NTNU
Norwegian University of
Science and Technology

En case-studie på bruk av rotårsaksanalyse innen informasjonssikkerhet

Forfattere
Thomas Havnegjerde Huse
Philip Brugmans Nyblom
Ole Martin Søgnen
Fredrik Løvaas Theien

Bachelor i informasjonssikkerhet
20 ECTS
Institutt for informasjonssikkerhet og kommunikasjonsteknologi
Norges teknisk-naturvitenskapelige universitet,

16.05.2018

Veileder Tom Røise

Sammendrag av Bacheloroppgaven

Tittel:	**En case-studie på bruk av rotårsaksanalyse innen informasjonssikkerhet**
Dato:	16.05.2018
Deltakere:	Thomas Havnegjerde Huse Philip Brugmans Nyblom Ole Martin Søgnen Fredrik Løvaas Theien
Veiledere:	Tom Røise
Oppdragsgiver:	Seksjon for Digital Sikkerhet, NTNU
Kontaktperson:	Gaute Wangen, gaute.wangen@ntnu.no, +47 907 08 338
Nøkkelord:	Rotårsaksanalyse, Informasjonssikkerhetsstyring, Case-studier
Antall sider:	171
Antall vedlegg:	11
Tilgjengelighet:	Åpen

Sammendrag:

Vanlig tilnærming til informasjonssikkerhetsstyring er gjennom risikostyring og hendelseshåndtering. Rotårsaksanalyse (RCA) skiller seg fra disse ved å gå i dybden på problemet og fjerne det ved rota. Siden denne tilnærmingen er lite brukt i informasjonssikkerhet, er en av våre problemstillinger å utrede hvor godt det fungerer. Tilnærmingen til dette var gjennom tre caser som omhandler ulike aspekter ved informasjonssikkerhet. Disse var å undersøke rotårsaken til: ulovlig fildeling ved NTNU, kompromitterte kontoer ved NTNU og misbruk av NTNU sine ressurser til utvinning av kryptovaluta. RCA består av forskjellige metoder og tilnærminger, men denne rapporten tar utgangspunkt i boken "Root Cause Analysis: Simplified Tools and Techniques" [1]. Resultatene fra første case viser at det er i stor grad tilgjengeligheten på tjenester som har noe å si for hvorfor de laster ned. I caset om kompromitterte kontoer viser vår undersøkelse at det er en kombinasjon av dårlig opplæring og utilstrekkelig tilgangskontroll som er rotårsakene. Grunnen til at folk velger å misbruke NTNU sine ressurser til kryptoutvinning kan tilskrives uklarheter i IT-reglement, samt lav prioritering fra Seksjon for Digital Sikkerhet. Etter utføringen av de tre casene ble det konkludert med at metodikken fungerer bra, men at noen verktøy fungerer bedre enn andre. Rapporten inkluderer derfor også en veileder for bruk av RCA innen informasjonssikkerhet – skrevet på bakgrunn av erfaringer fra dette bachelorprosjektet.

Summary of Graduate Project

Title:	**A case study on the use of root cause analysis in information security**
Date:	16.05.2018
Authors:	Thomas Havnegjerde Huse Philip Brugmans Nyblom Ole Martin Søgnen Fredrik Løvaas Theien
Supervisor:	Tom Røise
Employer:	The Digital Security Section, NTNU
Contact Person:	Gaute Wangen, gaute.wangen@ntnu.no, +47 907 08 338
Keywords:	Root Cause Analysis, Information Security Management, Case studies
Pages:	171
Attachments:	11
Availability:	Open

Abstract:

Common approach for information security management is either risk management or incident response. Root cause analysis (RCA) differs from these by identifying root causes and removing them. Since the approach is not often used in information security, one of our topics is to determine how well this approach works. To accomplish this, we looked at three cases tackling various aspects of information security. The cases were as following: illegal filesharing at NTNU, compromised accounts at NTNU and misuse of NTNU's resources to mine cryptocurrency. RCA is a collection of various methodologies and tools, however this report follows the methodology and tools presented in "Root Cause Analysis: Simplified Tools and Techniques" [1]. The results from the first case shows that it is largely the lack of availability that is the main reason for why students choose to download. In the case about compromised accounts we discovered that poor training and insufficient access control were the main causes. The reasons for why people chose to abuse NTNU's resources for cryptomining can be attributed to the ambiguities in the IT Policy of NTNU, as well as low priority from the Digital Security Section. Following the completion of the three cases, it was concluded that the methodology works well, but some tools works better than others. Therefore, the report also includes a guideline for using RCA in information security - written based on our experiences from this bachelor project.

Forord

Denne oppgaven er vår avsluttende bacheloroppgave i informasjonssikkerhet ved NTNU i Gjøvik. Oppgaven tar for seg bruksområder for rotårsaksanalyse innen informasjonssikkerhet.

Vi vil gjerne benytte anledningen til å takke vår veileder, Tom Røise, for godt samarbeid og gode veiledninger i løpet av prosjektperioden. Han stilte opp på møte hver uke, og det setter vi pris på. Vi vil også takke vår kontaktperson fra oppdragsgiver, Gaute Wangen, for å stille opp på møter når vi har trengt det. Han har også vært svært hjelpsom med teorien underveis. Takk til Christoffer Vargtass Hallstensen som har vært en verdifull kilde til informasjon angående oppgaven. Tilslutt vil vi takke alle som deltok på utgitte spørreundersøkelser og de som bidro på andre måter.

Innhold

Figurer

Tabeller

Akronymer og begreper

Akronymer

RCA står for Root Cause Analysis, og er en metode for problemløsning.

ROS står for Risiko- og sårbarhetsanalyse, og er en metode for å analysere risikoer og innføre tiltak for å føre dem ned til et akseptabelt nivå.

HPC står for High Performance Computing, og er gjerne snakk om en regneklynge med høy ytelse, også kjent som en superdatamaskin.

BYOD står for Bring Your Own Device, og innebærer alle enheter du tar med deg til jobb eller universitet og bruker der.

DNS står for Domain Name System og er en tjeneste som brukes for å oversette mellom domenenavn og IP-adresse på internett.

DHCP står for Dynamic Host Configuration Protocol, og brukes for å dynamisk tildele IP-adresser på en nettverk etter behov.

ISMS står for Information Security Management System, og er et system for å behandle og sette krav til ulike aspekter ved informasjonssikkerhet.

IAM står for Identity and Access Management, og er et system som behandler og autoriserer dine autentiseringsdata. Brukes også til å sette krav til passord.

SOC står for Security Operation Center, og er en sentralisert enhet som behandler sikkerhetshendelsen i en organisasjon.

2FA står for to-faktor autentisering og brukes når man snakker om to autentiseringsfaktorer, som for eksempel passord og kodebrikke.

VPN står for Virtual Private Network, dette gir en kryptert forbindelse til en server. Dette får det til å se ut som PCen kommer fra samme lokasjon som serveren.

Begreper

Rotårsak Er den underliggende årsaken som leder til et synlig problem. Årsaker har ofte et forløp hvor flere årsaker inngår, rotårsaken er den første og utløseren til denne kjeden.

Aktiva er et regnskapsmessig uttrykk for eiendeler eller rettigheter som har formueverdi.

Case er en enhet, og brukes gjerne som en case-studie, som betyr studie av en enhet eller et tilfelle.

Signifikans er et begrep som brukes for å beskrive sannsynligheten for at noe er et resultat av tilfeldigheter [2].

Konfidensinterval er en måte å angi feilmarginen av en måling eller en beregning på. Et konfidensintervall angir intervallet som med en spesifisert sannsynlighet inneholder den sanne (men vanligvis ukjente) verdien av variabelen man har målt [3].

Peer-to-peer er en betegnelse på en måte å organisere ressursdeling på. I denne rapporten snakker vi spesifikt om fildeling.

Symptom brukes i denne rapporten om en indikasjon på at et problem eksisterer. Et symptom kan i denne sammenhengen være notifikasjoner om brudd på opphavsrett, tap av omløpsmidler eller sikkerhetsvarsler.

Sit er studentsamskipnaden til NTNU i Trondheim, Gjøvik og Ålesund.

1 Introduksjon

Formålet med dette kapittelet er å introdusere prosjektet. Det gis en kort beskrivelse av bakgrunnen til prosjektet, deretter presenteres forskningsspørsmålene. Vi beskriver også vår motivasjon for oppgaven, forhåndsbestemte rammer og hvilke avgrensninger vi satt underveis. Helt til slutt inneholder dette kapittelet en oversikt over prosjektmål og en kort oversikt over hva rapporten inneholder.

1.1 Bakgrunn og introduksjon

Root Cause Analysis (RCA) er en metode for problemløsning som brukes for å identifisere rotårsaken til et problem. RCA er et lite brukt verktøy innen informasjonssikkerhet, men er av økende betydning. Vanlig tilnærming til informasjonssikkerhetsstyring er å utføre en risiko-og sårbarhetsanalyse (ROS-analyse) for så å gjennomføre tiltak som fører risikoene til et akseptabelt nivå. En annen hyppig brukt tilnærming er hendelseshåndtering der en planlegger hvordan det skal responderes på hendelser etter de er inntruffet. Rotårsaksanalyse skiller seg fra disse ved å gå i dybden på problemet, kartlegge hvilke rotårsaker som står bak, og innføre tiltak for å fjerne årsakene helt.

I dette prosjektet tar vi for oss rotårsaksanalysemetodikk og ser på hvordan det fungerer innenfor informasjonssikkerhet.

1.2 Problemstilling

Problemstillingen for dette prosjektet er todelt. Den ene delen skal dreie seg om bruk av metode og verktøy for å finne frem til rotårsaken for tre ulike caser. Hvert case omfatter en hendelse eller et problem NTNU har, som de ønsker å eliminere. De tre problemene er som følger:

1. Ulovlig fildeling på universitetsnettet til NTNU
2. Kompromitterte brukerkontoer ved NTNU
3. Misbruk av NTNU sine ressurser til utvinning av kryptovaluta

I tillegg til dette har vi en hovedproblemstilling knyttet til alle tre casene hvor vi redegjør for hvordan rotårsaksanalyse kan brukes innenfor informasjonssikkerhet. Denne vurderingen gjøres etter gjennomføring av casene for å se hvordan metoden og verktøyene fungerte. Dette dokumenteres til senere bruk.

Fra de tre casene skal vi bruke dokumentasjon og erfaringer til å utarbeide en veileder for gjennomføring av rotårsaksanalyse i informasjonssikkerhetssammenheng. Dette dokumentet skal inneholde informasjon om metode, fremgangsmåte og dokumentasjon av verktøy som fungerer bra i denne sammenhengen. Dokumentet skal kunne brukes aktivt av fagmiljøet når det skal utføres ytterligere rotårsaksanalyser. Derfor vil veilederen inneholde deler fra hovedrapporten. Dette dokumentet skal kunne være en selvstendig veileder.

I rapporten ønsker vi å redegjøre følgende forskningsspørsmål:

- Hva er rotårsaken til at studenter laster ned opphavsrettsbeskyttet materiale?
- Hva er rotårsaken til at brukerkontoer ved NTNU blir kompromittert?
- Hva er rotårsaken til misbruk av NTNU sin infrastruktur til utvinning av kryptovaluta?
- Hvor godt fungerer rotårsaksanalyse innen informasjonssikkerhet?
- Lønner det seg å benytte rotårsaksanalyse i informasjonssikkerhetssammenheng?
- Hvilke verktøy som ofte brukes i rotårsaksanalyse, fungerer best innen informasjonssikkerhet?

1.3 Motivasjon

Oppdragsgiver ønsker å få en bedre forståelse for bruk av rotårsaksanalyse innen informasjonssikkerhet, og eliminere problemer tilknyttet oppdragsgivers ansvarsområder [1]. Prosjektet skal bistå til økt forståelse ved å undersøke verktøy- og metodebruk fra RCA innenfor Seksjon for Digital Sikkerhet sitt fagfelt. Prosjektet skal presentere en tiltaksplan som eliminerer noen av problemene oppdragsgiver har i sitt ansvarsområde. En motivasjon er derfor økt tilgang på ressurser i form av arbeidskraft for å løse problemer.

Motivasjonen vår innebærer et ønske om økt kompetanse knyttet til risikoer og hendelser, og metodebruk for å håndtere disse. Vi ønsket dermed en oppgave som var styringsrelatert fremfor teknisk. Denne oppgaven handlet om noe som for oss var en ny tilnærming til informasjonssikkerhetsstyring. Vi ønsket derfor å være med å vurdere bruken av RCA i informasjonssikkerhet og om det burde benyttes i tillegg til ROS-analyse og hendelseshåndtering.

1.4 Rammer

Her defineres de forhåndsbestemte rammene som er satt.

- Prosjektet skal være aktivt i perioden 8. januar til 16. mai.
- Prosjektet er delt inn i tre hendelser som skal analyseres.
- Kommunikasjon med de ansatte foregår via oppdragsgiver.

1.5 Avgrensing

Innen rotårsaksanalyse finnes det flere verktøy og metoder, men på grunn av anbefalinger fra oppdragsgiver avgrenser vi oss til metoden og verktøyene beskrevet i boka “Root Cause Analysis: Simplified Tools and Techniques - second edition” av Bjørn Andersen og Tom Fagerhaug [1]. Generelt for prosjektet vil vi følge føringer fra Seksjon for Digital Sikkerhet.

Spesielt for hvert case gjelder:

Case 1: Caset avgrenses til studenter i Gjøvik som leier studenthybel fra Sit. Datainnsamlingen inkluderer ikke ansatte.

Case 2: Informasjonsinnsamlingen avgrenses til kun 167 personer av de som har blitt kompromittert.

Case 3: Ingen.

[1] Dette inkluderer blant annet: internett ved Sit Bolig, brukerkontoer ved NTNU og infrastrukturen til NTNU

1.6 Prosjektmål

Målet for prosjektet er å gå i dybden på tre ulike caser som hver omhandler en unik hendelse eller et problem NTNU har. Prosjektmålene deles inn i effektmål og resultatmål.

1.6.1 Effektmål

Effektmålene er det oppdragsgiver ønsker å oppnå med oppgaven og rapporten etter den er utredet og levert.

- Eliminere problemene beskrevet i de tre casene helt eller delvis ved implementering av tiltak beskrevet i rapporten
- Økt forståelse for bruk av RCA i informasjonssikkerhet
- Finne ut hvor fordelaktig det er å bruke RCA i informasjonssikkerhet og hvilke verktøy som fungerer best til dette

1.6.2 Resultatmål

Resultatmålene beskriver det prosjektet skal oppnå i det prosjektperioden er over, og oppgaven er utført og levert.

- Alle tre caser er ferdig utført
- En oversikt over hovedfunn fra tre caser med RCA
- Dokumentere bruk av RCA i informasjonssikkerhet, med forklaringer og konkluderinger av metode og verktøy
- Redegjørelse for hvor godt rotårsaksanalyse fungere innen informasjonssikkerhet, og om det lønner seg

1.7 Organisering av rapporten

Prosjektrapporten inneholder 11 kapitler i tillegg til vedlegg. Som vedlegg inkluderes delrapportene fra hvert case.

Kapittel 1: Introduksjon inneholder innledende informasjon om prosjektets helhet.

Kapittel 2: Casebeskrivelser inneholder detaljert oppgavebeskrivelse av hvert case vi skal analysere.

Kapittel 3: Teori inneholder bakgrunn og tidligere arbeid med rotårsaksanalyse, samt sammenlikning med eksisterende metodikk innen informasjonssikkerhet.

Kapittel 4: Metode inneholder beskrivelse av metoden vi benyttet når vi skulle tilnærme oss rotårsaksanalyse av informasjonssikkerhetshendelser. Kapittelet beskriver alle fasene i prosessen, samt verktøyene som ble benyttet.

Kapittel 5: Gjennomføring av metode inneholder en gjennomgang av valg av verktøy i hver fase, ulike spesifiseringer vi la til grunn og hvordan vi gjennomførte metoden i de ulike casene.

Kapittel 6: Resultater og analyse fra Case 1: Ulovlig fildeling på universitetsnettet til NTNU inneholder resultatene i hver fase fra det første caset.

Kapittel 7: Resultater og analyse fra Case 2: Kompromittertebrukerkontoer ved NTNU inneholder resultatene i hver fase fra det andre caset.

Kapittel 8: Resultater og analyse fra Case 3: Misbruk av NTNU sin infrastruktur til utvinning av kryptovalu inneholder resultatene i hver fase fra det tredje caset.

Kapittel 9: Diskusjon inneholder drøfting av empirien. Her stiller vi kritiske spørsmål til det materiale som er presentert tidligere i rapporten og sammenligner med omverdenen om mulig.

Kapittel 10: Veileder for bruk av RCA i informasjonssikkerhet inneholder en veileder vi har utarbeidet for bruk av RCA-metode og verktøy innen informasjonssikkerhet, på bakgrunn av våre erfaringer gjennom de tre casene.

Kapittel 11: Konklusjon inneholder en konklusjon av problemstillingen og de forskningsspørsmålene som ble satt i starten av rapporten. Her kommer en oppsummering av de viktigste funnene satt i et helhetsperspektiv, samt forslag til videre arbeid.

2 Casebeskrivelser

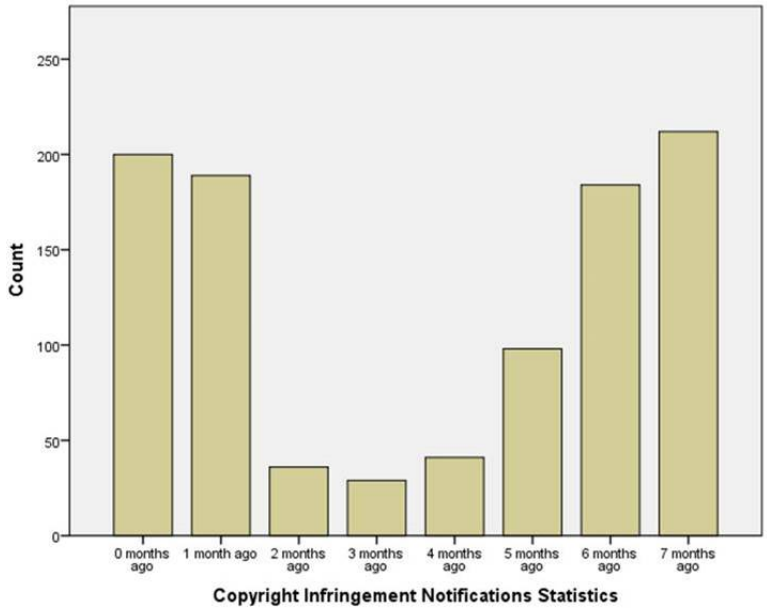
I dette kapittelet gir vi en detaljert beskrivelse av hvert case som gjennomføres.

2.1 Case 1: Ulovlig fildeling på universitetsnettet

NTNU har ansvar for nettet hos studenthyblene studentene leier fra Sit. Når studenter driver med ulovlig fildeling fra hybelen vil NTNU kunne holdes ansvarlig. Dette er et problem for NTNU, ikke bare i form av skadet omdømme, men det kan også være problematisk hvis opphavsrettshaverne går juridisk til verks. Oppgaven i dette caset er derfor å finne, ved hjelp av rotårsaksanalysemetodikken, rotårsaken(e) til hvorfor studenter laster ned opphavsrettsbeskyttet materiale. Det skal også presenteres en tydelig tiltaksplan for å eliminere rotårsaken(e).

Oversikt over oppgaven

Advokater til diverse filmselskaper ser etter IP-adresser til personer som laster ned opphavsrettsbeskyttede materiale, og sender disse personene notifikasjoner på e-post. Hver måned får NTNU ca. 150 og 200 unike notifikasjoner om brudd på opphavsretten ved ulovlig fildeling. Vi kan se at dette nummeret går kraftig ned i sommermånedene, som kan tilsi at studentene er hovedgrunnen til bruddene på opphavsrett. Disse tallene kan vi se i figur 1 under.



Figur 1: Oversikt over antall notifikasjoner i sommerhalvåret

Dersom opphavsrettshaverne begynner å håndheve opphavsretten i brevene de sender, kan NTNU komme i en dårlig posisjon. I dag gjør ikke NTNU noe med de mange

brevene de får, grunnet de store mengdene og at det er en fulltidsjobb i seg selv å håndtere dem.

Ulovlig fildeling foregår som regel ved hjelp av en protokoll som heter BitTorrent, som bruker peer-to-peer teknologi. Universitetet har per dags dato ikke mulighet til å blokkere denne, da protokollen også innebærer legitimt bruk. NTNU kan heller ikke overvåke de som laster ned ulovlig, og sperre nettet til disse. Datatilsynet har gitt beskjed til Seksjon for Digital Sikkerhet at studenthyblene må regnes som privat sfære, og dermed ikke sperre netttet fordi det blir regnet som inngrep i deres privatliv [1].

I caset avgrenser vi oss til NTNU Gjøvik, og ser bare på nettverket til de ulike studentbyene tilknyttet Sit Bolig. Nettet på campus faller ikke under problemstillingen, da universitetet kan overvåke dette. Universitetsnettet blir ikke regnet som privat sfære og brukere må holde seg til IT-reglementet, som gjør at Seksjon for Digital Sikkerhet kan sperre nettet til de som laster ned ulovlig.

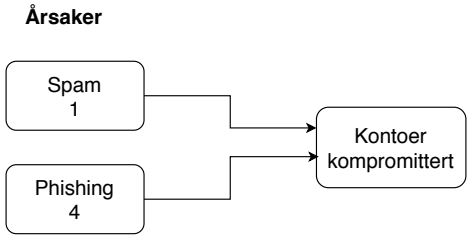
2.2 Case 2: Kompromitterte brukerkontoer ved NTNU

NTNU er et stort universitet med mange ansatte. NTNU er derfor et mål for aktører med ondsinnede hensikter. En av disse hensiktene er å få tilgang til brukerkontoer. Disse kontoene blir brukt til mye forskjellig. De brukes ofte for spam, innhenting av store mengder forskningsartikler og videre salg. Måten disse kontoene kommer på avveie er uvisst, men noen av hypotesene innebærer phishing og gjenbruk av brukernavn og passord på nettsider som har blitt kompromittert. Caset bygger på en konklusjon for videre arbeid i en tidligere rapport om rotårsaksanalyse innen informasjonssikkerhet [4]. Vår oppgave er dermed å bruke rotårsaksanalyse til å finne og presentere tiltak som eliminerer rotårsaken til at kontoer ved NTNU blir kompromittert.

Oversikt over oppgaven

I 2017 var kompromitterte kontoer alene årsaken til omtrent 70 sikkerhetshendelser ved NTNU. NTNU har siden 2005 fått 5415 kontoer kompromittert. Disse kontoene ble funnet i en stor datadump i desember 2017. Av disse 5415 kontoene var 101 av dem fremdeles aktive. Det vil si at brukernavn og passord fortsatt var gyldige innloggingskredentialer da de ble avdekket.

Universitetet kjenner bare årsakene til kompromitteringene i 5 av tilfellene. Phishing sto for fire og spam for en av hendelsene.

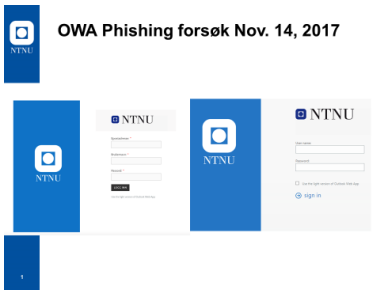


Figur 2: Kjente årsaker til kompromittert konto

Phishing er en av de få årsakene vi har data på, så det er en av årsakene vi vil holde fokus på i analysen. Bildet under viser eksempler på phishing e-post som har blitt sendt

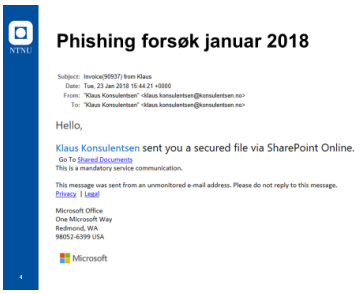
[1] Informasjon fra oppdragsgiver

til ansatte ved NTNU.



(a) Forsøk fra November 2017

(b) Forsøk fra Januar 2018

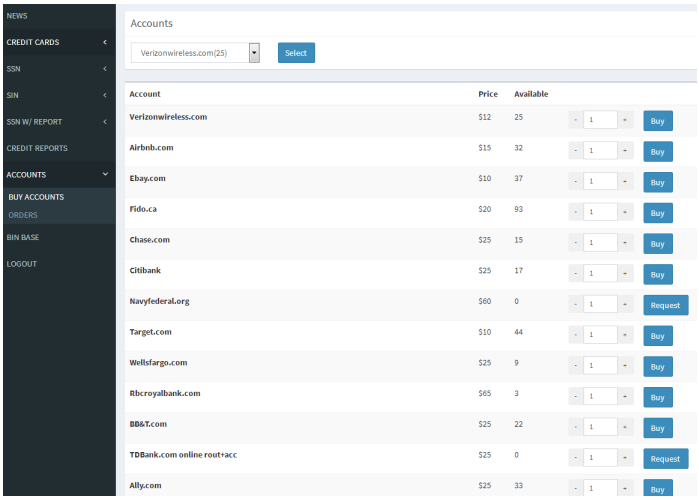


(c) Forsøk fra Januar 2018

Figur 3: Eksempel på phishing e-post som ble identifisert ved NTNU

Universitetet betaler for tilgang til databaser som inneholder tusenvis av forskningsartikler. 26 av de kompromitterte brukerne ble brukt av utenlandske aktører for å skaffe seg tilgang til forskningsartikler. Konsekvensen ved å ha kompromitterte kontoer som laster ned forskningsartikler er at NTNU risikerer å bli blokkert fra databasene. Angriperne derimot tjener på å ikke trenge å betale for tilgang til databasene. Det blir hentet ut flere tusen forskningsartikler per kompromitterte bruker. Universitetet vet ikke når det blir hentet ut artikler, eller om det er legitim bruk av artiklene. NTNU blir oppmerksom på problemet når de får beskjed fra samarbeidspartnere til NTNU, for eksempel de som tilbyr artikler.

