Bacheloroppgave

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

Daniel Christian Haraldsen Magnus
Bendik Berntsen Flobak
Abu Baker Mohammed Abdullah Al-Shammari
Inger Moren

Brettspillbasert opplæring i informasjonssikkerhet

Bacheloroppgave i IT-drift og informasjonssikkerhet
Veileder: Gaute Wangen & Ernst Gunnar Gran
Mai 2019

NTNU
Kunnskap for en bedre verden

Daniel Christian Haraldsen Magnus
Bendik Berntsen Flobak
Abu Baker Mohammed Abdullah Al-Shammari
Inger Moren

Brettspillbasert opplæring i informasjonssikkerhet

Bacheloroppgave i IT-drift og informasjonssikkerhet
Veileder: Gaute Wangen & Ernst Gunnar Gran
Mai 2019

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

NTNU
Kunnskap for en bedre verden

Sammendrag av Bacheloroppgaven

Tittel:	**Brettspillbasert opplæring i informasjonssikkerhet**
Dato:	20.05.2019
Deltakere:	Daniel Christian Haraldsen Magnus Bendik Berntsen Flobak Abu Baker Mohammed Abdullah Al-Shammari Inger Moren
Veiledere:	Gaute Wangen & Ernst Gunnar Gran
Oppdragsgiver:	Norsk Tipping Skatteetaten
Kontaktperson:	Trond Laupstad, trond.laupstad@norsk-tipping.no, 62514311 Anne Marie Dalen Øverhaug, AnneMarieDalen.Overhaug@skatteetaten.no, 90946548
Nøkkelord:	Opplæring, Sikkerhetskultur, Informasjonssikkerhet
Antall sider:	63
Antall vedlegg:	13
Tilgjengelighet:	Åpen

Sammendrag:

Opplæring av ansatte innen informasjonssikkerhet er viktig for organisasjoner. Dette blir tradisjonelt gjort gjennom E-læring og kurs. Oppgaven vår gikk ut på å lage et fysisk brettspill som skal brukes til opplæring i informasjonssikkerhet. Problemstillingen var å se på hvor effektivt brettspill er til opplæring i informasjonssikkerhet. Vi har gjennom prosjektet utført intervjuer hos oppdragsgivere for å få en oversikt over behovet for opplæring. Med hjelp av den informasjonen utviklet vi brettspillet. Brettspillet er også testet hos oppdragsgiverne for å se hvor mye de ansatte lærte av spillet. For å teste dette har vi brukt to forskjellige pre- og posttester, en metode for å prøve å finne årsak-og-effekt. En selvevaluering der de ansatte selv evaluerer sin kunnskap og en kunnskapstest der vi testet kunnskapen deres. Gjennom de resultatene så vi at de ansatte er positive til brettspill som læringsform, og at kunnskapen til de ansatte var høyere etter brettspillet enn før. Konklusjonen er da at brettspillet har en læringseffekt, men det er vanskelig å si hvor effektivt det er uten å måle det opp mot andre læringsformer og hvor godt kunnskapen sitter etter 6 måneder eller 1 år.

Summary of Graduate Project

Title:	**Board game based training in information security**
Date:	20.05.2019
Authors:	Daniel Christian Haraldsen Magnus Bendik Berntsen Flobak Abu Baker Mohammed Abdullah Al-Shammari Inger Moren
Supervisor:	Gaute Wangen & Ernst Gunnar Gran
Employer:	Norsk Tipping Skatteetaten
Contact Person:	Trond Laupstad, trond.laupstad@norsk-tipping.no, 62514311 Anne Marie Dalen Øverhaug, AnneMarieDalen.Overhaug@skatteetaten.no, 90946548
Keywords:	Training, Security culture, Information Security
Pages:	63
Attachments:	13
Availability:	Open

Abstract: Information security training for employees is important for organizations. This is traditionally done through E-learning and courses. Our task is to develop a physical board game which is going to be used for information security training of employees. Our topic question was to see how effective board games are for information security training. During our project we conducted interviews with our clients to get an overview of the need for training. With this information we developed the board game. In order to see how effective the board game was, we used two different pre-posttests, a method intended to find the cause and effect relationship. One test is a self-evaluation where the employees could evaluate their own knowledge. The other test was a knowledge test to test their actual knowledge. Through the results we saw that the employees are positive to board games as a form of training and that their knowledge increased after they played the board game. Our conclusion is that the board game has a learning effect, but it's hard to say how effective it is without comparing it to other types of training and whether or not they are able to retain the knowledge after 6 months or a year.

Forord

0.1 Takk til våre bidragsytere

Oppgaven er gjennomført med hjelp fra flere hold. Takk til nære som har latt oss teste intervjuer og spillet samt testene brukt i test fasen. Takk til de deltakende intervju- og testobjekter for å ha bidratt til å forbedre produktet. Takk til våre veiledere Gaute Wangen og Ernst Gunnar Gran for god oppfølging gjennom hele prosjektet. Takk til oppdragsgiverne, Norsk Tipping og Skatteetaten, for samarbeid i prosessen ved disposisjon av ansattes tid samt lokaler underveis i prosjektet. Til slutt, takk til medstudenter som har deltatt i uformelle tester, og Daniel Monsen for trofast utlån av transportmiddel.

0.2 Oppdragsgivere

Norsk Tipping har statlig, nasjonalt monopol på en rekke pengespill, og Kulturdepartementet avgjør selskapets spilleregler og hvor stor andel av innsatsbeløpet som skal gå til gevinster. Selskapets overskudd, de såkalte spillemidlene, fordeles i dag mellom idrett, kultur og humanitære formål. Midlene til idrettsformål fordeles av regjeringen, mens midler til kulturformål fordeles med to tredeler av Stortinget og en tredel av regjeringen. Gjennom Grasrotandelen kan i tillegg den enkelte spilleren gi et beløp tilsvarende 7 prosent av egen innsats til en lokal klubb eller forening.
Norsk Tippings enerett er begrunnet med at pengespill har potensial til å skape sosiale problemer for kundene, og det har vært bred politisk enighet om at sterk statlig regulering av pengespill er nødvendig av forbrukervern-hensyn. Eneretten er oppe til diskusjon med jevne mellomrom og flere partier har tatt til orde for å slippe til flere aktører, f.eks. gjennom lisensiering. Lotteritilsynet har i en utredning 2015 konkludert med at enerettsmodellen trolig er den beste for å forebygge pengespillproblemer, mens en annen statlig utredning konkluderer med at det neppe blir mer penger til overskuddsformålene ved en liberalisering av markedet. En utredning finansiert av den private spillbransjen hevder det motsatte. I desember 2016 la Regjeringen fram stortingsmeldingen "Alt å vinne". Der konkluderte Regjeringen med at enerettsmodellen skal videreføres[1].

Skatteetaten er underlagt Finansdepartementet, og har ansvaret for et oppdatert folkeregister og at skatter og avgifter blir fastsatt og innbetalt på riktig måte. Skatteetaten jobber ut fra visjonen om et samfunn der alle vil gjøre opp for seg. Målet er at det skal være enkelt å gjøre det riktig. Skattedirektør Hans Christian Holte understreker hvor viktig det er å forstå forskjellen på et samfunn der alle vil gjøre opp for seg, og et samfunn der det må brukes sanksjoner og kontroll for å få inn skattepengene. Skatteetaten må ha stor tillit i befolkningen, og gjøre det enkelt for alle å følge skattereglene.
Alle landets innbyggere kommer i kontakt med Skatteetaten. Denne kontakten har mye å si for folkets tillit til etaten. Derfor er det viktig at Skatteetaten alltid er imøtekommende og profesjonelle, i tillegg til å være nytenkende i måten etaten løser oppgaver på[2].

[1] *Norsk Tipping* https://no.wikipedia.org/wiki/Norsk_Tipping (Besøkt 06.03.2019)
[2] *Skatteetaten* https://www.skatteetaten.no/om-skatteetaten/om-oss/samfunnsoppdrag-strategi/ (Besøkt 06.03.2019)

Innhold

Figurer

Tabeller

Ordliste

2FA to-faktor autentisering. 29

avvik Avvik er hovedsaklig et informasjonssikkerhetsbrudd i forbindelse med arbeidsutførelse og arbeidspraksis. Et avvik kan ha store, små eller ingen konsekvenser. [3]. 2

BGL Board Game Learning (BGL) er brettspill med opplæring som formål. 10

hendelser En hendelse er noe som har skjedd. I dette tilfelle er det hendelser knyttet opp mot store organisasjoner i Norge som har vært utsatt for et digitalt angrep som for eksempel Hydro saken [4]. 2, 34

Likert skala Likert-skala, graderingsskala hvor svaret på hvert enkelt spørsmål graderes [5]. 23, 24, 26

modus Modus, også kalt typetall eller modalverdi, er et sentralitetsmål som beskriver den tallverdien som har det største antall observasjoner, altså den det er flest av. Modus er den instans det er mest sannsynlig å treffe på i en målt mengde. [6]. 26, 49

Phishing Phishing, på norsk også kalt nettfiske eller phiske, er en betegnelse på digital snoking eller «fisking» etter sensitiv informasjon, som passord eller kredittkortnummer [7]. 9, 25, 28

Polymorfisk virus Et virus som krypterer seg selv med en variabel nøkkel for å opptre annerledes enn hva den gjorde tidligere. 39

sikkerhetskultur Digital sikkerhetskultur er samfunnets felles verdier, holdninger, normer, kunnskaper og handlinger om det å kunne ta del i et digitalisert samfunn på en trygg måte. Den digitale sikkerhetskulturen skal gjøre både den enkelte, og samfunnet i sin helhet, mer mindre sårbare mot digitale trusler. Dette bidrar til å bygge tillit til de digitale tjenestene slik at samfunnet kan høste alle godene som digitaliseringen kan gi oss. [8]. 1, 2

Skadevare er en fellesbetegnelse på ondsinnet programvare. Eksempler på skadevare er virus, trojansk hest, og rootkit. 9

Sosial manipulering Utnytter menneskelig kontakt og sosiale evner for å få tak i eller påvirke informasjon. [9]. 9, 28, 39

Spear phishing Spear phishing (spydphiske) er en selektiv, avansert og sofistikerte form for phishing. [10]. 29

[3] *Informasjonssikkerhet - avvik* https://innsida.ntnu.no/wiki/-/wiki/Norsk/Informasjonssikkerhet+-+avvik (Besøkt 18.05.2019)
[4] *Hendelser, avvik og informasjonssikkerhetsbrudd* https://internkontroll-infosikkerhet.difi.no/hendelser-avvik-og-informasjonssikkerhetsbrudd (Besøkt 10.05.2019)
[5] *Likert skala* https://snl.no/Likert-skala (Besøkt 04.04.2019)
[6] *Typetall* https://no.wikipedia.org/wiki/Typetall (Besøkt 07.05.2019)
[7] *Phishing* https://no.wikipedia.org/wiki/Phishing (Besøkt 05.04.2019)
[8] *Nordmenn og digital sikkerhetskultur 2018* https://norsis.no/nordmenn-og-digital-sikkerhetskultur-2018/ (Besøkt 08.03.2019)
[9] *Sosial Manipulering* https://nettvett.no/sosial-manipulering/ (Besøkt 05.04.2019)
[10] *Phishing* https://no.wikipedia.org/wiki/Phishing (Besøkt 05.04.2019)

SPSS er en kommersiell programvarepakke med grafisk grensesnitt for statistiske beregninger. I 2009 skiftet produktet navn til PASW Statistics (Predictive Analytics SoftWare). SPSS er også navnet på firmaet som produserer og selger programpakken. [11]. 27

VPN Betegnelse på en datateknikk som anvendes for å skape «punkt-til-punkt»-forbindelser, såkalte «tunneler», gjennom et annet datanett (som for eksempel internett). En VPN-tunnel kan være kryptert, noe som er viktig når man ikke kjenner, eller er usikker på sikkerheten gjennom et eventuelt offentlig datanett, som for eksempel internett [12]. 29, 39

Acronyms

APT Advanced Persistent Threat. *Glossary:* APT

BGL Board Game Learning. *Glossary:* BGL

SPSS Statistical Package for the Social Sciences. 27, *Glossary:* SPSS

VPN Virtual Private Network. 39, *Glossary:* VPN

[11] *SPSS* https://no.wikipedia.org/wiki/SPSS (Besøkt 02.05.2019)
[12] *Virtual Private Network* https://no.wikipedia.org/wiki/Virtual_private_network (Besøkt 04.04.2019)

1 Innledning

Vi starter vår innledning ved å se på problemområdet vi sto ovenfor og hvilke avgrensninger vi har måttet gjøre i forhold til den oppgaven som ble presentert av oppdragsgiver. Deretter redegjør vi for vår konkrete oppgave og de problemstillinger som vi ønsket å besvare ved prosjektets slutt. Videre tar vi for oss målgruppen, bakgrunnen til prosjektets deltakere, og rammer. Innledningen avsluttes med gjennomgang av øvrige roller, selve rapporten, og praktisk informasjon.

1.1 Problemområde, avgrensning og oppgavedefinisjon

Det digitale trusselbildet mot norske bedrifter er økende [1]. Den økende digitaliseringen i hjemmet og på arbeidsplassen gjør det vanskelig for de ansatte å følge med på dagens sikkerhetsbilde. Arbeidsgivere har et stort behov for å ha en effektiv opplæring i sikkerhet, som bidrar til å engasjerer sine ansatte i det større sikkerhetsbildet. Angripere har økende tilgang til mer og mer maskinkraft som gjør at virksomheter føler seg nødt til å sette strengere krav og policyer til de ansatte. Generelt sett kan dette ende opp med å jobbe mot bedriftens ønske om økt sikkerhet.
For å bedre sikkerhetskultur innad i en bedrift er det viktig at de ansatte skjønner den generelle begrunnelsen bak retningslinjer, krav og policy. De ansatte kan da delta i diskusjoner slik at en middelvei mellom brukervennlighet og sikkerhet kan etableres [2].
Skatteetaten og Norsk Tipping har en strategisk plan om å bedre sikkerhetskulturen i sine bedrifter, og vil i den forbindelse etablere et årshjul hvor det skal tas i bruk ulike virkemidler for å sette fokus på sikkerhet, øke sikkerhetskompetansen, og få kontinuerlig og helhetlig fokus på sikkerhet gjennom året.
Som del av denne planen ønsket oppdragsgiver en tilbakemelding på hvilket kunnskaps- og kompetansenivå innenfor informasjonssikkerhet de ansatte bør ligge på, i tillegg til en opplæringsmetode basert på hvordan man kan nærme seg dette nivået igjennom en brettspillbasert læringsform. Den læringsformen som oppdragsgiver ønsket å benytte er basert på deres positive erfaring med denne typen metode fra tidligere [3].
Oppgaven er avgrenset til å dreie seg om opplæring i sikkerhets- kultur og kunnskap innad i oppdragsgivernes virksomheter. En fullstendig risikoanalyse av oppdragsgiverne var ikke en del av oppgaven, men vi benyttet deler av en slik prosess til å gi merverdi til oppdragsgiverne. Merverdien var i form av tilbakemeldinger basert på funn og analyse av gjennomførte intervjuer samt observasjoner som bachelor gruppen har gjort seg under prosjektets gang.
Vi fokuserte på et bredt spekter innen informasjonssikkerhet for å bedre den generelle forståelsen til de ansatte. Vi har i tillegg avgrenset fokuset til ansatte med mindre

[1] *Hackerangrep mot bedrifter øker* https://www.nrk.no/norge/hackerangrep-mot-bedrifter-oker_-_-de-kriminelle-har-alltid-overtaket-1.14214930 (Besøkt 07.05.2019)
[2] *Sikkerhetskultur* https://www.nsm.stat.no/om-nsm/tjenester/sikkerhetsstyring/sikkerhetskultur/ (Besøkt 12.03.2019)
[3] *Norsk Tipping fikk IT-sikkerhetspris* https://www.digi.no/artikler/norsk-tipping-fikk-it-sikkerhetspris/304627 (Besøkt 17.01.2019)

kunnskap innen informasjonssikkerhet. For en virksomhet er det viktig at den generelle terskelen for kunnskap er hevet. Dette gjør virksomheten mer robust i det at den gjennomsnittlige ansatte vil være mer på vakt og melde fra om hendelser, samt avvik en finner i arbeidet.
Programmering vil ikke være en del av dette prosjektet, opplæringen vil skje i workshop format og fokuset vil være på læringseffekt fremfor noe annet.

Vår oppgave var å produsere et fysisk brettspill rettet mot opplæring innen informasjonssikkerhet. Målgruppen for spillet var ansatte uten arbeidsoppgaver med konkret relevans innen sikkerhet i en alder mellom 35 - 45 år, men alderen var ikke av største prioritet. I prosjektet har vi gjennomført intervjuer for å samle informasjon om hva som engasjerer, samt få en forståelse for hvilket nivå de ansatte ligger på. Basert på denne informasjonen har vi utviklet et brettspill som fokuserer på generelle konsepter innen informasjonssikkerhet og bestepraksis som er nyttig for alle og enhver å kunne. Oppdragsgiverne ønsker i tillegg økt bevissthet rundt sikkerhetskultur slik at ansatte deltar i diskusjonen om sikkerhetsrelaterte problemstillinger. Problemstillingen vår var som følger: Hvor effektivt brettspill er i opplæring av informasjonssikkerhet?

I rapporten ønsker vi å svare på følgende forskningsspørsmål:

1. Hvilke virkemidler kan benyttes i et brettspill for å fremme læring?
2. Hvordan kan man engasjere deltakerne i spillet?
3. Hvordan kan vi teste effekten til brettspillet på de ansattes kunnskap?
4. Hvor godt fungerer brettspill for opplæring i informasjonssikkerhet?

1.2 Formål

Gjennom dette prosjektet ønsket vi å se på hvor god sikkerhetskulturen er hos oppdragsgiverne, samt å se på hvor informasjonssikkerhetsnivået ligger blant de ansatte i målgruppen. Vi ville også gi tilbakemelding til oppdragsgiverne over områder som kan forbedres, og avvik som vi oppdager gjennom prosjektets gang. Rapporten skal beskrive tanker rundt hvordan man kan lage et brettspill som skal fremme læring og funn hos virksomhetene som vil være relevante til brettspillets innhold. For å vise mer konkret hva målet med prosjektet er fokuseres det på to deler, effektmål og resultatmål.

Effektmål

Effektmålene representerer de langsiktige virkningene hos oppdragsgiverne ved prosjektet. De effektmålene som er satt representerer en ønsket endring fra dagens situasjon. Det betyr ikke nødvendigvis at punktene i effektmålene er dårlige per dags dato, men at det er punkter hvor det ønskes en forbedring fra dagens situasjon.

- Redusere risiko for ubevisste hendelser relatert til sikkerhet.
- Øke interessen for sikkerhet blant ansatte.
- Øke sikkerhetskulturen i bedriftene.

Resultatmål

For å oppnå effektmålene er det nødvendig å konkretisere hvordan disse skal oppnås, dette gjøres ved å lage resultatmål. Resultatmålene representerer hva som skal være gjennomført når prosjektet er ferdig.

- Utarbeide god og relevant opplæringsmateriell innen informasjonssikkerhet for ansatte.
- Produsere et brettspill.
- Måle effekten av opplæringen.

1.3 Målgruppe

Vi har tidligere snakket om målgruppen for brettspillene innad i virksomhetene. Når det snakkes om målgruppen her, menes det hvem som kan ha interesse av å lese prosjektrapporten. Prosjektrapporten kan være interessant å lese for følgende:

- Ledere som ønsker å forbedre sikkerhetskunnskapen hos de ansatte, og som ønsker å forbedre sikkerhetskulturen i sine bedrifter.
- Personer som ønsker å se hvordan man kan anvende brettspill til å formidle kunnskap.

Ifølge NorSIS [4] er nordmenn dårlig rustet til å møte den digitale revolusjonen. Derfor vil rapporten være til hjelp for de som ønsker å lære mer om informasjonssikkerhet og hva man kan gjøre for å bedre sine holdninger i den digitale verden.

1.4 Gruppens bakgrunn

Prosjektgruppen består av fire personer som tar en bachelor i IT-drift og informasjonssikkerhet ved NTNU i Gjøvik. Studiet tilsier at prosjektmedlemmene i stor grad er kvalifiserte til å gjennomføre denne oppgaven. Spesielt relevante fag for denne oppgaven er; "Systemutvikling (IMT2243)", "ITSM, risikohåndtering og risikoledelse (IMT2008)", "Innføring i IT-drift og informasjonssikkerhet (IMT1003)", "Incident Response, Ethical Hacking Forensics (IMT3004)". Gruppemedlemmene stiller også med diverse valgfag, hvorav Programvaresikkerhet (IMT3501) er relevant. Andre fag som ikke nødvendigvis er relevant i forhold til oppgaven er diverse programmeringsfag, datanettverk og nettverkssikkerhet, matematikk, operativsystemer, drift av tjenestearkitektur, databaser og modellering.

Ingen av gruppens medlemmer har erfaring med statistikk, men en av gruppens medlemmer er særdeles flink i matematikk og tok på seg ansvaret for å lære seg dette. Gruppens medlemmer har erfaring med brettspill, men ikke utvikling av det så det er noe alle må sette seg inn i. Rapporten er skrevet i LaTeX, noe alle medlemmene er kjent med fra tidligere. Medlemmene har litt erfaring med intervjuer gjennom prosjekter som er gjort tidligere i studieløpet. Spørreundersøkelser er det liten erfaring med fra før og er noe gruppen trenger å lære.

1.5 Rammer

1.5.1 Arbeidsmetode

Dette prosjektet har ikke handlet om programvareutvikling, og prosjektet har krevet lite iterativt arbeid. Vi så først på Scrum[5] som en mulighet for utviklingsmodell, men på

[4] *Nordmenn og digital sikkerhetskultur 2018* https://norsis.no/nordmenn-og-digital-sikkerhetskultur-2018/ (Besøkt 08.03.2019)

[5] *Scrum* https://no.wikipedia.org/wiki/Scrum (Besøkt 11.05.2019)

grunn av sterke sekvensielle preg i prosjektet og oppgavens natur ville tid brukt på møter om revidering ikke blitt brukt effektivt. Vi valgte derfor å bruke Fossefallsmodellen [6] i det generelle prosjektet, og benyttet en nedskalert versjon av Scrum under kravspesifikasjonen til brettspillet. Det ble holdt ukentlige gruppemøter hvor vi gikk gjennom det som har blitt gjort i tiden før møtet, og det som skulle gjøres gjennom uken. For gruppemedlemmene lokalisert på Gjøvik ble det satt en retningslinje om å møtes på universitetet kl. 09 - 17 hver dag, med unntak av opplegg i andre fag. Arbeid som hvert gruppemedlem har gjort til enhver tid ble kontinuerlig gjennomgått av de andre medlemmene for revidering og kvalitetssjekk.

1.5.2 Tidsmessige rammer

Innleveringsfristen er den eneste absolutte tidsmessige rammen vi har hatt. Den måtte overholdes for å gjøre prosjektet til en suksess. De andre rammene har vært litt mer fleksible. Vi hadde også mange muligheter til å subsidiere forskjellige komponenter under prosjektet dersom noe skulle gå galt. For eksempel har vi benyttet studenter som ikke går informasjonssikkerhets rettede linjer til spilltesten vår. Selv om vi har hatt muligheten til å være fleksible så har vi forholdt oss til milepælene som vi satte oss i begynnelsen av prosjektet M.

- Innsamling av informasjon fra oppdragsgivernes virksomheter innen 1. mars
- Prototype av spillet må være ferdig før slutten av påsken (23. april).
- Test av spillet 1. uken i mai.
- Innleveringsfrist for oppgaven er 20. mai

1.5.3 Økonomiske rammer

Siden oppdragsgivere holder til i Hamar og Oslo har dette innebæret transportkostnader som vi har stå for selv. Materialer brukt i presentasjon av brettspillet har blitt dekket av gruppemedlemmene med en grense på totalt 400kr.

1.6 Roller

Alle gruppemedlemmene har hatt et generelt ansvar for å jobbe godt med oppgaven. Dette har innebærert å utføre arbeidsoppgavene innen den satte tidsfristen og å føre opp antall timer som man har jobbet. De spesifikke rollene er beskrevet under:

- **Prosjektleder:** Daniel Magnus
  Lederen har hatt ansvar for å sette opp møter med gruppen, veiledere og oppdragsgivere, samt kommunikasjon mellom veiledere og oppdragsgivere. Lederen har hatt ansvaret for å lage en agenda for gruppemøter. Lederen har hatt ansvar for å fordele arbeidsoppgaver i samarbeid med de andre gruppemedlemmene under møter. Lederen har hatt ansvar for å løse konflikter innad i gruppen så godt det lar seg gjøre uten hjelp fra veiledere.
- **Sekretær:** Abu Baker Al-Shammari
  Personen har hatt ansvar for å skrive møtereferat, hatt oversikt over intervjuer og dataene fra spørreundersøkelsen. Sekretæren har også notere hva som trengs å jobbe med videre, også etter gruppemøter om noe mangler. Dokumentere valgene våre

[6] *Waterfall model* https://en.wikipedia.org/wiki/Waterfall_model (Besøkt 11.05.2019)

for å vise frem hvilke alternativer vi hadde, og hvorfor vi valgte det ene alternative fremfor det andre.

- **Oppdragsgivere:** Anne Marie Dalen Øverhaug (Skatteetaten), Trond Laupstad (Norsk Tipping) og Emil Volckmar Ry (Norsk Tipping)
  Oppdragsgiverne har bistå med personer til intervjuer og spilltester. De har også bistått med møtelokaler og veiledning.
- **Veiledere:** Gaute Wangen og Ernst Gunnar Gran
  Veilederne har bistå gruppen gjennom prosjektperioden ved å gi råd og generell veiledning til hvordan man skriver og gjennomfører en vitenskapelig rapport.

1.7 Organisering av rapport

Rapporten har følgende struktur:

1. **Relatert arbeid** Dette kapittelet inneholder arbeid som er relatert til vår oppgave.

2. **Metode** Dette kapittelet inneholder en beskrivelse av metodene vi har brukt gjennom prosjektet.

3. **Resultat fra intervju** Dette kapittelet inneholder de resultatene vi har fått gjennom intervjuer hos oppdragsgivere.

4. **Utviklingsprosess** Dette kapittelet inneholder utviklingsprosessen av brettspillet.

5. **Dataanalyse** Dette kapittelet inneholder dataanalyse av de resultatene vi har fått gjennom testing av brettspillet hos oppdragsgivere.

6. **Diskusjon** Dette kapittelet inneholder diskusjoner mot forskningsspørsmålene.

7. **Konklusjon** I dette kapittelet skal vi avslutte oppgaven med svar på problemstilling, kritikk av oppgaven og videre arbeid.

2 Relatert Arbeid

I dette kapittelet skal vi se på relatert arbeid. For å kunne si noe om hva som er relevant i forhold til vår oppgave må vi se på hovedinnholdet i den, altså problemstillingen. Problemstillingen som vi tar for oss i oppgaven er å se på om brettspill kan være en effektiv opplæringsmetode av informasjonssikkerhet. For å underbygge svaret på problemstillingen skal vi gjennom forskningsspørsmålene se på virkemidler for å fremme læring, hvordan engasjere deltakere, hvordan vi kan teste effekten av brettspillet og hvor godt brettspil som opplæringsmetode fungerer. Vår problemstilling innehar 4 hovedområder som vi kan si er relevant i forhold til det å se på tidligere arbeid, dette innebefatter; brettspill, opplæringsmetode, læring og informasjonssikkerhet.

2.1 Tidligere bacheloroppgaver

2.1.1 E-læring i arbeidslivet: Hvordan lykkes når grunnleggende læringsprinsipper møter dagens teknologi

Denne oppgaven[1] ble utgitt av Høyskolen Kristiania i 2018 og tar for seg, blant annet, hvordan ansatte lærer best gjennom å finne hvilke tilstedeværende faktorer som gir best uttelling i forhold til økt læring. Bacheloroppgaven konkluderer med at motivasjon er den viktigste faktoren for opplæring av ansatte. De viser til at uten motivasjon til selve læringen så vil de andre læringsmetodene og/eller læringsprinsippene som er benyttet ha mindre betydning, men valget av type læringsmetoder og/eller læringsprinsipper kan allikevel bidra til å øke motivasjon. Det anbefales å stimulere nysgjerrigheten til de ansatte som en god måte å motivere dem på, samt å dele opplæringen til "det man må vite" og "det som er fint å vite". For å finne grunnlagsdata til bruk i sin oppgave så har de blant annet benyttet en kvalitativ undersøkelse, dette i form av et dybdeintervju med aktuelle kilder.

Utbytte til videre bruk i oppgaven

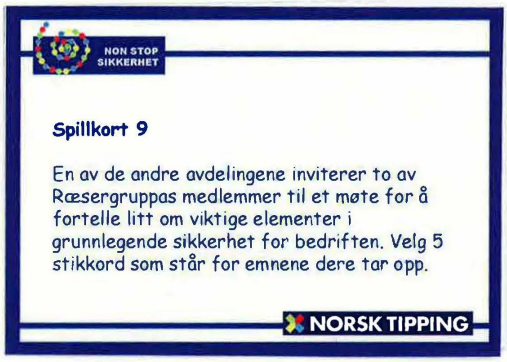
Siden vår oppgave i stor grad går ut på opplæring av ansatte og økt kompetanse innenfor informasjonssikkerhet så er det veldig relevant å se på denne oppgavens funn, på hva som fungerer best i forhold til faktorer som påvirker læring. Bacheloroppgaven viser at faktorene motivasjon og stimulering av nysgjerrighet (for å fremme motivasjon) er de faktorene som utpeker seg som gode måter å fremme læring. Derfor tar vi med oss disse to faktorene videre inn i arbeidet med utviklingen av brettspillet samt dets læringsmetoder og opplæringsinnhold.
De har i tillegg benyttet seg av dybdeintervju i sin undersøkelse for å innhente informasjon fra bedrifters ansatte og ledere. Og ettersom vi ønsker å innhente grunnlagsdata fra bedriftenes ansatte så er denne oppgavens kvalitative undersøkelse noe som er aktuelt å se på i forhold til hva de har lagt vekt på for valgt metode i forhold dybdeintervju, og i tillegg deres utforming av intervjuguide.

2.2 Sikkerhetsspill

2.2.1 Oppdragsgivers sikkerhetsspill

Norsk Tipping har tidligere selv utviklet et sikkerhetsspill (Non Stop Sikkerhet), og fikk i 2002 IT-sikkerhetspris for dette. Spillet tok for seg IT- og informasjonssikkerheten til selskapet med bakgrunn i å øke sikkerhetsforståelsen til de ansatte. De kunne dokumentere en økt sikkerhetsbevissthet hos selskapets ansatte ved bruk av sikkerhetsspillet[1].

Spillet var utformet på en slik måte at de ansatte fikk tildelt relevante og aktuelle sikkerhetsproblemer som scenario eller åpne spørsmål, hvorpå disse skulle diskuteres og løses av alle som gruppe før de gikk videre i spillet. De hadde også muligheten til å benytte ansattinstruksen som oppslagsverk. Se eksempel på spillkort i figur 1 nedenfor.
Selve spillbrettet er utformet med en enkelt rute fra start til mål, og feltene har forskjellige farger som viser til hvilken kategori det skal hentes spørsmål fra. I tillegg er det benyttet sterke farger (bedriftens farger) samt figurer med litt humoristisk preg. Se selve spillet i figur 2.
Brettspillet har fire forskjellige kategorier på spørsmålene. Dette inkluderer også kategorien bonusspørsmål som er et fordelskort i form av premie eller muligheten til å rykke frem 1 til 3 felter. De tre andre kategoriene er spørsmål innenfor generell sikkerhet, IT-sikkerhet og informasjonssikkerhet.



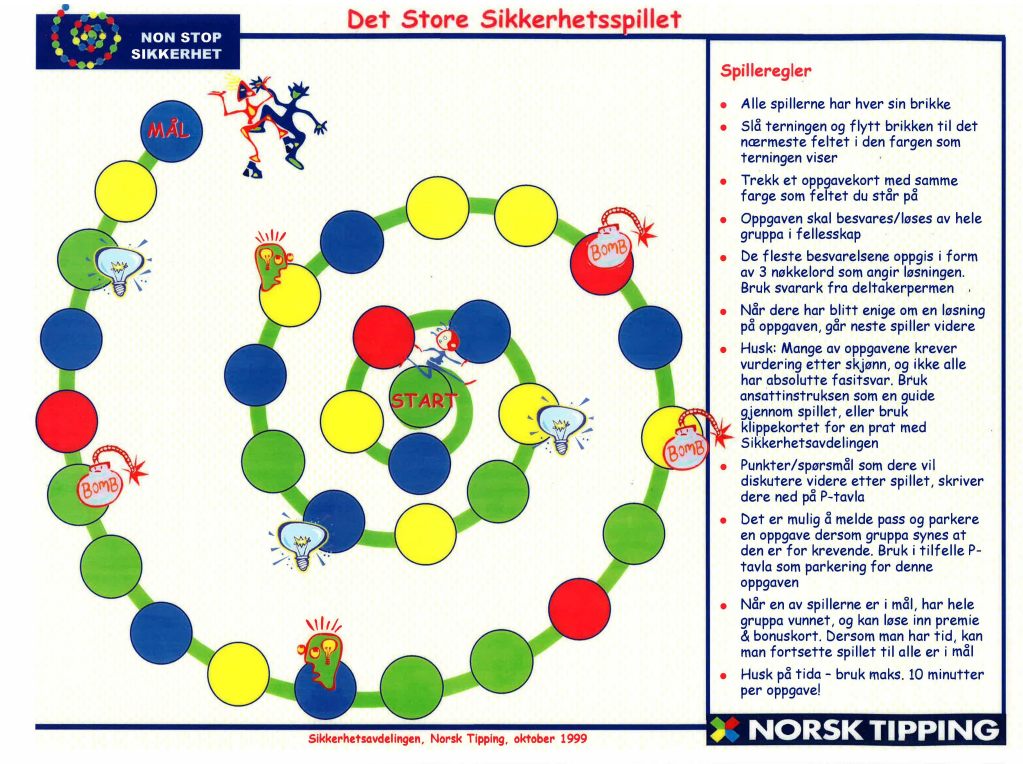
Figur 1: Eksempel på spillkort i Non Stop Sikkerhet

Mange av spillekortene inneholder spørsmål om informasjonssikkerhet som for så vidt er like relevant i dag som for 20 år siden. Andre kan vel sies å være litt utdaterte i forhold til utviklingen som har skjedd de siste 20 årene, hvilket trusselbilde vi står ovenfor i dagens bedrifter og samfunnet generelt, spesielt med tanke på digitalisering og teknologiske løsninger. I tillegg rettes mye av opplæringen (spørsmålene) seg mot den spesifikke bedriftens instrukser/policy og ikke så mye mot den generelle og grunnleggende opplæring innenfor informasjonssikkerhet.

Utbytte til videre bruk i oppgaven

Spillebrettet og spillet i seg selv er enkelt å forstå og lengden fra start til mål er ikke for lang slik at man kan komme igjennom innen rimelig tid. Dette kan bidra til at deltakeren opprettholder interessen, noe som kanskje gjør det enklere å delta i diskusjon, holde fokus og innta informasjon. Mye av læringen i spillet kan sies å basere seg på deling av

[1] *Norsk Tipping fikk IT-sikkerhetspris* https://www.digi.no/artikler/norsk-tipping-fikk-it-sikkerhetspris/304627 (Besøkt 17.01.2019)



Figur 2: Non Stop Sikkerhet

kunnskap og diskusjoner rundt aktuelle sikkerhetstemaer, noe som kanskje kan fremme en bedre sikkerhetskultur i bedriften i tillegg til økt sikkerhetskunnskap hos de ansatte. Områdene som er omtalt i dette avsnittet er noe vi ønsker å ta med videre i arbeidet med utviklingen av brettspillet.

2.2.2 Opplæringsmateriell i brettspill

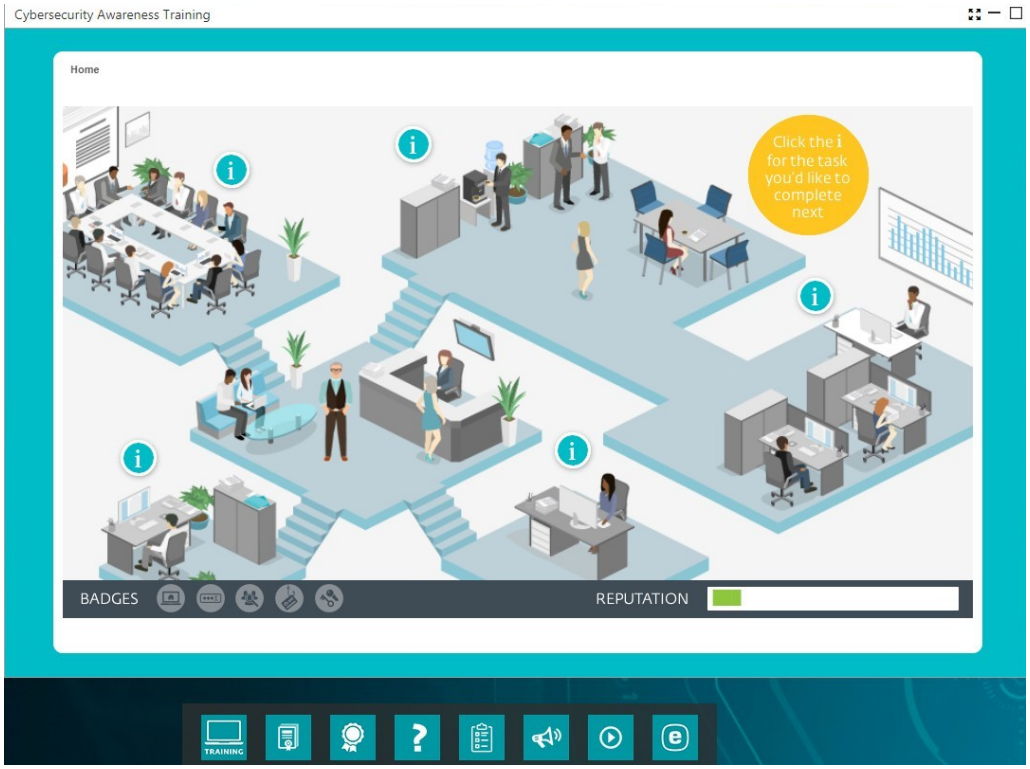
Utbyttet av opplæringen skal være økt kunnskap innenfor informasjonssikkerhet, men det skal omhandle kunnskap på nevnte området som er relevant for oppdragsgivers målgruppe og deres arbeidsområder. Målgruppen til brettspillet omfavner stillinger utenom IT-faget. Brettspillet skal derfor ta for seg den generelle kunnskapen og basis kunnskapen om informasjonssikkerhet med henblikk på dagens trusselsituasjon for norske bedrifter generelt. For å innhente/lage kunnskapsspørsmålene til brettspillet har vi derfor innhentet inspirasjon og opplæringsmateriell fra lærebøker[4], informasjonssikkerhetsspill[2], forskjellige quiz på nett som omhandler informasjonssikkerhet og bevissthet på informasjonssikkerhet, oppdragsgivernes egne sikkerhetspolicy/sikkerhetsinstruks (regler og instrukser som er generelle og lik), i tillegg til kunnskapen om informasjonssikkerhet som vi har tilegnet oss gjennom dette bachelorstudiet.

2.2.3 ESET Cybersecurity Awareness Training

Selskapet ESET har laget et cybersikkerhetstreningsspill som er tilpasset bedrifter som ønsker et opplæringsverktøy som går på det grunnleggende innenfor informasjonssikker-

[2] *ESET Cybersecurity Awareness Training* https://www.eset.com/us/cybertraining/ (Besøkt 15.03.2019)

het, og i forhold til dagens mest kjente trusler mot bedrifter generelt[3].
Spillet er nettbasert hvor den ansatte velger seg en avatar som inngår i spillets IT-avdeling og vil gjennom spillets forskjellige lokaliteter hjelpe andre ansatte med forskjellige problemer relatert til cybersikkerhet. Spillet er delt opp i forskjellige områder som relateres til en bedrifts lokaliteter, se figur 3. Spillet innehar 5 moduler som tar for seg områdene: Trusler (Skadevare, Phishing, Sosial manipulering), passordsikkerhet (beste praksis, 2FA og hvordan bruke det), internettsikkerhet (hva man bør se etter og hva man bør unngå), e-postsikkerhet (hva man bør se etter og hva man bør unngå) og forebyggende tiltak (beste praksis hjemme og på jobb). Hver modul (område på spillbrettet) inneholder et hovedspørsmål som du gjennom modulen skal finne svaret på, en kort opplæringsvideo innenfor modulens område (2 minutter), fulgt av flere oppgaver (spørsmål/scenario) som skal besvares. Disse oppgavene fremstilles på en litt humoristisk og annerledes måte (musikk, animasjon m.m.) slik at den som gjennomfører oppgavene kanskje kan holde interessen for opplæringen lenger. Etter å ha gjennomført alle 5 modulene (med nok riktige svar) kan det tas en sertifiseringstest med spørsmål som omhandler alle modulene.



Figur 3: Inspirasjon til utforming av spillebrettet

Utbytte til videre bruk i oppgaven

Selve "spillebrettet" viser tydelig at spillet omhandler en bedrift og dets forskjellige lokaliteter og avdelinger. Dette kan gjøre at spillerne klarer å knytte opplæringen til de forskjellige områdene (og de ansattes arbeidshverdag) som blir presentert, og er noe vi tar med videre i utviklingen av brettspillet. I tillegg inneholder spillet mange gode spørsmål/scenario og svaralternativer innenfor cybersikkerhet som vi ønsker å benytte fult ut

[3] *ESET Cybersecurity Awareness Training* https://www.eset.com/us/cybertraining/ (Besøkt 15.03.2019)

og/eller som inspirasjon til selvlagede spørsmål og svar.

2.3 Forskning på læringsmetoder

Det finnes flere forskninger rundt dette med brettspill som opplæringsmetode og effekten av den. En god del av det er rettet mot læring for studenter, men det finnes også undersøkelser som tar for seg opplæring med brettspill for ansatte i bedrifter. Vi tar for oss en av disse forskningene som retter seg litt mer mot ansatte i bedrifter for å se litt nærmere på hvilken opplæringseffekt en slik type opplæringsmetode kan ha.

Vi kommer også til å se på trendene for året som har gått som omhandler læringsmetoder. Her viser forskningen vi har tatt for oss, læringsmetoder som forskerne mener å ha en innvirkning på utformingen av dagens og morgendagens utdanningsmetoder.

2.3.1 Investigating retention and workplace implementation of board game learning in employee development

Denne artikkelen tar for seg forskning som omhandler dette med brettspill som læringsmetode i forhold til opplæring på arbeidsplassen[2]. Den ser på deltagernes opplevelse av BGL som et opplæringsverktøy, hvilken grad av læringen som deltagerne sitter igjen med, hvordan de implementerte læringen på deres arbeidsplass, hvordan forståelsen for deres arbeidsplass økte gjennom BGL og hvorvidt deres selvtillit fortsatt var høy etter at de hadde spilt brettspillet.

Utfall av undersøkelsen

Hovedfunnene i undersøkelsen viser til at deltakerne husket selve brettspillet godt og læringen fra brettspillet. De hadde også tatt i bruk noe av læringen fra brettspillet i sitt arbeid. Bakgrunnen for funnene ble innhentet i et intervju utført 1 år etter gjennomføring av brettspillet.

