt for [23].

Rommet er lagt opp til middels vanskelighetsgrad da svarene på pre-testen var ulike. Med tanke på dette er det lagt opp til utfordringer i rommet, men samtidig er ikke målet å gjøre escaperommet for vanskelig. Siden det er ulike hendelsesforløp og oppgaver og noen mennesker løser noen gåter raskere enn andre, kan rommet ta alt fra 20-40 minutter å gjennomføre. Antall spillere som gjør rommet sammen kan være alt fra 1-4. Escaperommet er lagt opp til at man kan samarbeide, men det skal også være mulig å gjennomføre alene. Dog vil det nok være morsommere og kanskje lettere å gjøre det sammen i en gruppe på 3-4 da man kan diskutere oppgavene og hendelsesforløpene. Spillerne er

mellom 18-79 år og alle avdelingene skal ha grunnlag for å kunne gjennomføre rommet. Kunnskapen til de ansatte vil være ulik da de fra drift og endringer gjennomsnittlig kan mer generelt om digital sikkerhet enn de fra økonomi, administrasjon og HR.

Escaperommet består av ulike hendelseforløp der noen deler/oppgaver ikke trengs å gjøres hvis man velger "riktig" valg, men uansett hvilket valg man tar vil man komme inn på hovedforløpet etter hvert. Historien som følges igjennom escaperommet starter med at en ansatt fra HDO får opp en README-fil på PC-skjermen på jobben. Ettersom man tar ulike valg og går igjennom ulike hendelsesforløp vil man ende opp med at avviket er meldt ifra til nærmeste leder, som igjen melder fra til CISO. Videre skal spillerne gjennom tre aktiviteter; analysere avviket, finne årsak og vurdere kritikalitet, lese igjennom README-filen på nytt og dokumentere avviket i en avviksrapport. Disse oppgavene kan gjennomføres i hvilken rekkefølge som helst, men må alle gjennomføres for å komme videre i rommet. Når man er videre derfra skal man finne tiltak og gjennomgå tiltakene. Til slutt får man et dekrypteringsverktøy for å løse siste oppgave og fullføre rommet.

Siste oppgave er som sagt en krypteringsoppgave. Andre oppgaver i escaperommet er labyrinter, gåter og koder man må lete seg fram til, men det er også noen oppgaver som kun handler om å forstå seg på hendelseshåndteringsplanen og reflektere rundt historien. De sistnevnte oppgavene er åpne tekstsvar og det er heller ikke et fasitsvar til disse oppgavene. Spillerne kommer derfor videre ved å fylle inn hva som helst. For noen kan dette være en mulighet til å gjennomføre rommet raskt, men målet er at det skal føre til refleksjon rundt sikkerhetshendelsen.

3.4.2.3 Nulldagssårbarhet

Kategori	**Forklaring**
Mål	Lære om nulldagssårbarheter
Tema	Hva er det overordnede temaet?
Spillere	
Antall	1-4
Kunnskap fra før	Ukjent
Alder	Alle
Avdeling	Alle, men spesielt rettet mot drift og endringer
Organisering	
Vanskelighetsgrad	Middels
Tid	20-30 minutter
Samarbeid	Ja, men kan også utføres alene
Historie	Angrep med ukjent kilde
Oppgaver	Ta riktige valg
Hendelsesforløp	3 hendelsesforløp, som blir samlet til 1 Kun en vei "ut"
Evaluering	Ingen evaluering planlagt - rommet skal testes av HDO senere

Tabell 3.5: Rammeverk nulldagssårbarhet

Målet med nulldagssårbarhet-rommet er å lære de ansatte i HDO om nulldagssårbarheter, samt å forsterke det de lærte om hendelseshåndteringsplanen i escaperommet om løsepengevirus. Rommet går ikke detaljert ned i stegene i hendelseshåndteringsplanen slik som rommet om løsepengevirus gjør, men flere av stegene er inkludert. Bakgrunnen for valg av tema er at utnyttelse av tekniske sårbarheter er noe flere organisasjoner peker på som en dagsaktuell metode for cyberangrep [22, 23, 25].

Rommet er lagt opp til middels vanskelighetsgrad, slik at det skal være mulig for alle de ansatte i HDO å komme seg igjennom rommet. Dog, basert på tema og eventuell angrepsvektor i en slik situasjon, kan man anta at det er de ansatte som jobber med IT og/eller cybersikkerhet til daglig som vil få mest ut av rommet. Fra gruppens erfaring med å teste rommet ble det på det meste brukt rundt 8 minutter, men siden gruppen har god kjennskap til rommet vil det antagelig ta de ansatte i HDO alt fra 20-30 minutter å gjennomføre. Rommet er lagt opp til at det kan tas individuelt eller i grupper opp til 4 stykker, men antageligvis vil det - i likhet med løsepengevirus-rommet, kanskje bli oppfattet som morsommere å gjøre rommet hvis de samarbeider, slik at de kan diskutere hva de skal gjøre ettersom de gjør framgang i rommet. Rommet vil være åpent for alle ansatte i HDO, uavhengig av stilling og/eller aldersgruppe.

Siden tema for rommet er basert på aktuelle trussel- og risikovurderinger, er det ukjent hvilken kunnskap de ansatte i HDO har om temaet fra før. Rommet bruker derfor få tekniske begreper slik at det skal være mulig å forstå alt av informasjon i rommet, uten å ha en IT-bakgrunn.

Historien som møter de ansatte i HDO er basert rundt et angrep fra en ukjent kilde. Angrepet rammer først en ekstern tredjepart og deltakerne i rommet må bestemme om dette er noe de ønsker å undersøke videre, eller om de vil la det ligge siden angrepet kun berører en tredjepart. Rommet består i likhet med rommet om løsepengevirus av forskjellige hendelsesforløp, men i dette rommet er hendelsesforløpene mer kompliserte. Avhengig av hvilke valg deltakerne tar i løpet av rommet vil de bli møtt av ny historie, men alle valgene vil til slutt lede inn på ett felles hendelsesforløp. I det felles hendelsesforløpet har angrepet spredd seg fra den eksterne tredjeparten og videre til HDO. Dette resulterer i at kritiske tjenester hos HDO går ned. I rommet er det kun to "direkte" oppgaver, i dette tilfellet en oppgave hvor de må vurdere kritikaliteten på hendelsen, og en krypteringsoppgave for å få isolert alle enhetene som er påvirket av angrepet. Krypteringsoppgaven er siste steget i rommet, og er det som må løses til slutt for å komme seg "ut" av rommet.

3.5 Gjennomføring av analyse

Det finnes flere forskjellige måter å analysere resultater på. Analysen i oppgaven har benyttet Microsoft Excel. Nettskjema, som blir brukt til spørreundersøkelsen, tilbyr eksportering av resultatene til Excel. Gruppen får derfor enkelt ut spørsmålene og svarene, illustrert i figuren nedenfor:

I hvilken grad opplever du selv at du behersker informasjonssikkerhet?
Høy grad
Høy grad
Høy grad
Middels grad
Middels grad
Høy grad
Middels grad
Middels grad
Middels grad
Høy grad
Høy grad
Høy grad
Høy grad
Høy grad

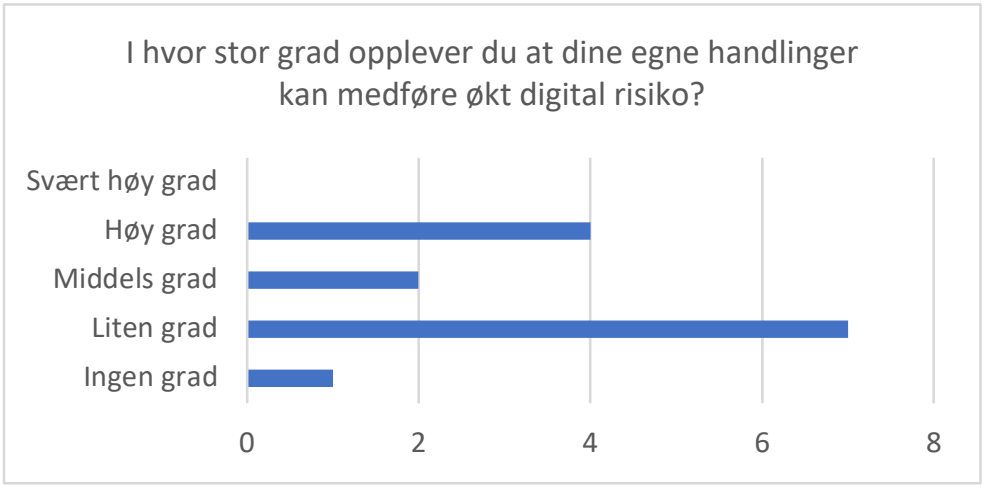
Figur 3.10: Responseksempel fra Microsoft Excel

For å lettere visualisere resultatene brukes Excel sin graffunksjon. For at dette skal fungere optimalt må man manuelt legge inn svaralternativene for hvert enkelt spørsmål og så oppsummere svarene.

I hvor stor grad opplever du at dine egne handlinger kan medføre økt digital risiko?	
SVARALTERNATIVER	**RESPONS**
Ingen grad	1
Liten grad	7
Middels grad	2
Høy grad	4
Svært høy grad	0
Totalt antall responser:	**14**

Figur 3.11: Eksempel på respons med svaralternativer fra Microsoft Excel

Videre brukes den innebygde graffunksjon og man ender opp med en graf lik den nedenfor.



Figur 3.12: Eksempel på graf

Kapittel 4

Testing

4.1 Introduksjon

Oppgavens datainnsamling kommer fra pre-testen, escaperom og post-testen, der post-testen er hovedkilden for informasjon. Det er avgjørende at et escaperom har blitt gjennomført for at man skal kunne lære noe av post-testen. Pre-testen er med på å lage et sammenligningsgrunnlag, slik at det kan bekreftes eller avkreftes at resultatene fra post-testen har blitt påvirket av escaperommet.

4.2 Pre-test

Som nevnt i kapittel 3 er pre-testen delt inn i fire hoveddeler; innledende spørsmål, selvvurderingsspørsmål, faglige spørsmål og generelle spørsmål. Alle spørsmålene fra pre-testen er presentert i tabeller senere i kapittelet. Testen foregikk digitalt og ble sendt ut via e-post den 14. mars. De første 20 som fikk tilsendt testen hadde i utgangspunktet 1,5 uke (til den 23. mars) på å svare på testen. Til den 23. mars var det fire responser på testen og gruppen ba derfor HDOs kontaktperson om å purre på resten. Det førte til at fem til svarte den 23. mars. Den 4. april var det 10 responser og gruppens kontaktperson sendte ut pre-testen til 20 ansatte til. Dette resulterte i fire svar til og det endte med 14 svar til sammen på pre-testen.

4.2.1 Innledende spørsmål

De innledende spørsmålene er der for å få et sammenligningsgrunnlag, slik at man kan se hvem escaperommene "treffer". Eksempelvis får de i aldersgruppen 40-49 mer ut av escaperommet enn de i aldersgruppen 18-29? Eller de på økonomiavdelingen i forhold til drift og endringer? I tillegg spør testen om spillerne har benyttet escaperom tidligere for å kartlegge hvilket vanskelighetsnivå de ulike gåtene og oppgavene skal ha.

Spørsmål	Alder?
Svar	18-29/30-39/40-49/50-59/60-69/70-79

Tabell 4.1: Alder

Spørsmål	I hvilken avdeling jobber du?
Svar	Tekstsvar

Tabell 4.2: Avdeling

Spørsmål	Har du vært i et escaperom tidligere?
Svar	Ja/Nei

Tabell 4.3: Tidligere erfaring

4.2.2 Selvvurderingsspørsmål

Selvvurderingsspørsmålene er inkludert i pre-testen for å få en subjektiv statistikk på hva deltagerne kan om digital sikkerhet og for å kartlegge deres viten om sikkerhetsrutiner i HDO. De tre første spørsmålene gir et sammenligningsgrunnlag for post-testen. Målet med disse spørsmålene er å se om de føler kompetansen øker eller synker etter escaperommene er tatt. De fire siste spørsmålene er inkludert for å få et inntrykk av hvor gode de ansatte er på digital sikkerhet og sikkerhetsrutiner generelt i HDO.

Spørsmål	I hvilken grad opplever du selv at du behersker informasjonssikkerhet?
Forklaring	Med informasjonssikkerhet mener vi de overordnede rutiner som du har rundt sikring av sensitiv informasjon, for eksempel forretningshemmeligheter.
Svar	Ingen grad/Liten grad/Middels grad/Høy grad/Svært høy grad

Tabell 4.4: Behersker informasjonssikkerhet

Spørsmål	I hvilken grad føler du deg forberedt på hva du skal gjøre hvis en sikkerhetshendelse skjer?
Forklaring	Med sikkerhetshendelse mener vi en hendelse, aktivitet eller situasjon som enten allerede har forårsaket skade eller kan forårsake skade på bedriften og/eller personell.
Svar	Ingen grad/Liten grad/Middels grad/Høy grad/Svært høy grad

Tabell 4.5: Forberedt på sikkerhetshendelse

Spørsmål	I hvor stor grad opplever du at dine egne handlinger kan medføre økt digital risiko?
Forklaring	Med økt digital risiko mener vi brudd på CIA-triaden: Konfidensialitet - informasjon ikke blir kjent for uvedkommende, integritet - informasjonen ikke blir endret av uvedkommende og tilgjengelighet - informasjon er tilgjengelig ved behov for de som er autorisert.
Svar	Ingen grad/Liten grad/Middels grad/Høy grad/Svært høy grad

Tabell 4.6: Egne handlinger

Spørsmål	Føler du at opplæringen du har fått i HDO har gitt deg økt kompetanse innenfor informasjonssikkerhet?
Svar	Ja/Noe/Nei

Tabell 4.7: Økt kompetanse

Spørsmål	I hvor stor grad er du kjent med retningslinjene din arbeidsplass har for informasjonsikkerhet?
Svar	Ingen grad/Liten grad/Middels grad/Høy grad/Svært høy grad

Tabell 4.8: Retningslinjer

Spørsmål	Er du kjent med hvorvidt HDO har en hendelseshåndteringsplan?
Svar	Ja/Noe/Nei

Tabell 4.9: Hendelseshåndteringsplan

Spørsmål	Hvor mye kan du om informasjonssikkerhet i forhold til de andre ansatte i HDO?
Svar	Under gjennomsnittet/Gjennomsnittlig/Over gjennomsnittet

Tabell 4.10: Kunnskap i forhold til andre

4.2.3 Faglige spørsmål

De faglige spørsmålene er til for å validere selvvurderingsspørsmålene, altså å sjekke om deltagerne faktisk kan det de sier de kan. De ulike spørsmålene går inn på temaer som phishing, passord, sikring av sensitiv informasjon utenfor kontoret og avviks-/hendelseshåndtering. De faglige spørsmålene er utformet på bakgrunn av HDOs opplæringspakke for nyansatte og denne er underlagt taushetserklæringen.

Til spørsmålet “hvilken av disse tror du er en phishing e-post?” fikk de ansatte presentert to bilder av to ulike e-poster fra tilsynelatende samme avsender, hvorav en av disse e-postene er en phishing e-post, den andre er ikke det.

Spørsmål	Hvilken av disse tror du er en phishing e-post?
Svar	Bilde 1/Bilde 2

Tabell 4.11: Phishing bilde

Spørsmål	Hvilke tegn gjør denne e-posten til en phishing e-post?
Svar	Tekstsvar

Tabell 4.12: Tegn phishing

Spørsmål	Hva legger du vekt på når du lager et sikkert passord?
Svar	Tekstsvar

Tabell 4.13: Lage sikkert passord

Spørsmål	Hvilken av disse ville du ha sett på som et sikkert passord?
Svar	NorgesLengsteInnsjoMjosaHarPlassTil91MillionerMennesker Komfortabelt/NlinnMhPt91mMk/Joggesko3!* /learkiegnerlane

Tabell 4.14: Passord

Spørsmål	Begrunn hvorfor valget ditt er et sikkert passord?
Svar	Tekstsvar

Tabell 4.15: Sikkert passord

Spørsmål	Hvis du jobber utenfor HDO's kontorer – hvilke steg tar du for å sikre jobben du gjør?
Svar	Tekstsvar

Tabell 4.16: Sikre jobben

Spørsmål	Hvis du oppdager et avvik/en hendelse, vet du hva du skulle gjort for å håndtere avviket/hendelsen?
Svar	Tekstsvar

Tabell 4.17: Håndtere avvik/hendelse

Spørsmål	Har du meldt fra avvik/hendelser tidligere?
Svar	Ja/Nei

Tabell 4.18: Meldt fra avvik/hendelse

Spørsmål	Sjekket du avviksplanen/hendelseshåndteringsplanen før du meldte hendelsen?
Svar	Tekstsvar

Tabell 4.19: Sjekke avviksplan/hendelseshåndteringsplan

4.2.4 Generelle spørsmål

For å kunne sammenligne escaperom som en form for opplæring blir det spurt om de har fått opplæring i digital sikkerhet og hva slags opplæring de eventuelt har gjennomgått.

Spørsmål	Har du fått organisert opplæring i digital sikkerhet i løpet av de siste to årene?
Svar	Ja/Nei

Tabell 4.20: Opplæring

Spørsmål	Hva slags opplæring har du fått?
Svar	Tekstsvar

Tabell 4.21: Hva slags opplæring

4.3 Escaperom

Escaperommene testes individuelt og når det passer for de ansatte i løpet av uke 17 og 18. De sendes ut til de 40 som også fikk tilsendt pre-testen. Disse 40 velges fordi gruppen trenger syv av de 14 som tok pre-testen til å ta et escaperom og post-testen, og de resterende syv som tok pre-testen til å bare ta post-testen. Gruppen trenger også syv til å ta et escaperom og post-testen og syv til å bare ta post-testen som ikke har tatt pre-testen. Siden begge testene er anonyme følges det med på om de svarer "ja" på om de har tatt pre-testen, på post-testen i Nettskjema, for å se om fordelingen blir riktig. For å få lik fordeling på gruppene var det ønskelig med 28 svar, men siden kun 14 av 40 svarte på pre-testen mener gruppen at det er lurt å sende ut til en større gruppe med en gang. I tillegg er det ingen måte for gruppen å vite hvem av de 40 som fikk tilsendt pre-testen som faktisk tok den.

Nulldagssårbarhet-escaperommet sendes ikke ut for testing da HDO ønsker å ha et escaperom som ingen har tatt, som de kan gjennomføre som en opplæringsøvelse i fellesskap senere.

4.4 Post-test

4.4.1 Innledende spørsmål

I post-testen spørres det etter alder og avdeling slik som i pre-testen (se 4.2.1). Dette er for å kunne sammenligne læringsutbyttet de ulike aldersgruppene og avdelingene får av escaperommene. I tillegg blir det spurt om de har tatt en tidligere spørreundersøkelse for bacheloroppgaven som refererer til pre-testen for å skille de ulike gruppene i designet (se valg av design). Til slutt i de innledende spørsmålene spørres det om de har testet et av escaperommene for å vise dem videre til de relevante faglige spørsmålene, og ikke minst for å vite hvem som testet hvilke escaperom, og hvem som ikke gjennomførte escaperom.

Spørsmål	Har du tatt en tidligere spørreundersøkelse fra oss?
Svar	Ja/Nei

Tabell 4.22: Tidligere spørreundersøkelse

Spørsmål	Har du tatt noen av disse escaperommene?
Svar	Basic/Løsepengevirus/Ingen

Tabell 4.23: Escaperom

4.4.2 Selvvurderingsspørsmål

I post-testen inkluderes de samme selvvurderingsspørsmålene (se 4.2.2) som i pretesten, for å sjekke om de ansatte føler de har lært noe av escaperommet. Spørsmålene "føler du at opplæringen du har fått i HDO har gitt deg økt kompetanse innenfor informasjonssikkerhet?", "i hvor stor grad er du kjent med retningslinjene din arbeidsplass har for informasjonsikkerhet?", "er du kjent med hvorvidt HDO har en hendelseshåndteringsplan?" og "hvor mye kan du om informasjonssikkerhet i forhold til de andre ansatte i HDO?" vises bare hvis de svarer "nei" til om de har tatt en tidligere spørreundersøkelse for bacheloroppgaven (innledende spørsmål). Dette er fordi deltagerne bare trenger å svare på disse spørsmålene en gang.

4.4.3 Faglige spørsmål

De faglige spørsmålene i post-testen er utformet for å gjenspeile læringsutbyttet fra basis og løsepengevirus escaperommet, og for å være like temaene fra pretesten. Noen av spørsmålene er kun for de som tok basisrommet, mens resten er åpent for alle å svare, selv om de ikke tok det escaperommet.

4.4.3.1 Basis:

Det første og andre spørsmålet under kommer bare opp hvis man svarer "ja" på at man tok basisrommet. Dette er fordi spørsmålene er basert på et eksempel fra det escaperommet.

Spørsmål	Basert på phishing-eksempelet i basic-rommet, tenker du at phishing alltid er lett å gjennomskue?
Svar	Ja/Nei

Tabell 4.24: Phishing-eksempel

Spørsmål	Vil du i framtiden være mer obs på potensielle phishing mailer, selv om mailen ser troverdig ut?
Svar	Ja/Nei

Tabell 4.25: Phishing mail

Spørsmål	Passordsikkerhet er viktig - er det noen ting du tenker at det ikke er lurt å ha i et passord?
Svar	Din eller næres navn og bursdag/Navnet på hunden din kombinert med dens bursdag/Favorittmaten kombinert med flere spesialtegn og en tilfeldig tallsekvens/Navnet på kona og datoen for bryllupsdagen

Tabell 4.26: Passordsikkerhet

4.4.3.2 Løsepengevirus:

De fem spørsmålene under er direkte basert på løsepengevirus escaperommet. Spørsmålene er rettet mot løsepengevirus, men også mot hendelseshåndterings-planen.

Spørsmål	Hva er det første du bør gjøre hvis du oppdager et avvik?
Svar	Si ifra til nærmeste leder/CISO /Spørre en tekniker om hjelp/ Finne ut av årsak til avviket og mer detaljer alene først

Tabell 4.27: Oppdager avvik

Spørsmål	Hva er oftest årsak til et løsepengevirus-angrep (kryss av for de du mener er riktig)?
Svar	Trykke på lenke/vedlegg i e-post/Infiserte nettsider/Ikke oppdatert operativsystem

Tabell 4.28: Løsepengevirus-angrep

Spørsmål	Hva er gode preventive tiltak for å unngå å bli angrepet av et løsepengevirus-angrep?
Svar	Tekstsvar

Tabell 4.29: Tiltak løsepengevirus

Spørsmål	Hvilke 5 punkter er obligatoriske å ha med i en avviksrapport i Simployer?
Svar	Tekstsvar

Tabell 4.30: Avviksrapport

Spørsmål	Hvilken plan skal følges hver gang en sikkerhetshendelse oppstår eller under opplæring/øvelse?
Svar	Tekstsvar

Tabell 4.31: Plan sikkerhetshendelse

De to generelle spørsmålene fra pre-testen er også inkludert i post-testen (se 4.2.4). I tillegg er det inkludert to spørsmål om hva de synes om escaperom som en opplæringsmetode. Ved å spørre om dette får gruppen deres subjektive mening om escaperom som læringsplattform.