Et annet punkt som gjør det lukrativt å kompromittere universitetskontoer er at disse kontoene kan bli solgt på nett, der kredentialer behandles som ferskvare. [5].



Figur 4: Pris på kontoer

Figur 4 viser at det er et stort marked for brukerkontoer, og siden NTNU har mange samarbeidspartnere er de et stort mål for trusselaktørene.

Denne analysen går ut på å identifisere rotårsaken til hvorfor NTNU har så mange kompromitterte brukerkontoer og komme med en tiltaksplan.

2.3 Case 3: Misbruk av NTNU sin infrastruktur til utvinning av kryptovaluta

Kryptovaluta har kommet mer i nyhetsbildet i det siste. Kryptovaluta er en anonym måte å betale og man kan utvinne kryptovaluta ved hjelp av regnekraft. Utvinningen kan bli gjort på flere måter. En kan installere et program på PCen eller det man kan utvinne direkte gjennom nettleseren med javascriptkode. Sistnevnte kan være en erstatning til reklame, eller en ondsinnet måte for nettsider eller andre å tjene penger på.

Oversikt over oppgaven

Dette caset går inn på rotårsaken til misbruk av NTNU sine ressurser og infrastruktur for å utvinne kryptovaluta. De to siste årene har både verdien og antallet kryptovaluta økt drastisk. Det finnes per dags dato over 1500 forskjellige kryptovalutaer [6]. Kryptovaluta blir utvinnet ved bruk av regnekraft. Dette betyr at enhver datamaskin kan delta i utvinningen. Siden november 2017 har NTNU sett en økning i kryptoutvinning med 8000% [2] og får i dag flere varsler angående kryptoutvinning om dagen. Siden universitetet sine ressurser ikke skal brukes til kommersiell vinning er dette blitt et stort problem [7].

Grunnen til økningen er at i 2017 begynte flere å spekulere i kryptovaluta og siden det er et uregulert marked var det veldig store svingninger. Svingninger som igjen førte til at det kom mange flere aktører på banen, som både leverandører og spekulanter.

Etter hvert vil vanskelighetsgraden for å utvinne nye mynter øke. Når vanskelighetsgraden øker trenger en mer datakraft og større maskinrigger til å utvinne valutaene [3].

NTNU forvalter stor regnekraft spredt på flere lokasjoner. NTNU har også hatt supermaskiner før; de har en nå og de får også en ny supermaskin. Supermaskiner er store

[2] Møte med oppdragsgiver
[3] Informasjon fra oppdragsgiver

datamaskiner med enorm datakraft. Disse er spesielt attraktive for aktører å misbruke til å utvinne kryptovaluta. Siden trenden har økt de siste årene, og NTNU er i besittelse av mye regnekraft, må NTNU aktivt jobbe for å beskytte infrastrukturen.

Siden dette er av økende trend, og Seksjon for Digital Sikkerhet har oppdaget at noe av universitetet sine ressurser har blitt brukt til utvinning av kryptovaluta tidligere, vil de undersøke måter å eliminere dette misbruket.

Caset deles inn i to fokusområder. Frivillig og ufrivillig utvinning av kryptovaluta. Frivillig utvinning mener vi interne aktører som bruker NTNU sine ressurser til egen vinning. Med ufrivillig utvinning mener vi de som får ressursene sine misbrukt uten samtykke.

Caset går ut på å identifisere rotårsaken til misbruk av NTNU sine ressurser til utvinning av kryptovaluta, og foreslå tiltak for å eliminere den.

3 Teori og tidligere arbeid

I dette kapittelet beskrives utvalget av faglitteratur som vi baserer oss på i dette prosjektet. Det beskrives hvorfor de ble valgt og hvordan vi fant frem til disse. I tillegg beskrives teorien i dypere detalj, og litt om historien bak metoden.

3.1 Utvalg av faglitteratur

Rotårsaksanalyse som helhet finnes det mye litteratur om, men metodene er veldig spredt. Innen informasjonsikkerhet finnes det lite bruk av rotårsaksanlayse. Vi har valgt boken "Root Cause Analysis: Simplified Tools and Techniques" av Fagerhaug og Andersen [1] som gir en generell beskrivelse av rotårsaksmetodikken, men ikke spesifikt for informasjonssikkerhet. Vi har i tillegg brukt en bacheloroppgave fra 2016 [8] som så på anvendelsen av rotårsaksanalyse innen informasjonssikkerhet. Vi har også brukt to rapporter som ble skrevet på den samme bacheloroppgaven i etterkant [4] [9].

3.1.1 Hvorfor ble disse valgt?

Vi valgte boken [1] på anbefaling av oppdragsgiver og fordi vi ville se hvor godt den fungerte innen informasjonssikkerhet. Forfatterne av boken [1] har i stor grad fokusert på de menneskelige årsakene og i mindre grad på tekniske årsaker. Vi ville se hvor godt denne tilnærmingen fungerer i informasjonsikkerhet, der de fleste problemer er menneskeskapt. Vi vil spesielt se hvor godt boka fungerte som en samlet metodikk for rotårsaksanalyse innen informasjonsikkerhet. Bacheloroppgaven [8] ble valgt da den er en av få studier som systematisk tar for seg rotårsaksanalyse i informasjonssikkerhetssammenheng.

3.2 Teori

Rotårsaksanalyse er en fremgangsmåte for å finne roten til et problem og eliminere det. RCA analyserer de underliggende faktorene og bruker årsakene til å finne roten til problemet. RCA er en reaktiv prosess som finner svar på problemer basert på skjulte årsaker og deres effekt, istedenfor å undersøke den mest åpenbare årsaken. Dette gjør at RCA er ofte komplekst og tidkrevende, men når rotårsaken først er funnet kan løsningene fjerne problemet helt.

3.2.1 Historie

Det har finnes flere varianter av rotåsaksanalyse opp gjennom tidene, men mannen som er kreditert med å finne opp rotårsaksanalyse er grunnleggeren av Toyota, Sakichi Toyoda. Hans versjon av RCA ble tatt i bruk av Toyota produksjonsprosess i 1958 og ble kalt "5 Whys". Som tidligere sagt har RCA forandret seg over tidene for å imøtekomme de forskjellige feltene. Nå brukes RCA som verktøy i flere felter som transport, medisin og luftfart [10].

3.2.2 Ulike nivåer av årsaker

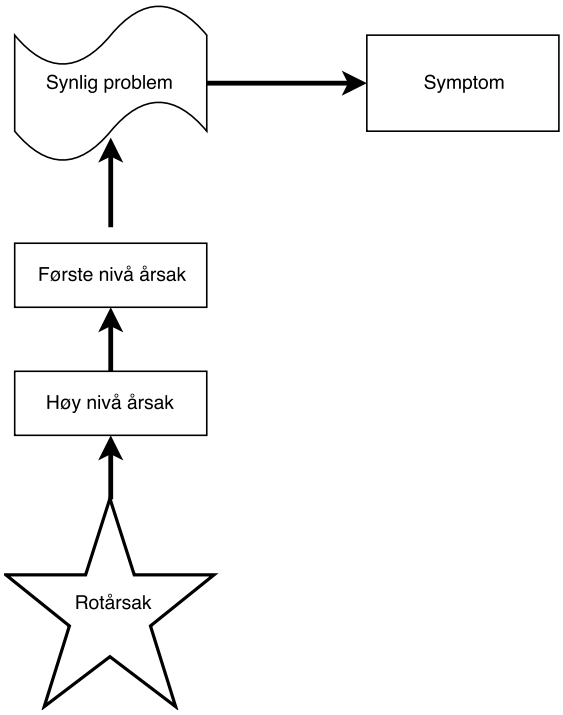
Et problem er som regel ikke et resultat av en årsak, men heller en kombinasjon av flere årsaker på flere forskjellige nivåer. Dette vil si at årsaker påvirker andre årsaker helt opp til det synlige problemet. Årsaker defineres i tre forskjellige grupper:

Symptomer er ikke å regne som faktiske årsaker, men heller bevis på eksisterende problemer.

Første-nivå årsak er årsåker som leder direkte til et problem.

Høy-nivå årsaker er årsåker som blir til første-nivå årsaker. Selv om de ikke direkte er årsak til problemmet, skaper høy-nivå årsak lenker i kjeden av årsak-virkningsforholdet som til slutt fører til problemet. Den høyeste nivå årsaken er rotårsaken.

Noen problemer har flere årsaker som er forbundet av de forskjellige faktorer som kombinert blir til problemet.



Figur 5: De forskjellige nivåer til problemet

Vi ser fra figuren at rotårsaken er det som setter i gang årsak-virkningskjeden som leder til det synlige problemet.

3.2.3 Root Cause Analysis: Simplified tools and techniques

Denne boken er andre utgave og bygger mer på hele problemet enn første utgaven. Der første utgaven stoppet etter å identifisert rotårsaken, gir andre utgave deg verktøy til å komme helt til løsningsimplenteringen. Den gjør det igjennom å strukturer analysen i 7 steg i en typisk fossefallmetodikk. Boken har i tillegg to ekstra kapittel der den tar for seg eksempelcaser og retningslinjer for verktøyvalg i form av et flytdiagram.

3.2.4 Tidligere arbeid innen informasjonssikkerhet

I 2016 ga NTNU en bacheloroppgave som heter "Bruk av rotårsaksanalyse i informasjonssikkerhet"[8]. Oppgaven ser på hvor godt rotårsaksanalyse fungerer i informasjonsikkerhet. For å finne det ut gikk de igjennom rotårsaksanalyse på tre caser. De så også på om det var kostnadseffektivt å benytte rotårsaksanalyse innen informasjonssikkerhet. Konklusjonen fra deres rapport var at det kunne være verdt det, men det måtte være verdt den tunge ressursbruken. Det viste seg å fungere best på caser med mye tid og ressurser. Konklusjonene de kom frem til var at de fikk tilstrekkelig svar på sine forskningspørsmål. For vår del er de viktigste konklusjonene til deres rapport[8] at de fant ut: ved bruk av rotårsaksanalyse var det mulig å komme frem til problemsituasjoner som ikke var synlig ved bruk av andre verktøy i informasjonssikkerhet. Dette gjaldt spesielt i et case med mye tid og ressurser til disposisjon. Basert på denne bacheloroppgaven ble det også skrevet to ytterligere rapporter [4] [9].

3.2.5 Rotårsaksanalyse sammenlignet med risikoanalyse

En risikoanalyse ser på sannsynligheten for at en trussel kan forekomme og mulige konsekvenser av dette. Risikoen regnes ut fra sannsynlighet og konsekvens, samt eksisterende kontroller. I risikoanalysen vil dataene brukes til å finne mulige preventive og reaktive tiltak som kan føre riskoen ned på et akseptabelt nivå. Rotårsaksanalyse vil på sin side gjøre en systematisk gjenomgang for å finne de underliggende årsakene til feil eller svikt. En rotårsaksanalyse gjøres etter et problem har oppstått for å stoppe det fra å skje igjen, i motsetning til riskoanalyse som gjøres for å behandle fremtidige situasjoner. Datainnsamlingen i risikoanalyseprosessen går ut på å identifisere aktiva, trusseler, eksisterende kontroller, sårbarheter og konsekvenser. Deretter gjøres et estimat på risikoen til de ulike truslene som truer aktiva. Til slutt gis det forslag til tiltak som vil føre risikoen ned til et akseptabelt nivå. Prosessen til rotårsaksanalyse skiller seg fra dette ved å være mer fokusert på verktøybruk, idémyldring og dataanalyse. Den er også mye mer krevende, i form av både tid og ressurser.

4 Metode

Vår tilnærming til anvendt rotårsaksanalyse i dette prosjektet er gjennom tre caser som omhandler informasjonssikkerhet. Utførelse av rotårsaksanalyse kan gjøres på ulike måter, men grunnstrukturen er ofte lik. Det handler i bunn og grunn om problemløsning. I tillegg til å analysere casene skal bruken av metoden vurderes ut i fra hvor godt den fungerer innen informasjonssikkerhet. Påfølgende seksjon vil forklare valg av metode.

4.1 Metodevalg

Hovedgrunnen til at rotårsaksanalyse brukes i dette prosjektet er, som nevnt tidligere, at vi skal undersøke bruksområder for denne analysemetoden i fagfeltet informasjonssikkerhet. Et problem er at rotårsaksanalyse ikke er en standardisert metode. Det er i hovedsak en metode for problemløsning, men det er mange foreslåtte tilnærminger til rotårsaksanalyse. En tidligere bacheloroppgave [8] kom frem til at boka "Root Cause Analysis: Simplified Tools and Techniques" av Fagerhaug og Andersen [1] beskriver en god og detaljert metode for hvordan rotårsaksanalyse bør utføres. Oppdragsgiver sa seg enig i at dette var et godt utgangspunkt når det skulle jobbes med rotårsaksanalyse, og anbefalte oss metoden. En grunn til at dette er en god metode er den detaljerte oppdelingen av de ulike fasene i RCA. Den skiller seg ut fra de fleste konkurrenter ved å detaljert beskrive hver fase, hvordan du skal gjennomføre den, og ikke minst verktøyene som kan brukes i gjennomføringen. Andre metoder går som regel bare gjennom det generelle hendelsesforløpet og anbefaler et par verktøy som kan brukes. Boken gir en praktisk beskrivelse av hvordan man gjennomfører rotårsaksanalyse. Den beskriver ikke bare hvilke verktøy du burde bruke, men også hvordan du bruker de og i hvilken sammenheng du bør bruke hvert verktøy. Dette bruker boken flytdiagram til å visualisere, og gjør det lett å velge rett verktøy til rett situasjon. Det er hjelpsomt siden oppgaven vår blant annet dreier seg om å finne ut hvilke verktøy som passer best til informasjonssikkerhetsproblemer. Flytdiagrammene finnes i vedlegg I.

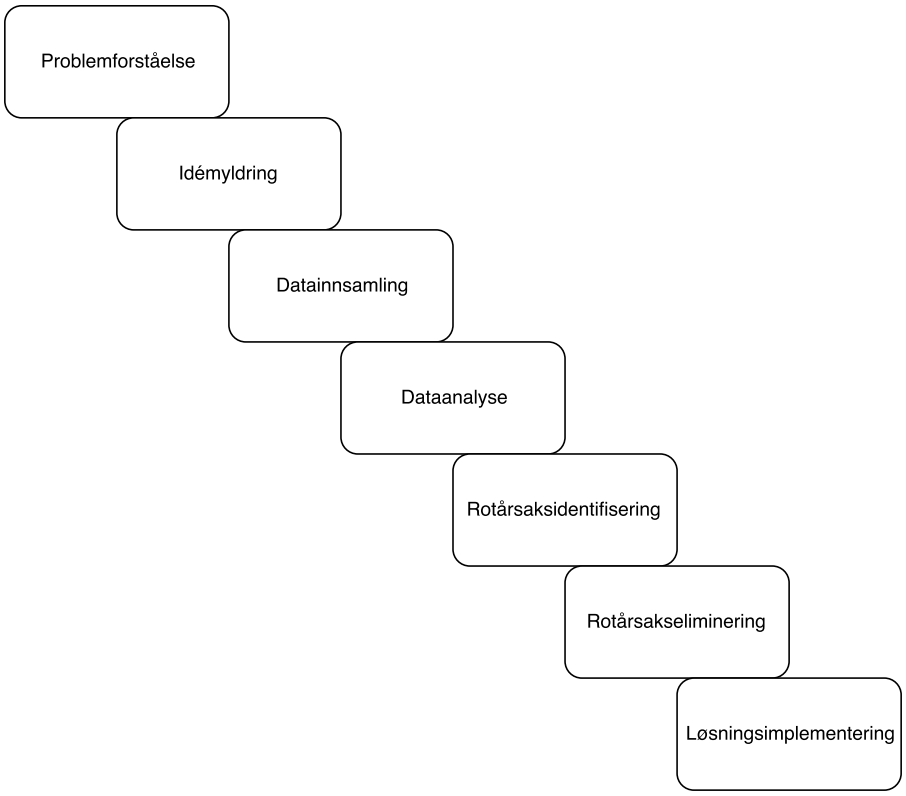
4.2 Metodekritikk

Selv om metoden er god, har den et par svakheter. For det første er den sekvensiell. Dette gjør at det blir vanskelig å jobbe parallelt i større grupper. For det andre er metoden heller ikke tilpasset informasjonssikkerhetshendelser, så vi må gjøre en egenvurdering i tillegg til metoden sin anbefaling på valg av verktøy.

4.3 Anvendt rotårsaksanalyse

Metoden innebærer syv steg (visualisert i figur 6), der hvert steg anbefaler et sett verktøy for å fullføre det. Bruk av et eller flere verktøy kommer helt an på problemet som skal løses. Valg av verktøy i hver fase er i stor grad basert på flytdiagrammene i boken av Andersen og Fagerhaug [1], som beskriver hvordan en velger riktig verktøy i hvert steg, for et bestemt problem. Selv om verktøyvalg er godt beskrevet tok vi med vår egen vurdering

på hvilke verktøy som skulle brukes, siden boken ikke er direkte tilpasset informasjonssikkerhetsoppgaver. Vi har også brukt noen få verktøy utover det boken anbefaler når det kommer til dataanalyse.



Figur 6: De syv fasene i rotårsaksanalyseprosessen

4.3.1 Problemforståelse

Problemforståelse går ut på å få en solid forståelse for problemet en ønsker å løse og kan også hjelpe med å skape enighet i teamet rundt hva problemet egentlig omfatter. Det er også viktig for å passe på at ressursene som benyttes i analysen brukes effektivt videre. Under beskrives de verktøyene som ble brukt i denne fasen.

Flytdiagram

Et flytdiagram viser flyten av aktiviteter i en prosess. I informasjonssikkerhet kan det brukes som en metode for å konkretisere og illustrere et problem ved eller angrep mot virksomhetens aktiva. Formålet er å skape en detaljert forståelse for en prosess som har med problemet å gjøre [1].

Kritiske hendelser

Hovedpoenget med kritiske hendelser er å identifisere de mest kritiske symptomene i problemet. Det kan hjelpe med å forstå hvilke aspekter ved problemet som trenger å løses, samt forstå problemets natur og konsekvenser for virksomheten [1]. Innen informasjonssikkerhet har man ofte logger med hendelsesdata. Det gjør det naturlig å bruke kritiske hendelser siden informasjonen ofte eksisterer på forhånd og trenger bare å bearbeides.

Ytelsesmatrise

Ytelsesmatrise er et diagram som tar i betraktning viktigheten og den nåværende ytelsen til en variabel. Dette gjør at man enkelt kan vurdere hvilken prioritering variablene som blir analysert har [1]. Matrisen går fra en til ni på hver akse og er delt inn i fire like store hjørneområder. Ut i fra hvor høy ytelse ytelse og hvor viktige de er, er variablene enten: uviktig, overdrevent, må forbedres eller ok. I informasjonssikkerhet kan det brukes til å vurdere virksomhetens aktiva opp mot for eksempel eksisterende kontroller.

4.3.2 Idémyldring

Målet med idémyldring er å generere så mange idéer som mulig om et gitt emne. I rotårsaksanalyse er målet stort sett å generere en liste over problemområder som kan forbedres, identifisere mulige konsekvenser, generere en liste over mulige årsaker til problemet og oppmuntre til å tenke på løsninger som kan eliminere problemet. Det finnes i hovedsak to typer idémyldring: strukturert og ustrukturert. I strukturert idémyldring har hver deltaker sin tur til å komme med idéer. Dette fører til lik deltagelse og at ingen dominerer prosessen med egne idéer. I ustrukturert idémyldring kan hvem som helst komme med idéer når som helst. Dette er ofte mer spontant, men kan føre til at en person dominerer prosessen [1].

Nominell gruppeteknikk (NGT)

Nominell gruppeteknikk er en strukturert metode for idémyldring som hjelper med å gå fra mange idéer, til å sitte igjen med de beste. Konseptet går ut på å myldre idéer og skrive dem ned på lapper, for så å anonymt gi idéene poeng fra en til fem. Et tallpoeng kan bare gis én gang. Til slutt blir tallene lagt sammen og du sitter igjen med de beste idéene.

4.3.3 Datainnsamling

Datainnsamling er et steg i prosessen der man skal være strukturert og samle inn så mye relevant informasjon om problemstillingen som mulig. En god datainnsamling er sentralt for gode resultater i senere faser. Under beskrives verktøyene som ble brukt for å samle inn informasjon.

Spørreundersøkelser

Spørreundersøkelser brukes når en er på utkikk etter å samle inn data om personers holdninger, følelser eller meninger om et spesifikt problem. En kan skille mellom to typer spørreundersøkelser: kvalitative og kvantitative spørreundersøkelser. Kvantitative undersøkelser handler om å få mange svar slik at en kan ta avgjørelser basert på tall som kan brukes til statistisk analyse. Kvalitative undersøkelser går ut på å samle detaljert informasjon om emnet. Dette kan hjelpe med blant annet å formulere hypoteser for å dirigere kvantitativ undersøkelse senere, eller å komplimentere en kvantitativ undersøkelse ved å bruke sitater fra åpne spørsmål [11]. Det brukes ofte elementer fra begge typene når en spørreundersøkelse lages. Når det er snakk om informasjonssikkerhet kan kvalitative undersøkelser brukes når det for eksempel skal samles inn informasjon om brukervaner på nett, eller grad av kunnskap og erfaring om informasjonssikkerhet. Kvalitative undersøkelser kan brukes når det kreves detaljert informasjon om et system eller indre forretningsprosesser.

Sampling

Hovedpoenget med sampling er å trekke ut deler av en populasjon, for å trekke konklusjoner om denne uten å trenge å undersøke alle enhetene [12]. I rotårsaksanalyse kan det brukes for å effektivt samle inn data om problemer eller årsaker, og skaffe en bedre forståelse av situasjonen [1].

4.3.4 Dataanalyse

I denne fasen blir dataene analysert og visualisert. Hovedmålet er å avklare mulige rotårsaker som har innvirkning på problemet, og hvilke av de som har størst innflytelse. Under beskrives de ulike verktøyene som ble brukt for å analysere dataene.

Histogram

Histogrammer, også kjent som søylediagram, brukes for å vise distribusjon og varians i et datasett. Dataene kan vises i form av lengde, tid, kostnad, mengde osv. Hovedoppgaven til et histogram er å presentere data på en oversiktlig måte slik at det er lett å se mulige relasjoner. I rotårsaksanalyse brukes det til å se hvilke årsaker som dominerer og for å forstå distribusjonen av forskjellige problemer, årsaker, konsekvenser osv. [1] Det er viktig å ha minst 30 svar for å lage et gyldig histogram [1].

Affinitetsdiagram

Affinitetsdiagram er et verktøy som kan brukes til å analysere kvantitative data. Formålet er å gruppere svar for å finne underliggende relasjoner mellom de resterende gruppene [1]. I vår rotårsaksanalyse ble det brukt til å utforske relasjoner mellom forskjellige årsaker, og gruppere relaterte årsaker inn i klasser som kan analyseres kollektivt senere.

Statistisk analyse

Statistisk analyse er ikke nevnt i boken [1] og inneholder flere verktøy.

One-way ANOVA

ANOVA, også kjent som variansanalyse, er en samlebetegnelse på en rekke statistiske metoder som tester likhet mellom to eller flere utvalg, der én eller flere faktorer gjør seg gjeldene [13].

Independent-samples t-test

Dette er en type t-test som brukes for å teste gjennomsnittet mellom to uavhengige grupper på samme avhengige variabel [14].

4.3.5 Rotårsaksidentifisering

De foregående fasene skal ha generert en liste over mulige rotårsaker og målet i denne er å identifisere de faktiske årsakene. Det kan kreves flere iterasjoner for å finne rotårsaken(e). Verktøy som ble brukt til identifisering er beskrevet under.

Årsak-virkningsdiagram (Fiskebeindiagram)

Et typisk årsak-virkningsdiagram undersøker og analyserer relasjonen mellom et problem og dets årsaker. Det fungerer som en kombinasjon av idémyldring og systematisk analyse. Det brukes for å generere og gruppere årsaker, og evaluere årsakene til problemet for å finne ut hvilke som mest sannsynlig er rotårsaker. Det finnes to typer årsaks-virkningsdiagrammer: fiskebeindiagram og prosessdiagram. Et prosessdiagram er

egentlig en samling av fiskebeindiagrammer der hver prosess har sitt eget diagram. Det finnes to ulike tilnærminger til å skape et fiskebeindiagram: spredningsanalyse og årsaksopplisting. Kort forklart, spredningsanalyse grupperer først og idémyldrer etterpå, mens årsaksopplisting idémyldrer først og grupperer etterpå [1].

5 Whys

5 Whys brukes for å undersøke høyere nivåer av årsaker. Som navnet beskriver, går det ut på å spørre "Why?" til en bestemt årsak for å komme frem til en ny årsak. Deretter blir det stilt spørsmål til den nye årsaken. Dette gjentar seg helt til det ikke er noen relevante årsaker å komme med. Den siste er da rotårsaken. Som en tommelfingerregel itererer man gjerne fem ganger, men det kan være både flere eller færre avhengig av problemet.