Deltakerne gir uttrykk for at erfaringen med brettspill som opplæringsmåte har vært fordelaktig i form av bedre ferdigheter innenfor området som opplæringen har tatt for seg, og en bedre forståelse av opplæringsområdets helhet innenfor bedriften. Som undersøkelsens hovedfunn viser, så føler majoriteten av deltakerne at de så absolutt husker læringen fra brettspillet og at de har fått en bedre forståelse av brettspillets opplæringsområde relatert til deres arbeidsplass. De følte også at selvsikkerhetsnivået i forhold til kunnskap innenfor opplæringsområdet hadde økt etter brettspillet, og at det hadde forblitt høyt lenge etter at spillet var utført.

Ut fra deltakernes tilbakemeldinger så konkluderes det med at implementeringene av brettspillet/BGL, og læringen fra det, har gitt deltakerne økt kunnskap og selvsikkerhet innenfor opplæringsområdet i tillegg til at læringen huskes selv etter et helt år.

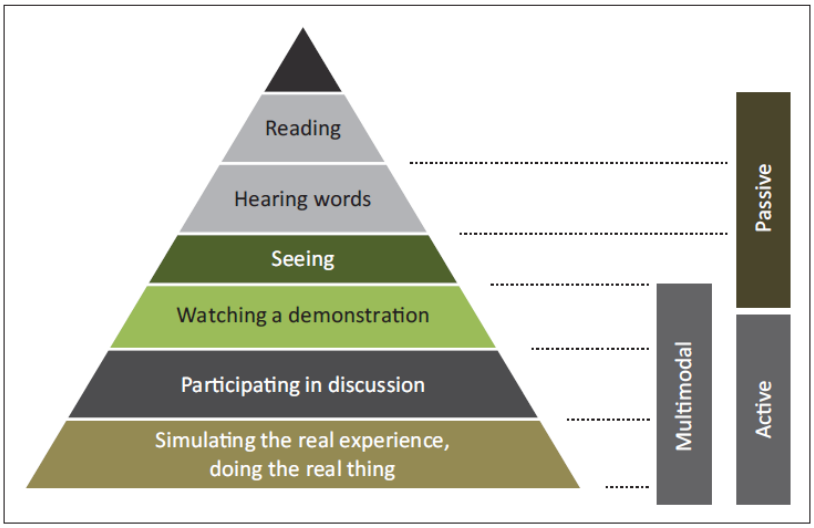
Forsking på effekt av læringsformen

Det refereres også til andre forskningsrapporter i artikkelen som viser til at læring gjennom spill gir et positivt utbytte i form av motivasjon og økt læringseffektivitet. På grunn av at man gjennom spill som regel innehar en mer aktiv rolle, og har mer interaksjon/-diskusjon med spillerne/gruppen, enn ved læring gjennom leksjoner e.l. viser forskning at man lærer mer.

Når det kommer til brettspill generelt så viser undersøkelsen til at disse innehar omgivelser som virker lite truende, lekent og konkurransepreget, noe som vil styrke læring og

bruk av innholdet i spillet. I tillegg vil utformingen av selve brettet visuelt gi deltakeren en kobling til innholdet i brettspillet.

Det vises også til tidligere forskning på hva som sitter igjen av læring. Her påvises det at det er forskjell på hvordan man lærer best, eller hvilken type læring som sitter igjen mest. Det læres mer når læringen praktiseres/brukes, læringen sitter bedre desto sikrere man er på at svaret man gir er korrekt, men det vises også til at voksne lærer på en annen måte enn unge studenter. Forskning viser at mennesker har en tendens til å huske mindre av det man leser og mer av det man gjøre. Å benytte spill i opplæring vil ha en positiv effekt på hjerneaktiviteten som stimulerer til mer læring og graden av læringen som huskes øker, og gjør at deltakerne av spillet engasjerer seg, noe som gir en effektiv forståelse av opplæringsområdet spillet tar for seg. Se figur 4 fra artikkelen som viser pyramiden av effektiviteten i læringsformer benyttet i forskning om voksen opplæring.



Source: Northwest Center for Public Health Practice, 2015, *Effective adult learning: A toolkit for teaching adults*, NWCPHP, University of Washington School of Public Health, Washington, DC, p.15

FIGURE 1: The cone of learning.

Figur 4: Effektivitet i læringsformer, voksenopplæring

Utbytte til videre bruk i oppgaven

Denne undersøkelsen gir oss en indikasjon på at brettspill kan være en god måte å gjennomføre opplæring av fokusområder i bedrifter. Spill i seg selv kan motivere i tillegg kan det stimulere hjerneaktiviteten og gjøre deltakerne engasjerte, og dette kan igjen føre til økt kunnskap og skape selvsikkerhet (hos de ansatte) innenfor opplæringsområdet brettspillet tar for seg. Faktorer i forhold til selve brettspillet som ut fra forskingen kan være viktig å ta med videre i utviklingen av brettspillet (for å fremme læring og bruk av opplæringsinnholdet i spillet);

- By opp til en mer aktiv rolle
- Omgivelser som virker lite truende
- Lekenhet
- Konkurransepreget
- Visuelt gi deltakerne en kobling til innholdet i brettspillet

I tillegg gir undersøkelsen viktige momenter å ta med seg videre knyttet til opplæringsdelen av brettspillet. Dette i form av læringsmetoder som gir best utbytte for effektiv opplæring og lengst læringseffekt, spesielt med tanke på opplæring av voksne. Dette innebefatter blant annet disse punktene;

- Mer læring når læringen praktiseres/brukes.
- Desto sikrere man er på svaret, desto bedre "sitter det".

2.3.2 Trends in learning Report 2018

The Open University har utgitt en rapport med bakgrunn i forskning som er utført av universitetets Institute of Educational Technology, som viser trender innenfor læring gjennom det siste året (2018)[7]. Rapporten viser til at det er en endring i opplæring ved bedrifter. Den endringen innebefatter at opplæringen baserer seg mer på hvordan folk lærer best og hvordan læringen kan brukes og implementeres i arbeidshverdagen til de ansatte. Universitets institutt anser seg selv for å være en av de ledene når det kommer til identifisering og utvikling av nye teknologiske metoder for å forbedre læring. Hvert år undersøker de det siste innenfor nyskapende undervisning og læring som de mener er med på å forme dagens og morgendagens utdanningsmåter. De utreder også konsekvenser ved å innføre disse nye innovasjonene i forhold til læring og utvikling på arbeidsplassen, i tillegg til hvordan de brukes på arbeidsplassen per dags dato.

Rapporten viser til 5 læremetoder; spaced learning, post-truth learning, immersive learning, student-led analytics og humanistic knowledge. Nedenfor vises en kort forklaring på de forskjellige læremetodene.

- Spaced learning: 3 korte læringssekvenser med kortere avbrekk som benyttes til relatert aktivitet. Repetisjon i denne formen for læring hjelper både menneskets korttids- og langtidsminne. Deler opp læring i mindre deler, gjør at læringen blir mer håndterbar, overkommelig og lettere å huske for de ansatte.
- Post-truth learning: Omhandler det å "tenke seg om", og/eller innhente informasjon før man gjør/utfører noe. Dette for å søke validitet for så å kunne ta gjennomtenkte og/eller logiske avgjørelser.
- Immersive learning: Benytte realistiske scenarioer som skal løses. En måte å utføre noe som ligner en reell situasjon, før en slik situasjon oppstår. Gjøre læringen mer

interaktiv, enklere å huske og man får trening på reelle situasjoner i et lukket og sikkert miljø.
- Learner-led analytics: Analyse av data for å finne den beste og mest målrettede læringsveien for enkeltpersoner, personalisere læringen. Kan også benyttes til å få en forståelse av ferdighetsnivået i en bedrift, se hvor "gapene" er og se etter trender.
- Humanistic knowledge building communites: Handler om fellesskapet innenfor en organisasjon og hvordan de hjelper hverandre til å utvikle kunnskap ved hjelp av deling. Gjør arbeidet mer engasjerende, øker samholdet (dette vil også kunne føre til økt tryggheten til hverandre), og får jobben til å fremstå mer "menneskelig".

Utbytte til videre bruk i oppgaven

Rapportens forskere har foretatt en vurdering i hva de mener er de beste læringsmåtene for bedrifter både i nåtid og nær fremtid. Derfor kan læremetodene nevnt i rapporten være aktuelle for vår oppgave. Læringsmetodene i denne rapporten baserer seg mest på teknologiske løsninger for å utføre læringsmetodene, men det betyr ikke at man er bundet av å benytte metodene kun ved hjelp av teknologiske løsninger. En god del av disse læringstypene er det fullt mulig å implementere i et brettspill. Det som kan være aktuelt å ta med videre i oppgaven er hovedinnholdet i alle læringsmetodene som denne rapporten tar for seg, altså følgende:

- Dele den informative/opplærende biten i mindre deler, med repetering i form av forskjellige vinklinger av spørsmål innenfor det samme området,
- måtte tenke seg om for å ta gjennomtenkte og/eller logiske beslutninger,
- benytte scenarioer/spørsmål som kan kobles til realistiske situasjoner,
- "personalisere" læringen gjennom data-analyse,
- fremme deling og samhandling som en del av læringen.

2.3.3 Oppsummering

Det finnes mye relatert arbeid som omfavner de områdene vi har fokusert på å hente informasjon om i dette kapittelet, og vi kunne nok sikkert ha hentet ut mer som hadde vært relevant for oppgaven vår. Vi har valgt å plukke ut det vi mener er mest relevant for oppgaven og som gir oss nok informasjon til å bygge oppunder utviklingen og opplæringsinnholdet av brettspillet, og som i tillegg kan være med å danne grunnlaget til svar på noen av våre forskningsspørsmål i oppgaven.

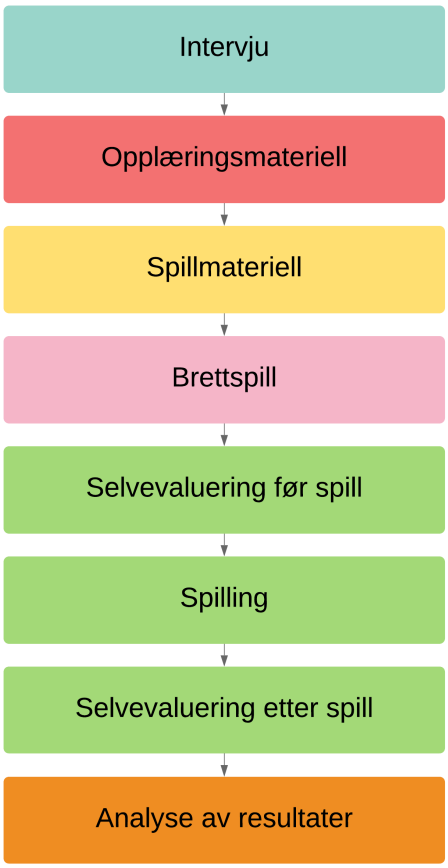
I innledningen refererte vi til 4 forskjellige områder som var relevant i forhold til relatert arbeid, og gjennom de forskjellige relaterte arbeidene har vi kunne hente ut faktorer og viktige punkter å ta med i videre arbeid, og som grunnlag til å kunne besvare noen av forskningsspørsmålene delvis eller helt.

Konklusjonen fra dette kapitelet er at brettspillet i seg selv bør være enkelt å forstå/-spilles, spillets "lengde" bør ikke være for lang, bør skape diskusjoner, inneholde konkurranse elementer, være lekent og viktigheten av et visuelt uttrykk som viser innholdet i spillet. Det kan nevnes at vi også har innhentet inspirasjon fra velkjente brettspill for å utforme elementene som omhandler konkurranse, lekenhet og forståelse i våres brettspill. I forhold til læring så vises det til at motivasjon er en av de viktigste faktorene for læring. For å fremme motivasjon må man finne måter å stimulere nysgjerrigheten rundt selve læringen. I tillegg kan dette med å ufarliggjøre og det å gi trygghet være viktige faktorer i forhold til læring. Når det kommer til opplæringsmetoder så ser vi at dette med å være

deltagende/delaktig er viktig. Dette påvises å bli mer og mer aktuelt desto eldre vi blir. Ettersom målgruppen for oppgaven også er rettet mot den litt eldre garde av ansatte så vil disse faktorene være viktige å ta med. I tillegg vises det til at man husker mer av det man lærer ved kortere intervaller av opplæringsinformasjon, med repetisjoner (gjerne gjennom å utføre det man har gått igjennom). Et annet moment som er viktig å ta med i betraktning, spesielt i forhold til brettspillets svaralternativer, er det med at; det man er sikker på er riktig, huskes bedre. Å dele kunnskap slik at man kan ta gjennomtenkte og logiske beslutninger er også en viktig faktor. For å kunne finne grunnlaget for utarbeidelsen av brettspillet er det viktig å innhente data fra målgruppen til brettspillet. Dette for å kunne skape et godt tilpasset brettspill med relevant innhold og riktig kunnskapsnivå på opplæringsmateriellet.

3 Metode

Dette kapittelet skal omhandle metoder vi har brukt for å besvare forskningsspørsmålene. Figur 5 representerer det vi gjorde gjennom oppgaven vår. Det er en veldig sekvensiell figur som gjorde det lett å se hva som skulle gjøres til enhver tid. De fleste punktene fra modellen kommer til å bli diskutert i dette kapittelet. Resultatet av spilltesten vil bli diskutert i kapittelet om dataanalyse 6.



Figur 5: Inkrementell plan for oppgaven

3.1 Intervju

I den innledende delen av datainnsamlingen dannet vi grunnlaget for videre arbeid med utvikling av brettspillets innhold og læringsmåter. Vi ønsket å lære mer om forskningsspørsmål 1 og 2, virkemidler til læring og engasjement i spill. Vi ønsket også å få et inntrykk av kunnskapsnivået til målgruppen slik at vi kan lage et spill som er tilpasset dem. Videre vil vi diskutere ulike metoder dette kan gjøres på, og finne den som eg-

ner seg best for gode resultater. Den følgende metoden er hentet fra boken "Hvordan gjennomføre undersøkelser" [[3] side 125-153].

3.1.1 Valg av samfunnsvitenskapelig metode

Grunnlaget som vi ønsker å hente baserer seg på innhenting av data i form av ord. Dette kalles for et kvalitativt resultat i den samfunnsvitenskapelige metoden. Hvis datainnsamlingen baserer seg på tall i stedet for ord så kalles det et kvantitativt resultat. I et spørreskjema med flervalg vil det kunne være mulighet for å uttrykke seg i form av ord hvis de faste svarene er bygd opp av setninger og ikke tall. Hvert svar er forhåndsdefinert og har en form for tall i rekkefølgen, derfor vil det anses som et kvantitativt resultat i den samfunnsvitenskapelige metoden.

Det finnes forskjellige typer data som kan samles inn, dette gjelder for begge metodene nevnt ovenfor (kvalitativ og kvantitativ). Primærdata for den kvalitative metoden vil være å innhente data direkte fra den primære kilden, som i dette tilfellet er målgruppen til spillet og oppdragsgiverne til denne oppgaven. Dette kan utføres enten ved å gjennomføre et intervju eller ved observasjon. Når det gjelder de kvalitative sekundær dataene så vil dette være tekster og opplysninger som ikke er innhentet direkte hos den primære kilden, men som kan være med å belyse og understøtte grunnlaget vi er på jakt etter å sette.

3.1.2 Fordeler og ulemper med den kvalitative metoden

Den kvalitative undersøkelsesmetoden er en åpen metode, det vil si en metode hvor det legges lite føringer på dataene som skal hentes inn. En av fordelene ved å velge en kvalitativ undersøkelsesmetode er at hver enkelt respondent vil kunne bidra til å finne forskjellene i forhold til oppfattelse av temaene vi ønsker å utdype ved hjelp av intervjuer. Og gjennom den kvalitative intervjuprosessen kan det også være at vi ser at det er områder eller avgjørelser som er tatt tidligere i prosjektet som burde endres.

Bakdelen med å benytte en kvalitativ tilnærming kan være at hvert enkelt intervju, med mange områder og tema som skal besvares, tar mye tid. Dette gjør derfor at man må velge et fåtall intervjuobjekter for at det skal være gjennomførbart. Problemet med at datainnsamlingen baserer seg på få respondenter er vurderingen om dette er representativt nok for en generell forståelse av områdene og temaene som det ønskes å belyse. Et annet problem kan være at en, gjennom denne metoden, blir sittende med store mengder data, og til tider mye ustrukturerte data på grunn av at den er innhentet uten de store føringene under selve intervjuet. Effekten av undersøkelsen er også et område som må tas i betraktning. Denne kan bli påvirket av flere forskjellige faktorer, for eksempel føringer som intervjueren ubevisst legger i spørsmål til intervjuobjektet eller generell utrygghet hos respondenten i intervjusituasjonen. Selv om fleksibiliteten i stor grad er en fordel ved den kvalitative metoden så kan den i visse situasjoner skape en uheldig situasjon ved at man stadig finner områder eller avgjørelser som burde endres på, slik at man ikke kommer frem til en avslutning.

3.1.3 Utførelsen av den kvalitative undersøkelsen

Ettersom hverken oppdragsgiver eller vi har kapasitet, ressurser eller tid til å gjennomføre en lengre periode med observasjoner vil vi fokusere på å utføre intervjuer. Vi vil gjennom åpne samtaler med oppdragsgiver innhente både primærdata og sekundærdata. Primærdata vil kunne være å få en tilbakemelding på deres syn av bedriftenes trusselbilde og sekundærdata i form av informasjonssikkerhets regler, instrukser og policy som benyttes. Sekundærdataene vil kunne være med å sette det ønskelige nivået for kunnskap om informasjonssikkerheten i bedriftene, i tillegg til annen sekundærdata vi innhenter som går på grunnprinsipper[1] og grunnkunnskap rundt informasjonssikkerhet og reelle trusler som berører oppdragsgiverne[2]. Formålet med intervjuene vil være å kartlegge hvilken kunnskap de innehar i forhold til informasjonssikkerhet, hva som skal til av virkemidler for å få de interessert i brettspill som opplæringsmetode, og hvilke opplæringsmetoder de synes fungerer best for dem. Her vil det også være begrensninger i forhold til antall intervjuobjekter på grunn av kapasitet, ressurser og tid både hos målgruppen og hos oss.

Vi valgte å intervjue 8 personer fra oppdragsgiver (4 personer hos hver av bedriftene) med en fordeling på 50/50 i forhold til kjønn. Dette med bakgrunn i overnevnte begrensninger, men vi mener også at antallet og fordelingen gir nok tilbakemeldinger til å kunne se et generelt nivå og standpunkt i målgruppen.

Generelle valg i forhold til intervju med primærkilden

Vi har valgt å utføre våre intervjuer på oppdragsgivernes arbeidsplasser med bakgrunn i å skape best mulig forutsetninger for innsamling av dataene vi er ute etter. Det vises til i den kvalitative undersøkelsesmetoden at fysisk tilstedeværelse i et åpent intervju skaper bedre kontakt med intervjuobjektet, noe som kan gjøre at det er lettere for respondent å «åpne seg» til oss som intervjuere og respondere med et ærlig svar. I tillegg har vi som intervjuere muligheten til å «føle på» når respondenten føler seg ukomfortabel slik at vi kan ufarliggjøre spørsmålene eller sette en strek for spørsmålet og gå videre.

I selve intervjuene har vi valgt å ikke benytte oss av lydopptak. Dette ville selvsagt ha vært til hjelp for oss i forhold til å sikre at vi har fått med all informasjon fra respondentene. Vi mente at dette hjelpemiddelet kan gjøre at respondenten er mer forsiktig med hva hun/han ytrer og kan føre til at vi ikke får en ærlig tilbakemelding. Dette bekreftes også i den samfunnsvitenskapelige metoden. Vi valgte i stedet for å ha en intervjuer og en som noterer i hvert intervju, slik at intervjuer kan fokusere på gode spørsmål/oppfølgingsspørsmål og god kontakt med intervjuobjektet, i tillegg til at den som noterte kun har fokus på dette.

Intervjuguide til intervjuet med primærkilden

I forbindelse med datainnhenting av den primære kilden benyttet vi oss av et åpent intervju, men med en pre-strukturert intervjuguide. Dette gjorde at vi hadde god oversikt over hvilke tema som skulle tas opp og belyses i løpet av intervjuene, i tillegg til rekkefølgen som temaene skulle tas opp. Vi benyttet oss av spørsmål som vi klassifiser-

[1] *Grunnprinsipper for IKT-sikkerhet, versjon 1.1* https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/ (Besøkt Mai. 2019)

[2] *Trusselvurdering 2019* https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2019/ (Besøkt Mai. 2019)

te med svært lav struktureringsgrad og middels struktureringsgrad. Tabell 1 beskriver spørsmålsklassifiseringen. Vi benyttet oss også av scenario spørsmål. Det lages en fiktiv, men virkelighetsbasert situasjon som de ansatte kan komme opp i. Dette for å se hvilke valg de tar, noe som kan vise kunnskapen rundt temaet som er fremstilt i scenarioet [3].

Spørsmålsklassifisering	Beskrivelse
Svært lav struktureringsgrad	Denne formen for spørsmål består av et åpent hoved-spørsmål, men har i tillegg underspørsmål/undertema for eventuelt å hjelpe intervjuobjektet med å bedre forstå hovedspørsmålet, eventuelt også for å finne ut flere detaljer rundt hovedspørsmålet.
Middels struktureringsgrad	Spørsmålsformen innehar et åpent hovedspørsmål, og har i tillegg undertema som benyttes til tema-punkter som intervjuer skal berøre, hvis ikke intervjuobjektet har vært innom disse temaene i svaret hun/han har gitt på hovedspørsmålet.

Tabell 1: Beskrivelse spørsmålsklassifisering

Selve intervjuguiden baserer seg på de viktige punktene som det vises til i den kvalitative undersøkelsesmetoden. Tabell 2 viser intervjuguidens tema, rekkefølge og overordnet innhold i spørsmålene. Intervjuguiden ligger som vedlegg A i oppgaven.

Introduksjon - forklarer hvem vi er - hva som er formålet med intervjuet - hva vi ønsker å oppnå og hvordan intervjuet vil bli utført - hvordan resultatdokumentet blir håndtert
Generelt - generelle spørsmål om intervjuobjektets arbeidshverdag i forhold til informasjons-sikkerhet og interessen for dette temaet.
Sikkerhetskultur - spørsmål som retter seg mot oppfatningen av bedriftens sikkerhetskultur og intervjuobjektets delaktighet i den.
Nivå - spørsmål om ulike tema innenfor informasjonssikkerhet, i tillegg til variasjon i vanskelighetsgrad, for å belyse kunnskapsnivået.
Rutiner - spørsmål for å se på effekten av dagens rutiner og eventuelle problemer med dem.
Opplæring - spørsmål som gir svar på bedriftens opplæring sett fra intervjuobjektets side, og hvilke metoder de føler at de lærer mest/best av.
Spillutvikling - spørsmål for å finne ut hva som engasjerer intervjuobjektet, som videre kan benyttes i utviklingen av oppgavens brettspill.

Tabell 2: Intervjuguidens tema

[3] *How to Approach a Scenario Interview* https://workbloom.com/interview/interview-types-how-approach-scenario-interview.aspx (Besøkt Feb. 2019)

3.2 Kravspesifikasjon og utvikling av brettspillet

Med hjelp av informasjon samlet inn i første innsamlingsrunde utviklet vi ideen til spillet. Til å hjelpe oss med kravspesifikasjon og konstruksjon av spillet tok vi inspirasjon fra "Build your own board game"[4] med følgende prosess:

1. Utforming av grunnide.
2. Regler og dynamikk.
3. Brettets utforming.

Denne prosessen blir benyttet senere i kapittelet Utviklingsprosess 5.

Vi ønsker å presentere en fungerende prototype som er en god representasjon for et eventuelt sluttprodukt med gode læringsmuligheter for deltagerne. Spillet skal være modulbasert, slik at oppdragsgiverne senere kan legge til egne ideer og ha forskjellige vanskelighetsgrader.

3.3 Måling av brettspillets effekt

For å finne ut hvor bra brettspillet fungerte ønsket vi å gjøre målinger på personene som deltok i brettspillet. Vi ville finne ut hvor godt brettspillet vårt fungerte i motsetning til deres generelle oppfatning av brettspill. I tillegg ville vi undersøke hvordan brettspillet endret holdningene til deltagerne. For å kunne gjøre dette bestemte vi oss for å ha en selvevaluering. Dette kunne gi oss gode, lesbare resultater på hvor godt brettspillet fungerte og hvordan deltagernes holdninger har endret seg. Videre ønsket vi en måte å si noe om hvilke kunnskaper deltagerne fikk ut av spillet. Å spørre om kunnskap i selvevalueringen ville ikke produsert konkrete resultater og kunne være utsatt for subjektivitet. En kunnskapstest ville dekke dette behovet. Resultatet fra kunnskapstesten ville gi gruppen muligheter til å inkludere spesifikke spørsmål om hyppige tema i spillet og gi godt grunnlag for å si noe om utbytte i konkrete tema.

3.3.1 Pre- og posttest

Pre- og posttest er en måte å utføre praktiske eksperimenter på. I dette underkapittelet vil vi gå gjennom forskjellige typer pre- og posttester og metoden for hvordan vi skal gjennomføre dem. Disse metodene er tatt fra boken "Practical Research, Planning and Design"[5].

Grunnen til at vi valgte å gjennomføre en pre- og posttest er så vi kan forsøke å svare på problemstillingen vår; Hvor effektivt brettspill er i opplæring av informasjonssikkerhet. En pre- og posttest er også svaret til forskningsspørsmålet om hvordan vi kan teste effekten av brettspillet på de ansattes kunnskap. For å klare å svare godt på forskningsspørsmålene er det viktig å følge oppskriften på hvordan en pre- og posttest skal lages og gjennomføres, og for å sitte igjen med troverdige resultater.

Vi kommer til å gjennomføre to forskjellige pre- og posttester. En av testene er en selvevaluering, og den andre testen vil være en kunnskapstest. Hvordan hver av disse

[4] *Build your own board game* https://www.instructables.com/id/Build-your-Own-Board-Game/ (Besøkt 02.03.2019)

metodene blir utført vil bli beskrevet i dette underkapittelet.

3.3.2 Kontrollere de forstyrrende variablene

Boken snakker om å maksimere den interne validiteten når en forsker ønsker å identifisere årsak-og-effekt forhold. Det er seks punkter boken trekker frem når det kommer til å maksimere validiteten [5][s.198-202]. De punktene skrevet her holder vi korte for leserens skyld.

1. Ha det likt for alle

   Utfør testene helt likt. Har man flere grupper som skal testes er det viktig at alle har samme utgangspunkt.

2. Inkluder en kontrollgruppe

   Ha en kontrollgruppe som ikke påvirkes av eksperimentene. Dersom man skal teste effekten av noe, burde man ha en kontrollgruppe som forblir upåvirket. Dermed kan man måle effekten av testgruppen med kontrollgruppen og se forskjellen.

3. Tilfeldig sammensatte grupper

   Mennesker er forskjellige. Noen er mer motiverte enn andre, og andre har kanskje mer kunnskap innen forskjellige felt. Å kontrollere variabler som kunnskap og motivasjon så det er likt for alle, er bortimot umulig. For å løse dette kan forskeren sette sammen grupper helt tilfeldig. Når forskeren deler personer inn i vilkårlige grupper, kan forskeren stort sett si at gruppene er ganske like og at forskjeller mellom dem bare er tilfeldig. Spesielt statistisk analyse, der en forsker sammenligner to eller flere grupper, baserer seg på antagelsen om at gruppene er tilfeldig sammensatt og at forskjeller i tidligere behandlinger mellom gruppene er helt tilfeldig.

4. Ha en eller flere pretester for å få en oversikt over ekvivalens før eksperimentet

   Noen ganger er det ikke mulig å tilfeldig inndele grupper, for eksempel kan det være at forskeren må bruke grupper som allerede eksisterer. Et alternativ i denne situasjonen er å se på andre variabler som kan påvirke den avhengige variabelen og fastslå om gruppene er like i forhold til de variablene.

5. Utsett deltagerne for alle de eksperimentelle behandlingene

   Dersom man har flere eksperimenter som skal testes, kan det være smart å utsette gruppene for alle eksperimentene for å kontrollere forstyrrende variabler. (Behandling i vårt tilfelle er selve brettspillet)

6. Statistisk kontroll for forstyrrende variabler

   Det er delvis mulig å gjøre dette ved hjelp av statistikk, som ANCOVA (parital correlation, analysis of covariance) og SEM (structural equation modeling).

3.3.3 Valg av design for kunnskapstest

Det er mulig å gjennomføre pre- og posttest på mange forskjellige måter. Hver av metodene har sine gode og dårlige sider. Vi skal gå gjennom noen av de vi synes er mest relevante for oss og komme til et valg av metode. Disse metodene er beskrevet på side 202-205 [5].
Tx: Dette er eksperimentet, eller i vårt tilfelle spillet.
Obs: Dette er observasjon, som vil være kunnskapstesten i vårt tilfelle.
—: Dette betyr at ingenting skjer, i vårt tilfelle vil det være at de ikke deltar i pre- eller posttest og/eller spillet.

Design 1- Engangs eksperimentell case-studie

Dette designet har en lav intern validitet siden det er umulig å fastslå om deltakernes resultater i posttesten er grunnet eksperimentet. Dette designet er lett å gjennomføre, men resultatet er meningsløst.

Gruppe	Spill	Etter spill
Gruppe 1	Tx	Obs

Tabell 3: Design 1- Engangs eksperimentell case-studie

Design 2 - Én gruppe pretest-posttest design

Med denne metoden vet vi at det har skjedd en endring, men vi har ikke utelukket andre mulige forklaringer på hvorfor det det har skjedd en endring. Det kan ha noe med andre faktorer enn testen å gjøre.

Gruppe	Før spill	Spill	Etter spill
Gruppe 1	Obs	Tx	Obs

Tabell 4: Design 2 - Én gruppe pretest-posttest design

Design 3 - Statisk gruppesammenligning

Med denne metoden er det ikke mulig å si noe om hvordan tilstanden var før eksperimentet ble utført. Dette gjør det ikke mulig å vite om eksperimentet hadde noen observert endring mellom gruppene.

Gruppe	Spill	Etter spill
Gruppe 1	Tx	Obs
Gruppe 2	—	Obs

Tabell 5: Design 3 - Statisk gruppesammenligning

Det som er ulempen med disse metodene er at alle gjør det vanskelig å konkludere hva årsaken er til endringen. Dette er noe som er viktig å vite i forhold til forsknings-

spørsmål og problemstilling. De neste designene er bedre egnet for å kunne konkludere med årsak til endring.

Design 4 - Pretest-posttest kontrollgruppe design

Med denne metoden kan vi med rimelig grunnlag konkludere med at eksperimentet har noe med resultatet å gjøre. Et potensielt problem med denne metoden er; å evaluere deltakerne før eksperimentet kan, i seg selv, påvirke hvordan deltakerne svarer på eksperimentet. For eksempel kan pretesten påvirke deltakernes motivasjon. Dette kan føre til at de ønsker å dra mer nytte av eksperimentet enn det de ellers ville uten pretest. Dette designet forutsetter at gruppene er tilfeldig utvalgt.

Gruppe	Før spill	Spill	Etter spill
Gruppe 1	Obs	Tx	Obs
Gruppe 2	Obs	—	Obs

Tabell 6: Design 4 - Pretest-posttest kontrollgruppe design

Design 5 - Solomon fire-gruppe design

Denne metoden er svaret til problemstillingen for den forrige metoden, hvilken påvirkning har pretesten på eksperimentet? Å ta med to grupper som ikke blir pretestet gir en bestemt fordel. Dersom forskeren ser at gruppe 3 og 4 har mange like forskjeller som gruppe 1 og 2 har, kan forskeren lettere generalisere funnene sine til situasjoner der ingen pretest er gitt. Dette gjør at Solomon fire-gruppe design øker den eksterne validiteten av eksperimentet.

Gruppe	Før spill	Spill	Etter spill
Gruppe 1	Obs	Tx	Obs
Gruppe 2	Obs	—	Obs
Gruppe 3	—	Tx	Obs
Gruppe 4	—	—	Obs

Tabell 7: Design 5 - Solomon fire-gruppe design

Valg av design

Dette er da noen av designene som vi kan velge å bruke. Siden spilltesten hos oppdragsgiverne skal bestå av 4 grupper er det ganske naturlig å velge design 5 [tabell 7]. Siden oppdragsgiverne ønsker å teste spillet på alle, må vi gjøre noen endringer til Solomon sin metode. Med litt veiledning fra veilederne har vi kommet opp med et alternativ til Solomon fire-gruppe design. Vi vil derfor ha en metode hvor en gruppe gjennomfører pretesten og spillet, og en annen gruppe gjennomfører spillet og posttesten. Dette gjør at den/de gruppene som gjennomfører pretesten vil ha samme funksjon som en kontrollgruppe. Vi kan da sammenligne resultatet fra kontrollgruppen med gruppen som

gjennomfører posttesten. Designet vil se slik ut:

Gruppe	Før spill	Spill	Etter spill
Gruppe 1	Obs	Tx	—
Gruppe 2	Obs	Tx	—
Gruppe 3	—	Tx	Obs
Gruppe 4	—	Tx	Obs

Tabell 8: Design 6 - Vårt design

Grunnen til at vi ikke har en gruppe som utfører både pre- og posttest er grunnet problemet med design 4 [tabell 6], at pretesten i seg selv kan ha en påvirkning på resultatet.

3.3.4 Valg av design for selvevaluering

Vi har bestemt at alle deltagerne skal utføre selvevalueringen både før og etter spillet. Vi nevnte tidligere problemet med design 4 - Pretest-posttest kontrollgruppe design [tabell 6], at pretesten har en påvirkning på selve eksperimentet. Grunnen til at vi gjør en pretest og posttest på alle er at denne selvevalueringen ikke har noe med utfallet på spillet eller kunnskapstesten å gjøre. Ved å ha en slik selvevaluering kan vi se utviklingen i hvordan deltagerne ser på sin egen kunnskap om informasjonssikkerhet. Det er ikke et fasitsvar de kan gi oss her, men vi vil gjøre oss noen tanker rundt hvilken vei utviklingen går.

Et eksempel på et selvevaluerings spørsmål: “Brettspill fungerer godt til opplæring i informasjonssikkerhet.” Her vil deltagerne få muligheten til å velge i hvilken grad de er enig/uenig ved hjelp av Likert skala. Dersom utviklingen går fra uenig til enig kan det gi en antydning at spillet har fungert godt til opplæring. Går utviklingen fra enig til uenig kan det motsatte antydes. Siden alle skal ta denne testen før og etter er det veldig viktig at alle deltagerne får et unikt nummer. Det unike nummeret blir trukket når vi deler inn i grupper. Dette hjelper oss også med å ha tilfeldig sammensatte grupper [3.3.2 punkt 3] der de som trakk partall er en gruppe, og de som trakk oddetall er en annen gruppe.

Eksempelspørsmålet er et av forskningsspørsmålene våre. Selvevalueringen vil da fungere som en ekstra metode til å svare på forskningsspørsmålet. Siden vi bruker to metoder for dette kan man med større sikkerhet si om brettspillet fungerer/ikke fungerer til opplæring. Dette er viktig informasjon for oss i forhold til hvor godt vi kan gi en konklusjon til problemstillingen vår.

Selvevalueringen før spillet kommer til å bli besvart før kunnskapstesten. Dette gjøres siden kunnskapstesten kan ha en påvirkning på hva deltagerne svarer på selvevalueringen. Når de som gjennomfører kunnskapstesten før spillet gjør selvevalueringen etter spillet kan de reflektere over hva de hadde svart annerledes på dersom de hadde fått den på nytt. Dette er noe vi kan få en indikasjon på når vi analyserer resultatene.

Selvevalueringen etter spillet kommer også til å bli besvart før kunnskapstesten for de som skal gjennomføre den etter spillet. Dette er igjen fordi kunnskapstesten kan ha en

påvirkning på hva deltagerne svarer på selvevalueringen. Når vi analyserer resultatene fra kunnskapstesten kan vi da se om det stemmer i forhold til de resultatene vi får av selvevalueringen.

3.3.5 Innholdet i pre- og posttest

Selvevaluering

Boken [5] snakker om hvordan man skal lage en spørreundersøkelse. Siden pre- og posttesten er en spørreundersøkelse er det naturlig å følge formelen for hvordan spørreundersøkelsen skal lages. Boken [5][side 166-170] går gjennom 12 punkter for hvordan man lager og analyserer en spørreundersøkelse. Vi tar bare med de punktene som er mest relevante her. Alle punktene ligger i bibliografi D med en beskrivelse.

- Hold det kort

  Spørsmålene burde være så korte som mulig og bare formidle informasjon som er viktig i forhold til hva som skal undersøkes. Dette gjøres ved å stille seg 2 spørsmål: "Hva planlegger jeg å gjøre med informasjonen jeg spør om?" og "Er det absolutt nødvendig å ha denne informasjonen til å løse en del av forskningsspørsmålene?"

- Gi enkle, spesifikke instruksjoner

  Formidle akkurat hvordan du vil respondenten skal svare. Ikke tro at de er kjent med Likert skala. For eksempel, "kryss av for hvor enig du er i følgende påstand:..."

- Bruk enkelt, klart og entydig språk

  Skriv spørsmål som kommuniserer akkurat hva du vil vite. Unngå å bruke terminologi som respondenten ikke forstår. Unngå ord som "vanligvis" og "flere"

- Ordlegg spørsmålene på en måte som ikke gir føringer til det rette eller foretrukne svaret

  Ta dette spørsmålet som eksempel: "Hvilke strategier har du bruk for å slutte å røyke?" Dette impliserer at den som svarer har prøvd å slutte. Dette kan lede til at personen svarer på noe hen aldri har prøvd.

- Fastslå hvordan svarene skal tolkes før undersøkelsen blir sendt ut

  Ha en plan for hvordan svarene kan gjøres om til tallverdier så det er mulig å gjøre statistisk analyse.

- Ha en pilot-test for å fastslå validiteten til spørsmålene

  Det er viktig å se om spørsmålene er klare og de klarer å formidle den ønskede informasjonen. De som utfører pilot-testen burde i hvert fall svare på spørsmålene. En bedre måte å gjøre dette på er å stille spørsmål til respondenten gjennom

utføringen av undersøkelsen. Spørsmål som: “Les spørsmålet høyt”, “Hvilken informasjon vil dette spørsmålet ha fra deg?”, “Hvilket svar er mest riktig for deg på dette spørsmålet?”, “Kan du forklare hvorfor du valgte det svaret?”. Gjennom å stille slike spørsmål er det lett å se hvilken type svar man kan få. Dersom undersøkelsen inkluderer begge kjønn og forskjellig religiøs/kulturell bakgrunn, burde pilot-testen inneholde respondenter fra forskjellig kjønn og sosiale lag.

- Granske det nesten ferdige produktet en gang til og vær sikker på at det tilfredsstiller behovene våre
  For å gjøre dette anbefaler boken [5] å bruke følgende mal:

Skriv spørsmålet under	**Hvorfor stiller vi dette spørsmålet? Hvilken sammenheng har det til forskningsspørsmålene?**
Spørsmål...	Hvorfor... Sammenheng til forskningsspørsmål...

Tabell 9: Mal for kvalitetssikring av spørsmål

- Utforme spørreundersøkelsen så den ser attraktiv og profesjonell ut

  Undersøkelsen burde være bra printet, ikke ha noen skrivefeil, og kanskje to eller flere farger. Det burde understrekes at vi som gjennomfører undersøkelsen er profesjonelle og at vi setter stor pris på at respondentene deltar.

Kunnskapstest

Her må vi lage spørsmål til testen som er forskjellig fra de spørsmålene som blir stilt i spillet, men samtidig spørsmål de skal klare å svare på ved å spille spillet. Da vi lagde spørsmålene var vi ikke begrenset til å bare ha flervalgsoppgaver. I kunnskapstesten kunne vi ha eksempler på Phishing der vi testet evnen deres til å skille en legitim side fra en ondsinnet. Grunnen til at vi ikke kunne bruke spørsmål fra spillet er fordi da vil resultatet mest sannsynlig reflektere hvor mange av spørsmålene fra pre- og posttesten som ble stilt i spillet. Dette ville da gjøre at et eventuelt resultat får veldig stor vilkårlighet.

Når det er sagt er det fortsatt mulig at resultatet fra kunnskapstesten reflekterer hvilke spørsmål som ble stilt under spillet. Spillet er ikke designet for å gå gjennom alle spørsmålene vi har laget. Dette vil ta for lang tid å gjennomføre. Vi kan heller ikke velge ut 40 spørsmål som alle skal spille med, og som dekker alle temaene i kunnskapstesten. Dette vil føre til at vi i stor grad påvirker utfallet av kunnskapstesten som gjør at resultatet vårt ikke blir troverdig. For oppdragsgiverne så vil det være aktuelt å gjøre dette siden de vil styre hva de ansatte skal lære. Siden vi skal se på den helhetlige effekten av spillet er dette ikke aktuelt.

3.3.6 Kvalitativ eller kvantitativ metode etter posttesten

Vi ønsker en tilbakemelding utenom statistikken fra pre- og posttesten som gir oss informasjon om hva de synes om brettspillet. Gruppen hadde en diskusjon på hvilken metode vi burde bruke, hva som er positivt og negativt med de forskjellige metodene. Det er

viktig å presisere at vår hovedoppgave er å måle effekten av brettspill, som gjøres ved å bruke pre- og posttesten, men tilbakemeldingene gir informasjon og detaljer på hva som gikk bra og dårlig i spillet.

Kvantitativ metode innebærer å få svar fra alle som deltok i spillet, der de krysser av på svaralternativer. Bruk av svaralternativer gjør det mulig å gjennomføre en statistisk analyse av svarene på en praktisk, visuell og enkel måte. De spørsmålene som gir deltagerne mulighet til å komme med utdypende meninger gir oss en indikasjon på hvordan opplevelsen av spillet var. Når det dreier seg om evaluering av spillet og eget utbytte blir det naturlig å bruke en Likert skala.

En annen måte er å plukke ut en person fra hver spillgruppe og intervjue personen. Da kan vi få detaljer på hvordan det fungerte for deltageren og hvordan hen følte gruppen opplevde spillet. Vi ønsker å ha samme prosess for alle objektene og ser et problem i at svarene fra de få vi velger ut kan være veldig forskjellige fra den generelle oppfatningen til resten av deltagerne. Sammenligning av svar er vanskeligere med kvalitative datapunkter. Det er begrenset med tid å utføre spillet, pre- og posttest og samtidig ha tid til intervjuet også.

Det vi har kommet fram til i gruppen og gjennom samtaler med veiledere, er å ha et åpent spørsmål på slutten av selvevalueringen. Der kan deltagerne fritt gi tilbakemeldinger på hvordan de syntes spillet har vært, og eventuelt ting som kan bli bedre.

3.4 Statistikk

Gjennom pre- og posttestene ønsker vi å finne ut i hvilken grad spillerne har blitt påvirket i forhold til problemstillingen og forskningsspørsmålene våre. Her vil vi benytte statistikk for å vise trendene mellom pre- og posttestene samt forskjeller mellom gruppene som hadde kunnskapstesten før, og de som hadde kunnskapstesten etter spillets gjennomførelse. Disse statistikkene vil gi oss mulighet til å analysere resultatet og komme fram til en konklusjon om hvilken grad spillet har påvirket/oppnådd problemstillingen og forskningsspørsmålene. For å lære om forskjellige metoder og begreper innen statistikk ble boken “Statistics For Dummies 2nd Edition”[6] brukt.