Spørsmål	Hva synes du om opplæring innen digital sikkerhet gjennom escaperom vs. tidligere opplæring du har fått?
Svar	Tekstsvar

Tabell 4.32: Escaperom vs. tidligere opplæring

Spørsmål	Føler du at du lærte mer av å ta et escaperom vs. tradisjonell opplæring?
Svar	Ingen grad/Liten grad/Middels grad/Høy grad/Svært høy grad

Tabell 4.33: Utbytte av escaperom

Kapittel 5

Analyse

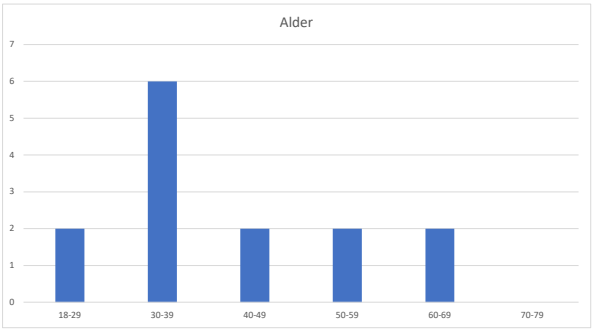
5.1 Introduksjon

Analysekapitlet består av flere deler: først går kapitlet gjennom resultatene fra pre-testen for å kartlegge hvilket nivå de ansatte ligger på før de tar escaperom, slik at disse resultatene kan sammenlignes med resultatene av post-testen. Videre vil kapitlet se på resultatene av basisrommet - hvilke valg spillerne har tatt og om det er noen oppgaver de har hatt problemer med å løse. Resultater fra rommet om løsepengevirus vil ikke bli gjennomgått, da det inneholder informasjon som er underlagt taushetsplikt. Til slutt går kapitlet igjennom resultatene av post-testen, for å undersøke om de som har tatt escaperommene føler de har lært noe, og om de føler de har lært *mer* enn ved tradisjonell opplæring.

5.2 Resultat av pre-test

Som illustrert i tabellen nedenfor er majoriteten av de ansatte som har svart på pre-testen i aldersgruppen 30-39 år. Dette samsvarer godt med snittet oppdragsgiver anslo i 3.3.3.

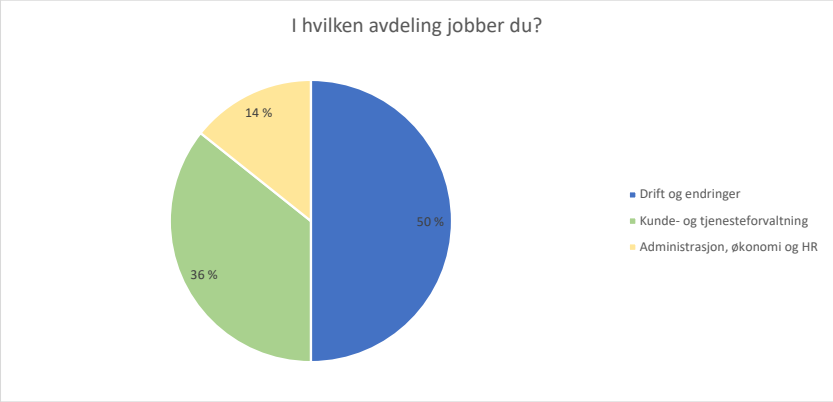
5.2.1 Alder



Figur 5.1: Spørsmål: Alder

5.2.2 Avdeling

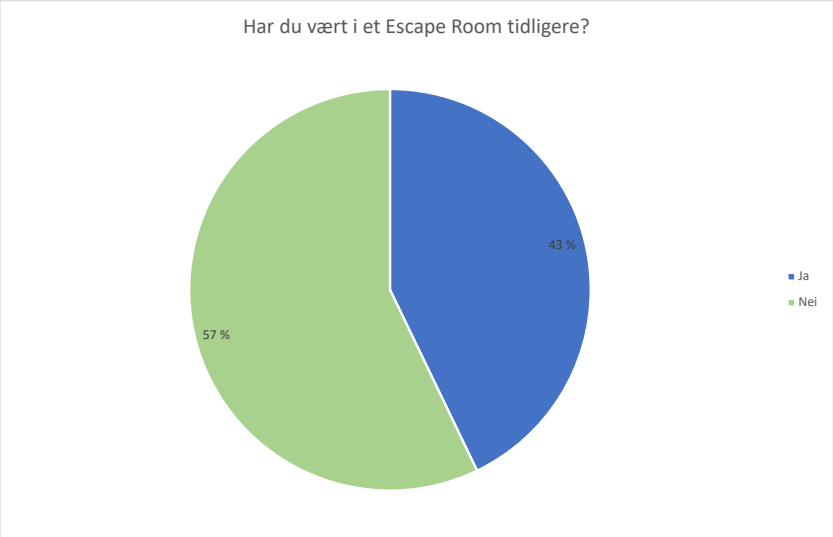
Figuren under viser at majoriteten, 50% av de som har svart på pre-testen, jobber i avdelingen drift og endringer. De resterende 50% er fordelt på kunde- og tjenesteforvaltning og administrasjon, henholdsvis 36% og 14%. Dette samsvarer forholdvis godt med fordelingen i uttrekket som ble gjort til pre-testen.



Figur 5.2: Spørsmål: I hvilken avdeling jobber du?

5.2.3 Tidligere erfaring med escaperom

Figur 5.3 viser at nesten halvparten av respondentene på spørreundersøkelsen har vært i et escaperom tidligere.

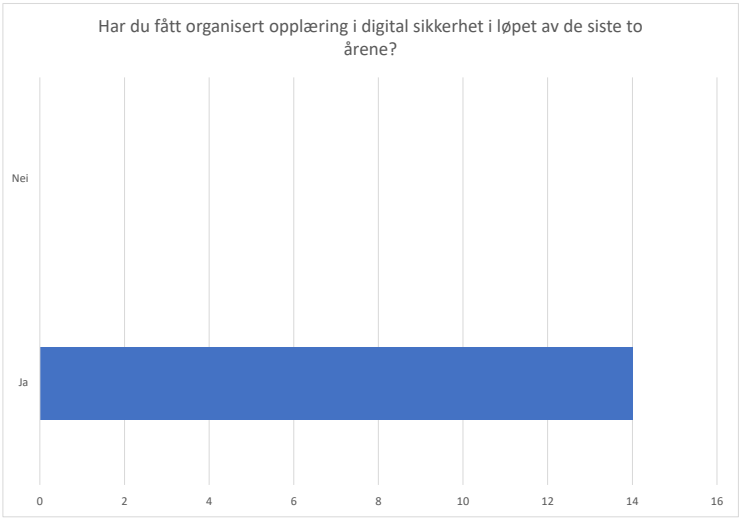


Figur 5.3: Spørsmål: Har du vært i et escaperom tidligere?

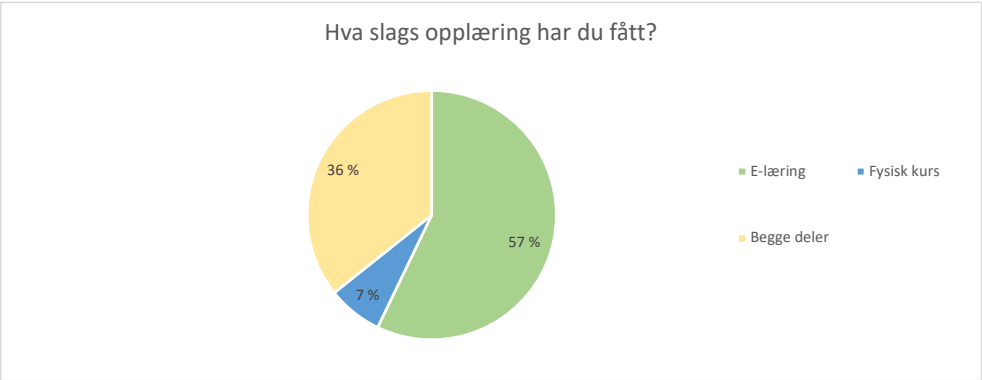
5.2.4 Tidligere opplæring

Som vist i figur 5.4 oppgir alle de som har svart på spørreundersøkelsen at de har fått organisert opplæring i digital sikkerhet i løpet av de siste to årene. Figur 5.5 viser at 57% av disse har fått opplæring via e-læring, mens 7% oppgir at de har fått opplæring ved hjelp av fysiske kurs. Til slutt oppgir 36% at de har fått opplæring ved hjelp av kombinasjon av e-læring og fysiske kurs.

Totalt har 93% av de ansatte fått opplæring via e-læring, noe som gir et godt sammenligningsgrunnlag når de i post-testen vurderer basisrommet opp mot opplæring de tidligere har fått.



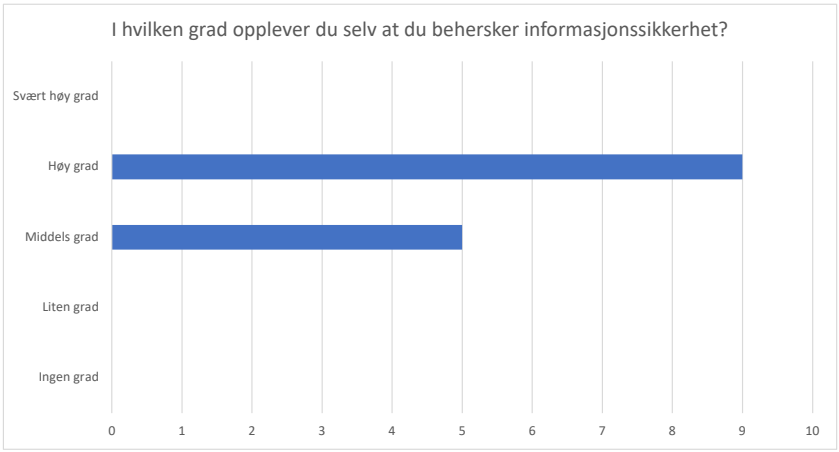
Figur 5.4: Spørsmål: Har du fått organisert opplæring i digital sikkerhet i løpet av de siste to årene?



Figur 5.5: Spørsmål: Hva slags opplæring har du fått?

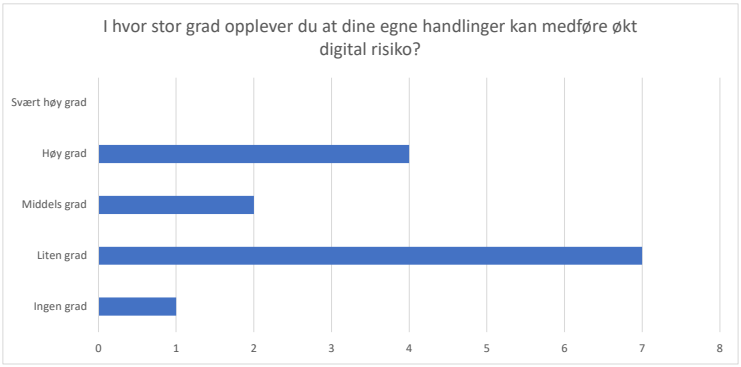
5.2.5 Selvvurdering av kompetanse

Som vist i figuren nedenfor opplever de fleste ansatte i HDO at de behersker informasjonssikkerhet i en middels til høy grad. Det er ingen av de ansatte som har svart at de i liten eller ingen grad behersker informasjonssikkerhet.



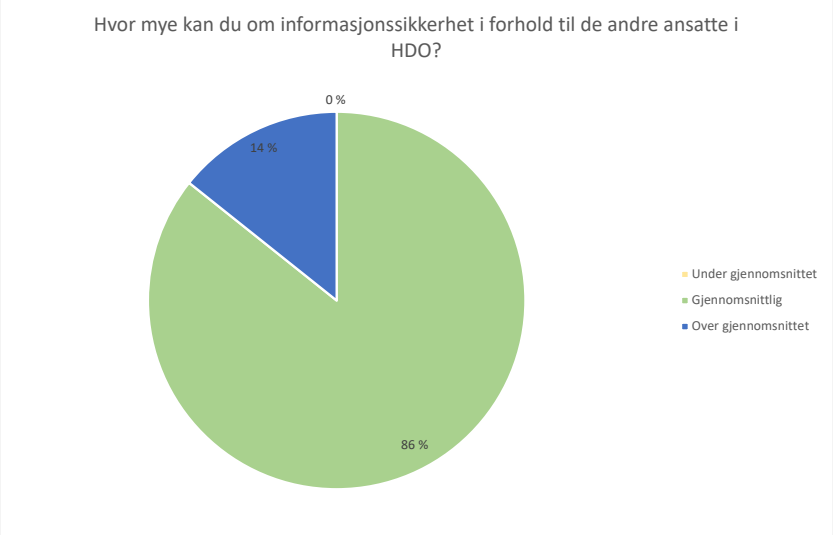
Figur 5.6: Spørsmål: I hvilken grad opplever du selv at du behersker informasjonssikkerhet?

Figuren nedenfor viser at 43% av de ansatte i HDO mener at egne handlinger kan føre til økt digital risiko i middels eller høy grad, men overvekten av de ansatte, 57%, føler at egne handlinger i liten grad kan medføre økt digital risiko. Dette er en nedgang på 13% i forhold til den generelle oppfatningen i den norske befolkningen. I NorSIS sin rapport "Nordmenn og digital sikkerhetskultur" [1], oppgir hele 70% av de som har blitt spurt at den største digitale risikoen er at andre skal gjøre noe mot dem, ikke at de selv gjør noe feil.



Figur 5.7: Spørsmål: I hvor stor grad opplever du at dine egne handlinger kan medføre økt digital risiko?

I 5.8 oppgir de fleste av de som har svart på spørreundersøkelsen at de selv føler at de kan omtrent like mye om informasjonssikkerhet som de andre ansatte i HDO.

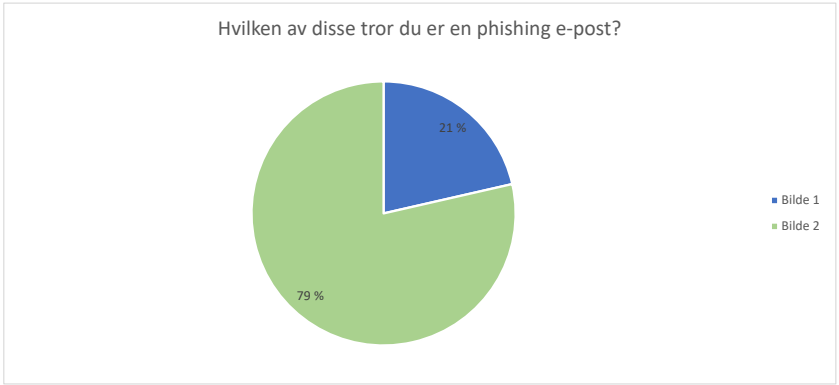


Figur 5.8: Spørsmål: Hvor mye kan du om informasjonssikkerhet i forhold til de andre ansatte i HDO?

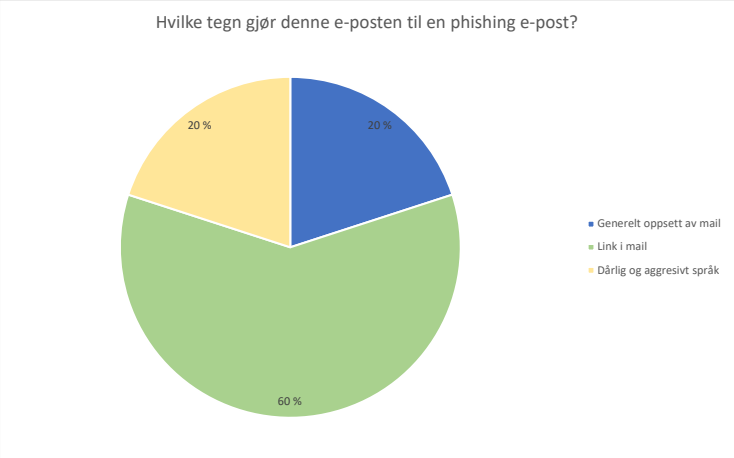
5.2.6 Faglige spørsmål

5.2.6.1 Phishing

I figur 5.9 ble de ansatte bedt om å velge mellom to bilder - bilde 1 var en legitim e-post, mens bilde 2 var en phishing e-post. De aller fleste ansatte - 79% klarte å identifisere hvilken av e-postene som var phishing. En overvekt av de ansatte, 60% oppgir i 5.10 at de kjente igjen phishing e-posten siden det var en link i mailen mottaker ble bedt om følge. I tillegg reagerte de også på at e-posten hadde et dårlig og forholdsvis aggressivt språk, og at det generelle oppsettet av mailen var mistenkelig.



Figur 5.9: Spørsmål: Hvilken av disse tror du er en phishing e-post?



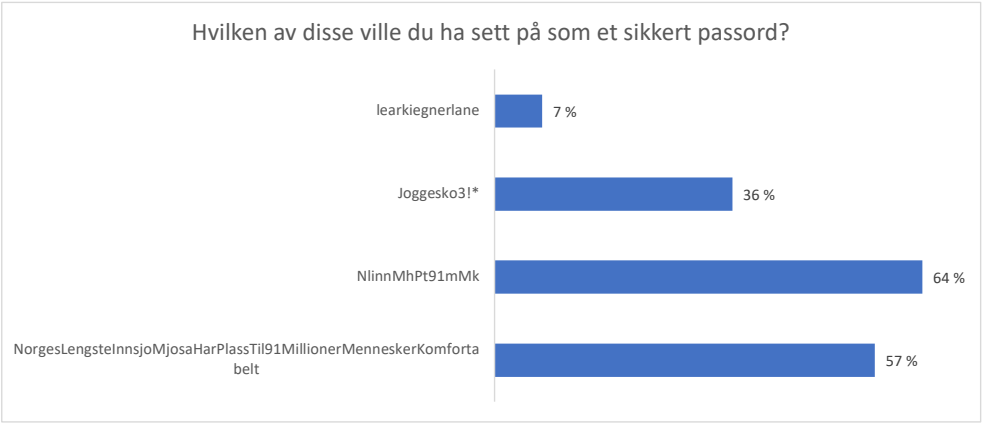
Figur 5.10: Spørsmål: Hvilke tegn gjør denne e-posten til en phishing e-post?

5.2.6.2 Passord

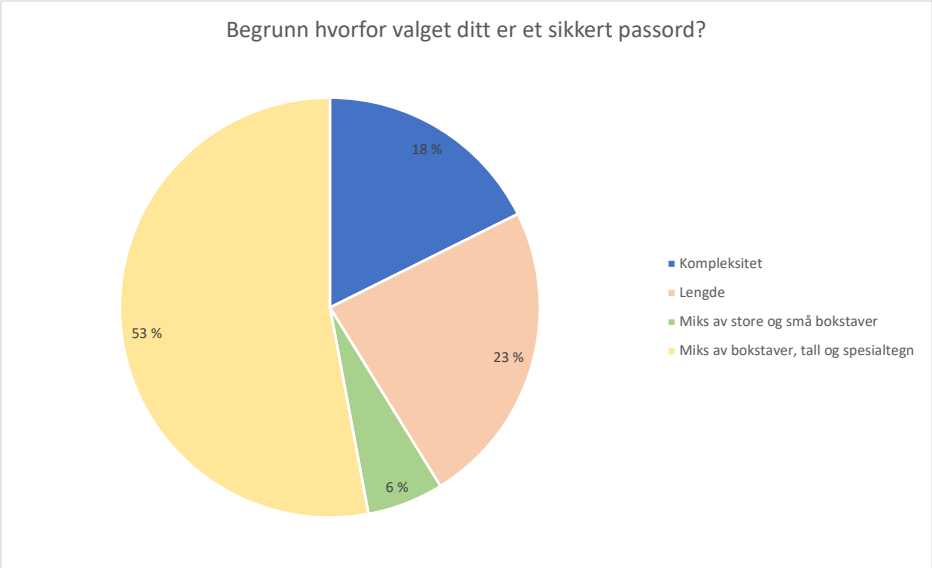
I 5.11 ble de ansatte bedt om å velge hvilke(-n) av passordene under de ville ansett som sikre passord:

- learkiegnerlane
- Joggesko3!*
- NlinnMhPt91mMk
- NorgesLengsteInnsjoMjosaHarPlassTil91MillionerMenneskerKomfortabelt

Passordet som blir ansett som tryggest av alternativene de fikk er "NlinnMhPt91mMk". I 5.12 oppgir de fleste ansatte at de har valgt de passordene de har på bakgrunn av at det var en kombinasjon av bokstaver, tall og spesialtegn. Det er derfor interessant at de to passordene som blir ansett som tryggest ikke har spesialtegn. Samtidig oppgir henholdsvis 23% og 18% at de også har valgt passordene de har valgt på bakgrunn av lengde og kompleksitet, krav de to tryggeste oppfyller.

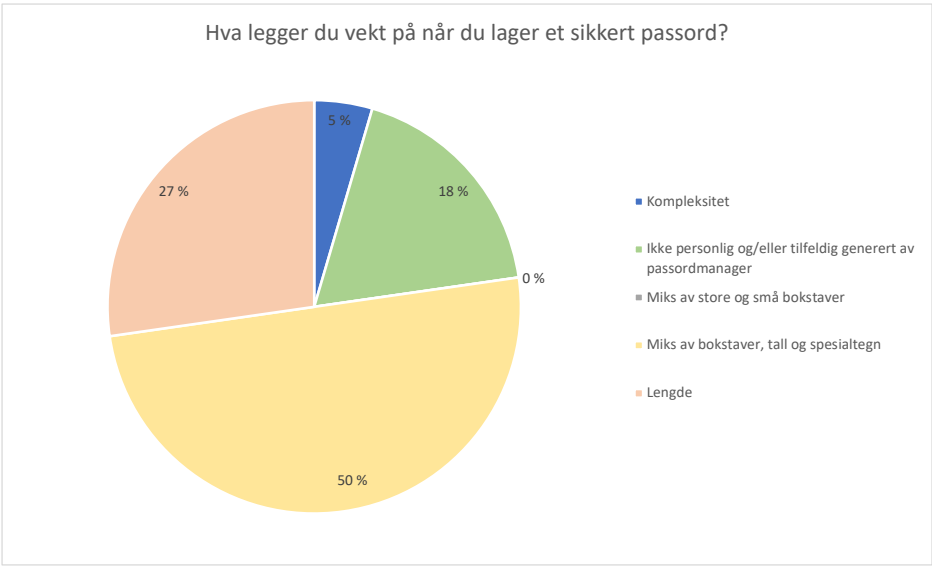


Figur 5.11: Spørsmål: Hvilken av disse ville du ha sett på som et sikkert passord?



Figur 5.12: Spørsmål: Begrunn hvorfor valget ditt er et sikkert passord?

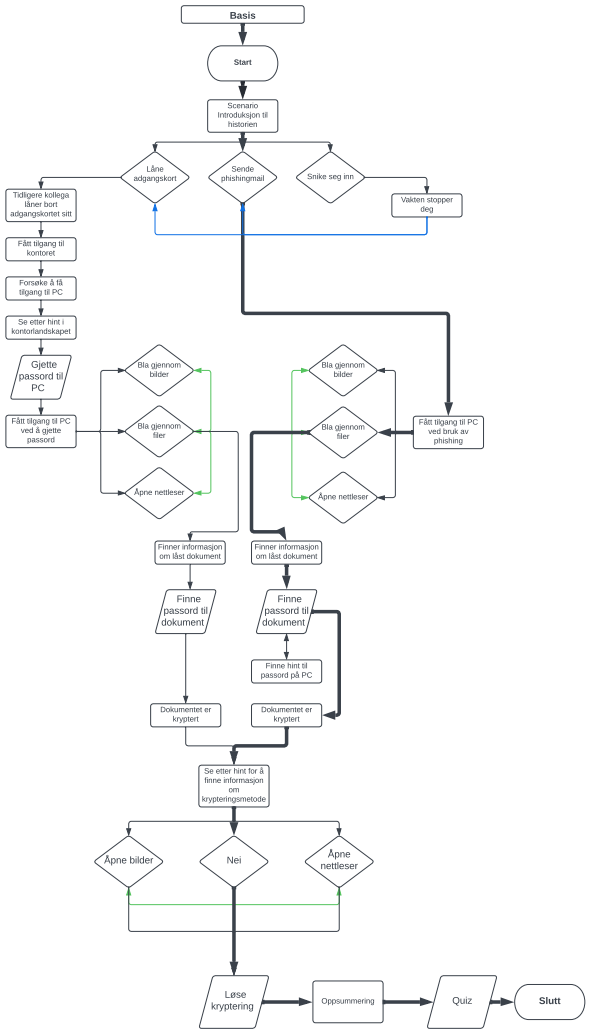
I likhet med 5.12 oppgir de ansatte også i 5.13 at de legger vekt på en miks av bokstaver, tall og spesialtegn når de lager passord. Flere, 27%, sier at de også er opptatt av at passordet skal være langt nok og 18% nevner også at de vektlegger passord som er upersonlig eller tilfeldig generert av en passordmanager.



Figur 5.13: Spørsmål: Hva legger du vekt på når du lager et sikkert passord?