Feiltreanalyse

Feiltreanalyse er en top-down, deduktiv analyse der en uønsket tilstand av et system analyseres ved hjelp av boolsk logikk for å kombinere en rekke hendelser [15]. I RCA brukes det for å få en klar oversikt over mulige årsaker, og for å se relasjoner mellom årsaker eller identifisere grupper med relaterte årsaker [1].

4.3.6 Problemeliminering

Denne fasen innebærer å komme med mulige løsninger til problemet for å eliminere rotårsaken. Boken til Fagerhaug og Andersen [1] beskriver to mulige tilnærminger til denne fasen. En tilnærming for å stimulere kreativitet når man leter etter løsninger, og en for å konstruere og utvikle løsninger. Vi har prøvd et verktøy fra hver tilnærming og de er beskrevet under.

De seks tenkehattene

Formålet med de seks tenkehattene er å oppmuntre til å se problemet og løsningene fra forskjellige synsvinkler. Konseptet går ut på at personene får hver sin hatt som skal illustrere deres holdning til problemene [1].

Hvit hatt skal være kald, nøytral og objektiv, personen skal fokusere på fakta.

Rød hatt skal representere sinne, og skal bare fokusere på mageføelsen og egne følelser.

Svart hatt skal være pessimistisk og negativ, og fokusere på hvorfor idéen er dårlig.

Gul hatt er optimistisk og positiv, og skal fokusere på hvorfor idéen er bra og vil fungere.

Grønn hatt representerer gresset, fruktbarhet og vekst, og skal fokusere på å våre kreativ og komme på nye idéer.

Blå hatt er koblet til himmelen, og skal fokusere på å se tingene fra et høyere perspektiv.

Systematisk Innovativ Tenkning (SIT)

SIT er en problemelimineringsmetode som baserer seg på konseptet om en "lukket verden". Dette betyr at den fokuserer på at løsningene på problemet ofte finnes i det fagområdet problemet eksisterer i. SIT baserer seg på å undersøke en eller flere kjernekomponenter ved hjelp av fem hovedprinsipper [1]:

Attributtavhengighet vurderer å endre en nøkkelvariabel i et produkt for å skape forbedring.

Komponentkontroll ser på hvordan et produkt er knyttet til omgivelsene.

Erstatning handler om å erstatte en del av et produkt med noe annet fra produktets omgivelser.

Forkastning vurderer å forbedre problemet ved å fjerne en komponent.

Oppdeling har som mål å splitte et produkts attributter i to, som for eksempel splittelsen av sjampo fra balsam.

Hovedprinsippet i vårt prosjekt er å fokusere på at løsningene er tilknyttet fagområdet informasjonssikkerhet.

4.3.7 Løsningsimplementering

I den siste fasen er målet å implementere løsningene som ble funnet i foregående fase. I vår rapport vil implementeringen beskrives til beste evne, men ikke implementeres siden vi ikke har mulighet til dette. Implementeringen inkluderer blant annet organisering, utvikling av en implementeringsplan, skape et konsensus om de nødvendige endringene og selvfølgelig implementeringen. Implementeringen av løsningen kan sies å være en suksess når symptomene forsvinner. Verktøyene beskrives under.

Trediagram

Et trediagram er et verktøy som er enkelt å bruke og er passende for å dele opp større oppgaver inn i mindre, mer håndterlige aktiviteter. Det er et verktøy som hjelper til å organisere arbeidet som må gjennomføres for å implementere tiltakene som er anbefalt. I informasjonssikkerhet kan dette benyttes for å strukturere oppgavene og planlegge implementeringsprosessen av løsningen. Et trediagram visualiserer hierarkiet i aktivitetene som må gjennomføres, eller enklere sagt, rekkefølgen av gjøremål for å fullføre implementeringen.

Kraftfeltsanalyse

En kraftfeltsanalyse er basert på den oppfatningen at alle situasjoner er resultatet av krefter som virker for og i mot den faktiske tilstanden. En forandring i disse kreftene vil fremkalle en endring, noe som kan brukes til å endre ting i ønsket retning. I rotårsaksanalyse brukes det for å få innsikt i endringsklimaet til en mulig implementering, samt å planlegge aktiviteter som skal til for å implementere løsningen [1]. Verktøyet kartlegger krefter som virker for endringen, og krefter som virker i mot.

5 Gjennomføring av metode

Dette kapittelet vil gå gjennom bruk av metoden i de tre casene. Det beskrives hvilke verktøy som ble brukt i hver fase, hvorfor vi valgte de, ønsket utbytte av verktøyene, spesifiseringer vi la til grunn og hvordan det ble gjennomført. Tabell 1 under viser de ulike verktøyene vi benyttet i hver fase, i hvert case.

Tabell 1: Matrise som viser valg av verktøy fra metoden i de tre casene

	Verktøy	Brukt	Case 1	Case 2	Case 3
Problemforståelse	Flytdiagram	x	x		
	Kritiske hendelser	x	x	x	
	Spiderdiagram	-			
	Ytelsesmatrise	x			x
Idémyldring	Idémyldring	x	x	x	x
	Idéskriving	-			
	Is-is not matrise	-			
	NGT	x			x
	Parvis sammenligning	-			
Datainnsamling	Sampling	x		x	
	Spørreundersøkelse	x	x	x	x
	Sjekkliste	-			
Dataanalyse	Histogram	x	x	x	
	Paretodiagram	-			
	Spredningsdiagram	-			
	Problemkonsentrasjonsdiagram	-			
	Relasjonsdiagram	-			
	Affinitetsdiagram	x	x	x	x
Rotårsaksidentifisering	Årsak-virkningsdiagram	x	x	x	
	Matrisediagram	-			
	5 Whys	x		x	x
	Feiltreanalyse	x			x
Rotårsakseliminering	De seks tenkehattene	x	x		
	TRIZ	-			
	SIT	x	x	x	x
Løsningsimplementering	Trediagram	x	x	x	
	Kraftfeltanalyse	x			x

Vi kan se over at det er noen verktøy vi har brukt alle casene, og noen vi ikke har brukt i det hele tatt. Under spesifiserer vi grunner til hvorfor dette er tilfellet.

Grunner til bruk av verktøy i alle caser:

Idémyldring ble brukt i alle casene fordi ingen i gruppen dominerte prosessen.

Spørreundersøkelse ble brukt i alle casene fordi det var det mest logiske datainnsamlingsverktøyet for hvert av casene.

Affinitetsdiagram ble brukt i alle casene fordi vi hadde minst ett spørsmål som var kvalitativt, og det var et behov for å analysere disse.

SIT er en utvikling av TRIZ, der TRIZ er mer praktisk rettet. Dette passer ikke alltid så bra i informasjonssikkerhet, og SIT ble heller brukt fordi den er mer friflytene.

Grunner til at noen verktøy ikke ble brukt i noen av casene:

Spiderdiagram ble ikke brukt fordi det ikke var nødvendig eller mulig med ekstern sammenligning i noen av casene.

Idéskriving ble ikke brukt fordi ingen dominerte prosessen, og siden det ikke var behov for å skjule idéer mens de utvikles, ble ikke idéskriving brukt.

Is-is not matrise ble ikke brukt fordi forskjeller ikke var forventet.

Sjekkliste ble ikke brukt på grunn av tiden det ville ta for å logge hendelser i de ulike casene.

Paretodiagram ble ikke brukt fordi vi ikke hadde tilstrekkelig data til å analysere hvilke årsaker som utgjorde mest effekt.

Spredningsdiagram ble ikke brukt i casene fordi vi ikke hadde noe datasett der resultatene var såpass spredt at spedningsdiagram gir oss noe relevante resultater.

Problemkonsentrasjonsdiagram er i hovedsak fokusert på fysiske lokasjoner, med et fysisk problem. Siden våre caser handler om informasjonssikkerhet, ble det ikke relevant å utføre denne i noen av casene.

Relasjonsdiagram ble ikke brukt fordi vi hadde ikke så altfor mye data i numerisk form.

Matrisediagram ble ikke brukt fordi de andre verktøyene i denne fasen ble ansett som mer passende til det vi ønsket å gjøre.

TRIZ er mer praktisk rettet enn SIT, derfor valgte vi heller SIT.

Verktøyvalgene er i stor grad basert på flytdiagrammene i boka som beskriver vårt utgangspunkt til rotårsaksanalyse [1], og blir valgt basert på disse og et par andre variabler. Flytdiagrammene vi tar utgangspunkt i for hver fase kan sees i vedlegg I. I neste avsnitt vil vi gå gjennom alle casene og begrunne verktøyvalg, beskrive ønsket utbytte av verktøyene og dokumentere hvordan de ble brukt, med fokus på spesifiseringen vi la til grunn ved bruk av de.

5.1 Case 1: Ulovlig fildeling på universitetsnettet

5.1.1 Problemforståelse

Flytdiagram

Valg og ønsket utbytte av verktøy

Ved å bruke et flytdiagram prøver vi å kartlegge hendelsesforløpet, og hvordan bruksmønsteret til en bruker av nettet til NTNU kan se ut, med fokus på fildeling. Vi håper dette kan gi oss en helhetlig forståelse av hva årsaken til fildeling kan være, og kanskje vi kan bruke dette til å utvikle tiltak senere i prosessen.

Spesifiseringer

Det gjøres en antagelse at private fildelingstjenester ikke er med i statistikken fra universitet og at det ikke kommer noen opphavsrettsnotiser fra brukere som bruker private tjenester. Med private tjenester mener vi lukkede nettsamfunn som bare er til for å distribuere opphavsrettsbeskyttet materiale gratis.

Gjennomføring

Vi fulgte metoden for å lage et flytdiagram, fra boken om rotårsaksanalyse [1].

1. Vi samlet alle på gruppen for å diskutere prosessen, og hadde med oss post-it lapper
2. Vi definerte brukerne som studenter ved NTNU i Gjøvik som bor i Sit Bolig.
3. Vi definerte hvilke aktiviteter som gjøres for at universitetet skal få en notifikasjon.
4. Så flyttet vi rundt på lappene til de kom i en naturlig rekkefølge.

Kritiske hendelser

Valg og ønsket utbytte av verktøy

For å gå dypere i detalj har vi tatt en titt på kritiske hendelser som inngår i problemstillingen. Vi har valgt å bruke kritiske hendelser til å dele opp problemet i mindre stykker for å spørre studenter som bor i Sit Bolig om hva de laster ned hvis de først gjør det. Ved bruk av dette verktøyet ønsker vi å få en dypere forståelse av hva studentene laster ned slik at vi kan se om det er noen kategorier som er mest fremtredende. Dette kan føre til at vi blir mer effektive i senere arbeid da vi kan fokusere på det som er viktigst.

Spesifiseringer

Det er bare studenter som bor i Sit bolig som har blitt registrert som svar. Vi prøvde å være så upartiske som mulig når det kom til valg av respondenter, men det var fortsatt stor overvekt av informatikkstudenter.

Gjennomføring

Det første som ble gjort var å definere de mest relevante kategoriene av nedlastningsmateriale. Dette ble basert på egen erfaring med blant annet hyppigheten til de ulike kategoriene. Vi hadde en viss anelse om hvilke som var de store synderne, men ønsket å bekrefte våre mistanker. Følgende kategorier ble fremhevet:

- Filmer og serier
- Skolebøker
- Programvare til skolebruk
- Programvare og bøker utenom skolebruk
- Spill
- Musikk
- Annet

Intervjuene var i stor grad uformelle “intervjuer” med få spørsmål. Det viktigste vi trengte å vite var om personen bodde i Sit Bolig, siden det er bare beboere derfra som er relevante i vår problemstilling, i tillegg til hvilke kategorier de laster ned fra. Resultatene ble fortløpende ført inn i statistikken. Intervjuobjektene var i stor grad bekjente vi visste bodde i Sit Bolig, og derfor var det en overvekt av IT studenter.

Spørsmål stilt til intervjuobjekter:

- Bor du, eller har du bodd i Sit Bolig i løpet av studiet? (Hvis nei, avslutt intervju)
- Bruker du, eller har du brukt Torrents til å laste ned opphavsrettsbeskyttet materiale mens du bodde i Sit Bolig? Hvis ja, hvilke av følgende kategorier laster du ned fra? (Viser kategoriene)

5.1.2 Idémyldring

Valg og ønsket utbytte av verktøy

Det finnes som sagt flere måter å utføre en idémyldring på, men vi benyttet oss av den ustrukturerte idémyldringen på bakgrunn av verktøyets egenskap til å generere mange idéer hurtig, og på grunn av dens spontane natur.

Spesifiseringer

Det er spesielt viktig å ikke omformulere eller diskutere forslagene etterhvert som de kommer, dette skal gjøres etter idémyldringsøkten er over. Vi valgte å strukturere idémyldringen som et tankekart ettersom dette var en kjent løsning for gruppen.

Gjennomføring

Det første som ble gjort når økten startet var å kommunisere og skrive opp problemstillingen på en tavle.

Problemet ble definert som hvorfor personer bruker Torrents til å laste ned opphavsrettsbeskyttet materiale. Når idéstrømmen begynte å gå langsomt, stoppet vi og vurderte det vi hadde kommet fram til. Vi kom blant annet fram til at vi burde spesifisere problemstillingen ytterligere og valgte derfor å spesifisere den til hvorfor folk laster ned på universitetetnettet. Vi forkortet dette til: "Hvorfor Torrenting på universitetetnettet?" for enkelthets skyld. Det ble kjørt enda en økt med denne nye problemstillingen og vi fikk mer spesifikke resultater.

5.1.3 Datainnsamling

Spørreundersøkelse

Valg og ønsket utbytte av verktøy

I vår situasjon har vi valgt kvantitativ undersøkelse på bakgrunn av et par faktorer. For det første ønsker vi at undersøkelsen skal være helt anonym, siden spørsmålene omhandler potensielle lovbrudd. For det andre er målgruppen et stort antall personer, så det kan være nyttig å samle inn data fra så mange av de som mulig.

Det vi ønsker å få ut av spørreundersøkelsen er data på utvalgte spørsmål vi mener er relevante for oppgaven. Spørsmålene er utarbeidet for å utforske hvorfor studenter som bor i studentbyer laster ned opphavsrettsbeskyttet materiale, som blant annet inkluderer undersøkelse av økonomiske perspektiver og tilgjengelighet på tjenester. I tillegg ønsker vi også innsikt i hvordan dette kan stoppes.

Spesifiseringer

Vi brukte Google Forms til å lage spørreundersøkelsen og motta data fra den. Vi setter krav til antall respondenter og utfører en rekke tiltak for å oppnå nok besvarelser, slik at undersøkelsen kan si noe om rotårsaken med relativt høy sikkerhet. Det er et krav å få minst 30 besvarelser som hadde lastet ned opphavsrettsbeskyttet materiale mens de har bodd i hybelen. Videre er det også ønskelig med relativ likhet i antall respondenter

mellom de ulike fakultetene og studentbyene. Det hadde vært ideelt med minst 30 respondenter i hver kategori her også, men det er ønsketenkning i denne sammenhengen. Under prosessen ble også totalt antall beboere fra alle studentbyene i Sit Bolig kartlagt. Boligtorget ga oss innbyggertallene fra hver studentby, og vi regnet oss frem til totalt 522 beboere. Det er viktig å presisere at det kan være usikkerheter knyttet til disse tallene, siden det kan hende ikke alle boligene har en beboer.

Gjennomføring

Hypotesen vi hadde når vi utformet undersøkelsen var at folk laster ned opphavsrettsbeskyttet materiale fordi det er lett tilgjengelig, tilknyttet liten til ingen kostnad og ikke minst fordi det er svært lav risiko for represalier.

En god undersøkelse vil alltid kreve kartlegging av demografi, og i vår undersøkelse valgte vi å kartlegge studentby, kjønn, alder og fakultet. Kjønn og alder er ganske selvforklarende, mens studentby ble valgt på bakgrunn av at Kallerud har mye raskere nedlasting- og opplastingshastighet enn de andre stedene. Vi anså også at det ville være forskjell på hvor mange som laster ned mellom for eksempel informatikkstudiene og helsestudiene. Videre ble resultatene i de foregående fasene brukt til å utforme spørsmålene. Spørreundersøkelsen inkluderer spørsmål om hvor godt en rekke påstander stemmer for den enkelte der respondentene svarer på en likert-skala fra 1-5, der 1 er i liten grad og 5 er i stor grad. Likert-skala ble valgt fordi det er en anerkjent måte å få inn kvantitative svar på hvor enige personer er med en påstand. Samtidig kan man enkelt sammeligne forholdene mellom svarene på de forskjellige påstandene ved hjelp av statistisk analyse. Til slutt inkluderer spørreundersøkelsen et spesielt viktig spørsmål om hva som skal til for at personen stopper med ulovlig nedlasting. Dette er et frisvar der vi kommer til å analysere individuelle svar hver for seg. Spørreundersøkelsen kan leses i sin helhet i vedlegg J.

Siden spørreundersøkelsen er elektronisk var et av de første tiltakene som ble forsøkt å få tak i en e-post liste fra Sit. Dette fikk vi ikke fra dem. Istedenfor spredde vi den på relevante facebook-sider. Et av prosjektgruppens medlemmer jobber på Studenthuset her på Gjøvik, og fikk spørreundersøkelsen delt på deres facebook-side. Senere i prosessen ble også undersøkelsen delt på facebook-siden til linjeforeningen INGa og klassesidene til sykepleierne og webutvikling. Undersøkelsen ble også delt gjennom venner og bekjente; disse var for det meste informatikkstudenter. I tillegg ble det laget en plakat som ble hengt opp på oppslagstavler på universitetet, i vaskeriene ved de ulike studentbyene, og mange ble også plassert i postkassene til Sit sine boliger. Plakaten finnes i vedlegg D.

5.1.4 Dataanalyse

Histogram

Valg og ønsket utbytte av verktøy

Hovedgrunnen til å bruke histogrammer er for å skape en visuell forståelse av dataene som en ellers ikke får fra tabeller o.l. Da blir det enklere å se korrelasjoner og sammenhenger i datasettet. For dette caset ønsker vi å visualisere hvilke mulige rotårsaker som er mest utbredt, og forstå distribusjonen av hendelser, problemer, årsaker, konsekvenser osv. Analyse av spørsmålene tilknyttet likert-skala er viktig for å finne mulige rotårsaker. Ellers ønsker vi også å finne sammenhenger mellom de ulike spørsmålene, for å se

relevante korrelasjoner mellom de.

Spesifiseringer

Det statistiske verktøyet SPSS ble brukt til å lage histogrammene. For at et histogram skal være gyldig, det vil si hvis vi skal kunne konkludere sikkert med noe, må det være minst 30 svar.

Gjennomføring

For å starte analysen eksporterte vi dataene til det statistiske verktøyet SPSS. Deretter ble diagramverktøyene brukt til å lage histogrammer ut fra svarvariablene. Noen spørsmål ble klynget sammen for å kunne se relasjoner mellom variablene visuelt. Vi testet først ut hypotesene våre, deretter ble det sjekket relativt tilfeldig om det var noen andre relevante data å vise i histogrammene.

Affinitetsdiagram

Valg og ønsket utbytte av verktøy

I spørreundersøkelsen inkluderte vi et kortsvar spørsmål som skulle gi oss svar på hva som kreves for at de stopper med ulovlig fildeling. For å analysere denne dataen var det bare affinitetsdiagram som passet dette.

Spesifiseringer

Det nettbaserte verktøyet draw.io ble brukt til å konstruere affinitetsdiagrammet.

Gjennomføring

Alle tekstsvarene, inkludert de engelske, ble analysert og kategorisert. Deretter ble dette lagt inn i verktøyet Draw.io og tildelt fargekoder og tallverdier som tilsier hvor mange som svarte i den kategorien.

Statistiske analyseverktøy

Valg og ønsket utbytte av verktøy

På enkelte spørsmål ble det spurt om påstander og respondentene ble bedt om å svare på en likertskala fra 1-5. Disse dataene er perfekt for å gjøre beregninger på. Derfor har vi valgt å benytte oss av one-way ANOVA analyse og Independent Sample t-test. Vi ønsket å benytte en independent t-test for å undersøke forskjeller mellom variabler der den uavhengige variabelen bestod av to grupper. Vi ville utforske om det var noen signifikant forskjell når det kom til om folk laster ned, mellom Kallerud og de andre studentbyene. I tillegg ville vi se på om det var noen signifikante forskjeller mellom IT fakultetet og de andre fakultetene. Ønsket utbytte ved bruk av ANOVA-analysen er å gi oss et bilde av om påstandene har noen signifikant verdi knyttet til demografien.

Spesifiseringer

Vi benytter t-test når den uavhengige variablen har to kategorier. One-way ANOVA brukes når det er flere enn to kategorier. Generelt regner vi med en signifikans på:

$$\alpha \leq 0,05$$

Gjennomføring

Vi delte opp demografien og ga svarene et tall istedenfor en streng. Vi delte inn Kallerud og de andre studentbyene hver for seg, siden det var få svar på de andre studentbyene,

slik at det ble jevn fordeling. Det samme ble også gjort med IT og de andre fakultetene.

Forholdet mellom tallverdiene og svarkategoriene er som følger:

Kjønn:

- Kvinne: 1
- Mann: 2

Fakultet:

- Fakultet for arkitektur og design: 1
- Fakultet for informasjonsteknologi og elektroteknikk: 2
- Fakultet for ingeniørvitenskap: 3
- Fakultet for medisin og helsevitenskap: 4
- Fakultet for økonomi: 5

Når det er bare snakk om IT fakultetet mot andre:

- Andre fakulteter: 1
- Fakultet for informasjonsteknologi og elektroteknikk: 2

Alder:

- Under 20: 1
- 20-25: 2
- 26-30: 3
- 31-35: 4
- Over 35: 5

Studentby (Kallerud mot andre):

- Kallerud: 1
- Andre studentbyer: 2

Har du lastet ned:

- Nei: 1
- Ja: 2

5.1.5 Rotårsaksidentifisering

Årsak-virkningsdiagram

Valg og ønsket utbytte av verktøy

I dette caset var det kommet frem til hovedårsaker som ble relevante til å sette inn i et fiskebeindiagram. Ved bruk av dette verktøyet ønsker vi å sitte igjen med en visuell fremstilling av rotårsaken til problemet. Dette vil gjøres ved å identifisere hva som skaper årsakene som kom frem av dataanalysen.

Spesifiseringer

Det er anbefalt å bruke en tusjtavle for å tegne opp fiskebeindiagrammet, men vi valgte å bruke et nettbasert program som er laget for å skape diagrammer med flere brukere involvert i sanntid. De hadde en egen mal for fiskebeindiagram som vi valgte å gå ut fra.

Gjennomføring

Stegene vi fulgte i prosessen er hentet fra boka om rotårsaksanalyse [1] og ble som følger:

1. Vi beskrev problemet klart og tydelig
2. Vi tegnet opp problemet på slutten av fiskebeindiagrammet
3. Vi identifiserte hovedkategoriene av årsakene til problemet og tegnet det opp på fiskebeinene i diagrammet
4. Vi idémyldret alle mulige årsaker i hver kategori, en kategori om gangen, og skrev det inn i diagrammet fortløpende
5. Til slutt analyserte vi de identifiserte årsakene og bestemte de mest sannsynlige rotårsakene

5.1.6 Rotårsakseliminering

De seks tenkehatter

Valg og ønsket utbytte av verktøy

I denne fasen har vi valgt å bruke vektøyet seks tenke hatter fordi vi ville stimulere til kreativitet når forslag ble fremmet. Ønsket utbytte med bruk av seks tenkehatter, er å skape en forståelse rundt rotårsaken og komme opp med mulige tiltak for å eliminere problemet. Siden problemet virker vanskelig å fikse fra universitetet sin side måtte vi komme med noen kreative løsninger, og de seks tenkehattene fungerer godt for dette.

Spesifiseringer

Siden vi bare var fire, og det egentlig kreves seks, måtte to av oss innehave to roller samtidig.

Gjennomføring

Siden vi bare var fire tok to av oss på seg to hatter og resten en. Så startet vi å diskutere problemstillingen og hvordan vi burde gå inn for å eleminere rotårsaken. Hver enkelt gruppemedlems tilnærming var basert på hatten de hadde på hodet. Etter at vi var ferdig med de seks tenkehattene gikk vi fort igjennom de forskjellige forslagene, for å se på hva som var praktisk gjennomførbart. De andre forslagene ble luket bort.

Systematisk Innovativ Tenkning

Valg og ønsket utbytte av verktøy

Vi har valgt å benytte SIT i henhold til boken [1]. Ønsket utbytte med bruk av seks tenkehatter, er å skape en forståelse rundt rotårsaken og komme opp meg mulige tiltak for å eliminere problemet. Siden problemet virker vanskelig å fikse fra universitetet sin side måtte vi komme med kreative løsninger. De seks tenkehattene fungerer godt til dette.

Spesifiseringer

Ikke alle hovedprinsippene kunne gi tiltak. Der det ikke var mulig ble det presisert “Ikke gjennomførbart”.

Gjennomføring

Det første som ble gjort var å liste opp alle komponenter som eksisterer i problemets naturlige omgivelser. Deretter ble hver komponent analysert ut fra de fem hovedprinsip-

pene til SIT, der tiltak ble beskrevet. De mest lovende tiltakene ble tatt videre til en mer detaljert gjennomgang. Deretter ble det plukket ut fra de igjen, de tiltak som var mest egnet, og ble videre ført inn i en tiltaksplan.

5.1.7 Løsningsimplementering

Trediagram

Valg og ønsket utbytte av verktøy

Trediagram benyttes for å skape en liste over aktiviteter som må gjennomføres for å innføre de spesifikke tiltakene.