3.4.1 Verktøy

Selvevalueringene benytter en Likert skala, og i kunnskapstesten vil det bli benyttet poengsum mellom 0 og 12.
Med en Likert skala, som er en ordinal skala, er det ukjent hvilken distanse som ligger mellom de forskjellige kategoriene[5], derfor vil det ikke være relevant å finne gjennomsnitt og deviasjon i svarene, men vi vil bruke median og modus samt fremstille resultatet i et histogram med frekvensene fra evalueringene før og etter. Det vi hovedsakelig leter etter i sammenligningen mellom selvevalueringene er trenden til deltakerne.

Resultatene fra kunnskapstesten vil være kvantitative variabler. Vi kommer til å analysere disse resultatene med gjennomsnitt og median. Resultatene vil bli plottet i et spred-

[5] *Ordinal data* https://en.wikipedia.org/wiki/Ordinal_data (Besøkt 02.05.2019)

ningsplott for å kunne se trender samt hvor ekstreme resultater ligger. Vi vil også se på skjevheten i dataene ved å plotte resultatene i et histogram.

Vi tenkte opprinnelig å bruke SPSS til statistikk, men etter å ha innsett at vi ikke har bruk for mer avanserte statistiske formler og metoder valgte vi å heller bruke en form for excel. Excel er mer allment kjent og derfor har gruppemedlemmene allerede god kjennskap til mulighetene og hvordan programmet fungerer. I tillegg er det gode skybaserte løsninger som gjør at flere medlemmer kan jobbe med statistikken samtidig og få tilgang til den fra andre enheter. Med tanke på alt dette valgte gruppen å benytte Google Sheets, dette er i tillegg der resten av materialet til bachelor oppgaven er lagret, som vil gjøre det enklere å finne frem.

3.4.2 Ønsket oppnåelse

Med resultatene vi har samlet inn og bearbeidet vil vi lete etter endringer mellom hvert objekt sin selvevaluering før og etter samt endringer mellom gruppene som tok kunnskapstesten før og etter. For kunnskapstesten vil ikke bare den totale poengsummen til hvert individ være relevant, men også gruppenes samlede poengsum på hvert spørsmål. Med tanke på selvevalueringen vil det være variert om et positivt resultat er en forskyvning mot veldig enig eller veldig uenig. For eksempel med påstanden “Brettspill fungerer godt til opplæring i informasjonssikkerhet” er en endring mot “veldig enig” gunstig, men for påstanden “Sikkerheten på arbeidsplassen er sikkerhetsavdelingen sitt ansvar.” er en endring mot “veldig uenig” gunstig.
Et godt grunnlag for analyse og drøfting videre vil være tydelige endringer mellom før og etter testene, men det vil også være mulig å si noe om tilfeller hvor det ikke er noen endring.

4 Resultat fra intervju

4.1 Oppsett og gjennomførelse

I løpet av de to intervjurundene ble det intervjuet 4 ansatte hos Norsk Tipping, og 4 ansatte hos Skatteetaten, i tillegg ble det mulig å ta 2 ekstra intervjuer hos Skatteetaten, 10 intervjuobjekter totalt. Prosjektgruppen delte seg i to grupper, og tok 5 intervjuer hver, derfor vil formuleringer av spørsmål og oppfølgingsspørsmål variere. Dette betyr at ikke alle intervjuobjektene ble stilt akkurat de samme spørsmålene, men dette er ikke et problem ettersom formålet til intervjuene var inspirasjon til brettspillet og å finne behovet for opplæring. I tillegg, grunnet valg av kvalitativ metode, vil mange svar variere, og det vil være få like konkrete svar. Gruppen vil derfor tyde svarene og trekke konklusjoner deretter. Under intervjuene sa gruppen fra angående taushetsplikt og at intervjuet var anonymt, slik det ikke skulle være et hinder ved å dele informasjon.

Nedenfor vil resultatene bli gjennomgått og hvordan det påvirket vår prosess. Intervjuguiden som ble brukt i intervjuene ligger som vedlegg A til oppgaven. De konkrete svarene fra de forskjellige intervjuobjektene vil ikke bli lagt ved grunnet sensitive opplysninger om oppdragsgivernes virksomheter, men generelle ikke sensitive tendenser vil bli trukket fram under.

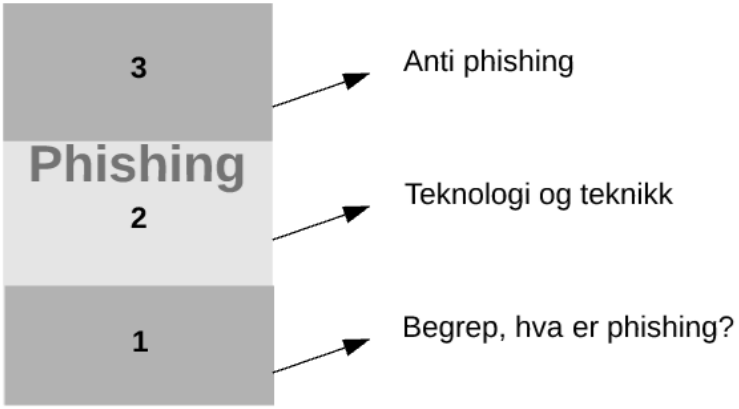
4.1.1 Generelle sikkerhetstendenser

Mellom de to virksomhetene var det noen få merkbare forskjeller, men stort sett var det generelle tendenser som gikk igjen. Først og fremst sikkerhetskultur, jevnt over var det lite prat om sikkerhet mellom ansatte, hovedsakelig grunnet ingen insentiv til å prate om det. På tross av dette mente alle intervjuobjektene at de fint kunne delt erfaringer rundt det å bli phishet, med noe varierende omfang, noen mente de kunne dele med alle, andre mente de kunne dele kun med nære venner. Kommunikasjon mellom ansatte og ledelse var varierende, stort sett forekommer dette ovenfra og ned i hierarkiet. Ansatte i begge virksomheter hadde inntrykk av at sikkerhetsavdelingene hadde stort fokus på sikkerhet, men i noen tilfeller ble det uttrykt at de mente det var sikkerhetsavdelingene som hadde fullstendig ansvar for sikkerhet.

Intervjuobjektene hadde god kjennskap til Phishing, men ellers liten teknisk kunnskap rundt sårbarheter. Det som ble trukket frem mest var ulike former for Sosial manipulering og det å få kjennskap til passord. Gruppen fikk inntrykk av at de ansatte ikke forstår hensikten bak policyer, som for eksempel hvorfor et passord skal være 15 tegn, men når objektene ble spurt om det er noen policyer de ikke forstår hensikten med hadde de lite å peke til.

Gjennom intervjuene fikk gruppen samlet opp informasjon angående hvor de manglet kunnskap, hva de kunne og hva vi burde inkludere med i spillet med tanke på opplæring. Figur 6 viser hvordan gruppen deler inn et begrep, for eksempel Phishing. Første punkt

er begrep, det å vite hva phishing er. Andre punktet (Teknologi og teknikk) handler mer om teknikker innen phishing, for eksempel Spear phishing, hvordan blir de utført og hva teknologien bak det er? Punkt nummer tre (Anti phishing) handler om hvordan man beskytter seg mot phishing, eksempelvis ikke trykke på linker inkludert i epost eller det med å holde musepekeren over linken for å sjekke hvor den er linket til.



Figur 6: Oversikt over begreper

Mange av objektene har mye kunnskap om hvordan man beskytter seg mot phishing, gjennom å holde musen over linken eller å ikke trykke på linken i det hele tatt. Vi anser det som relevant for de ansatte å ha kjennskap til begreper innen informasjonssikkerhet. Det samme gjelder begreper som VPN og 2FA. Objektene bruker 2FA til vanlig (mobil-bank) og VPN når de arbeider, men de vet ikke hva begrepet er.

De ansatte var ikke helt fornøyde med E-læring. De mente det var for enkelt å hoppe gjennom videoene som blir sendt, eller ikke følge med. Dersom videoene ble etterfulgt av en test var det som regel bare å prøve seg frem flere ganger til man fikk det til, og så blir det glemt.

4.1.2 Relevant for brettspillet

5 av 10 intervjuobjekter antydet at de foretrakk individuell læring når de skulle lære noe nytt. Mange trakk frem at gruppearbeid var bedre innen opplæring når det gjaldt noe vanskelig eller om noe er veldig teknisk. De trakk også frem at de ønsket mer engasjerende opplæring og bedre opplæring i de praktiske og grunnleggende ferdighetene. Diskusjoner mellom ledelsen og arbeiderne var en god måte å forstå sikkerhet på, samt bruke praktiske og visuelle hjelpemiddel for å skape engasjement og interesse. Når objektene ble spurt om de foretrakk visuell, praktisk, eller teoretisk nevnte 7 av 10 at å gjøre ting praktisk er en god metode å lære på. Gruppen ser på dette som en mulighet til å introdusere læring gjennom workshop arbeid, dette støttes av utsagn fra 6 objekter om at de kunne ønske opplæring i møter med andre ansatte og ledere.

Intervjuobjektene ble spurt konkrete spørsmål i forhold til brettspill. Det kom fram at

det var varierende interesse for brettspill, én gang i året nederst i skalaen, til annenhver uke øverst. Alle objektene nevnte konkurranse som viktig for et brettspill og mange av objektene ville spille brettspill på grunn av det sosiale. Angående kompleksitet var det veldig varierende. Noen foretrekker enkle spill som krever liten tid å sette seg inn i, andre mente det ville bli kjedelig om spillet var for lett.

4.2 Konklusjon

Et spill med god læringseffekt er den største prioriteringen, men basert på objektenes utsagn om konkurranse og det å lære selv er det viktig å legge fokus på konkurranse delen av brettspillet. Det betyr at det vil være viktig for gruppen å finne en balanse som gjør at spillet er engasjerende og lærerikt. De ansatte hadde noe grunnleggende kunnskap om tema innen informasjonssikkerhet, men dette varierte veldig. Spillet må ha elementer som gjør det litt komplisert for å holde interessen til de som spiller. Det er også viktig å passe på at det ikke tar for lang tid å sette seg inn i regler og hvordan spillet fungerer. Angående sikkerhetskultur vil det være positivt for den generelle arbeidsplassen å gi insentiv til prat om sikkerhet i en eller annen form.

4.3 Tilbakemelding

I tillegg til prosjektoppgaven ga vi tilbakemelding til oppdragsgiverne om funnene våre fra intervjuene. Funnene varierte i grad av sensitivitet og vil derfor ikke bli diskutert her. Funnene ble først diskutert blant gruppen og det ble også diskutert mulige tiltak for å forbedre avvik/tendenser. Dette ble presentert for oppdragsgiverne først gjennom møte, og deretter ble det laget et dokument med funn og foreslåtte tiltak som ble sendt kryptert til en av oppdragsgiverne.

5 Utviklingsprosess

I dette kapittelet beskriver vi utviklingsprosessen av brettspillet. Vi kommer til å gå inn på valgene vi har gjort og forskjellige utkast av spillbrett, kort og regler. Når dette kapittelet er over vil spillet være ferdig utviklet og klar for testing hos oppdragsgivere.

5.1 Utforming av spillet

5.1.1 Utforming av grunnide

Grunnideen til spillet er at spillerne vil besvare spørsmål som gir spillerne poeng ved riktig svar. Etter diskusjon med oppdragsgiver har det blitt presentert et ønske om å inkludere en rolle "Gamemaster" som kan delta i spillet som en slags administrator. Vi har lagt opp til at det skal være mulig å spille både med og uten denne administratoren. Dersom administratoren er med vil denne personen lese opp spørsmål og svaralternativ, samt presentere forklaring på riktige svar etter at et lag har besvart spørsmålet. Dersom det ikke er en administrator til stede vil lagene etter tur utføre det som ville vært administratoren sin oppgave. Læringsutbyttet fra spillet vil variere etter administrator sine kunnskaper og engasjement, derfor legger vi opp til at spillet og testen skal gjennomføres med minst mulig avhengighet til en administrator. Dette betyr at vi ikke kommer til å involvere egne kunnskaper annet enn det vi har forberedt til spillet på forhånd, slik at vi ikke påvirker resultatet av testen. Etter endt prosjekt vil en administrator kunne påvirke spillet positivt på eget initiativ, men spillet skal fungere uten.

Under ideutviklingen av spillet fastsatte vi noen aspekter som ville øke spillets engasjerende effekt og læringseffekt. Disse ble inspirert av informasjon fra intervjuobjektene samt gruppens erfaringer rundt brettspill. Forskjellige funksjoner i spillet ble implementert med en eller flere av disse aspektene i tankene og vil gi oss et grunnlag for å diskutere virkemidlene som fungerte godt og dårlig.

- **Konkurranse:** Dette er noe alle intervjuobjektene nevnte som engasjerende i brettspill. Det spiller på spillernes konkurranseinstinkt og motiverer spillerne til å lære, i tillegg gir det opplæringen et konkret mål.
- **Diskusjon:** 5 av 10 intervjuobjekter nevnte spesifikt at det sosiale var noe som gjorde at de ville spille brettspill. Gruppen tenkte at med diskusjon vil det bli fremmet både læring, og en lettere atmosfære rundt spillet som trolig kan distrahere spillerne bort fra at det er opplæring.
- **Kompleksitet:** Det varierte mellom intervjuobjekter hvor mye tid de var villige til å sette av til brettspill, for noen var det flere timer og andre mindre enn én time. Når det dreier seg om opplæring er det viktige å holde spillet lett å forstå slik at en opplæringsøkt kan bli startet fort og det skal være liten innsats fra deltagerne å starte. På tross av dette mente vi det fortsatt var viktig å komplisere spillet på noen måter, slik at det ikke ble ren tilfeldighet hvem som vant til slutt.
- **Strategi:** 6 av 10 svarte de likte å strategisere i spill, dette kan oppsummeres i valg

spilleren kan gjøre som vil ha noe å si for deres prestasjon i spillet.

Etter å ha fastslått disse aspektene begynte vi med diskusjon av spillernes inndeling. Relevante momenter er læringseffekt og engasjement i forhold til konkurranse. Diskusjon har stor verdi fordi om spillerne reflekterer rundt svarene i spillet vil det oppfordre til bedre sikkerhetskultur og deling av kunnskaper. Engasjement er også viktig, spillerne må ha lyst til å spille spillet for å kunne lære. Vi endte opp med laginndelinger med 2 spillere på hvert lag, og 4 lag. Med dette har spillerne i de forskjellige lagene mulighet til å diskutere seg imellom og det vil være konkurranse mellom de forskjellige lagene. Lagenes størrelse gjør det lett å føle seg inkludert i diskusjonen og enklere å rivalisere mellom forskjellige lag. I tillegg vil lagstørrelsene også være fleksibel. Dersom man har en person for mye eller for lite vil det ikke være vanskelig å enten redusere antall lag, eller øke antall spillere på et lag. Vi vil derimot anbefale at ingen lag overstiger 3 deltakere fordi det da blir vanskeligere å delta aktivt i spillet. Med det sagt så er det mulig å spille spillet individuelt om man ikke er nok personer til å forme lag.

5.1.2 Regler og dynamikk

Spillet vil bli spilt med én terning og et brett som ikke har noe med målet til spillet i seg selv å gjøre, men vil gi forskjellige type spørsmål og spill-endringer til spillerne, det er disse spørsmålene som legger grunnlaget for aspektet diskusjon. Det er antall poeng som avgjør hvem som vinner og disse blir talt utenom dette brettet.
Brettet deles inn i 4 soner som har relevans overfor deres arbeidsplass. De 4 sonene vi har tatt utgangspunkt i er Resepsjon, Arbeidsplassen, Sikkerhetskultur og Godt & Blandet. Lagene vil få spørsmål ettersom hvilken sone de er i, og spørsmålene vil være relevante for disse sonene.
Grunnideen i seg selv var ensformig, og for å gjøre spillet mer engasjerende startet vi på regler og dynamikk i spillet som ville tilby forandring mellom spillerundene.

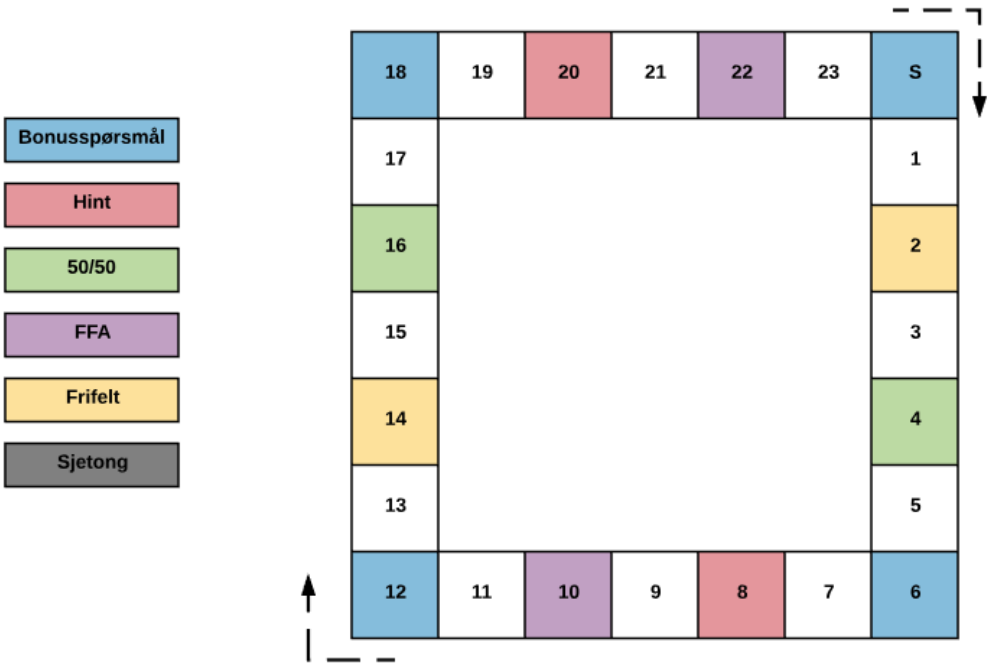
- **Stjele sjetong:** To felter introduseres hvor man får en stjele sjetong for hver gang man passerer et av feltene, men hvert lag kan kun ha én sjetong til enhver tid. Stjelesjetongen kan brukes til å stjele et spørsmål fra et annet lag, så sant andre regler ikke er i spill og svaralternativene ikke enda har blitt lest opp. Dette vil gjøre at spillerne er interessert i de andre lagenes spørsmål også, og ikke bare sine egne. Stjelesjetongen spiller på aspektene konkurranse, kompleksitet og spesielt strategi. En god spiller kan, for eksempel, velge å bruke sin stjelesjetong på bonusspørsmål og få et forsprang over de andre spillerne på den måten. En mindre god spiller kan velge å bruke sin sjetong på å stoppe en bedre spiller fra å få poeng.
- **Frifelt:** Flere felt vil være frifelt, når et lag står på disse feltene vil det ikke være mulig for andre lag å stjele spørsmålet som de får. Frifeltet legger til kompleksitet og gir spillere som har mistet mange spørsmål mulighet til å komme tilbake i spillet.
- **50/50:** Lander et lag her vil de få et spørsmål og dersom ingen andre lag stjeler spørsmålet vil to av de gale svaralternativene ikke bli lest opp. Stjeler et annet lag dette spørsmålet vil de få alle de 4 svaralternativene.
- **Alle mot Alle:** Når et lag lander her vil spørsmålet bli lest opp og alle lag vil ha mulighet til å svare på spørsmålet. Det første laget som prøver å svare får spørsmålet og vil eventuelt kunne få poeng. Dette feltet passer inn med aspektene konkurranse

og kompleksitet.

- **Bonusspørsmål:** Alle hjørnene i spillebrettet vil være bonusspørsmål. Dette feltet gjelder som et frifelt og vil gi laget et vanlig spørsmål, etterfulgt av et vanskeligere oppfølgingsspørsmål. Laget kan velge om de vil ta oppfølgingsspørsmålet eller ikke. Dersom de svarer riktig på oppfølgingsspørsmålet vil de få bonuspoeng, svarer de feil vil de få trekk. Bonusspørsmålene var lagt opp til å være vanskeligere og ville derfor forhåpentligvis skape diskusjon i tillegg til å legge til kompleksitet til spillet.
- **Hint:** Det vil være en bunke med hint kort, og om et lag lander på et hint felt vil de kunne trekke et hint kort, memorere det, og legge det tilbake nederst i hint bunken. Dersom et spørsmål kommer opp senere og hintet var relevant vil de kunne stjele dette spørsmålet og forhåpentligvis svare riktig.

5.1.3 Brettets utforming

For å opprette reglene i spillet trengte vi først et oppsett på feltene. Dermed ble brettet utviklet til å ligne et monopolbrett [figur 7], bestående av 24 felter formet som et kvadrat med 7 felter langs hver side, og hvor midten av brettet er tomt. Feltene mellom hjørnefeltene (altså de 5 i midten) vil være sone feltene og det vil være andre spesialfelt inne i disse sonene i tillegg. Bonusspørsmål feltene er ikke inkludert i noen av sonene da disse blir plukket fra en egen bunke. Det vil være umulig for en spiller å fullstendig passere en side uten å lande på bonusspørsmål eller en av sone feltene minst én gang. Stjelesjetong feltene ligger på to av hjørnene, hvert 12. felt. Med forbehold om at kast med én terning har gjennomsnitts utfall 3.5 vil det ta rundt 4 kast å komme seg til neste stjelesjetong. Med flaks kan de få til dette på minimum 2 kast. Dette gjør at spillerne vil ha tid til å bruke stjelesjetongene sine, men også at de føler presset til å måtte bruke den ene de kan ha før de har mulighet til å få en ny.



Figur 7: Original ide

5.1.4 Tidsbruk

Brettspill varierer stort i tiden det tar å fullføre dem. Mange mer ambisiøse brettspill tar flere timer å gjennomføre, og noen krever flere dager. Når det dreier seg om opplæring er tidsbruk viktig. Er gjennomføringen for kort får spillerne mindre utbytte, tar det for lang tid derimot vil det bli vanskelig å fokusere på spillet og vanskeligere å huske det man får ut av spillet. Vi vil sikte på å la spillerne spille i 40 minutter da dette gir dem tid til å komme gjennom en god mengde spørsmål, men også at spillet ikke tar så lang tid at interessen avtar. Med forbehold om at hvert spørsmål tar 1 minutt å svare på og det blir brukt minst mulig tid til alt annet vil det totalt bli lest opp 40 spørsmål og hver spillgruppe vil trekke 10 spørsmål hver. For å opprettholde dette på best mulig måte vil spillet være tidsbasert og når gjennomføringen passerer 40 minutter vil det bli annonsert for spillerne slik at de har muligheten til å bruke sine resterende sjetonger og tjene sine siste poeng.

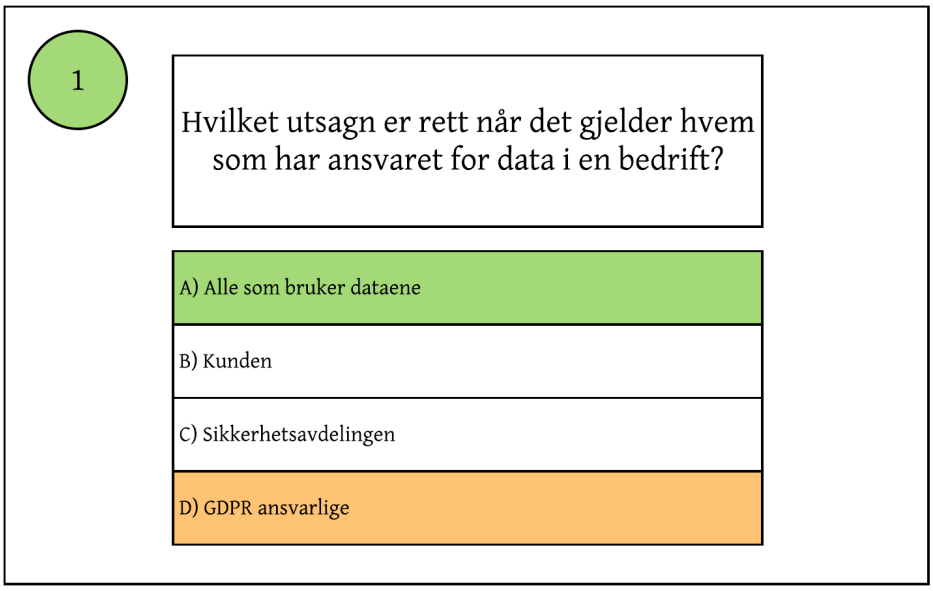
5.1.5 Spørsmålene

Spørsmålene er konstruert mot resultatene [4.2] fra intervjuene, trusler presentert i PST sin trusselvurdering[1] og hendelser som er relevant til organisasjonene Skatteetaten og Norsk Tipping. Gruppen lagde også generelle spørsmål individuelt og deretter delte dem inn i de passende sonene til brettspillet. Spørsmålene varierer over et vidt spekter innen informasjonssikkerhet. Det lå en utfordring i å holde spørsmål og svaralternativer korte og konsise, som er viktig for å redusere størrelsen på spillekortene og for å gjøre det enkelt å forstå. Når spørsmålene ble delt inn i soner var det mulig å se hvor det var behov

[1] *Trusselvurdering* https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2019.pdf (Besøkt 01.04.2019)

for flere spørsmål og eventuelt om noen spørsmål kunne flyttes til en annen sone. Det var viktig å ha noen gode svaralternativer til hvert spørsmål. Om et spørsmål har dårlige svaralternativer vil spillerne føle mindre behov for å diskutere seg fram til svaret. Humor i alternativer er noe som er inkludert, dette fremmer engasjement og er et kreativt virkemiddel innen læring[2].

Å bruke humor er en vanskelig prosess der man må være forsiktig med antall alternativer som inneholder humor, og samtidig har læringsutbytte. I noen tilfeller var det flere riktige svar, det ble løst ved å kutte ut det mindre viktige svaret, eller jobbe dem sammen i ett. Å ha flere riktige svaralternativer på et spørsmål ville komplisert utførelsen av spillet med tanke på fasit og spesialfelt som for eksempel 50/50. Figur 8 viser hvordan et spillkort ser ut. Det alternativet som er grønt er det riktige svaret. Et problem vi måtte ta stilling til er hva man må gjøre dersom spilleren lander på 50/50 felt. Da må den som stiller spørsmålet vite hvilke svaralternativer som skal være med. For å holde spillet konsistent har vi valgt å fargelegge det andre svaralternativet med oransje. Da bestemmer vi hvilket alternativ som skal bli valgt til enhver tid. Det er ikke nødvendig å ha et ekstra svaralternativ på bonusspørsmålene siden det er umulig å få et bonusspørsmål og lande på et 50/50 felt samtidig.

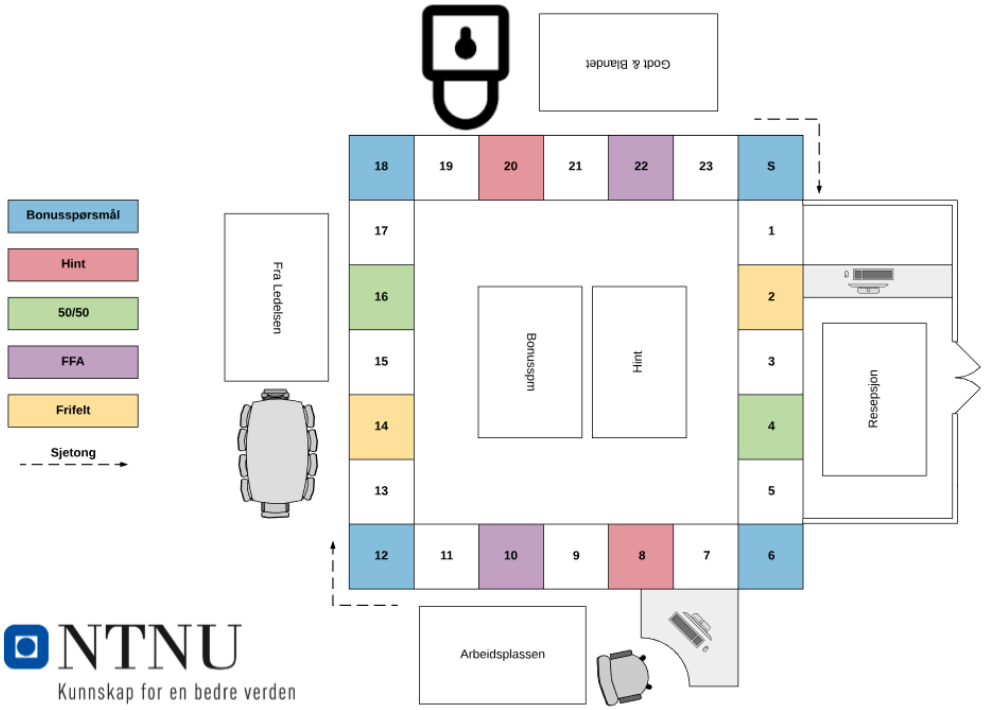


Figur 8: Eksempel vanlig spørsmål

[2] *Humor i skolen på ramme alvor* https://www.duo.uio.no/handle/10852/30808 (Besøkt 23.04.2019)

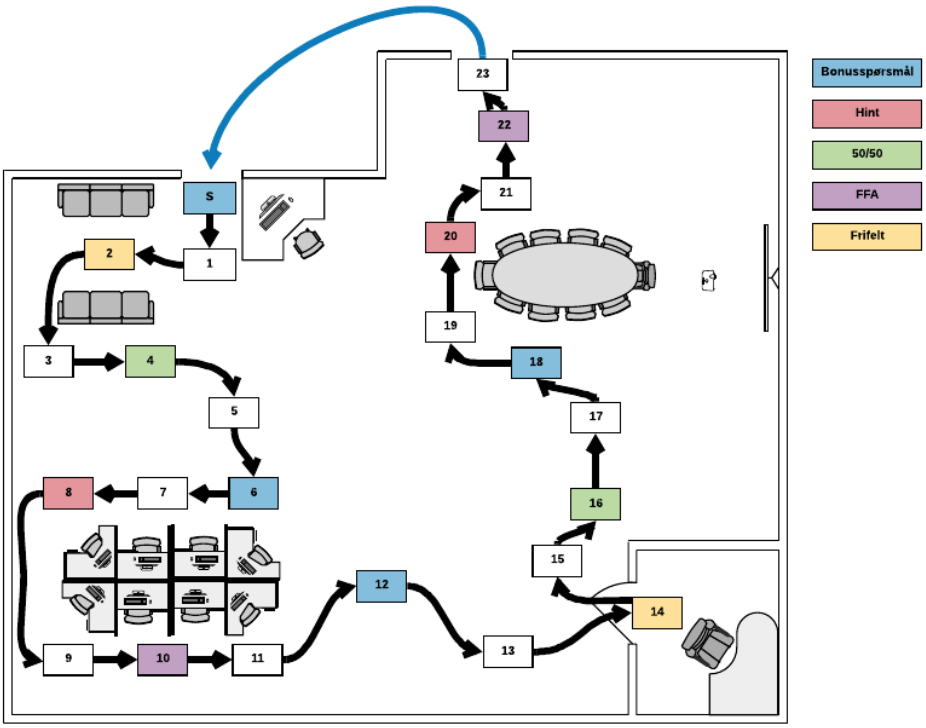
5.2 Design

Når det gjelder utformingen av brettspillet er det to forskjellige tankeganger som utpeker seg. Å lage noe som er lett gjenkjennelig og har en klar struktur, eller noe nytt og spennende med mer dynamisk struktur. Det ble laget et forslag til hvert av de to forskjellige tankegangene. Figur 9 er det brettet som er utviklet med klar struktur i tankene, samt at det skal være lett gjenkjennelig. Dette brettet syntes vi ble noe enkelt i utformingen, og vi var interessert i å se hvor vi kunne ta utformingen med noe mer spennende i tankene.



Figur 9: Brettspillutforming 2.0

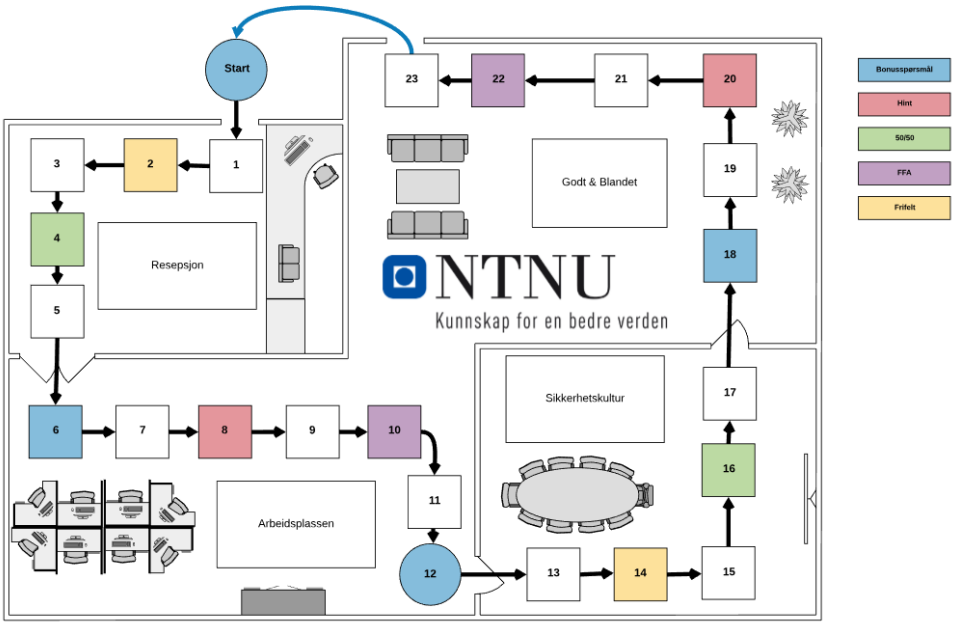
Figur 10 er det brettet som er utviklet med noe mer spennende i tankene. Et problem vi så med denne utformingen er at det kan oppfattes som lite oversiktlig, men grunnideen til denne utformingen er noe vi ønsker å beholde. Det er også vanskelig å skille mellom hvor de forskjellige sonene er. Bakgrunnen til dette designet var at figur 9 lignet på verdens mestselgende brettspill Monopol[3]. Ved å plassere feltene forskjellige plasser på brettet vil utformingen virke nytt på de som spiller spillet, noe vi antok ville gjøre spillet mer interessant for deltagerne.



Figur 10: Brettspillutforming 3.0

Utfordringen ble å finne en kombinasjon mellom å være oversiktlig og lett å forstå, samtidig som det skal være noe nytt og spennende. Figur 11 er det brettet vi endte opp med. Vi har tatt størst utgangspunkt i figur 10, men det er gitt mer struktur og fylt kontoret med flere elementer. Her har vi også løst problemet med at det ikke kommer tydelig fram hvilken sone man er i til enhver tid.

[3] *Monopol (brettspill)* https://no.wikipedia.org/wiki/Monopol_(brettspill) (Besøkt 23.04.2019)



Figur 11: Brettspillutforming 4.0

Siden oppdragsgiverne har ytret et ønske om å sette sitt eget preg på spillet har vårt fokus ligget på funksjonalitet og illustrasjon av et eventuelt sluttprodukt. Vi har ikke lagt fokus på designprinsipper og andre virkemidler i utformingen.

5.2.1 Materialer

Spillets brett og spørsmål ble printet i A3 format på 250 gram papir. Dette ble gjort for å øke kvaliteten på prototypen, men også for å gjøre innholdet på spørsmålene mindre synlig fra baksiden. Til stjelesjetonger ble det brukt pokersjetonger og spillebrikkene ble tatt fra et annet brettspill.

5.3 Testing i utviklingsfasen

Testen som ble utført var nødvendig for å få en god spilltest hos oppdragsgiverne. Dette gav oss muligheten til å få avdekket kompleksitet og ytelsen i spillet før den ordentlige testen. Det var en mulighet å teste det innad i gruppen, det ville spart oss tid og vi kunne sette i gang handling etter vi hadde avdekket svakheter i spillet. Et viktig element for oss som skal administrere spillet var objektivitet. Det er viktig at den kunnskapen deltagerne sitter igjen med kommer fra spillet, og ikke basert på hvor mye administratoren involverte seg i diskusjoner eller forklaringer. Testing utført på personer som ikke har bakgrunn innen informasjonssikkerhet gir oss en indikasjon på hvor vanskelighetsgraden ligger, i kontrast til personer med bakgrunn innen informasjonssikkerhet.

Testen hadde fokus på vanskelighetsgrad, brukervennlighet, tilbakemeldinger fra deltagerne, og eventuelle observasjoner som ikke ble regnet med i malen for testingen. Vanskelighetsgraden handler om spørsmålene er vanskelige å forstå, om spørsmålene var for korte eller for lange, og i hvor stor grad de var relevante. Brukervennligheten blir

definert som "the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use"[4].

Fokuset kan deles inn i tre hovedelementer[5]:

Intuisjon:	om brukeren gjør de rette tingene
Effektivitet:	hvor lang tid brukeren bruker på å utføre oppgavene
Tilfredshet:	subjektiv vurdering fra brukeren

Første punktet viser om brukeren er i stand i å utføre en oppgave og informasjon på hvor mange feil som blir gjort underveis. Det andre punktet omhandler hvor lang tid det ble brukt eller hvor mye ressurser som ble brukt til å utføre en oppgave. Det siste punktet fokuserer på hvilken grad brukeren er tilfreds med bruken av selve produktet.

5.3.1 Resultat fra første spilltest

Vi utførte en spilltest [C] på fire personer der vi sjekket vanskelighetsgraden, brukervennligheten og dynamikken. Bakgrunnen til objektene vi utførte testen på var:

- To deltagere Webdesign årsstudium
- En deltager Første år bachelor BITSEC
- En deltager Tredje år bachelor programmering

Totalt var det fire lag, med en deltager på hvert lag. Før spilltesten begynte måtte administratoren (oss) forklare reglene, som var forståelige og ukomplisert for deltagerne. To av deltagerne hadde ikke innsikt innen sikkerhet og var derfor litt skeptisk om at det var et spill for dem, de to resterende har vært innom sikkerhet i studiet. Deltagernes første reaksjoner var at brettet var utformet elegant, veldig selvbeskrivende, enkelt, og forståelig at de måtte gå gjennom forskjellige soner.

Antall Poeng	Deltagernummer	Bakgrunn
16	1	Programmering
10	2	Webdesign
6	3	Webdesign
5	4	Informasjonssikkerhet

Tabell 10: Poengtabell for deltagerne som var med på spilltest

Noen spørsmål hadde ukjente begreper som var uforståelig for noen av deltagerne, *eksempelvis begrep som Sosial manipulering, Virtual Private Network (VPN) og Polymorfisk virus*. Majoriteten av spørsmålene var forståelige. Lange spørsmål eller lange svaralternativer var problematisk for deltagerne. Dette resulterte i at de ba administratoren repetere svaralternativene og/eller spørsmålet. De foreslo en løsning på problemet ved å ha alle kortene digitalt så det er mulig for alle å se spørsmålet og gruble over det. Vanskelighetsgraden varierte, deltagerne mente dette var positivt. Variasjon bidrar til at flere føler seg inkludert og kan svare på spørsmål. Totalt ble det stilt 40 spørsmål.

[4] *ISO 9241-11:2018(en)* https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en (Besøkt 01.04.2019)

[5] *Kan vi måle brukervennlighet?* https://www.visma.no/blogg/kan-vi-male-brukervennlighet/ (Besøkt 01.04.2019)

Spørsmålene ble besvart på mellom 30 og 60 sekunder. Reglene og brettets utforming var som beskrevet over, veldig selvbeskrivende og forståelig. Dette medførte at deltagerne ikke gjorde feil under spilltesten. Tilfredshet ble vurdert gjennom observasjon, deltagerne konkurrerte med hverandre og var veldig engasjerte. Spilltesten skulle vare 45 minutter, men varte 55 minutter. Dette kan knyttes til at spillet var så engasjerende at de/vi glemte tiden.

Flere observasjoner under testen var at deltagerne diskuterte mellom seg uten påvirkning av bachelorgruppen. Etter at en deltager svarte feil så ble det skapt en diskusjon mellom andre deltagere om hvorfor det var feil svar og hvorfor det andre alternativet var rett. Scenario og erfaringer fra deltagerne ble lagt frem under diskusjonene, dette observerte vi som fri flyt av informasjon som er noe vi ønsket (2.3.2 siste punkt). Det ble lagt merke til at etter den andre runden så begynte den ene deltageren å bruke stjelesjetongen. Dette skapte en slags dominoeffekt og førte til at de andre deltagerne begynte å bruke sjetongen også. En deltager fikk frastjålet mange spørsmål og virket irritert, men dette førte til mer konkurranse.

Tilbakemeldinger vi fikk var både positive og negative. De syntes spillet var veldig bra. De som ikke hadde bakgrunn innen sikkerhet følte de var inkludert og kunne være med på konkurransen. Belønning etter man svarer rett var noe de savnet. De mente at å bare få poeng ikke var så veldig engasjerende. Spørsmålene burde enten bli delt ut fysisk eller vist digitalt på en skjerm eller PC. For å redusere antall tapte runder for spiller(e) som blir frastjålet mye kan det bli lagt til flere Alle-mot-Alle felter, slik at alle kan delta. Det var mye relevant opplæringsmateriale, som for eksempel e-post og offentlig WIFI. Etter spillets slutt kunne det bli tatt en runde med spørsmål som enten ble svart feil på eller var vanskelige slik at de får utbytte av å huske forklaringene på de vanskelige spørsmålene. Et annet forslag som ble presentert var å endre stjele tidspunktet til etter spørsmålets besvarelse, om en spiller mente at den andre spilleren svarte feil på et alternativ. Dette ville gjøre at alle fikk delta på sine spørsmål, og andre kan prøve å få poeng dersom de mener at feil svar ble gitt, i bytte mot lavere engasjement fordi man ikke kan direkte stjele et spørsmål fra andre.

5.3.2 Videre utvikling etter første spilltest

Etter spilltesten var det klart at det var et forbedringspotensial. Det første som ble bestemt er at hint-feltene skal fjernes. Hint-feltene var noe som ikke var prioritert i tiden frem mot testen. Da deltagerne ble spurt etter testen hvorvidt hint hadde gjort noen forskjell på spillet, svarte alle at det ikke hadde hatt noen særlig effekt på spillet. Med fjerningen av hint-feltene måtte de bli erstattet med noen andrefelt. Alle-mot-alle feltene var noe av det mest positive og engasjerende med spillet. Å implementere flere slike felter gir mening basert på de tilbakemeldingene vi fikk. Vi ble gjort oppmerksomme på at alle-mot-alle feltene kunne utnyttes ved å svare et tilfeldig alternativ bare for å hindre de andre deltagerne fra å få poeng. Løsningen på dette problemet var å endre regelen for disse feltene litt. Originalt sa regelen at de som svarer først "får" spørsmålet, dette er noe som ble endret på. Dersom man svarer feil mister man muligheten til å svare igjen

på det spørsmålet. De andre spillerne vil da ha ett mindre svaralternativ å forholde seg til, som gjør det lettere å velge riktig.

Vi bestemte oss for å redusere lagene slik at det ville være kun en spiller på hvert lag. Gjennom spilltesten hadde spillerne gode diskusjoner på tross av at de spilte mot hverandre og det var en avslappet atmosfære. Dermed var vi ikke redde for at det ble lite med diskusjon dersom man spiller uten lag. Spillet vil gå raskere fordi spillerne ikke trenger å være enige, og det vil være mer konkurranse mellom spillerne.