5.3 Resultat av escaperom

Basisrommet sitt første valg er "hva er ditt første steg?" for å komme deg inn i bedriftens systemer. Her valgte alle "send en phishingmail for å få tilgang til sjefens PC". Ved dette valget fikk spillerne kun en passordoppgave, likevel har en person tatt begge passordoppgavene, noe som kan tyde på at personen har trykket på tilbakeknappen. Alle greide passordoppgaven som førte de videre til en krypteringsoppgave som de også har svart riktig på. Basisrommet ble avrundet med en quiz for å oppsummere læringen, og alle quizspørsmålene ble besvart korrekt. Figuren under viser med tykk strek hvilket hendelsesforløp spillerne valgte. Spillerene benyttet seg av hintene "bla igjennom bilder" og "åpne nettleser" som vises med grønne piler, men figuren viser ikke dette da det ikke er relevant for hendelsesforløpet.

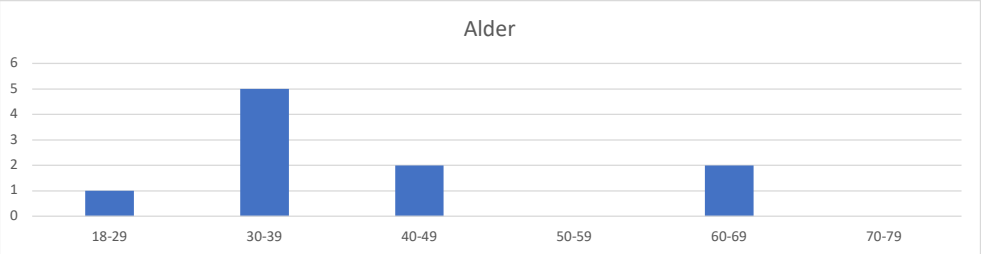


Figur 5.14: Figur som viser hendelsesforløpet spillerne valgte.

5.4 Resultat av post-test

5.4.1 Alder

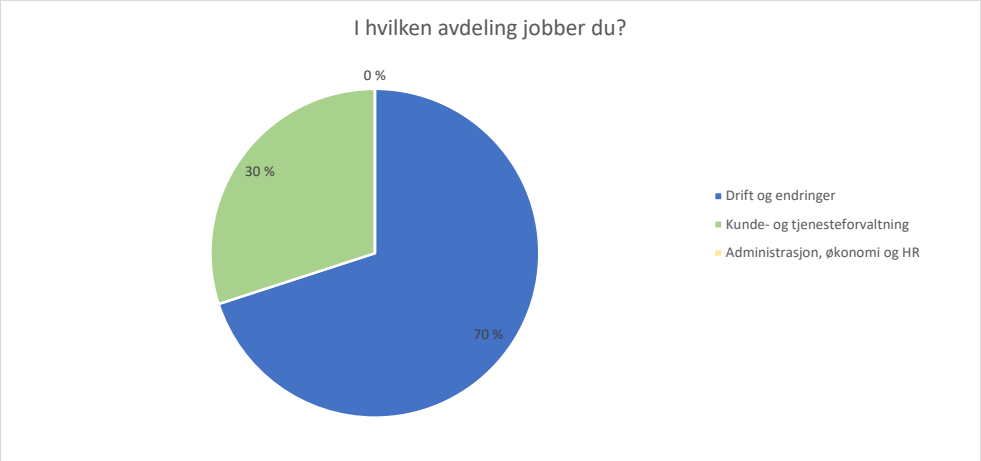
Majoriteten av de ansatte som har tatt post-testen er som i pre-testen i aldersgruppen 30-39 år. På bakgrunn av at det er fire færre svar i post-testen enn i pre-testen er fordelingen ganske lik (reduksjonen er minimal), med unntak av aldersgruppen 50-59 som gikk fra to til null.



Figur 5.15: Spørsmål: Alder

5.4.2 Avdeling

Som illustrert i figur 5.16 har det kommet inn flest svar fra drift og endringer, nest flest fra kunde- og tjenesteforvaltning, henholdsvis 70% og 30%, og ingen svar fra administrasjon, økonomi og HR, noe som gjør at fordelingen på post-testen ikke er representativ for den faktiske fordelingen i HDO.

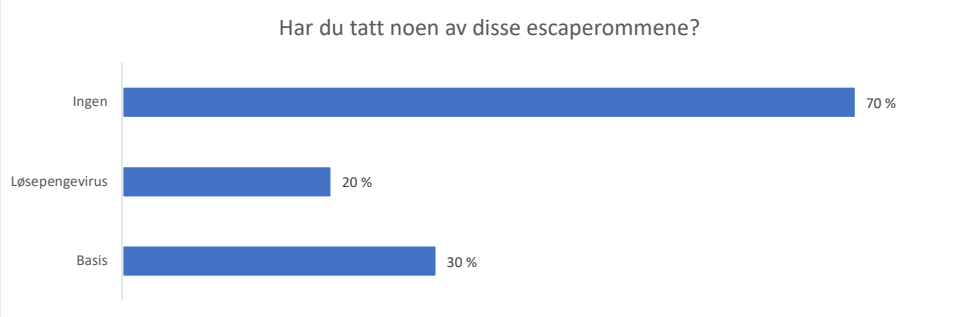


Figur 5.16: Spørsmål: I hvilken avdeling jobber du?

5.4.3 Tidligere escaperom eller spørreundersøkelse

Seks stykker endte opp med å ta pretesten og post-testen, mens fire ikke hadde tatt pre-testen. Syv ansatte svarte på post-testen uten å ha tatt escaperom, mens to tok både basisrommet og løsepengevirus og en person tok bare basis.

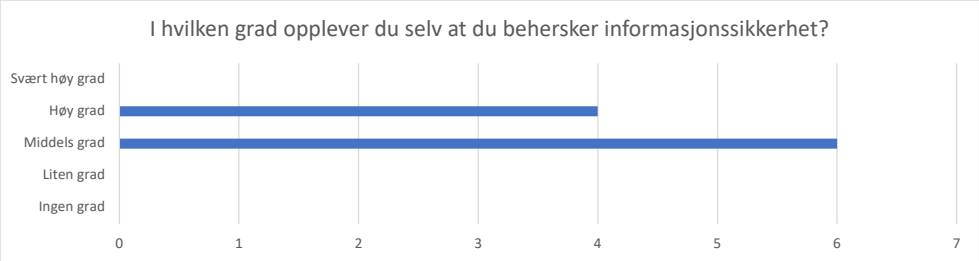
Figur 5.17: Spørsmål: Har du tatt en tidligere spørreundersøkelse fra oss?



Figur 5.18: Spørsmål: Har du tatt noen av disse escaperommene?

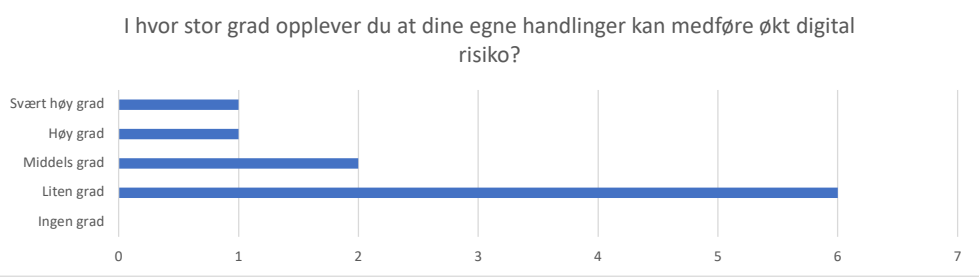
5.4.4 Selvvurdering av kompetanse

Som i pre-testen vurderer de ansatte seg til å beherske informasjonssikkerhet i middels og høy grad. Motsatt av pre-testen er at de fleste har svart middels grad.



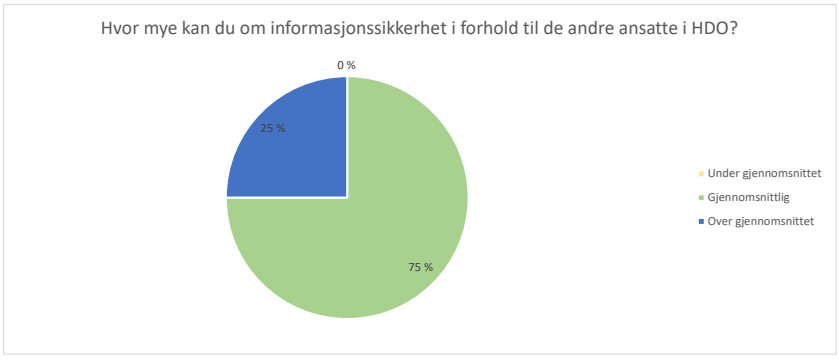
Figur 5.19: Spørsmål: I hvilken grad opplever du selv at du behersker informasjonssikkerhet?

Flesteparten mener fortsatt at deres egne handlinger i liten grad kan medføre digital risiko, men til forskjell fra pre-testen har en svart i svært høy grad og null i ingen grad.



Figur 5.20: Spørsmål: I hvor stor grad opplever du at dine egne handlinger kan medføre økt digital risiko?

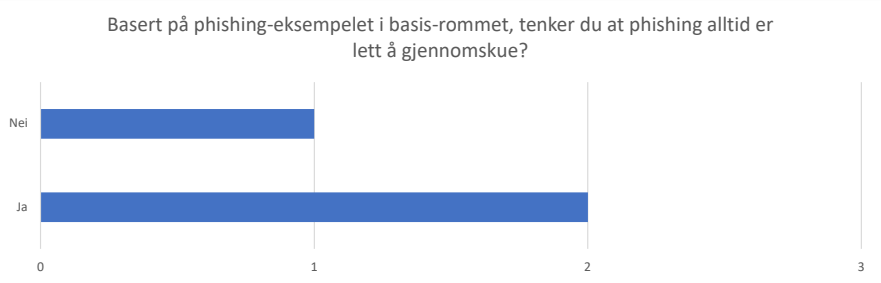
Tre av fire mener at de i forhold til andre i HDO har gjennomsnittlig kunnskap om informasjonssikkerhet, og den siste sier den kan over gjennomsnittet. Fordelingen er vinklet i samme retning som i pre-testen.



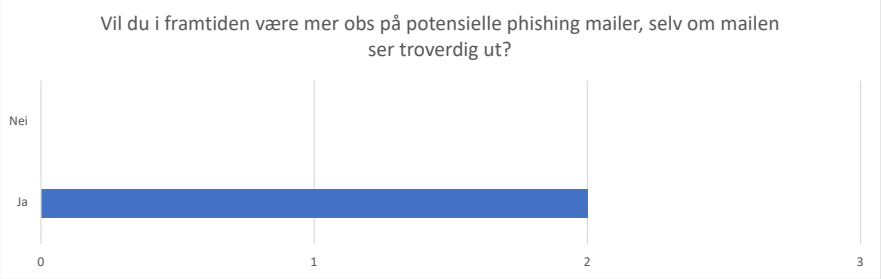
Figur 5.21: Spørsmål: Hvor mye kan du om informasjonssikkerhet i forhold til de andre ansatte i HDO?

5.4.5 Faglige spørsmål:

Av de tre som tok basisrommet mener én at phishing ikke alltid er lett å gjennomskue, mens to mener at det er det. Disse to mener de i framtiden vil være mer oppmerksomme på potensielle mailer, selv om mailen ser troverdig ut.



Figur 5.22: Spørsmål: Basert på phishing-eksempelet i basic-rommet, tenker du at phishing alltid er lett å gjennomskue?

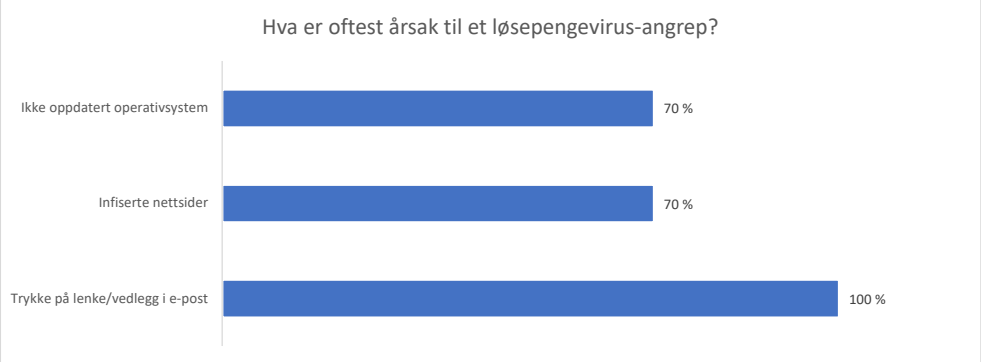


Figur 5.23: Spørsmål: Vil du i framtiden være mer obs på potensielle phishing mailer, selv om mailen ser troverdig ut?

Åtte av ti mener at "din eller næres navn og bursdag", "navnet på hunden din kombinert med dens bursdag" og "navnet på kona og datoen for bryllupsdagen" ikke er lurt å ha med i et passord. De siste to mener at det er "favorittmaten kombinert med flere spesialtegn og en tilfeldig tallsekvens" som ikke er lurt å ha med i et passord.

Figur 5.24: Spørsmål: Passordsikkerhet er viktig - er det noen ting du tenker at det ikke er lurt å ha i et passord?

Figur 5.25 viser at alle mener at å trykke på lenke/vedlegg i e-post er en yppig årsak til et løsepengevirus-angrep. I tillegg mener også syv at et ikke oppdatert operativsystem er en årsak og syv mener også at infiserte nettsider kan være en årsak.



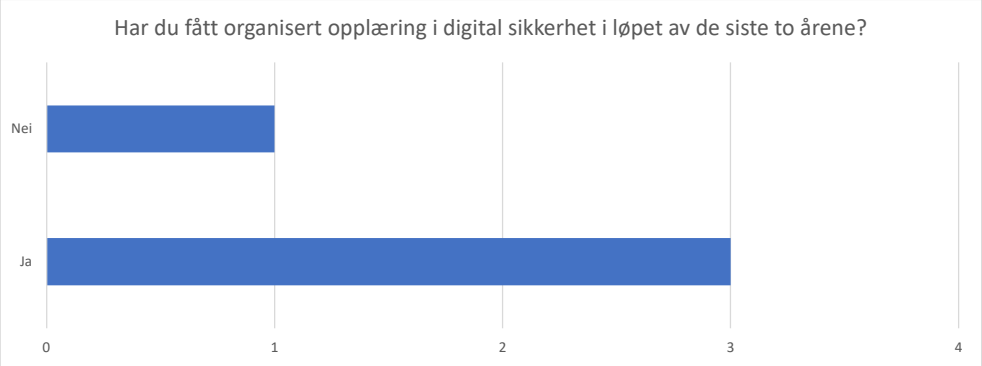
Figur 5.25: Spørsmål: Hva er oftest årsak til et løsepengevirus-angrep?

Spørsmålet under var et åpent spørsmål og det er derfor mye ulike svar. Halvparten mener at å være kritisk til lenker i e-post er et godt tiltak, og 30% mener at å ha et oppdatert operativsystem er viktig. I tillegg er det mange som peker på det å være varsom og årvåken og ha gode rutiner ved bruk av nettsider, usikre kilder og internett.

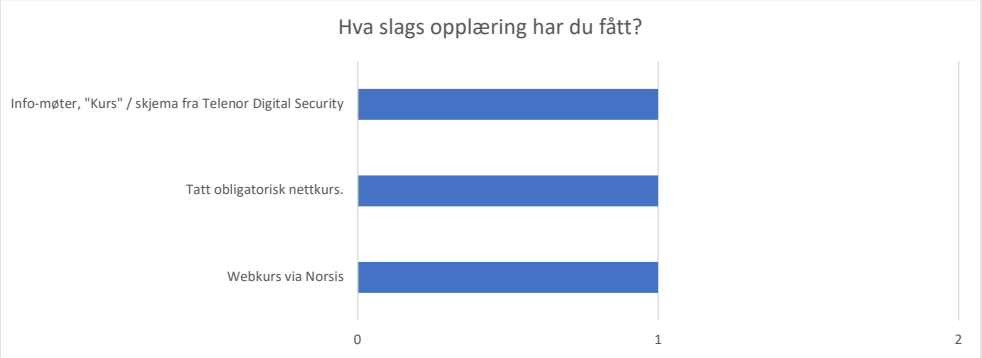
Figur 5.26: Spørsmål: Hva er gode preventive tiltak for å unngå å bli angrepet av et løsepengevirus-angrep?

5.4.6 Generelle spørsmål:

Tre av fire som ikke har tatt pre-testen svarte at de har fått organisert opplæring i løpet av de siste to årene. Den siste har ikke det. Opplæringsmetodene som de tre har fått er Webkurs, Info-møter, og "Kurs"/skjema og obligatorisk nettkurs.

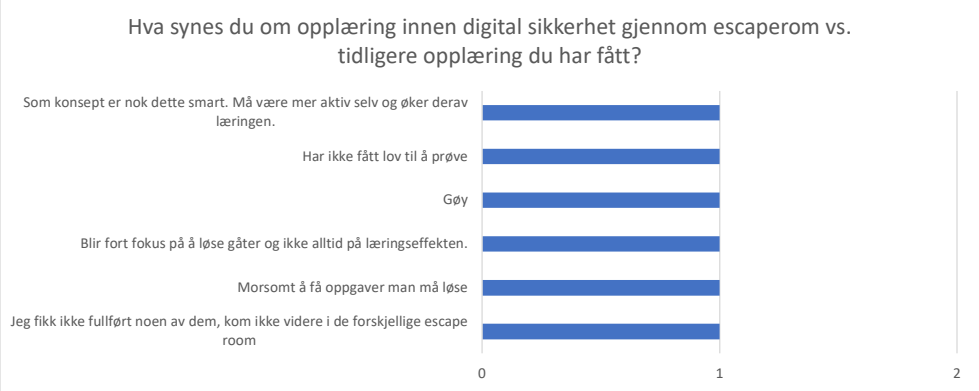


Figur 5.27: Spørsmål: Har du fått organisert opplæring i digital sikkerhet i løpet av de siste to årene?



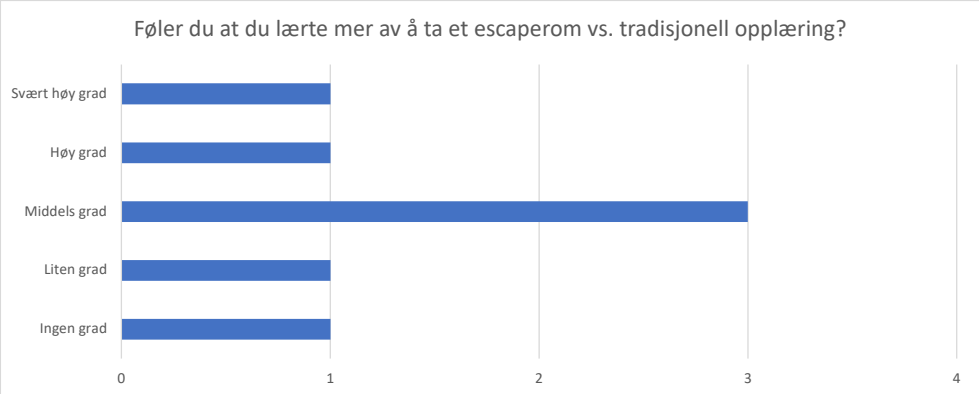
Figur 5.28: Spørsmål: Hva slags opplæring har du fått?

I figur 5.29 kom det flere ulike tilbakemeldinger som rangerer fra at det var "gøy" og "morsomt å få oppgaver man kan løse" til "blir fort fokus på å løse gåter og ikke alltid på læringseffekten" og "jeg fikk ikke fullført noen av dem, kom ikke videre i de forskjellige escape room". Det var også en som skrev "har ikke fått lov til å prøve".



Figur 5.29: Spørsmål: Hva synes du om opplæring innen digital sikkerhet gjennom escaperom vs. tidligere opplæring du har fått?

Figur 5.30 viser at spredningen er stor angående om de følte selv at de lærte mer av å ta et escaperom enn ved tradisjonell opplæring. Tre av syv svarte i middels grad mens på svært høy, høy, liten og ingen grad var det en person på hver.



Figur 5.30: Spørsmål: Føler du at du lærte mer av å ta et escape room vs. tradisjonell opplæring?

Kapittel 6

Diskusjon

6.1 Introduksjon

Diskusjonskapitlet består av flere deler hvor det blir gått igjennom, diskutert og sammenlignet resultater fra post-testen, slik at det kommer frem om escaperommene har hatt en effekt på læringsutbyttet hos de ansatte i HDO. Disse resultatene legger grunnlaget for konklusjonen i kapittel 7 og gruppens svar på problemstillingen. Kapitlet går også inn på refleksjoner som har blitt gjort basert på resultatet av escaperommene. I tillegg går kapitlet inn på hvilke erfaringer gruppen har fått i løpet av prosessen med å skrive bacheloroppgave, hvilke begrensninger gruppen har hatt og hvilket arbeid som kan gjøres videre.

6.2 Begrensninger

6.2.1 Begrensninger ved Google Forms

Google Forms ble den mest hensiktsmessige platformen for å utvikle escaperom. Likevel er det funksjoner Google Forms mangler som det hadde vært nyttig å ha tilgang til for å øke følelsen av å gjennomføre et escaperom og ikke en test, og dermed også øke læringsutbyttet. Gruppen ønsket i utgangspunktet å lage escaperommene som virtuelle rom der man kan bevege en avatar gjennom rommet slik som i Mozilla Hubs for å skape følelsen av å være i et escaperom. Dette er en funksjon gruppen gjerne ønsket å ha med da gruppen tror den positive opplevelsen av rommene hadde økt, og rommet hadde blitt mer interaktivt, og dermed hadde kanskje læringsutbyttet også økt. Det var også et ønske å inkludere lyder (musikk, stemmer) og videoer. I Forms har man mulighet til å lenke til videoer/lydfiler fra andre nettsider, men det kan ikke direkte vises i skjemaet i Forms. Hadde de vært direkte inkludert i Google Forms hadde dette trolig blitt brukt for å øke læringsutbyttet [12].

Andre funksjoner som gruppen savnet i Forms var mulighetene til å sette en tidsbegrensning på ulike oppgaver, fjerne “tilbake”-knappen slik at man ikke kan bevege

seg bakover etter man har tatt et valg og at man kunne hatt en bildekarusell slik at bildene kunne komme ved siden av hverandre istedet for under hverandre. Gruppen ønsket også at Forms kunne være mer interaktivt ved at man for eksempel kan trykke på bildet for å komme til det bildet viser, slik at man kan komme seg videre/rundt i rommet uten å måtte trykke på "neste". Rommene ble utformet så godt de kunne blitt i Google Forms, men det hadde vært ønskelig med flere muligheter, og ideelt sett hadde en blanding av Google Forms og Mozilla Hubs vært en god plattform for å utforme escaperommene.

6.2.2 Begrensninger ved HDO

Ettersom HDO er en mellomstor bedrift med rundt 70 ansatte og ikke alle de ansatte kunne delta i testingen, var gruppen klar over at det ville bli få personer i testgruppene (10 per gruppe). Det som ikke ble forutsett var at responsen på pre-testen, escaperommene og post-testen skulle bli manglende. Oppdragsgiver var ansvarlig for å finne deltagere til disse testene, og selvom de ble sendt ut til 40 stykker tilsammen kom det ikke nok svar. Det ble dermed ikke nok personer i de ulike testgruppene (se figur 6.1).

Escaperommene "nulldagssårbarheten" og "løsepengevirus" ble skreddersydd til HDO og rommene inkluderer derfor informasjon underlagt taushetsplikt. Alt om disse kan derfor ikke skrives om i oppgaven. Dette gjør at også flere spørsmål fra post-testen heller ikke kan inkluderes. I tillegg kunne ikke gruppen personidentifisere de ansatte som tok pre-testen, og kunne derfor ikke følge opp disse i post-testen. Det førte til at gruppen i mindre grad kunne bruke svarene på pre-testen i diskusjonen.

6.2.3 Tidsbegrensninger

Innledningsvis ble det valgt å jobbe med og opparbeide kunnskap om escaperom og utviklingen av dette, da dette var nytt for gruppen. For å utvikle rommene var det en tidsbegrensning og valget ble derfor å prioritere kvalitet i oppgavene og ikke utseende til rommet. På grunn av dette ble det ikke mulig å lage rom helt fra bunnen av.