Spesifiseringer

Diagrammverktøyet draw.io ble brukt til å konstruere trediagrammet.

Gjennomføring

Dette verktøyet startet med å gruppere hovedtiltak til rotårsaken, deretter ble hver aktivitet som må gjennomføres for at tiltaket skal bli gjennomført gruppert. Disse underpunktene ble gruppert etter hvilken rekkefølge de skal bli implementert slik at tiltaket er mulig å gjennomføre.

5.2 Case 2: Kompromitterte brukerkontoer ved NTNU

5.2.1 Problemforståelse

Kritiske hendelser

Valg og ønsket utbytte av verktøy

For å lære mer om bakgrunnen til problemet bruker vi verktøyet kritiske hendelser for å se på frekvensen av misbruk som er registrert fra de kompromitterte kontoene. Slik kan vi kartlegge og forstå hva de kompromitterte kontoene brukes til. Ved bruk av dette verktøyet ønsker vi å få en oversikt over hvilke handlinger de kompromitterte kontoene utfører. Dette går i stor grad ut på hva som er motivasjonen til trusselaktørene. Vi ønsker å danne et bilde av hva de ønsker å oppnå ved å kompromittere kontoene, slik at vi kan bruke den informasjonen senere til å finne rotårsaken til at de blir kompromittert.

Spesifiseringer

Informasjonen som brukes i dette verktøyet ble gitt av oppdragsgiver. Dataene sier bare noe om frekvensen av sikkerhetshendelser, og ikke noe om viktigheten.

Gjennomføring

Sammen med oppgavebeskrivelsen fikk vi en liste over loggførte sikkerhetshendelser som hadde foregått det siste året hvor kompromitterte kontoer var involvert. Dataene ble sortert i synkende rekkefølge og lagt inn i en tabell for å visualisere frekvensen til de enkelte sikkerhetshendelsene, og dermed fokusområdene til trusselaktørene.

5.2.2 Idémyldring

Valg og ønsket utbytte av verktøy

Vi har valgt å benytte idémyldring på basis av RCA boken [1] sin fremgangsmåte for valg av verktøy, og på bakgrunn av vår tidligere kunnskap om hvordan brukere vanligvis kompromitteres. Vi valgte å organisere idémyldringen som et tankekart ettersom dette var en kjent løsning for gruppen. Den ustrukturerte tilnærmingen til idémyldring ble brukt på grunn av dens uformelle struktur. Ingen er heller dominerende i gruppen, som gjør det mulig for alle å komme med innspill. Hvis noen i gruppen hadde vært dominerende hadde vi heller gått over til å bruke skriftlig idémyldring, også kjent som idéskriving. Ønsket utbytte ved å bruke idémyldring var for å få en forståelse av hva som kan være rotårsaken til at ansatte sine kontoer blir kompromittert, og hvordan passord og brukernavn kan komme på avveie.

Spesifiseringer

Det er spesielt viktig å ikke omformulere eller diskutere forslagene etterhvert som de kommer, dette skal gjøres etter idémyldringsøkten er over.

Gjennomføring

Det første som ble gjort når økten startet var å kommunisere og skrive opp problemstillingen på en tavle. Vi diskuterte og prøvde å komme på mulige måter trusselaktører kan kompromittere brukerkontoer til de ansatte ved universitetet, og hvordan passord og brukernavn kan komme på avveie.

5.2.3 Datainnsamling

Spørreundersøkelse

Valg og ønsket utbytte av verktøy

Grunnen til at vi valgte i hovedsak kvantitativ spørreundersøkelse er at vi ønsker å finne relasjoner mellom dataene vi samler inn. Det er også mulighet for å gjøre statistiske beregninger på disse, noe vi anser som relevant for datainnsamlingen i dette caset. Fremstilling av data i grafer og tabeller er også et moment som gjorde at valget ble kvantitativ metode. Med den elektroniske spørreundersøkelsen ønsker vi å få informasjon fra personer som allerede har fått brukeren sin kompromittert. Informasjonen vil bestå av blant annet personens passordvaner, kjennskap til retningslinjer om passordbruk og epost-aktivitet. Vi håper å få minst 30 respondenter, som vil være akkurat nok for en kvalitativ analyse.

Spesifiseringer

Undersøkelsen var kvalitetskontrollert flere ganger av forskjellige personer, inkludert medstudenter, veileder og ikke minst oppdragsgiver. Undersøkelsen ble laget i SelectSurvey, med tilhørende NTNU tema for utformingen. Dette ble gjort for å få spørreundersøkelsen til å virke legitim, siden den har NTNU sin logo i hjørnet og nettadressen tilhører NTNU sitt domene. Noen av spørsmålene skal besvares på en skala fra 1-6. Denne skalaen valgte vi fordi vi ville tvinge respondentene til å havne på den ene eller andre siden av spekteret, og ikke velge i midten dersom de ikke visste.

Spørreundersøkelsen ble sendt ut til totalt 167 personer, men den nådde bare 157 av e-post addressene. Alle disse hadde fått sin NTNU konto kompromittert i tidsperioden 1. November 2016 til 1. April 2018. E-post listen ble opprettet av oppdragsgiver basert på intern data og sent ut på vegne av Seksjon for Digital Sikkerhet.

Det ble oppdaget et par småfeil i spørreundersøkelsen etter den var utsendt. Blant annet var det glemt et “vet ikke” alternativ på spørsmålet om de hadde en formening om hvor lang tid det hadde gått fra kompromittering til de fikk beskjed. Dette fikk vi fikset ved å legge til tekst om at du kunne la det være blankt om du ikke visste, slik at det ikke gikk altfor mye ut over svarene, og spørsmålet ble endret til å ikke være obligatorisk. Det var også glemt en kommentarboks helt i slutten av spørreundersøkelsen, som vi bestemte at vi ikke kunne plassere inn etter den var utsendt. Det var også et par småfeil i formulering, men dette fikk vi endret underveis. Endringene ble gjort på natten da vi antok ingen svarte.

Gjennomføring

Det første som ble gjort var å finne ut hva vi ville ha informasjon om. Deretter ble spørsmål for å få svar på dette lagd. Videre definerte vi hypoteser til nesten hvert spørsmål. Vi skrev også en tekst som skulle bli sendt ut sammen med spørreundersøkelsen for å oppmuntre til å ta den. Her ble det brukt mye patos ettesom dette er et ømfintlig tema. Undersøkelsen ble sendt ut på fredag 20. April.

5.2.4 Dataanalyse

Histogram

Valg og ønsket utbytte av verktøy

Vi har igjen valgt å benytte histogrammer for å fremlegge dataene fra spørreundersøkelsen. Dette gjøres fordi det er en god måte å fremstille data på et tilfredstillende vis for leserne. Ved å benytte histogram håper vi å få en visuell fremstilling av data som gjør det raskt og enkelt å forstå disse, og derfor lettere kunne trekke konklusjoner. I dette caset vil histogrammer stort sett bli brukt for å få en oversikt over svarprosent på enkeltsspørsmål.

Spesifiseringer

Det statistiske verktøyet SPSS ble brukt til å lage histogrammene. For at et histogram skal være gyldig, det vil si hvis vi skal kunne konkludere sikkert med noe, må det ha minst 30 svar.

Gjennomføring

Dataene ble eksportert til SPSS og diagramverktøyet ble valgt for å konstruere histogrammene. Deretter ble de analysert og eksportert til rapporten dersom et resultat ble funnet.

Affinitetsdiagram

Valg og ønsket utbytte av verktøy

Et av spørsmålene i spørreundersøkelsen var et kortsvar der respondentene kunne svare om de hadde noen formening om hvordan de ble kompromittert. Ved å bruke affinitetsdiagram håper vi på å få samlet og gruppert disse dataene slik at vi kan se om noe blir sagt flere ganger, og kan være en mulig årsak.

Spesifiseringer

Det nettbaserte verktøyet draw.io ble brukt til å konstruere affinitetsdiagrammet.

Gjennomføring

Hvert enkelt svar ble analysert hver for seg og gruppert under en av mange hovedkategorier. Deretter ble disse hovedkategoriene tegnet som bokser i nettleserverktøyet Draw.io. Disse boksene inkluderer frekvens av svar og differensiering av svarene under hovedkategoriene.

Statistiske analyseverktøy

Valg og ønsket utbytte av verktøy

Spørreundersøkelsen inkluderer blant annet spørsmål om kjennskap til ulike dokumentasjon og bevissthet på sikkerhet. Dette er spørsmål som blir besvar på en skala fra 1-6. Dette er data som statistisk analyse kan bli benyttet på. Det er også mange ja/nei spørsmål som disse verktøyene kan brukes på. Ved å bruke statistiske analyseverktøy som ANOVA og Independent-samples t-test ønskes det å finne tilsynelatende skjulte relasjoner eller forskjeller mellom demografien og kjennskap til retningslinjer, bevissthet på sikkerhet og e-post og passordvaner. Vi ønsker også å se om det er noen relasjoner mellom andre spørsmål. ANOVA ble brukt dersom den uavhengige variabelen består av mer enn to grupper. Dersom den bestod av to grupper ble Independent t-test heller brukt.

Spesifiseringer

Vi benytter t-test når den uavhengige variablen har to grupper. One-way ANOVA brukes når det er flere enn to grupper. Generelt regner vi med en signifikans på:

$$\alpha \leq 0,05$$

Gjennomføring

For demografien og de andre spørsmålene som ikke hadde tallsvar, ble svarene transformert til tall.

Forholdet mellom tallverdiene og svarkategoriene er som følger:

Kjønn:

- Mann: 1
- Kvinne: 2

Primærrolle:

- Ansatt: 1
- Student: 2

År ved NTNU:

- Under 2: 1
- 2-4: 2
- 5-9: 3
- 10-15: 4
- Over 15: 5

Alle Ja/Nei spørsmål:

- Ja: 1
- Nei: 2

Deretter ble testene kjørt på variablene.

5.2.5 Rotårsaksidentifisering

Årsak-virkningsdiagram

Valg og ønsket utbytte av verktøy

I dette caset har vi valgt et fiskebeindiagram på bakgrunn av at årsakene er spredt over flere variabler, og det er mulig at ytterligere årsaker eksisterer. Ved bruk av dette verktøyet ønsker vi å sitte igjen med en visuell fremstilling av rotårsakene til problemet. Dette vil gjøres ved å identifisere hva som skaper årsakene vi har funnet frem til i foregående fase.

Spesifiseringer

Det er anbefalt å bruke en tusjtavle for å tegne opp fiskebeindiagrammet, men vi valgte å bruke det nettbaserte programmet draw.io [16]. Draw.io er laget for å skape diagrammer med flere brukere involvert i sanntid. De hadde en egen mal for fiskebeindiagram som vi valgte å gå ut fra.

Gjennomføring

Stegene vi fulgte i prosessen er hentet fra boka om rotårsaksanalyse [1] og ble som følger:

1. Først ble problemet definert og skrevet i slutten av fiskebeindiagrammet.
2. Deretter ble hovedkategoriene skrevet ned i bokser. Disse er direkte tilknyttet resultatene fra analysen.
3. Videre startet vi å idémyldre alle mulige årsaker under hver kategori, en kategori om gangen. Disse ble fortløpende skrevet inn i diagrammet.
4. Til slutt analyserte vi de identifiserte årsakene og bestemte de mest sannsynlige rotårsakene

5 Whys

Valg og ønsket utbytte av verktøy

Etter fiskebeindiagrammet mente vi at det var sannsynlig at høyere nivå av årsaker kunne eksistere bak de identifiserte årsakene. Ved å bruke 5 Whys er det ønskelig å konfirmere om årsakene som ble fremhevet i fiskebeindiagrammet er faktiske rotårsaker, og ikke bare lav-nivå årsaker.

Spesifiseringer

Det ble tatt utgangspunkt i fem iterasjoner, men det er mulighet for flere eller færre avhengig av om spørsmålet kan besvares på en fornuftig måte.

Gjennomføring

Med dette verktøyet tar vi utgangspunkt i casebeskrivelsen, nemlig rotårsaken til kompromitterte kontoer ved NTNU. Ut fra dette brukte vi årsaker fra fiskebeindiagrammet over for å komme på årsaker som skal analyseres, samt prøvde å idémyldre et par nye. For hver av disse årsakene ble det spurt: “Hvorfor er dette en årsak av det orginale problemet?”. For hvert svar spør vi hvorfor igjen og igjen helt til vi finner rotårsaken.

5.2.6 Rotårsakseliminering

Systematisk Innovativ Tenkning (SIT)

Valg og ønsket utbytte av verktøy

Grunnen til at SIT ble valgt er at vi mener problemet kan løses i problemets naturlige omgivelser. Ved å bruke SIT metoden ønsker vi å få kreative idéer på hvordan vi kan finne en løsning til kompromitterte kontoer ved NTNU.

Spesifiseringer

SIT burde helst gjennomføres av 10-12 personer fra en rekke forskjellige fagområder, men siden vi ikke hadde så mange tok vi bare utgangspunkt i prosjektgruppen. Ikke alle SIT-prinsipper finner løsninger som er gjennomførbare for alle komponenter. I disse tilfellene vil det stå: “Ikke gjennomførbart”.

Gjennomføring

Først ble alle komponentene som omhandler problemet listet opp. Etter det ble de fem hovedprinsippene fra SIT brukt sekvensielt på komponentene for å utvikle løsninger på problemene. Deretter ble de mest relevante løsningene valgt ut og beskrevet i ytterligere

detalj. Videre ble de mest realistiske og gjennomførbare idéene trukket ut og fremhevet i en tiltaksplan.

5.2.7 Løsningsimplementering

Trediagram

Valg og ønsket utbytte av verktøy

For å få en oversikt over hva som må gjøres for å implementere tiltaksplanen bruker vi Trediagram til å dele opp aktivitetene og bestemme rekkefølgen. Ønsket utbytte ved å bruke trediagram er å redegjøre for og strukturere de aktiviteter som må gjøres for å innføre de spesifikke tiltakene.

Spesifiseringer

Trediagrammets aktiviteter gjøres i samme rekkefølge som en postorder trealgoritme. Dette betyr at aktivitetene gjøres fra venstre til høyre, der en starten nederst til venstre. Det er derimot ingen gitt rekkefølge man kan innføre tiltakene i, og noen tiltak vil ikke kunne eller behøve å innføre sammen.

Gjennomføring

Gjennomføringen av trediagrammet startet ved å gruppere hovedtiltak til rotårsaken. Deretter ble hver aktivitet som må gjennomføres for at tiltaket skal bli gjennomført delt opp. Disse underpunktene ble plassert etter hvilken rekkefølge de skal bli implementert slik at tiltaket er mulig å gjennomføre.

5.3 Case 3: Misbruk av NTNU sin infrastruktur til utvinning av kryptovaluta

5.3.1 Problemforståelse

Ytelsesmatrise

Valg og ønsket utbytte av verktøy

Vi har valgt å benytte ytelsesmatrise i dette caset for å utforske bruk av et nytt verktøy. Det ble også valgt fordi det er fordelaktig å undersøke de eksisterende kontrollene og fokusere på de kontrollene som ikke fungerer som ønsket. Ved bruk av dette verktøyet er det ønskelig å undersøke hvordan eksisterende kontroller fungerer i forhold til deres viktighet for NTNU.

Spesifiseringer

Vi definerte viktighet som hvor mye IT-reglementet stopper utvinning av kryptovaluta. Ytelse ble satt effekten av de eksisterende kontrollene som er i IT-reglementet per nå.

Gjennomføring

Prosessen startet ved å finne ut hvilke aspekter av problemet som skulle vurderes. Gruppen kom fram til å vurdere formene for kontroller som stopper eller reduserer sjansen for at trusselaktørene misbruker NTNU sin infrastruktur.

Disse skulle vurderes basert på viktighet og ytelse.

Matrisen ble tegnet opp i Excel der hver akse ble konstruert fra en til ni, og matrisen ble delt inn i fire områder:

Uviktig: Når både viktigheten og ytelsen er fra en til fem.

Overdrevent: Når viktigheten er fra en til fem og ytelsen er fra fem til ni.

Ok: Når både viktigheten og ytelsen er fra fem til ni.

Må forbedres: Når viktigheten er fra fem til ni, mens ytelsen bare er fra en til fem.

5.3.2 Idémyldring

Idémyldring

Valg og ønsket utbytte av verktøy

Vi har valgt å benytte Idémyldring på basis av RCA boken [1] sin fremgangsmåte for valg av verktøy. Vi ønsker ved bruk av idémyldring å få en forståelse av hva som kan være rotårsaken til at NTNU sine ressurser blir misbrukt til utvinning av kryptovaluta. Vi ønsker også å skape et godt grunnlag av idéer som kan brukes i datainnsamling i neste del av oppgaven.

Spesifiseringer

Det er spesielt viktig å ikke omformulere eller diskutere forslagene etterhvert som de kommer, dette skal gjøres etter idémyldringsøkten er over. Det ble gjennomført to idémyldringer på forskjellige aspekter av problemet.

Gjennomføring

Vi startet idémyldringen med å finne ut hva som burde fokuseres på av hvordan og hvorfor universitetet sine ressurser blir misbrukt til utvinning av kryptovaluta. Vi kom frem

til at begge deler var like viktige, og at vi burde ha to idémyldringer for å komme med flest mulige idéer som ville kunne hjelpe oss i hva som burde spørres om i datainnsamlingen. Den første idémyldringen omhandlet hvordan, mens den andre omhandlet hvorfor NTNU sine ressurser blir misbrukt til utvinning av kryptovaluta. Idémyldring prosessen var litt annerledes enn de vi hadde i de andre oppgavene. Denne gangen lignet det mer på idéskriving, der vi alle skrev inn idéene våre i et dokument. Det kunne fortsatt ikke defineres som det metoden beskriver som idéskriving siden dette ikke var anonymt.

Nominell gruppeteknikk (NGT)

Valg og ønsket utbytte av verktøy

Ettersom vi har dårligere tid på dette caset enn på de tidligere, har vi valgt å benytte NGT for å prioritere idéer. NGT er også et verktøy vi er interessert i å prøve ut for hovedrapporten.

Spesifiseringer

Ingen.

Gjennomføring

NGT ble utført ved at alle satte seg ned sammen og hadde 15 poeng hver å gi til forskjellige idéer. Idéene ble laget utifra forarbeidet som var blitt gjort i idémyldringsprosessen. De idéene som lignet på hverandre ble slått sammen og noen ble omformulert. Hver deltaker delte ut 1, 2, 3, 4 eller 5 poeng til idéene de mente var best. Dette var basert på hva de trodde ville være det viktigste å fokusere på videre i analysen. Etter vi var ferdige, gikk oppdragsgiver igjennom resultatene. Disse dataene kan sees i tabell 12.

5.3.3 Datainnsamling

Intervju

Valg og ønsket utbytte av verktøy

Siden vi hadde begrenset med tid (en måned), valgte vi å begrense informasjonsinnsamlingen til ett kvalitativt intervju.

Ønsket utbytte med dette intervjuet er å få et overblikk over hvordan utvinningsverktøy blir brukt, og hvordan de eksterne aktørene får verktøyene inn på PCene til de som oppholder seg på nettet til NTNU.

Spesifiseringer

På grunn av tidsbegrensningen og problemets tekniske art, begrenser vi datainnsamlingen til ett intervju. Det ble tatt lydopptak av intervjuet. Dette ble transkribert i etterkant.

Gjennomføring

Intervjuet ble gjennomført med en senior sikkerhetsanalytiker som jobber på SOCen til NTNU.

Vi utformet et intervju der spørsmålene bestod av diverse temaer vi ønsket å belyse for å finne rotårsaken. En del av spørsmålene gikk ut på å finne ut hvordan utvinningen blir oppdaget, hva slags handlingsrom de har for å håndtere hendelser og hvordan utvinningen som regel foregår.

Under intervjuet spurte vi om vi fikk ta lydopptak, og vi fikk ja til dette. Dermed kunne vi lett gå tilbake til svarene for å få det mest mulig nøyaktig til neste fase. Dette

ble transkribert i etterkant.

5.3.4 Dataanalyse

Affinitetsdiagram

Valg og ønsket utbytte av verktøy

Dataene våre besto ikke av nummere, men meninger og idéer så derfor har vi benyttet affinitetsdiagram.

Ønsket utbytte av å bruke affinitetsdiagram er å finne bindinger eller fellesnevnere som kan være til hjelp for å fjerne rotårsaken.

Spesifiseringer

Det nettbaserte verktøyet draw.io ble brukt til å konstruere affinitetsdiagrammet.

Gjennomføring

Analysen ble gjennomført ved å bruke transkripsjon fra intervjuet og stykke svarene opp i fem hovedgrupper. Disse hovedgruppene ble utredet mens analysen ble gjennomført.

5.3.5 Rotårsaksidentifisering

5 Whys

Valg og ønsket utbytte av verktøy

Vi valgte å benytte 5 whys siden vi mener det er sannsynlig at det finnes høy-nivå årsaker.

Ved å bruke 5 Whys er det ønskelig å finne rotårsaken til årsakene fremhevet i affinitetsdiagrammet. Målet her er å få frem rotårsaker, som vi kan bruke videre i rotårsakselimineringen.

Spesifiseringer

Vi tok utgangspunkt i å spørre "hvorfor" til vi fant rotårsaker. Om vi følte det vi kom frem til gikk veldig langt fra problemet, skulle vi gå et steg tilbake og prøve igjen; spesielt om vi kommer ned til lønnsomhet. Dette gjør vi fordi lønnsomhet kan være en rotårsak til at folk driver med utvinning, men ikke nødvendigvis til at dette skjer på NTNU.

Gjennomføring

Med dette verktøyet tar vi utgangspunkt i casebeskrivelsen; nemlig rotårsaken til krypto-utvinning på NTNU. Ut fra dette brukte vi funnene fra analysen for å komme på årsaker, samt prøvde å idémyldre et par nye. For hver av disse årsakene ble det spurt: "Hvorfor er dette en årsak av det originale problemet?". For hvert svar spør vi hvorfor igjen og igjen helt til vi finner rotårsaken. Det ble tatt utgangspunkt i fem iterasjoner, men det er mulighet for flere eller færre avhengig av om spørsmålet kan besvares på en fornuftig måte.

Feiltreanalyse

Valg og ønsket utbytte av verktøy

Ettersom det var flere årsaker som var bundet sammen etter gjennomføring av 5 Whys, valgte vi å benytte feiltreanalyse.

Ved bruk av dette verktøyet ønsker vi å få en oversikt over relasjoner mellom de forskjellige årsakene. Vi ønsker også å få sortert ut de årsakene som NTNU ikke har

mulighet til å gjøre noe med.

Spesifiseringer

Analysen bygger på hva som ble gjort i 5 Whys. Verktøy som ble brukt til utforming av tabellen var draw.io.

Gjennomføring

Med dette verktøyet tar vi utgangspunktet i resultatene fra 5 Whys til å finne rotårsakene. Her gikk vi steg for steg nedover og ser på årsaken til at enhver uønsket hendelse inntreffer.

5.3.6 Rotårsakseliminering

Systematisk Innovativ Tenkning (SIT)

Valg og ønsket utbytte av verktøy

Vi ville opprinnelig se på hvordan TRIZ fungerer. Da vi studerte verktøyet nøyere kom vi fram til at det kun var brukt til fysiske produkter. Seks tenkehatter ble ikke gjort da vi kun var to personer på denne delen. SIT ble valgt da vi ikke har vært helt fornøyd med verktøyet i de tidligere casene og vi ønsket å se om det er casene eller verktøyet sin feil.

Spesifiseringer

SIT burde helst gjennomføres av 10-12 personer, fra en rekke forskjellige fagområder, men siden vi ikke hadde så mange tok vi bare utgangspunkt i prosjektgruppen. Ikke alle SIT-prinsipper finner løsninger som er gjennomførbare for alle komponenter. I disse tilfellene vil det stå: “Ikke gjennomførbart”.

Gjennomføring

Det første som ble gjort var å liste opp alle komponenter som eksisterer i problemets naturlige omgivelser. Deretter ble hver komponent analysert ut fra de fem hovedprinsippene til SIT, der tiltak ble beskrevet. De mest lovende tiltakene ble tatt videre til en mer detaljert gjennomgang. Deretter ble det plukket ut fra de igjen, de tiltak som var mest egnet, og ble videre ført inn i en tiltaksplan.

5.3.7 Løsningsimplementering

Kraftfeltsanalyse

Valg og ønsket utbytte av verktøy

Vi valgte kraftfeltsanalyse fordi vi vi ville teste ut flere verktøy.

Ønsket utbytte fra kraftfeltsanalyse er å få vite hva som er for og hva som er mot implementering av tiltakene. Dette verktøyet gir en oversikt over hvilke tiltak som er lettest å gjennomføre.

Spesifiseringer

Ingen.

Gjennomføring

Kraftfeltsanalysen ble gjort ved at vi tok tiltakene fra problemelimineringen og hadde en idémyldring for å se hva som talte for og imot tiltakene. Deretter ble styrken av disse kreftene estimert. Tilslutt ble alt lagt inn i en figur som viser styrkene både for og imot

et gitt tiltak.