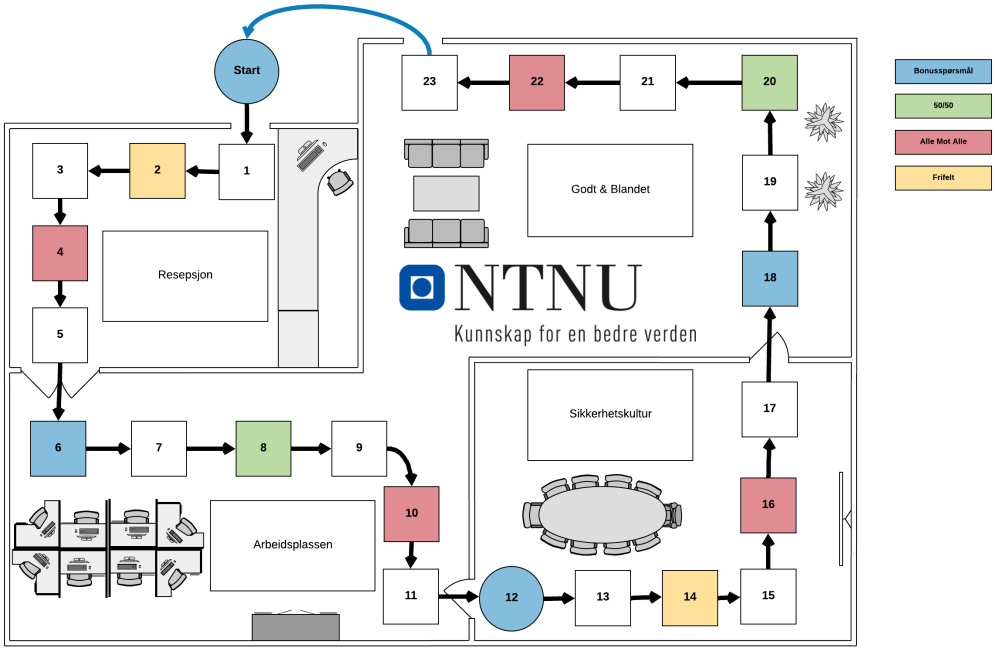
Når det kommer til forslaget om å endre stjeleregelen valgte vi å beholde den gamle regelen, men med en modifikasjon. For å forhindre at noen blir utestengt fra spillet av de andre ved å kontinuerlig stjele spørsmålene til en person, åpner vi for å bruke stjele sjetongen som et forsvar. Dersom noen prøver å stjele spørsmålet ditt, kan du, om du ønsker, velge å forsvare spørsmålet ditt ved å benytte din egen sjetong. Personen som prøvde å stjele vil da få tilbake sjetongen sin. Dette åpner for at de andre spillerne kan prøve å stjele spørsmålet den samme runden, men vi endrer regelen slik at det bare kan brukes én sjetong per "tur". Vi observerte også at spørsmål ble som regel stjålet da noen landet på bonusspørsmål feltet. Ved å ha muligheten til å forsvare seg mot å få spørsmålene stjålet åpner det for litt mer taktikk rundt når man burde stjele, og når man burde forsvare.

Det var ingen av deltagerne som benyttet seg av å velge et vanlig spørsmål på bonusfeltene. Ut ifra den tilbakemeldingen vi fikk så var det et sjansespill på hvor vanskelig bonusspørsmålet er, noe som var spennende. Vi valgte derfor å fjerne muligheten til å velge et vanlig spørsmål i stedet for bonusspørsmålet.
Det var et ønske fra en av deltagerne om at spillkortene ble vist digitalt på en skjerm. Dette fordi det til tider var vanskelig å huske hva det ble spurt om, og hvilke svaralternativer man hadde. Dermed slipper man å spørre om å få repetert spørsmålet og/eller svaralternativene. Vi velger å ikke gjøre dette da vi ikke anser dette problemet som særlig stort. Man har ett minutt til rådighet når man skal svare, og det er godt innenfor tiden å lese opp svaralternativene på nytt dersom deltageren ønsker det.

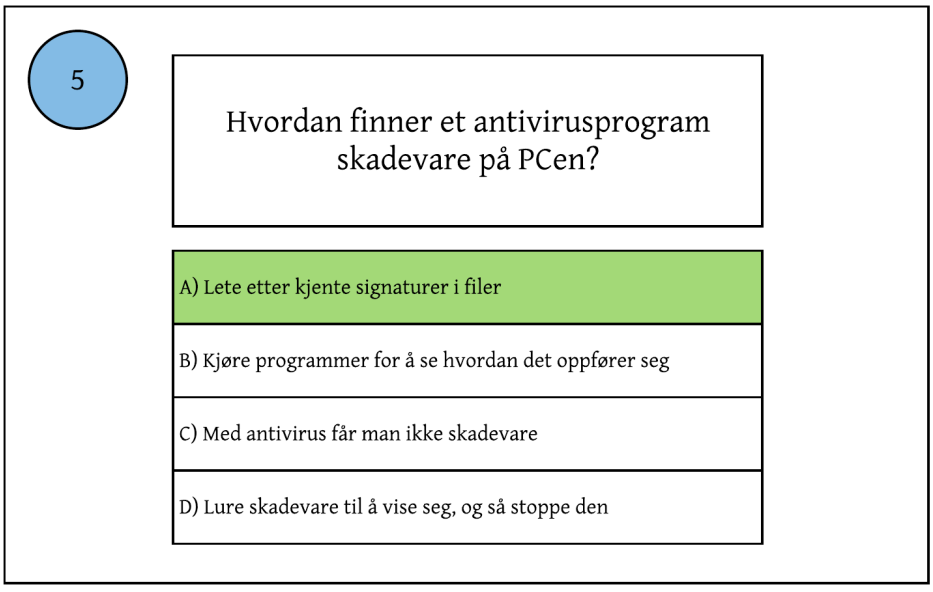
Med disse forbedringene har spillbrettet endret seg litt. Figur 12 er det spillbrettet som ble presentert til oppdragsgiverne. Det eneste som endret på spillbrettet er at hintfeltene er erstattet med alle-mot-alle felter.

Andre endringer som ble gjort med spillet er spørsmålene. Det var flere spørsmål som var tvetydige i forhold til svaralternativene. Alle spørsmålene ble revidert og de som var tvetydige har blitt endret. Figur 13 er et eksempel på et spørsmål som er tvetydig. Her er alternativ A riktig, men alternativ B er riktig i forhold til noen antivirusprogrammer. Dette problemet ble løst ved å endre på svaralternativ B til noe som ikke kan tolkes som riktig.

Det ferdige produktet ligger som vedlegg H.



Figur 12: Brettspill etter første spilltest



Figur 13: Eksempel på tvetydig spørsmål

6 Dataanalyse

I dette kapittelet skal vi presentere resultatene våre fra spilltesten hos oppdragsgiverne. Vi kommer til å gjøre dataanalyse på de resultatene vi har og presentere vår tolkning av de. Vi kommer ikke til å se på forskjeller mellom Norsk Tipping og Skatteetaten i denne analysen.

6.1 Gjennomgang av spilltesten

Oppdragsgiverne hadde som oppgave å finne ansatte som skulle være med på spilltesten. De ønsket i utgangspunktet personer mellom 35-45 år, men dette viste seg å være litt utfordrende. De fikk derfor friere tøyler til å velge personer som skulle være med på spilltesten, men fortsatt finne ansatte som ikke jobbet med informasjonssikkerhet til vanlig.

Vi begynte med å samle alle de ansatte på ett rom. Her introduserte vi oss og forklarte hvordan gjennomgangen kom til å være. Vi delte de ansatte inn i tilfeldige grupper ved å få dem til å trekke en lapp hver med tall på. De ansatte som trakk partall var en gruppe, og oddetall var en annen gruppe. Tallet de trakk ble brukt som deltagernummer. Gruppene ble så tatt til forskjellige rom for gjennomføringen. Her fikk alle en selvevaluering før spillingen begynte. De som trakk partall hadde også kunnskapstesten før spillet.

Spørsmålskortene ble stokket om for å gjøre det tilfeldig hvilke spørsmål de ble stilt. Reglene for spillet var enkelt for de ansatte å forstå. Stjelesjetong regelen var de litt usikre på til å begynne med, men det var lett å forstå da de begynte å bruke den. Gjennomsnittlig ble det stilt 50 spørsmål per spillgruppe som tok mellom 45 minutter - 1 time. Vi observerte at noen spørsmål fikk deltagerne til å dele sine egne erfaringer rundt det spørsmålet gikk ut på. Vi ønsket at spillet skulle ha en slik virkning. Bruken av stjelesjetongen var veldig varierende blant gruppene. Deltagerne var skeptiske til å bruke stjelesjetongen dersom ingen hadde brukt den før. Dette observerte vi også under spilltesten med studenter 5.3.1.

I forhold til hva vi fokuserte på i utvikling av grunnide 5.1.1 observerte vi følgende gjennom spilltesten:

- **Konkurranse:** Majoriteten av spillerne ble synlig mer engasjerte de gangene det ble landet på et alle-mot-alle felt. Dette var også tydelig rundt bruk av stjelesjetongen. I noen gjennomføringer var det ikke mulig å vise poengene hver deltager hadde til enhver tid. I de gjennomføringene hvor de var synlige var det mer konkurranse i form av at andre spillere stjal mer aktivt fra poeng lederen.
- **Diskusjon:** Det var varierende grad av diskusjoner innenfor de ulike gruppene, noen deltagere var svært aktive og delte mye, andre var mer passive og fulgte spillets gang. Det kunne virke som det ble mer diskusjon i etterkant av alle-mot-alle

spørsmålene, som kan være fordi alle spillerne følte seg mer involverte enn hva de gjorde når en annen spiller fikk et spørsmål. Vi forventer at mengden diskusjon vil øke med en administrator som oppfordrer aktivt til diskusjon og evt. stiller oppfølgingsspørsmål til deltagerne.

- **Kompleksitet:** Reglene ble forklart i forkant av hver gjennomføring. Den mest kompliserte regelen i spillet er stjelesjetong og dens bruk, som måtte i noen tilfeller repeteres, men utover det ble det brukt relativt lite tid på å forklare spillet.
- **Strategi:** Stjelesjetongen hadde varierende grad av bruk, noen grupper hadde stort svinn fordi de ikke brukte stjelesjetongen, andre grupper brukte alle stjelesjetongene uten svinn. Vi opplevde allikevel at stjelesjetongen var en suksess, spillere med strategisk interesse fikk brukt dem på gode måter, og de var ikke til noe hinder for spillere som tilsynelatende ikke puttet så mye tankegang i bruken av sjetongen. De kunne da bruke den til å forsvare egne spørsmål som igjen ga de mer offensive spillerne muligheter senere.

Etter spillet utførte alle den samme selvevalueringen som de gjorde før spillet. Etter selvevalueringen fikk oddetallsgruppen kunnskapstesten. Etter alle var ferdige kunne de åpent gi tilbakemeldinger eller stille spørsmål. Generelt syntes majoriteten at det var en ny og engasjerende læringsform, og de følte at de hadde lært noe gjennom spillingen. Mange ga også utrykk for at kunnskapstesten var vanskelig. Flere mente at spillet var litt for teknisk og benyttet for mange tekniske begreper. Gruppen observerte i noen tilfeller at disse deltagerne fortsatt husket navnene etter testens gjennomførelse, men ikke nødvendigvis hva det var. Dermed kan det hende at de hadde fått et større læringsutbytte fra de tekniske begrepene enn de selv trodde i det at de vil kjenne igjen begrepene ved en senere anledning, men dette kan vi ikke si sikkert.

Selvevalueringen E og kunnskapstesten F er lagt til som vedlegg.

6.1.1 Vanskelighetsgrad

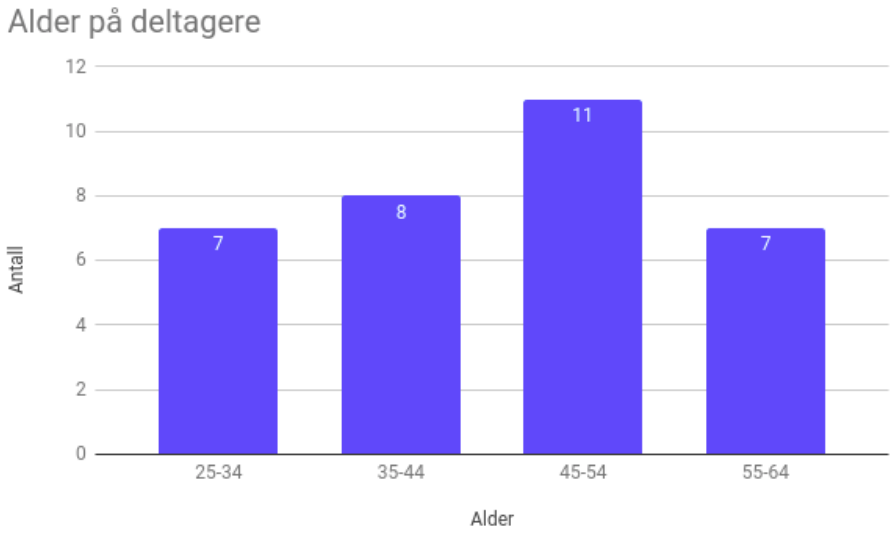
I 6 av 8 grupper noterte vi hvor mange spørsmålskort deltagerne var innom og hvor mange av disse spørsmålene som ble besvart riktig. Med dette ønsker vi å si noe om vanskelighetsgraden. Det var viktig med en god balanse, deltagerne burde få en følelse av oppnåelse gjennom spillet, men også at det fortsatt var mer å lære. I tabell 11 ligger antall kort lest i løpet av spillet og hvor mange spørsmål som ble riktig besvart i løpet av hver gjennomføring. For noen grupper var prosent riktig høyt og for andre lavt. Vi så for oss den ideelle vanskelighetsgraden til å være rundt 2/3 slik at deltagerne får en balanse av oppnåelse og utfordring i spørsmålene. Dermed skulle spillet vært litt vanskeligere enn hva det var.

	Gr.2	**Gr.4**	**Gr.5**	**Gr.6**	**Gr.7**	**Gr.8**	**Snitt**
Antall riktig	37	41	29	42	34	42	37.5
Totalt antall	47	60	40	53	42	56	49.67
Prosent	78.72%	68.33%	72.50%	79.25%	80.95%	75.00%	75.79%

Tabell 11: Antall riktig besvarte spørsmål

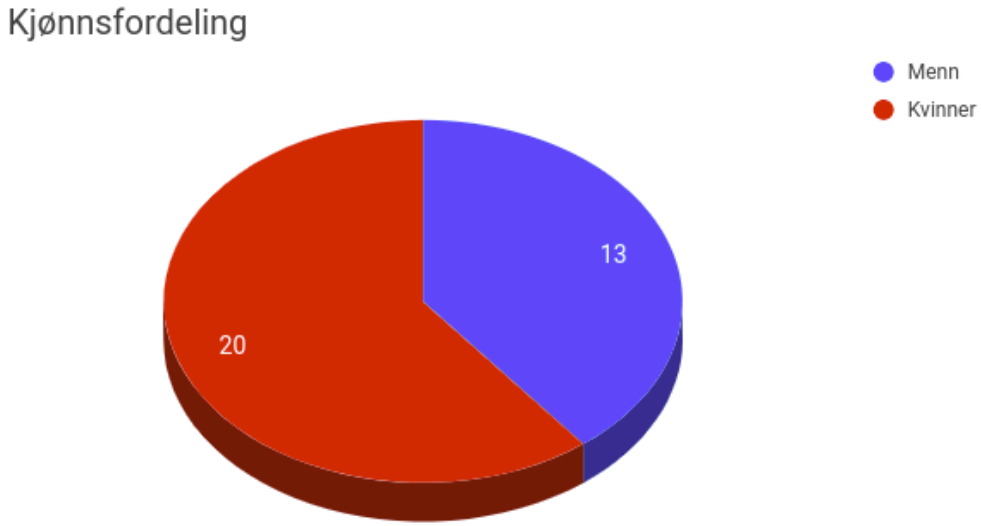
6.2 Demografi

Vi begynner analysen med hvordan demografien ser ut. Totalt hadde vi 33 deltagere. Aldersfordelingen mellom disse er vist i histogram 14. Vi ser at det var en veldig variert aldersfordeling.



Figur 14: Aldersfordeling

Kjønnsfordelingen er vist i kakediagram 15. Det var en kjønnsfordeling på ca. 40% menn og ca. 60% kvinner.



Figur 15: Kjønnsfordeling

6.3 Resultater fra selvevalueringen

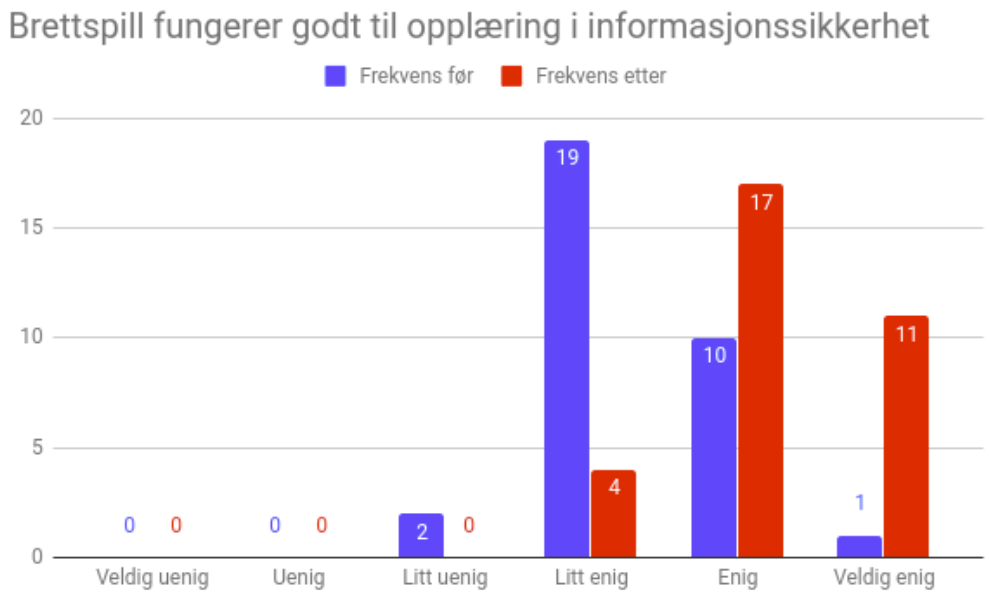
Resultatene er fremstilt med ett søyle diagram og en tabell. Diagrammet viser frekvensen av svar på selvevalueringen før og etter. Vi ville finne ut hvilken side av skalaen de forskjellige personene lå på etter pretesten i motsetning til posttesten. Dersom en deltager har utgangspunkt i "Enig" siden og allikevel hatt en endring i retning "Veldig enig" har dette en helt annen betydning enn en deltager med utgangspunkt på den andre siden av skalaen. Vi valgte derfor å vise hver deltagers endring i en tabell for å kunne si noe om dette. Tabellen benytter verdier mellom 1 - 6 hvor 1 er "Veldig uenig" og 6 er "Veldig enig". Den forteller konkret hvor mange deltagere som hadde endret mening i en konkret retning, og hvor mye endringen har vært for deltageren. Endringer i retning "Veldig enig", kalt "positiv endring", vil bli gitt fargen grønn, og endringer i retning "Veldig uenig", kalt "negativ endring", vil bli gitt fargen rød. Om én deltager svarte "Litt uenig" på pretest og "Enig" på posttesten ville dette være en verdi på 2, om endringen hadde gått motsatt vei ville endringen være -2.

6.3.1 Tolkning av spørsmål 1

"Brettspill fungerer godt til opplæring i informasjonssikkerhet"

Vi stilte dette spørsmålet fordi vi ønsket en tilbakemelding fra deltagerne om spillet fungerte til opplæring. Dersom resultatet viser en endring mot "Veldig Enig" etter spillet kan det tyde på at brettspill fungerte godt til opplæring. Viser resultatet en endring mot "Veldig uenig" etter spillet kan det tyde på at brettspill ikke fungerte så godt til opplæring. Dersom det ikke var noen endring mellom før og etter kan det tyde på at spillet ikke har hatt noen særlig påvirkning på de som deltok.
Dersom alle deltagerne hadde svart "Veldig enig" både før og etter, ville dette vært lovende for brettspill som virkemiddel i opplæring generelt, men ville sagt oss lite om hvordan brettspillet hadde påvirket deltagerne. Det mest optimale utfallet ville ha vært hvis resultatene etter spillet hadde hatt stor endring mot "veldig enig". Resultatet [16] viser en stor positiv endring i svarene til deltagerne. I svarene fra pretesten lå 90.6% av deltagerne på 4 og 5, mens etter testen lå 87.5% på 5 og 6.

På dette spørsmålet ble én deltager fjernet fra statistikken på grunn av et svar utenom alternativene som var gitt.



Figur 16: Spørsmål 1 selvevaluering

Tabell 17 viser at det ikke var noen som hadde en negativ endring, og 71.8% av alle deltagerne hadde en positiv endring i en eller annen grad. Flere av disse hadde også en endring på mer enn ett alternativ. Dette resulterte i en høy samlet endring for gruppen.

Deltager	19	11	18	4	12	33	37	34	32	38	20	16	15	17	8	7	9	5	6	25	23	21	31	26	28	24	22	2	3	1	27	35	36
Før	4	5	5	5		5	5	4	4	6	4	4	5	5	4	4	4	4	4	5	5	4	5	4	3	4	4	4	4	3	4	4	4
Etter	4	5	5	5		5	5	4	4	6	5	5	6	6	5	5	5	5	5	6	6	5	6	5	4	5	5	6	6	5	6	6	6
Endring	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2

Figur 17: Spørsmål 1 selvevaluering

Deltagerne var positive til brettspill i opplæring allerede før gjennomgangen og under gjennomgangen har deres oppfatning av hvor godt brettspill fungerer økt. Disse resultatene kan antyde at deltagerne var reseptive ovenfor å få opplæring gjennom brettspill og at opplevelsen i løpet av testen gjorde dem mer interesserte i denne læringsformen. Det er ikke urimelig å anta at de var engasjerte i spillet, noe som stemte overens med observasjoner gruppen gjorde seg under testen.

6.3.2 Tolkning av spørsmål 2

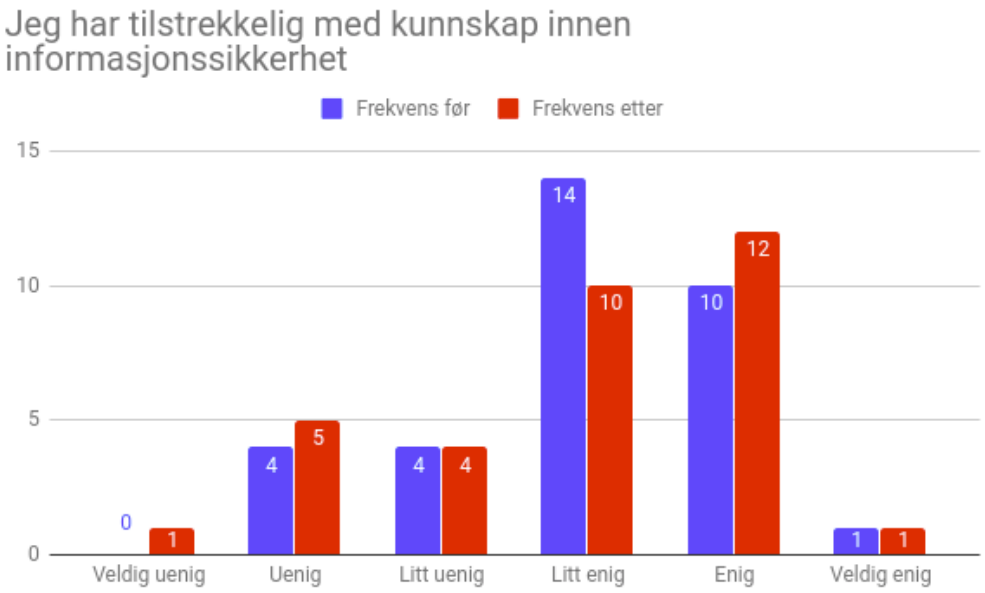
"Jeg har tilstrekkelig med kunnskap innen informasjonssikkerhet"

Dette spørsmålet viser hvor bevisste deltagerne var rundt informasjonssikkerhet og avdekke deres holdninger til kunnskap rundt informasjonssikkerhet. På grunn av omfanget i informasjonssikkerhet er det vanskelig å kunne alt og det er en vanlig holdning i informasjonssikkerhet at man aldri kan være helt sikker.

Hvordan hver av deltagerne tolket hva som er tilstrekkelig kunnskap innen informa-

sjonssikkerhet varierer. Spillet dekker mange områder innen informasjonssikkerhet, men hver av dem er på et grunnleggende nivå. En måte å tolke dette spørsmålet på er at en positiv endring vil være det beste. Dette kan indikere at spillet har gitt mye kunnskap til deltagerne, og at de føler seg bedre rustet til å takle informasjonssikkerhet i fremtiden. En negativ endring kan bety at deltagerne skjønner at det ligger mye mer bak alt innholdet i spillet og forstår at det er lurt å være mer forsiktig. Vi mener da at en negativ endring det mest optimale utfallet.

Figur 18 viser resultatet fra dette spørsmålet. Her ser vi en stor spredning både før og etter, og at det ikke er noen store endringer i gruppen som en helhet.



Figur 18: Spørsmål 2 selvevaluering

Selv om den generelle endringen for gruppen som en helhet har vært liten, ser vi at endringene blant deltagerne har vært stor i begge retninger. Tabell 19 viser at omtrent like mange har hatt positiv og negativ endring, dette forklarer den lille endringen for gruppen som en helhet. Vi ser at majoriteten av deltagere med negativ endring ligger på "Enig" siden av skalaen, men de fleste har endt opp på den andre siden. Vi ser i tillegg to deltagere som har endret sin mening 2 alternativer og én deltager med en endring på 3. Disse tre deltagerne lente alle sammen opprinnelig mot "Enig", men endte opp på uenig siden.

Majoriteten av deltagerne med positiv endring hadde utgangspunkt på "Enig" siden av skalaen og deretter økt ett alternativ. De få som var på "Uenig" siden har endret mening i større grad. Resultatet viste at 6 av 8 deltagere, med positiv endring, endte opp på "Enig" og de resterende 2 deltagerne "Litt enig".

Deltager	24	11	26	19	6	33	31	22	32	20	15	18	8	3	1	9	4	25	27	23	35	37	34	38	36	16	17	2	7	12	28	5	21
Før	5	4	5	4	3	2	3	5	5	4	4	4	3	4	5	5	5	2	5	5	4	3	6	4	5	4	4	4	4	4	4	2	2
Etter	2	2	3	3	2	1	2	4	4	4	4	4	3	4	5	5	5	2	5	5	4	3	6	4	5	5	5	5	5	5	5	4	4
Endring	−3	−2	−2	−1	−1	−1	−1	−1	−1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	2	2

Figur 19: Spørsmål 2 selvevaluering

Vanskelighetsgraden 11 på spillet kan ha hatt noe å si for resultatet. Dersom en deltager svarer riktig på alle spørsmålene kan deltageren få inntrykk av å ha tilstrekkelig med kunnskap. Fra deltagernes standpunkt kan det antyde at de som hadde positiv endring fikk en følelse av oppnåelse i løpet av spillet, og de med negativ endring følte det var mange utfordrende spørsmål. På tross av dette var det ideelt å se en negativ endring på dette spørsmålet. Målet var å gi økt kunnskap, men også å åpne øynene til de som spiller om at informasjonssikkerhet er veldig omfattende. Siden gruppene med positiv og negativ endring var omtrent like store vil det ikke ha vært lurt å bare øke vanskelighetsgraden, men heller gjøre det tydeligere i spillet at informasjonssikkerhet har et stort omfang.

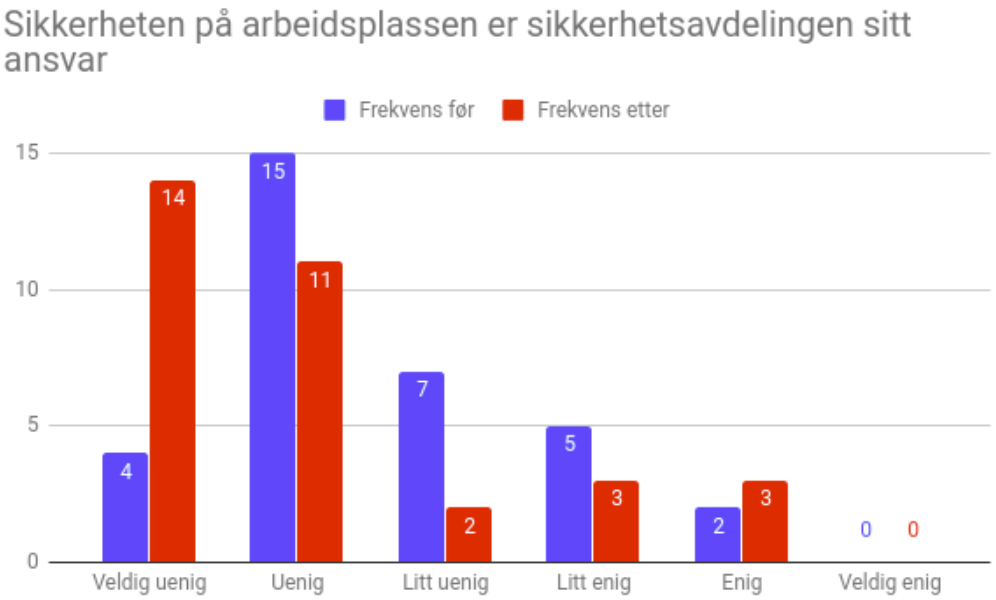
6.3.3 Tolkning av spørsmål 3

“Sikkerheten på arbeidsplassen er sikkerhetsavdelingen sitt ansvar”

Dette spørsmålet ble stilt for å finne ut hvilke holdninger de ansatte har om ansvarsfølelse rundt informasjonssikkerhet. Alle har et ansvar for informasjonssikkerhet og dette er noe vi hadde et fokus på i utviklingen av spillet.

Dersom resultatet viser en endring mot “Veldig enig” etter spillet kan det tyde på at deltagerne mener at sikkerhetsavdelingen har alt ansvaret for sikkerhet på arbeidsplassen. Dersom resultatet viser en endring mot “Veldig uenig” etter spillet kan det tyde på at deltagerne mener at alle har et ansvar for sikkerheten på arbeidsplassen, ikke bare sikkerhetsavdelingen.

I figur 20 er det en stor endring i retning “Veldig uenig”. Resultatene før spillet viste at modus lå på “Uenig” med 45.45% av alle deltagerne. Etter spillet ble modus “Veldig uenig” med 42.42% av deltagerne.



Figur 20: Spørsmål 3 selvevaluering

Tabell 21 viser at 1 deltager hadde en positiv endring og 15 deltagere hadde en negativ endring.

Deltager	3	5	38	20	19	11	15	18	17	8	2	1	33	28	36	7	9	4	6	12	25	27	23	21	35	31	37	26	24	22	34	32	16
Før	3	4	3	3	2	2	2	3	2	2	2	3	2	2	4	2	2	5	4	2	1	3	1	2	5	2	1	2	2	4	1	4	3
Etter	1	2	1	2	1	1	1	2	1	1	1	2	1	1	3	2	2	5	4	2	1	3	1	2	5	2	1	2	2	4	1	4	5
Endring	-2	-2	-2	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2

Figur 21: Spørsmål 3 selvevaluering

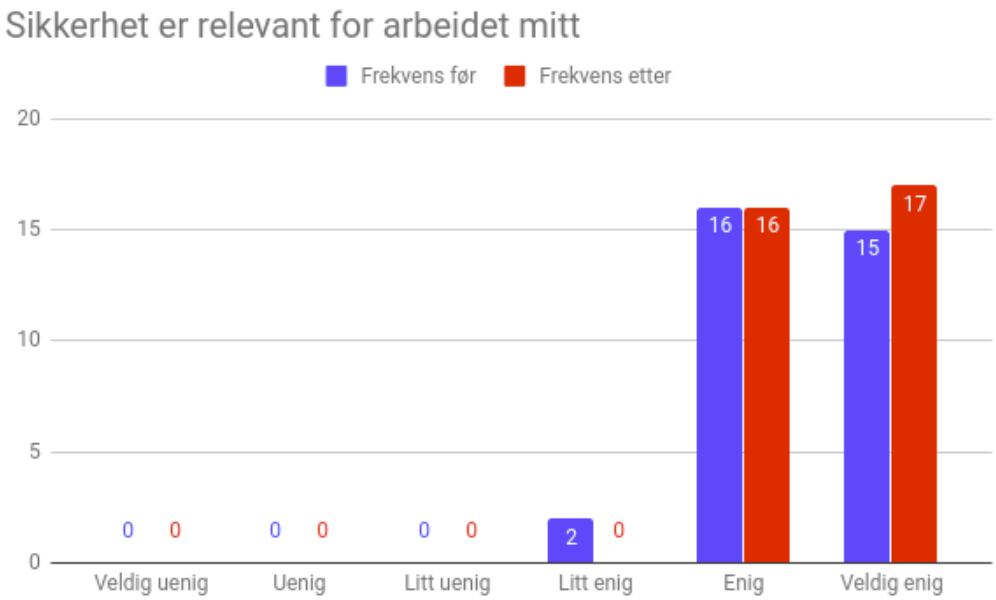
Gjennom utviklingen av brettspillet har vi hatt et fokus på å fremme god sikkerhetskultur. For at en bedrift skal ha en god sikkerhetskultur er det viktig at alle ansatte vet at de har et ansvar for sikkerheten. At vi ser en negativ endring mot "Veldig uenig" kan tyde på at spillet har gjort majoriteten oppmerksomme på at alle har et ansvar for sikkerheten. Det er noen deltagere som er mer på "enig" delen av spekteret. Dette kan være fordi spørsmålet ikke var tydelig nok, og det kan også være fordi deltagerne ikke fikk noen spørsmål som omhandlet akkurat hvem som har ansvaret for sikkerheten.

6.3.4 Tolkning av spørsmål 4

"Sikkerhet er relevant for arbeidet mitt"

Det vi ønsker å få ut av dette spørsmålet er å finne ut hvor viktig de ansatte syntes sikkerhet er for arbeidet deres. Mange av spørsmålene i spillet inneholder informasjon vi mener er relevant for alle. Dersom resultatet viser en endring mot "Veldig enig" kan det tyde på at sikkerhet er relevant for arbeidet sitt. Dersom resultatet viser en endring mot "Veldig uenig" kan det tyde på at deltagerne mener sikkerhet ikke er viktig for arbeidet sitt.

I figur 22 ser vi at endringene mellom før og etter testen var svært små, men alle svarene ligger på “Enig” og “Veldig Enig”.



Figur 22: Spørsmål 4 selvevaluering

Tabell 23 viser endringer som ikke er så tydelige gjennom diagrammet 22, men det er ikke store nok endringer til å ha noen innvirkning på resultatet.

Deltager	17	20	19	11	16	15	18	2	7	9	5	4	6	12	25	27	23	33	35	31	37	26	28	24	34	32	38	36	8	3	1	21	22
Før	6	5	5	6	5	6	6	6	5	5	5	6	5	5	6	6	6	6	6	5	6	6	5	5	6	5	6	5	5	5	4	4	5
Etter	5	5	5	6	5	6	6	6	5	5	5	6	5	5	6	6	6	6	6	5	6	6	5	5	6	5	6	5	6	6	5	5	6
Endring	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1

Figur 23: Spørsmål 4 selvevaluering

Endringen i dette spørsmålet var liten både for gruppen som helhet og blant deltagerne. Det mest optimale resultatet på dette spørsmålet er en endring mot “Veldig enig”. Dette er mest sannsynlig fordi de allerede var klar over hvor relevant sikkerhet var for arbeidet deres.

6.4 Resultater fra kunnskapstesten

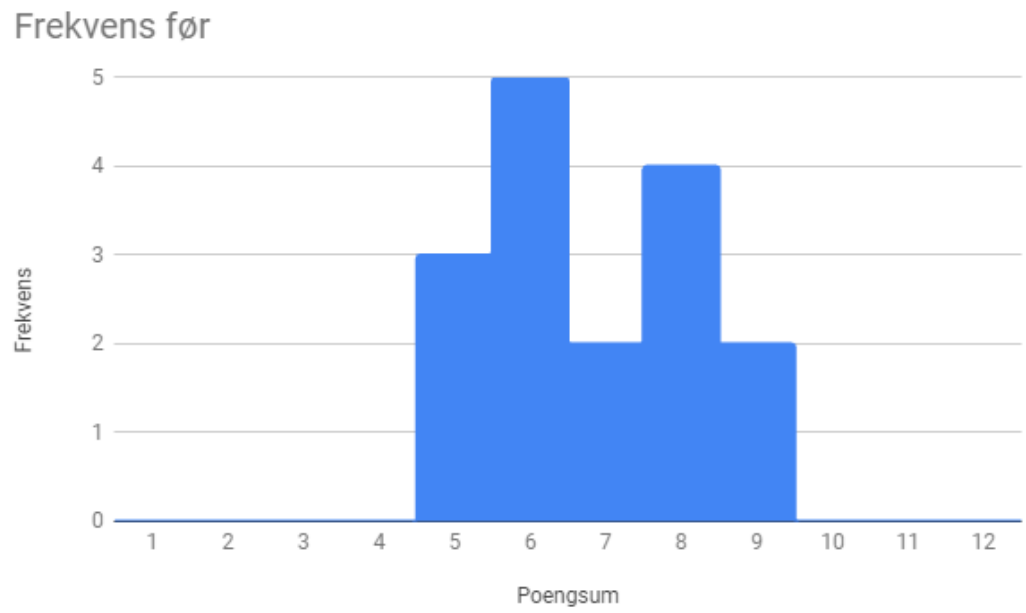
Før vi begynner med analyse av resultatet skal vi gå inn på hvordan vi ga poeng på kunnskapstesten 24.

Flervalgsoppgaver	1 poeng for riktig svar. 0 poeng for feil svar eller mer enn ett svar
Evalueringsoppgave	1 poeng for riktig svar. 0 poeng for feil svar
Åpent spørsmål	VPN = 50%, HTTPS = 15%, Antivirus = 15%. Dersom alle disse er nevt får deltageren 100%. 20% kan gis utenom de nevnte punktene dersom det er en annen god metode
Avkrysningsoppgave	3 riktige alternativer. 1/3 poeng for hvert riktig alternativ. Minus 1/3 poeng for hvert galt alternativ
Rangeringsoppgave	Dersom 1,2,3 er: "Være tilkoblet et offentlig nettverk uten ekstra sikkerhetsmekanismer", "Logge inn på en nettside som begynner med http://" og "Laste ned en film fra en ulovlig nettside", vil deltageren få 100%. Dersom ikke alle disse alternativene er med i topp 3, vil deltageren få 1/3 poeng for hvert av disse alternativene som er med i topp 3

Figur 24: Retting av kunnskapstest

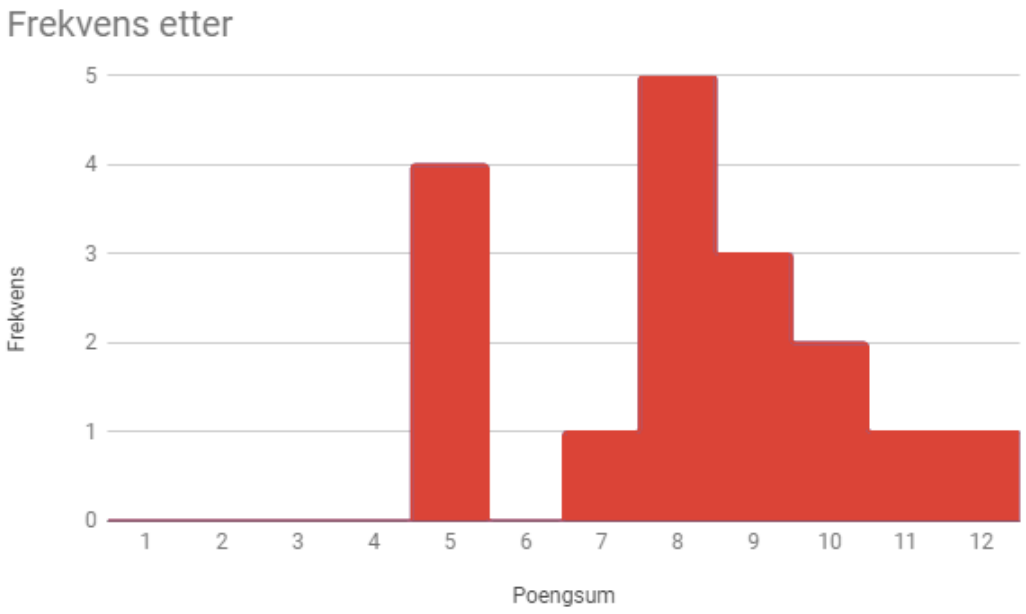
I resultatet fra kunnskapstesten hadde vi 16 deltagere som gjorde den før spillet, og 17 som gjorde den etter spillet. For å vise forskjellen mellom gruppene som tok pre- og posttesten grupperte vi poengsummene ved å runde dem opp til nærmeste hele tall. Disse frekvensene ble plottet i et histogram.

Figur 25 viser resultatene fra pretesten. Her ser vi en relativ liten spredning hvor alle deltagerne ligger omtrent midt på skalaen.



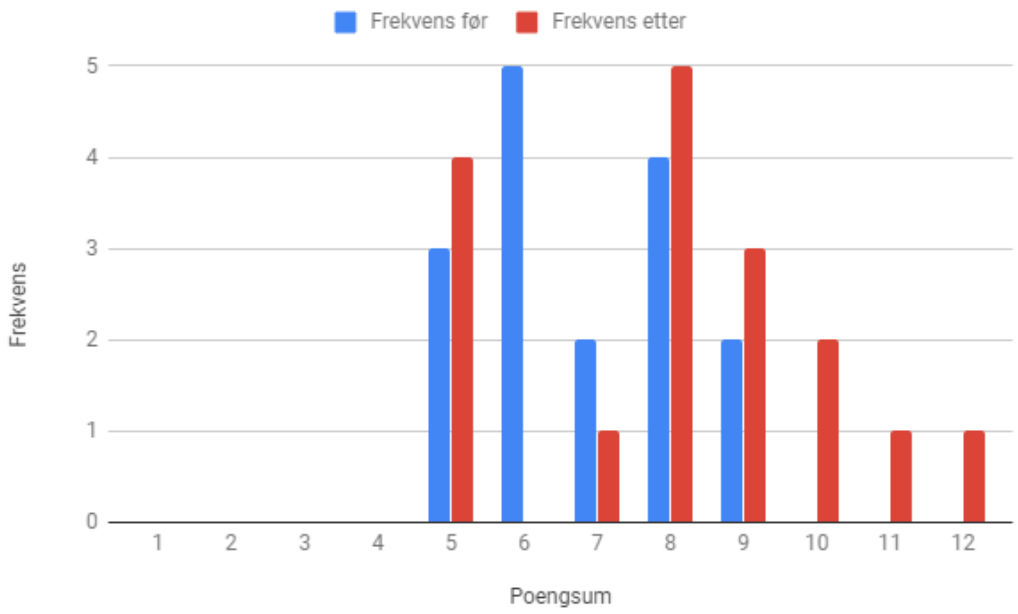
Figur 25: Frekvens resultater før

Figur 26 viser resultatene fra posttesten. Her ser vi en større spredning og en generell forskyvning mot den høyere enden av skalaen.