Etter at HDOs ansatte tok escaperommene kom det tilbakemeldinger som kan benyttes til å videreutvikle rommene. Blant annet var det et ønske om å erstatte risikomatrisen i escaperommet om nulldagssårbarhet, med HDO sin risikomatrise. Disse tilbakemeldingene kom sent i prosessen og det ble derfor ikke mulig for gruppen å implementere endringer da fokuset måtte bli på å skrive rapporten. Hvis tidsrammene hadde hatt rom for det kunne rommene blitt endret slik at læringsutbyttet og opplevelsen hadde blitt enda bedre.

Å få svar på både pre-test, escaperom og post-test viste seg å ta lengre tid enn forventet. Ønskelig skulle de ansatte hos HDO fått mer tid på å gjennomføre de

to sistnevnte slik at det hadde kommet flere resultater. På grunn av bacheloroppgavens innleveringsfrist 20. mai ble denne tiden begrenset.

6.2.4 Begrensninger av Covid-19

Den 13. desember 2021 kom regjeringen med nye koronatiltak for å begrense smitten i samfunnet [32]. Disse skulle vare i minst fire uker og gruppen var forberedt på en digital start på bacheloroppgaven. Gruppen har sittet sammen på skolen under hele bachelorskrivingen, samt hatt digitale møter med veileder og oppdragsgiver. De fleste i HDO har også hatt hjemmekontor i vår og det har vært få fysisk på jobb.

Covid-19 har ikke begrenset arbeidet mellom gruppemedlemmene, men det har begrenset resultatene. Hadde HDO sine ansatte ikke vært på hjemmekontor hadde det vært mulig å gjennomføre testingen med gruppen fysisk til stede på et bestemt tidspunkt. Dette hadde potensielt gitt flere svar da deltagerne hadde vært samlet og måtte sitte til de var ferdige, samt at de ville hatt mulighet til å få hjelp. Slik kunne det potensielt blitt flere svar. Dette ville også gitt resultatene på samme tidspunkt, noe som hadde vært mer tidseffektivt.

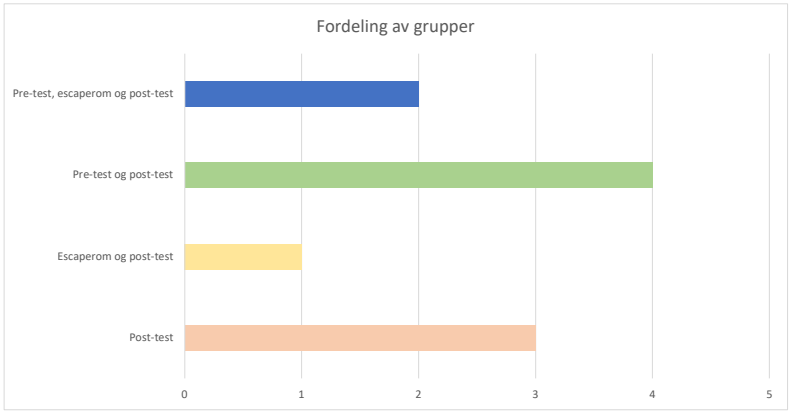
6.3 Resultater

6.3.1 Introduksjon

Denne delen går igjennom og sammenligner post-test-resultatene fra kapittel 5 for å se om escaperommet har hatt en effekt. Grafene i de påfølgende seksjonene er delt inn i de fire gruppene fra design 5:

- **Gruppe 1:** Pre-test, escaperom og post-test
- **Gruppe 2:** Pre-test og post-test
- **Gruppe 3:** Escaperom og post-test
- **Gruppe 4:** Post-test

Antallsfordelingen på hver gruppe er illustrert i Figur 6.1 nedenfor. Fargene i grafene vil konsistent representere de samme gruppene gjennom kapittelet.



Figur 6.1: Fordeling av grupper

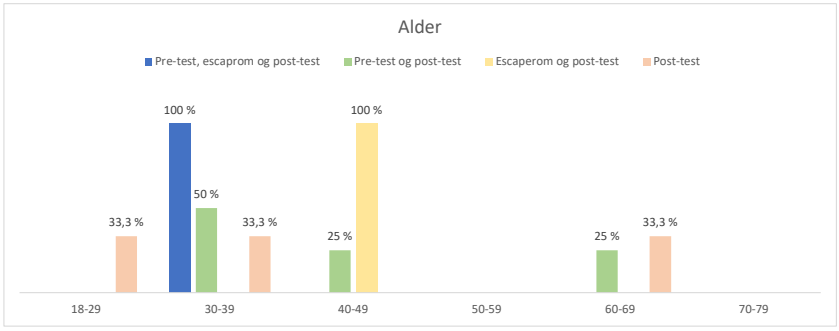
I gruppe 1 var det to deltagere, i gruppe 2 var det fire deltagere, i gruppe 3 var det en deltager og i gruppe 4 var det tre deltagere. I design 5 er det lagt opp til at testgruppene skal ha tilnærmet likt antall deltagere, men på grunn av for få svar ble ikke dette oppnådd.

6.3.2 Innledende spørsmål

Som vist i figur 6.2 er deltagerne generelt spredt over flere aldersintervaller, men hvis man ser på de enkelte designgruppene er det mindre spredt. Kun ansatte i aldersintervallene 30-39 og 40-49 tok escaperom (gruppe 1 og 3). Gruppe 2 og 4 har en jevnere og bredere aldersfordeling. Dette kan være fordi antall deltagere i disse gruppen er høyere enn i gruppe 1 og 3.

De fleste deltagerene ligger i intervallene 30-39 år og 40-49 år og rundt her blir aldersgjennomsnittet. Dette samsvarer med antagelsen fra gruppens kontaktperson om at snittalderen i HDO er 35-45 år (se 3.3.3).

Ideelt sett skulle det vært deltagere i aldersintervallet 50-59 år, og flere aldersintervaller burde ha tatt escaperom for at resultatene skulle representert HDO på en bedre måte. Forskjellige aldersgrupper kan ha forskjellig erfaring med digitale spill, og dermed hadde en tilbakemelding fra et bredere utvalg vært mer optimalt.

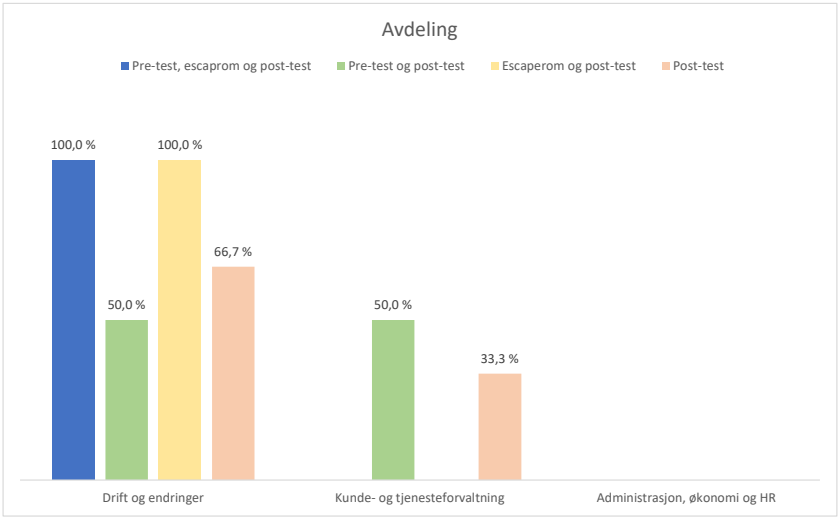


Figur 6.2: Alder

Som vist i figur 6.3 Avdeling var avdelingen drift og endringer representert i alle designgruppene. Fra avdelingen kunde- og tjenesteforvaltning var det kun deltagere i designgruppene 2 og 4, og fra administrasjon, økonomi og HR var det ingen deltagere.

Figur 3.2 viser at HDO består av rundt 70 ansatte der 10% jobber på administrasjon, økonomi og HR, 33% på kunde- og tjenesteforvaltning og 57% på drift og endringer. Målet var å få resultater som var representative for hele HDO, men da kun ansatte på drift og endringer tok escaperom, ble resultatene av dets effekt lite representative.

En grunn til at det var flest deltagere fra drift og endringer til sammen, og at også bare deltagere fra denne avdelingen tok escaperom, kan være at 2/3 av de som fikk muligheten til å delta i testen var fra denne avdelingen. I tillegg er dette den største avdelingen i HDO. En annen teori er at drift og endringer består av IT-personell og det kan tenkes at disse er mer selvsikre innenfor digital sikkerhet og mer engasjerte på team og dermed tryggere på å gjennomføre testene/escaperom.



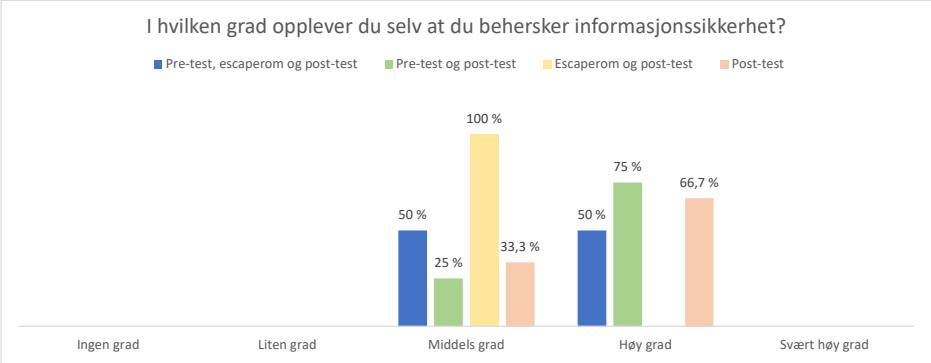
Figur 6.3: Avdeling

6.3.3 Selvvurderingsspørsmål

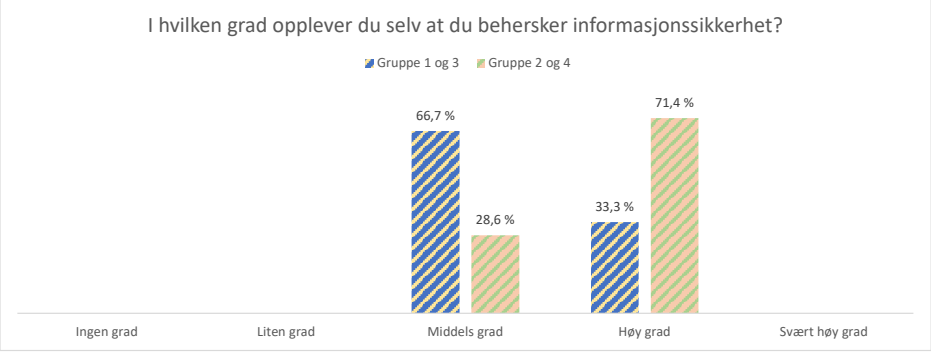
Figur 6.4 viser svarsfordelingen på spørsmålet "i hvilken grad opplever du selv at du behersker informasjonssikkerhet?". Alle svarene ligger på middels til høy grad. Svarene viser at 2/3 som har tatt escaperom opplever i middels grad at de behersker informasjonssikkerhet, og 1/3 i høy grad (se figur 6.5). Av de som ikke har tatt escaperom er disse svarene motsatt, altså mener flesteparten, 5/7, at de i høy grad behersker informasjonssikkerhet, og 2/7 mener i middels grad.

Utifra dette kan man se at opplevelse av behersking av informasjonssikkerhet er lavere blant de som tok escaperom. Dette kan tyde på at escaperom hjelper spillerne å innse at informasjonssikkerhet kan være mer komplisert enn de først hadde antatt. Det kan også tyde på at spillerne ikke fikk til escaperommet og av den grunn føler de behersker det i mindre grad.

At svarene ligger såpass høyt kan også være fordi HDO har en stor avdeling for drift og endringer med hovedsakelig IT-ansatte, og som man kan se i 6.3 avdeling er det flest deltagere fra denne avdelingen med i testen. Hadde de andre avdelingene vært mer representert kan det tenkes at gruppen hadde sett en jevnere fordeling i svaralternativene.



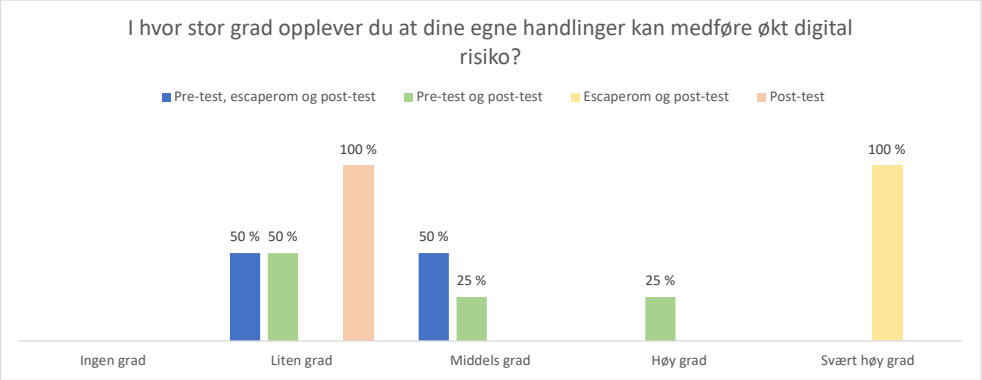
Figur 6.4: I hvilken grad opplever du selv at du behersker informasjonssikkerhet?



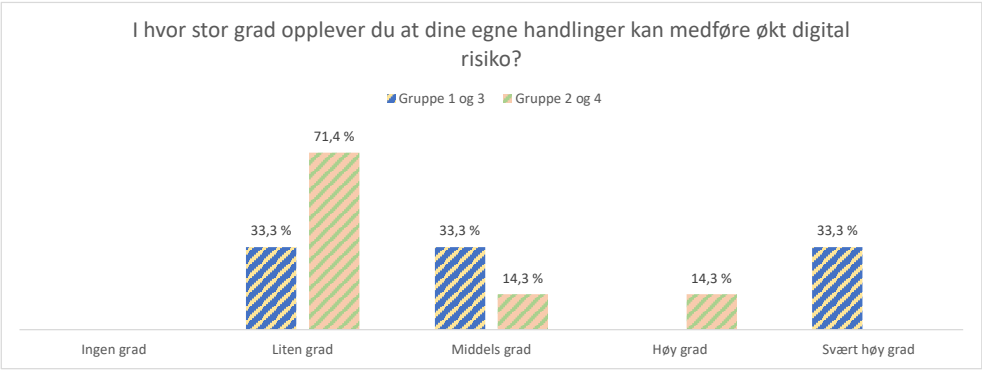
Figur 6.5: Gruppe 1 og 3 og Gruppe 2 og 4

Figur 6.6 viser svarfordelingen på spørsmålet "i hvor stor grad opplever du at dine egne handlinger kan medføre økt digital risiko?". Generelt lener svarene seg mot i middels til liten grad, utenom én person som mener at sine egne handliner kan medføre økt digital risiko i høy grad og én i svært høy grad. Denne personen som har svart i svært høy grad har tatt escaperom, men ikke pre-test. Den andre gruppen som har tatt escaperom (og pre-test), gruppe 1, ligger på liten og middels grad. Fordi det bare er en person i gruppe 3 kan ikke gruppen si noe for sikkert, men en teori når man sammenligner gruppe 1 og 3 kan være at å få det samme spørsmålet i pre-testen har en effekt som tilsynelatende gjør at deltagerne i mindre grad opplever at egne handlinger kan føre til økt digital risiko.

Ved å sammenligne gruppene som har tatt escaperom med de som ikke har tatt escaperom ser man at gruppe 1 og 3 har en spredt, men jevn fordeling, mens gruppe 2 og 4 har en overvekt av deltagere som mener at deres egne handlinger i liten grad medfører økt digital risiko. Dette kan bety at escaperommet har hatt en opplysende effekt på egne handlinger.



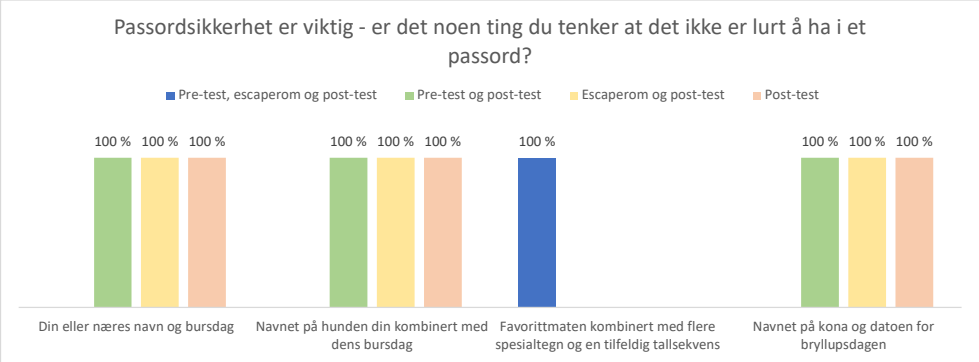
Figur 6.6: I hvor stor grad opplever du at dine egne handlinger kan medføre økt digital risiko?



Figur 6.7: Gruppe 1 og 3 og Gruppe 2 og 4

6.3.4 Faglige spørsmål:

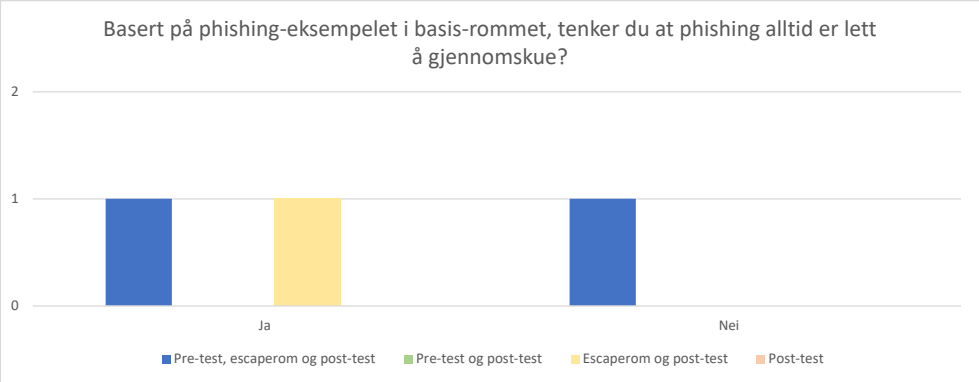
Figur 6.8 viser fordelingen av svar i passordsikkerhetsspørsmålet som er et flervalgsspørsmål. Det er kun gruppe 1 som svarte forskjellig fra de andre. Denne gruppen er kun to personer og de resterende åtte svarte alle det samme. Da dette spørsmålet ble utformet var det ikke ønskelig at man åpenbart skulle se det riktige svaralternativet, men hvis det var en av alternativene som man ikke skulle huke av på så var det tiltenkt at det var alternativ tre; "favorittmaten kombinert med flere spesialtegn og en tilfeldig tallsekvens". Dette er fordi dette svaralternativet inneholder spesialtegn, bokstaver og tall. Når åtte deltagere svarer riktig og de to siste, som har tatt escaperom, svarer det motsatte kan man teoretisere om at de to misforstod spørsmålet. Dette kan tenkes fordi det i basisrommet kommer frem at spesielt alternativ fire er et dårlig passord. Med dette i bakhodet og det faktum at den tredje personen som har gjennomført escaperom har svart riktig (gruppe 3), har det trolig vært en misforståelse av spørsmålet, og ikke et tilfelle mislykket læring.



Figur 6.8: Passordsikkerhet er viktig - er det noen ting du tenker at det ikke er lurt å ha i et passord? Svar fordelt på de ulike gruppene.

Figur 6.9 viser at gruppe 1 sine to svar er fordelt med et på "ja" og et på "nei" til at phishing er lett å gjennomskue. Den siste personen som tok escaperom (men ikke pre-test), altså gruppe 3, mener også at phishing alltid er lett å gjennomskue. Dette resultatet er mangelfullt da det bare ble stilt til de som tok escaperommet, noe som var en feil fra gruppens side. Det er derfor vanskelig å si noe om escaperommets effekt på opplæring om phishing da det ikke kan sammenlignes med gruppe 2 og 4 som ikke fikk opplæringen. I tillegg var ikke phishingoppgaven i basisrommet en interaktiv oppgave, og dette kan ha hatt en påvirking på resultatet.

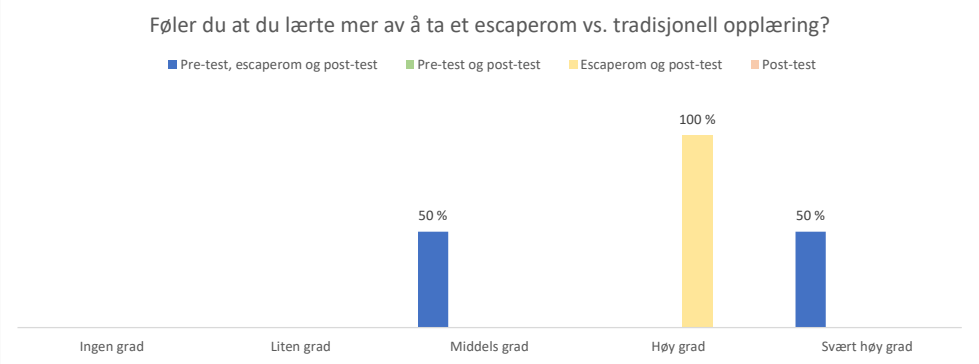
Dette spørsmålet var ment som et faglig spørsmål for å teste deltagernes phishingkunnskaper, men i ettertid fremstår det mer som et subjektivt spørsmål. Om escaperommet har hatt en påvirkning på deltagernes phishingkunnskaper er derfor usikkert.



Figur 6.9: Basert på phishing-eksempelet i basisrommet, tenker du at phishing alltid er lett å gjennomskue? Svar fordelt på de som har tatt escaperom.

6.3.5 Generelle spørsmål

Alle som tok escaperom oppgir at de i middels til høy grad føler de fikk mer ut av opplæring gjennom escaperom vs. tradisjonell opplæring. Dette er svært positivt. De fra gruppe 1 mener i henholdsvis middels grad og svært høy grad at de fikk mer ut av escaperom, mens den fra gruppe 3 fikk i høy grad mer ut av escaperom vs. tradisjonell opplæring.



Figur 6.10: Føler du at du lærte mer av å ta et escaperom vs. tradisjonell opplæring?

6.3.5.1 Tilbakemeldinger:

I post-testen ble spørsmålet "hva synes du om opplæring innen digital sikkerhet gjennom escaperom vs. tidligere opplæring du har fått?" stilt, og gruppen fikk flere ulike tilbakemeldinger:

- Gøy.
- Morsomt å få oppgaver man må løse.
- Blir fort fokus på å løse gåter og ikke alltid på læringseffekten.
- Som konsept er nok dette smart. Må være mer aktiv selv og øker derav læringen.
- Jeg fikk ikke fullført noen av dem, kom ikke videre i de forskjellige escape room.
- Har ikke fått lov til å prøve

De tre øverste tilbakemeldingene er fra deltagere som har tatt escaperom og de tre siste er fra deltagere som har ikke tatt escaperom. En av disse skrev "har ikke fått lov til å prøve". Det er ukjent hvorfor vedkommende ikke fikk lov til å prøve. En annen fikk ikke fullført escaperommene som kan tyde på at det var for vanskelig, eventuelt at det ikke var gode nok hint. En annen teori er at personen ikke var kjent med escaperom og det dermed ble vanskelig å forstå konseptet og prosessen. Escaperommet burde hatt en informasjonsside om escaperom for å forsøke og hindre dette.

Av tilbakemeldingene fra de som tok escaperommene var det to positive og en konstruktiv. Den konstruktive tilbakemeldingen mente at det ble "fokus på å løse gåter og ikke alltid på læringseffekten". De to positive mente at det var gøy/morsomt. Dette viser at en slik type opplæring kan ende opp med et større fokus på spillet enn læringen, gjerne fordi det er gøy/morsomt og dette blir da fokuset.