6 Resultater og analyse fra Case 1: Ulovlig fildeling på universitetsnettet til NTNU

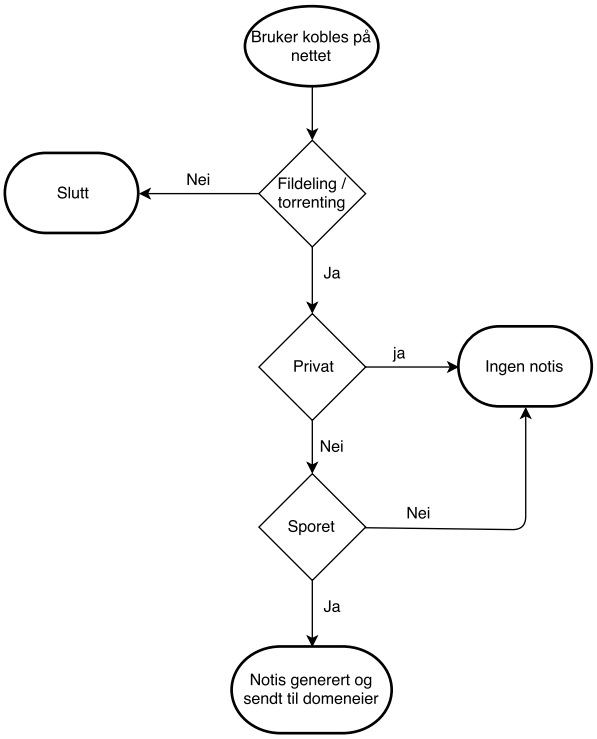
I dette kapittelet fremlegger vi våre resultater i alle fasene i case 1.

6.1 Problemforståelse

I denne fasen vil vi forsikre oss om at problemet er forstått i dypere detalj. Verktøyene som brukes her skal gi en bedre forståelse av omfanget og de ulike aspektene ved et problem.

6.1.1 Flytdiagram

Flytdiagrammet under viser det vi anser som et normalt hendelsesforløp til hvordan man laster ned materiale på universitetsnettverket.



Figur 7: Flytdiagram for fildeling

Først kobles en bruker seg til universitetetnettet, enten gjennom VPN, direkte fra campus eller studenthybler. Deretter velger brukeren enten å bruke nettet legitimt eller starter å laste ned filer. Hvis brukereren bruker det til legitimt bruk bryr vi oss ikke om disse. Hvis vedkommende har bestemt seg for å laste ned, har personen muligheten til å gjøre dette gjennom en privat nedlastingsside. Det neste som kan skje med de som bruker

offentlige tjenester er at de torrentene de laster ned blir sporet, og da får domeneeier et notis om ulovlig nedlasting.

6.1.2 Kritiske hendelser

For å gå dypere i detalj har vi undersøkt kritiske hendelser som inngår i problemstillingen.

Tilnærmingen fokuserte på hva studenter laster ned når de bedriver ulovlig fildeling. Derfor ble det stilt spørsmål til studenter ved Sit Bolig. På forhånd hadde vi en hypotese om at det var filmer og serier som ble lastet ned hyppigst.

Spørsmål stilt til intervjuobjekter:

- Bor du, eller har du bodd i Sit Bolig i løpet av studiet? (Hvis nei, avslutt intervju)
- Bruker du, eller har du brukt torrents til å laste ned opphavsrettsbeskyttet materiale mens du bodde i Sit Bolig? Hvis ja, hvilke av følgende kategorier laster du ned fra? (Viser kategoriene)

Dette er resultatet fra spørringene:

Antall spurt: 13

Antall som aldri laster ned: 4

Tabell 2: Oversikt over kvantiteten av kritiske hendelser ved torrenting av opphavsrettsbeskyttet materiale

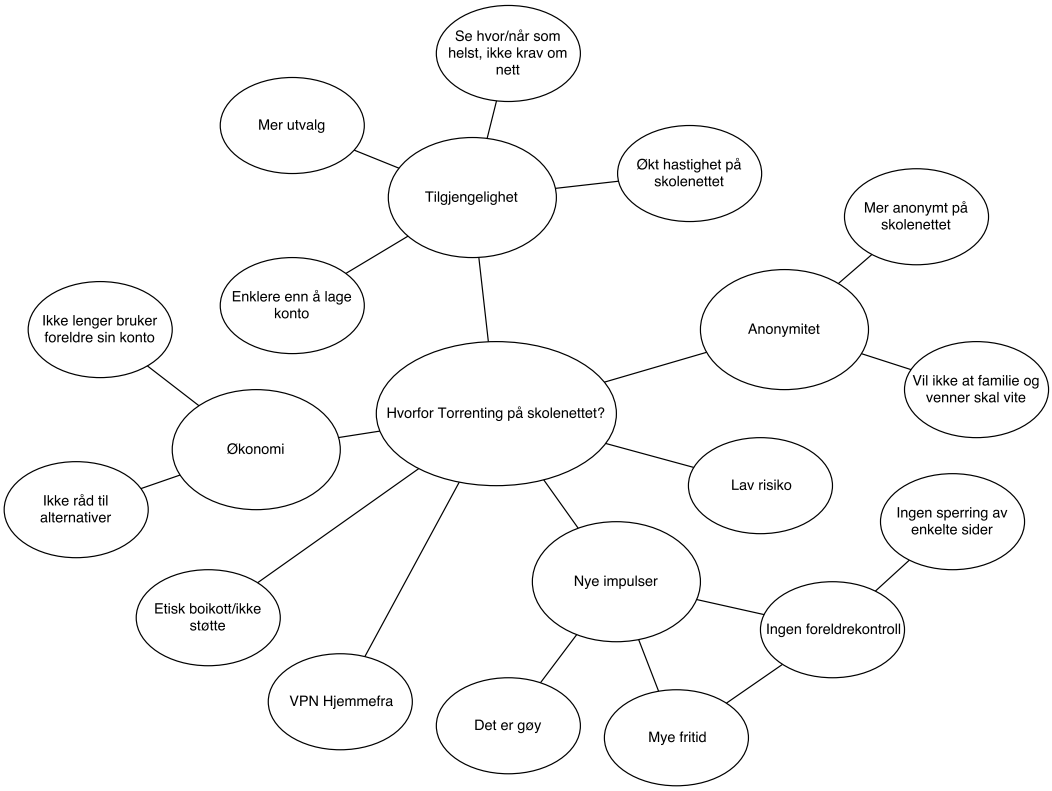
Fildelingskategori	Frekvens
Filmer og serier	8
Spill	3
Skolebøker	2
Musikk	2
Programvare og bøker utenom skolebruk	1
Programvare til skolebruk	0
Annet	0

Merk: Hver person kan svare at de laster ned fra flere kategorier.

Vi kan se at det er filmer og serier som er den med størst frekvens i undersøkelsen, noe som bekreftet vår hypotese. Dette funnet vil tilsi at vi kan fokusere mye mer på filmer og serier senere i prosessen siden vi vet dette er en stor del av problemet.

6.2 Idémyldring

Denne seksjonen presenterer resultater og konklusjoner fra idémyldringsfasen. Problemstillingen i idémyldringen ble definert som “Hvorfor folk torrenter på universitetsnettet”. Etter idémyldringen var ferdig ble det gjort en vurdering av resultatene og de ble kategorisert i henhold til likhetstrekk, under en fellesnevner som for eksempel Økonomi. Resultater og gruppering er som vist i figur 8 under.



Figur 8: Resultater og gruppering av idémyldringen

Resultatene er gruppert inn i fire hovedkategorier: Økonomi (som går på kjøpekraften til den enkelte person), tilgjengelighet (hvor god tilgang en har på tjenester), anonymitet (foreldre kunne blant annet overvåke før, samt at de føler seg tryggere når det er flere på samme nett) og nye impulser (mer frihet og fritid, og påvirkning av nedlastningskulturen).

Merk at noen årsaker kunne ikke plasseres i én kategori og er derfor direkte knyttet til problemstillingen.

6.3 Datainnsamling

Hypotesen vi går inn i undersøkelsen med er at folk laster ned opphavsrettsbeskyttet materiale fordi det er lett tilgjengelig, tilknyttet liten til ingen kostnad og ikke minst fordi det er svært lav risiko.

Den ferdige spørreundersøkelsen finnes i vedlegg J.

Undersøkelsen ble begrenset til Gjøvik og endte med 97 svar totalt. Dette er 18.6% av de 522 beboerne i Sit Bolig. Av disse var det 34 som svarte at de hadde lastet ned opphavsrettsbeskyttet materiale i hybelen, det er 35% av de spurte.

For å øke besvarelsene ble det laget en plakat som ble lagt i postkasser og hengt opp på diverse tavler. Denne plakaten finnes i vedlegg D.

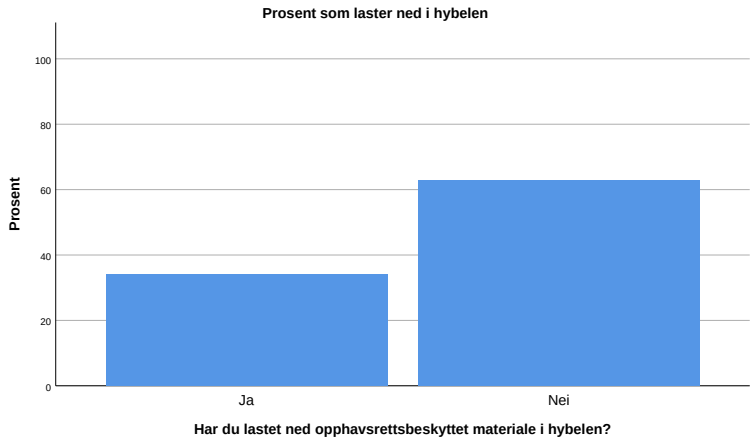
Det ble også laget en engelsk versjon for de internasjonale studentene.

6.4 Dataanalyse

I denne fasen analyseres dataene som er samlet inn, og ved hjelp av statistiske verktøy kan vi trekke konklusjoner basert på svarene.

6.4.1 Omfang

Figur 9 under viser hvor stor andel av de 97 som ble spurt som laster ned. Rundt 35% sier at det laster ned, som er en stor del av studentmassen. Det kan ha en påvirkning at undersøkelsen har en overvekt av studentene kommer fra informatikk- og datarelaterte studier, men det diskuterer vi nærmere senere.



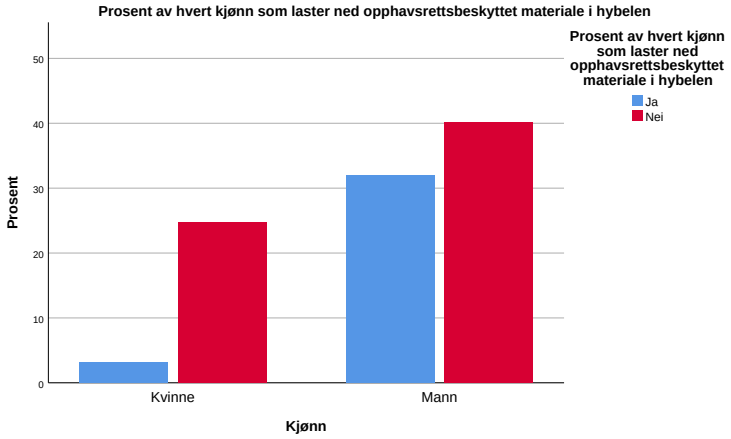
Figur 9: Hvor mange som laster ned av de spurte

6.4.2 Demografi

I spørreundersøkelsen ble informasjon om fire forskjellige demografier samlet inn: Kjønn, fakultet, studentby og alder. Det er viktig å nevnte at det ikke ble samlet inn lik mengde svar fra alle kategoriene, så dette må vi tenke på når vi analyserer dataene. Det var for eksempel overvekt av menn som besvarte undersøkelsen. Av respondentene var det 27.8% kvinner og 72.2% menn. Det var også overvekt av personer som er mellom 20 og 25 år; disse tilsvarte 74.2% av de spurte. På fakultet og studentby ønsket vi i hovedsak å få inn relativt spredte svar, men det ble overvekt av personer fra fakultet for informasjonsteknologi og elektroteknikk. I tillegg ble det også en overvekt av personer fra Kallerud studentby. Disse inkluderte henholdsvis 50.5% og 52% av respondentene. De komplette frekvenstabellene over demografien finnes i vedlegg E.

Kjønnsforskjeller

Vi ønsket også å undersøke om det er noen kjønnsforskjeller i hvem som laster ned. Under ser vi forholdet mellom kjønnene.

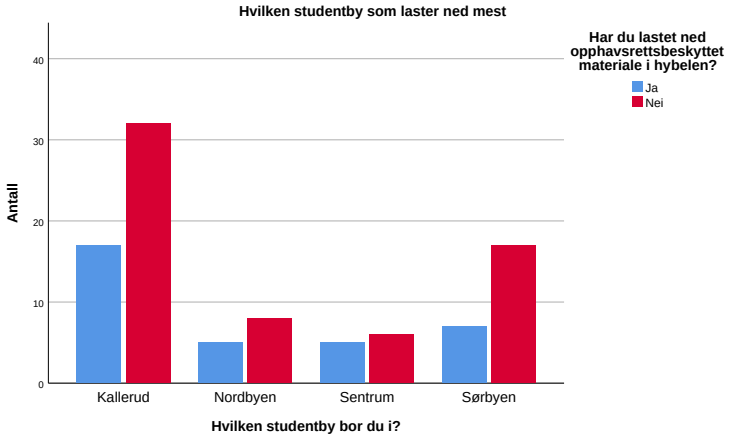


Figur 10: Hvor mange fra hvert kjønn som laster ned

Vi kan se over at det er i hovedsak menn som laster ned ulovlig, mens kvinner har svart at de i stor grad ikke laster ned. Dette blir selvfølgelig påvirket at det er få kvinner i IT-relaterte studier, som vi har funnet ut at utgjør noe mer av nedlastingen. Det er derimot vanskelig å vite helt sikkert om det er fordi kvinner er underrepresentert i IT studier som gir utslag, eller om det er kvinner generelt sett som ikke laster ned. Der er likevel en mer signifikant forskjell mellom kjønnene enn det er mellom IT studier og andre studier som vist i figur 71, så vi velger å tolke det som at kvinner laster ned mindre enn menn.

Forskjeller mellom studentbyer

Samtlige studentbyer har et kablet nettverk fra Uninett som er godt egnet for nedlasting, enten det er lovlig eller ulovlig nedlasting. Det er derimot noen forskjeller i hastighet på enkelte studentbyer. Kallerud har ti ganger så høy hastighet på nettet som de andre studentbyene. Derfor ønsket vi å undersøke om dette hadde noe relevans i forhold til hvor mange som laster ned ulovlig.



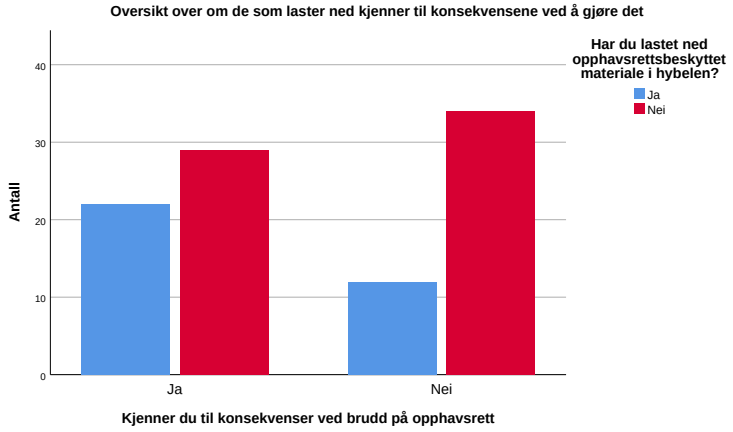
Figur 11: Hvor mange fra hver studentby som laster ned

På grunn av lav oppslutning på Nordbyen og Sentrum er det vanskelig å si noe sikkert

på dem, mens Kallerud og Sørbyen ikke varierer så veldig fra hverandre. Når vi bruker histogrammer ser vi ingen signifikant forskjell mellom studentbyene når det kommer til nedlasting som vi kan si med sikkerhet.

6.4.3 Konsekvenser ved nedlasting

Et spørsmål som ble spurt i spørreundersøkelsen var hvor godt kjent de var med mulige konsekvenser ved ulovlig nedlasting. Det kunne være relevant å se om det var noen spesiell sammenheng mellom de som ikke kjente til konsekvensene og de som lastet ned.



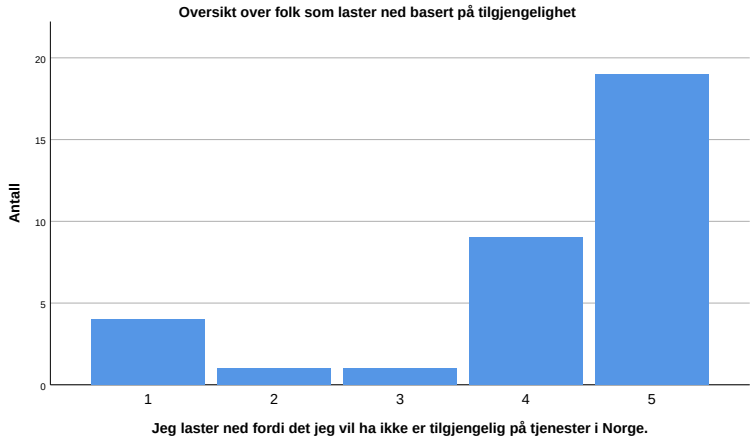
Figur 12: Hvor mange som kjenner til konsekvenser ved å laste ned

Det viser seg faktisk at de som laster ned har bedre kjennskap til konsekvensene enn de som ikke gjør det. Det kan kanskje ha noe å gjøre med at de er mer opptatt av problemområdet enn de som ikke laster ned. De som ikke laster ned i første omgang har kanskje ingen grunn til å sjekke konsekvensene av det. I tillegg fant vi ut at IT-studenter kjenner konsekvenser bedre enn de andre, og de har også høyere andel nedlastere. Vi prøvde å kjøre samme test på hvor godt de kjenner til IT-reglementet til NTNU [7] og kom til samme konklusjon som over. Dette histogrammet kan sees her. En grunn til dette kan også være at IT-studenter kjenner bedre til IT-reglementet, som vist her. Og siden IT studenter er i overvekt, må dette tas i betraktning.

En mulig teori vi ønsket å prøve ut var om mange som lastet ned ikke kjente til konsekvensene ved ulovlig nedlasting eller NTNU sitt IT-reglementet, og lastet ned på grunn av det. Dette ble altså delvis motbevist.

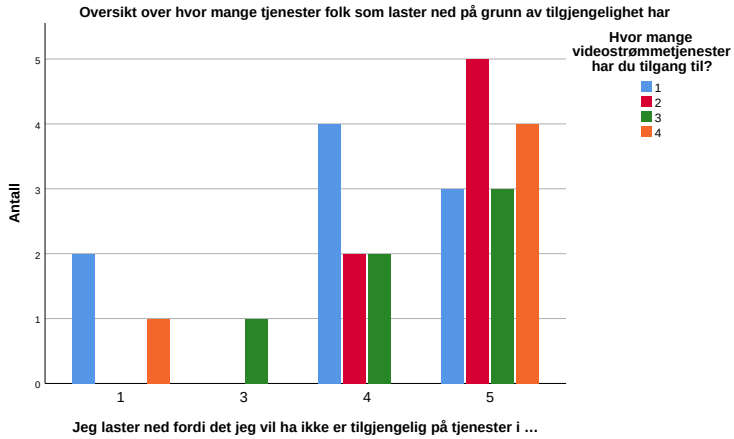
6.4.4 Årsaker til nedlasting

I spørreundersøkelsen kom vi med seks påstander til hvorfor respondentene laster ned, som de besvarte på en likert-skala fra 1 til 5, der 1 er i liten grad og 5 er i stor grad. Etter å ha analysert alle seks påstandene ved hjelp av SPSS og histogrammer fant vi én påstand som hadde en graftopp der respondentene svarte positivt. De aller fleste svarte de var enige i at de lastet ned på grunn av tilgjengelighet som vist i figur 13 under.



Figur 13: Hvor mange som laster ned på grunn av tilgjengelighet av de spurte

Dette vil si at det er godt mulig at tilgjengeligheten er en årsak til om en laster ned eller ikke, og er verdt å dokumentere til videre analyse. Siden tilgjengelighet betyr så mye, var det naturlig å utforske det ytterligere. Vi fant ut at det kunne være relevant å vite om de som brydde seg om tilgjengelighet hadde tilgang på strømmetjenester, og i så fall hvor mange.



Figur 14: Korrelasjonen mellom de som laster ned på grunn av tilgjengelighet og hvor mange tjenester de har tilgang på

Her viser det seg at de som laster ned på grunn av tilgjengelighet også har en god del strømmetjenester. Dette sier at mange av disse er storforbrukere av film og serier, og at det ikke har så mye å si om de har tilgang til tjenestene eller ikke. Dette vil muligens utelukke en løsning i form av at NTNU tilbyr en tjeneste, siden de kommer til å laste ned uansett.

6.4.5 Statistisk analyse

I denne delen benytter vi et par statistiske verktøy for å analysere dataene. Verktøyene vi har brukt er en independent-samples t-test og en one-way ANOVA. Begge disse ble

beregnet i det statistiske verktøyet SPSS. Vi regner med en signifikans på

$$\alpha \leq 0,05$$

Independent-samples t-test

Vi valgte å kjøre en independent-samples t-test for å undersøke om det at Kallerud har ti ganger så raskt nett har noen innvirkning på om en laster ned eller ikke. Vi delte opp Kallerud og de andre studentbyene hver for seg, og oversatte nei og ja svarene fra om du hadde lastet ned til henholdsvis 1 og 2. Under ser vi statistikken for svarene.

Group Statistics

	Hvilken studentby bor du i?	N	Mean	Std. Deviation	Std. Error Mean
Har lastet ned	Kallerud	49	1.3469	.48093	.06870
	Andre	48	1.3542	.48332	.06976

Figur 15: Gruppestatistikk av studentbyer for om de laster ned eller ikke

Vi kan allerede her se at svarene ikke differensierer noe særlig. I testen under ser vi selfølgelig derfor at det ikke er noen signifikans.

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Har lastet ned	Equal variances assumed	.022	.883	-.074	95	.941	-.00723	.09791	-.20160	.18714
	Equal variances not assumed			-.074	94.937	.941	-.00723	.09791	-.20161	.18716

Figur 16: Independent-sample t-test av studentbyer mot om de laster ned eller ikke

Dette betyr at det er ingen forskjeller på personer som bor på Kallerud og de som bor på andre studentbyer når det kommer til om de laster ned, til tross for ti ganger så rask nedlasting og opplasting.

ANOVA-analyse

I denne analysen ser vi på forskjeller mellom IT fakultetet og de andre fakultetene i henhold til svarene som ble gitt på påstandene. Det ble i tillegg også kjørt analyser basert på kjønn og alder, men med alder var datafordelingen for lav på enkelte alternativer til å kunne si noe om det så den har uteblitt i rapporten. På kjønn brukte vi ANOVA til å se forskjeller i svar på påstandene og kjennskap til IT-reglement. Bare kjennskap til IT-reglement vises her siden det var det eneste med både tilstrekkelig svar fra hvert kjønn og signifikans i forskjellen.

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
Jeg laster ned fordi jeg føler jeg ikke har råd til alternativer.	Andre	13	3.38	1.502	.417	2.48	4.29	1	5
	IT	21	2.71	1.189	.260	2.17	3.26	1	5
	Total	34	2.97	1.337	.229	2.50	3.44	1	5
Jeg laster ned fordi det jeg vil ha ikke er tilgjengelig på tjenester i Norge.	Andre	13	4.15	1.463	.406	3.27	5.04	1	5
	IT	21	4.10	1.300	.284	3.50	4.69	1	5
	Total	34	4.12	1.343	.230	3.65	4.59	1	5
Når jeg laster ned på skolenettet føler jeg meg mer anonym enn ellers.	Andre	13	2.08	1.188	.329	1.36	2.79	1	5
	IT	21	1.48	.750	.164	1.13	1.82	1	3
	Total	34	1.71	.970	.166	1.37	2.04	1	5
Jeg laster ned fordi det er lav sannsynlighet for å bli tatt	Andre	13	3.54	1.450	.402	2.66	4.41	1	5
	IT	21	2.62	1.161	.253	2.09	3.15	1	4
	Total	34	2.97	1.337	.229	2.50	3.44	1	5
Jeg laster ned fordi jeg synes kvaliteten på strømmetjenester er for dårlig	Andre	12	3.58	1.676	.484	2.52	4.65	1	5
	IT	21	3.00	1.449	.316	2.34	3.66	1	5
	Total	33	3.21	1.536	.267	2.67	3.76	1	5
Jeg laster ned fordi jeg ikke ønsker å støtte selskapet som eier opphavsretten.	Andre	13	2.00	1.472	.408	1.11	2.89	1	5
	IT	21	1.86	1.153	.252	1.33	2.38	1	4
	Total	34	1.91	1.264	.217	1.47	2.35	1	5
Hvor kjent er du med IT-reglementet til NTNU?	Andre	44	2.07	1.246	.188	1.69	2.45	1	5
	IT	52	2.65	1.266	.176	2.30	3.01	1	5
	Total	96	2.39	1.284	.131	2.13	2.65	1	5

Figur 17: Descriptives for IT fakultetet og de andre fakultetene når det kommer til påstander

I tabellen over ser vi at IT studentene sier seg mer uenig i samtlige påstander, og noen mer enn andre. De svarer i tillegg at de er bedre kjent med IT-reglementet. Det er spesielt påstandene om råd til alternativer, anonymitet, sannsynlighet for å bli tatt og kjennskap til IT-reglementet som er mest relevant å se på. ANOVA analysen under viser om det er noe signifikans mellom svarene.