Figur 26: Frekvens resultater etter

Til slutt kombinerte vi disse to diagrammene for å enkelt kunne sammenligne de to i figur 27. Vi ser en forskyvning i resultatene mellom de to gruppene, gjennomsnittet økte med 19.72% og medianen økte med 25.08% 12.

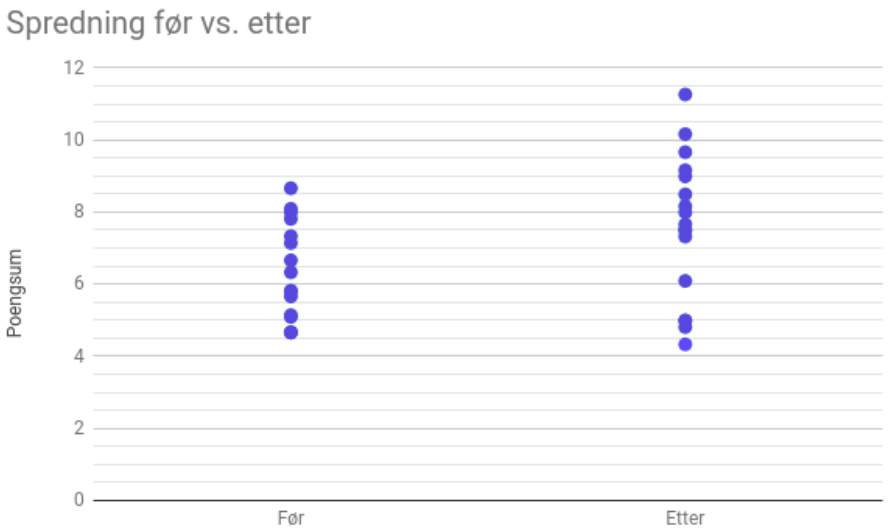


Figur 27: Frekvens resultater kombinert

	Før	Etter
Gjennomsnitt	6.34	7.59
Median	6.07	7.66

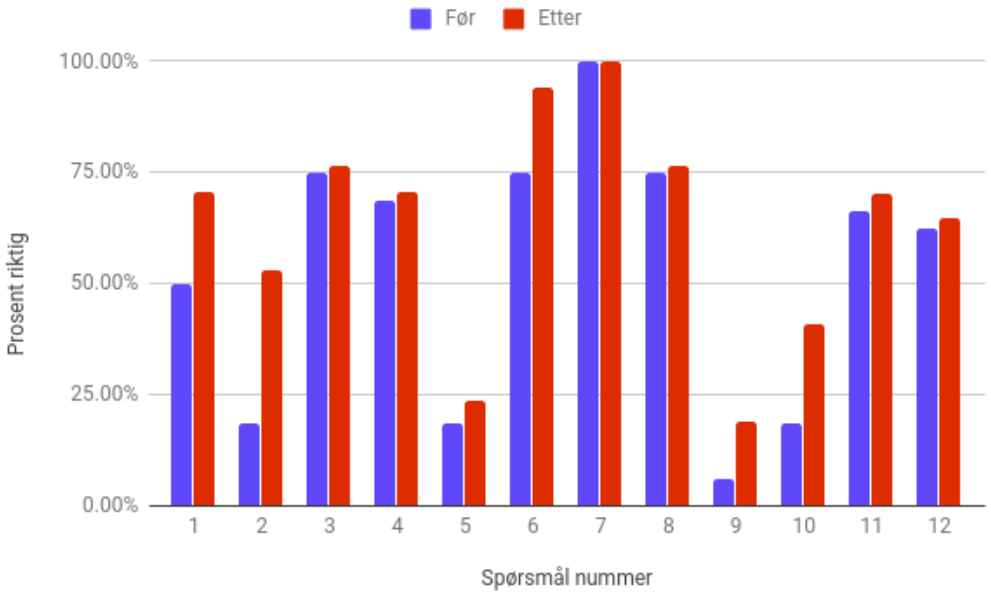
Tabell 12: Sentralmål resultater

I figur 28 har vi plottet alle resultatene for å vise spredning og ekstremverdier. Posttesten har større spredning, men har til gjengjeld en gruppering mellom 7-10 som ligger høyere enn resultatene fra pretesten. Det er også flere ekstremverdier i posttesten som påvirker gjennomsnittet.



Figur 28: Spredning i kunnskapstesten

Siden det er en forskjell i antall deltagere før og etter betyr det for oss at sammenligning mellom gruppenes totale poengsum per spørsmål blir målt i prosent. Figur 29 viser prosent av hvor mange som svarte riktig på hvert spørsmål før og etter spillet. Her ser vi at flere av spørsmålene har ca. like mange riktige før og etter spillet. Den lille forskjellen mellom dem skyldes at vi regner i prosent. Spørsmål 1, 2, 6, 9 og 10 er de spørsmålene som har en endring mellom før og etter spillet. Det er også viktig å presisere at det ikke er noen negativ endring på noen spørsmål. Dette kan i noen tilfeller skyldes at deltagerne kunne det fra før av, eller at spillet har fått kunnskapen opp på nivå med de som tok testen før spillet.



Figur 29: Prosent riktig per spørsmål

Spørsmål 1 handlet om hvorfor man bør oppdatere programvare. Vi ser at 50% av deltagerne visste dette før spillet. Etter spillet ser vi en økning på ca. 20%. Dette kan tyde på at spillet har økt bevissthet rundt å oppdatere programvare.

Spørsmål 2 er det spørsmålet med størst endring. Spørsmålet handlet om hvilket av de følgende passordene som er sikrest. I spillet har vi flere spørsmål der vi går inn på at lengde er bedre enn kompleksitet når det kommer til passord. Tidligere var beste praksis å ha et komplekst passord, og det er dette de ansatte har lært om passord. I de spillene der deltagerne trakk spørsmål som omhandlet passordlenge observerte vi at majoriteten klarte å svare riktig på dette spørsmålet. Det var bare 1 gruppe som ikke trakk noen spørsmål som omhandlet passordlengde, og alle i den gruppen svarte feil på det spørsmålet. Siden den gruppen står for 25% av feil svar på denne oppgaven, er det ca. 1 person som svarte feil på dette spørsmålet selv om ett passordlengde spørsmål ble stilt under spillet.

Spørsmål 5 handlet om å sikre USB-minnebrikker. Her ser vi at kunnskapen før spillet var veldig liten. Etter spillet har det ikke skjedd noen endring. Dette kan tyde på at spillet

ikke har formidlet dette godt nok. Det kan også være på grunn av at spørsmålet i testen var uklart.

Spørsmål 6 handlet om hvorfor man bør oppdatere antivirusprogram regelmessig. Dette er nok et spørsmål som omhandler oppdatering av programvare. Vi ser har at 75% kunne dette før spillet, noe som er ganske høyt. Etter spillet har det skjedd en økning på ca. 20%. Siden dette er en like stor endring som spørsmål 1 som omhandlet det samme, er det sannsynlig at spillet har fungert til å øke bevissthet rundt oppdatering av programvare. Grunnen til at flere svarte riktig før spillet på dette spørsmålet kan være fordi det var lettere å tolke enn det forrige spørsmålet om det samme.

Spørsmål 9 er klart det vanskeligste spørsmålet vi stilte i kunnskapstesten. Dette var et åpent spørsmål der de skulle skrive ned måter å sikre seg på åpne nettverk. Spillet går inn på flere måter å beskytte seg på, hovedsakelig VPN. På dette spørsmålet var det ingen som fikk 100% riktig. Dette kan skyldes at spillet ikke gikk nok inn på forskjellige måter å beskytte seg på. Det kan også skyldes at vi var veldig strenge da det kom til retting av denne oppgaven. Hadde vi vært snillere i rettingen hadde økningen trolig vært den samme.

Spørsmål 10 handlet om å identifisere skadevare. Her ser vi at ca. 20% svarte riktig før spillet. Etter spillet har det skjedd en økning på ca. 20%. En fallgruve i dette spørsmålet er svaralternativet phishing. Stort sett alle deltagerne hadde kjennskap til ordet phishing. Det var veldig mange på dette spørsmålet som svarte at phishing var skadevare, noe det ikke er. De lave resultatene kan skyldes at vi gav -1/3 poeng dersom de svarte på feil alternativer på dette spørsmålet, men det var ikke mulig å få mindre enn 0 poeng.

6.4.1 Tolkning av resultatet

Vi ønsket å se en positiv endring mellom resultatene før spillet og etter spillet. Siden spilltesten ble utført av 2 grupper samtidig ble det lagt stort fokus på at det skulle bli gjennomført likt av begge parter. Ved bruk av de figurene over kan vi se at det har skjedd en endring. Den gjennomsnittlige poengsummen per deltager har økt med 19.72%. For å sette det i perspektiv så er dette en økning på 1.25 poeng. Det er ikke urimelig å si at spillet har spilt en rolle i denne endringen. Mer diskusjon om dette blir gjort i kapittel 7.4.

7 Diskusjon

I dette kapittelet diskuteres forskningsspørsmålene en for en, og en konklusjon til hver av dem basert på innholdet i rapporten.

7.1 Forskningsspørsmål 1 - Hvilke virkemidler kan benyttes i et brettspill for å fremme læring?

Spørsmål og forklaring til spørsmålene er de virkemidlene som danner grunnlaget for læring. Uten disse er det vanskelig å se for seg at brettspillet klarer å formidle læring. . "Trends in learning Report 2018" 2.3.2 viser til at å ha flere spørsmål som er relativt like, men med forskjellig vinkling, er en god læringsmetode. Rapporten viser også til at å fremme deling og samhandling som en del av læringen er en god opplæringsmetode. Vi så gjennom spilltesten at det var nyttig for deltagerne å høre andres erfaringer. Andre virkemidler som har blitt brukt er fokus på at det skal være interaktivt ved bruk av terning og stjelesjetong, og lekent og konkurransepregete ved bruk av stjelesjetong og alle-mot-alle felter 2.3.1. Å utforme brettspillet på en måte som visualiserer en arbeidsdag, og har spørsmål knyttet til arbeidsdagen, er noe som har blitt brukt i tidligere spill 2.2.3. Dette var noe vi også prøvde å gjøre med vårt brettspill, og tilbakemelding fra deltagerne på utformingen har vært positiv. Figur 4 viser at en aktiv rolle er en god måte å lære på, og brettspillet er et godt virkemiddel til å få deltagerne til ta en aktiv rolle.

Det som burde blitt lagt mer fokus på var bruk at stjelesjetongen. Det varierte veldig på hvor mye deltagerne brukte den. Som virkemiddel for å fremme læring var intensjonen at deltagerne skulle ta sjanser på spørsmål de kanskje kunne. Reglene rundt stjelesjetongen burde endres litt for å gjøre at deltagerne bruker den mer.

7.2 Forskningsspørsmål 2 - Hvordan kan man engasjere deltakerne i spillet?

Å få deltagerne engasjerte i spillet har vært et fokus gjennom utviklingen av brettspillet. Gjennom det arbeidet som ble gjort i relatert arbeid i forhold til hvordan man kan engasjere deltagerne i spillet, kom vi fram til de fire punktene for grunnideen til brettspillet 6.1. Gjennom observasjoner under spilling av brettspillet kan vi si at konkurranse skapte mest engasjement. Rundt diskusjon og strategi var det varierende med engasjement, noen spillere var meget strategiske og ønsket mer informasjon som, for eksempel, poengene til de andre deltakerne for å gjøre beslutninger. Andre spillere virket ikke til å ha noen konkret begrunnelse bak valgene sine. Vi observerte ikke at kompleksiteten til spillet skapte engasjement for spillerne, men som vi fant i undersøkelsene vi gjorde i forkant av ideutviklingen 4.2 var det mer sannsynlig at større kompleksitet ville minske engasjementet til spillerne. Våre observasjoner tilsier at mengden kompleksitet i spillet ikke hadde noen negativ innvirkning.

Spørsmålene i spillet er i stor grad det som står for læring og engasjement. Uten spørsmålene hadde ikke spillet fungert til vårt formål. Humor var noe vi prøvde å inkludere i noen spørsmål. Gjennom observasjoner så vi at noen av spørsmålene skapte latter, men mesteparten av latteren kom gjennom deltagernes egne erfaringer og vitser. Dette er noe spillet kunne gjort bedre.

Spillet vil bli benyttet i virksomhetene og antakeligvis bli brukt i en avdeling av gangen. Det er da rimelig å anta at spillerne vil kjenne hverandre bedre og det vil være mer avslappet atmosfære samt bedre diskusjoner. Dette vil ha mye å si for engasjementet til spillerne ettersom at mange av intervjuobjektene våre hevdet en av hovedgrunnene deres til å spille brettspill var det sosiale. En god administrator som deltar på diskusjonen og den uformelle samtalen vil også ha en positiv innvirkning på dette.

7.3 Forskningsspørsmål 3 - Hvordan kan vi teste effekten til brettspillet på de ansattes kunnskap?

For å teste effekten av brettspillet valgte vi å bruke en pre- og posttest i form av en kunnskapstest som omhandler forskjellige områder innen informasjonssikkerhet. Pre- og posttest er en god metode for å finne årsak-og-effekt til det man skal teste, i vårt tilfelle, brettspillet. Det er mange måter å utføre pre- og posttester på. Ved å benytte de seks punktene for å kontrollere de forstyrrende variablene 3.3.2, og ved å bruke pre- og posttest designet vårt 8, vil det øke den interne validiteten på eksperimentet. Dette gjør at man, med større sikkerhet, kan si at resultatet er riktig.

Dersom disse testene skulle blitt gjort på nytt hadde noen ting blitt endret. Det var relativt liten tid mellom utviklingen av spillet og spilltesten. I metoden for pre- og posttest var det noen ting som det ikke var tid til å gjennomføre. Dette inkluderer en pilot-test for å fastslå validiteten til spørsmålene. Dette hadde gjort kunnskapstesten bedre. Resultatene fra kunnskapstesten viste at det var noen spørsmål som de fleste kunne. Slike spørsmål hadde vi endret på slik at det knyttes mer opp mot tema i brettspillet de kanskje ikke er så kjent med fra før av, for eksempel skadevare. Til slutt antar vi at resultatene ville vært mer konsise dersom spredning i alderen til deltagerne var mindre. De yngre deltagerne virket til å ha større kunnskap rundt generell informasjonssikkerhet og dette kan ha påvirket resultatene.

7.4 Forskningsspørsmål 4 - Hvor godt fungerer brettspill for opplæring i informasjonssikkerhet?

Det er vanskelig å si noe om hvor godt brettspillet har fungert til opplæring uten å sammenligne det med andre læringsmetoder. Med det sagt så har vi utført to forskjellige pre- og posttester som skal hjelpe oss med å finne en konklusjon på dette spørsmålet. Fra spørsmål 1 i selvevalueringen 6.3.1 kan vi se at brettspillet har økt deltagernes meninger om hvor godt de syntes spillet fungerte til opplæring. Med resultatene fra kunnskapstesten 27 kan vi se at det har vært en positiv endring i kunnskap innen informasjonssikkerhet.

En ting som holder resultatet tilbake fra å være mer troverdig er at det var relativt få

personer som gjorde kunnskapstesten før og etter. For at resultatet skal bli mer troverdig skulle mengden med personer som tok testen før og etter vært minst 30 stykker.

Skulle vi gjort prosjektet på nytt ville vi først og fremst funnet en måte å inkludere en fullverdig administrator i spillet. Enten ved å fylle denne rollen selv, med retningslinjer for hvordan det skal gjøres, eller benytte en ansatt fra oppdragsgiverne som ville være representativ for den administratoren de vil bruke i senere tid.

Vi ville også ha brukt tid på å få spørsmål og forklaringer digitalisert, slik at disse kunne vises på en projektor foran deltagerne. Dette ville gjort at de kunne lese både spørsmål og svaralternativer flere ganger og muligens husket denne informasjonen bedre. I tillegg ville det vært lettere å vise dem forklaringene for forskjellige spørsmål. 50/50 feltene gjorde dette vanskelig fordi vi hadde markert hvilke svaralternativ som var med i 50/50 og hvilket som var riktig.

Med det sagt så peker begge resultatene fra testene i samme retning. Dette kan tyde på at brettspill fungerer til opplæring i informasjonssikkerhet.

8 Konklusjon

Problemstillingen har vært å se hvor effektivt brettspill er i opplæring av informasjonssikkerhet. Forskningsspørsmål 3 og 4 har vært viktige for å komme frem til en konklusjon. 2 forskjellige pre- og posttester har vært gjennomført for å kartlegge eventuelle endringer i kandidatenes kunnskapsnivå. Gjennom selvevalueringen så vi at de ansatte mener brettspill fungerer godt til opplæring. Kunnskapstesten viser at det har vært en liten økning i kunnskap etter at de ansatte gjennomførte spillet. Gjennom disse observasjonene kan vi konkludere med at brettspill fungerer i opplæring av informasjonssikkerhet på noen områder, spesielt på det å engasjere deltagerne, men at den helhetlige økningen i kunnskap er relativt liten. Hvor effektivt brettspillet er, er vanskelig å svare på siden vi ikke har noe å måle økningen i kunnskap kontra andre læringsmetoder, og hvor godt kunnskapen sitter etter 6 måneder eller 1 år.

Tidligere forskning rundt brettspill som opplæringsmetode viser at dette er en effektiv måte å lære på. Grunnen til at resultatet ikke var bedre kan skyldes at det ikke var et forhåndsbestemt utvalg av spørsmål i brettspillet. Grunnen til at vi ikke gjorde dette er fordi det hadde gjort at resultatet hadde blitt lite troverdig i forhold til brettspillet sin helhetlige opplæringseffekt. Vi anbefaler de som skal bruke spillet å ha et forhåndsbestemt utvalg av spørsmål som er knyttet til sine egne læringsmål. Dersom man kan bestemme hvilke spørsmål som blir stilt er det ikke urimelig å anta at dette øker kunnskapen mer enn den måten vi har gjennomført det på.

8.1 Kritikk av oppgaven

Det var ingen klar opplæringsplan som lå til grunn for oppgaven. Vi prøvde derfor å kartlegge behovet for opplæring gjennom intervjuene hos oppdragsgiverne. Det ble brukt mye tid på å finne metode, utvikle en intervjuguide, gjennomføre intervjuer og å analysere resultatene. Denne tiden kunne blitt brukt til bedre utvikling av spillet, og testing gjennom utviklingsperioden.

8.2 Fremtidig arbeid

Med prosjektets slutt vil konseptet være ferdigstilt og overlevert til Norsk Tipping og Skatteetaten. Det vil da være opp til dem å tilpasse utforming og elementer i spillet til deres bruk. Norsk Tipping vil hyre en grafisk designer over sommeren, og har snakket om å bruke sluttproduktet i opplæring av nye ansatte samt under nasjonal sikkerhetsmåned i oktober. Skatteetaten ønsker også å benytte spillet i oktober, men har også planer om å benytte spillet i et årshjul for opplæring i informasjonssikkerhet.

Gjennom denne oppgaven har vi sett på om brettspill fungerer til opplæring i informasjonssikkerhet. Det som hadde vært interessant å se er hvor godt denne metoden fungerer i forhold til andre læringsmetoder. Hvordan måler denne læringsmetoden seg mot

E-læring og/eller foredrag. Videre arbeid vil da være å utvikle en opplæringsplan som skal gjennomføres med bruk av brettspillet, E-læring og foredrag. Ha forskjellige grupper som gjennomfører en av de metodene. For å måle dette kan det være gunstig å benytte vår pre- og posttest design sammen med en godt utviklet kunnskapstest, eventuelt også en selvevaluering.

8.2.1 Forbedring av brettspillet

Brettspillet som det er nå har en viss opplæringseffekt. Brettspillet er et godt utgangspunkt for oppdragsgiverne å videreutvikle spørsmål til den opplæringsplanen de har. Her kan de ha forskjellige spørsmål rettet mot forskjellige avdelinger. Det er noen avdelinger som drar mer nytte av å vite om enkelte områder innen informasjonssikkerhet enn andre. Vi anbefaler da oppdragsgiver å lage en opplæringsplan til forskjellige avdelinger som fokuserer på de viktigste områdene for dem. Dersom dette gjøres er det viktig å finne ut av hvilken vanskelighetsgrad spørsmålene burde ha. Det er en utfordrende balanse å finne. Noen liker lette spørsmål, andre liker litt vanskeligere spørsmål. Vi anbefaler å øke vanskelighetsgraden litt på de spørsmålene som ikke er bonusspørsmål.

Dersom oppdragsgiverne ønsker å lage egne spørsmål, anbefaler vi å fokusere på svaralternativene. På grunn av mengden med spørsmål er det mange som varierer i kvalitet. Det er flere spørsmål som har “alle over” svaralternativer. Noen få slike svaralternativer kan fungerer, men det er da viktig at det noen ganger er feil svar.

Det kan være gunstig å senke mengden med tekniske begreper. Det var den tilbakemeldingen vi hørte mest fra deltagerne. Vi anbefaler å inkludere noen tekniske begreper som “Phishing”, “VPN” og “2FA”, men droppe andre tekniske begreper som “Bruteforce”, “Shouldersurfing” og “Tailgating”.

For oppdragsgiverne anbefaler vi å finne en måte å vise spørsmål og alternativer. Dette kan være å vise spørsmålskortene på en skjerm slik at de kan gruble litt over hvilket alternativ som er riktig. Dette kan spare tid og kan gjøre det lettere å huske informasjonen.

8.3 Evaluering av gruppens arbeid

Gruppens arbeid har fungert godt. 3 av medlemmene har jobbet sammen på skolen, og ett medlem har jobbet fra Tyskland. De tre medlemmene som jobbet på skolen har jobbet sammen på prosjekter før og er godt kjent med hverandres arbeidsmetoder. Det har til tider vært utfordrende å holde medlemmet i Tyskland oppdatert til enhver tid, men det har ikke vært et stort problem. Medlemmet i Tyskland har vært med på møter gjennom videosamtaler på Facebook.

Gruppen har klart å overholde tidsfrister som ble fastsatt tidlig i prosjektet. Det har til tider vært mye å gjøre, og til tider mindre å gjøre. Alle medlemmene hadde fag ved siden av som måtte prioriteres i perioder. Det har vært en utfordring å balansere skriving på rapporten og utvikling av brettspillet. Dette er noe som kunne blitt gjort bedre. Under det første møtet med oppdragsgivere kom vi fram til at det er viktig med kommu-

nikasjon mellom partene. Det har blitt sendt ukentlige møtereferater fra gruppemøter til oppdragsgivere. Da har de hatt oversikt over hva som blir gjort og har hatt muligheten til å komme med innspill.

Arbeidsfordelingen har vært en utfordring. Til tider har det vært vanskelig å alltid ha en oppgave som må gjøres. Selv om det alltid er noe som kan gjøres har det vært vanskelig å konkretisere akkurat hva det er. Dette var ikke alltid tilfellet da det i perioder var veldig klart hva som skulle gjøres og når det skulle være ferdig. Ukentlige møter med veiledere har vært til stor hjelp, spesielt i tider der gruppen ikke var helt sikker på hva som måtte gjøres. Til tross for de utfordringene under prosjektet har gruppen klart å levere et produkt de, og oppdragsgiverne, er fornøyd med.

Bibliografi

[1] MK Andfossen A Edvardsen. *E-læring i arbeidslivet: Hvordan lykkes når grunnleggende læringsprin-sipper møter dagens teknologi*. Høyskolen i Kristiania, 2018.

[2] M. Wait M. Frazer. *Investigating retention and workplace implementation of board game learning in employee development*. Pearson, 2018.

[3] D. I. Jacobsen. *Hvordan gjennomføre undersøkelser*. HøyskoleForlaget, 2005.

[4] R. Tamassia M. Goodrich. *Introduction to Computer Security*. Pearson Education Limited, 2014.

[5] Jeanne Ellis Ormrod Paul D. Leedy. *Practical Research, planning and design. Eleventh Edition*. Pearson, 2015.

[6] Deborah J. Rumsey. *Statistics For Dummies 2nd Edition*. John Wiley Sons Inc, 2016.

[7] *Trends in learning Report 2018*. Open University, 2018.

Vedlegg

A Intervjuguide

INTERVJUGUIDE

Introduksjon:

Vi er en gruppe fra NTNU Gjøvik som går siste året på studiet IT drift og informasjonssikkerhet, og i den forbindelse skal vi skrive en bacheloroppgave om brettspillbasert opplæring i informasjonssikkerhet og bevissthet rundt sikkerhetskultur.
Formålet med intervjuet er å få en oversikt hvilke nivå dere ligger på innenfor informasjonssikkerhet, hva som engasjerer dere og hvilke temaer vi trenger å inkludere i spillet for å øke kunnskapen innen informasjonssikkerhet.
Vi ønsker å utvikle et bra opplæringsspill innenfor informasjonssikkerhet og er derfor avhengig av så ærlige svar som mulig, slik at det forhåpentligvis resultere i et bra opplæringsmateriell som gjør at dere kan øke kompetansen innenfor informasjonssikkerhet og digitalisering.
Intervjuet er anonymt, dere vil vær referert til som et nummer i dokumentene.
Intervjuet vil ikke bli tatt opp, bare notert ned av oss. Vi har alle signert bedriftens taushetserklæring.

Generelt

- Hva er ditt navn og hvor lenge har du jobbet her?
- I hvilken avdeling jobber du i?
  - Hvilke hovedarbeidsoppgaver har du?
    - Har arbeidsoppgavene dine stor relevans innen informasjonssikkerhet?
- Synes du det er interessant med informasjonssikkerhet?
  - Synes du det er mye styr i media akkurat nå?
  - Hvis ja, hva er det som interesserer deg, hvor fant du det?

Sikkerhetskultur

- Hvordan opplever du sikkerhetskultur på jobben?
  [Definisjon sikkerhetskultur: handler om atferd knyttet til sikkerhet, for eksempel i forhold til informasjon eller objekter. Sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd.]
- Har du noen tanker rundt sikkerhetsproblemer som arbeidsplassen står ovenfor?
  - Phishing
  - Lite opplæring
  - Sikkerhetskulturen er lav eller dårlig
  - Vanskelig opplæring
  - Trusselbilde/trusler og trender

- **Scenario:** Du har blitt phishet, og det er nå løst. Hadde du følt at det gikk fint å fortelle det til kollegaen/er eller er det sensitivt for deg?

- Har du noen gang opplevd at en kollega har delt erfaringer i forhold til sikkerhetshendelser med deg?
    - Tailgating
    - Phishing
    - Sikkert passord
        - Hvis ja, hvor ofte? Og har dette hjulpet deg å håndtere lignende situasjoner?
        - Hvis nei, hadde du ønsket at slik informasjon var delt mellom dine kollegaer?

- Føler du at det er veldig strengt og at det ikke er akseptabelt å gjøre feil?

Nivå

- Vet du hvordan man blir hacket? Ulike typer angrep?
    - Brute force
    - Lekkede passord
    - Malware
    - Session
    - Cookies
    - Kryptering
    - Eavesdropping
    - Shoulder Surfing
    - To faktor autentisering

- Vet du hva policyen er for bruk av jobbmail og passord?

- Bruker du to-faktor autentisering (2FA) i dag?

- **Scenario:** Du mottar e-post fra en kollega, som har funnet en morsom video. Innholdet er en lenke, hva gjør du?
    - HTTP/HTTPS
    - .php/.html
    - Sjekker linken
    - Hvem er avsenderen?

- Hva er det du legger vekt på når du lager passord?
    - Gjenbruk passord
    - Oppbygning/sammensetning
    - Store, små bokstaver/tall, spesialtegn

- Vet du hvordan man sikrer filer? (Kryptere, lagre, sende - vil helst at de skal gå inn på disse punktene)
    - Kryptere
    - Lagring
    - Sending av informasjon/dokumenter
    - Om du bruker mail, pleier du å kryptere mailen?

        - Hvis ja, hvilken type kryptering bruker du?
- Hvor ofte oppdatere programvaren din?
    - Hvis ja, hva får deg til å oppdatere? Hva oppdaterer du?
        - OS
        - Chrome
        - Adobe
        - Flash
    - Hvis nei, hvorfor ikke? Vet du farene ved å ikke oppdatere programvaren?

- Føler du at restriksjoner på din PC bruker forhindrer deg i arbeidet (PC)?
    - Hvis nei, hva med når du skal laste ned dokumenter eller programvare som du trenger under arbeid?
    - Hvis både ja eller nei, er det noen konsekvenser ved å bruke administrator brukeren til vanlig bruk?

Rutiner

- Har du meldt fra hendelser (angående IT sikkerhet)?
    - Phishing
    - Konto er kompromittert
    - Noen har brutt policy
    - Ulåst PC
    - Passord på skrivebord
    - Tailgating

- Bruker du antivirusprogram (privat/jobbsammenheng)?
    - Hvis ja, hvilket?
        - Føler du deg trygg når du bruker det?
            - Hva tror du det hjelper mot?
    - Hvis nei, hvorfor ikke?
        - Tror du du ville følt deg tryggere hvis du hadde brukt et antivirusprogram?
- Skriver du ned passordene dine?
    - Password manager
    - Text fil på pc / mobil
    - Papirlapp / Post-it

    - Hvis ja, hvordan bruker du passordet eller oppbevarer du det?
    - Hvis nei, hvorfor ikke?

- Er det noen rutiner du ikke er klar over hensikten med?
    - Skru av pcen når man er ferdig på jobb
    - Bruke jobbmail eller samme passord andre plasser
    - Hvorfor dette dokumentet er fortrolig
    - Er det noen policyer som er utydelige?
        - Hvordan eller hvem skal man melde fra til
        - Hvordan man kryptere

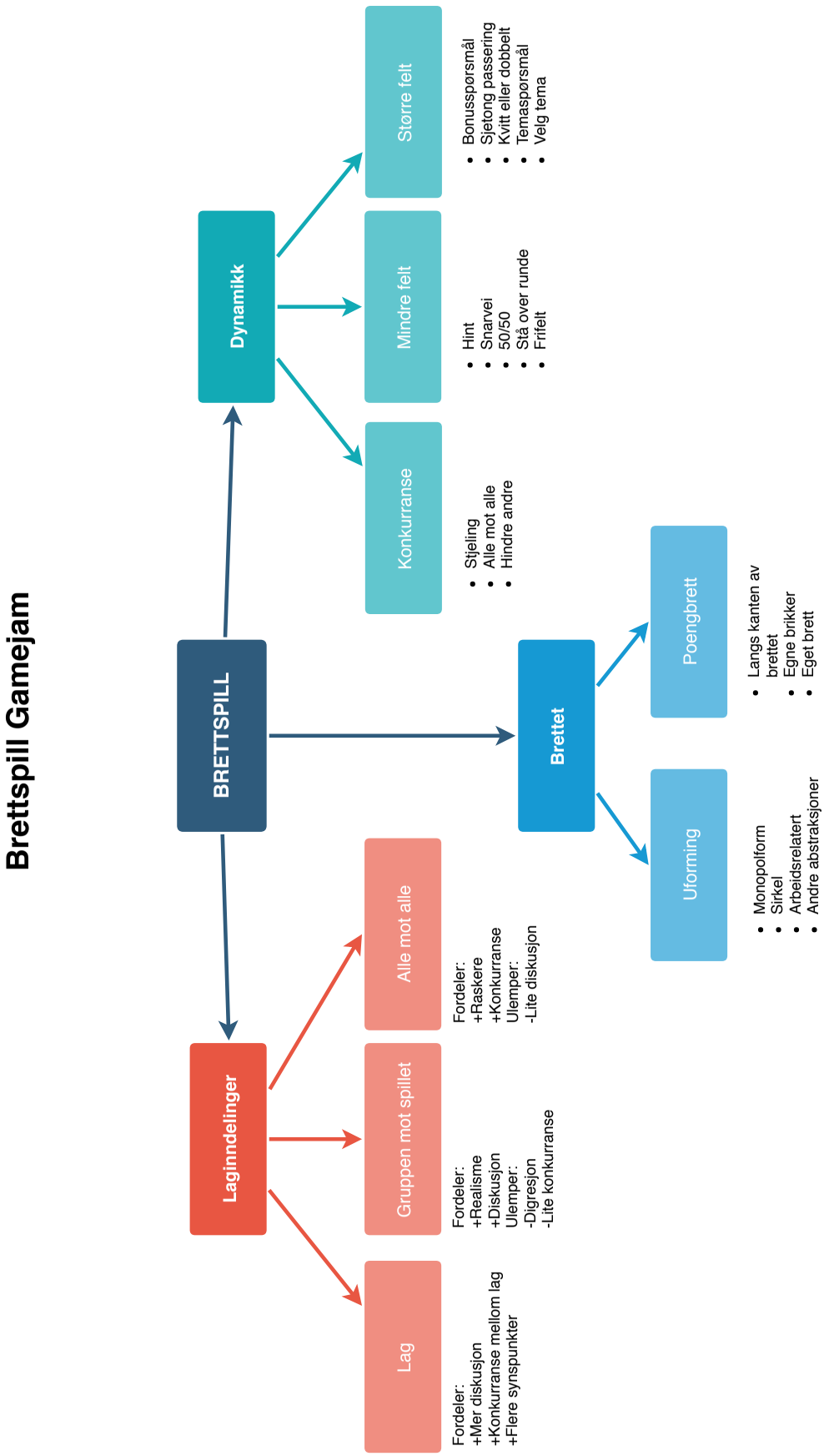
Opplæring

- Hvor ofte får du opplæring i informasjonssikkerhet?
    - Hva lærte du?
    - Kan du fortelle meg mer om det du lærte?
    - Var det vanskelig å forstå?
    - Hvordan lærer du best / hvilken metode fungerte best for deg?
    - Hvis du var ansvarlig for opplæring, hadde du gjort noe endringer?
        - Metode (kahoot/video/bilde)
        - Visuelt, teoretisk, praktisk. Kanskje rangere dem?
        - Temaer du føler trengst mer dybde på
    - Kunne du tenkt deg at brettspill kan være en måte å lære på?
- Lærer du best på egenhånd, eller i grupper?

Spillutvikling

- Når spilte du brettspill sist?
    - Spiller du brettspill ofte?
    - Har du et eller flere favoritt brettspill?
    - Hva er det som engasjere deg når du spiller brettspill?
        - Humor
        - Lagspill
        - Konkurranse
        - Spilldynamikk
        - Kompleksitet
        - Enkelt å forstå
    - Hvor lang tid burde det ta å spille et brettspill?
    - Har brettspillets utseende noen påvirkning i forhold til interessen for og/eller engasjement i spillet?

B Gamejam


Brettspill Gamejam
BRETTSPILL
Dynamikk
Større felt
Bonusspørsmål
Sjetong passering
Kvitt eller dobbelt
Temaspørsmål
Velg tema
Mindre felt
Hint
Snarvei
50/50
Stå over runde
Frifelt
Konkurranse
Stjeling
Alle mot alle
Hindre andre
Laginndelinger
Alle mot alle
Fordeler:
+Raskere
+Konkurranse
Ulemper:
-Lite diskusjon
Gruppen mot spillet
Fordeler:
+Realisme
+Diskusjon
Ulemper:
-Digresjon
-Lite konkurranse
Lag
Fordeler:
+Mer diskusjon
+Konkurranse mellom lag
+Flere synspunkter
Brettet
Poengbrett
Langs kanten av brettet
Egne brikker
Eget brett
Uforming
Monopolform
Sirkel
Arbeidsrelatert
Andre abstraksjoner

C Spilltest

Spilltest

Dato: 03.04.2019
Antall personer: 4
Kommentarer:
2 objekter med bakgrunn innen webdesign, årsstudium.
1 objekt med bakgrunn innen informasjonssikkerhet, første året i bachelor.
1 objekt med bakgrunnen innen programmering, tredje året i bachelor.

Vanskelighetsgrad:

- **Er spørsmålene forståelige?**
- **Er det for lange eller korte?**
- **Er de vanskelige?**
- **Relevante?**

Noen spørsmål er ikke forståelige siden de er ukjent for objektet.
Det oppstod problematikk når objektene fikk lest opp et langt spørsmål med lange svaralternativer.
Game-master kan ha et påvirkende kraft når masteren leser opp svaralternativene og eventuelt ler eller er mer tydelig på noen av alternativene.

Noen av spørsmålene hadde gul alternativ på “alle over”, som gir objektet et syn på at det ikke er rett og at de andre alternativet er det rette. Andre spørsmål var litt vage, en ny gjennomgang av spørsmålene er viktig og skal bli gjort.

Brukervennlighet:

- **Effektivitet (gjør brukeren de rette tingene?)**
- **Effektivitet (hvor lang tid brukeren bruker for å utføre oppgavene)**
- **Tilfredshet (vurdering fra bruker)**

Brukerne utfører spillet rett, reglene er enkle å forstå.

Brettet er enkelt og selvbeskrivende, forståelig at de går gjennom forskjellige soner.

Spørsmålene ble besvart i tide (mellom 30 og 60 sekunder), men spørsmål som var lange eller vanskelige resulterte i at det varte lenge. Dette frembringer ikke noe problematikk for spillet eller for andre deltagere.

Man la merke til at objektene konkurrerte med hverandre, men objektene som ble frastjålet spørsmålene ble litt irritert. Denne irritasjonen observeres som en god irritasjon som fremmer at objektet ønsker hevn og vil bruke sjetongen mer.

Observasjoner:

- **Ting som ikke står ovanfor som er viktig å dokumentere**

Det ble lagt merke til at etter den andre runden så begynte det ene objektet å bruke stjele sjetongen. Dette skapte en slags dominoeffekt, andre objekter begynte å bruke sjetongen også.

Noen spørsmål som var vanskelige eller som ble besvart feil på resulterte at noen andre konkurrenter hjalp å diskutere og forklare hvorfor det var feil og hvorfor det andre alternativet var rett. Alle var med på diskusjonen.

Spillet skulle vare i 45 minutter, men siden det var et stort engasjement og konkurranse i spillet endte vi på 55 minutter.

En mulighet hadde vært å hatt minuspoeng ved FFA, slik at det ikke blir misbrukt.

Tilbakemeldinger:

- **Hva syns objektene om spillet?**
- **Fritt for tilbakemeldinger**

Objektene syns det var et godt spill. De som ikke hadde bakgrunn i sikkerhet følte de fikk spørsmål de kunne svare på, noe de ikke tenkte ville skje når de visste at spillet hadde fokus på sikkerhet.
Det ene objektet mente at man burde få noe belønning for å svare rett, enn å bare få skrevet opp poenget sitt på et ark.
De ønsket at spørsmålene kunne bli delt ut til objektet eller vist opp på en skjerm slik at de ikke misforstår eller ber om repetisjon på spørsmålene eller alternativene.
En objektet som ble frastjålet spørsmål hyppig, nevnte at det ble kjedelig å bli fratatt en runde. Et innspill ble lagt frem at det kunne være mer “Free for all” felter slik at objektet kunne være med.
Et annet forslag som ble lagt frem er at man kunne bare stjele om objektet mente at det andre objektet svarte feil på et alternativ. Med andre ord, svare etter objektet har angitt sitt angivelige feil svar.
De mente de lærte mye som var relevant til dem, men et annet forslag var at vi kunne ha en siste runde der vi gikk gjennom spørsmål som ble besvart feil på eller som objektene brukte lang tid på.
Minus poeng om man stjeler også et forslag, som kunne hindre sabotering.

D Oppskrift spørreundersøkelse

Notater fra boken Practical research, planning and design Side 166 - 170, spørreundersøkelser

1. Hold det kort
    1.1. Spørsmålene burde være så korte som mulig og bare formidle informasjon som er viktig i forhold til hva som skal undersøkes. Dette gjøres ved å stille seg 2 spørsmål: "Hva planlegger jeg å gjøre med informasjonen jeg spør om?" og "Er det absolutt nødvendig å ha denne informasjonen til å løse en del av forskningsspørsmålene?"
2. Hold respondentens oppgave enkel og konkret
    2.1. Gjør det så enkelt å lese og svare som mulig. Det er mer sannsynlig at folk svarer på undersøkelsen dersom de oppfatter det som raskt og enkelt å gjennomføre.
    2.2. Åpne spørsmål tar tid for de som utfører undersøkelsen og for de som skal tolke svarene. Det vil også variere veldig på hvor mye/lite folk velger å dele i disse spørsmålene.
3. Gi enkle, spesifikke instruksjoner
    3.1. Formidle akkurat hvordan du vil respondenten skal svare. Ikke tro at de er kjent med Likert skala.
4. Bruk enkel, klar og entydig språk
    4.1. Skriv spørsmål som kommuniserer akkurat hva du vil vite. Unngå å bruke terminologi som respondenten ikke forstår. Unngå ord som "vanligvis" og "flere"
5. Gi en begrunnelse til hvorfor man ønsker svar på noe som kan virke uklart
    5.1. Gi respondenten en begrunnelse for hvorfor det er viktig å gjennomføre svare på spørsmålene. Hvert spørsmål burde ha en begrunnelse til hvorfor vi ønsker å ha svar på dette.
6. Sjekk etter unødvendige implisitte forutsetninger i spørsmålene
    6.1. For eksempel spørsmålet: "Hvor mange sigaretter røyker du om dagen". Her impliserer man at respondenten røyker selv om det er mulig å svare ingen. Spørsmålet burde heller formuleres på denne måten: "Røyker du sigarettet?". Svarer man ja går man til neste spørsmål, svarer man nei hopper man over neste spørsmål, eventuelt hoppe frem til spørsmål X.
7. Ordlegg spørsmålene på en måte som ikke gir føringer til det rette eller foretrukne svaret
8. Fastslå hvordan svarene skal tolkes før undersøkelsen blir sendt ut
    8.1. Ha en plan for hvordan svarene kan gjøres om til tallverdier så det er mulig å gjøre statistisk analyse.
9. Sjekk for konsistens
    9.1. Unngå å ha spørsmål som kan motsi hverandre. Unngå ha ha 2 spørsmål som skal finne ut om det samme. Det kan oppstå at de to svarene ikke stemmer med hverandre.
10. Ha en pilot-test for å fastslå validiteten til spørsmålene
    10.1. Det er viktig å se om spørsmålene er klare og de klarer å formidle den ønskede informasjonen. De som utfører pilot-testen burde hvertfall svare på spørsmålene.

En bedre måte å gjøre dette på er å stille spørsmål til respondenten gjennom utføringen av undersøkelsen. Spørsmål som: "Les spørsmålet høyt", "Hvilken informasjon vil dette spørsmålet ha fra deg?", "Hvilket svar er mest riktig for deg på dette spørsmålet?", "Kan du forklare hvorfor du valgte det svaret?". Gjennom å stille slike spørsmål er det lett å se hvilke type svar man kan få. Dersom undersøkelsen inkluderer begge kjønn og forskjellig religiøs/kulturell bakgrunn, burde pilot-testen inneholde respondenter fra forskjellig kjønn og "bakgrunn".

10.2. Å gjennomføre en pilot-test er et steg i riktig retning for å fastslå validiteten, altså at den måler det den faktisk skal måle.

11. Granske det nesten ferdige produktet en gang til og vær sikker på at det oppnår behovene våre.

11.1. Her må man gå gjennom gang på gang, spørsmål for spørsmål, og se om spørsmålene gir svar på det vi vil ha svar på. Et tips for å gjennomføre dette er å ha en tabell til hvert spørsmål som inneholder følgende:

Skriv spørsmålet under	Hvorfor stiller vi dette spørsmålet? Hvilken sammenheng har det til forskningsspørsmålene?
…..	…..