Disse tilbakemeldingene er ikke overraskende da målet med seriøse spill er å øke motivasjon gjennom engasjerende spillelementer, samtidig som en bieffekt av dette kan være at spillerne mister fokuset på læringen [14, 16]. Selv om tilbakemeldingene er forståelige er det likevel ikke et ønsket resultat da målet var å utvikle escaperom som unngikk dette. Til tross for at escaperommene ble testet på en liten gruppe og det dermed er vanskelig å si noe sikkert, kan disse tilbakemeldingene være representative for tilbakemeldingene man hadde fått med en større testgruppe.

6.4 Refleksjoner

For å kunne trekke en konklusjon om escaperom sin effekt på læringen til HDO-ansatte, var det ønsket å teste et så representativt utvalg som mulig. Dette skulle inkludere et utvalg fra alle avdelingene i alle aldersgrupper. For pre-testen, det første som ble utsendt, ble dette utvalget relativt representativt selv om kun 14 av 20 svarte.

Deretter skulle escaperommet ideelt blitt tatt av halvparten (syv) som tok pre-testen, og i tillegg av tilsvarende antall som ikke hadde tatt pre-testen. På basisrommet endte gruppen opp med fem svar og løsepengevirus ble testet av tre stykker. For å utføre testingen etter design 5, skulle alle som tok escaperom også ta post-testen og dette ble det gitt beskjed om. Potensielt kunne det dermed vært minst fem i gruppe 1 og 3 tilsammen, men da ikke alle tok post-testen ble det bare tre stykker i disse gruppene. Det er nok flere grunner til at det ble så få svar på escaperommene og på post-testen (10 stykker). Da pre-testen ble utsendt tok det lang tid før det kom svar, se 4.2, og de ansatte fikk derfor lengre tid enn først planlagt. Sammen med at det ble brukt lengre tid på å utforme escaperommene enn planlagt, ble det mindre for deltagerne å teste escaperom og ta post-testen. En annen grunn kan være at folk ikke hadde lyst. Det ble estimert at det ville ta 20-40 minutter, og de ansatte kan ha tenkt at de ikke hadde lyst eller mulighet til å bruke tiden sin på det. Ved å ha mer direkte kontakt med de ansatte, kunne det muligens ha kommet flere svar. Det kunne også blitt satt opp en tid for at alt (pre-test, escaperom og post-test) kunne blitt gjennomført fysisk med gruppen tilstede. Da kunne gruppen lettere hjulpet hvis noen stod fast, og sørget for at alle spillerne greide å gjennomføre da noen av testdeltagerne hadde problemer (se 6.3.5) med å starte og fullføre escaperommet. Som nevnt i begrensninger ville dette ha vært vanskelig da mange i HDO fortsatt var på hjemmekontor.

Gruppen burde vært forbredt på at en alternativ testgruppe kanskje ville være nødvendig. Som nevnt i 6.2.2 var det kjent at det kanskje kunne bli et for lite testutvalg på grunn av HDO sin størrelse, men gruppen var ikke forberedt på hvor få responser det ble. Hvis dette utfallet hadde blitt tatt hensyn til fra starten av, kunne andre personer blitt hentet inn for å teste basisrommet slik at det hadde blitt nok responser både på testene og selve escaperommet. Dog ville dette ført til endringer på målgruppen for basisrommet.

Resultatene er delt i tre deler; selvvurdering, faglige og generelle. Noen av spørsmålene fra post-testen har ikke blitt inkludert på grunn av taushetsplikten ovenfor HDO. Dette gjorde at det er få resultater å trekke en konklusjon fra. De to selvvurderingsspørsmålene som er inkludert er; “i hvilken grad opplever du selv at du behersker informasjonssikkerhet?” og “i hvor stor grad opplever du at dine egne handlinger kan medføre økt digital risiko?”. Disse er ment som en subjektiv vurdering av de ansattes kunnskap. De faglige spørsmålene handler om

passordsikkerhet og phishing og er ment som en faglig og objektiv vurdering av læringsutbyttet til de ansatte. De generelle spørsmålene handlet om opplæring i escaperom vs. tradisjonell/tidligere opplæring. Av spørsmålene som er inkludert, er det i etterkant tydelig at det bare er spørsmålet om passordsikkerhet som ikke er et selvvurderingsspørsmål. Dette gjør at grunnlaget for en konklusjon om hvorvidt escaperom er et effektivt virkemiddel for å lære om dagens trusler innen cybersikkerhet eller ikke, i hovedsak blir basert på synsing fra deltagerne da selvvurderingsspørsmål hovedsakelig peker på egen følelse av kunnskap [17].

I tillegg til at spørsmålene i testene er få og selvvurderingsbaserte, er det i ettertid tydelig at også spørsmålene fra post-testen er mangelfulle. Dette skjedde fordi spørsmålene fra pre-testen var mangelfulle, og da post-testen skal være relativt lik pre-testen for at resultatene fra disse skal kunne sammenlignes, ble det dessverre sånn. Det burde vært flere faglige spørsmål med høyere og mer varierende vanskelighetsgrad. Dette ville gitt et bedre bilde på hvorvidt escaperommet hadde en effekt på læringen eller ikke. Uavhengig av hvor gode spørsmålene var, kunne ikke pre-testen brukes til å avkrefte at den hadde effekt på kunnskapen til de ansatte eller ikke, og oppgaven har derfor lav intern gyldighet i resultatene. Dette var på grunn av HDOs begrensninger som ikke var medregnet før starten av testingen. Det var nemlig ingen måte å være sikker på at nok personer fra hver designgruppe tok escaperom og post-testen, da det var ukjent hvem som tok pre-testen. For å løse dette måtte escaperom og post-test utsendes til de som hadde fått pre-testen (uavhengig om de tok den eller ikke) og gruppen måtte håpe på det beste. Dette er en nok hovedgrunnen til at designgruppene ble så ulike på antall.

I utgangspunktet var det ønskelig å teste alle tre escaperommene fordi de var ganske ulike og det ville vært interessant å se hvilket oppsett på rommet folk likte best. Kun basis og løsepengevirus endte opp med å bli testet for å gi HDO mulighet til å kjøre nulldagssårbarhet som en felles opplæringsøvelse i etterkant. I ettertid kan man reflektere over hvorvidt det var hensiktsmessig å teste to rom, spesielt når det var så få testdeltagere. Da ikke alle tok alle rommene ble gruppe 1 og 3 teoretisk sett delt i to, fordi resultatene fra basis og løsepengevirus måtte bearbeides hver for seg. Dette gjorde at gruppen fikk flere testgrupper enn tiltenkt. Gruppen burde også ha tenkt at på at på grunn av taushetsplikten er det mange resultater fra løsepengevirus og nulldagssårbarhet som ikke kunne tas med i oppgaven. Samtidig ble det tenkt at basisrommet ville være for enkelt kunnskapsmessig for noen, kanskje spesielt på avdelingen drift og endringer. Hvis kun basisrommet hadde blitt testet, hadde kanskje ikke disse resultatene vært representative for escaperommene som var skreddersydd til HDO.

6.5 Erfaringer knyttet til prosess

Prosessen med å skrive bacheloroppgave har vært mer utfordrende enn antatt og det er flere grunner til dette. Blant annet var oppgaven veldig åpen. Dette er i utgangspunktet veldig positivt, men det førte til få retningslinjer som gjorde det vanskelig å starte prosessen med å lage rommene på grunn av usikkerhet knyttet til innhold. I tillegg ble prosessen mer iterativ enn antatt - grensen mellom prosessene ble mer flytende enn tenkt og flere prosesser ble slått sammen. I tillegg, i stedet for å fullføre én prosess, ble gruppen gående fram og tilbake mellom flere prosesser da nye idéer stadig ble introdusert og oppgavens innhold oppdatert. Under utviklingen av escaperomene fungerte ikke alt slik det var tenkt, og det måtte endres på oppgaver, hendelsesforløp og selve romdesignet. I tillegg ble tilbakemeldinger fra veileder, oppdragsgiver og Grethe Østby tatt i betrakning.

Det oppdaterte Gantt-skjema - vedlegg D, viser at flere av de planlagte prosessene ble forlenget og slått sammen, og at de overlapper mer enn originalt planlagt. Prosessen med å finne innhold og å designe escaperommene ble endelig avsluttet 8. april. Implementasjon, inkludert pre-test og ferdigstilling av escaperommene ble avsluttet 22. april. Evaluering, herunder testing av escaperommene, post-test og sammenfatning av resultatene ble fullført 8. mai. Førsteutkastet av bacheloroppgaven var også ferdig til 8. mai slik at den kunne leses gjennom av veiledere. Selve oppgaven ble endelig ferdigstilt 18. mai, slik at det gjensto kun å lese over og generering av forside før selve innleveringen 20. mai.

Alt i alt, selv om prosessen ble mer iterativ enn antatt og nye tidsfrister ble satt, har gruppen holdt et godt tidskjema. Hovedutfordringen har vært å få nok ansatte i HDO til å ta pre-test og post-test, og ikke minst selve escaperommene. Dette fordi HDO ønsker å bruke escaperommene til opplæring ved en senere anledning, noe som ga oppgaven et dårligere grunnlag for konklusjon enn ønsket. Dette kunne ha blitt løst ved å sette av mer tid, spesielt til testing av escaperommene og post-testen, men dette ville gått utover innholdet i escaperommene.

6.6 Videre arbeid

Uavhengig av resultatene bør escaperommene testes på en større gruppe mennesker da oppgavens resultat kun er basert på en liten testgruppe. En eventuell større testing bør foregå med en observatør til stede for å veilede, informere, observere og sørge for at deltagerne ikke tar snarveier, som for eksempel tilbake-knappen.

I tillegg bør det gjøres undersøkelser på hvorvidt escaperom gjør at brukere tilegner seg mer eller mindre læringsutbytte, enn ved andre typer e-læring og/eller fysisk læring. Det å utvikle escaperom krever både tid og kompetanse, og resulterer i et sluttprodukt som skal gjennomføres relativt raskt og kun kan gjøres én gang. Det kan derfor være lurt å undersøke om kostnadene av denne utviklingen er verdt den eventuelle læringseffekten, eller om mer tradisjonelle former for e-læring eller fysisk læring - som man gjerne er vant med fra tidligere, blir like effektivt.

Det finnes rammeverk for fysiske escaperom til utdanning, men ikke til virtuelle. Selvom denne oppgaven utviklet et rammeverk for virtuelle escaperom til utdanning basert på SERF og EscapED, er det rom for videreutvikling og testing av dette. Et slikt rammeverk kan eventuelt innlemmes i en spillplattform for utdanningsescaperom. Det vil være flere fordeler med en slik platform; det kan inkludere maler for oppgaver slik at det vil være lettere å utvikle escaperom og det kan utvikles slik at team-arbeid blir en naturlig del av opplevelsen. For at disse oppgavemalene skal gi grunnlag for effektive læringsoppgaver bør det gjøres mer forskning på hvilke elementer som gir effektiv læring i digitale spill. Her bør også kostnad vs. effekt vurderes.

Kapittel 7

Konklusjon

Den første hypotesen var: “Escaperom kan være et effektivt virkemiddel for å lære om dagens trusler innen cybersikkerhet”. Basert på resultatet av testene kan dette verken bekreftes eller avkreftes. Som nevnt i 6.4 ble det stilt for få spørsmål i både pre- og post-testen, i tillegg til at testene fikk for få svar. Dette gjør at det - i tillegg til at hypotesen ikke kan bekreftes eller avkreftes, heller ikke kan bli gjort antagelser om hva resultatet ville vært.

Den andre hypotesen var: “Ansatte føler at de lærer mer om cybersikkerhet ved bruk av escaperom enn ved tradisjonell opplæring”. Igjen er det vanskelig å bekrefte eller avkrefte denne hypotesen, da spørsmålene som ble stilt i testene var for få og upresise kombinert med dårlig respons på både testene og escaperommet. Responsen testene fikk var positiv, og basert på dette tyder det på at hypotesen kan stemme, men det vil kreves mer testing for å kunne endelig bekrefte den.

I tillegg til hypotesene hadde gruppen følgende forskningsspørsmål:

- **F1:** Hvordan kan et escaperom utformes for å være et effektivt virkemiddel i opplæring?
- **F2:** Hva er dagens trusler innen cybersikkerhet?

Forskningsspørsmålene omhandler opplæring, utforming og innhold i escaperomene. Det første forskningsspørsmålet omhandler teorien brukt for å utforme og legge til rette for effektiv opplæring via escaperom. Dette ble gjort ved å tilpasse og slå sammen rammeverkene nevnt i 2.4.2 til et rammeverk som er tilpasset virtuelle escaperom og målgruppen. Det har blitt brukt flere elementer som ble dratt frem i 2.4.1 som positive for enkeltindividers læring. Eksempelvis ble det implementert illustrasjoner både i form av hint og gåter. I escaperomene om løsepengevirus og nulldagssårbarheten er det lagt opp til oppgaver hvor brukerne - hvis de velger å ta rommene i felleskap, kan diskutere hva de bør gjøre videre og hva de skal svare på de forskjellige oppgavene. Det har også vært et fokus på at

det skal være en rød tråd gjennom hvert av rommene, slik at historien brukeren blir fortalt gir mening fra start til slutt. På denne måten har det blitt lagt til rette for at visuelle, auditive og kinestetiske lærere skal få et utbytte av escaperommene.

Det andre forskningsspørsmålet fokuserer på å identifisere hvilke cybersikkerhetstrusler dagens samfunn står ovenfor. Artiklene og rapportene i 2.5 peker på flere ulike trusler, men noen gjennomgående temaer i flere av de er trusler som løsepengevirus, phishing og nulldagssårbarheter. Flere av artiklene peker på at trusselaktiviteten øker, noe som gjør det enda viktigere for både bedrifter og de ansatte i bedriften å være sitt ansvar bevisst, slik at alle kan være med på å forhindre fremtidige sikkerhetshendelser. Temaene nevnt ovenfor har derfor vært hovedfokuset i de tre escaperommene gruppen har laget.

Etter gruppens mening har det blitt utformet escaperom som kan være et effektivt virkemiddel i opplæring, samtidig som det også kan ha et dagsaktuelt fokus på cybersikkerhet. Men på grunn av problematikken rundt pre- og post-testen nevnt i 6.4, kan hvorvidt denne meningen faktisk stemmer ikke verifiseres.

Det var også et mål å oppnå følgende effekt- og resultatmål:

- **E1:** Øke sikkerheten ved å øke kompetansen hos de ansatte i bedriften.
- **E2:** Øke interessen for sikkerhet hos alle ansatte, også hos de som ikke jobber med sikkerhet.
- **E3:** Redusere risikoen for uønskede hendelser relatert til innholdet i escaperommene.
- **R1:** Lage opplæringsmateriell som er dagsaktuelt og legger til rette for effektiv læring.
- **R2:** Utarbeide 3 opplæringspakker, hvorav én er skreddersydd til HDO sin tjenesteportefølje.
- **R3:** Måle effekten av escaperommene.

Effektmålene er igjen, i likhet med hypotesene, noe som verken kan bekreftes eller avkreftes at har blitt oppnådd. Resultatene gjør at man ikke kan konkludere om kompetansen eller interessen for cybersikkerhet hos de ansatte i HDO har økt. På grunn av dette kan det ikke konkluderes med at escaperommene har redusert risikoen for sikkerhetshendelser.

Basert på resultat av forskningsspørsmålene er det usikkert hvorvidt gruppen har oppnådd det første eller tredje resultatmålet. Men det har blitt laget tre escaperom, hvorav to har vært skreddersydd til HDO. HDO har dermed fått to escaperom som er relevante for jobben de gjør og verktøyene de benytter til daglig.

Til slutt, problemstillingen var følgende: "Kan virtuelle escaperom være et effektivt virkemiddel for å lære om dagens trusler innen cybersikkerhet?"

Alt i alt, er det ikke mulig å bekrefte hvorvidt escaperom kan være et effektivt virkemiddel for å lære om dagsaktuelle trusler innen cybersikkerhet basert på gruppens tester. Men basert på de få tilbakemeldingene gruppen fikk, virker det som escaperom kan være både et effektivt og morsomt virkemiddel for å lære andre om cybersikkerhet. Det vil kreves omfattende testing for å verifisere hvorvidt de positive tilbakemeldingene vil være i fler- eller mindretall, og for å bekrefte eller avkrefte om escaperom som læringsverktøy faktisk øker kompetanse og/eller interesse innenfor cybersikkerhet.

Bibliografi

[1] NorSIS. «Nordmenn og digital sikkerhetskultur 2021,» NorSIS - Norsk senter for informasjonssikring. (2021), adresse: https://norsis.no/wp-content/uploads/1637/76/NorSIS_Nordmenn_og_digital_sikkerhetskultur_2021_Web.pdf (sjekket 19.01.2022).

[2] S. Nicholson. «Peeking behind the locked door: A survey of escape room facilities.» (2015), adresse: http://scottnicholson.com/pubs/erfacwhite.pdf (sjekket 25.01.2022).

[3] V. W. Haagensen. «Østre Toten kan få kjempegebyr etter at de ble hacka,» NRK. (apr. 2021), adresse: https://www.nrk.no/innlandet/ostre-toten-kan-bade-bli-erstatningsansvarlig-og-fa-gebyr-etter-at-persondata-kom-pa-avveie-1.15446840 (sjekket 29.01.2022).

[4] D. Shala. «Datainnbruddet mot Stortinget er ferdig etterforsket,» PST. (des. 2020), adresse: https://www.pst.no/alle-artikler/pressemeldinger/datainnbruddet-mot-stortinget-er-ferdig-etterforsket/ (sjekket 29.01.2022).

[5] H. Stolt-Nielsen og M. Lysberg. «Nytt datainnbrudd på Stortinget: To dataangrep på tre uker. Her ble det første angrepet avdekket.,» Aftenposten. (sep. 2021), adresse: https://www.aftenposten.no/norge/i/G304k9/to-dataangrep-paa-tre-uker-paa-stortinget-kontaktnettverk-norske-stand (sjekket 29.01.2022).

[6] E. A. Solhaug. «(+) Alvoret gikk opp for Marius (33) og kollegene da de leste meldingen fra hackerne: – Du føler deg jo helt hjelpeløs når noe sånt skjer,» Toten Idag. (okt. 2021), adresse: https://www.totenidag.no/alvoret-gikk-opp-for-marius-33-og-kollegene-da-de-leste-meldingen-fra-hackerne-du-foler-deg-jo-helt-hjelpelos-nar-noe-sant-skjer/f/5-109-58703 (sjekket 29.01.2022).

[7] Bokmålsordboka. «effektiv,» Språkrådet og Universitetet i Bergen. (), adresse: https://ordbokene.no/bm,nn/search?q=effektiv&scope=ei (sjekket 22.04.2022).

[8] S. Clarke, D. J. Peel, S. Arnab, L. Morini, H. Keegan og O. Wood. «escapED: A Framework for Creating Educational Escape Rooms and Interactive Games For Higher/Further Education.» (2017), adresse: http://dx.doi.org/10.17083/ijsg.v4i3.180 (sjekket 14.02.2022).

[9] J. C. Snyder, «A Framework and Exploration of a Cybersecurity Education Escape Room,» 2018. adresse: http://hdl.lib.byu.edu/1877/etd10312 (sjekket 02.02.2022).

[10] A. G. Erlingsen. «Adaptive and Gamified Learning Technologies to Support Motivation and Engagement.» (2021), adresse: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2829215 (sjekket 03.05.2022).

[11] G. Games. «What are serious games?» Grendel games. (), adresse: https://grendelgames.com/what-are-serious-games/ (sjekket 04.04.2022).

[12] T. M. T. Nguyen. «An exploration on using a storytelling game in history education.» (2021), adresse: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2977293 (sjekket 04.04.2022).

[13] S. S. Noesgaard og R. Ørngreen. «The Effectiveness of E-Learning: An Explorative and Integrative Review of the Definitions, Methodologies and Factors that Promote e-Learning Effectiveness.» (2015), adresse: https://files.eric.ed.gov/fulltext/EJ1062121.pdf (sjekket 01.05.2022).

[14] G. Games. «Serious games, gamification and game-based learning: what's the difference?» Grendel Games. (), adresse: https://grendelgames.com/serious-games-gamification-and-game-based-learning-whats-the-difference/ (sjekket 01.05.2022).

[15] V. Guillén-Nieto og M. Aleson-Carbonell. «Serious games and learning effectiveness: The case of It's a Deal!» (2012), adresse: https://doi.org/10.1016/j.compedu.2011.07.015 (sjekket 13.05.2022).

[16] D. Eng. «Weaknesses of Games Based Learning.» (2019), adresse: https://www.universityxp.com/blog/2019/10/23/weaknesses-of-games-based-learning (sjekket 15.05.2022).

[17] M. B. Roozeboom, G. Visschedijk og E. Oprins. «The effectiveness of three serious games measuring generic learning features.» (2015), adresse: https://bera-journals.onlinelibrary.wiley.com/doi/full/10.1111/bjet.12342 (sjekket 13.05.2022).

[18] Study.com. «John Dewey on Education: Impact & Theory,» Study.com. (2019), adresse: https://study.com/academy/lesson/john-dewey-on-education-impact-theory.html (sjekket 11.05.2022).

[19] S. Nicholson. «Ask Why: Creating a Better Player Experience through Environmental Storytelling and Consistency in Escape Room Design.» (2016), adresse: https://scottnicholson.com/pubs/askwhy.pdf (sjekket 27.02.2022).

[20] Mozilla. «Welcome to Hubs,» Mozilla. (), adresse: https://hubs.mozilla.com/docs/welcome.html (sjekket 22.04.2022).

[21] G. LLC. «How to use Google Forms,» Google LLC. (), adresse: https://support.google.com/a/users/answer/9917017?visit_id=637871902946864306-573820301&rd=1 (sjekket 22.04.2022).

[22] Etterretningstjenesten. «Fokus 2022,» E-tjenesten. (2022), adresse: https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Fokus-2022-til-web.pdf/_/attachment/inline/ec6bec00-d2d3-41c0-af08-02b3b494e8b7:e4014ab4d0e3bd8b2509e7974430fe121e0473ba/Fokus-2022-til-web.pdf (sjekket 19.03.2022).

[23] P. sikkerhetstjeneste. «Nasjonal trusselvurdering 2022,» PST. (2022), adresse: https://www.pst.no/globalassets/ntv/2022/nasjonal-trusselvurdering-2022-pa-norsk.pdf (sjekket 19.03.2022).

[24] N. sikkerhetsråd. «Mørketallsundersøkelsen 2020,» Næringslivets sikkerhetsråd. (2020), adresse: https://www.nsr-org.no/uploads/documents/Publikasjoner/Morketalls-2020-web.pdf (sjekket 19.03.2022).

[25] N. sikkerhetsmyndighet. «Risiko 2022,» NSM. (2022), adresse: https://nsm.no/getfile.php/137798-1644424185/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf (sjekket 19.03.2022).

[26] NorSIS. «Trusler og trender 2021,» NorSIS - Norsk senter for informasjonssikring. (2021), adresse: https://norsis.no/wp-content/uploads/2021/03/NorSIS_Trusler_Trender_2021_Digital.pdf (sjekket 19.03.2022).

[27] P. D. Leedy og J. E. Ormrod, *Practical Research: Planning and Design, Global Edition*. Pearson Education Limited, 2015.

[28] G. Andersen. «Valg av forskningsmetode.» (2019), adresse: https://ndla.no/nb/subject:1:54b1727c-2d91-4512-901c-8434e13339b4/topic:2:432baee9-5671-47ce-870e-48b8fc3b7a42/topic:2:7d43618f-5198-4b32-9e3f-74c7d73ffb27/resource:1:56937 (sjekket 29.04.2022).

[29] N. ved Universitetet i Oslo, Universitetet i Oslo. (2022), adresse: https://nettskjema.no/ (sjekket 10.05.2022).

[30] ENISA. «Capture-The-Flag Competitions: all you ever wanted to know!» ENISA. (2021), adresse: https://www.enisa.europa.eu/news/enisa-news/capture-the-flag-competitions-all-you-ever-wanted-to-know (sjekket 04.05.2022).