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Jeg laster ned fordi jeg føler jeg ikke har råd til alternativer.	Between Groups	3.608	1	3.608	2.085	.158
	Within Groups	55.363	32	1.730		
	Total	58.971	33			
Jeg laster ned fordi det jeg vil ha ikke er tilgjengelig på tjenester i Norge.	Between Groups	.028	1	.028	.015	.904
	Within Groups	59.502	32	1.859		
	Total	59.529	33			
Når jeg laster ned på skolenettet føler jeg meg mer anonym enn ellers.	Between Groups	2.898	1	2.898	3.293	.079
	Within Groups	28.161	32	.880		
	Total	31.059	33			
Jeg laster ned fordi det er lav sannsynlighet for å bli tatt	Between Groups	6.787	1	6.787	4.162	.050
	Within Groups	52.183	32	1.631		
	Total	58.971	33			
Jeg laster ned fordi jeg synes kvaliteten på strømmetjenester er for dårlig	Between Groups	2.598	1	2.598	1.105	.301
	Within Groups	72.917	31	2.352		
	Total	75.515	32			
Jeg laster ned fordi jeg ikke ønsker å støtte selskapet som eier opphavsretten.	Between Groups	.164	1	.164	.100	.754
	Within Groups	52.571	32	1.643		
	Total	52.735	33			
Hvor kjent er du med IT-reglementet til NTNU?	Between Groups	8.175	1	8.175	5.172	.025
	Within Groups	148.565	94	1.580		
	Total	156.740	95			

Figur 18: Forskjellen mellom IT fakultetet og de andre fakultetene når det kommer til påstander

Det viser seg å være signifikant forskjell på IT og de andre fakultetene når det kommer til lav sannsynlighet for å bli tatt og kjennskap til IT-reglement. Respondenter fra IT fakultetet er mer uenig i at de laster ned på grunn av lav sannsynlighet for å bli tatt $(\alpha = 0,050)$, og de kjenner også IT-reglementet bedre $(\alpha = 0,025)$.

Descriptives

Hvor kjent er du med IT-reglementet til NTNU?

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
1	27	1.85	1.167	.225	1.39	2.31	1	5
2	69	2.59	1.276	.154	2.29	2.90	1	5
Total	96	2.39	1.284	.131	2.13	2.65	1	5

Figur 19: Descriptives for kjønn når det kommer til kjennskap til IT-reglement

Kvinner er 1 og menn er 2 i disse tabellene. Vi ser fra tabellen over at kvinner svarer at de kjenner til IT-reglementet noe dårligere enn menn.

ANOVA

Hvor kjent er du med IT-reglementet til NTNU?

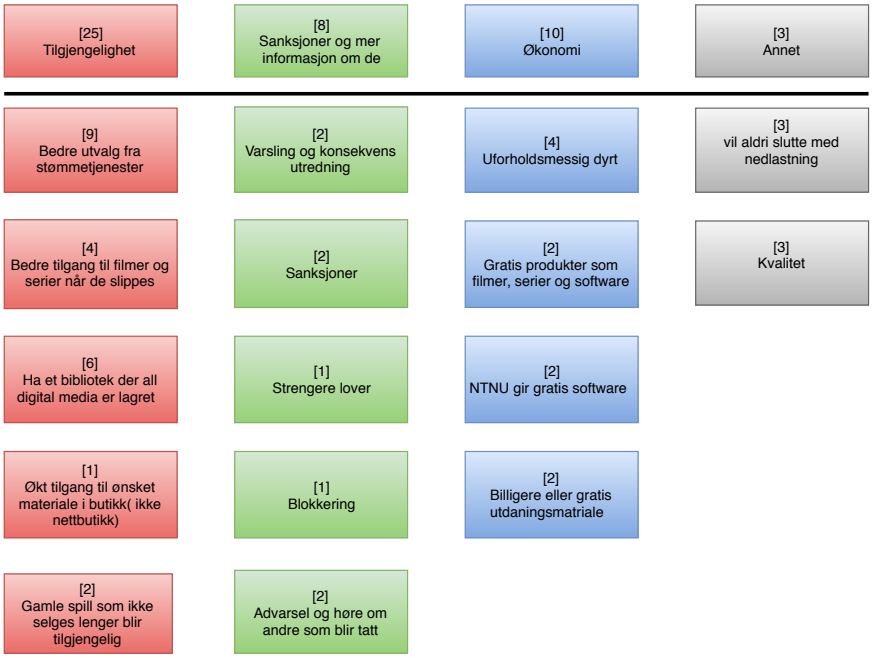
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	10.694	1	10.694	6.883	.010
Within Groups	146.045	94	1.554		
Total	156.740	95			

Figur 20: Forskjellen mellom kjønnene når det kommer til kjennskap til IT-reglement

I tabellen over ser vi at menn svarer at de har generelt sett bedre kjennskap til IT-reglementet, til tross for at vi fra tidligere vet at menn er overrepresentert i de som laster ned ulovlig. Noe av det kan forklares med at IT-studenter stort sett er menn, og de kjenner reglementet bedre.

6.4.6 Affinitetsdiagram

I spørreundersøkelsen spurte vi om hva som skal til for at deltagerne vil slutte med fildeling. Svarende vi fikk ble sortert inn i 16 grupper, og organisert under fire hovedkategorier. Hvis noen av deltakere har kommet med flere forslag har hvert av forslagene fått en stemme.



Figur 21: Hva skal til for at personer vil slutte med nedlasting?

Denne analysen gir oss ikke rotårsaken til at studenter laster ned, men kan brukes til å gi pekepinne på hva studenter mener skal til for at de vil slutte med nedlasting. Vi kan se på affinitetsdiagram at det er virker å være tre grunner til at personer laster ned. Det å gjøre materiale mer tilgjengelig virker som den beste løsningen for å stoppe personer fra å laste ned. Dette samsvarer med de tidligere funnene i figur 13. Problemet med tilgjengelighet er at det er et mer global problem, basert på at en del av de tradisjonelle mediene fortsatt bruker geografiske begrensinger. Så da har vi igjen kategoriene økonomi

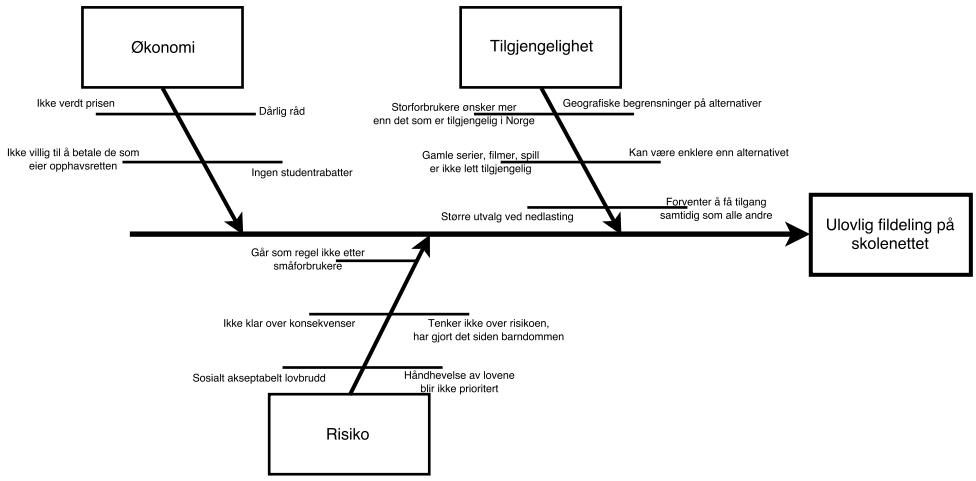
og sanksjoner. Ser man på saksjoner så er det flere som mener at det å opplyse om konsekvenser og andre som blir tatt kan være et godt tiltak, som er tildels motstridende med figur 12. På økonomi eksisterer det et flertall som mener at de har ikke har noe imot å betale for produktet så lenge de mener det er rimelig. Og et mindretall som vil ha gratis produkter. Her kan NTNU kanskje gjøre noe i form av muligens studentrabatter eller de betaler for produktet.

6.5 Rotårsaksidentifisering

Arbeidet i denne fasen går ut på å identifisere rotårsaken.

6.5.1 Årsak-virkningsdiagram

Problemet i fiskebeindiagrammet ble beskrevet som ulovlig fildeling på universitetnettet. Hovedkategoriene vi ønsket å utforske har vi basert på dataanalysen i forrige fase for å finne de mest relevante. Disse var etter vår mening Økonomi, Risiko og Tilgjengelighet. Idémyldringen var i stor grad basert på data og funn fra analysen, med innslag fra den første idémyldringen og andre nye idéer som dukket opp.



Figur 22: Fiskebeindiagram over hovedkategorier og årsaker

Etter videre analyse av figuren har vi kommet frem til at rotårsaken til fildeling er en kombinasjon flere faktorer, men én skiller seg ut, nemlig tilgjengelighet. Med tilgjengelighet mener vi spesifikt at folk bedriver ulovlig fildeling fordi det er dårligere utvalg på alternative tjenester i Norge. Det finnes også noen mindre årsaker som påvirker folk til å laste ned. Blant dem er at mange føler tjenestene ikke er verdt prisen de må betale når de bare får tilgang på en begrenset mengde materiale. Den siste årsaken går på at håndheving av lovene knyttet til ulovlig fildeling ikke blir prioritert, og derfor har skapt en kultur der det er sosialt akseptabelt å laste ned. Rotårsakene er listet etter viktighet der den første er hovedårsaken:

1. Dårligere utvalg på alternative tjenester i Norge
2. Tjenestene er ikke verdt prisen
3. Håndheving og kommunisering av lovene knyttet til ulovlig fildeling blir ikke prioritert

6.6 Rotårsakseliminering

Arbeidet i denne fasen går ut på å finne løsninger for å eliminere rotårsaken.

6.6.1 De seks tenkehattene

Ut i fra prosessen med de seks tenkehattene kom vi fram til både gjennomførbare og ikke gjennomførbare tiltak.

Gjennomførbare tiltak

- Tilby produkter fra selskap som universitetet får flest notifikasjoner fra.
- Stenge torrentprotokollen for alle på nettverket.
- Grense på nedlastning og opplastning av data.
- Være strengere når det gjelder oppfølging av IT-reglementet.
- Bytte ISP til studentboligene.
- Oppmerksomhetskampanje om konsekvenser.
- Avtale med kino for billige eller gratis nye filmer

Ikke gjennomførbare tiltak

- Alt av materiale blir gratis og tilgjengelig på ett samlet sted
- Fjerne geografiske blokkeringer

Noen av disse vil ikke være gjennomførbare for NTNU så vi har valgt å ikke ta de med videre til implementering, men de er fortsatt interessante å nevne. Av de 11 forslagene er det kun 4-5 vi mener har høy sannsynlighet for å bli kvitt rotårsaken, helt eller delvis; eller flytter rotårsaken vekk fra NTNU ansvarsområde. Etter videre vurdering har vi kommet fram til de mest lovende løsningene for å fjerne rotårsaken. Disse beskrives i ytterligere detalj under.

Tiltak som fjerner rotårsaken til at folk laster ned

1. Alt av materiale blir gratis og tilgjengelig på ett samlet sted
2. Fjerne geografiske blokkeringer
3. Tilby produkter fra selskap som universitetet får mest notis fra
4. Prøve for studenter for å få full hastigehet på nettverk

Tiltak som fjerner rotårsaken til at universitetet får notifikasjon fra opphavsrettshaverne

1. Bytte ISP til studentboligene
2. Stenge torrentprotokollen for alle på nettverket

Rotårsaken til at folk bedriver ulovlig fildeling er ikke et problem som lett kan løses av universitetet. Vi har gitt et par forslag til hva som kan fjerne rotårsaken helt, men av disse er ikke alle gjennomførbare for universitetet. Vi har også foreslått et par tiltak som ikke fjerner rotårsaken og noen som fjerner rotårsaken til hvorfor folk laster ned. De tiltakene som ikke fjerner rotårsaken vil flytte rotårsaken bort fra NTNU sitt ansvarsområde.

6.6.2 Systematisk Innovativ Tenkning (SIT)

Alle komponenter som eksisterer i problemets naturlige omgivelser listes under:

- Lite kunnskap om konsekvenser
- Raskt internett

- Alt er tilgjengelig samtidig overalt
- Økonomi

På hver komponent blir de fem hovedprinsippene fra SIT brukt til å myldre frem idéer på ulike tiltak som kan fjerne rotårsakene eller bedre problemet.

Lite kunnskap om konsekvenser

- **Attributtavhengighet** Løfte opp kunnskapen om konsekvenser og lover.
- **Komponentkontroll** Ha en test for å se at folk forstår IT-reglementet og mulig kursing.
- **Erstatning** Ikke gjennomførbart
- **Forkastning** Ikke gjennomførbart
- **Oppdeling** Ikke gjennomførbart

Raskt internett som universitetet eier

- **Attributtavhengighet** Sperre torrenting protokollen.
- **Komponentkontroll** Ikke gjennomførbart.
- **Erstatning** Ha tregere internett, slik at folk ikke laster ned hjemme.
- **Forkastning** Fjerne internett fra Sit boligene eller bytte ISP.
- **Oppdeling** Ikke gjennomførbart

Tilgjengelighet

- **Attributtavhengighet** Få rettighetshaverne til å samle alt innhold til ett sted
- **Komponentkontroll** Ikke gjennomførbart.
- **Erstatning** Tilby gratis filmer/serier og spill.
- **Forkastning** Ikke gjennomførbart
- **Oppdeling** Ikke gjennomførbart

Økonomi

- **Attributtavhengighet** Mer penger fra lånekassen.
- **Komponentkontroll** Universitetet tilbyr det som blir lastet ned mest
- **Erstatning** Universitetet gjør innhold gratis
- **Forkastning** Ikke gjennomførbart
- **Oppdeling** Ikke gjennomførbart

Løsningene sorteres deretter og diskuteres ut fra hvilke som er mest relevante.

Løfte opp kunnskapen om konsekvenser og lover Universitetet tilbyr et kurs, gjerne ett nettkurs, med en tilhørende prøve for å se hvor mye folk får med seg.

Bytte ISP Bytter Sit ISP vil ansvaret for notisene flyttes fra universitetet til den nye ISP.

Tilby gratis produkter Her kan universitetet se gjennom de ulike notisene de har fått, og finne ut hvilket selskap som blir lastet ned mest, for så å prøve å tilby deres filmer og serier.

Alt materiale tilgjengelig på ett sted Om alt materialet er tilgjengelig på ett sted vil dette fjerne problemet med at eneste og/eller enkleste måten å få tak i produkter er ved å laste dem ned.

Deretter diskuteres løsningene videre og de mest lovende idéene blir med i tiltaksplanen.

6.6.3 Tiltaksplan

Gjennomføring av disse tiltakene vil i hovedsak administreres av universitetet og Sit.

Alt av materiale blir gratis og tilgjengelig på ett sted

Dette tiltaket vil fjerne rotårsaken helt og holdent. Alt materiale blir gratis, gitt ut på samme tid over hele verden og tilgjengelig på ett sted. Dette tiltaket har svært høy kost, men også høy nytte. Universitetet må skaffe avtaler med alle produsenter og tilby det til studentene. Dette vil fjerne rotårsaken, men er urealistisk.

Tilby produkter fra selskap som universitetet får flest notiser fra

Går ut på å finne de mest populære selskapene som universitetet får notis fra, skaffe en avtale med rettighetshaverne eller som er distributør for rettighetshaverene og gjøre dette tilgjengelig for studenter. Dette vil fjerne rotårsaken på at de laster ned fra dette selskapet. Dette har middels start kostnad som starter med å kartlegge hvilke firmaer som har høy frekvens av notiser. Kostnaden tilknyttet dette tiltaket er i hovedsak det å få til en avtale med rettighetshaverene, eller distributørene av materialet i Norge.

Kurs for studenter i bruk av universitetsnettet

Etablere et kurs for studenter om hvordan man skal bruke universitetsnettet. Nye studenter som kommer til NTNU vil ha som krav å gjennomføre kurset, som en del av signereingen av IT-reglementet. Kurset kan avluttes med en test, for å se hvor mye av IT-reglementet studenten har fått med seg. Denne testen kan muligens brukes i forbindelse med initiativ eller straff ettersom hvor godt studenten gjør det. Dette kurset kan bli for omfattende for hele universitetet og kan heller bare bli gitt til Sit leietakere. Dette prosjektet kan bli både tidkrevende og ha en høy kostnad, så vi foreslår for å begrense ressursbruken at dette prosjektet blir en mulig bacheloroppgave.

Sit bytter ISP

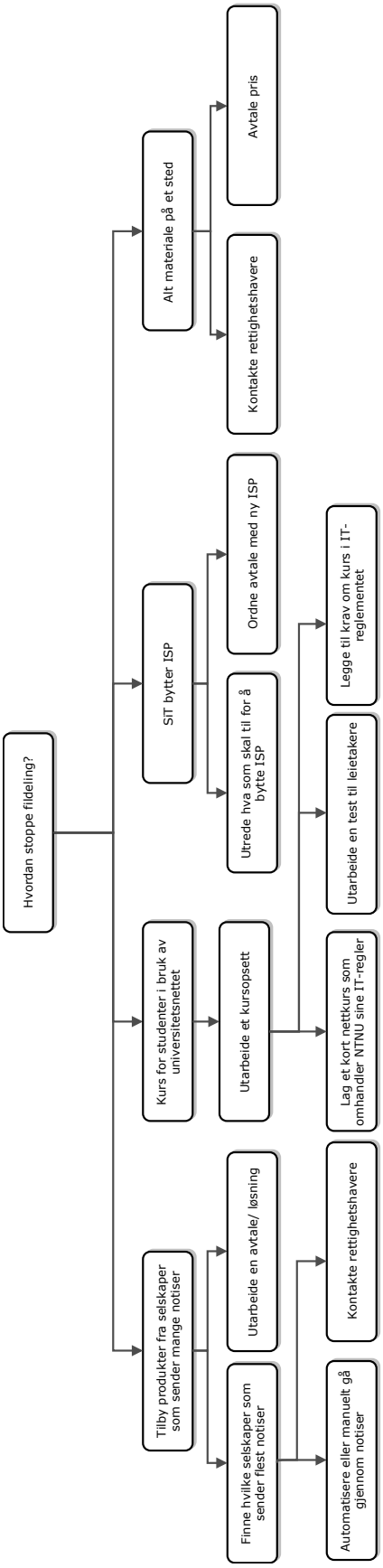
Det å bytte ISP eller splitte studenthjemmene fra universitetnettverket vil være en dyr og tidkrevende prosess, men dette kan være verdt å gjennomføre. Dette vil ikke fjerne rotårsaken til problemet, men vil flytte problemet vekk fra NTNU sitt ansvarsområde.

6.7 Løsningsimplementering

Arbeidet i denne fasen går ut på å utrede en tiltaksplan og lage et forslag til hvordan dette skal implementeres.

6.7.1 Trediagram

For å implementere tiltakene beskrevet over brukes trediagram for å strukturere og dele opp aktivitetene som må gjøres. Dette vil fungere som et enkelt utkast til en prosjektplan.



Figur 23: Trediagram til tiltak mot ulovlig fildeling

6.8 Kostnad-nytte-analyse

Denne seksjonen tar for seg en kostnad-nytte-analyse av nytteverdien til bruk av rotårsaksanalyse for case 1.

6.8.1 Kostnad for gjennomføring

I denne analysen definerer vi kostnad som tid brukt på en iterasjonen av metoden. Vi definerer en skala for kostnad fra 1 til 5 der nivåene tilsvarer følgende tidsbruk:

1. Under 50 timer
2. 50-150 timer
3. 150-250 timer
4. 250-400 timer
5. Over 400 timer

Tabell 3 under viser tidsbruken i enkeltfasene i dette caset. Dette inkluderer tid brukt til å dokumentere alt som har med de enkelte fasene å gjøre. Dette er samlet tidsbruk fra fire personer.

Tabell 3: Tidsbruk i de ulike fasene i case 1

Case 1		
Fase	**Verktøy brukt**	**Timer totalt**
Problemforståelse	Flytdiagram og kritiske hendelser	16-20t
Idémyldring	Idémyldring	16-20t
Datainnsamling	Spørreundersøkelse	80-100t
Datanalyse	Analyseverktøy	100-120t
Rotårsaksidentifisering	Årsak-virkningsdiagram	14-18t
Rotårsakseliminering	6 tenkehatter og SIT	20-24t
Løsningsimplementering	Trediagram	14-20t
Sum		**260-322t**

Dersom kosten på caset går over flere nivåer regner vi med medianen til ytterpunktene for å plassere kostnaden. Basert på kostnadsnivåene vi definerte over, plasseres tidsbruken på case 1 til:

$$\text{Kostnad} = 4$$

6.8.2 Nytte av resultatene

I denne analysen definerer vi nytten som egen oppfatning av hvor gode resultatene fra caset var. Det vurderes ut fra om vi tror det kan finnes andre underliggende årsaker, og hvorvidt vi mener problemet blir løst dersom rotårsakene fjernes, hvis det er gjennomførbart. Nytten defineres på en skala fra 1 til 5.

I dette caset kom vi frem til at tilgjengeligheten på tjenester var i hovedsak rotårsaken til at studenter laster ned. Vi vurderer dette til å være relativt korrekt og at det ikke eksisterer så mange flere rotårsaker enn dette. Vi vurderte også økonomi og lav risiko som mindre rotårsaker. Eneste problemet med dette caset er at det er nærmest umulig for NTNU i seg selv å fjerne den første rotårsaken. Vi definerer derfor nytten til:

$$\text{Nytte} = 4$$

6.8.3 Total nytteverdi

Når vi regner ut kostnad-nytte deler vi kostnaden på nytteverdien.

$$\frac{\mathit{Kostnad}}{\mathit{Nytte}} = \mathit{Totalnytteverdi}$$

I dette caset blir regnestykket slik:

$$\frac{4}{4} = 1$$

Svarene på regnestykket kan bli fra 0,2 til 5. Jo lavere denne nytteverdien er, jo bedre fungerte metoden til caset.

7 Resultater og analyse fra Case 2: Kompromitterte brukerkontoer ved NTNU

I dette kapittelet fremlegger vi våre resultater i alle fasene i case 2.

7.1 Problemforståelse

7.1.1 Kritiske hendelser

Sammen med oppgavebeskrivelsen fikk vi en liste over loggførte sikkerhetshendelser som hadde foregått det siste året hvor kompromitterte kontoer var involvert. Dataene ble sortert i synkende rekkefølge og lagt inn i en tabell for å visualisere frekvensen til de enkelte sikkerhetshendelsene, og dermed fokusområdene til trusselaktørene.

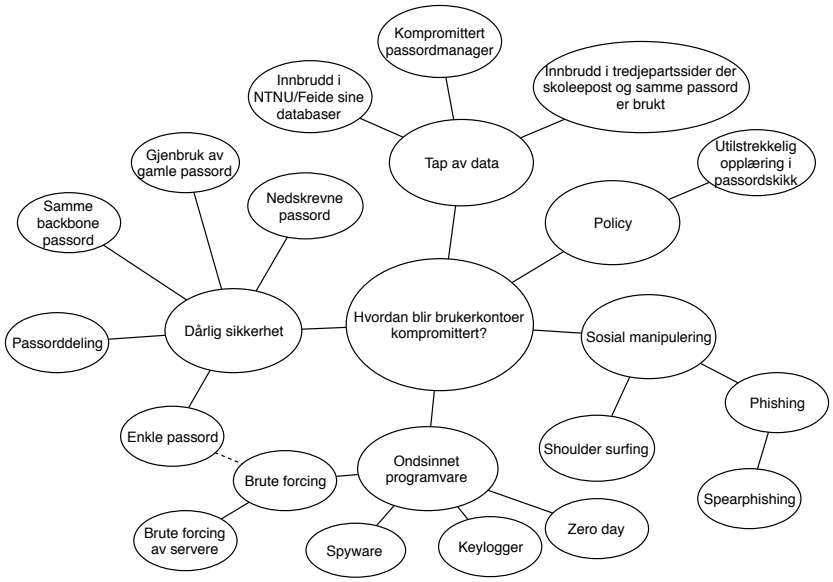
Sikkerhetshendelser	Frekvens
Spam	46
Misuse (uthenting av forskningsartikler)	26
Negligible/Fixed/Failed Attack	8
Phishing	7
Whaling	2
Brute force	2
DDOS out	1
Traded credentials	1
Hackingtools exploits and kits	1
Copyright/Piracy	1

Tabell 4: Oversikt over hva kompromitterte ansattkontoer blir brukt til

Fra tabellen ser vi at spam er den hendelsen med høyest frekvens, men etter diskusjon med oppdragsgiver var ikke dette problemet av størst viktighet. Det er fordi dette er noe som enkelt blir lagt merke til og er trolig ikke hovedgrunnen til at aktørene aktivt går inn for å kompromittere NTNU sine brukerkontoer. Når det kommer til "misuse" i tabellen ovenfor referer det til hendelser der uvedkommende misbruker NTNU sine ressurser, spesielt i form av å stjele forskningsartikler på NTNU sin regning. Dette var en av de største problemene med kompromittering av kontoene, siden det førte til økonomisk tap for NTNU og fare for utestengelse fra artikkeldatabasene.

7.2 Idémyldring

I denne fasen ble det gjort en idémyldring. Problemet som ble fremhevet var hvordan brukerkontoer ble kompromittert. Resultatet fra idémyldringen, gruppert i henhold til likhetstrekk, vises i figur 24 under.



Figur 24: Resultater og gruppering av idémyldringen

Resultatene er gruppert inn i 4 hovedkategorier:

Dårlig sikkerhet er alt fra enkle passord til passordgjenbruk.

Tap av data inkluderer at for eksempel sider som dropbox har en lekkasje av brukerinformasjon.