12. Utforme spørreundersøkelsen så den ser attraktiv og profesjonell ut.

12.1. Undersøkelsen burde være bra printet, ikke noen skrivefeil, og kanskje to eller flere farger. Det burde understrekes at vi som gjennomfører undersøkelsen er profesjonelle og at vi setter stor pris på at respondentene deltar.

E Selvevaluering

Selvevaluering - etter

Deltagernummer:

I denne undersøkelsen skal du selv vurdere hvor enig/uenig du er i de forskjellige påstandene.
Du kan bare krysse av for ett alternativ per påstand.

Brettspill fungerer godt til opplæring i informasjonssikkerhet.

- ❑ Veldig uenig
- ❑ Uenig
- ❑ Litt uenig
- ❑ Litt enig
- ❑ Enig
- ❑ Veldig enig

Jeg har tilstrekkelig med kunnskap innen informasjonssikkerhet

- ❑ Veldig uenig
- ❑ Uenig
- ❑ Litt uenig
- ❑ Litt enig
- ❑ Enig
- ❑ Veldig enig

Sikkerheten på arbeidsplassen er sikkerhetsavdelingen sitt ansvar

- ❑ Veldig uenig
- ❑ Uenig
- ❑ Litt uenig
- ❑ Litt enig
- ❑ Enig
- ❑ Veldig enig

(Fortsetter på neste side)

Sikkerhet er relevant for arbeidet mitt

- ❏ Veldig uenig
- ❏ Uenig
- ❏ Litt uenig
- ❏ Litt enig
- ❏ Enig
- ❏ Veldig enig

Har du noen kommentarer/tilbakemeldinger til spillet eller gjennomførelsen av testen?

F Kunnskapstest

NTNU

Ferdighetstest

I denne ferdighetstesten skal vi teste kunnskapen din i informasjonssikkerhet. Spørsmålene her varierer fra hverandre, følg instruksjonene på hvordan de skal besvares. Noen oppgaver kan ha felt der vi ønsker en begrunnelse til svaret du har gitt (en kort setning eller stikkord holder).

Flervalgsoppgaver: Det er bare ett svar per spørsmål som er riktig. Kryss av for det alternativet du velger.

Hva er den største sikkerhetssårbarheten ved å ikke oppdatere programvare?

- ❑ Mangel på funksjonalitet
- ❑ PCen mister ytelse
- ❑ Feil blir ikke fikset
- ❑ Databasen blir ikke oppdatert

Hvilket passord er det sikreste?

- ❑ #U*2#o6&rw
- ❑ laH4FY#v2Ar!g@j
- ❑ AbrahamPihlsVeg5
- ❑ HeiBilMosjonLuftballongBolle

Hvorfor valgte du det alternativet?

Hvilken link er mest sannsynlig ondsinnet?

- ❑ https://www.youtube.com/watch?v=dQw4w9WgXcQ
- ❑ https://reclamus.com/9uj8n76b5.exe
- ❑ https://helpx.adobe.com/acrobat/kb/link-html-pdf-page-acrobat.html
- ❑ https://www.google.com/search?q=am+i+malicious%

Hvorfor valgte du det alternativet?

1

Hvilket alternativ øker sikkerheten på epostkontoen din mest?

- ❏ HTTP
- ❏ Antivirus
- ❏ Backup
- ❏ 2-faktor-autentisering

Hvilket alternativ er best for å sikre din USB-minnebrikke mot skadevare?

- ❏ Bare bruk den når du er alene
- ❏ Ikke koble den til en Bluetooth enhet
- ❏ Bruk en brannmur (Firewall) program
- ❏ Ikke forlat den uten tilsyn

Hvilken påstand beskriver hvorfor det er viktig å oppdatere antivirusprogram regelmessig?

- ❏ For å beskytte PCen fra alle kjente skadevarer
- ❏ For å sikre at programvaren klarer å identifisere eldre skadevare
- ❏ For å beskytte PCen fra spam
- ❏ For å forhindre spredning av ondsinnede programmer på internett

Hvilken av de følgende påstandene er riktig for hvorfor man skal låse PCen når man forlater den?

- ❏ For å forhindre uautorisert adgang
- ❏ For å begrense strømbruk
- ❏ For å forhindre at data blir korrupt
- ❏ For å forhindre PCen fra å bli defekt

(Fortsetter på neste side)

Påstand: Kryss av for det alternativet du er mest enig med.

Jeg føler meg trygg når jeg er logget på nettverket til en internett cafè uten ekstra sikkerhetstiltak.

- ❏ Helt enig
- ❏ Litt enig
- ❏ Nøytral
- ❏ Litt uenig
- ❏ Helt uenig

Åpent spørsmål: Dette er fritekstspørsmål. Svar så godt du klarer med den kunnskapen du har. Det er tilstrekkelig å bare skrive nøkkelord.

Hvordan kan man sikre seg på offentlige nettverk?

Kryss av for de alternativene du tror er riktige: En eller flere av alternativene er riktige.

Hvilke av alternativene er skadevare?

- ❏ Phishing
- ❏ Virus
- ❏ HTTPS
- ❏ Dataorm
- ❏ URL-padding
- ❏ Bruteforce
- ❏ Rootkit

Ranger alternativene: Her skal du rangere alternativene. Alle alternativene skal ha en rangering. 1 utgjør den største risikoen, 2 utgjør nest største risiko, osv., helt ned til 7 som er den minste risikoen.

Hva utgjør de største risikoene på internett?

___ Logge på nettbanken

___ Laste ned en film fra en ulovlig nettside

___ Trykke på en link som kommer fra youtube

___ Laste ned utvidelser til nettleseren fra Chrome Web Store

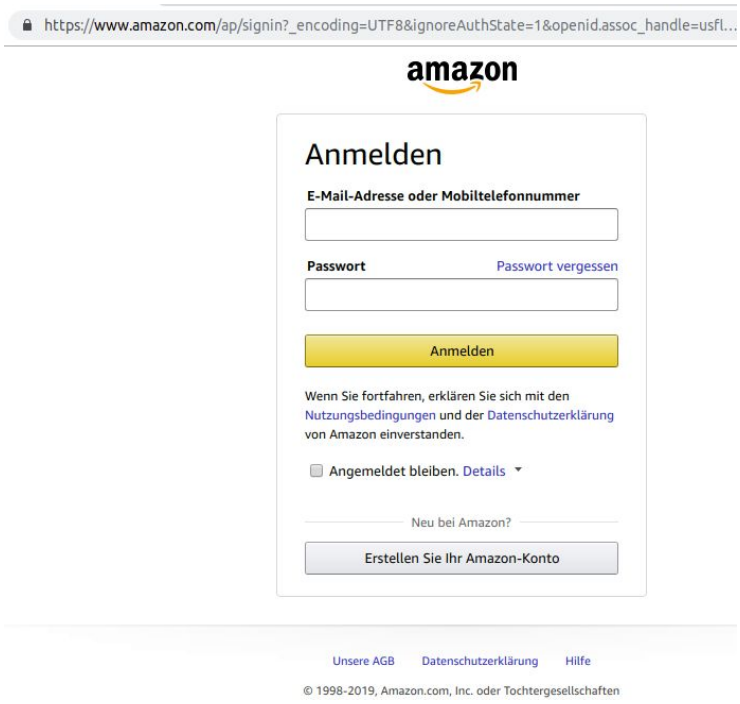
___ Lagre kortinformasjonen din på amazon.com

___ Være tilkoblet et offentlig nettverk uten ekstra sikkerhetsmekanismer

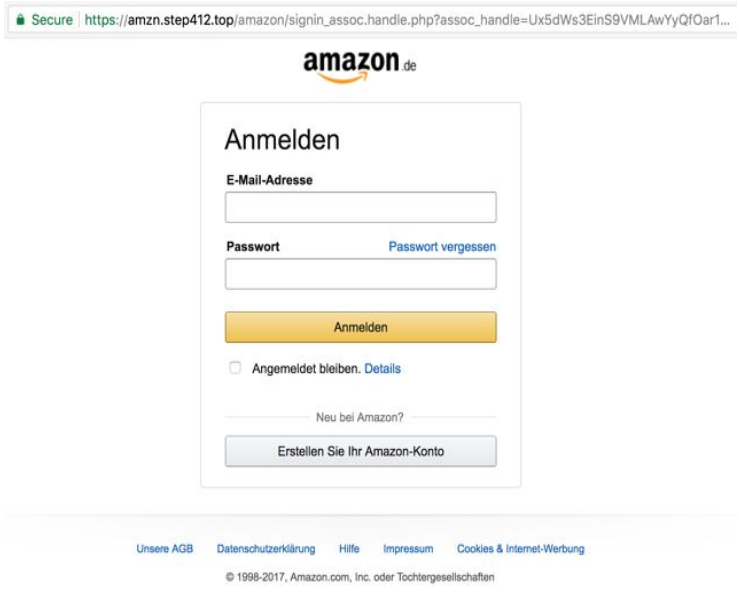
___ Logge inn på en nettside som begynner med http://

Hvilken side er ondsinnet?

A) ---------->



B) ---------->



C) Ingen av alternativene

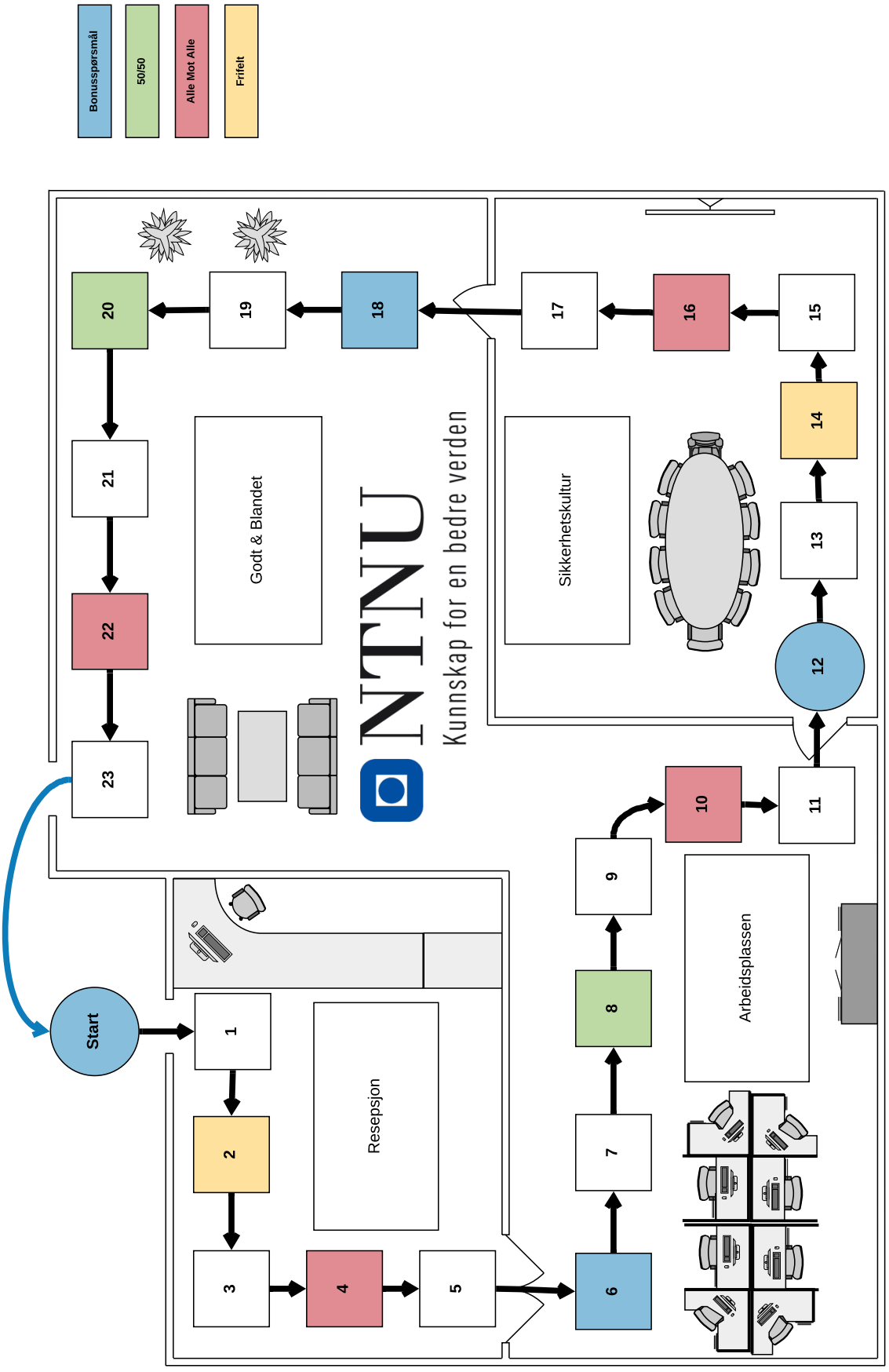
Hvorfor valgte du det alternativet?

G Poeng for kunnskapstest

Kandidat nr.	Organisasjon	Før/etter	Spørsmål 1	Spørsmål 2	Spørsmål 3	Spørsmål 4	Spørsmål 5	Spørsmål 6	Spørsmål 7	Spørsmål 8	Spørsmål 9	Spørsmål 10	Spørsmål 11	Spørsmål 12	Sum individ:
1	Skatteetaten	Før	0	0	1	1	0	1	1	1	0	0.33	0.33	1	6.66
2	Skatteetaten	Før	1	0	0	0	0	1	1	1	0.15	0	0.66	1	5.81
3	Skatteetaten	Før	1	0	1	0	0	1	1	1	0	0	0.66	0	5.66
4	Skatteetaten	Før	1	0	1	1	0	1	1	1	0	0.33	1	0	7.33
5	Skatteetaten	Før	1	0	1	1	0	1	1	1	0.15	0.33	0.66	0	7.14
6	Skatteetaten	Før	0	0	1	0	1	1	1	0	0	0	0.66	0	4.66
7	Skatteetaten	Før	1	1	1	1	0	1	1	1	0.1	0.33	0.66	0	8.09
8	Skatteetaten	Før	0	0	0	1	0	0	1	1	0	0.33	0.33	1	4.66
9	Norsk Tipping	Før	1	0	1	1	0	1	1	1	0	0.33	0.66	1	7.99
10	Norsk Tipping	Før	0	1	1	1	1	1	1	1	0	0	0.66	1	8.66
11	Norsk Tipping	Før	1	0	1	0	0	1	1	0	0.15	0	0.66	1	5.81
12	Norsk Tipping	Før	0	0	1	0	1	1	1	1	0	0.33	1	0	6.33
13	Norsk Tipping	Før	0	1	1	1	0	1	1	1	0.15	0	0.66	1	7.81
14	Norsk Tipping	Før	0	0	1	1	0	0	1	0	0	0	0.66	1	4.66
15	Norsk Tipping	Før	0	0	0	1	0	0	1	1	0.15	0.33	0.66	1	5.14
16	Norsk Tipping	Før	1	0	0	1	0	0	1	0	0.1	0.33	0.66	1	5.09
		Sum spørsmål:	8	3	12	11	3	12	16	12	0.95	2.97	10.58	10	101.5

Kandidat nr.	Organisasjon	Før/etter	Spørsmål 1	Spørsmål 2	Spørsmål 3	Spørsmål 4	Spørsmål 5	Spørsmål 6	Spørsmål 7	Spørsmål 8	Spørsmål 9	Spørsmål 10	Spørsmål 11	Spørsmål 12	Sum individ:
21	Skatteetaten	Etter	0	0	0	1	0	1	1	0	0	0.33	0.66	1	4.99
22	Skatteetaten	Etter	1	0	1	0	0	1	1	1	0	0.66	0.66	1	7.32
23	Skatteetaten	Etter	0	1	0	0	0	1	1	0	0	0	0.33	1	4.33
24	Skatteetaten	Etter	1	0	1	1	0	1	1	1	0.5	0.66	1	1	9.16
25	Skatteetaten	Etter	1	1	1	1	1	1	1	1	0.6	0.66	1	1	11.26
26	Skatteetaten	Etter	1	1	1	1	0	1	1	1	0	0.33	0.66	0	7.99
27	Skatteetaten	Etter	1	1	0	1	0	0	1	1	0.15	0.33	1	1	7.48
28	Skatteetaten	Etter	0	1	1	1	0	1	1	1	0	0.33	0.33	1	7.66
29	Norsk Tipping	Etter	0	0	1	1	0	1	1	0	0.1	0.33	0.66	1	6.09
30	Norsk Tipping	Etter	0	0	0	1	0	1	1	1	0.15	0	0.66	0	4.81
31	Norsk Tipping	Etter	1	0	1	0	1	1	1	1	0.2	0.66	0.66	0	7.52
32	Norsk Tipping	Etter	1	0	1	0	0	1	1	0	0	0.33	0.66	0	4.99
33	Norsk Tipping	Etter	1	0	1	1	1	1	1	1	0	0.33	0.66	1	8.99
34	Norsk Tipping	Etter	1	1	1	1	0	1	1	1	0	0.66	1	1	9.66
35	Norsk Tipping	Etter	1	1	1	1	0	1	1	1	0.5	0.33	0.66	0	8.49
36	Norsk Tipping	Etter	1	1	1	0	0	1	1	1	0.5	0.66	1	0	8.16
37	Norsk Tipping	Etter	1	1	1	1	1	1	1	1	0.5	0.33	0.33	1	10.16
		Sum spørsmål:	12	9	13	12	4	16	17	13	3.2	6.93	11.93	11	129.06

H Brettspill og spørsmålskort



16

En som skal levere varer ser stresset ut og vil komme inn, hva gjør du?

A) Han er åpenbart stresset, så du slepper han inn

B) Ikke slippe personen inn

C) Slepper han inn men følger med på han

D) Han har på seg klær fra tjenesten, og slipper han inn

15

Hva er “tailgaiting” ?

A) Er når noen går tett inntil deg på gata

B) Når noen går inn uten adgangskort

C) Når noen sniker seg med inn igjennom en sikret dør/inngang

D) Du følger noen tett for å sjekke om de bruker adgangskortet riktig

14

Hvilken av disse alternativene er en form for sosial manipulering?

A) Spamming

B) Fly fishing

C) Shoulder surfing

D) Tail surfing

13

Sosial manipulering er når...

A) Når noen deltar i et prosjekt om sosiale medier

B) Noen aksesserer en fil med et "stjålet" passord

C) Noen utnytter normal menneskelig oppførsel til å innhente informasjon

D) Alle over

12

Når du bruker adgangskortet på vei inn kommer en person etter deg, hva gjør du?

A) Be personen benytte sitt eget adgangskort

B) Anta at personen jobber her

C) Holder døren åpen for dem

D) Regner med at personen etter deg stopper personen

11

Når du benytter et offentlig Wi-Fi nettverk så bør du:

A) Føle deg trygg og sikker

B) Taste inn ditt kredittkortnummer

C) Verifisere navnet på Wi-Fi nettverket med firmaet du besøker

D) Sende e-poster med sensitiv informasjon

10

Hvilket er et faresignal med tanke på sosial manipulering?

A) Noen som svarer vagt på spørsmål

B) Noen som spør etter ditt passord på telefon eller i en e-post

C) Noen som sier at det haster eller presser deg til å handle raskt

D) Alle punktene over

17

Hva bør du passe på dersom du bruker en PC på en nettkafe?

A) Det er ikke lov å bruke offentlig PC

B) Ikke legge igjen sensitiv informasjon

C) Ikke slette noen filer

D) Alle over

8

Hvordan beskytter VPN deg når du er logget på et åpent WI-FI?

A) Kommunikasjonen blir kryptert

B) Den styrker passordene dine

C) Den krever passord for å koble seg på nettet

D) Alle over

7

Hvordan kan man best beskytte seg når man er logget på et åpent WI-FI?

- A) Sterke passord
- B) Backup av systemet
- C) Ikke trykke på noen linker
- D) VPN

6

Hva er en risiko ved å bruke åpen WI-FI?

- A) Det er ingen risiko ved dette
- B) Det påløper skjulte kostnader
- C) Andre kan se hva du gjør på nettverket
- D) Alle over

5

Hva er en måte å forsvare seg mot innsideangrep?

- A) Antivirus
- B) Ikke koble seg på nettet
- C) Gi minst mulig tilganger til ansatte
- D) Det er umulig

4

Hva burde man gjøre om man legger merke til en person uten adgangskort?

- A) Det er ansvaret til vakten eller resepsjonen.
- B) Be personen skaffe seg nytt adgangskort
- C) Se stygt på personen
- D) Stoppe personen og be om adgangskort

24

Om en person oppdager at man har rettigheter til programvare man ikke burde ha tilgang til, hva er best å gjøre?

- A) Sikkerhetsavdeling tar seg av dette
- B) Ingenting
- C) Melde fra
- D) Teste ut programvaren

23

Hvilke av disse angrepene skjer mest?

- A) Phishing
- B) Ransomware
- C) USB - hacking
- D) Bruteforce

1

Hvorfor sier policy at man skal skru av PCen når man er ferdig på jobb?

- A) Mindre prosessorbruk
- B) Strømsparing
- C) Du kan ikke hackes
- D) PCen oppdateres

18

Hvorfor kan det være farlig å koble seg på jobbnettverket med privat IT-utstyr?

- A) Sikkerhetsavdelingen tar ned nettverket
- B) Nettet går saktere
- C) Passordet til nettverket kommer på avveie
- D) Det kan inneholde virus

1

Hvem har ansvaret for sikkerheten i organisasjonen?

- A) Du
- B) Sikkerhetsavdelingen
- C) Lederen
- D) Alle over

2

Om det er noe du ikke ser hensikten i å gjøre bak en rutine, hva skal du gjøre?

- A) Fortsette som før
- B) Melde fra til lederen
- C) Gjøre det du tror er riktig
- D) Spør kollega

3

Hvordan kan du forbedre sikkerhetskulturen i en organisasjon?

- A) Kreve sterke passord
- B) Leie inn konsulenter som forbedrer kulturen
- C) Dele informasjon med andre
- D) Alle over

5

Hvordan kan man oppnå bedre opplæring innen sikkerhet?

- A) Tilbakemelding til ledelsen
- B) Sjekke statistikk på kurs-gjennomføring
- C) Ha sterke passord
- D) Alle over

6

Hvilke av disse er viktige områder innen sikkerhetskultur?

- A) Ledelse og utvikling
- B) Rettferdighetskultur
- C) Læring
- D) Alle over

10

Hvorfor bør man være kritisk med hva man deler på internett?

- A) Ikke så farlig, man har ytringsfrihet
- B) Informasjonen kan brukes til å lure deg eller andre
- C) Det er ikke sikkert alle liker det du deler
- D) Informasjonen kan oppfattes som krenkende

11

Hva er den sikreste formen for autentisering?

- A) Noe du vet
- B) Noe du er
- C) Noe du har
- D) Alle over kombinert

12

Hva er faren ved å bruke samme passord flere steder?

- A) Det øker sjansen for phishing angrep
- B) Det er ingen risiko
- C) Blir passordet knekt/lekket kan det bli brukt flere steder
- D) Det er mer sårbart mot passord gjetting

13

Hva er trusselen ved å bruke IoT (Internet of Things) gjenstander?

- A) De har sjeldent fokus på sikkerhet
- B) De bruker mye internett
- C) De tar mye plass
- D) Alle over

15

Hva kan du gjøre for å få IoT gjenstander sikrere å bruke?

- A) Endre standardpassorder
- B) Koble de på et separert nettverk
- C) Konfigurere personvernsinstillinger
- D) Alle over

16

Hvorfor bør du alltid bruke "logg ut" funksjonen når du skal logge av tjenester?

- A) Da blir sesjonen gyldig
- B) Da kan ingen få tak i passordet
- C) Slik at ingen andre kan bruke kontoen din
- D) Alle over

17

Hva er spear-phishing?

- A) Et phishingangrep inni et annet angrep
- B) Det er det samme som ransomware
- C) En måte å fiske på
- D) Et målrettet phishingangrep

18

Hvordan kan angripere finne informasjon til et målrettet phishingangrep?

- A) Sosiale medier
- B) Sosial manipulering
- C) Spionere på deg
- D) Alle over

19

Hvem er hackerne?

- A) Snille dataeksperter
- B) Slemme dataeksperter
- C) Snille og slemme dataeksperter
- D) Kina

20

Hva står forkortelsen 2FA for?

- A) 2 fakta autorisasjon
- B) Second factor autorisation
- C) To-faktor autentisering
- D) Andre faktorer for autentisering

21

Hvor mange av kontoene dine burde ha samme passord?

- A) To eller færre
- B) Ingen
- C) De burde alle ha samme passord slik at man ikke glemmer dem
- D) Fire eller færre

22

Hvilken faktor i passordet er det forskere er enige om at er det mest viktigste mot gjetting av passord?

- A) Kompleksitet (store/små bokstaver, tall & spesialtegn)
- B) Lett å huske
- C) Lengde
- D) Svigerinnen til din mors onkel sitt mellomnavn

23

Hvorfor ønsker bedrifter at de ansatte skal ha lange og komplekse passord?

- A) Vanskeligere å gjette
- B) Vanskeligere for brukere å logge på
- C) Vanskeligere å huske det
- D) Enklere for brukeren å dekryptere passordet

1

Hvilket utsagn er rett når det gjelder hvem som har ansvaret for data i en bedrift?

- A) Alle som bruker dataene
- B) Kunden
- C) Sikkerhetsavdelingen
- D) GDPR ansvarlige

2

Om en kollega finner ut hva passordet ditt er, hva er smart å gjøre?

- A) Kollegaen har taushetsplikt
- B) Skifte passordet
- C) Spør kollegaen om passordtips
- D) Ignorer det

5

Hva gjelder når du skal koble en privat enhet på jobbnettverket?

- A) Kun 2 private enheter er tillatt
- B) Bruke nettverkskabel når man skal koble seg på
- C) Ikke bruke private enheter
- D) Spør IT-avdelingen om hjelp

6

Hvordan kan en angriper lett sende en falsk e-post og utgi seg som deg?

- A) Må ha brukernavn og passord
- B) Må hacke tjenesten
- C) Putte en falsk E-post i navnfelt
- D) Må ha tilgang til PCen din

8

Du får tilsendt brukernavn og passord fra en kollega for å sende en mail fra brukeren hans, hva burde du gjøre?

- A) Sende mailen
- B) Finne på en unnskyldning og ikke gjøre det
- C) Avviser det og nevner at det er i mot policyen
- D) Ignorere det

9

Hva er forskjellen på HTTP og HTTPS?

- A) HTTP gir deg internett
- B) HTTPS er kryptert
- C) HTTPS er raskere
- D) HTTP er tryggere

10

Hva er en måte å se hvor en hyperlink går?

- A) Kopiere linkadressen og lime inn i et dokument
- B) Trykke på F12 og finne linken
- C) Holde musen over og se hvor den tar deg
- D) Alle over

11

Hva er to-faktor-autentisering?

- A) Det er en ekstra autentisering for å sikre kontoen din
- B) Det er en type sikkerhetsspørsmål som "gatenavn der jeg vokste opp"
- C) Det er et annet ord for tilbakestill passordet
- D) Alle over

12

Hva bør du passe på ersom du bruker en PC som ikke er din?

- A) Det er ikke lov å bruke noen andre sin PC
- B) Sende en tullemail til alle i avdelingen
- C) Ikke se på dokumentene deres
- D) Alle over

13

Hva heter fenomenet der noen ser på hva du gjør uten at du er oppmerksom på det?

- A) Bakhodetitting
- B) Drive-by-titting
- C) Skuldertitting
- D) Overwatching

14

Hva er en fare ved shouldersurfing/skuldertitting?

- A) Personen kan se sensitive bilder
- B) Det er en fare for fysisk skade
- C) Det er lett å skremme personen
- D) Personen kan se passord/pinkode

15

Hva er utfordringen med forkortede lenker?

- A) De inneholder skadevare
- B) Man mister passordet sitt ved å trykke på de
- C) Det er vanskelig å se hvor de tar deg
- D) Alle over

17

Hvor finner du firmaets domene i en e-postadresse?

- A) Etter @ tegnet
- B) før @ tegnet
- C) etter "." tegnet
- D) Kan stå både før og etter @ tegnet

18

Du får en mail fra netflix om en ny serie du har lyst til å se, hva kan du fjøre for å garantere sikkerheten?

- A) Selv gå inn på netflix og finne frem
- B) Holde inne CTRL knappen når man klikker på linken
- C) Be en kollega klikke på linken
- D) Åpne linken i sikkermodus

19

Du finner en ukjent minnepenn på kontoret. Hva vil være best å gjøre?

- A) Koble den til en PC og slette alle filene
- B) Koble den til en PC i sikkermodus, og formatere den
- C) La være å koble den til noen PC
- D) Koble den til en PC for å se hvem som eier den

20

Hva er malware?

- A) Skade på en vare
- B) Skadelig programvare
- C) Antivirusprogram
- D) Varer du finner i butikken

21

Hva bør du gjøre hvis du mottar en e-post med et vedlegg fra en ukjent avsender?

- A) Kontakt IT-avdelingen
- B) Lagre vedlegget på PCen og åpne det
- C) Åpne det
- D) Videresende til en kollega for å sjekke

22

Når det gjelder oppbevaring av passord så bør du:

- A) Skrive de ned på en post-it lapp
- B) Lagre de i en excel fil
- C) Oppbevare de utilgjengelig for andre
- D) Dele de med venner og familie medlemmer

10

Hva er fordelen ved å kryptere mobilen?

A) Det gjør at man får plass til mer på mobilen

B) Det gjør at mobilen går raskere

C) Mister man mobilen vil ingen ha tilgang til innholdet

D) Alle over

11

Hvorfor bør man ikke la nettsider lagre kortinformasjonen din?

A) De kan benytte seg av kortet selv

B) Det er ikke så farlig å la nettsider lagre informasjonen

C) Fordi kortinformasjonen blir delt med alle

D) Hvordan informasjonen oppbevares varierer

12

Hva bør du være oppmerksom på når du betaler på nett?

A) At nettsiden har gyldig sertifikat

B) Tilkoblingen er HTTPS

C) Ikke være tilkoblet et offentlig nettverk

D) Alle over

13

Hva bør man være oppmerksom på når man laster ned utvidelser til nettleseren?

A) At du ikke laster ned feil program

B) Bare laste ned fra legitime steder

C) Å laste ned Adblock først

D) Ikke gi fra deg passordene dine

14

Hva må du være oppmerksom på når du skal installere en sikker app?

A) At du har nok lagringsplass

B) At appen har riktig ikon

C) Ikke laste ned fra en tredjepart

D) Alle over

15

For å sikre mobilen er det best å...

A) Ikke laste ned for mange apper på mobilen

B) Bruke den minst mulig

C) Gi minst mulig rettigheter til apper

D) Alle over

16

Du benytter mobilen til netthandel, hva er sikkert?

A) Bør bare utføres med mobildata

B) Sjekk at nettstedet er anerkjent

C) Sjekke om siden benytter https

D) Alle ovenfor

17

Velg ut den påstanden som utgjør den største risikoen:

A) Installere iPhone programvareoppdatering

B) Koble til en ukjent USB til pcen din

C) Last ned en høyt rangert app fra Google Play Store

D) Koble til en kjent USB til pcen din

18

Velg ut den påstanden som utgjør den største risikoen:

A) Se etter sko å kjøpe på boozt.com

B) Koble din eksterne harddisk til pc'n

C) Klikke på "Du vant!" pop-up

D) Klikke på "oppdatere og start på nytt" på windows pc

19

Velg ut den påstanden som utgjør den største risikoen:

- A) Laste ned en kindle e-bok fra amazon
- B) Hoppe over Mac OS programvareoppdatering
- C) Følge med din venn's flytur via flightradar24.com
- D) Søke etter windows update på pc

20

Velg ut den påstanden som utgjør den største risikoen:

- A) Klikke på en e-post link for å verifisere din bankkonto
- B) Ta backup på filene dine i DropBox
- C) Leie en film på iTunes
- D) Legge inn kode på autentiserings appen din

21

Velg ut den påstanden som utgjør den største risikoen:

- A) Gå direkte til en nettside i stedet for å klikke på tilsendt e-post link
- B) Bruke en programvare brannmur
- C) Laste ned en film fra en torrent nettside
- D) Laste ned en film fra Viaplay

22

Hvilken av disse alternativene er en dårlig løsning?

- A) Benytte en passord manager for å lagre alle dine passord
- B) Lage nye, unike passord når dine gamle passord må byttes ut
- C) Dele passordet ditt med nære venner
- D) Alle over

28

Hvor blir passord lagret når nettleser lagrer passordene dine?

- A) Lokalt i nettleser
- B) På server hos nettleser leverandøren
- C) Lagres i skyen
- D) Lagres hos nettstedet

29

Hvilke av disse enhetene kan **ikke** bli infisert med skadevare?

- A) Android enhet
- B) Apple enheter
- C) Smartkjøleskapet
- D) Ingen av de over

25

Hva vil det si at en side kommer høyt i et google søk, utenom annonser?

- A) Siden er sikker
- B) Siden er usikker
- C) Siden har fått mange besøkende
- D) Siden er sertifisert av google

26

Hvor ofte burde du ta backup på pcen?

- A) En gang i uken
- B) Bare når du mistenker at det kan oppstå et problem
- C) Hver dag
- D) Når du oppretter nye filer som du ikke vil miste

27

Det sies at "ingenting er gratis", men hva med alle gratis apper og tjenester?

- A) Det finnes ingen kostnader
- B) Det finnes mest sannsynlig skjulte økonomiske kostnader
- C) Din personlige informasjon er betalingen
- D) Det er ikke noe å tenke på

1

Hva er kravet for at et virus kan fungere?

- A) Det ondsinnede programmet kjøres
- B) Mangel på antivirusprogram
- C) Tilkobling til internett
- D) Man bruker noe annet enn MAC

2

Hva er noe et datavirus kan gjøre?

- A) Slette filer
- B) Stjele passord
- C) Gjøre pcen tregere
- D) Alle svarene over

3

I datasammenheng, hva er en trojansk hest?

- A) En pakke med forskjellige programmer
- B) Informasjon om hvordan trojanske hester ble brukt
- C) Et program som skjuler sine ondsinnede intensjoner
- D) Et program som alltid lurer antivirusprogrammer

7

Hva er noe man bør unngå når man lager passord?

- A) Bruk av personlige opplysninger
- B) Å bruke samme passord som andre steder
- C) Å lage et nesten likt passord som andre
- D) Alle over

8

Hva er faren ved å ha på WI-FI på mobilen til enhver tid?

- A) Mobilen kan prøve å koble seg på åpne nettverk
- B) Det bruker mye strøm
- C) Det kan ødelegge nettverkskortet i mobilen
- D) Alle over

9

Hvorfor bør man oppdatere mobilen så fort det er mulig?

- A) Det reduserer strømforbruket
- B) For å rette opp i feil fra den tidligere versjonen
- C) For å opprettholde garantien på mobilen
- D) Det er ikke så viktig å oppdatere

2

Hvordan vet man at man er koblet til en sikker nettside?

- A) HTTPS og grønn nøkkellås
- B) Rød lås ved siden av lenken
- C) Alle nettsider som begynner med www
- D) HTTPS og rød nøkkellås

4

I datasammenheng, hva er et virus?

- A) Et program som reklamerer for pornografisk materiale
- B) Kode som legger til funksjonalitet på PCen
- C) En sky-tjeneste
- D) Kode som gjenskaper seg selv

5

Hvordan finner et antivirusprogram skadevare på PCen?

- A) Lete etter kjente signaturer i filer
- B) Lure skadevare til å vise seg, og så stoppe den
- C) Med antivirus får man ikke skadevare
- D) Finner alle filer som ender med .ssh

6

Hva kjennetegner et polymorfisk virus?

- A) Et virus som er umulig å finne
- B) Et virus som endrer på signaturen sin
- C) Et virus som er mindre enn andre typer virus
- D) Et virus som er større enn andre typer virus

7

Hva kjennetegner et rootkit?

- A) Det infiserer PCen din uten internettilgang
- B) Den er flinkere til å skjule seg selv
- C) Det er et virus som har oppnådd målet sitt
- D) Alle over

8

Hva er ransomware?

- A) Skadevare som bruker webkameraet ditt uten at du vet det
- B) Skadevare som stjeler penger fra deg
- C) Skadevare som krypterer PCen din og krever penger for å låse den opp
- D) Et phishingangrep

9

Hva er den beste måten å motvirke ransomware?

- A) Ha sterke passord
- B) Skru av PCen med en gang
- C) Ikke del passordene dine
- D) Ha backup

10

Hva reduserer sjansen for suksessfulle bruteforce angrep mest?

- A) 8 tegn med tegn fra andre språk
- B) 10 tegn med tilfeldige bokstaver og tall
- C) 12 tegn med små/store bokstaver
- D) En lang setning

11

I forhold til passord, hva er et ordbokangrep(dictionary attack)?

- A) Et angrep som bruker varianter av kjente passord
- B) Et angrep som ser hva du skriver inn på tastaturet
- C) Et angrep som prøver alle mulige kombinasjoner
- D) Alle over

12

Hva vil det si at en nettside har et sertifikat?

- A) At de har retten til å være en nettside
- B) At de har retten til å ta vare på informasjonen du gir dem
- C) At nettsiden er de som de gir seg ut for å være
- D) At nettsiden ikke prøver å lure deg

20

I forhold til passord, hva er et bruteforce angrep?

- A) At noen finner passordet på en post-it lapp
- B) At angriperen tilbakestiller passordet
- C) Å prøve alle mulige kombinasjoner
- D) Å finne passordet på nettet

14

Hvilket er et phishingangrep rettet mot mobilen?

- A) Metasploit
- B) Whaling
- C) Scimming
- D) URL-padding

15

I datasammenheng, hva er en cookie?

- A) Det er noe man ikke trenger å godkjenne at nettsider bruker
- B) Små programmer som samler inn informasjon
- C) En mappe med besøkte nettsider
- D) Små tekstfiler med informasjon

16

Hva er en sikkerhetstrussel forbundet med cookies?

- A) Den kan brukes til å stjele identiteten din
- B) Den kan inneholde virus som infiserer PCen
- C) Den smaler på data som blir lagret på enheten
- D) GDPR

18

Hva er målet med en orm? (en dataorm)

- A) Å kryptere pcen og kreve løsepenger
- B) Å ødelegge pcen
- C) Å spre seg til andre maskiner
- D) Å stjele passordene dine

19

Hva er en måte å beskytte seg mot dataormer?

- A) Oppdatere all programvare
- B) Ha sterke passord
- C) Ha forskjellige passord
- D) Bruke to-faktor-autentisering

I Forklaring til spørsmål

I.1 Resepsjon

Nr	Forklaring		Nr	Forklaring		Nr	Forklaring
1	Grunnen til at du blir bedt å skru av pcen etter jobb er fordi da blir pcen oppdatert etter den nyeste versjonen. Utdaterte programvarer er en sikkerhetsrisiko.		4	Det kan selfølgelig skape dårlig stemning mellom deg og personen det gjelder, men det er også lurt å huske på at du gjør dette for sikkerhes skyld. Et godt sikkerhetskultur er når personen du spør forstår hvorfor du spør.		5	Det gjør det vanskeligere for en "insider" å få tilgang til f.eks. kritisk informasjon
6	Det kan hende at andre som er logget på nettverket er nysgjerrige på hva du driver med. Feilkonfigurasjon på din side kan føre til at andre kan se dokumentene dine.		7	VPN står for Virtual Private Network og kobler deg til et privat nettverk gjennom det åpne nettverket.		8	VPN krypterer all trafikk så ingen se den infromasjonen som blir sendt mellom deg og "endepunktet" (nettsiden du besøker)
10	Sosial manipulering er å utnytte vanlig menneskelig oppførsel (spiller på fristelser, frykt og tillit som oftest) for å innhente informasjon som kan benyttes til uærlige/ondsinnede handlinger.		11	For å sikre at man ikke benytter seg av usikret nettverk som er satt opp av aktører med uærlig/ondsinnet hensikter.		12	Viktig i forhold til at uautoriserte personer ikke kommer inn, men også i forhold til registrering av hvem som er i bygget hvis det skulle oppstå en nødsituasjon
13	Sosial manipulering er å utnytte vanlig menneskelig oppførsel (spiller på fristelser, frykt og tillit som oftest) for å innhente informasjon som kan benyttes til uærlige/ondsinnede handlinger.		14	En handling for å skaffe seg nyttig informasjon (slik som passord, brukernavn, kode osv.) gjennom observasjon.		15	Når en person kommer seg inn til et avgrenset område eller et kontrollpunkt sammen med en autorisert person for å obervere systemer og områder, tilegne seg konfidensiell informasjon med hensikt i å benytte det til uærlige/ondsinnede handlinger
16	Man må alltid følge ruitne, når man begynner å tøye grenser så vil dette ofte resultere i at man blir mer og mer uforsiktig og uoppmerksom på hva som kan skje.		17	Eksempel her er hvis du logger inn på facebook fra en annen sin pc, så burde du passe på å logge helt av og sjekke at ingen innloggingsopplysninger "henger igjen"		18	Spredning av virus er noe som er vanlig om enheten er kompromittert, da vil den "smitte" andre enheter internt. Det vil si at PCer som er relatert til arbeid kan også bli påvirket og dette kan være fatalt for organisasjonen.

I.2 Sikkerhetskultur

Nr	Forklaring		Nr	Forklaring		Nr	Forklaring
1	Alle har ansvaret for sikkerheten i en organisasjon. Du som en ansatt kan påvirke mer enn du tror, dine handlinger påvirker organisasjonen.		2	Det er lurt å melde fra til lederen, dette skaper forståelse for lederen om at definisjonen ikke er klar og kan også hjelpe deg å forklare deg hensikten bak rutinen.		3	Informasjonsflyt mellom kollegaer eller ledere og kollegaer er viktig. Hva trengs mer fokus på? Hva kan forbedres? Deling av erfaringer mellom kollegaer er lærerikt for begge parter.
5	Tilbakemelding til ledelsen hjelper ved å gi en indikasjon på hva som fungerer bra og hva som kan forbedres. Statistikk vil ikke alltid gi et detaljert bilde.		6	Ledelse, utvikling, rettferdighetskultur og læring er viktige områder innen sikkerhetskultur. Ledelsens atferd, straff og skyld, læring av feil og kontinuerlig utvikling er stikkord for dette.		10	Man kan finne overraskende mye infromasjon om personer ved å se på hva som blir lagt ut av informasjon på sosiale nettverk
11	Noe du vet - passord, noe du er - fingeravtrykk, noe du har - kodebrikke		12	Passord databaser kan lekkes og dermed benyttes til å få tilgang til andre kontoer, derfor er det lurt å benytte forskjellige passord.		13	IoT er dagligdagse gjenstander som vaskemaskin, kaffemaskin, kjøleskap som kan kobles på nettet. Det har vært mange tilfeller av dårlig sikkerhet i slike enheter.
15	Enheter vil ofte være konfigurert for brukervennlighet, men dette vil ofte være dårlig sikkerhet.		16	Det kan hende at noen nettsider ikke har gode rutiner for dette, så det er aldri feil å logge ut når man er ferdig		17	Et målrettet phishing angrep. Her er angriperen ute etter å ta deg spesifikt og bruker informasjon om deg som er funnet andre steder. Man kan finne mye informasjon om en person ved å bruke lovlige metoder
18	Det finnes mange måter å få informasjon om en person. Bruker du for eksempel deler av adressen din i passord, koder eller lignende?		19	Det kan forsåvidt også være personer uten noe særlig teknisk kunnskap. Man kan kjøpe sofistikerte "hacke"programmer med bruksanvisninger så en 5-åring klarer å gjennomføre det		20	Tilgangskontroll hvor du må angi et tilleggsbevis i tillegg til et vanlig passord/kode
21	Er en konto kompromittert så vil mest sannsynlig hackeren prøve påloggingsinformasjonen (brukernavn og passord) på flere nettsider.		22	Kompleksitet og smarthet i passordet vil gjøre det vanskeliger å gjennkjenne, men desto lengere det er desto vanskligere og lengre tid vil bli brukt på å dekryptere det.		23	Lange passord gjør det vanskeligere å gjette, kompleksitet gjør det vanskeligere å dekryptere.