[31] T. Bårdgård. «Kryptering,» Nasjonal Digital Læringsarena. (2020), adresse: https://ndla.no/nb/subject:1:81b3892a-78e7-4e43-bc31-fd5f8a5090e7/topic:2:04bfbcd4-889a-4539-86f1-2ddc6acc039c/resource:d26d52da-e727-40d7-b925-4dd622880ab9 (sjekket 04.05.2022).

[32] Regjeringen. «Strengere nasjonale tiltak for å begrense smitten,» Regjeringen. (2021), adresse: https://www.regjeringen.no/no/dokumentarkiv/regjeringen-stoere/utdaterte-aktueltsaker/smk/strengere-nasjonale-tiltak-for-a-begrense-smitten/id2892042/ (sjekket 13.05.2022).

Vedlegg A

Prosjektavtale

Prosjektavtale mellom NTNU og oppdragsgiver.

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 informasjonssikkerhet og kommunikasjonsteknologi	
Veileder ved NTNU: Shao-Fang Wen e-post og tlf. shao-fang.wen@ntnu.no, +47 40 67 72 80	
Ekstern virksomhet: Helsetjenestens driftsorganisajon for nødnett HF (HDO) Ekstern virksomhet sin kontaktperson, e-post og tlf.: Arnt-Helge Nilsen Øyan, arnt-helgenilsen.oyan@hdo.no, +47 41 04 48 04	
Student: Fødselsdato:	Anett Voldheim Øverstad 13.11.1992
Ev. flere studenter[1] Fødselsdato:	Emma Rønningstad 16.11.1999
Student: Fødselsdato:	Thea Fritzvold Hatlem 05.04.1998

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:	17.01.2022
Sluttdato:	20.05.2022

Oppgavens arbeidstittel er: Opplæringspakker sikkerhetshendelser

[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:

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

Der oppgaven bygger på, eller videreutvikler materiale og/eller metoder (prosjektbakgrunn) som eies av den eksterne, eies prosjektbakgrunnen fortsatt av den eksterne. Hvis studenten

[2] Jf. Lov om opphavsrett til åndsverk mv. av 15.06.2018 § 1

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:		24/01/2022
Ekstern virksomhet: Dato:	Ant Helge N.	25.01.2022
Student: Dato:	Anett V. Qvestad	24/01/2022
Ev. flere studenter	Emma Rønningstad	24/01/2022
	Thea Hatlen	24/01/2022

Vedlegg B

Prosjektplan

Prosjektplan som viser planen for bacheloroppgaven.

NTNU

Kunnskap for en bedre verden

INSTITUTT FOR INFORMASJONSSIKKERHET
OG KOMMUNIKASJONSTEKNOLOGI

DCSG2009
BACHELOROPPGAVE

PROSJEKTPLAN

Thea Fritzvold Hatlem, Emma Rønningstad og Anett Voldheim Øverstad

JANUAR 2022

Innhold

Kapittel 1

Mål og rammer

1.1 Bakgrunn

«Stadig flere nordmenn opplever at de får bedre ferdigheter i digital sikkerhet på nett etter å ha gjennomført opplæring. Samtidig er det slik at hele 68% av nordmenn ikke har fått organisert opplæring i digital sikkerhet i løpet av de siste to årene. Nærmere 3 av 10 nordmenn mener de ikke får tilstrekkelig med informasjon til å vurdere de truslene som finnes på nett. 1 av 10 mener de i liten eller svært liten grad selv er i stand til å vurdere risikoene som møter dem på nettet. Dette er et klart signal at selv om flere får bedre ferdigheter i digital sikkerhet, er det fremdeles en stor gruppe nordmenn som ikke har tilstrekkelige digitale ferdigheter. Spesielt norske arbeidsgivere må ta mer ansvar med å få på plass en god digital sikkerhetskultur – det innebærer blant annet god opplæring.» [1]

Helsetjenestenes driftsorganisasjon for nødnett HF, heretter omtalt som HDO, mener at et viktig aspekt av sikkerhetsholdningen til en organisasjon er som NorSIS peker på: det å utføre regelmessig trening og opplæring. HDO ønsker i denne forbindelsen å få utarbeidet en eller flere opplæringspakker, basert på konseptet «cyber escape rooms», på tvers av ansvar og roller i organisasjonen. Cyber escape rooms er - i likhet med vanlige escape rooms, et spill hvor deltagerne må løse gåter, finne hint og gjøre oppgaver for å løse en eller flere spesifikke oppgaver, men med bakgrunn i informasjon- og cybersikkerhet [2].

HDO ønsker, og dette er også et mål fra oss, at disse skal skape bevisstgjøring rundt sikkerhetshendelser, samtidig som de gir ansatte mestringsfølelse og en mulighet til å bygge relasjoner med hverandre. For å finne innhold til opplæringspakkene vil vi intervjue ansatte og lese trusselvurderinger, slik at vi sikrer at opplæringspakkene er både relevante for HDO, men også dagsaktuelle i henhold til dagens trusselbilde.

Målgruppen for opplæringspakkene er alle ansatte i HDO, uavhengig av stilling og teknisk kompetanse. Dette er både etter oppdragsgiver og vårt eget ønske –

oppdragsgiver ønsker at opplæringspakkene skal få alle opp på et nivå som skaper økt forståelse og tilrettelegger for samarbeid, til tross for ulik kompetanse. For vår egen del anser vi det som viktig at alle ansatte, uavhengig av organisasjon, har en viss kompetanse innenfor informasjonssikkerhet, slik at man forhindrer uønskede sikkerhetshendelser.

1.2 Prosjektmål

Vi har valgt å dele opp mål for prosjektet i to deler: effekt- og resultatmål. Effektmål er de langsiktige målene vi ønsker å oppnå, basert på sluttproduktet vi leverer. Resultatmål er det vi konkret ønsker å levere ved prosjektslutt.

1.2.1 Effektmål

- Øke sikkerheten ved å øke kompetansen i bedriften.
- Øke interessen for sikkerhet hos alle ansatte, også hos de som ikke jobber med sikkerhet.
- Redusere risikoen for uønskede hendelser relatert til innholdet i opplæringspakkene.

1.2.2 Resultatmål

- Lage opplæringsmateriell som er dagsaktuelt og legger til rette for effektiv læring.
- Utarbeide 3 opplæringspakker, hvorav én er skreddersydd til HDO sin tjenesteportefølje.
- Måle effekten av opplæringspakkene.

1.3 Rammer

1.3.1 Tidsmessige rammer

- Prosjektplan og samarbeidsavtale skal være levert og signert innen 31. januar 2022.
- Bacheloroppgaven skal leveres innen 20. mai 2022.

1.3.2 Språkrammer

Selve rapporten og prosjektplanen blir skrevet på norsk, da det ses som mest naturlig siden oppdragsgiver er et norsk foretak og alle intervjuobjektene er norske.

1.3.3 Andre rammer

Rapporten vil bli skrevet i Overleaf – et nettbasert LaTex-verktøy. På grunn av den pågående koronapandemien vil møter og intervjuer bli gjennomført både digitalt via Microsoft Teams og fysisk, avhengig av den lokale smittesituasjonen.

Kapittel 2

Omfang

2.1 Problemområde og problemstilling

I januar 2021 ble Østre Toten kommune utsatt for et løspengevirus, hvor rundt 1800 filer ble lekket på det mørke nettet, cirka 200 av disse filene inneholdt personsensitive opplysninger [3]. Det tok kommunen over et halvt år før alt av systemer og programmer var tilbake til normalen. Stortinget har gjentatte ganger blitt utsatt for dataangrep, hvor det også har blitt hentet ut sensitivt innhold [4, 5]. Både Østre Toten og Stortinget hadde sårbarheter som kunne vært lukket, ved hjelp av opplæring av de ansatte [4, 6].

«Dreiningen til angrep mot mennesker fremfor virksomhetens IT-systemer gjør det enda viktigere at den enkelte ansatte har kompetanse om hvordan svindlere jobber og hva de skal være på vakt mot. Det er de som blir angrepsvektoren, ikke systemet.»[1]

Sitatet fra Norsk senter for informasjonssikring (NorSIS) hjelper med å illustrere hvor viktig det er at ansatte har kompetanse innenfor informasjonssikkerhet. Den fortsatt økende digitaliseringen, gjør at kompetansen til ansatte må øke tilsvarende. Det er derfor viktig at opplæringen ansatte mottar, oppdaterer de ansattes kunnskap i henhold til dagens trusselbilde og skaper en bevisstgjøring hos de ansatte. Cyber escape rooms er en form for e-læring kalt spillifisering – bruken av spillelementer og spilldesign utenfor det som tradisjonelt blir betegnet som spill.

Problemstillingen vår er derfor: Kan cyber escape rooms være et effektivt virkemiddel for å lære om dagens trusler innen cybersikkerhet?

2.2 Problemavgrensning

Oppgaven vil fokusere på preventiv opplæring innenfor informasjonssikkerhet ved hjelp av cyber escape rooms. Målet med opplæring vil være å gi de ansatte innsikt i hva de kan gjøre for å forhindre sikkerhetshendelser hos HDO. For å identifisere relevante trusler og potensielle sikkerhetshendelser hos HDO, vil vi intervjue ansatte.

I tillegg vil vi lese relevante trusselvurderinger for å sikre at opplæringspakkene også er relevante for dagens trusselbilde. De ansatte vil også bli intervjuet for å finne ut hva slags opplæring og kunnskap de allerede har fått innenfor informasjonssikkerhet, og hva de og HDO gjør for å opprettholde denne kunnskapen. Basert på denne informasjon vil vi forsøke å legge innholdet i opplæringspakkene på et nivå som alle vil forstå, og som vil tilrettelegge for samarbeid på tvers av rollene og inngående kunnskap om informasjonssikkerhet i organisasjonen.

Cyber escape rommet vi lager vil være satt opp som et fysisk spill, da vi verken har kompetansen eller tid til å opparbeide oss denne i løpet av tiden vi har til rådighet, som kreves for å lage det virtuelt. Rommet vil derfor måtte jobbes med og utvikles mer senere.

Kapittel 3

Prosjektorganisering

3.1 Roller

- Leder – Anett
- Sekretær – Emma
- Kvalitetssikrer – Thea
- Kildeansvarlig – Emma
- Grupperomsansvarlig – Anett og Thea
- Snacksansvarlig – alle

3.2 Ansvarsfordeling

Felles: Hele gruppen har ansvar for å bidra til å skrive en god oppgave som tilfredsstiller gruppens mål. I tillegg skal gruppemedlemmene føre opp tiden man har brukt på alt bachelorrelatert i et felles Excel-dokument. Når man innhenter informasjon, skal kilden skrives opp i kildedokumentet. Det skal også være en rullerende arbeidsoppgave å lage en presentasjon som oppsummerer ukens arbeid, samt å presentere den til veilederen.

Leder: Lederen skal sørge for fremgang i prosjektet. Det vil være lederens jobb at gruppen overholder frister slik at vi kan levere en god oppgave den 20. Mai. I tillegg vil hun ha hovedansvar for å sette opp og lede møter både internt og med veileder og oppdragsgiver, samt annen kommunikasjon med de to sistnevnte og eventuelt andre.

Sekretær: Sekretæren skal lage møtereferat og notere under møtene med HDO, bachelorveilederen og eventuelt andre, og laste opp dette i Teams.

Kvalitetssikrer: Kvalitetssikreren skal sørge for kvalitet i alt arbeidet som ferdigstilles. Hun vil ha et større ansvarsområde under korrekturlesing av rapporten, samt å sørge for at utformingen til rapporten er sammenhengende, forståelig og estetisk.

Kildeansvarlig: Den kildeansvarlige har ansvar for at alt som brukes av kilder lagres i et kildedokument med datoen informasjonen brukes. Hun må også ha kontroll på hvilken informasjon som uthentes, slik at det blir referert riktig gjennom teksten. I tillegg skal alle kilder siteres i slutten av hovedrapporten med Harvardstil.

Grupperomsansvarlig: Anett har ansvar for å booke grupperom i oddetallsuker og Thea har ansvar for å booke i partallsuker.

Snacksansvarlig: Dette er en rullerende rolle, slik at en person tar med snacks hver torsdag.

3.3 Rutiner

- Timer skal føres inn i en timeliste på Teams, denne skal være oppdatert i slutten av uken.
- Når vi arbeider sammen, skal vi jobbe i 50 minutters økter med 10 minutters pause. Lunsjpausen skal være lengre, på 30-45 minutter.
- Møte med veileder og oppdragsgiver er henholdsvis kl. 9:30-10:00 og 11:00-12:00 på mandager.
- På fredager kl. 14:00 skal vi ha et internt møte hvor vi oppsummerer uken.
- Vi skal jobbe ca. 30 timer i uken, men er klare for å putte inn tiden som trengs for å fullføre det vi skal.
- Vi bruker oppgavesystemet på nettsiden Trello til å fordele oppgaver. Når en oppgave er fullført skal den markeres som fullført, og deretter skal gruppen korrekturlese den før den arkiveres.
- Det er viktig å være åpne, ærlige og si ifra hvis man er misfornøyde med noe på en hyggelig måte.

3.4 Grupperegler

- Vi skal jobbe fra klokken 9-15 med forbehold – dette kan endre seg ettersom vi erfarer hvordan vi best jobber. I tillegg skal det være rom for å dra på forelesinger eller ha andre møter i denne tiden hvis det er nødvendig.
- Vi skal jobbe effektivt mandag til fredag så helgen kan være fri.
- Vi skal møte til avtalt tid.
- Man skal melde ifra hvis man ikke kan delta på avtalte arbeidsøkter på forhånd.

- Når vi skal jobbe skal det være fullt fokus på arbeidet.
- Vi følger timeplanen for uken som vi sammen utarbeider med hensyn til andre møter og forelesinger.
- Oppgaver skal fordeles likt slik at alle bidrar like mye.
- Oppgaver skal gjøres ferdig til avtalt tid, og hvis det ikke er mulig må man si ifra på forhånd.

Kapittel 4

Planlegging, oppfølging og rapportering

4.1 Prosessrammeverk

Vi har valgt å bruke Scrum som vårt prosessrammeverk for prosjektet. For oss er det viktig å kunne gjøre endringer basert på våre observasjoner, eller tilbakemeldinger fra oppdragsgiver/veileder før vi har gått gjennom hele prosessen, noe Scrum gjør mulig ved de ulike sprintene. Vi har sammen diskutert lengden på sprintene og har kommet frem til at ulik sprintlengde passer for ulike perioder. Gjennomførelsen av hver sprint vil planlegges første dagen en ny sprint starter. I tabellen under er oversikten over sprintene våre gjennom prosjektet.

Periode	Antall sprinter	Lengde på sprint
Design	2	1,5 uke
Implementasjon (prototype)	3	1 uke
Krav	1	2 uker
Implementasjon (endelig)	3	1 uke
Evaluering	1	3 uker
Bachelorskriving	1	5 uker

Tabell 4.1: Sprinter

Rollene for modellen er Product Owner, Scrum Leader, Scrum Team og Interessenter. De har vi fylt slik:

- Product Owner – Oppdragsgiver: HDO
- Scrum Leader – Anett
- Scrum Team – Anett, Emma og Thea
- Interessenter – Veileder, NTNU

Det er vanlig å ha en Daily Scrum – et 15 minutter daglig møte hvor progresjonen evalueres. Dette har vi valgt å ikke bruke da vi jobber sammen tre dager i uka og kan diskutere progresjonen (og annet) disse dagene.

4.2 Plan for statusmøter og beslutningspunkter i perioden

4.2.1 Statusmøter

Vi har valgt å ha statusmøter på fredager kl. 14:00 for å oppsummere hvordan uken har vært, hva vi har fått jobbet med og for å diskutere spørsmål eller annet som har kommet den uken. Da får vi også mulighet til å forberede møtene vi skal ha mandager med veileder og oppdragsgiver.

4.2.2 Beslutningspunkter

For oss blir det naturlig å ta beslutninger hver gang vi er ferdig med en periode (se Gantt). Da har vi nådd en milepæl og er klar for en ny periode. Det blir også naturlig for oss å ta beslutninger ettersom de dukker opp. Vi arbeider med oppgaven sammen tre dager i uken og har derfor mulighet til å diskutere og bli enige om eventuelle beslutninger som må tas.

Kapittel 5

Organisering av kvalitetssikring

5.1 Dokumentasjon og standarder

Alt av dokumenter lagres i gruppens team på Teams der kun gruppemedlemmene har tilgang. Dette inkluderer møtereferat, timelister, kildelister, notater, prosjektplanen og bachelorrapporten. Med NTNU-brukerne er dette sikret med to-faktor autentisering. I tillegg vil de større tekstene som prosjektplanen og selve bacheloroppgaven lagres på en minnepenn etter hvert som det blir ferdig og vi fullfører kapitler.

Selve bacheloroppgaven skal skrives i LaTex på nettsiden Overleaf hvor kun gruppen vil ha tilgang på filen. Dermed vil oppgaven vår ligge tre steder; Overleaf, Teams og en minnepenn for å sikre oss mot datatap.

For å fordele oppgaver bruker vi Trello. Med denne nettsiden kan man opprette oppgaver med tidsfrist og fordele de mellom gruppemedlemmene. Ved å bruke dette systemet sørger vi for at alle bidrar, arbeidsmengden er jevnt fordelt, oppgaver blir fullført innen ønsket tid, samt at vi ikke glemmer hva som må gjøres. Når en oppgave er fullført, vil den bli flyttet til en liste for fullførte, men ikke korrekturleste oppgaver slik at gruppen kan lese over før den arkiveres og markeres som ferdig.

For å sikre kvalitet i det som skrives vil vi gjøre god research om temaet som vi kan vise til. Et eksempel på dette er SERF, Snyder Escape Room Framework. Dette er et rammeverk basert på research om læring og escape rooms, og viser hvordan man kan utvikle et godt escape room og hvilke elementer man bør tenke på.

5.2 Plan for inspeksjoner og testing

For å utvikle et produkt eller et konsept som passer til HDO ønsker vi å gjøre god research for å kartlegge demografien og hvilke behov de har med tanke på sikkerhetsopplæring. Opplæringspakkene som blir utviklet skal testes i to runder.

Først skal prototypen testes på studenter, venner og foreldre da dette lar oss dekke en variert gruppe med mennesker. Deretter skal deres tilbakemeldinger brukes for å forbedre opplæringspakkene før de testes på HDO sine ansatte. Dette vil ønskelig skje i uke 9 og 12-13. Ideelt vil begge testrundene foregå fysisk, noe som bør være mulig da det ikke krever nærkontakt med mange mennesker. Smitteregler vil bli tatt hensyn til, og i verste fall kan testingen foregå digitalt.

5.3 Risikoanalyse

Vi har valgt å utarbeide en risikoanalyse for å bevisstgjøre oss selv på ulike risikoer vi kan stå overfor i løpet av prosjektperioden. Vi har også utarbeidet noen tiltak til disse risikosenarioene slik at vi har et oppslagsverk for å raskere kunne løse en eventuell kritisk situasjon. I tabellen nedenfor har vi definert fem nivåer av sannsynlighet og fem nivåer av konsekvens. Det er vanskelig å definere hvert av nivåene helt konkret (f.eks. Sannsynlig = en gang i uken, eller Medium konsekvens = blir forsinket med opptil en uke), da risikosenarioene er relativt ulike. Men ved å se på samlet risiko (lav, middels, høy og svært høy/fargekodene), kan vi se hvor kritisk utfallet blir til hvert enkelt av risikosenarioene.

Når det gjelder tiltak har vi valgt å utforme flest tiltak for de fem første risikosenarioene. Dette er fordi vi ser på dem som mest kritiske, noe som reflekteres i risikoanalysen. Men vi vil også kommentere enkle tiltak for resten av risikoene nederst i dette delkapittelet.

	Svært høy konsekvens	**Stor konsekvens**	**Medium konsekvens**	**Liten konsekvens**	**Ingen konsekvens**
Svært sannsynlig					
Meget sannsynlig		**1, 2**	**3**		
Sannsynlig			**8**	**9, 10**	
Mindre sannsynlig	**4**	**5, 7**			
Usannsynlig	**6**		**11, 12**		

Tabell 5.1: Risikoanalyse
Svært høy: Rød, Høy: Oransje, Middels: Gul, Lav: Grønn

Risiko 1:

Risikoscenario	Avgrenser oss for mye – oppgaven blir for lite avansert
Beskrivelse	Vi får for lavt nivå på oppgaven og det blir dermed lite å reflektere over
Sannsynlighet	Meget sannsynlig
Konsekvens	Stor konsekvens
Samlet risiko	Svært høy

Tabell 5.2: Risiko 1

Tiltak til risiko 1 – Avgrenser oss for mye – oppgaven blir for lite avansert: Her som på risiko 1 og 2 må vi ha et godt scope for oppgaven og en klar problemstilling. Dette risikosenarioet er det motsatte av risiko 2, men for denne gjelder det også å ha ukentlige møter med veileder da han kan fange opp om oppgaven blir for snever. Om vi likevel ser at oppgaven blir for lite avansert er det mulig å dra inn mer faglig innhold og/eller utvide scopet i noen grad.

Risiko 2:

Risikoscenario	Gå utenfor avgrensningene av oppgaven (utenfor scope)
Beskrivelse	Vi beveger oss utenfor de rammene vi har satt for oppgaven og får for mye å gjøre.
Sannsynlighet	Meget sannsynlig
Konsekvens	Stor konsekvens
Samlet risiko	Svært høy

Tabell 5.3: Risiko 2

Tiltak til risiko 2 – Gå utenfor avgrensningene av oppgaven: Denne risikoen krever også at vi setter et godt scope og en klar problemstilling. Vi må være sikre på hva som skal med og ikke for å unngå å gå utenfor avgrensningene vi har satt. Vi har ukentlige møter med veileder, som er et preventivt tiltak da han kan fange opp om vi beveger oss for lagt utenfor oppgaven. Havner vi likevel der at vi har for mye å gjøre bør vi igjen se på hvilke avgrensninger vi satt og gjøre en vurdering om det vi har tatt med er innenfor oppgaven eller om vi bør ta vekk noe.

Risiko 3:

Risikoscenario	Faglig innhold er ikke som forventet
Beskrivelse	Vi har ikke fått inkludert nok fra tidligere pensum og/eller opplæringspakkene er ikke avanserte nok.
Sannsynlighet	Meget sannsynlig
Konsekvens	Medium konsekvens
Samlet risiko	Høy

Tabell 5.4: Risiko 3

Tiltak til risiko 3 – Faglig innhold er ikke som forventet: For å unngå at vi ikke møter våre faglige forventninger til opplæringspakkene vil vi sette et godt scope og en god problemstilling nå i starten av prosjektet. Vi utformer et Gantt-skjema slik at vi har oversikt over tidsfrister, og dermed får tid til å gjøre alt vi har planlagt. Det vil også bli gjort god research på forhånd slik at vi får en oversikt over hva som er rimelig å forvente av faglig innhold. Skulle det skje at vi likevel står ovenfor dette risikosenarioet, vil vi ta et ekstraordinært møte (mulig med veileder) for å diskutere hvordan vi løser problemet. Det er mulig å lage en ny plan for hvordan vi får dratt inn det faglige vi mangler og også legge inn flere timer med arbeid for å få økt det faglige innholdet.

Risiko 4:

Risikoscenario	Datatap
Beskrivelse	Vi mister dokumentasjon, notater, rapporten, mm.
Sannsynlighet	Mindre sannsynlig
Konsekvens	Svært høy konsekvens
Samlet risiko	Høy

Tabell 5.5: Risiko 4

Tiltak til risiko 4 – Datatap: Vi kommer til å lagre dokumentene våre i sky (dvs. Teams og Overleaf). Ved å bruke skylagring unngår vi risikoen ved å miste data ved at våre PC-er blir ødelagt. Vi kommer som sagt til å skrive i LaTeX (Overleaf), men ønsker å ha en backup av alt på Teams. I tillegg kan vi lagre viktige dokumenter på minnepinne eller lokalt på hver av våre PC-er.