Sosial manipulering vil si å få tak i informasjon ved å lure noen.

Ondsinnet programvare er programvare brukt som hjelpemiddel for å få tak i brukerinformasjon.

7.3 Datainnsamling

Under idémyldringen ble det avdekket en rekke faktorer som kunne være medvirkende i at ansatte og studenter ved NTNU fikk sin konto på avveie. Vi brukte denne informasjonen aktivt da spørreundersøkelsen ble konstruert. Spørreundersøkelsen slik den fremstår for respondenten finnes i vedlegg B. Når spørsmålene ble laget ble det bestemt hypoteser til spørsmålene. Disse er listet i tabell 5 under.

Tabell 5: Hypoteser til spørsmålene for kompromitterte kontoer

Spørsmål	Hypoteser
Din alder?	Eldre er overrepresentert i statistikken over tapte kontoer
Ditt kjønn?	Flere kvinner enn menn har blitt kompromittert
Hva er din primærrolle ved NTNU?	Det er ansatte som er målgruppen til trusselaktørene
I hvilken by jobber/studerer du primært?	Gjøvik har høyere sikkerhetskompetanse
I hvor mange år har du jobbet/studert ved NTNU eller de tidligere høgskolene?	Folk med lavere ansiennitet kjenner universitetets retningslinjer bedre
Når fant du ut at NTNU kontoen din var blitt kompromittert?	Folk vet ikke at de har blitt kompromittert før de blir kontaktet
Har du noen formening om hvor lang tid kontoen var kompromittert før Seksjon for Digital Sikkerhet kontaktet deg?	Ingen hypotese grunnet vagt spørsmål
Har du noen formening om hvordan kontoen din ble kompromittert?	Ingen hypotese grunnet åpent svar
Bruker du din NTNU e-post til å registrere deg på ulike tjenester på nett i forbindelse med jobben/studiet?	Over halvparten bruker NTNU e-post til tjenester i forbindelse med jobb
Bruker du din NTNU e-post til å registrere deg på tjenester på nett til privat bruk?	Under halvparten bruker NTNU e-post til privat bruk
På en skala fra 1-6, der 1 er lite bevisst og 6 er svært bevisst, hvor bevisst er du på sikkerhet når du... besøker nettsider? lager passord? sjekker e-post?	Folk er generelt sett lite bevisste
Har du i din tid hos NTNU lagt merke til phishing-forsøk mot deg på din NTNU e-post?	Phishing er en svært utbredt angrepsvektor
Har du blitt lurt av phishing på din NTNU e-post?	Av de som har blitt kompromittert har under en tredjedel blitt lurt av phishing
Har du i løpet av din tid ved NTNU eller de andre høgskolene, oppdaget virus eller annen skadevare på maskinen din?	Virus og annen skadevare er utbredt
Bruker du ditt NTNU passord på flere tjenester?	Passordgjenbruk er utbredt
Brukte du regler til å generere ditt NTNU passord?	De fleste bruker ikke passordregler til å generere passord
Er ditt NTNU passord tilfeldig sammensatt av bokstaver, tall og/eller tegn?	De fleste bruker ikke tilfeldig sammensatte passord
Hvor mange tegn består ditt NTNU passord av?	Over halvparten har passord på under 12 tegn
Har du i løpet av din tid ved NTNU delt NTNU passordet ditt med andre?	Passorddeling er ikke særlig utbredt
Omtrent hvor ofte bytter du ditt NTNU passord?	Passord byttes for det meste sjeldnere enn hvert andre år
Bruker du en passordmanager?	De fleste bruker ikke passordmanager, og mange vet ikke engang hva det er
På en skala fra 1 til 6, hvor godt kjent er du med... NTNU sine retningslinjer for behandling av brukernavn, passord og andre autentiseringsdata? IT-reglementet til NTNU? NTNU sine prinsipper for informasjonssikkerhet?	Det er svært lite kjennskap til retningslinjer
Har du fått opplæring i passordsikkerhet fra NTNU?	Under en fjerdedel har fått opplæring i passordskikk fra NTNU

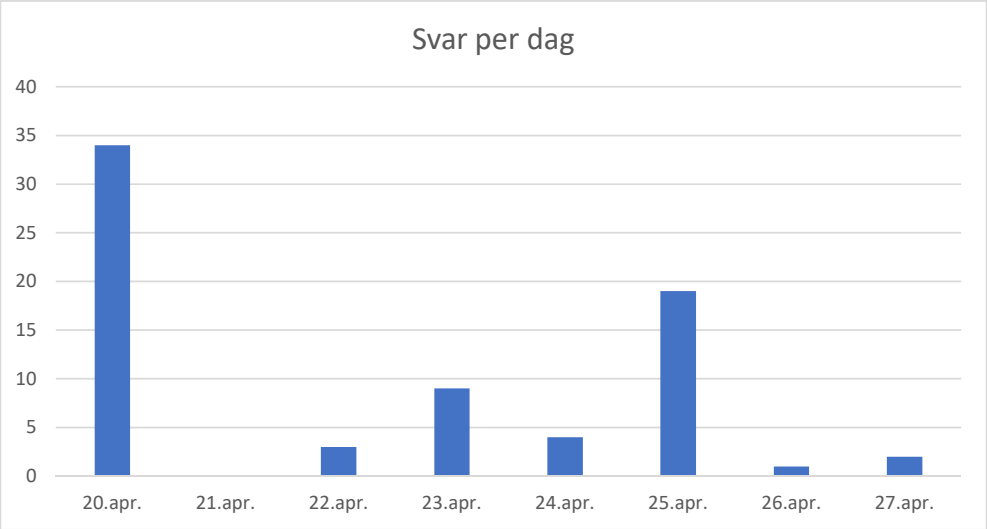
Av de som e-posten ble sendt ut til fikk vi totalt 72 gyldige respondenter, mens 26 stoppet rett etter åpning av undersøkelsen eller underveis. Undersøkelsen var aktiv i perioden fra 20. April til og med 27. April. I løpet av denne tiden ble det sendt ut én purring den 25. April.

7.4 Dataanalyse

I denne fasen analyseres dataene som er samlet inn, og ved hjelp av statistiske verktøy kan vi trekke konklusjoner basert på svarene. Verktøyet vi bruker til å utføre mesteparten av analysene er SPSS.

7.4.1 Svarstatistikk

Spørreundersøkelsen ble mottatt av 157 personer som har fått kontoen kompromittert. Av disse var det 72 som svarte. Det var i tillegg 26 som startet spørreundersøkelsen, men ikke fullførte. Figur 25 under viser statistikk over hvor mange svar som kom inn per dag.



Figur 25: Antall svar vi fikk per dag

Det var tydelig mest svar dagen spørreundersøkelsen ble lansert, og 25. April, hvor vi sendte ut en purre e-post. Det bør nevnes at undersøkelsen ble sendt ut på en fredag, og 21. og 22. April var en lørdag og søndag. Derfor gikk antall svar litt opp igjen på mandag 23. April.

7.4.2 Demografi

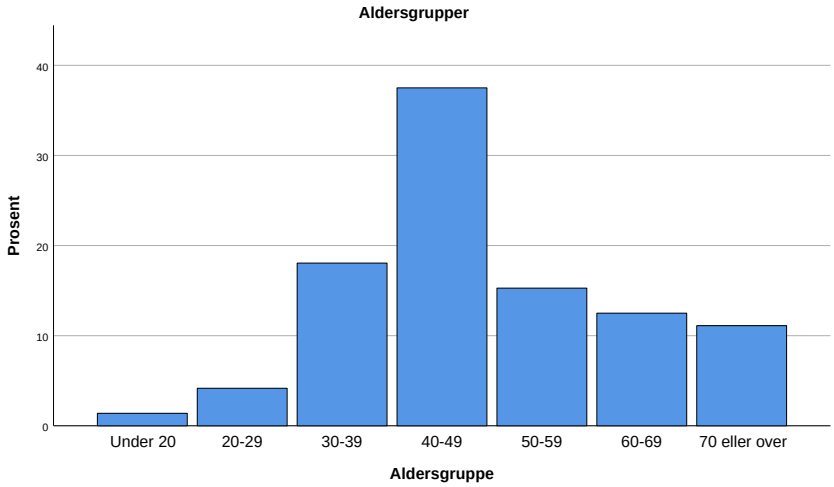
I denne delen fremlegges resultatene fra demografien i spørreundersøkelsen. Disse blir om mulig sammenliknet med generelle tall fra NTNU for å få et innblikk i demografien til de som har blitt kompromittert, kontra NTNU sine ansatte og studenter generelt. Vi fokuserer stort sett på de ansatte siden antall studenter i undersøkelsen var få.

Aldersgruppe

Aldersgruppene ble kategorisert i intervaller på 10 år. Fra de ulike kategoriene fikk vi:

- Under 20: 1 person
- 20-29: 3 personer
- 30-39: 13 personer
- 40-49: 27 personer
- 50-59: 11 personer
- 60-69: 9 personer
- 70 eller over: 8 personer

Under ser vi aldersfordelingen visuelt fremstilt i et histogram.

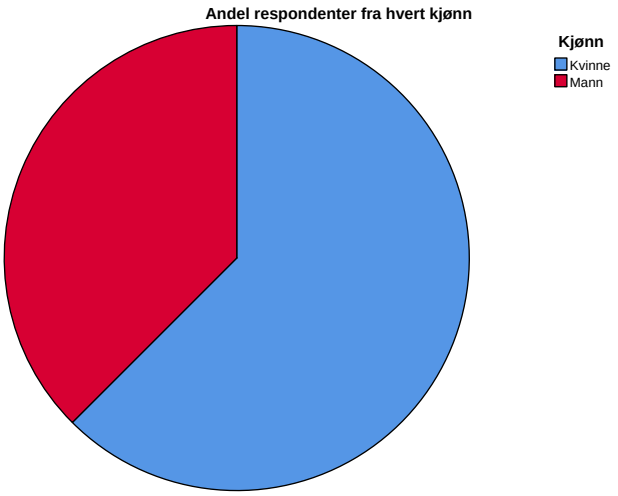


Figur 26: Aldersgrupper av respondentene

Ut fra resultatene kan vi konkludere med at de som har blitt kompromittert er stort sett middelaldrene til eldre personer. Disse personene er også noe eldre enn gjennomsnittsalderen til de som jobber ved NTNU [17].

Kjønn

Av de 72 respondentene var det 45 kvinner og 27 menn. Det er henholdsvis 62,5% og 37,5%. Under er kjønnsfordelingen visualisert i et sektordiagram.

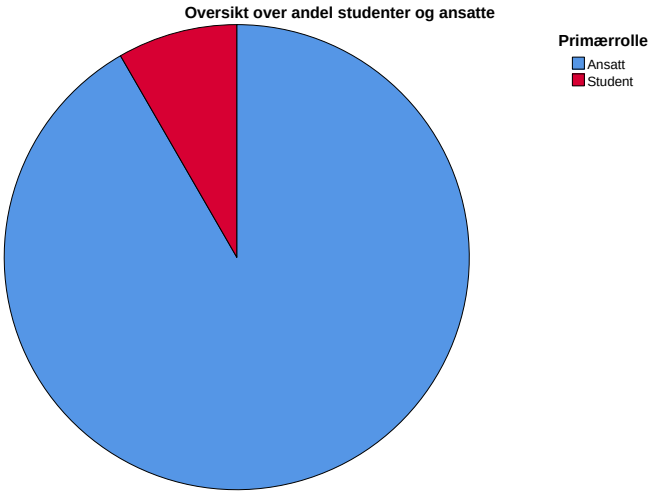


Figur 27: Andel fra hvert kjønn

De fleste av de som har svart er kvinner. Av de ansatte ved NTNU er det 41% kvinner totalt [18]. Totalt sendte vi ut spørreundersøkelsen til 167 e-postadresser, der 157 av de mottok. Vi har tall på at 91 av de 167 vi først sendte ut til var kvinner. Dette er omtrent 55%. For å kunne si noe om antallet kvinner som svarte på spørreundersøkelsen må vi se på om svarene våre er representative for hele samplet. Vi brukte en kalkulator for å regne ut konfidensintervallet for vårt sample [19]. Utregningen kom fram til at vi er 95% sikre på at feilmarginen for dette spørsmålet er $\pm 8,5\%$. I og med at andelen kvinner totalt på NTNU er 41%, kan vi fastslå at kvinner er noe mer utsatt for å få kontoen kompromittert, men denne forskjellen er ikke stor.

Primærrolle

Av de 72 respondentene var det 6 studenter og 66 ansatte. Dette er henholdsvis 8,3% og 91,7%. Sektordiagrammet under viser fordelingen.



Figur 28: Primærrolle ved NTNU

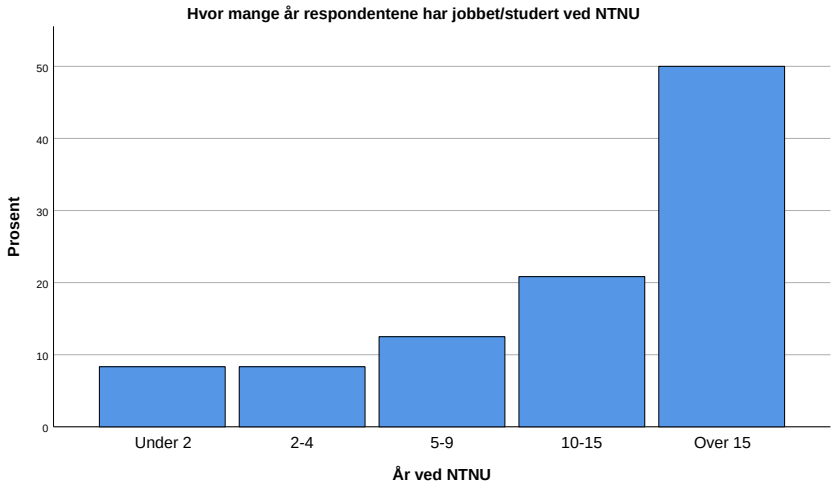
Fra dataene kan vi se at ansatte er overrepresentert i de som blir kompromittert. Vi har data på at det er 18 studenter i vårt sample, altså står studenter for omtrent 10% av de kompromitterte. På samme måte som i forrige seksjon, ble konfidensintervallet regnet ut [19]. Utregningen kom frem til at vi er 95% sikre på at feilmarginen er på $\pm 5,12\%$. Det er desidert flere studenter enn ansatte ved NTNU [18]. Derfor kan vi med høy sikkerhet si at trusselaktørenes målgruppe er de ansatte og ikke studenter.

Primærby

Av de 72 respondentene var det bare en fra Ålesund og resten var fra Trondheim. Det var ingen respondenter fra Gjøvik.

År ved NTNU

Bare 6 personer, eller 8,3% av respondentene hadde jobbet eller studert ved NTNU i under 2 år og i 2 til 4 år. 9 personer, eller 12,5% hadde jobbet eller studert her i 5 til 9 år, og 15 personer, eller 20,8% hadde jobbet eller studert her i 10 til 15 år. Hele 36 personer, eller akkurat halvparten av respondentene har vært hos NTNU i over 15 år. En oversikt over disse tallene finnes i histogrammet under.

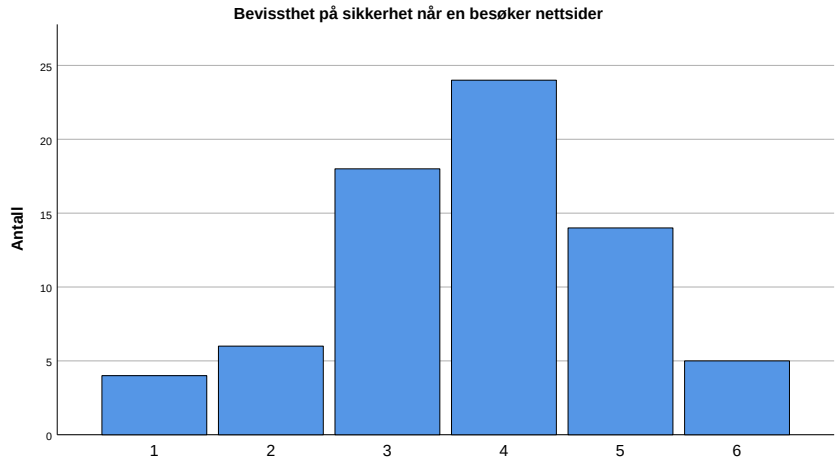


Figur 29: Antall år ved NTNU

7.4.3 Bevissthet på sikkerhet

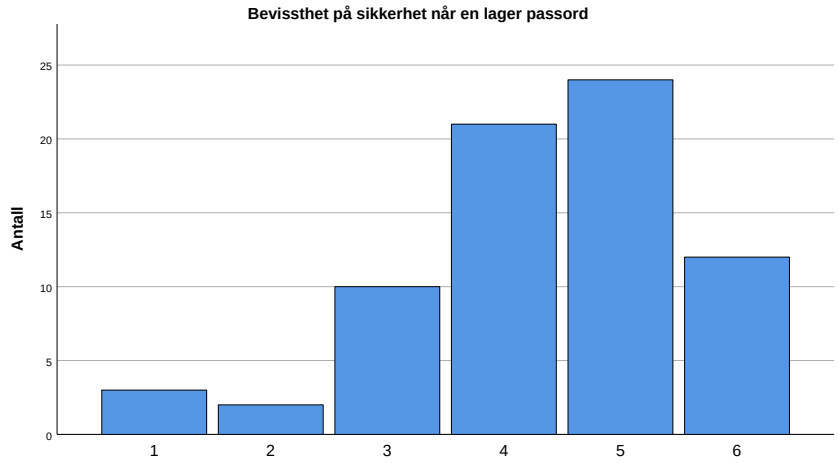
Spørsmålene skulle gi svar på hvor sikkerhetsbevisst en tenker når man besøker nettsider, lager passord og sjekker e-post. Hypotesen som ble fremhevet her var at folk generelt sett er lite bevisste.

Histogrammet i figur 30 viser en tilnærmet normalfordelt situasjon, men med noe fler svar på høyresiden. De fleste er derfor litt mer bevisste på sikkerhet når de besøker nettsider enn de er ubevisste.



Figur 30: Bevissthet på sikkerhet når en besøker nettsider

Når det kommer til sikkerhet når en lager passord svarer respondentene at de generelt sett er bevisste på dette. Figur 31 under viser at fordelingen er konsentrert hovedsaklig på høyresiden.



Figur 31: Bevissthet på sikkerhet når en lager passord

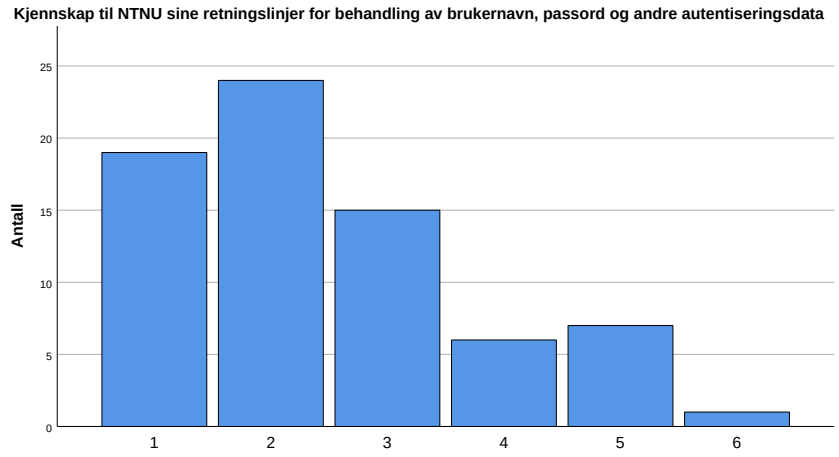
Figur 32 under viser bevissthetsfordelingen når det kommer til sjekking av e-post. Dette var noe vi spesielt ønsket å se på siden en av hovedhypotesene våre til kompromitterte brukerkontoer er phishing. Histogrammet viser at respondentene stort sett er bevisste på sikkerhet når de sjekker e-post.

Figur 32: Bevissthet på sikkerhet når en sjekker e-post

7.4.4 Kjennskap til retningslinjer, reglementer og prinsipper

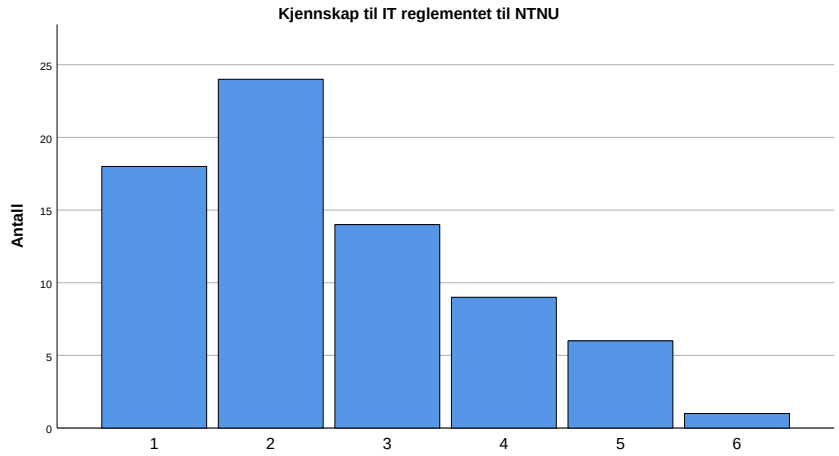
Disse spørsmålene handler om hvor godt kjennskap respondentene har til NTNU sine retningslinjer for behandling av autentiseringsdata, IT-reglementet og prinsipper for informasjonssikkerhet. Hypotesen vi hadde her var at de aller fleste hadde lite kjennskap til disse.

Det viser seg fra figur 33 at respondentene kan lite om NTNU sine retningslinjer for behandling av brukernavn, passord og andre autentiseringsdata.



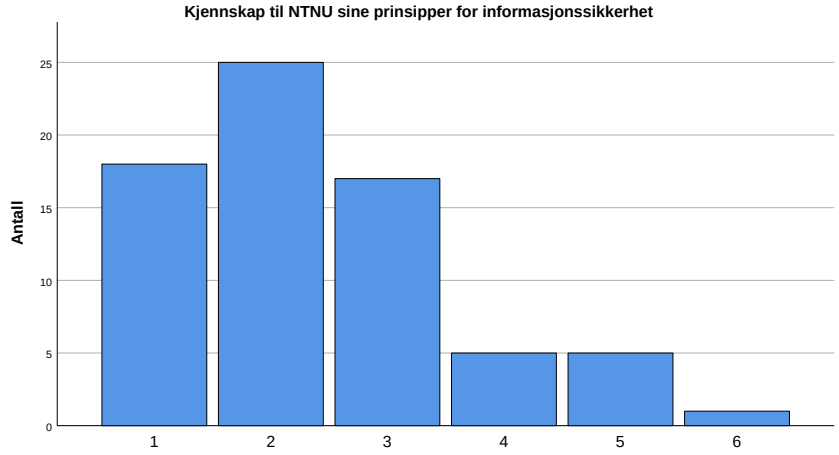
Figur 33: Kjennskap til retningslinjer

Figur 34 viser at respondentene ikke kjenner så godt til IT-reglementet til NTNU. Over 70% svarte 3 eller under på hvor godt de kjente IT-reglementet til NTNU, der 1 var lite kjent og 6 var meget kjent.



Figur 34: Kjennskap til IT-reglement

Under viser figur 35 at folk har dårlig kjennskap til NTNU sine prinsipper for informasjonssikkerhet. Der står det blant annet at brukere er ansvarlige for enhver bruk av innloggingskredentialier og at de holder dette konfidensielt [20].

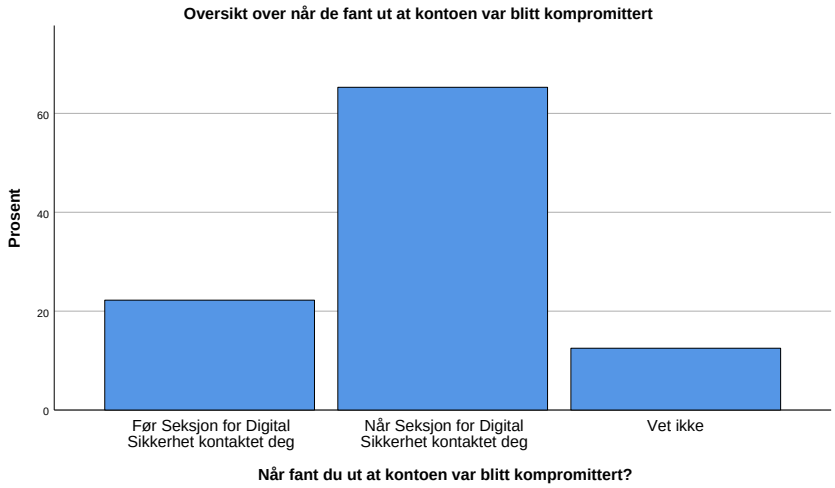


Figur 35: Kjennskap til NTNU sine prinsipper for informasjonssikkerhet

Det viser seg at hypotesen vi hadde stemte. Det er lite kjennskap til styringsdokumentene.