I.3 Arbeidsplass

Nr	Forklaring		Nr	Forklaring		Nr	Forklaring
1	Alle som bruker dataen har ansvaret. Alle organisasjoner med sensitiv eopplysninger må fokusere og følge deres rutine og policy for håndtering av denne type data. GDPR ansvarlig er dem som finner ut om det har vært et brudd.		2	Selv om kollegaen din er en del av organisasjonen din er det fortsatt en risiko for at vandalisme eller sabotasje kan skje. Det er lurt å skifte passordet etter det, til noe som ikke er likt det gamle.		5	Privat enhet kan ikke kobles på det interne nettverket, dette skaper en svært høy risiko for angrep og spredning av virus.
6	En angriper kan bytte navn-alias til e-posten din og utgi seg for å være deg. Er dette ikke fanget opp av e-post tjenesten kan dette være utmerket for å phishing-angrep.		8	Du skal ikke gjøre dette, det kan skape tillit mellom dere, men det er en risiko for at de blir delt videre eller observert fra andre. Brukernavn og passord skal bare holdes for seg selv.		9	En enkel huskeregel: aldri oppgi informasjon dersom tilkoblingen er HTTP
10	Dette er noen måter å se hvor adressen tar deg, å holde musen over er den enkleste måten		11	2FA er en ekstra kode man må skrive inn i tillegg til passordet. BankID er en form for 2FA. Det kan også være i form av en kode på sms eller i en app		12	Eksempel her er hvis du logger inn på facebook fra en annen sin pc, så burde du passe på å logge helt av og sjekke at ingen innloggingsopplysninger "henger igjen"
13	Det kan være at du håndterer sensitive opplysninger som andre kan stå bak og se. (Shouldersurfing på engelsk)		14	Det er greit å skjule pinkoden når man taster det inn. Be andre snu hodet når du skriver inn passordet, ingen skam i å spørre om dette		15	Forkortede lenker er skummelt siden man ikke ser hvor de går. Det finnes nettsider der man kan sjekke hvor de går, Virus Total er et eksempel på en slik tjeneste
17	Domene er en navnestreng som benyttes for å nå tjenester på nettverk og internett.		18	Ser om siden linken viser til er reel, i forhold til at den finnes på firmaets nettside		19	Kan inneholde en eller annen form for skadevare som kan skade både pc og nettverket den er tilkoblet.
20	Et program som er lagd med intensjon om å gjøre skade på en computer, server, nettverk eller liknende. Noen eksempler kan være datavirus, ormer, trojanere eller ransomware.		21	Hvis du er usikker på avsender og innholdet i e-posten, ta kontakt med IT-avdelingen slik at de kan se på den. Bedre å spørre en gang for mye enn en gang for lite.		22	Å oppbevare passord blir generelt sett ned på, men det kan gjøres dersom man lagrer dem sikkert. Password managers blir for eksempel benyttet hyppig til å lagre passord kryptert lokalt på PC.
23	Phishing er det mest vanlige angrepet av desse her. Merk at ikke alle er like lette å skille ut. Når man sender til mange nok mottakere vil det som regel være noen som går på, og menneskelig feil er ofte hvordan et angrep blir vellykket generelt.		24	Det er alltid lurt å melde fra, sikkerhetsavdelingen kan ha muligheten for å sjekke det, men er ofte opptatt med andre viktige saker. Rettigheter kan ofte bli gitt og bli glemt etter prosjektet er ferdig, derfor er det lurt å melde ifra når dette skjer.		23	Lange passord gjør det vanskeligere å gjette, kompleksitet gjør det vanskeligere å dekryptere.

I.4 Godt & Blandet

Nr	Forklaring		Nr	Forklaring		Nr	Forklaring
1	Brukereg må laste ned programmet for at det skal være mulig for viruset å begynne sitt angrep		2	Det kan variere veldig hva et virus kan gjøre, et virus kjører ondsinnet kode på maskinen og har dermed tilgang til mange av computerens funksjoner.		3	En trojansk hest ser ut til å være et program som er til hjelp for deg, men som gjør noe ondsinnet på siden
7	Et passord skal helst være uforutsigbart slik at det er vanskelig for andre å resonere eller gjette seg fram til passordet.		8	Man vet aldri hvem som fisker etter informasjon på offentlige nettverk. Det er ulovlig å gjøre det ved mindre man eier nettverket		9	Det er alltid smart å oppdatere så fort det er mulig, dette gjelder ikke bare mobiler. Sikkerhetshull kan ha blitt reparert og oppdateringen vil dermed gjøre deg sikrere.
10	Krypteres innholdet på mobilen vil det være vanskelig for andre som finner mobilen å se innholdet, uansett hvor kyndige de er.		11	Det er praktisk, men igjen så vet man ikke hvordan disse nettsidene oppbevarer den informasjonen. Ganske synd hvis noen tømmer kontoen din fordi du ikke gidder å skrive inn kortinformasjonen når du skal handle på nettet		12	Sertifikatet er som regel den nøkkellåsen som er til venstre for der det står "HTTPS", den er det mulig å trykke på
13	Bare last ned fra chrome web store, eller det tilsvarende til firefox/safari/edge		14	Kun laste ned fra App Store/Play Store. Er det sider som reklamerer for appene sine i nettleseren er det best å søke de opp i app store/play store		15	Handlelisteappen trenger ikke å ha tilgang til hvor du er, mikrofon, kamera og telefonbok...
16	HTTPS => viser til at dataoverføringen er kryptert, mobildata => sikrer mot uærlige/ondsinnede aktører gjennom usikrede trådløse nettverk, anerkjent => viser til at tidligere kunder godt fornøyd og anser nettsiden som trygg		17	En ukjent USB kan inneholde en eller annen form for skadevare og kan skade både pc og nettverket den er tilkoblet		18	Er mest sannsynligvis en form for adware med uærlige/ondsindig hensikt, rute deg videre til gratis programvare hvorpå det installeres spyware som samler personlig informasjon om deg uten din tilatelse, og kan sporer nettsidene du besøker m.m, som igjen mest sannsynlig selges informasjon videre til tredjepart uten din viten.
19	Oppdatering av programvare er med på å holde enheten din sikker. Oppdateringer korrigerer sikkerhetshull slik at disse sårbarehetene ikke kan utnyttes av hackere.		20	Aktører som sender phishing mail kan "forkle" e-postadressen og linken slik at de visuelt ser legitime ut.		21	Torrent er en form for fildeling, muligheten til å laster ned filer av hverandre. For det første er det ukjent om den/de du laster ned filmen fra innhar rettigheter til å dele filmen, mest sannsynlig ikke, og er derfor ulovlig og straffbart. For det andre er dette en kilde til å laste ned innhold som kan påføre skade/kompromittere din datamaskin og nettverk den er tilkoblet.
22	Man skal aldri dele sine passord. Det er lett for andre å utnytte andres brukere og forholde seg anonym.		25	Google viser de sidene med flest besøkende først, dette betyr ikke nødvendigvis at siden er sikker.		26	Man kan sette opp automatisk kjøring av back-up, som det er det mest normale, men strengt tatt så er det kun nødvendig når man har lagret filer/bilder som man ikke ønsker å miste.
27	Ved nedlasting av apper eller inernett tjenester ligger det som regel med en form for brukeravtale, disse inneholder gjerne informasjon om hva selskapet kan innehente på oss. Dette er kanskje informasjon som også deles videre til tredjepart.		28	Ingen garanti for at selskapet som står bak nettstedet lagrer disse passordene kryptert.		29	De aller fleste enheter kan bli hacket, jo mer kompliserte de er jo flere muligheter. Det kommer også an på hvor mange som har lyst til å finne sikkerhetshull i en valgt enhet.

I.5 Bonus

Nr	Forklaring		Nr	Forklaring		Nr	Forklaring
2	En god indekasjon på at en nettside er sikker er at den bruker HTTPS protokollen og du får en grønn nøkkellås til venstre for lenken. Det er fortsatt mulig å ha HTTPS og grønnlås selv om det er en farlig nettside, men sannsynligheten for det er lavt siden det er et sertifikasjon man trenger for dette.		4	Mange betegner virus som generell skadevare, men det er det ikke. Skadevaren virus har fått det navnet siden den oppfører seg ganske likt som et bakterielt virus		5	Alle programmer har signaturer. Antivirusprogrammer leter etter kjente signaturer for skadevare. Det vil si hvis det er en helt ny type skadevare så kan det være vanskelig for antivirusprogrammet å oppdage dette
6	Et virus som endrer på signaturen sin. Et antivirus finner disse ved å se om programmer endrer signaturen sin.		7	Rootkits er flinkere til å skjule seg selv siden de ofte lever i minnet, eller "dypere" ned i PCen		8	Dette er noe man kanskje har hørt om i media. Mest kjent er angrepet mot Hydro i mars 2019. Skadevaren krypterer da harddisken og krever løsepenger for å låse opp PCen igjen. Det er alikevel ingen garanti for at den blir låst opp dersom du betaler
9	Det vil ta flere livstider å knekke krypteringen. Har du ikke backup kan du håpe på at de dekrypterer PCen dersom du betaler		10	Dette er noe som er mye diskutert, og det man generelt sier seg enige i er at man burde prioritere lengde over kompleksitet		11	Det er en type passord gjetting angrep, men her benytter man seg av en ordliste med masse forskjellige passord og prøver alle med litt forskjellige varianter av hver
12	Det er en tredjepart som deler ut sertifikater. Eierne av nettsiden må da bevise at de eier nettsiden		14	URL-padding er når man har lange lenker som ser legitime ut, men som gjemmer sin egentlige hensikt senere i lenken...noe som er vanskeligere å se for mobilbrukere		15	En cookie samler på mye forskjellig informasjon
16	Når man logger inn får man en "token". Denne blir lagret som en cookie. Får noen denne kan man bruke den og "være deg" på den nettsiden		18	Målet til ormen er å spre seg til så mange enheter som mulig inntil den har infisert X antall enheter eller en annen betingelse er oppfylt		19	Ormer benytter seg av sårbarheter i tidligere versjoner av programvarer
20	Bruteforceangrep prøver alle mulige kobinasjoner. Skulle man bruteforce en pin-kode på 4 tall, ville alle kombinasjoner mellom 0000 og 9999 blitt prøvd.						

J Gruppereferat fra moter

Møtereferat

Dato: 21.01.2019 **Varighet:** 1t 30 min **Tilstede:** Daniel Magnus, Abu Baker Al-Shammari, Inger Moen, Bendik Flobak

Agenda:

- [x] Riskoanalyse
- [x] Hva har blitt gjort siste sprint?
- [x] Planlegge hva som skjer neste sprint
- [x] Gant skjema
- [x] Neste møte med oppdragsgiver

Diskusjon:

Vi har gant skjema (mal) så det er bare å fylle inn data.

Figuren til risikomatrise er ferdig, finne ut hva som skal være der og gi det score.

Diskuterte hvordan tiden skal bli brukt og hvordan vi skal gå frem.

Mål og rammer, litt fokus på spill (vi burde fokusere på det vitenskaplige).

Inger har samlet informasjon og kunnskap når det gjelder opplæring.

Spillideer - spillere sammen mot en fiktiv hacker.

Høre med Erik Hjelmås, med tanke på teambasedlearning.

Et dokument på risikoanalyse finnes lokalt.

Følge opp:

- Purre på oppgavebeskrivelse
- Sjekke Anne Marie sin kontrakt (epost)
- Sende dokumentene (gruppereglene) til Ernst og Gaute.
- Strukturen på dokumentene, i noen delkapittel.
- Begynne å tenke på det som skjer etter forprosjektet, slik at vi utnytter arbeidskraften.
- Vi kan vise oppdragsgiver planen, slik vi kan avtale tid og møter.
- Informasjon, spørsmål generelt og spesielle spørsmål (med Gaute).
- Bli ferdig med gant, omfang, risikoanalyse, begynne med bacheloroppgaven (malen til Simon) research, evt begynne med innleiing.

Neste møte:

25.01.2019 - møte med veilederene (bare Gaute denne dagen)

28.01.2019 - scrum review

Møtereferat

Dato: 28.01.2019 **Varighet:** 2 t **Tilstede:** Abu Baker Al-Shammari, Bendik Flobak, Daniel Magnus og Inger Moren

Agenda:

Research spørreundersøkelse

Beskrive ståsted

Innledning på rapporten + sjekk trello backlog (WBS)

Utarbeide relatert arbeid (sjekke ut bachelor oppgave)

Pengebruk (ha det med til oppdragsgiver)

Gjer oss klar til møte med oppdragsgiver

Gå gjennom det som er in review og til done om alle er enige

Diskusjon:

Sendt inn forprosjektet, og begynne på selve oppgaven

Undersøkelses metoder,

Forskjellige tester

Begynne å skrive innledningen, og dele inn oppgavene på trello i mindre deler

Forskningsspørsmål, vi vet hva vi skal gjøre så vi må finne ut spørsmålene.

Hvilket nivå skal de være på?

Følge opp:

Dele oppgavene på trello

Gjør klar spørsmålene til tirsdag, slik at vi får de svarene vi trenger for å gå videre

Jobbe videre med litt research

Neste møte:

Mandag 04.02.2019 - sprint review

Tirsdag 05.02.2019 - oppdragsgiver

Møtereferat

Dato: 04.02.2019 **Varighet:** 45 min **Tilstede:**Bendik Flobak, Daniel Magnus, Inger Moen, Abu Baker Al-Shammari

Agenda:

Diskture neste møte med oppdragsgiver

Diskusjon:

- Finne ut av hva de tenker om problemstilling og det rundt
- Intervju, undersøkelser (tid og dato + antall personer vi må intervjue)
- Samle spillere til oss for å teste spillet etter påske
- Presentere post og pre test
- Må få spørsmålene med 1999
- Hva har DERE lyst å ha med?
- Policy, tidligere arbeids f.eks (trusselvurderinger / risikoanalyse)
- Høre med dem angående fremtidige møter + møtereferat
- Tips hvor lang påskeferie dem har
- 25 (skatteetaten)/26 (norsk tipping) - datoer intervju

Følge opp:

Ser hva vi finner ut av imorgen, og delegere oppgaver.

Forprosjektplanen rettes i løpet av uka, går sikkert gjennom review.

Neste møte:

05.02.2019 - møte med oppdragsgiver

08.02.2019 - møte med veiledere

Møtereferat

Dato: 11.02.2019

Varighet: 40 min

Tilstede: Bendik Flobak, Daniel Magnus, Inger Moren, Abu Baker Al-Shammari

Agenda:

- Finne ut hva vi skal gjøre til neste gang
    - Jobbe med intervjuspørsmål
    - Gå gjennom spørsmålene, velge de beste
    - Fortsette å skrive på Overleaf samtidig som vi jobber med prosjektet
- Diskutere om vi trenger Gaute sin statistikk (trusselbilde til NTNU)
- Høre hva Inger har researchet om, presentere det
- Nettvett, NSM grunnprinsipp - mye å hente her mtp intervju

Diskusjon:

- Inger forsker og skrive i dokumentet angående undersøkelse
    - Går gjennom funn hun har funnet
    - Får den informasjonen vi må ha
- Sikkerhetsinstruksen, hva er relevant for begge
    - Et dokument i SharePoint som inneholder generelt punkter innenfor informasjonssikkerhet
- Kan være skremmende med 4 stk som intervjue 1 person
    - Legge det inn i metodebruk i dokumentet
- Datoer må bli fastsatt slik at Inger kan komme til Norge og være med på intervju (Bekreftelse)
- Bare å legge inn formål og intervjuspørsmål underveis, så har vi en "speed date" for å fjerne eller legge til spørsmål som vi mener er relevant til intervjuet.
- Vi burde ha et spill i tankene som vi tror passer til oppgaven før intervju slik at vi har en slags oversikt, spillet må ikke være fastsatt (Ha en spillkveld med medlemmer i gruppen for å teste ut spill)
- Kan vi spør Trond om statistikk på trusselbilde

Følge opp:

- Sende referatet i dag til oppdragsgivere
- Datoer til intervjue
- Spøre veiledere om vi kunne delt det opp (fordeler/ulemper?)
    - Forslag: kan vi rulere sånn at det blir konsistent?
- NorSIS - trussler og trender 2018/2019 (se litt på dette og finn ut om det relevant)

Neste møte:

Fredag 15.02.2019 - Veiledermøte

Fredag 15.02.2019 - Diskutering angående intervjuspørsmål (etter veiledermøte)

Møtereferat

Dato: 18.02.2019 **Varighet:** 30 min **Tilstede:** Bendik Flobak, Daniel Magnus, Inger Moren og Abu Baker Al-Shammari

Agenda:

- Er møtene satt?
- Intervjuguiden?
- Hva vi gjør etter pre og post testen
- Hvordan ligger vi an på statistikk (kunnskap)

Diskusjon:

- Bendik har startet å lest bok om statistikk slik at vi har grunnlag og kompetanse når vi får inn tall og data.
- Vi må teste intervjuspørsmålene på personer, slik at vi kan kutte spørsmål om det er for mye.
- Anne Marie har skaffet 2 miljøer (26 eller 28 februar) og NT 27 februar. Vi skal få mer informasjon onsdag. Intervjuene skjer i Oslo.
- Emil ga beskjed 4 mars klokken 10, han lurte på om det er noe han burde forbrede seg på
- Vi prøvde en type brettspill i dag, men det var ikke så veldig relevant innen læring men spillet skapte mer diskusjon.
- I rapporten når det gjelder metode så er det kommentert litt.
- Veilederene sine tips om hvordan det skjer etter (fritekst på spørreundersøkelsen) og vi kan legge til dokumentasjon på hvorfor vi valgte det og andre muligheter.

Følge opp:

- Hvor lang tid tar intervjuet?
- Spørsmål som må bli fjernet/endret
- Dokumentet innen hva de skal forbrede seg på
- Escape room skal vi prøve å få til å spille, sjekke om det fungerer til opplæring og er relevant til vår oppgave.
- Baker kan gå gjennom metode (innen scenario), legge til om det er noe ekstra som trengst dokumentasjon på.

Neste møte:

Fredag 22.02.2019 - veiledermøte blir kansellert

Mandag 25.02.2019 - review

Møtereferat

Dato: 25.02.2019
Varighet: 1t
Tilstede: Daniel Magnus, Inger Moren, Abu Baker Al-Shammari

Agenda:

- Intervjuguide
- Datoer er satt, hvor vi møtes og klokkeslett osv
- Deles i to grupper, en som spør og en som skriver
- Må begynne å tenke litt på spill
- 4 mars, møte med oppdragsgiver

Diskusjon:

- Intervjuet er fikset og klart til bruk
- Inger og Baker testet ut intervjuet, la inn forslag til endringer
- Endringene har blitt gjort, det ferdige dokumentet blir lagt til mandag (ASAP)
- Gruppeinndeling, vi må huske å gå gjennom notatene etter intervju
- Valg av spill blir mer spesifisert etter intervjuresultatet
- Vi må opprette dokument om vi har spørsmål til oppdragsgiver

Følge opp:

- Gjør oss klar til intervju perioden, god spurt nå =)
- Tenke litt på spill (baktanke)
- Sende intervjuguiden til oppdragsgiver, om de har noen forslag eller tilbakemelding

Neste møte:

27.02.2019 - Intervju hos NT (klokken 10)

28.02.2019 - Intervju hos Skatteetaten

29.02.2019 - Veiledermøte

Møtereferat

Dato: 25.03.2019

Varighet:

Tilstede: Daniel Magnus, Inger Moren, Abu Baker Al-Shammari, Bendik Flobak

Agenda:

- Spillets framgang, hvordan ligger vi an?
- Hvor mange spørsmål har vi, hvordan ligger vi an der?
- Gå gjennom spørsmålene vi har
- Sonene i spillet, hva skal vi ha med?
- Testing av spillet før presentasjonen hos oppdragsgiveren
- Hvordan skal malen være for testingen, hva skal vi legge i rapporten?
- Med tanke på design, en i kollektivet til Baker kan designe brettspillet i fargene til Norsk Tipping og Skatteetaten

Diskusjon:

- Baker har sendt ut invitasjon for kollektivet angående spilltest, venter på respons.
- Spilltesten er viktig for å finne feil ved spillet og sjekke dynamikken. Vi skal teste spillet denne uken.
- Vi tenker at vi burde vente til testing før neste uke, for å få en god test.
- Vi må gå gjennom spørsmålene og fin pusse de, vi har svært gode spørsmål.
- Gaute eller Erik med tanke på material til kort og spill.
- Vi deler inn de inn i soner, **resepsjon, arbeidsplass, ledelse og godt og blandet.**
- Kommentere spørsmål på kommentar kolonnen om det skal være endringer.

Følge opp:

- Lage plan på hva vi skal se etter (testen).
- Skrive i rapporten, falt litt bak i de siste ukene.
- Skrive om funn og spillutvikling.
- Spørsmålene skal finpusset og satt sone på dem.
- Bendik tar kontakt med Hjelmås angående materiale.
- Legge inn ny kolonne i excel for svarbeskrivelse.

Neste møte:

Fredag 29.03.2019

Møtereferat

Dato: 08.04.2019

Varighet: 1t 15min

Tilstede: Bendik Flobak, Daniel Magnus, Abu Baker Al-Shammari

Agenda:

- Gå gjennom hva vi gikk gjennom med Gaute på fredag
- Har vi spørsmål til onsdag? (Hva skjer onsdag)
- Printe spillet på tykt papir - relatert til spørsmål
- Hva skal vi gjøre med forslagene test-objektene snakket om?
    - Flere FFA?
    - Stjelesjetong
    - Siste runde med gjennomgang
    - Ha spørsmål på skjermen?
    - Bonusspørsmål
- Fordeling av arbeidsoppgaver

Diskusjon:

- Gaute var veldig fornøyd, han likte spillet veldig godt
- Spørsmålene må vi gå gjennom igjen for å finpusse de litt ekstra
- Begynne med pre og post test
    - 10 stk som må være de samme både før og etter
- Bytte hint felter med FFA er endret
- FFA - fortsetter til noen svarer riktig (1 forsøk på hvert lag)
- Fortsetter som før, å ha det digitalt fører til lengre tidsbruk
- Siste runde med gjennomgang kan knyttes opp mot at vi ikke hadde forklaring under test
- Stjelesjetong etter svar (om du trur valgt alternativ er feil) vs det vi har nå
    - Kan hende at de ikke bruker sjetong om 1 forslaget havner i spillet
    - Frifelter har vi fortsatt
    - Beholder stjelesjetong, men kan bruke sjetongen for å beskytte seg (den som prøvde å stjele for den tilbake, og den som beskyttet seg mister sin)

Følge opp:

- Sende rapporten til Gaute og Ernst (helst i løpet av dagen)
- Legge inn bilder/figurer i rapporten

- Skrive diskusjonen og endringene vi hadde i dag i rapporten
- Selvevaluering 10 spm til fredag (høre hva de syns)
    - Mer jobbing med det blir forklart 09.04
- Lage et dokument på spørsmål til oppdragsgiver
    - Fastsette tid
    - Sammensette gruppe
- Printe ut nye spillbrettet før onsdag - Bendik sender mail til kopi-mannen

Neste møte:

K Timeliste

	Daniel		Baker		Bendik		Inger	
Dato	Timer	Beskrivelse	Timer	Beskrivelse	Timer	Beskrivelse	Timer	Beskrivelse
2019-01-17	4.5	1 time scanne og sende prosjektavtale til oppdragsgiver, 1,5 time på å skrive bakgrunn og rammer. 30 min på å skrive gruppregler, 30 min på å lage timeliste, 1 time på møteinnkallelse for veiledere(1. gang, var vanskelig å finne ut av	2.5	2 time Skrive på rapporten, hovedinndeling av prosjektet. Gjorde litt research på hvilke elementer vi skulle ha med på den hybride versjonen av Scrum. Skrive om rolle og møtene. 1/2 time Gjorde research på møtereferat. lagde en mal for oss, slik vi kan bruke det på mandag. Skrev referat fra møtet på onsdag	2.5	1 time scannet inn prosjektavtale, formatert og sendt videre til Daniel. 30 minutter lest igjennom lynkurset til Tom Røise. 1 time gjort meg kjent med rapporten på overleaf og begynt å skrive på omfang.	4	3,5 t søkt etter/lest om opplæringsmetoder, 0,5 t satt over og scannet signert grupperegler
2019-01-18	6	2,5 timer Kommunisert med oppdragsgiver og diverse administrerende ting, 1,5 time på å utarbeide et gantt skjema, 2 timer lesing av rapporter og skriving i latex	6	Skrev på del 4 overleaf. og signerte NDA Diskuterte med Bendik angående del 4. Drøfter spillideer Konfigstyring Lagde risikomatrise Noen notater til neste møte med veileder og oppdragsgiver	5.5	Scannet inn taushetsspliktер, sendt videre. Jobbet med del 4. Scannet gruppregler. Jobbet med del 2. Drøftet forskelige spillideer. Begynt på WBS.	5	3,5 t søkt etter/lest om opplæringsmetoder, 0,5 t satt over og scannet signert taushetserklæring, 1 t gjennomgang av mål og rammer
2019-01-19								
2019-01-20								
2019-01-21	5	Møte 2 timer, Gantt og diverse 3 timer	7	Møte 2 timer. Jobbet med dokumentet, fikset litt på matrisen. Diskuterte litt mer om spillet.	7	Møte til 10. Jobbet med Omfang. Gjort endringer på planlegging. Lagd tabell til risiko scenarier. Jobbet med ideen til spillet. Diskutert prosjektplan med veileder, fått kommentarer. Jobbet med incentiv til deltakere i spørreundersøkelsen. Satt risiko samsynlighet og konsekvens. Review av andre gruppemedlemmers arbeid.	2	Gruppemøte fra 8 til 10.
2019-01-22	1	1 time overleaf, måtte ta en dag jobbing ed andre fag	0.5	Jobbet med dokumentet	3	Funnet linker angående TBL og ferdighetstester, dokumentert disse.	3.5	Jobbet med forslag til problemstilling, 1 t laget skisse oppdraget, lest igjennom referat, lest om overleaf
2019-01-23	4	Skrive i overleaf, snakke med oppdragsgiver, forberede veiledermøte	2	Diverse	4	Forbedringer i prosjektplanen. Skrevet milepæler. Fikset utseende. Skrevet notater til veiledermøte.	4.5	Lest om overleaf, lagt til info vedr.bruk av overleaf i Organisering av kvalitetssikring. Lest igjennom/lagt til innspill på oppgavene: Mål og rammer, Plan for gjennomføring og organisering av kvalitetssikring i review (trello), satt igjennom ny dokumentasjon på google drive
2019-01-24	5	1 time veiledermøte, 4 timer med gjennomgang av overleaf	5	Møte med veileder, skrive møtereferat og jobbe med dokumentet	4	Veiledermøte. Forbedringer i Overleaf. Endret milepæler til å samsvare med ny plan.	4	Møte med veileder. Lest igjennom/lagt til kommentar på oppgaver i review (trello), Lagt til forslag/kommentarer i overleaf på: Mål og rammer, Omfang, Planlegging, Organisering og Plan for gjennomføring
2019-01-25	3	3 timer med overleaf, levert oppgaven	3	Jobbet med dokument, skrev agenda for neste møte og diskuterte om hva vi skulle gjøre videre i prosjektet. Startet med det 'ekte' dokumentet	3	Endringer i Overleaf. Laget mappe til spill research. Funnet linker angående spillresearch. Planlagt møte mandag.	2	Korrigering av forslag i overleaf/avsluttet kommertarer overleaf, googlet og lest om informasjonssikkerhetskultur, Notert ned punkter etter forprosjektet i individuelle refleksjonsnotater
2019-01-26								
2019-01-27								
2019-01-28	5	Gruppemøte, research spørreundersøkelser, forelesning	5	Gruppemøte, skrevet møtereferat. Sjekker opp informasjon angående spørreundersøkelse	7	Møte med gruppe. Organisert kommende møter. Bestilt statistikk bok. Kopierte over ting som kan være i introduksjon fra forprosjektet og begynt på revidering av introduksjonen.	5.5	Gjennomgang av dokumenter før gruppemøte. lest om baseline testing, gruppemøte kl.10:00, lest om oppbygging av en oppgave - satt på oppdeling av innledning, redigert noe tekst i innledning, lest/satt på oppsett på tidligere bachelroppgaver
2019-01-29	6	Research av spørreundersøkelser, sett på overleaf., lest tidl. bachelor oppgaver	6	Research på spørreundersøkelsen. Leste gjennom rapporter, og overleaf.	5	Lest introduksjoner til andre bachelor oppgaver. Research rundt best practice av passord. Lagt inn forslag til forskningsspørsmål.		
2019-01-30	7	Skrevet på overleaf og lest diverse bachelroppgaver			5	Drøfting rundt introduksjonen. Sett etter relevant arbeid. Lest bachelor oppgaver. Ordnet med bestillingen av boken.	5.5	Laget forslag til endring av tekst under avsnitt Oppgave i Innledingen, lest/satt på bachelroppgaver, lest om /søkt på akademisk oppgave skriving
2019-01-31	5	Gjort research	5	Research, jobbing med litt med oppsettet av det nye dokumentet			5.5	Lest rapport om opplæringsprogrammer (Anne Marie), lagt til kommentar på spørsmål til veileder, satt på/lest om forskningsspørsmål, satt på/lest om oppgave skriving, satt på/lest bachelroppgaver

	Daniel		Baker		Bendik		Inger			
Dato	Timer	Beskrivelse	Timer	Beskrivelse	Timer	Beskrivelse	Timer	Beskrivelse		
2019-02-01	3	Møteforberedelser, møte og ettermøtesamtale	3	Møteforberedelser, møte og ettermøtesamtale	3	Møteforberedelser, møte og drøfting rundt møte mandag.				
2019-02-02										
2019-02-03										
2019-02-04	1	Gruppemøte, (Karrieredag, det ble prioritert)	1	Gruppemøte	1	Gruppemøte før møte 05.02	3	Lest igjennom kommentarer i forprosjektet fra veileder, lest igjennom bacheloroppgave - læringsutbytte, gruppemøte, lest litt om ntnu selectsurvey, lest litt om NSMs grunnprinsipper for IKT-sikkerhet		
2019-02-05	5	Møte norsk-tipping og skatteetaten	5	Møte oppdragsgivere	5	Møte oppdragsgivere	4	Møte oppdragsgiverne		
2019-02-06	7.5	Gjort endringer i forprosjektet, lest policy til NT, sendt referat til oppdragsgivere	7.5	Endret forprosjektet, gått gjennom policy. La inn møtereferat fra igår	6	Skrevet møtereferat, endringer på hovedrapportens innledning. Begynt å lese policy	2	Lest igjennom sikkerhetsinstruks NT, Notert ned viktige punkter å ta med seg fra sikkerhetsinstruksen NT (omhandler infosec)		
2019-02-07	5	Research intervju	4	Lest ferdig policy og lagd oppsett for spørsmål til spill og intervju	4.5	Idemyldring rundt spørsmål til intervju. Gjennomgang av endringer på forprosjektet. Lest videre på policy. Lest på kilder om kalitative intervju.	5.5	Sjekket/lest litt om Nasjonal strategi for digital sikkerhet, fortsetter viktige punktrt sikkerhetsins. NT, lest litt om kvalitativ metode intervju, sett fort igjennom grunnprinsipper for ikt-sikkerhet NSM, sett på veiledninger nettvett.no, sett på/lagt til forlag intervju spørsmål		
2019-02-08	4.5	Jobbet med spørsmål til intervju, møte med veiledere	4.5	Møte med veiledere. Spørsmål til intervju samt oppsett	4.5	Møte med veiledere. Begynt på metodikk i rapporten. Funnet relaterte studier til opplæring med brettspill.	2	Møte med veiledere, lest innledning og oppsummering og sett på figurer/bilder study om brettspill i opplæring innenfor helsefag, begynt på metode for første innsamling		
2019-02-09										
2019-02-10							4.5	lest meg opp på metode - undersøkelsesdesign og kvalitativ/kvantitativ tilnærming		
2019-02-11	5	Gruppemøte, jobbet med spørsmål, sett på sikkerhetsinstuks, forelesning, send referat til oppdragsgiver, sett på non stop sikkerhet	5	Gruppe møtet, skrevet referat. Sendt og lagt inn i Drive. Gått gjennom spørsmål, lagt til litt intervjuspørsmål samt formål. Diskutert litt og sett gjennom spillet fra NT	7	Gruppemøte, Skrevet avsnitt om metodikk i overleaf. Fylt på med ønsket utbytte på metodikk. Lest gjennom policy og sett opp mot notater. Jobbet med intervjuspørsmål. Diskutert ideer til spillet	5.5	lest meg opp på metode - undersøkelsesdesign og kvalitativ/kvantitativ tilnærming, gruppemøte, fortsetter med metode første innsamling		
2019-02-12	5.5	Mye diskusjon, jobbet litt med rettskrivning	5.5	Jobbet med spørsmål og intervju. Diskuterte MASSE om resultat og videre arbeid. La inn notater angående metoder når man intervjuer. Gikk gjennom spørsmål fra NON STOP, sjekket om de kunne brukes. Notert litt angående formål og noen indirekte spørsmål under intervju. Dokumentet har kategori. Hjalp med tips and tricks på overleaf.	5	Diskusjon rundt spill og tesfasen. Jobbet med metode. Lest på relatert arbeid. Hentet statistikk fra Gaute	4.5	fortsetter med metode første innsamling, lagt til viktige punkter å tenke på ift intervju (metode) i dok på google drive,		
2019-02-13	5	Skrevet og rette på overleaf, lest bacheloroppgaver	5	Skrevet mer utfyllende om metoden bak scenario, gjort mye research på det	5	Lest på trussel statistikk fra Gaute. Lest på relatert arbeid.	5	fortsetter med metode første innsamling, sett igjennom ny info på google drive mappa		
2019-02-14	4	Jobbe med intervjuspørsmål	4	Intervjuspørsmål dokumentet, laget og fjernet spørsmål			6.5	fortsetter med metode første innsamling, sett igjennom intervjuspørsmål		
2019-02-15	5	Møte med veileder. Ferdigstille intervjuspørsmål	4	Møte med veileder, gikk gjennom sammen med gruppen for å ferdigstille intervjuspørsmål	5	Møte veileder, ferdigstilling av intervjuspørsmål	4	oppdatert kalender, veiledermøte, gruppemøte - gjennomgang spørsmål		
2019-02-16										
2019-02-17										
2019-02-18	3.5	Gruppemøte, lese gjennom det som var skrevet om intervju og laget kommentarer, prøve et brettspill (sheriff of nottingham)	3.5	Review sammen med gruppen, lagde ferdig dokumentet og oppsette slik at det er lettere å notere ned under intervju. Check boxes ble også lagt til. Testet spill	2.5	Testet spill	1	Sett igjennom intervju pdf, sett igjennom kommentarer overleaf, sett igjennom møteref fra sist veiledermøte, gruppemøte		
2019-02-19	4.5	Prøvd forskjellige brettspill	4.5	Testet ut brettspill	4.5	Prøvd brettspill				
2019-02-20			2	Prøvde ut intervju på 2stk			6	Korrigeringer i Metode intervju, forberedelser til intervju, test intervju med tilbakemeldinger på spørsmålen - brukte 56 minutt.		
2019-02-21							1.5	Lest igjennom SE's sikkerhetsinstruks + etiske rettningslinjer + send bekreftelse til AM, lagt til dok med tilbakemeldinger på intervjuspørsmålene		
2019-02-22										
2019-02-23										
2019-02-24										

	Daniel		Baker		Bendik		Inger			
Dato	Timer	Beskrivelse	Timer	Beskrivelse	Timer	Beskrivelse	Timer	Beskrivelse		
2019-02-25	4	Gruppemøte	5	Gruppemøte, skrev ned referat. Lagde ferdig komplett versjon av intervju i pdf og doc format.			4.5	Endre ut fra kommentrarer på overleaf/metode/intervju, gruppemøtte -gått gjennom intervjuspørsmålene, oppretter tabeller i overleaf/metode/intervju, lest referat gruppemøte		
2019-02-26	3	Kommunisert med oppdragsgivere, sett på endringer i overleaf, sett på intervjuguiden	3	Intervjuguide, oppsett, endringer	3	Intervjuguide	0.5	Gjennomgått intervju		
2019-02-27	4	Intervjuer hos Norsk Tipping	4	Intervju NT	4	Intervju NT	4.5	Intervju hos NT		
2019-02-28	5	Intervjuer hos Skatteetaten	5	Intervju Skatteetat	5	Intervju Skatteetaten	5	Intervju hos SE		
2019-03-01	4	Veiledermøte, føre inn resultater i sharepoint	3.5	Veiledermøte, referat er skrevet og dokumentene er tilgjengelig på sharepoint.	4	Veiledermøte, resultater fra intervju	1	veiledermøte		
2019-03-02										
2019-03-03										
2019-03-04	1	Gruppemøte			1	Gruppemøte				
2019-03-05	6	Ført inn resultater fra intervjuer i sharepoint, gjort research på spøremål til spill	3.5	Difi dilemma, lagt til resultater i sharepoint. Laget noen notater på hva vi skal jobbe med videre	5	Innføring av trender fra intervju	2	Sjekke nye/oppdaterte dokumenter, sett igjennom excel resultat dokument		
2019-03-06	8	Gruppemøte, rapportskriving-forelesning, forberedelser til oppdragsgivermøte, reasearch trusler og trender	7	Møte sammen angående funn, laget nytt dokument på SP angående felles funn. Skrevet ned hva vi skal jobbe med videre. Notat på hvorfor vi valgte å ha spørreundersøkelse med frittsvar etter post test.	6	Gruppemøte, lynkurs, forberedelser til møte med oppdragsgiver, begynt på ny introduksjon	3.5	Møte - gått igjennom resultat dokumentet lagt til konklusjoner på utvalgte hovedspørsmål, sett igjennom punkter i dok aktuelle funn, lest igjennom spørsmål til oppdragsgiver		
2019-03-07	2	Møte med oppdragsgiver	2	Møte med oppdragsgiver	2	Møte med oppdragsgiver	2	Møte med oppdragsgiver		
2019-03-08	8	Møte med veileder, skriving i latex	8	Møte med veiledere, skrevet i latex og slettet ubruklig ting fra malen	4	Møte med veileder, skriving i rapport.	5.5	Veiledermøte, ferdig metode intervju, laget intervjuguide og lagt til i oppgaven (overleaf)		
2019-03-09			3	Skrevet oppsummering til Anne Marie, kan også brukes i rapporten og gått gjennom difi dilemma						
2019-03-10										
2019-03-11	6	Gruppemøte og game jam	6	Gamejam, gruppemøte. Noterte ned alt som ble sagt	7.5	Gruppemøte, gamejam, skriving på rapport	5	Lest igjennom sammendrag interv SE, sett igjennom møteref veiledere og oppdragsgivere, lest igjennom avsnitt om begrunnelse fritt svar post-test, møte diskusjon spill		
2019-03-12	5	Skrevet på overleaf, undersøkt spørsmål til spill	3	Lagde figur, sjekket litt difi (roller) og begynte å skrive litt til utkask	5	Skriving på innledning. Lest og gjort mindre endringer på sammendrag til SE. Lest diskusjon rundt testundersøkelsen				
2019-03-13	6	Gruppemøte/game jam	6	Gruppemøte/game jam	6	Guppemøte, game jam	5.5	Gått gjennom overleaf, jobbet med forslag til spill, møte diskusjon spill		
2019-03-14	1	Veiledermøte, jobbet med andre fag	1	Veiledermøte, jobbet med andre fag	4	Veiledermøte, lest statistikk	1.5	Veiledermøte, søkt etter infosec spørsmål relevant for ansatte		
2019-03-15		Her var jeg dårlig, så ble ikke noe jobb den dagen	3	Researchet på spørsmål og hvordan vi kunne dele de sonene i spillet.	1	Lest om statistikk, jobbet med matte	3.5	Søkt etter infosec spørsmål relevant for ansatte, sett på sikkerhetsspillet til ESET		
2019-03-16										
2019-03-17										
2019-03-18	3	Gruppemøte	3	Gruppemøte	5.5	Gruppemøte, lest statistikk.	5	Sjekket spillet ESET, gruppemøte, omformulert scenario spørsmål/spørsmål fra ESET spillet til norsk		
2019-03-19		Jobbintervju hos EVRY, ikke tilstede for å jobbe	4	Research til spørsmål og laget noen spørsmål	2.5	Lest statistikk				
2019-03-20	6	Jobbet med spørsmål til spillet	5	Las principes of information security samt andre spørsmål rettet mot sertifiseringer som kunne blitt med i spillet. Laget noen spørsmål i dokumentet.	6	Lest statistikk	5	Omformulert scenario spørsmål/spørsmål fra ESET spillet til norsk		
2019-03-21	5	Jobbet med spørsmål til spillet	2	Gikk gjennom spørsmålene mine, måtte fjerne noen (følte de var ikke relevant) la noen til mtp ITSM	3	Lest NSM risikovurdering, lest statistikk	5	Sett etter nye kilder for informasjonssikkerhetsspørsmål		
2019-03-22	5	Oppdateringsmøte med veileder. Skrevet inn spørsmål i felles dokument	3	Møte med veileder, addet mer spørsmål	1	Veiledermøte	4	Omformulert spørsmål fra div kilder til norsk, legge inn spørsmålene i exceldok.		
2019-03-23										
2019-03-24										