Risiko 5:

Risikoscenario	Problemer med oppdragsgiver eller veileder
Beskrivelse	Vi mister kontakt med oppdragsgiver/veileder, eller får lite/ingen hjelp.
Sannsynlighet	Mindre sannsynlig
Konsekvens	Stor konsekvens
Samlet risiko	Middels

Tabell 5.6: Risiko 5

Tiltak til risiko 5 – Problemer med oppdragsgiver eller veileder: Å ha fast avtalte ukentlige møter vil redusere risikoen i dette senarioet. Da vet vi at vi har en tid i uka for å kunne få veiledning og hjelp. Men hvis veileder/oppdragsgiver slutter å møte opp på møtene, eller vi ikke får den hjelpen vi mener vi trenger så kan vi først ta ny kontakt med den det gjelder. Hvis dette ikke hjelper, kan vi ta kontakt med bachelor-ansvarlig for vårt studie og få han til å ta kontakt med veileder/oppdragsgiver.

Risiko 6:

Risikoscenario	Et av medlemmene i teamet blir alvorlig syk
Sannsynlighet	Usannsynlig
Konsekvens	Svært høy konsekvens
Samlet risiko	Middels

Tabell 5.7: Risiko 6

Risiko 7:

Risikoscenario	Et familiemedlem til en i teamet blir alvorlig syk/dør
Sannsynlighet	Mindre sannsynlig
Konsekvens	Stor konsekvens
Samlet risiko	Middels

Tabell 5.8: Risiko 7

Risiko 8:

Risikoscenario	Står fast – kommer oss ikke videre med oppgaven
Sannsynlighet	Sannsynlig
Konsekvens	Medium konsekvens
Samlet risiko	Middels

Tabell 5.9: Risiko 8

Risiko 9:

Risikoscenario	Uenigheter i teamet
Sannsynlighet	Sannsynlig
Konsekvens	Liten konsekvens
Samlet risiko	Lav

Tabell 5.10: Risiko 9

Risiko 10:

Risikoscenario	Forsinkelser med oppgaven
Sannsynlighet	Sannsynlig
Konsekvens	Liten konsekvens
Samlet risiko	Lav

Tabell 5.11: Risiko 10

Risiko 11:

Risikoscenario	Et av medlemmene i teamet bidrar ikke
Sannsynlighet	Usannsynlig
Konsekvens	Medium konsekvens
Samlet risiko	Lav

Tabell 5.12: Risiko 11

Risiko 12:

Risikoscenario	Et av medlemmene i teamet følger ikke de avtalte reglene
Sannsynlighet	Usannsynlig
Konsekvens	Medium konsekvens
Samlet risiko	Lav

Tabell 5.13: Risiko 12

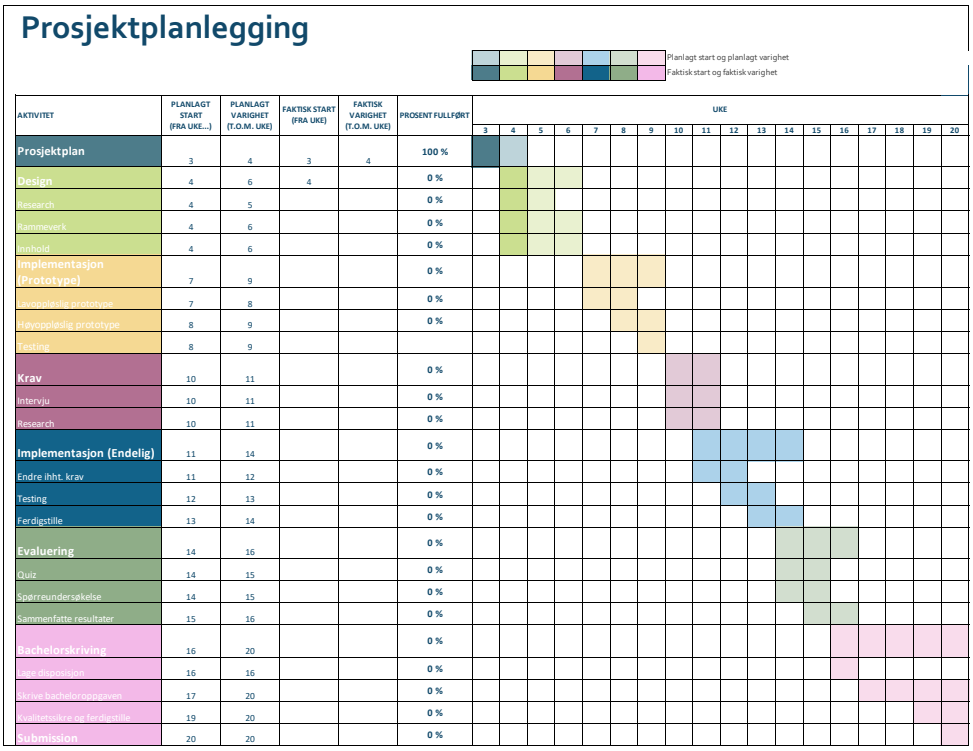
Tiltak for de resterende risikoene (6-12): For risiko 6-12 har vi valgt å ikke utarbeide spesifiserte tiltak til hvert senario da de ligner noe på hverandre, men vil her nevne noen som kan brukes til flere. I tillegg anser vi den samlede risikoen til å være lavere enn på risiko 1-5. For risiko 6 og 7 vil vi gi personen så mye tid som den trenger og de to andre vil prøve å kompensere så godt som mulig i den tiden nr. 3 er borte. For risiko 8, 9 og10 er det viktig at vi lytter godt til hverandres meninger, kommer med konstruktive tilbakemeldinger og prøver å oppmuntre og motivere hverandre slik at vi kommer oss ut av uenigheter/forsinkelser og kommer oss videre med oppgaven. Når det gjelder risiko 11 og 12 vil vi måtte ta et ekstraordinært møte og diskutere hvorfor teammedlemmet ikke følger regler/bidra. Her kan vi også bruke veileder til hjelp om det trengs.

Kapittel 6

Plan for gjennomføring

6.1 Gantt

Vi har utarbeidet et Gantt-skjema for å holde oss innenfor tiden og planlegge hvor mye tid vi kan bruke på de ulike periodene.



Prosjektplanlegging

Planlagt start og planlagt varighet
Faktisk start og faktisk varighet

AKTIVITET	PLANLAGT START (FRA UKE...)	PLANLAGT VARIGHET (T.O.M. UKE)	FAKTISK START (FRA UKE)	FAKTISK VARIGHET (T.O.M. UKE)	PROSENT FULLFØRT	UKE 3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Prosjektplan	3	4	3	4	100 %																		
Design	4	6	4		0 %																		
Research	4	5			0 %																		
Rammeverk	4	6			0 %																		
Innhold	4	6			0 %																		
Implementasjon (Prototype)	7	9			0 %																		
Lavoppløslig prototype	7	8			0 %																		
Høyoppløslig prototype	8	9			0 %																		
Testing	8	9																					
Krav	10	11			0 %																		
Intervju	10	11			0 %																		
Research	10	11			0 %																		
Implementasjon (Endelig)	11	14			0 %																		
Endre ihht. krav	11	12			0 %																		
Testing	12	13			0 %																		
Ferdigstille	13	14			0 %																		
Evaluering	14	16			0 %																		
Quiz	14	15			0 %																		
Spørreundersøkelse	14	15			0 %																		
Sammenfatte resultater	15	16			0 %																		
Bachelorskriving	16	20			0 %																		
Lage disposisjon	16	16			0 %																		
Skrive bakgrunnskapittel	17	20			0 %																		
Kvalitetssikre og ferdigstille	19	20			0 %																		
Submission	20	20			0 %																		

Bibliografi

[1] NorSIS. «Nordmenn og digital sikkerhetskultur 2021,» NorSIS - Norsk senter for informasjonssikring. (2021), adresse: https://norsis.no/wp-content/uploads/1637/76/NorSIS_Nordmenn_og_digital_sikkerhetskultur_2021_Web.pdf (sjekket 19.01.2022).

[2] S. Nicholson. «Peeking behind the locked door: A survey of escape room facilities.» (2015), adresse: http://scottnicholson.com/pubs/erfacwhite.pdf (sjekket 25.01.2022).

[3] V. W. Haagensen. «Østre Toten kan få kjempegebyr etter at de ble hacka,» NRK. (apr. 2021), adresse: https://www.nrk.no/innlandet/ostre-toten-kan-bade-bli-erstatningsansvarlig-og-fa-gebyr-etter-at-persondata-kom-pa-avveie-1.15446840 (sjekket 29.01.2022).

[4] D. Shala. «Datainnbruddet mot Stortinget er ferdig etterforsket,» PST. (des. 2020), adresse: https://www.pst.no/alle-artikler/pressemeldinger/datainnbruddet-mot-stortinget-er-ferdig-etterforsket/ (sjekket 29.01.2022).

[5] H. Stolt-Nielsen og M. Lysberg. «Nytt datainnbrudd på Stortinget: To dataangrep på tre uker. Her ble det første angrepet avdekket.,» Aftenposten. (sep. 2021), adresse: https://www.aftenposten.no/norge/i/G304k9/to-dataangrep-paa-tre-uker-paa-stortinget-kontaktnettverk-norske-stand (sjekket 29.01.2022).

[6] E. A. Solhaug. «(+) Alvoret gikk opp for Marius (33) og kollegene da de leste meldingen fra hackerne: – Du føler deg jo helt hjelpeløs når noe sånt skjer,» Toten Idag. (okt. 2021), adresse: https://www.totenidag.no/alvoret-gikk-opp-for-marius-33-og-kollegene-da-de-leste-meldingen-fra-hackerne-du-foler-deg-jo-helt-hjelpelos-nar-noe-sant-skjer/f/5-109-58703 (sjekket 29.01.2022).

Vedlegg C

Oppgavebeskrivelse

Oppgavebeskrivelsen fra HDO.

Opplæringspakker sikkerhetshendelser

HDO – landsdekkende, tilgjengelig og nyskapende

Helsetjenestens driftsorganisasjon for nødnett HF (HDO)

Om

HDO skal bidra til å realisere de samlede målsetninger for den nasjonale medisinske nødmeldetjenesten. Selskapet skal yte effektive og brukervennlige tjenester for brukere av Nødnett i den akuttmedisinske kjeden i alle de regionale helseforetakene, i alle landets kommuner, og for andre relevante samarbeidspartnere. Vår oppgave er å sørge for enhetlige og stabile kommunikasjonsløsninger og fagsystemer, herunder teknisk utvikling, test, implementering, drift og opplæring av brukere. HDO er organisert som en del av spesialisthelsetjenesten og er eid av de 4 helseregionene.

Oppgaven

Sikkerhetsholdningen til en organisasjon avhenger av flere aspekter som eksempelvis sikkerhetspolicy, bevisstgjøring, og tekniske løsninger. Grunnlaget til holdningen baseres gjerne på en risikovurdering for å identifisere mulige svakheter som igjen kan utbedres. Målet er å ha oversikt over risikoer og legge de på et hensiktsmessig nivå.

En annen viktig aspekt er å utføre regelmessig trening og opplæring i organisasjonen. Denne metodikken er ofte brukt i nødetater for å øke samhandling, forståelse, kompetanse, og forventninger. I mange sammenheng kan det direkte oversettes til håndtering av en sikkerhetshendelse. Ofte er det kryssfaglig team bestående av ledelse og tekniske eksperter som skal samarbeide vurdere situasjonene og ta avgjørelser. Effektiviteten er avhengig av elementer som tidligere interaksjoner og samarbeid mellom medlemmene, sammensetning av teamet, lederskap, og kulturen til organisasjonen.

Målet med oppgaven er å lage «virtuelle cyber escape rooms», eller opplæringspakker, basert på sikkerhetshendelser med et grunnlag i effektiv læring og treningsmetodikk. Antall opplæringspakker kan vi diskutere og bli enige om, men minimum en skal være skreddersydd til HDO's tjenesteportefølje.

Effektiv læring og trening
Det er ingen hemmelighet at personer lærer best på forskjellige måte. For å kunne sikre en god effekt er det behov for å forstå hvordan man kan lære og best mulig effekt av treningen. Eksempel kan være hvordan nødetatene måler oppnådd effekt før (planlegging), under (gjennomføring), og etter (lærdom) en treningsseanse. Målet er at folk oppnår mestringsfølelse og bevisstgjøring samtidig som man bygger relasjoner med hverandre og blir komfortable. For å ikke glemme ha det litt gøy også naturligvis.

Opplæringspakker
Som allerede nevnt skal det lages et antall opplæringspakker basert på sikkerhetshendelser. Hver opplæringspakke burde minimum inneholde metodikk, anbefalt lag-komposisjon, framgangsmåte, nødvendig informasjon for deltakere og opplæringsansvarlig. Det er også greit å ta stilling til størrelse, at metodikken og metodikk varierer noe, og aktuell målgruppe da det kan være tidkrevende og komplekst å utarbeide 3-4 kryssfaglige pakker. Utover det står dere fritt til å løse oppgaven. Ønsker dere å bruke script for å legge spor i

infrastrukturen? Kanskje dere ønsker å lage en mal for en virtuell maskin som har blir tatt over? Hva med en klientmaskin? Hvordan tenker en angriper og hvordan kan dette oversettes til et opplærings scenario?

Det er viktig å påpeke at vi ikke ønsker å introdusere ekte skadevare, noe som kan ødelegge, eller føre til uforutsett nedetid på tjenester.

Konfidensialitet
Studentene kan i løpet av prosjektperioden få tilgang til informasjon om øvrig infrastruktur eller annen konfidensiell informasjon. Sluttrapporten skal ikke inneholde informasjon av slik karakter, og det vil bli pålagt studentene å signere taushetserklæring.

Kontaktopplysninger
Arnt-Helge Nilsen Øyan
E-post: Arnt-HelgeNilsen.Oyan@hdo.no
Tlf: +47 41 04 48 04

Besøksadresse: Hans Mustads gate 31, 2821 Gjøvik
Postadresse: Postboks 72, 2801 Gjøvik
www.hdo.no

Vedlegg D

Gantt-skjema

Oppdatert Gantt-skjema som viser hvordan den faktiske fremtiden var i løpet av bacheloroppgaven.

Prosjektplanlegging

AKTIVITET	PLANLAGT START (FRA UKE...)	PLANLAGT VARIGHET (T.O.M. UKE)	FAKTISK START (FRA UKE)	FAKTISK VARIGHET (T.O.M. UKE)	PROSENT FULLFØRT	UKE 3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Prosjektplan	3	4	3	4	**100 %**																		
Design	4	7	4	14	**100 %**																		
Research	4	6	4	9	**100 %**																		
Rammeverk	4	7	6	11	**100 %**																		
Innhold	4	7	4	14	**100 %**																		
Implementasjon	8	11	8	16	**100 %**																		
Prototype	8	11	8		**100 %**																		
Pre-test	9	10	8		**100 %**																		
Ferdigstille	11	14			**100 %**																		
Evaluering	12	16	17	18	**100 %**																		
Testing	12	13	17	18	**100 %**																		
Post-test	14	15	17	18	**100 %**																		
Sammenfatte resultater	15	16	17	18	**100 %**																		
Bachelorskriving	16	20			**100 %**																		
Lage disposisjon	16	16			**100 %**																		
Skrive bacheloroppgaven	17	20			**100 %**																		
Kvalitetssikre og ferdigstille	19	20	19		**100 %**																		
Innlevering	20	20	20	20	**95 %**																		

Vedlegg E

Timeliste

Timelister som viser timene vi har jobbet i løpet av bacheloroppgaven.

E.1 Timeliste - Anett

UKE	DAG	ANTALL TIMER	TYPE ARBEID
3	Mandag	2,5	Møte med veileder + HDO, generell diskusjon
	Tirsdag	3	Lesing av bacheloroppgaver + svar på spørsmål
	Onsdag	6	Møte, lesing av bacheloroppgaver + trusselvurderinger
	Torsdag	4	Møte
Antall timer	Fredag	2	Prosjektplan
	Lørdag	3	Presentasjon
21	Søndag	0,5	Presentasjon
4	Mandag	6,5	Møte med veileder + HDO, generell diskusjon, mindmapping
	Tirsdag	3,5	Lest artikler/oppgaver fra Steven
	Onsdag	5	Jobbet på skolen med prosjektplan
	Torsdag	3,5	Jobbet på skolen med prosjektplan + design
Antall timer	Fredag	2	Jobbet med prosjektplan
	Lørdag		
21,5	Søndag	1	Leste over prosjektplan + jobbet med overleaf
5	Mandag	2	Møte med veileder + gruppemøte + sendt prosjektplan til veileder
	Tirsdag	4	Research
	Onsdag	4,5	Skolen + research
	Torsdag	4,5	Skolen + research
Antall timer	Fredag	5	Research
	Lørdag		
20	Søndag		
6	Mandag	5	Møte med veileder + generell diskusjon
	Tirsdag	4	Leste artikkel fra Steven + research
	Onsdag	3	Møte + Mozilla Hubs + scenario
	Torsdag	5	Egenjobbing
Antall timer	Fredag	2	Egenjobbing
	Lørdag		
19	Søndag		
7	Mandag	5,5	Møte med veileder + generell diskusjon + Mozilla Hubs
	Tirsdag	6	Jobbe med Mozilla Hubs
	Onsdag	7	Egenjobbing
	Torsdag	5,5	Egenjobbing
Antall timer	Fredag	3	Møte + scenario
	Lørdag		
27	Søndag		

UKE	DAG	ANTALL TIMER	TYPE ARBEID
8	Mandag	6	Møte med HDO + oppsett av framework
	Tirsdag	2	Egenjobbing
	Onsdag	6	Generell diskusjon - lage oppgaver + scenario
	Torsdag	6	Generell diskusjon - lage oppgaver + overleaf
Antall timer	Fredag	1	Egenjobbing
	Lørdag		
21	Søndag		
9	Mandag	4,5	Møte med HDO + generell diskusjon
	Tirsdag		
	Onsdag	7	Lynkurs + egenjobbing
	Torsdag	8	Egenjobbing
Antall timer	Fredag	4,5	Jobbet på skolen med escape room og scenarioer
	Lørdag		
24	Søndag		
10	Mandag	4	Jobbet på skolen + møte med Steven
	Tirsdag	5,5	Møte + egenjobbing
	Onsdag	5	Jobbet på skolen
	Torsdag	6	Jobbet på skolen + møte med Erik og Grethe
Antall timer	Fredag		
	Lørdag	3	Lese stoff fra Grethe
23,5	Søndag		
11	Mandag	6	Møte hos HDO + skolejobbing
	Tirsdag	5	Jobbet på skolen
	Onsdag	5	Egenjobbing
	Torsdag		
Antall timer	Fredag	2	Egenjobbing
	Lørdag	3	Egenjobbing
21	Søndag		
12	Mandag	5,5	Jobbet på skolen
	Tirsdag		
	Onsdag	7,5	Jobbet på skolen
	Torsdag	5	Jobbet på skolen
Antall timer	Fredag	5	Egenjobbing
	Lørdag		
23	Søndag		

UKE	DAG	ANTALL TIMER	TYPE ARBEID
13	Mandag		SPANIA
	Tirsdag		
	Onsdag		
	Torsdag		
Antall	Fredag		
timer	Lørdag		
0	Søndag		
14	Mandag	7	Møte med Steven + HDO
	Tirsdag	4	Egenjobbing
	Onsdag		
	Torsdag	5	Egenjobbing + møte med Grethe
Antall	Fredag	7	Egenjobbing + statusmøte
timer	Lørdag	6	Egenjobbing
29	Søndag		
15	Mandag	4	Jobbet på skolen
	Tirsdag	7	Egenjobbing
	Onsdag	5,5	Egenjobbing
	Torsdag	5	Egenjobbing
Antall	Fredag		
timer	Lørdag	2	Egenjobbing
23,5	Søndag		
16	Mandag	2	Egenjobbing
	Tirsdag	6	Skolen - jobbet med basic escape room
	Onsdag	5	Egenjobbing
	Torsdag	1,5	Egenjobbing
Antall	Fredag	6	Skolen - jobbet med post-test
timer	Lørdag		
20,5	Søndag		
17	Mandag	8	Skolen - jobbet med post-test, escape room, bacheloroppgave
	Tirsdag	5	Skolen
	Onsdag	5,5	Skolen + jobbe litt hjemme
	Torsdag	3	Egenjobbing
Antall	Fredag	3	Skolen
timer	Lørdag	3,5	Egenjobbing
34	Søndag	6	Skolen

UKE	DAG	ANTALL TIMER	TYPE ARBEID
18	Mandag	7	Egenjobbing
	Tirsdag	11	Skolen
	Onsdag	8	Skolen
	Torsdag		
Antall	Fredag	5	Egenjobbing
timer	Lørdag	8,5	Egenjobbing
39,5	Søndag		
19	Mandag	4	Skolen, møte med HDO
	Tirsdag	10	Skolen
	Onsdag	7,5	Skolen
	Torsdag	5,5	Egenjobbing
Antall	Fredag	9	Skolen
timer	Lørdag	1	Egenjobbing
37	Søndag		
20	Mandag	3,5	Egenjobbing
	Tirsdag	5	Skolen + egenjobbing
	Onsdag	8	Skolen
	Torsdag	9,5	Skolen
Antall	Fredag	!!FERDIG!!	
timer	Lørdag		
26	Søndag		

E.2 Timeliste - Emma

UKE	DAG	ANTALL TIMER	TYPE ARBEID
3	Mandag	2,5	Møte med Steven, HDO og generell planlegging
	Tirsdag	0	
	Onsdag	5,5	Gruppemøte og leste en bachelor oppgave hjemme
	Torsdag	6	Gruppemøte 9-13, prosjektplanarbeid, leste en opg.
Antall timer	Fredag	0,5	Prosjektplanarbeid 30 min
	Lørdag	0	
14,5	Søndag	0	
4	Mandag	6	Skolen; møte HDO+veileder+prosjektplan+tankekart
	Tirsdag	2,5	Leste oppgaver fra Steven om cyber escape rooms
	Onsdag	5	Skolen; prosjektplan, + 30 min hjemme
	Torsdag	3	Skolen; prosjektplan + design
Antall timer	Fredag	0	
	Lørdag	0	
17	Søndag	0,5	Så over prosjektplanen
5	Mandag	2	Møte med Steven + gruppen
	Tirsdag	4	Research
	Onsdag	5	Skolen; research
	Torsdag	6,5	Skolen + research hjemme
Antall timer	Fredag	4	research hjemme
	Lørdag	0	
21,5	Søndag	0	
6	Mandag	4,5	Skolen; møter + research
	Tirsdag	5	Leste om escapED fra Steven + research
	Onsdag	4	Møte (47 min) + litt annet
	Torsdag	4	Skolen + research hjemme
Antall timer	Fredag	2	
	Lørdag	0	
19,5	Søndag	0	
7	Mandag	4	Møte med Steven, Mozilla Hubs prototype + research
	Tirsdag	5	mozilla hubs
	Onsdag	3,4	research hjemme
	Torsdag	4	møte + litt annet
Antall timer	Fredag	5	møte + litt annet
	Lørdag	0	
24,4	Søndag	3	puzzles for basic

UKE	DAG	ANTALL TIMER	TYPE ARBEID
8	Mandag	6	møte med HDO + puzzles
	Tirsdag	6,5	puzzles
	Onsdag	8	skolen
	Torsdag	5,5	skolen; 4.5t, hjemme; skrive om teori
Antall timer	Fredag	5	teori-skriving
	Lørdag	0	
0	Søndag	0	
9	Mandag	4	skolen
	Tirsdag	4,5	lesing og gjøring av stevens materiale
	Onsdag	7	lynkurs rapportskriving + litt på skolen
	Torsdag	6	skolen
Antall timer	Fredag	4,5	på skolen
	Lørdag	0	
0	Søndag	0	
10	Mandag	6	40 min møte steven, annet
	Tirsdag	5,5	30 min gruppemøte + scenarioer
	Onsdag	5	skolen; scenarioer og basic escape rom
	Torsdag	8	skolen; scenarioer , møte med erik + grete
Antall timer	Fredag	2	lese litt fra Grethe
	Lørdag	0	
0	Søndag	0	
11	Mandag	3,00	1,5 hos HDO + 1,5 t skolen
	Tirsdag	4,5	4,5 skolen
	Onsdag	8	
	Torsdag	6	
Antall timer	Fredag	5,5	
	Lørdag	0	
0	Søndag	0	
12	Mandag	4,5	møter og litt research
	Tirsdag	6,5	
	Onsdag	5	4 t skolen, 1 t hjemme
	Torsdag	5	skolen
Antall timer	Fredag	4	skolen
	Lørdag	3	escape room hjemme
0	Søndag	0	

UKE	DAG	ANTALL TIMER	TYPE ARBEID
13	Mandag	1,5	
	Tirsdag	0	
	Onsdag	0	
	Torsdag	1	
Antall timer	Fredag	0	
	Lørdag	0	
2,5	Søndag	0	
14	Mandag	0	
	Tirsdag	0	
	Onsdag	0	
	Torsdag	2	escaperom
Antall timer	Fredag	1	litt escaperom
	Lørdag	0	
3	Søndag	0	
15	Mandag	0	
	Tirsdag	1	
	Onsdag	2	
	Torsdag	0	denne uken var jeg syk :(
Antall timer	Fredag	0	
	Lørdag	3	
6	Søndag	0	
16	Mandag	0	
	Tirsdag	5	skolen; fullføre basic
	Onsdag	6	
	Torsdag	7	
Antall timer	Fredag	5	posttest
	Lørdag	4	skriving + møtereferat
27	Søndag	0	
17	Mandag	6	møter + skolen + litt hjemme
	Tirsdag	5	skolen
	Onsdag	5,5	skolen
	Torsdag	3	
Antall timer	Fredag	5	skolen
	Lørdag	0	
26,5	Søndag	2	jobbe hjemme

UKE	DAG	ANTALL TIMER	TYPE ARBEID
18	Mandag	7	
	Tirsdag	10	10:00-20:00 skolen
	Onsdag	7	
	Torsdag	7	
Antall timer	Fredag	5	i ttown
	Lørdag	6,00	jordbærpikene
43	Søndag	1	teori
19	Mandag	2	jobbing på bussen
	Tirsdag	10	skolen; rapport
	Onsdag	4	skolen; rapport
	Torsdag	8	
Antall timer	Fredag	9	skolen; rapport
	Lørdag	8	
46	Søndag	5	4 timer på skolen, 1 hjemme
20	Mandag	6,5	lese over rapport hjeme + skriving
	Tirsdag	7	4.5 skolen, 2.5 hjemme
	Onsdag	9	
	Torsdag	9,5	
Antall timer	Fredag	0	Ferdig :D
	Lørdag		
32	Søndag		

E.3 Timeliste - Thea

UKE	DAG	ANTALL TIMER	Type arbeid
3	Mandag	2	
	Tirsdag	2,5	
	Onsdag	5,5	
	Torsdag	4	
	Fredag	2,5	
SUM	Lørdag		
16,5	Søndag		
4	Mandag	6	Arbeidet sammen på skolen, møter
	Tirsdag	3	Leste References Cyber Escape Rooms
	Onsdag	5,5	prosjektplanen
	Torsdag	3,5	Prosjektplan + starte research design
	Fredag	3	Research
SUM	Lørdag		
21	Søndag		
5	Mandag	3	Møte med veileder
	Tirsdag	4	Research
	Onsdag	5	Skolen + research
	Torsdag	7	Skolen + research
	Fredag	2	Research om læring
SUM	Lørdag		
21	Søndag		
6	Mandag	7	Møter med HDO, research
	Tirsdag	5	Lese Practical Research
	Onsdag	4	Lese Practical Research
	Torsdag	5	Læring
	Fredag		
SUM	Lørdag		
24	Søndag	3	Lese Effektiv Læring
7	Mandag	6	Møter, leseing, mozilla hubs
	Tirsdag		
	Onsdag	4,5	Mozilla Hubs
	Torsdag	4	Forslag hvordan måle læring
	Fredag	5	Møter + scenario
SUM	Lørdag	4,5	Scenario
24	Søndag		

UKE	DAG	ANTALL TIMER	TYPE ARBEID
8	Mandag	7,5	Scenarioer, rammeverk, læring
	Tirsdag	2	Læringsdesign
	Onsdag	6	Scenarioer, rammeverk, læring
	Torsdag	4,5	Scenarioer, rammeverk, læring
	Fredag	7	Scenarioer, rammeverk, læring
SUM	Lørdag		
27	Søndag		
9	Mandag	7	Skolen
	Tirsdag	5	Lesing
	Onsdag	5	Lynkurs + research
	Torsdag	2	Lesing
	Fredag	6,5	skolen
SUM	Lørdag		
25,5	Søndag		
10	Mandag	6	Skolen
	Tirsdag	3	Møte
	Onsdag	8	Skolen
	Torsdag	6	Skolen
	Fredag	7	Skolen
SUM	Lørdag		
30	Søndag		
11	Mandag	6	Møte HDO + skolen
	Tirsdag		
	Onsdag	4	Escape Room
	Torsdag	5	Escape Room
	Fredag		
SUM	Lørdag		
19	Søndag	4	Skolen
12	Mandag	5,5	Skolen: Escape Room
	Tirsdag	8	Escape Room
	Onsdag		
	Torsdag	6,5	Skolen: Escape Room
	Fredag	5,5	Escape Room
SUM	Lørdag		
25,5	Søndag		

UKE	DAG	ANTALL TIMER	TYPE ARBEID		UKE	DAG	ANTALL TIMER	TYPE ARBEID
	Mandag	3				Mandag	5	Skolen: metode, testing
	Tirsdag					Tirsdag	11	Skolen: metode, testing
13	Onsdag	4			18	Onsdag	6	Skolen: metode, testing
	Torsdag		Spania			Torsdag		Trondheim
	Fredag					Fredag		
SUM	Lørdag				SUM	Lørdag		
7	Søndag				22	Søndag		
	Mandag	4	Escape Room			Mandag		
	Tirsdag					Tirsdag	10	Skolen: analyse
14	Onsdag	3	Escape Room		19	Onsdag	5	Skolen: analyse
	Torsdag	3	Escape Room			Torsdag		
	Fredag	5	Escape Room			Fredag	11	Analyse og diskusjon
SUM	Lørdag				SUM	Lørdag	8,5	Diskusjon
18	Søndag	3	Escape Room		40	Søndag	5,5	Diskusjon
	Mandag	4	Escape Room			Mandag	4	Lese over
	Tirsdag	6	Escape Room			Tirsdag	7	Konklusjon, lese over
15	Onsdag				20	Onsdag	8	Lese over
	Torsdag					Torsdag	6,5	Lese over
	Fredag		Påske			Fredag		
SUM	Lørdag				SUM	Lørdag		
10	Søndag				25,5	Søndag		
	Mandag	6,5	Skolen - ferdigstille escape room					
	Tirsdag	4	Endre escape room etter tilbakemeldinger					
16	Onsdag	6	Post-test og skrive					
	Torsdag							
	Fredag	5	Post-test					
SUM	Lørdag	5,5	Post-test, skrive introduksjon					
29	Søndag	2						
	Mandag	7	Post-test, introduksjon					
	Tirsdag	6	Introduksjon					
17	Onsdag	5	Introduksjon					
	Torsdag	5	Teori					
	Fredag	5	Teori					
SUM	Lørdag							
33,5	Søndag	5,5						

Vedlegg F

Møtereferat fra møter med veileder

Møtereferat fra møter med veileder.

F.1 Møte 17. januar

Møtereferat		
Veileder	Til stede: Steven, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	
Introduksjon		
Plan	• Hva skal vi gjøre; lese tekster, snakke om emnet • Planlegge milepæler • Hvilke metoder skal brukes? Hvilke ressurser trengs?	

F.2 Møte 24. januar

Møtereferat		
Veileder	Til stede: Steven, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	
Om oppgaven	• Avklar emnet • Sikkerhetsopplæring, vi er lærerne • Å lære bort er nytt for oss, bruke gamification • HDO er i helsesektoren, sektoren må være i bakgrunnen, og HVEm er deltagerne i kurset vi lager	
Planer	Denne uken • Prosjektplan • Hva skal vi gjøre	
Cyber escaperom	Loop; cyber escaperom -> rammeverk -> realization • Cyber escaperom er for vagt • Se rammeverkene SERF og escapED • Realization er miljøet og redskapene	
Må gjøre	• Lese oppgaver Steven har lagt ut • Finne ut hva HDO vil • Lage ukentlig plan + exceltabell slik han viste • Escaperomscenario, hva ville interessert oss?	
Annet	• 1,5 måned vil trenges for rapportskriving • To tilnærminger; waterfall eller agile	

F.3 Møte 31. januar

Møtereferat		
Veileder	Til stede: Steven, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	
Tips	• Lag en liste med designideer/draft og gi til Steven før uken er over (bare et dokument med våre ideer til torsdag) • Han foreslår designfase hele februar • Sjekke med HDO at fysisk escaperom er ok? • I april bør vi begynne å skrive oppgaven • Han trenger ikke presentasjoner, kun å liste det vi har gjort fra gang til gang	

F.4 Møte 14. februar

Møtereferat		
Veileder	Til stede: Steven, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	

Tips/ting å gjøre	• Ikke heng oss opp i rammeverk; bruk escapED og SERF
	• Begynn å lage prototyper med enkle oppgaver
	• Kom opp med scenarioer og spør HDO hvilke de liker best
	  o Hva er HDO interessert i?
	  o Vi fikk en liste fra møtet med sikkerhetsfolka, skal vi se på disse?
	• For hvert scenario, fyll ut escapED punktene	

Til neste gang	• Kom opp med to scenarioer til neste mandag	

F.5 Møte 28. februar

Møtereferat		
Veileder	Til stede: Steven, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	
Tips	• Escaperom i google forms	
Til neste gang	• Lag slides med scenarioene og deres innhold • Start og implementer passordsikkerhet i google forms o Lag en “prototype”	

F.6 Møte 7. mars

Møtereferat		
Veileder	Til stede: Steven, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	
Siden sist	• Laget scenarioer som er godkjent av HDO • Laget og sendt ut pre-test til HDO • Startet med basis-rommet	
Må gjøre/planer	• Informere HDO om at vi trenger diverse testsubjekter • Bruke scenario-arket om phishing til å lage oppgaver?	
Tips fra Steven	• Han vil at vi skal ta oppgaver i stedet for å lage alle fra scratch • Beskriv scenarioene som en roman – det trengs mere detaljer enn "a worm" • Prøv å gjør scenarioene mer spennende med litt skremselsfaktorer osv.	

F.7 Møte 21. mars

Møtereferat		
Veileder	Til stede: Steven, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	
Pre-testen	• Steven hadde noen spørsmål	
Escaperommene	• Viste draft for basic o Han syntes 10-15 er for mange spørsmål o Sørg for at rommet ikke blir som en prøve o Maks 20 min o Disse bør bli ferdig innen 20 dager/3 uker	
Om teksten	• Bør startes å skrive (vi har startet) • Se latex-oppgaven i slutten av mars • Tenk på en kul tittel til oppgaven	
Til neste gang	• Se første versjon av escaperommet	

F.8 Møte 4. april

Møtereferat		
Veileder	Til stede: Steven, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	
Escaperom utvikling	• Gi mer bakgrunnsinformasjon (roller, ansvar, miljø) for å gi kontekst • Støttematerialet for gåtene må være effektive (deltagerne skal løse gåtene med støttematerialet) • Siden det ikke er en quiz, må det gis kunnskap i scenarioet • Finn brukbare cybersikkerhetsquizer og presenter de visuelt. Tekst er ikke nok for cybersikkerhetsopplæring.	
Evaluering	• Tenk på hvordan effektiviteten skal representeres i teksten, vinkle spørsmålene for å få svarene vi ønsker.	
Skriving	• Lag en tidslinje for når kapitlene skal ferdigstilles	

F.9 Møte 25. april

Møtereferat		
Veileder	Til stede: Steven, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	
Testing	• Bare bruke Excel i stedet for analysesoftware hos NTNU • Bruke spørsmål som "hadde du det gøy", for å måle fornøyeligheten til escape rommene	
Oppgaveteksten	• God start på oppgaveteksten • Se møtechat for flere tips • Ha med en setning om cyber escape room sin innovasjon • Ha med mer om hvor dårlig cyber security er i Norge • Ha med "kan dette motivere læreren til å lære" i hypotesen • Skriv veldig generisk • Skriv øke kompetansen til individene i bedriften IKKE til bedriften	
To do:	• Fullføre metode og teori i løpet av tirsdag	

Vedlegg G

Møtereferat fra møter med oppdragsgiver

Møtereferat fra møter med oppdragsgiver. Informasjon som er underlagt taushetsplikt er sensurt med ■.

G.1 Møte 24. januar

Møtereferat		
HDO	Til stede: Arnt-Helge, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	
Generelt fra Arnt-Helge	• Taushetserklæring er sendt ut og skal signeres ila uken. • Møte med HDO sin sikkerhetsledelse i uke 6	
HDO oppsett	Består av ledelse og teknikere. Opplæring hovedsakelig for teknikerne, [redacted].	
Oppgaveoppsett	HDO ønsker opplæringspakker de kan lære av, ellers står vi meget fritt. Hvor oppfinnsomme kan vi være? Tre opplæringspakker er bra, der minst en må være tilpasset HDO. • Greier vi selv å tenke ut et scenario skreddersydd til HDO? • HDO ser [redacted] Oppgaven trenger ikke å være anonym, de trenger bare bruksrett.	
To do:	• Skrive under taushetserklæring • Lese om dagens trusselbilde • Finne scenarioer for HDO	

G.2 Møte 7. februar

Møtereferat		
HDO	Til stede: Arnt-Helge, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	
Inkludere hele HDO	Arnt-Helge ønsker at hele HDO skal inkluderes i sikkerhetsøvelsene, hvordan skal dette gjøres? • Hvor inkluderte vil disse ikke-tekniske gruppene være i en faktisk sikkerhetshendelse?	
Møtet med CISO	De vil snakke om pakkene som skal skreddersys til HDO. De vil også snakke om sikkerhet og HDO, samt de tidligere opplæringseventene de har hatt.	
To do:	Forberede oss på møtet med CISO.	

G.3 Møte 7. februar med sikkerhetsledelsen

Møtereferat		
HDO og CISO	Til stede: Anett, Emma, Thea, Arnt-Helge, Kristian Frogner og Vidar Grønland	Referent: Emma
Sak:	Innhold:	
Viktig for HDO	• Ivareta det HDO leverer og at det er sikkert og følger regler • Kommunene de samarbeider [redacted] • På bakgrunn av [redacted] og komplekst trusselbilde har de en viktig jobb	
Ansatte	Miks av ansatte der HR og økonomi blir referert til som "ikke nevneverdige med tanke på sikkerhet"	
Opplæring	HDO bruker en NorSIS opplæringspakke for nasjonal sikkerhetsmåned. I oktober er det dermed litt ekstra sikkerhetsfokus. Intern opplæring: • [redacted] • [redacted] • [redacted]	
Gamle øvelser	2018 – [redacted] • [redacted] • [redacted]g Nå - [redacted]	

	• [redacted] • [redacted] • Er løsningene deres gode nok? 3. gang [redacted] • [redacted] • [redacted] I fjor – [redacted] • Standard hendelse [redacted] • Lære opp teknisk personale [redacted] I år - [redacted] • Finne kodeord • Teknisk • [redacted] • Brukte MITRE sitt rammeverk (I teorien) for å oppdele angrepet • [redacted] • [redacted]
Ønsker for vår oppgave	Hvis HDO [redacted] • [redacted] • [redacted] HDO har en servicedesk [redacted]

	Overordna viktig for HDO
	• Øve på sannsynlige hendelser
	• Dagens [redacted]
	• [redacted]
	• Nytt punkt; [redacted]
	• [redacted]
	• [redacted]
	• [redacted]
	• Escape rommet bør inneholde noe form for hendelseshåndtering
	• [redacted]
	  ○ [redacted]
	  ○ [redacted]

Anbefalt lesestoff	Helse CERT sin trusselvurdering, ligger åpent • https://www.nhn.no/Personvern-og-informasjonssikkerhet/helsecert/situasjonsbilde-2021 • På denne linken er det også nasjonalt beskyttelsesprogram [redacted]

G.4 Møte 21. februar

Møtereferat		
HDO	Til stede: Arnt-Helge, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	
Oppgaveidé	• Oppsummeringsrapport i forkant av escape rommet for HDO • https://attack.mitre.org/, kunne måle seg mot dette, en slags CTF	
Sikkerhetsscenarioer HDO	Hvis [redacted] Hvis en hendelse i HDO [redacted] Eksempel på hendelse: [redacted] [redacted]	
Om nødnettet	Nødnette [redacted] - [redacted] - [redacted] - [redacted] - [redacted] - Norge har [redacted]	

G.5 Møte 28. februar

Møtereferat		
HDO	Til stede: Arnt-Helge, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	
Scenarioene	Ferdig med scenarioene • Selv om det er gamification bør det være reelle scenarioer med utbytte. • 3 scenarioer -> grunnleggende, ransomware og zero-day	
To do:	Sende beskrivelser av ulike scenario til Arnt-Helge	

G.6 Møte 7. mars

Møtereferat		
HDO	Til stede: Arnt-Helge, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	
Status	Jobber videre med escaperom.	
To-do:	Møte hos HDO neste mandag, 14.03 kl. 09	

G.7 Møte 14. mars

Møtereferat		
HDO	Til stede: Arnt-Helge, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	
Escaperom	Utfordring med oppbygging av rommene • Innholdet er OK, men vanskelig å bygge opp rommene skikkelig • Vært i kontakt med Grethe Østby for ideer	
Pre-test	Arnt-Helge tar tilfeldig uttrekk fra AD og sender spørreundersøkelsen i løpet av dagen	

G.8 Møte 21. mars

Møtereferat		
HDO	Til stede: Arnt-Helge, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	
Escaperom	Ferdig med oppsettet på 2 av 3 escaperom. • Hovedsaklig igjen å gå over	
Pre-test	For få svar på pre-test – utsetter fristen i en uke (28.mars).	
To do:	Mulig nytt møte med CISO?	

G.9 Møte 28. mars

Møtereferat		
HDO	Til stede: Arnt-Helge, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	
Escaperom	• Snart ferdig med escaperommene o Presentert et rom til Arnt-Helge, de to andre neste uke	
Pre-test	Fortsatt for få svar, Arnt-Helge purrer på nytt	

G.10 Møte 4. april

Møtereferat		
HDO	Til stede: Arnt-Helge, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	
Escaperom	Må endre på oppgave i escaperommene i henhold til tilbakemelding fra veileder. Sender oversikt over endringer til Arnt-Helge	
Pre-test	Fortsatt for få svar – Arnt-Helge tar nytt uttrekk via AD og sender ut på nytt.	

G.11 Møte 25. april

Møtereferat		
HDO	Til stede: Arnt-Helge, Anett, Emma, Thea	Referent: Emma
Sak:	Innhold:	
Sende ut escape rommene og post test	• Gjøres i dag, Arnt-Helge må purre på de • Sende email med instruks på fremgangsmåte, inneholder også instrukts til de som har tatt pre-test	

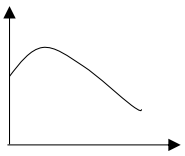
G.12 Møte 9. mai

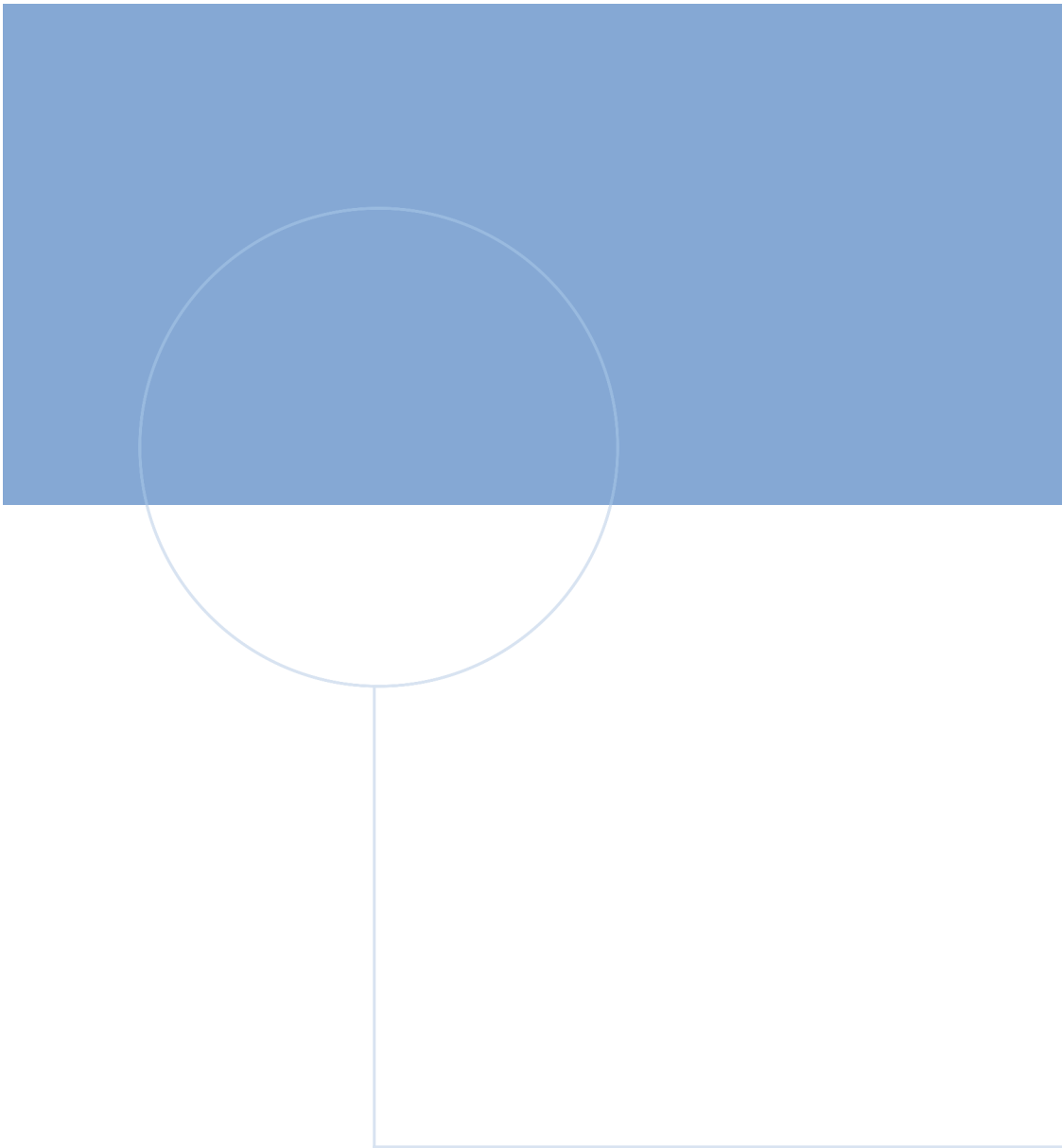
Møtereferat		
HDO	Til stede: Arnt-Helge, Anett, Thea	Referent: Anett
Sak:	Innhold:	
Escaperommene	For få svar på escaperommene, men har ikke mer tid til å la de ansatte teste mer	
Bacheloroppgaven	Arnt-Helge ønsker ikke å lese over • Vi må være obs på taushetsplikten	
Generelt	Kansellerer de neste møtene, fokuserer på oppgaven	

Vedlegg H

Møtereferat fra møte med Grethe Østby

Møtereferat fra møte med Grethe Østby 10. mars.

Møtereferat		
Grethe Østby	Til stede: Grethe, Anett, Emma, Thea	Referent: Anett
Sak:	Innhold:	
Escaperom	Generelt: • Fundament for escape room er team-based learning • Vær obs på å ikke gi all info med en gang, man ville ikke fått det i en reel situasjon • 5 steg i hendelseshåndtering: o 1.Etterretning/ikke ta beslutninger på feil grunnlag o 2. Personell o 3. Operasjon o 4. Logistikk o 5. Informasjon (internt, eksternt - media) • Ved en hendelse: o Kaos, y-akse o Tid, x-akse 	
Undersøke	• Undersøk decision trees – 3 alternativer, • Konrad Lunde – beredskap • Lovverket – hva er lovverket i forhold til hendelseshåndtering • Serious games	



NTNU

Kunnskap for en bedre verden