	Daniel		**Baker**		**Bendik**		**Inger**			
Dato	Timer	Beskrivelse	Timer	Beskrivelse	Timer	Beskrivelse	Timer	Beskrivelse		
2019-03-25	5	Gruppemøte, gjøre ferdig spørsmål	5	Gruppemøte, jobbet med spørsmål og skisse av brettet	7	Gruppemøte, skrevet på rapport, lagd gamejam kart	5.5	Omformulert spørsmål fra div kilder til norsk, legge inn spørsmålene i exceldok, gruppemøte		
2019-03-26	6	Skrevet beskrivelse til fasti, sett på spørsmål til ferdighetstest	2	Deltid, jobbet mer med spørsmålene	5	Skrevet på overleaf, Forberedt punkter å gå igjennom	5	Justere spørsmålene i exceldok, overleaf skrevet litt om NT sitt tidligere spill		
2019-03-27	6	Jobbet med spørsmål, utformet hvordan spørsmålskort skal se ut	2	Deltid, jobbet med NT resultat (dokument lokalt på PC)	6	Skrevet på overleaf, Gått gjennom spørsmål	7	Lagt til beskrivelse av svar infosec spørsmålene + justering		
2019-03-28	5	Jobbet med spørsmål, laget alle bonusspørsmål	5	Skrev ned spørsmål til ledelse og resepsjon	3	Skrevet på overleaf, laget bonusspm. Fordelt soner bedre	6	Justere spørsmålene i exceldok, gruppemøte om infosec spørsmål, nye spørsmål resepsjonen		
2019-03-29			4	Veiledermøte, skisse til spillet er oppdatert men trengst å vises på gruppemøte.	6	Veiledermøte, Lett etter glossary i rapport, laget utkast til brett	3	Notert litt på refleksjonsnotater, nye spørsmål resepsjon, veiledermøte, lest referat		
2019-03-30										
2019-03-31			4	Skrev 3 avsnitt om testing og skisse til mal						
2019-04-01	7	Gruppemøte, gjennomgått alle spørsmål - ferdig	7	Gruppemøte, gått gjennom spørsmål og skrevet i rapporten	9	Gruppemøte, spørsmål, utforming av brett	5.5	Gruppemøte, justere spørsmål - lagt over i nytt dok		
2019-04-02	6	Laget ferdig spørsmålskort for arbeidssted, vært med i statistikk workshop med gaute	3	Lagt inn spørsmål i spørsmålskort-malen. Leste opp på hva som er viktig å ha med på test-mal	5	Lagt spørsmål på kort, eksperimentert med utskrifter, workshop om statistikk	0.5	Lest om læringsmetoder, sett på undersøkelse om brettspill læring, lagt inn spørsmål i kortmal		
2019-04-03	6	Printet ut spillkort og testet spillet	6	Printet ut spillkort, testet spill	8	Printet ut kort, testet spill	1.5	begynte å legge inn sprm i print mal - men allerede gjort		
2019-04-04	2	Jobbet med overleaf	2	Testrsultater fra i går ble		Syk	0.5	lest på undersøkelsen om brettspill i læring		
2019-04-05	7	Veiledermøte, jobbet med overleaf, og gjort om på spørsmål	6	Veiledermøte, referat, skrev på rapport angående testing.		Syk				
2019-04-06							1	endret på spørsmål		
2019-04-07										
2019-04-08	6	Gruppemøte, skrevet i overleaf	3	Gruppemøte, referat lagd	7	Gruppemøte, skrevet i overleaf. Endringer på brett	5.5	lest meg opp på oppdateringer og møteref google disk, gruppemøte, forts. under relatert arbeid overleaf		
2019-04-09	1	PCen konka			5	Selv evaluering spørsmål, lest etter glossary i rapport. PC support	6	Lagt til resten av spørsmålene i sikkerhetskultur på lucidc., forts. under relatert arbeid overleaf, søking etter info/inspirasjon til selvevalueringen (pre-, posttest), hentet spørsmål fra sjekkIT omformulert/tilpasset til selvevalueringstesten		
2019-04-10	3	møte skatteetaten	3	Møte med skatteetaten	3	Møte skatteetaten	1	hentet spørsmål fra sjekkIT omformulert/tilpasset til selvevalueringstesten		
2019-04-11	7	Jobbet med spørsmål. Jobbet litt på overleaf. Laget regler for spillet. Jobbet med selvevalueringen		Intervju	6	Jobbet med spørsmål, Jobbet med selvevaluering	5.5	forts. under relatert arbeid overleaf, diskusjon pre- og posttest, diskusjon antall som spiller redusere fra 8 (2 i en gruppe) til 4		
2019-04-12	3	Møte, plan videre		Intervju	6	Møte, Skrevet referat, jobbet med plan videre, skrevet på rapport	0.5	Delvis tilkoblet/tilstede veiledermøte		
2019-04-13										
2019-04-14	1	Tatt notater på hvordan man lager spørreundersøkelser								
2019-04-15										
2019-04-16										
2019-04-17										
2019-04-18	4	Research på pre-posttest og skrevet i overleaf								
2019-04-19	2	Laget og testet brukervennligheten på regler, fikset på pre-posttest, laget ny inkrementell plan								
2019-04-20										
2019-04-21										
2019-04-22										
2019-04-23	7.5	Skrevet om spørreundersøkelse i overleaf, møte, kunnskapstest	5.5		5	Gjort klart kort til utskrift, begynt på forklaringer	4.5	lest meg opp på oppdateringer og møteref google disk/trello/overleaf, gruppemøte		

	Daniel		**Baker**		**Bendik**		**Inger**			
Dato	Timer	Beskrivelse	Timer	Beskrivelse	Timer	Beskrivelse	Timer	Beskrivelse		
2019-04-24	6.5	Jobber med kunnskapstest og selvevaluering, snakket med gaute om kunnskapstest og selvevaluering, skrevet litt på overleaf			6	Gjort klart kort til utskrift, sendt til utskrift, gjort ferdig forklaringer	4.5	jobbet med relatert arbeid overleaf		
2019-04-25	2	Revidert kunnskapsspørsmål og selvevaluering			4	Lest på statistikk fra Gaute, begynt på utforming av metodikk	5.5	jobbet med relatert arbeid overleaf		
2019-04-26	1	møte			2	Møte, hentet utskrift	2.5	jobbet med relatert arbeid overleaf, veiledermøte		
2019-04-27	3.5	Ferdigstille ferdighetstest og selvevaluering			1	Sortert utskrifter				
2019-04-28	0.5	Hjulpet bendik			1	Skrevet ut evaluering, test og regler	0.5	jobbet med relatert arbeid overleaf		
2019-04-29	5.5	Spilltest hos NT	5.5	Spilltest hos NT	5.5	Spilltest NT	5.5	Utført spilltest hos NT		
2019-04-30	5	Skrevet inn resultater for NT			5	Jobbet med resultater NT	1.5	jobbet med relatert arbeid overleaf		
2019-05-01	4	Skrevet om diverse i overleaf, printet ut alt for test hos skatteetaten		Jobbe medjobbintervju	4	Jobbet med forskjellige grafer, skrevet ut til SE	3	jobbet med relatert arbeid overleaf		
2019-05-02	5	Spilltest hos skatteetaten	5	Spilltest hos skatteetaten	5	Spilltest SE	5	Utført spilltest hos SE		
2019-05-03	7	Møte, analyse av resultater	4	Møte og analyse	7	Møte, analyse, revideringer, metodikk statistikk				
2019-05-04					4	Statistikk				
2019-05-05										
2019-05-06	7	rettskriving		Intervju	7	Statistikk, rettskriving	1	sett igjennom\lest statistikk		
2019-05-07	6.5	Dataanalyse	6	Analyse og rettskriving	8	Statistikk og analyse	2.5	sett igjennom kommentarer fra Gaute - sendt mail for oppklaring, sett igjennom punkter på trello, sett igjennom\lest statistikk, korrigering		
2019-05-08	8	Dataanalyse	6	Analyse + rettskriving	8	Statistikk og analyse	4.5	korrigering og jobbet med tillegg relatert arbeid, sett igjennom\lest statistikk		
2019-05-09	8	Dataanalyse		Syk	8	Dataanalyse, andre revideringer	5.5	jobbet med tillegg relatert arbeid		
2019-05-10	7.5	Veileermøte, rapportskriving	7.5	Møte, gå gjennom rapport	7.5	Møte, rapport	7	jobbet med tillegg relatert arbeid		
2019-05-11	7	Skrive på rapporten	7	Rapportskriving	7	Drøftiong, konklusjon, revideringer	4	jobbet med tillegg relatert arbeid		
2019-05-12	5	Ferdigstille rapporten	5	Ferdigstille rapporten	5	Ferdigstille rapporten				
2019-05-13										
2019-05-14										
2019-05-15										
2019-05-16										
2019-05-17										
2019-05-18										
2019-05-19										
2019-05-20										
	365.5	timer	284	timer	350.5	timer	270.5	timer	Timer totalt	1270.5

L Prosjektavtale Norsk Tipping

NTNU

Norges teknisk-naturvitenskapelige universitet

Vår dato Vår referanse

Prosjektavtale

mellom NTNU Fakultet for informasjonsteknologi og elektroteknikk (IE) på Gjøvik (utdanningsinstitusjon), og

NORSK TIPPING AS v/ TRONO ZAUPSMED

(oppdragsgiver), og

Daniel Magnus, Abu Baker Al Shammari, Inger Maren og Bendik Flobak

(student(er))

Avtalen angir avtalepartenes plikter vedrørende gjennomføring av prosjektet og rettigheter til anvendelse av de resultater som prosjektet frembringer:

1. Studenten(e) skal gjennomføre prosjektet i perioden fra 7.1.19 til 20.5.19.

   Studentene skal i denne perioden følge en oppsatt fremdriftsplan der NTNU IE på Gjøvik yter veiledning. Oppdragsgiver yter avtalt prosjektbistand til fastsatte tider. Oppdragsgiver stiller til rådighet kunnskap og materiale som er nødvendig for å få gjennomført prosjektet. Det forutsettes at de gitte problemstillinger det arbeides med er aktuelle og på et nivå tilpasset studentenes faglige kunnskaper. Oppdragsgiver plikter på forespørsel fra NTNU å gi en vurdering av prosjektet vederlagsfritt.

2. Kostnadene ved gjennomføringen av prosjektet dekkes på følgende måte:
   - Oppdragsgiver dekker selv gjennomføring av prosjektet når det gjelder f.eks. materiell, telefon/fax, reiser og nødvendig overnatting på steder langt fra NTNU på Gjøvik. Studentene dekker utgifter for ferdigstillelse av prosjektmateriell.
   - Eiendomsretten til eventuell prototyp tilfaller den som har betalt komponenter og materiell mv. som er brukt til prototypen. Dersom det er nødvendig med større og/eller spesielle investeringer for å få gjennomført prosjektet, må det gjøres en egen avtale mellom partene om eventuell kostnadsfordeling og eiendomsrett.

3. NTNU IE på Gjøvik står ikke som garantist for at det oppdragsgiver har bestilt fungerer etter hensikten, ei heller at prosjektet blir fullført. Prosjektet må anses som en eksamensrelatert oppgave som blir bedømt av intern og ekstern sensor. Likevel er det en forpliktelse for utøverne av prosjektet å fullføre dette til avtalte spesifikasjoner, funksjonsnivå og tider.

4. Alle bacheloroppgaver som ikke er klausulert og hvor forfatteren(e) har gitt sitt samtykke til publisering, kan gjøres tilgjengelig via NTNUs institusjonelle arkiv hvis de har skriftlig karakter A, B eller C.

Tilgjengeliggjøring i det åpne arkivet forutsetter avtale om delvis overdragelse av opphavsrett, se «avtale om publisering» (jfr Lov om opphavsrett). Oppdragsgiver og veileder godtar slik offentliggjøring når de signerer denne prosjektavtalen, og må evt. gi skriftlig melding til studenter og instituttleder/fagenhetsleder om de i løpet av prosjektet endrer syn på slik offentliggjøring.

Den totale besvarelsen med tegninger, modeller og apparatur så vel som programlisting, kildekode mv. som inngår som del av eller vedlegg til besvarelsen, kan vederlagsfritt benyttes til undervisnings- og forskningsformål. Besvarelsen, eller vedlegg til den, må ikke nyttes av NTNU til andre formål, og ikke overlates til utenforstående uten etter avtale med de øvrige parter i denne avtalen. Dette gjelder også firmaer hvor ansatte ved NTNU og/eller studenter har interesser.

5. Besvarelsens spesifikasjoner og resultat kan anvendes i oppdragsgivers egen virksomhet. Gjør studenten(e) i sin besvarelse, eller under arbeidet med den, en patentbar oppfinnelse, gjelder i forholdet mellom oppdragsgiver og student(er) bestemmelsene i Lov om retten til oppfinnelser av 17. april 1970, §§ 4-10.

6. Ut over den offentliggjøring som er nevnt i punkt 4 har studenten(e) ikke rett til å publisere sin besvarelse, det være seg helt eller delvis eller som del i annet arbeide, uten samtykke fra oppdragsgiver. Tilsvarende samtykke må foreligge i forholdet mellom student(er) og faglærer/veileder for det materialet som faglærer/veileder stiller til disposisjon.

7. Studenten(e) leverer oppgavebesvarelsen med vedlegg (pdf) i NTNUs elektroniske eksamenssystem. I tillegg leveres ett eksemplar til oppdragsgiver.

8. Denne avtalen utferdiges med ett eksemplar til hver av partene. På vegne av NTNU, IE er det instituttleder/faggruppeleder som godkjenner avtalen.

9. I det enkelte tilfelle kan det inngås egen avtale mellom oppdragsgiver, student(er) og NTNU som regulerer nærmere forhold vedrørende bl.a. eiendomsrett, videre bruk, konfidensialitet, kostnadsdekning og økonomisk utnyttelse av resultatene. Dersom oppdragsgiver og student(er) ønsker en videre eller ny avtale med oppdragsgiver, skjer dette uten NTNU som partner.

10. Når NTNU også opptrer som oppdragsgiver, trer NTNU inn i kontrakten både som utdanningsinstitusjon og som oppdragsgiver.

11. Eventuell uenighet vedrørende forståelse av denne avtale løses ved forhandlinger avtalepartene imellom. Dersom det ikke oppnås enighet, er partene enige om at tvisten løses av voldgift, etter bestemmelsene i tvistemålsloven av 13.8.1915 nr. 6, kapittel 32.

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk

12. Deltakende personer ved prosjektgjennomføringen:

NTNUs veileder (navn): _____

Oppdragsgivers kontaktperson (navn): Trond Laabakk

Student(er) (signatur): Daniel Magnus dato 09/01-19

Abdbaker Alshammari dato 09/01-19

Inger Moen dato 9/1-19

Bendik B. Flobak dato 17/01-19

Oppdragsgiver (signatur): Trond Laabakk dato 17/1-19

Signert avtale leveres digitalt i Blackboard, rom for bacheloroppgaven.
Godkjennes digitalt av instituttleder/faggruppeleder.

Om papirversjon med signatur er ønskelig, må papirversjon leveres til instituttet i tillegg.
Plass for evt sign:

Instituttleder/faggruppeleder (signatur): _____ dato _____

M Forprosjekt

Forprosjektplan for spillbasert opplæring

Bacheloroppgave

Al-Shammari Abu Baker, **Flobak** Bendik Berntsen, **Magnus** Daniel Christian Haraldsen, **Moren** Inger

IT-Drift og Informasjonssikkerhet ved Institutt for informasjonssikkerhet og kommunikasjonsteknologi

NTNU - Gjøvik

Norge

7 januar 2019

Innhold

Tabeller

1 Mål og rammer

1.1 Innledning

"Alle organisasjoner har en eller annen form for sikkerhetskultur. Den kan være god eller dårlig, men sikkerhetskultur er noe vi ofte først blir bevisst når vi opplever sikkerhetsbrudd eller sikkerhetstruende hendelser. Sikkerhetsbrudd er ofte et resultat av individers eller organisasjoners manglende sikkerhetsbevissthet, og sikkerhetsatferd. Dette kan skyldes manglende kunnskaper og evne til å foreta riktige beslutninger, eller det er handlinger hvor noen bevisst velger å omgå sikkerhetsrutiner og prosesser."[1] Dette sitatet fra Nasjonal Sikkerhetsmyndighet (NSM) beskriver godt hva sikkerhetskultur er.

Skatteetaten og Norsk Tipping har en strategisk plan om å bedre sikkerhetskultur i sine bedrifter og vil i den forbindelse etablere et årshjul hvor det skal tas i bruk ulike virkemidler for å sette fokus på sikkerhet, øke sikkerhetskompetansen, og få kontinuerlig og helhetlig fokus gjennom året. Skatteetaten og Norsk Tipping ønsker å utvikle et spill som bidrar til å oppnå disse målene. Gjennom intervju med ansatte skal vi få økt innsikt i hvilke opplæringsbehov som er til stede, og sammen med trusselbildet til bedriftene vil dette danne grunnlaget for å utarbeide godt og hensiktsmessig opplæringsmateriell.
Målgruppen for spillet er ansatte i alderen 35-45 år som ikke driver med sikkerhetsrelatert arbeid til vanlig. Grunnen til dette er at det er viktig å få alle ansatte opp på et akseptabelt nivå i forhold til informasjonssikkerhet for å redusere sannsynligheten for brukerrelaterte feil. Det betyr ikke at ansatte utenfor målgruppen ikke skal prøve spillet, men Skatteetaten og Norsk Tipping mistenker at dette er den mest utsatte gruppen hvor brukerrelaterte feil skjer.

1.2 Prosjektmål

Vi har delt prosjektmål opp i to deler, effektmål og resultatmål. Effektmål er langsiktige mål ved prosjektet. Resultatmål er det som skal være oppnådd når prosjektet er ferdig.

1.2.1 Resultatmål

- Utarbeide god og relevant opplæringsmateriell innen informasjonssikkerhet.
- Lage et brettspill der målet er å lære om informasjonssikkerhet og øke interessen for sikkerhetskultur.
- Måle effekten av opplæringen.

1.2.2 Effektmål

- Redusere risiko for ubevisste hendelser relatert til sikkerhet.
- Øke interessen for sikkerhet blant ansatte.

1.3 Rammer

Originalt så skulle det utvikles et digitalt spill. Ettersom vi ikke har kompetanse til å lage et spill som lever opp til oppdragsgiveres standard så skal vi ikke utvikle et digitalt spill, men heller et brettspill.

1.3.1 Tidsmessige rammer

- Innlevering av forprosjekt, signering av prosjektavtale og signering av gruppekontrakt skal skje innen 1. februar 2019.
- Bacheloroppgaven skal leveres 20. mai 2019

1.3.2 Økonomiske rammer

Siden oppdragsgivere holder til i Hamar og Oslo så vil det innebære transportkostnader. Vi vil stå for dette selv, men skulle det oppstå økonomiske utfordringer ved dette må vi høre med oppdragsgivere om det er mulig å få sponset turer. Materialer brukt i presentasjon av brettspillet vil være dekket av gruppemedlemmene med grense på totalt 400kr.

2 Omfang

2.1 Problemstilling

Sikkerhetskultur er en utfordring for norske bedrifter. Den økende digitaliseringen i hjem og arbeidsplass gjør det vanskelig for ansatte å følge med på dagens sikkerhetsbilde. Denne økende digitaliserginen fører med seg flere og nye trusselaktører som ønsker å utnytte digitaliseringen til egen vinning. Utfordringen for bedrifter er å holde alle ansatte bevisste på denne økende trenden, og for å beholde bedriftenes verdier må det gjøres noen tiltak. Norsk Tipping og Skatteetaten har derfor et behov for opplæring av de ansatte, og de vil produsere et brettspill med målet om at det skal være en effektiv læremåte for ansatte i målgruppen. Norsk Tipping har vært borti brettspill før da de i 1999 utga Non-Stop sikkerhetsom fikk IT-Sikkerhetsforum sin årlige sikkerhetspris i 2002 [2]. Norsk Tipping vil senere vurdere å digitalisere konseptet vi lager og bruke det i Nasjonal sikkerhetsmåned 2019 til opplæring av ansatte.
Vår problemstilling for prosjektet vil dermed være; Kan brettspill bli brukt til effektiv opplæring i sikkerhet?

2.2 Problemavgrensing

Oppgaven vil dreie seg om informasjonssikkerhet innad i Skatteetaten og Norsk Tipping, og hvordan best formidle opplæring til de ansatte ved hjelp av brettspill. En fullstendig risikoanalyse av Skatteetaten og Norsk Tipping vil ikke være en del av oppgaven, men deler av en slik prosess vil bli benyttet for å identifisere relevante punkter for opplæring. Etter å ha samlet inn informasjon om aspekter ved informasjonssikkerhet som burde bli satt mer fokus på av ansatte vil vi produsere brettspillet. Brettspillet vil fokuseres rundt de med lite tidligere kunnskap i sikkerhet. Vi vil ikke ta hensyn til de med mer kompetanse under produksjonen av spillet. Grunnen til dette er at vi fokuserer på å få alle ansatte opp på et akseptabelt nivå innen informasjonssikkerhet, og vi mener å fokusere på å opplære ansatte som driver med sikkerhet til vanlig vil være dårlig bruk av tiden vår. Spillet vi ender opp med i prosjektet vil være en prototyp brukt til konseptbevis. Vi vil holde fokus på det som er relaterer til opplæring og interessen til de ansatte og vil derfor ikke bruke mye ressurser på for eksempel det grafiske. Spillet må derfor jobbes mer med senere for å oppnå et fullstendig produkt.

3 Prosjektorganisering

3.1 Ansvarsforhold og roller

Roller

- Leder: Daniel Magnus
- Grupperomsansvarlig: Bendik Flobak
- Sekretær: Abu Baker Al-Shammari

Ansvarsforhold

- **Felles:** Alle har ansvar for å levere arbeidsoppgaver i tide. Det forventes at det som leveres skal ha en god kvalitet og være relevant i forhold til den arbeidsoppgaven som er gitt. Gruppemedlemmene har ansvar for å føre opp antall timer jobbet på oppgaver som er gitt. Hvert medlem har ansvar for å føre opp kilder til det de har brukt, leser man noe man føler er relevant må det skrives ned slik at det kan finnes igjen senere.
- **Leder:** Lederen har ansvar for å sette opp møter med gruppen, veiledere og oppdragsgivere, samt kommunikasjon mellom veiledere og oppdragsgivere. Lederen har ansvaret for å lage agenda for gruppemøter. Lederen har ansvar for å fordele arbeidsoppgaver. Dette gjøres i samarbeid med de andre gruppemedlemmene under møter. Lederen har ansvar for å løse konflikter innad i gruppen så godt det lar seg gjøre uten hjelp fra veiledere.
- **Grupperomsansvarlig:** Den ansvarlige har ansvaret for å reservere grupperom 2 uker fram i tid. Er dette ikke mulig må dette gis beskjed om til gruppelederen.
- **Sekretær:** Personen har ansvar å skrive et møtereferat, ha oversikt over intervju og dataene fra spørreundersøkelsen. Sekretæren skal også notere hva som trengs å jobbe med videre etter gruppemøter om noe mangler. Dokumentere valgene våre for å vise frem hvilke alternativer vi hadde, og hvorfor vi valgte det ene alternative fremfor de andre.

3.2 Rutiner og regler i gruppa

Grupperegler er lagt med som vedlegg, underskrevet av alle på gruppen. Rutiner i gruppen er som følger:

- Føre inn antall timer arbeid i timelisten
- Føre inn i kalenderen når personer har forelesninger, og ellers er utilgjengelig
- Møte opp til avtalt arbeidstid
- Oppdatere seg på oppgaver som ligger under "In review" på Trello før gruppemøter (Disse begrepene blir beskrevet under 5.2)

4 Planlegging, oppfølgning og rapportering

4.1 Hovedinndeling av prosjektet

Vårt prosjekt består av en gruppe på fire personer. Vi vil derfor bruke en relativt enkel systemutviklingsmodell. Erfaring fra tidligere prosjekter og etter undersøkelser av bacheloroppgaver uten programutvikling har vi valgt å bruke en hybrid variant av Scrum [3]. Scrum har enkle faser og siden vi er uerfarne med slike omfattende oppgaver og utvikling av fysisk spill ser vi en stor fordel i at vi kan gå tilbake og gjøre endringer når behovet viser seg. Dermed blir en sekvensiell modell, som for eksempel fossefallsmodellen[4], ikke egnet til vår oppgave selv om disse er enklere enn Scrum. Det er derimot viktig å ikke låse seg i en utfordrende oppgave i for lang tid da vi må ha en kontinuerlig progresjon i prosjektet. Kommunikasjon er en veldig viktig faktor for valget, siden vi har et gruppemedlem som vi kommuniserer med via internett. Sprintene våre vil vare i én uke og våre sprint-møter vil hjelpe kommunikasjonen innad i gruppen. Sprint-møtene vil også gi oss muligheten til å få oversikt over hvor langt vi har kommet og hva som må gjøres videre. Vi låner en form for pair programming da tre av fire gruppemedlemmer jobber sammen på NTNU i Gjøvik sine lokaler. Dette kan også regnes som daily scrum, men vi har ikke noe avsatt møte til gjennomgang hver dag. Planlegging og prat om det som er gjort tidligere samt gjennomgang av hverandres oppaver vil skje kontinuerlig.

Våre sprinter vil vare i én uke hver med sprint møter på mandager. Etter møtene våre vil vi

sende et referat til oppdragsgiver. Kommunikasjon med oppdragsgiver er viktig for både oss og dem, slik at de får en oversikt på hvordan vi ligger an og hva vi jobber med. Dette skaper engasjement hos begge parter og et godt samarbeid. Rollene for modellen er Product owner, Trond Laupstad og Anne Marie Øverhaug, og Scrum master, Daniel Magnus.

4.2 Plan for statusmøter

Etter hver sprint så har vi lagt inn en sprint review hver mandag, der vi går gjennom alle sammen hva hver enkelt har gjort eller ikke fått til. Vi vil samarbeide og hjelpe den enkelte om det var en oppgave som ikke har blitt løst eller var vanskelig å løse. Gruppelederen er med på å dele ut oppgaver den dagen. Alle oppgaver blir lagt til på backlog (5.2). Grupperomansvarlig har ansvaret for å reservere rom hver mandag, slik at vi kan ha møtet uten forstyrrelser. Vi bruker også Facebook eller eventuelt andre medium for å kommunisere med medlemmene om de ikke er fysisk tilstede. Sekretæren har ansvar for å loggføre hva som blir diskutert under møtet og skrive et referat slik at gruppemedlemene kan se tilbake på det. Dette referatet blir også sendt til oppdragsgiverene.

5 Organisering av kvalitetssikring

5.1 Dokumentasjon og standardbruk

Møtereferat for oppdragsgivere, veiledere og gruppen blir lagret i Google Drive[5], her vil også kalender og timeliste være tilgjengelig samt andre dokumenter som produseres av gruppen. Drivener privat og bare de som er medlem i gruppen har tillatelse til å lese og skrive filene. Sikkerhet er veldig viktig faktor for oppgaven siden vi har signert en taushetserklæring. Derfor vil lagring av sensitive dokumenter bli diskutert med oppdragsgiver for å sikre at oppdragsgiver er tilfreds med våre rutiner. Gruppens medlemmer har ansvaret for å ha To-faktor autentisering (2FA) på slik at uautoriserte personer ikke har tilgang til driven".

5.2 Konfigurasjonsstyring

Vi skriver rapporten vår i LaTeX[6], og bruker Overleaf[7] som editor. Vi vil bruke en mal laget av tidligere foreleser Simon McCallum[8], muligens med noen modifikasjoner der vi ser det nødvendig.

Rapporten som opprettes i Overleaf er privat og deles til gruppens medlemmer via dens unike web-link (kun kjent for eier av dokumentet og de som eier har delt linken med). Dette gjør at alle kan jobbe på samme dokument og sikrer at det alltid vil være siste versjon av rapporten som hentes opp og jobbes med. Overleaf benytter Amazon S3 til lagring av data (Amazon utfører backup av data)[9] For å sikre rask gjenoppretting ved eventuelle tap av informasjon eller tilgjengelighet til rapport, tas det backup i form av kopi av rapporten etter endt dag, denne lagres lokalt hos en av gruppemedlemmene.

Trello[10] blir brukt for å få oversikt over av oppgavene, hvem som jobber med hva og hva som er blitt gjort og ikke gjort. Det er bare gruppemedlemmene som har tilgang til Trello. De kan skrive, endre, kommentere eller slette oppgaver. De forskjellige kategoriene på Trello er Backlog, In progress, In review og Done.

- **Backlog** - Samling av mindre oppgaver som skal utføres i løpet av en periode.
- **In progress** - En oppgave som det jobbes med tilegnes en eller flere gruppemedlem.
- **In review** - Når et utkast av en oppgave er ferdig blir dette sjekket i denne fasen av de andre gruppemedlemmene.
- **Done** - Når alle gruppemedlemmene har blitt tilfreds med det nåværende utkastet.

5.3 Risikoanalyse

Sannsynlighet	Konsekvens				
	Ufarlig	Mindre farlig	Farlig	Kritisk	Katastrofalt
Usannsynlig			5		1
Lite sannsynlig			2 6	4	7
Sannsynlig				3	
Ganske sannsynlig					
Svært sannsynlig					

Figur 1: Risikomatrise

Oppsettet av tabellene har vi valgt å ha med:

- **Risikonummer** - Nummeret som representerer risikoen i tabellen over
- **Risikoscenario** - En kort beskrivelse av risikoscenario
- **Sannsynlighet** - Sannsynlighet fra 1 (usannsynlig) til 5 (svært sannsynlig)

- **Konsekvens** - Konsekvens fra 1 (ufarlig) til 5 (katastrofalt)
- **Samlet risiko** - Plasseres i risikotabellen over. Sannsynlighet vertikalt og konsekvens horisontalt

Tabellene under har verdiene K (konsekvens), S (sannsynlighet) og samlet risiko som er basert på figur 1 over. Risikomatrisen vil ikke benytte score for samlet risiko da matrisen ikke er symmetrisk, som resulterer i gap i rangeringen vår. For eksempel vil Sannsynlig-Katastrofalt være rangert høy, men Svært sannsynlig-Farlig er rangert middels selv om de har samme score. Forklaring på de følgende fargene i matrisen:

- **Grønn:** Lav risiko for gruppen og prosjektet.
- **Gul:** Middels risiko for gruppen og prosjektet.
- **Rød:** Høy risiko for gruppen og prosjektet.

Tabell 1: Scenario 1

Risikonummer	1
Risikoscenario	Dokumenter forsvinner, slettet eller fjernet
Sannsynlighet	1
Konsekvens	5
Samlet risiko	Middels

5.3.1 Tiltak - Dokumenter forsvinner, slettet eller fjernet

Vi vil ta backup av LaTeX-dokumentet i Overleaf daglig, etter endt arbeid. Drive blir brukt hovedsaklig til deling av dokumenter mellom gruppemedlemmene. Kritiske dokumenter for prosjektet skal opprettes på en lokal maskin av et gruppemedlem før det deles slik at det er lagret lokalt.

Tabell 2: Scenario 2

Risikonummer	2
Risikoscenario	Gruppemedlem kan ikke møte på grunn av sykdom eller har et langtidsfravær
Sannsynlighet	2
Konsekvens	3
Samlet risiko	Lav

5.3.2 Tiltak - Gruppemedlem fravær

Ved planlagt fravær må det meldes fra i god tid slik at oppgaver kan eventuelt delegeres. Ved sykdom må det meldes fra så fort som mulig. Det blir da opp til resten av gruppen å gi denne personen oppgaver å løse hjemmefra, dersom dette lar seg gjøre.

Tabell 3: Scenario 3

Risikonummer	3
Risikoscenario	For lite kontakt med oppdragsgiver eller tredjepart
Sannsynlighet	3
Konsekvens	5
Samlet risiko	Middels

5.3.3 Tiltak - Lite kontakt med arbeidsgiver eller tredjepart

Vi vil holde oppdragsgiverne oppdatert om vår fremgang i prosjektet slik at de føler seg mer involvert og investert i prosjektets utførelse. Dersom vi skulle miste kontakt med oppdragsgiver er vår kontinuitetsplan å gjennomføre spilltesten på studenter ved NTNU i Gjøvik som har liten erfaring med sikkerhet.

Tabell 4: Scenario 4

Risikonummer	4
Risikoscenario	Flere undersøkelser gjør at vi havner bak tidskjemaet
Sannsynlighet	2
Konsekvens	4
Samlet risiko	Middels

5.3.4 Tiltak - Havne bak tidsskjema

Vi vil be oppdragsgiverne om å finne folk som vil være tilgjengelige på datoen vi tester spillet. Disse vil da forhåpentligvis si seg enig i å delta i denne øvelsen. Vi håper at dette vil gi dem insentiv til å svare på undersøkelsene.

Tabell 5: Scenario 5

Risikonummer	5
Risikoscenario	Et gruppemedlem forlater gruppen
Sannsynlighet	1
Konsekvens	3
Samlet risiko	Lav

5.3.5 Tiltak - Gruppemedlem forlater gruppen

Viktig med god kommunikasjon i gruppen. Sørge for at alle føler at de gjør arbeid som er viktig i forhold til oppgaven. Være flinke til å engasjere hverandre og håndtere situasjoner som kan skape konfliker på en god måte.

Tabell 6: Scenario 6

Risikonummer	6
Risikoscenario	Kommunikasjon innad i gruppen er manglende
Sannsynlighet	2
Konsekvens	3
Samlet risiko	Lav

5.3.6 Tiltak - Manglende kommunikasjon i gruppen

Vi kommuniserer på facebook angående alt relatert til oppgaven. Trello blir benyttet til fordeling av oppgaver. Det blir ukentlige videomøter med hele gruppen, ett på mandag og ett på fredag under veiledningstime. Flere videomøter blir planlagt dersom det er nødvendig.

Tabell 7: Scenario 7

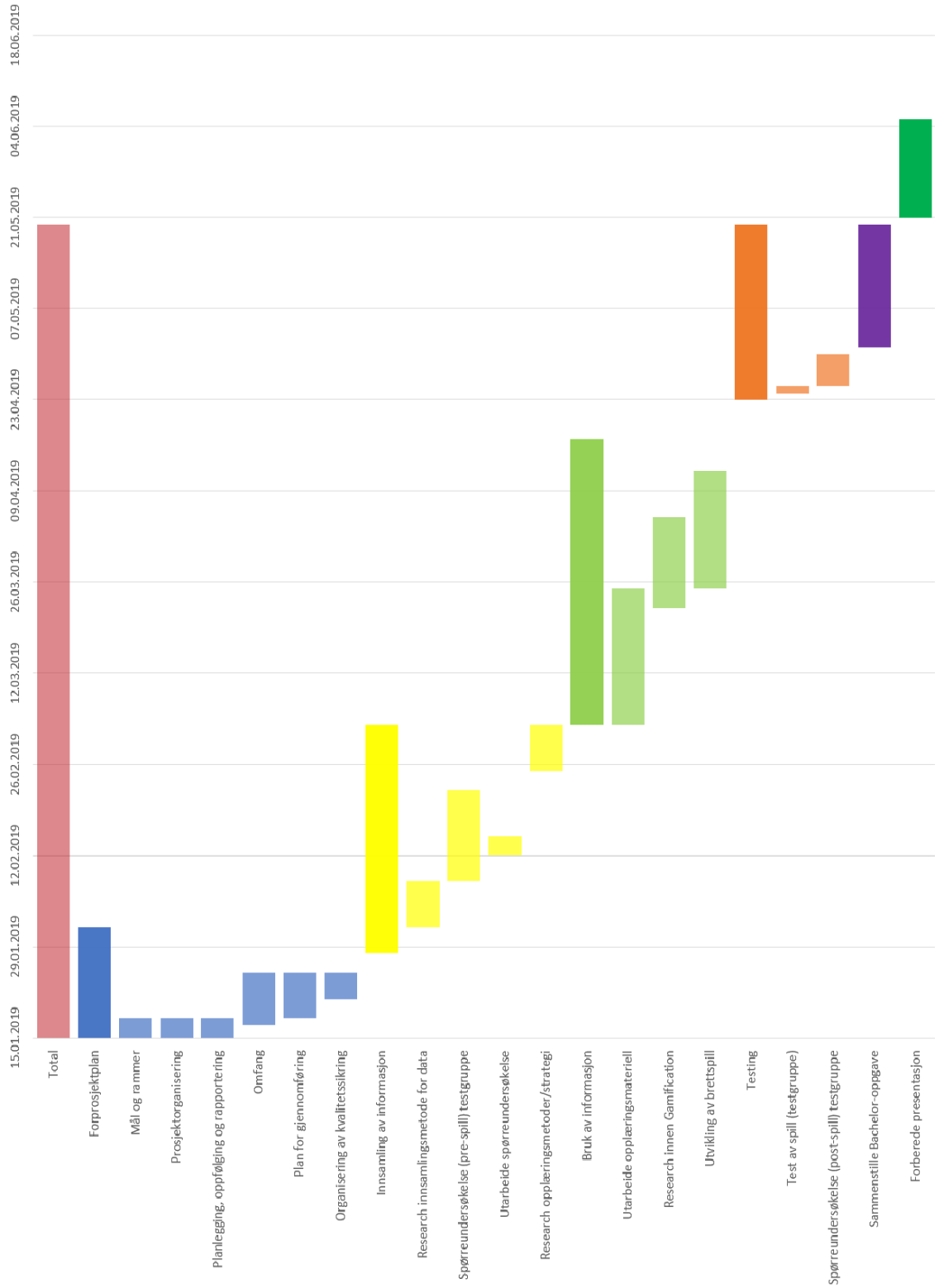
Risikonummer	7
Risikoscenario	Integriteten for resultatet er manglede
Sannsynlighet	2
Konsekvens	5
Samlet risiko	Middels

5.3.7 Tiltak - Integriteten for resultatet er manglede

Det er viktig å ha en god dialog med oppdragsgivere. De må vite hvor viktig det er for alle parter at de ansatte som blir intervjuet svarer sant. Dette kan vi gjøre ved å skape en personlig kobling til de ansatte og forsikre dem om at svarene er anonyme for alle andre utenom oss som utfører intervjuet.

6 Plan for gjennomføring

6.1 GANTT-skjema



6.2 Tid og ressursplan

Tid og ressursplanen er den tabellen GANTT-skjemaet er basert på. Her ser man med datoer hvor lang tid vi skal bruke på forskjellige oppgaver gjennom prosjektet (Lengde = antall dager). Det vi vil presisere her er at vi kontinuerlig skriver på bacheloroppgaven. Det som står i linje nr. 26 **Sammenstille Bachelor-oppgave** vil innebære analyse av pre- og posttest samt rettskrivning og tilbakemelding fra veiledere og oppdragsgivere.

5	Aktivitet	Ansvarlig	STARTDATO	SLUTTDATO	LENGDE
6	Total		07.01.2019	20.05.2019	133
7	**Forprosjektplan**		07.01.2019	01.02.2019	25
8	Mål og rammer		14.01.2019	18.01.2019	4
9	Prosjektorganisering		14.01.2019	18.01.2019	4
10	Planlegging, oppfølging og rapportering		15.01.2019	18.01.2019	3
11	Omfang		17.01.2019	25.01.2019	8
12	Plan for gjennomføring		18.01.2019	25.01.2019	7
13	Organisering av kvalitetssikring		21.01.2019	25.01.2019	4
14	**Innsamling av informasjon**		28.01.2019	04.03.2019	35
15	Research innsamlingsmetode for data		01.02.2019	08.02.2019	7
16	Spørreundersøkelse (pre-spill) testgruppe		08.02.2019	22.02.2019	14
17	Utarbeide spørreundersøkelse		12.02.2019	15.02.2019	3
18	Research opplæringsmetoder/strategi		25.02.2019	04.03.2019	7
19	**Bruk av informasjon**		04.03.2019	17.04.2019	44
20	Utarbeide opplæringsmateriell		04.03.2019	25.03.2019	21
21	Research innen Gamification		22.03.2019	05.04.2019	14
22	Utvikling av brettspill		25.03.2019	12.04.2019	18
23	**Testing**		23.04.2019	20.05.2019	27
24	Test av spill (testgruppe)		24.04.2019	25.04.2019	1
25	Spørreundersøkelse (post-spill) testgruppe		25.04.2019	30.04.2019	5
26	**Sammenstille Bachelor-oppgave**		01.05.2019	20.05.2019	19
27	**Forberede presentasjon**		21.05.2019	05.06.2019	15

6.3 Milepæler og beslutningspunkter

Basert på GANTT-skjemaet har vi da noen konkrete milepæler:

- **1. Februar:** Innlevering av forprosjektrapport.
- **22. Februar:** Spørreundersøkelser er ferdigstilt og sendt av gårde. Vi vil etterspørre svar på undersøkelsene innen 1. Mars.
- **15. April:** Kravspesifikasjon, research og utvikling av spill. Dersom vi her ikke har fått inn tilstrekkelig svar på undersøkelsene vil vi bruke inspirasjon fra kilder. Her vil vi også vurdere om/hvor mye vi må jobbe i påsken. Her skal også research om statistikk være ferdig.
  Vi har som mål å ha skrevet mesteparten av bacheloroppgaven på dette tidspunktet så vi kan få tilbakemelding fra veiledere og oppdragsgivere.
- **22. April:** Påskeferiens slutt, vi vil planlegge en dato for testing av spillet så fort som mulig etter denne datoen.
- **20. Mai:** Rapporten leveres inn, før dette skal analyse av testene, drøfting rundt funn, og rapporten i sin helhet være ferdig.

Akronymer

2FA To-faktor autentisering. 7

NSM Nasjonal Sikkerhetsmyndighet. 2

Referanser

[1] N. Sikkerhetsmyndighet, “Sikkerhetskultur,” https://www.nsm.stat.no/om-nsm/tjenester/sikkerhetsstyring/sikkerhetskultur/, (Besøkt 06.02.2019).

[2] E. Rossen, “Norsk tipping fikk it-sikkerhetspris,” https://www.digi.no/artikler/norsk-tipping-fikk-it-sikkerhetspris/304627, (Besøkt 17.01.2019).

[3] Wikipedia, “Scrum,” https://no.wikipedia.org/wiki/Scrum, (Besøkt 06.02.2019).

[4] ——, “Waterfall model,” https://en.wikipedia.org/wiki/Waterfall_model, (Besøkt 06.02.2019).

[5] ——, “Google drive,” https://no.wikipedia.org/wiki/Google_Drive, (Besøkt 06.02.2019).

[6] ——, “Latex,” https://no.wikipedia.org/wiki/LaTeX, (Besøkt 06.02.2019).

[7] Overleaf, “About us,” https://no.overleaf.com/about, (Besøkt 06.02.2019).

[8] S. McCallum, “Bachelor thesis template (ntnu),” https://github.com/COPCSE-NTNU/bachelor-thesis-NTNU, (Besøkt 18.01.2019).

[9] Overleaf, “Overleaf privacy terms overview,” https://www.overleaf.com/legal#Security, (Besøkt 23.01.2019).

[10] Trello/Atlassian, “Reading from the web,” https://trello.com/tour, (Besøkt 06.02.2019).

Vedlegg

A Grupperegler

Grupperegler

- Oppgaver skal distribueres på alle medlemmer. Om du har gjennomført en oppgave som ligger i backloggen på Trello skal denne flyttes til review. Da skal andre i gruppen lese det du har skrevet og gjøre seg kjent med innholdet. Om det ikke er tilfreds-stillende så flyttes gjøremålet tilbake til backloggen og du må prøve å gjøre innholdet ditt bedre eller spørre om hjelp av andre gruppemedlemmer.
- Det forventes at alle møter opp til alle møter om de ikke har meldt ifra at de ikke kan i forveien.
- Det er også viktig å presisere at gruppens medlemmer aktivt må spørre og bidra til at gjøre-mål lages.
- Det forventes at diskusjonene i gruppemøtene og på gruppechatten skal være saklig, og uten personangrep.
- Det forventes at alle gruppemedlemmene stiller forberedt til felles møter.
- Fravær skal meldes ifra meldes ifra så tidlig som mulig. Dette gjøres som innlegg på Facebook gruppen.
- Det forventes at man møter opp til møter i tide.
- Ved møte over internett, i.e., skype/facebook, forventes det at vedkommende er tilgjengelig 5 minutter før møtestart.
- Det forventes at gruppemedlemmer jobber minst 30 timer i uken.
- Gruppemedlemmer må føre inn timer i timelisten som ligger på Google Docs.

Konsekvenser

- Forsenkomming: Er man ikke tilstede på møtet før møtestart vil vedkommende få en advarsel.
- Møter man ikke opp til faste møter, uten å gi beskjed, vil vedkommende få 2 advarsler.
- Dersom gruppens medlemmer ikke leverer arbeidsoppgaver vil det bli diskutert og stemt i gruppemøter om vedkommende har tatt på seg for mye arbeid til gitt tidsrom og om det skal gis advarsel. Dersom avstemming er likt vil gruppeleder sin stemme telle dobbelt.

Brettspillbasert opplæring i informasjonssikkerhet

NTNU

Kunnskap for en bedre verden