7.4.5 Respondentenes egen oversikt

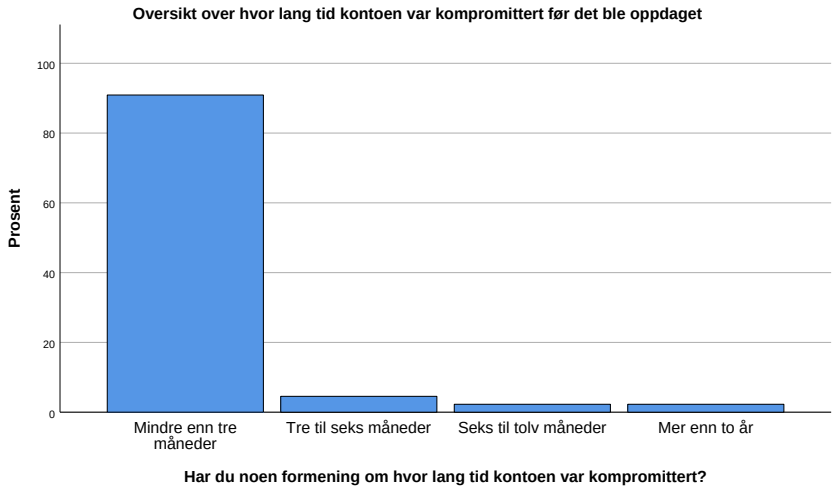
Over 60% av respondentene viste ikke at kontoen var blitt kompromittert før Seksjon for Digital Sikkerhet ringte, og kun 20% svarte at de fant ut av det før og resten svarte at de ikke vet.



Figur 36: Viser når de fant ut at de var blitt kompromittert

Hypotesen vår her var korrekt. De vet ikke at de har blitt kompromittert før de blir kontaktet.

Respondentene svarte at de trodde kontoen var kompromittert mindre enn tre måneder før Seksjon for Digital Sikkerhet kontaktet dem, som vist i figur 37. Denne statistikken kan vi ikke være helt sikre på, fordi halvveis i undersøkelsen fikk vi tilbakemeldiner på at det var flere som ikke ville fullføre spørreundersøkelsen siden dette svaret var obligatorisk og det ikke var noe alternativ for "vet ikke". Vi fjernet da kravet om å svare halvveis ut i undersøkelsen.

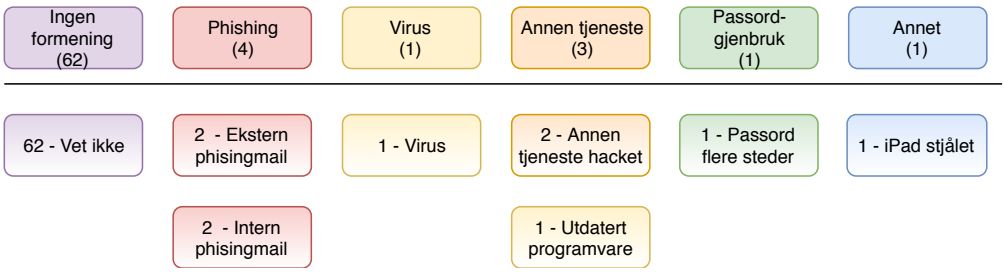


Figur 37: Viser hvor lang tid de tror de var kompromittert

Formening om hvordan det skjedde

Affinitetsdiagramet viser at 62 av respondentene ikke har noen formening om hvordan kontoen ble kompromittert. Det var fire som trodde det skjedde på grunn av phishing og tre som trodde det var på grunn av at en annen tjeneste ble hacket eller utdatert programvare. I tillegg var det bare en som svarte at passordgjenbruk var problemet, og

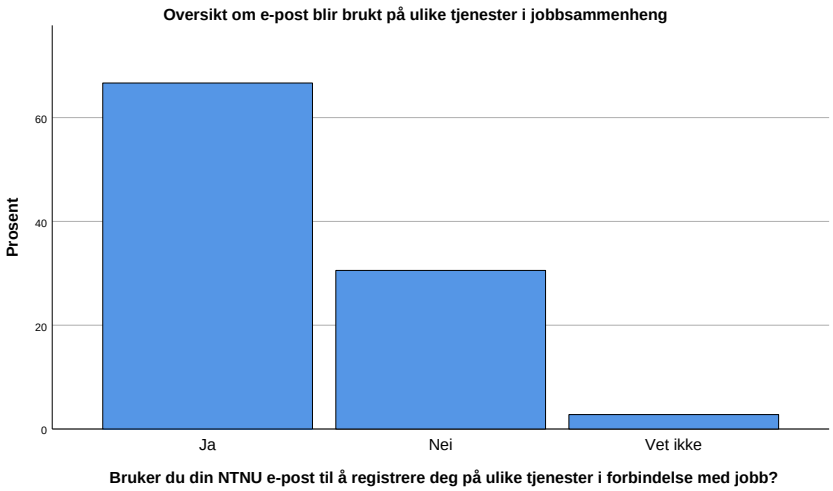
samme antall svarte at det var virus.



Figur 38: Affinitetsdiagram av respondentenes formening over hvordan kontoen ble kompromittert

7.4.6 Bruker- og passordvaner

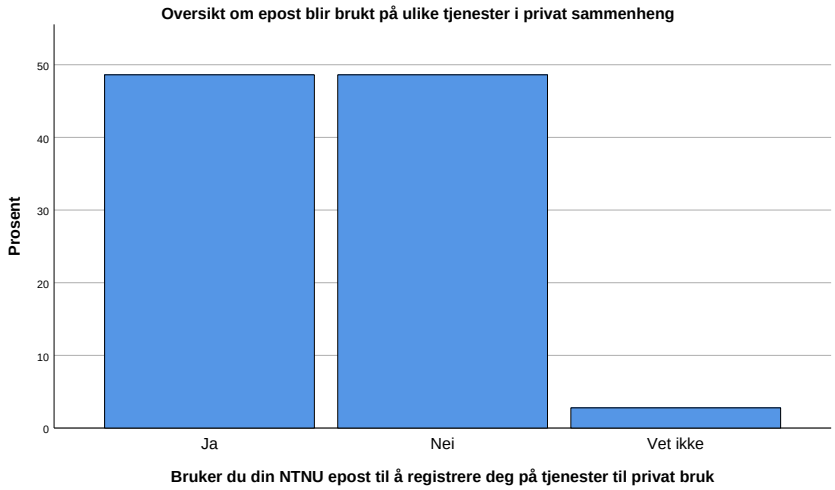
Som vi kan se i figur 39 under, bruker over 60% av respondentene NTNU e-posten til å registrere seg på tjenester i forbindelse med jobb.



Figur 39: Viser hvor mange som bruker NTNU e-post til andre jobbrelaterte tjenester

Hypotesen vår var korrekt, over halvparten bruker NTNU e-posten i forbindelse med jobb.

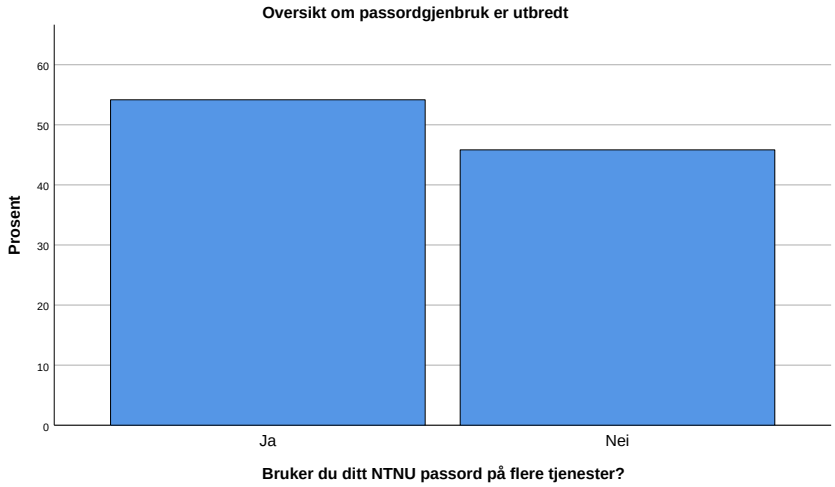
48,6% av respondentene bruker NTNU e-posten sin til private tjenester. Den samme andelen gjør ikke det og de restende (2,8%) har svart at de ikke vet. Dette blir vist i figur 40.



Figur 40: Viser hvor mange som bruker NTNU e-post til private tjenester

Hypotesen vår var korrekt, litt under halvparten bruker NTNU e-posten til privat bruk. Selv om det er under halvparten som bruker NTNU e-posten til privat bruk, så er dette noe som burde unngås.

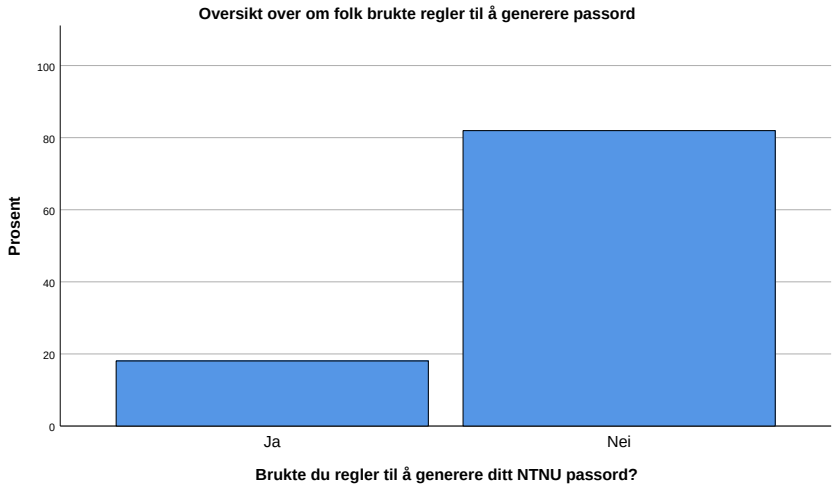
Over 50% av respondentene bruker NTNU passordet på flere tjenester som vist i figuren under.



Figur 41: Oversikt over gjenbruk av NTNU passord

Hypotesen vår her var korrekt, over halvparten bruker samme NTNU passord på flere tjenester. Dette var også en av hovedhypotesene til caset.

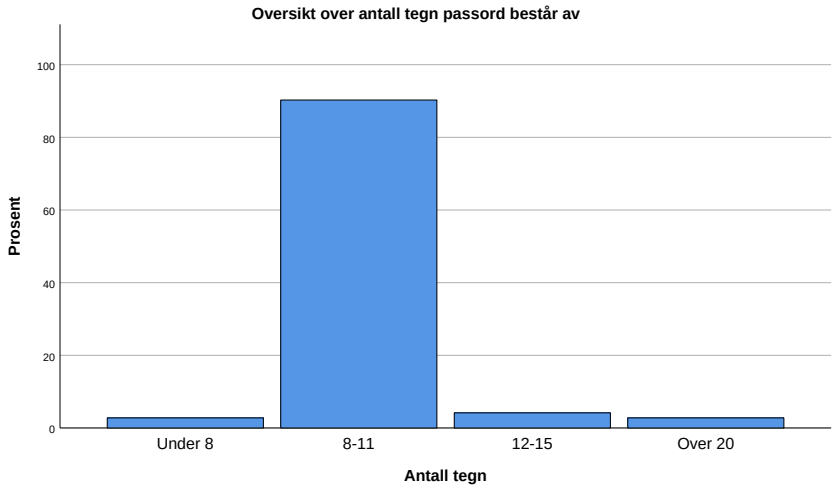
Over 80% av respondentene svarte at de ikke brukte regler til å generere passord. Det er mulig for feiltolkning av spørsmålet, i og med at regler kan bety to forskjellige ting. Det kan bety regle, i form av “Lisa-gikk-til-NTNU” for NTNU-passord, eller så kan man tolke det som en regel.



Figur 42: Viser hvor mange som bruker passordregler

Vi kan derfor ikke si noe med sikkerhet om hypotesen vår ble bekreftet eller avkreftet.

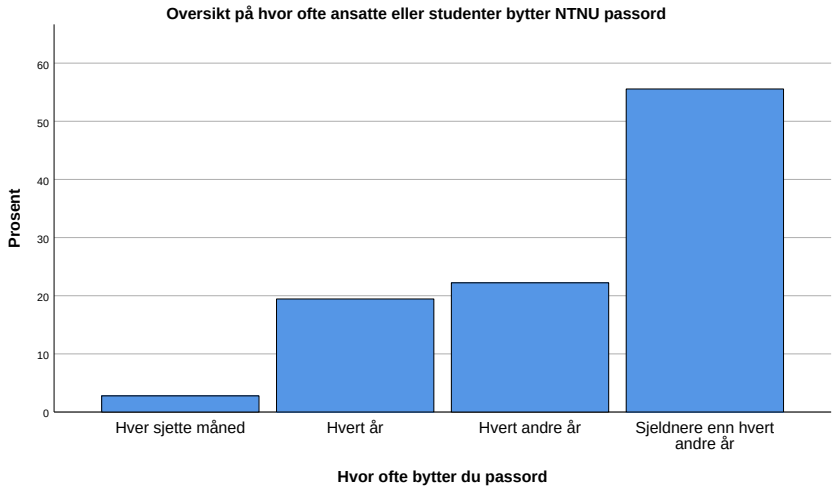
Over 80% av respondentene har passord som er mellom 8-11 tegn. Resterende fordelte seg likt utover de andre valgene.



Figur 43: Antall tegn på passord

Hypotesen vår var korrekt, de fleste bruker passord som er under 12 tegn. Det er mulig vi burde ha splittet opp intervallene ytterligere jo mindre antall tegn det var snakk om.

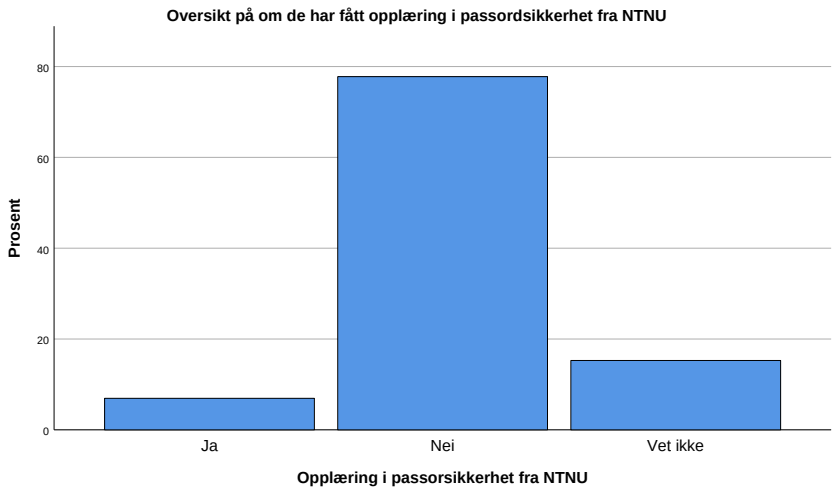
Figur 44 viser statistikken over hvor ofte respondentene bytter passord. Over 50% sier at de bytter passord sjeldnere enn hvert andre år, over 20% sier at de bytter hvert andre år, rett under 20% sier at de bytter hvert år og resten sier at de bytter hver sjette måned.



Figur 44: Viser hvor ofte de bytter passord

Hypotesen var korrekt, flertallet av respondentene bytter passord sjeldnere enn hvert andre år. I henhold til en innsida-side som beskriver hvordan en skal håndtere slike data så skal passord byttes hver sjette måned og tvungen passordbytte hvert år. Dette viser at respondentene ikke kjent med disse retningslinjene.

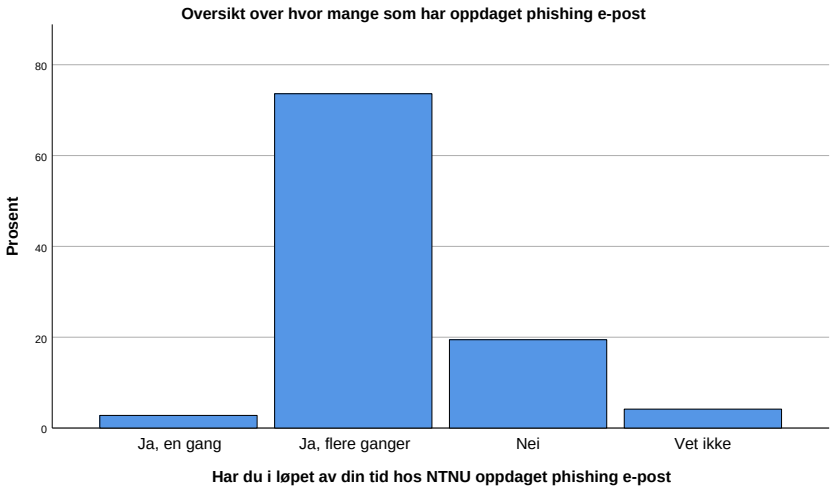
I figur 45 ser vi antallet som sier at de har fått opplæring i passordsikkerhet fra NTNU. Ut fra tabellen ser vi at under 80% av respondentene sier at de ikke har fått opplæring i passordsikkerhet. 15% sier at de ikke vet om de har fått opplæring og resten sier at de har fått det.



Figur 45: Viser hvor mange som har fått opplæring i passordsikkerhet

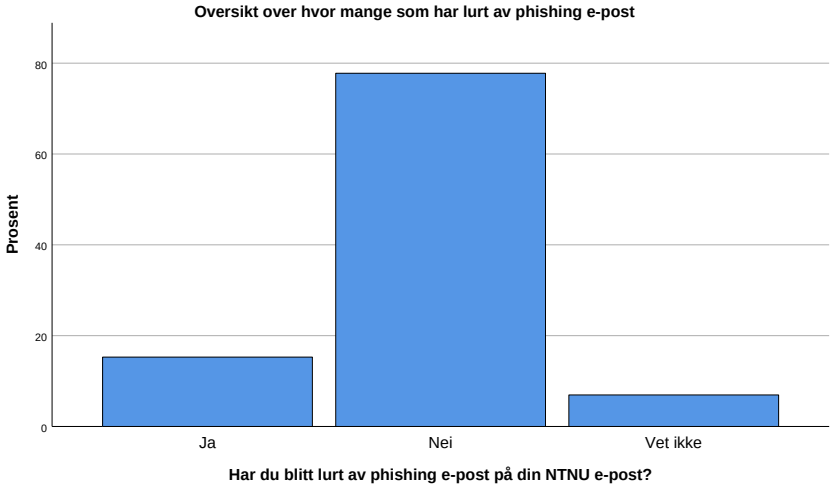
7.4.7 Phishing

Over 70% av respondentene sa at de har oppdaget phishing e-post en eller flere ganger på sin NTNU e-post, og rett under 20% som ikke har oppdaget phishing e-post. Resten av respondentene svarte at de ikke vet. Dette vises i figur 46 under.



Figur 46: Viser hvor mange som har oppdaget phishing e-post

Over 70% av respondentene sier at de ikke har blitt lurt av phishing e-post, og under 20% sier at de har blitt lurt. Som vist i tabellen under.



Figur 47: Viser hvor mange som sier de har blitt lurt av phishing

7.4.8 Statistisk analyse

I denne delen bruker vi statistiske analyseverktøy for å finne relasjoner. De mindre relevante analysene er plassert i vedlegg H. Som en generell regel for utføring av analysen har vi valgt et signifikansnivå på:

$$\alpha \leq 0,05$$

ANOVA på alder mot bevissthet og kjennskap

Denne testen sjekker om det er signifikans mellom alder på respondenten, og hvor bevisste de er på sikkerhet og hvor godt de kjenner til de ulike retningslinjene og reglementene. Alle spørsmålene er besvart på en skala fra 1 til 6, der 1 er lite bevisst eller kjent, og 6 er svært bevisst eller kjent. I tabellen under beskrives svarene til datasettet som er analysert.

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean Lower Bound	95% Confidence Interval for Mean Upper Bound	Minimum	Maximum
Bevisst på sikkerhet når nettsider besøkes	Under 20	1	5.00	.	.	.	.	5	5
	20-29	3	5.00	.000	.000	5.00	5.00	5	5
	30-39	13	3.92	1.038	.288	3.30	4.55	2	5
	40-49	27	3.44	1.281	.247	2.94	3.95	1	6
	50-59	11	4.27	1.272	.384	3.42	5.13	3	6
	60-59	9	4.00	1.000	.333	3.23	4.77	3	6
	Over 70	7	2.71	1.113	.421	1.69	3.74	1	4
	Total	71	3.75	1.239	.147	3.45	4.04	1	6
Bevisst på sikkerhet når passord lages	Under 20	1	6.00	.	.	.	.	6	6
	20-29	3	5.33	1.155	.667	2.46	8.20	4	6
	30-39	13	3.85	1.144	.317	3.16	4.54	2	5
	40-49	27	4.11	1.188	.229	3.64	4.58	1	6
	50-59	11	4.82	1.168	.352	4.03	5.60	3	6
	60-59	9	4.56	.882	.294	3.88	5.23	3	6
	Over 70	8	4.50	1.690	.598	3.09	5.91	1	6
	Total	72	4.35	1.235	.146	4.06	4.64	1	6
Bevisst på sikkerhet når e-post sjekkes	Under 20	1	6.00	.	.	.	.	6	6
	20-29	3	5.33	.577	.333	3.90	6.77	5	6
	30-39	13	3.77	1.363	.378	2.95	4.59	2	6
	40-49	27	4.30	1.463	.282	3.72	4.87	1	6
	50-59	11	4.45	1.572	.474	3.40	5.51	1	6
	60-59	8	4.13	1.126	.398	3.18	5.07	2	5
	Over 70	7	3.86	2.116	.800	1.90	5.81	1	6
	Total	70	4.23	1.476	.176	3.88	4.58	1	6
Kjennskap til retningslinjer for behandling av autentiseringsdata	Under 20	1	5.00	.	.	.	.	5	5
	20-29	3	2.00	1.000	.577	-.48	4.48	1	3
	30-39	13	2.23	1.013	.281	1.62	2.84	1	5
	40-49	27	2.37	1.182	.227	1.90	2.84	1	5
	50-59	11	2.00	1.183	.357	1.21	2.79	1	5
	60-59	9	3.22	1.394	.465	2.15	4.29	1	6
	Over 70	8	2.75	1.909	.675	1.15	4.35	1	5
	Total	72	2.46	1.310	.154	2.15	2.77	1	6
Kjennskap til NTNU sitt IT reglement	Under 20	1	5.00	.	.	.	.	5	5
	20-29	3	2.33	1.155	.667	-.54	5.20	1	3

Figur 48: Descriptive av alder mot bevissthet på sikkerhet og kjennskap til retningslinjer, del 1

	30-39	13	2.46	1.127	.312	1.78	3.14	1	5
	40-49	27	2.19	1.075	.207	1.76	2.61	1	5
	50-59	11	2.45	1.440	.434	1.49	3.42	1	5
	60-59	9	3.67	1.118	.373	2.81	4.53	2	6
	Over 70	8	2.13	1.642	.581	.75	3.50	1	5
	Total	72	2.50	1.300	.153	2.19	2.81	1	6
Kjennskap til NTNU sine prinsipper for informasjonssikkerhet	Under 20	1	5.00	.	.	.	.	5	5
	20-29	3	1.67	.577	.333	.23	3.10	1	2
	30-39	13	2.31	1.032	.286	1.68	2.93	1	5
	40-49	26	2.31	1.050	.206	1.88	2.73	1	5
	50-59	11	2.45	1.440	.434	1.49	3.42	1	5
	60-59	9	3.00	1.414	.471	1.91	4.09	1	6
	Over 70	8	2.00	1.414	.500	.82	3.18	1	4
	Total	71	2.39	1.224	.145	2.10	2.68	1	6

Figur 49: Descriptive av alder mot bevissthet på sikkerhet og kjennskap til retningslinjer, del 2

Fra dataene over kan vi se at generelt sett går bevisstheten på sikkerhet og kjennskapen til retningslinjene ned etterhvert som respondentene blir eldre. Dette gjelder spesielt for bevissthet på sikkerhet når nettsider besøkes og kjennskap til IT-reglementet.

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Bevisst på sikkerhet når nettsider besøkes	Between Groups	20.236	6	3.373	2.475	.032
	Within Groups	87.200	64	1.363		
	Total	107.437	70			
Bevisst på sikkerhet når passord lages	Between Groups	13.435	6	2.239	1.534	.181
	Within Groups	94.884	65	1.460		
	Total	108.319	71			
Bevisst på sikkerhet når e-post sjekkes	Between Groups	11.279	6	1.880	.852	.535
	Within Groups	139.063	63	2.207		
	Total	150.343	69			
Kjennskap til retningslinjer for behandling av autentiseringsdata	Between Groups	16.215	6	2.703	1.663	.144
	Within Groups	105.660	65	1.626		
	Total	121.875	71			
Kjennskap til NTNU sitt IT reglement	Between Groups	22.426	6	3.738	2.490	.031
	Within Groups	97.574	65	1.501		
	Total	120.000	71			
Kjennskap til NTNU sine prinsipper for informasjonssikkerhet	Between Groups	13.256	6	2.209	1.542	.179
	Within Groups	91.702	64	1.433		
	Total	104.958	70			

Figur 50: ANOVA av alder mot bevissthet på sikkerhet og kjennskap til dokumenter

I tabellen over ser vi at når det kommer til alder basert på bevissthet på sikkerhet når nettsider besøkes er dette signifikant siden $\alpha = 0,032$. Dette betyr at vi kan konkludere med at jo eldre folk blir, jo mindre bevisste er de på sikkerhet når de besøker nettsider. Dette gjelder også for kjennskap til NTNU sitt IT-reglement, der signifikansen er på $\alpha = 0,031$.

En post-hoc test kunne ikke kjøres her fordi en av kategoriene bare hadde ett svar.

ANOVA på år ved NTNU mot passord-, e-post- og andre brukervaner

Denne testen sjekker om det er signifikans mellom antall år respondenten har vært hos NTNU, og om de bruker NTNU e-posten sin på andre tjenester, om de har blitt lurt av phishing og om de benytter sitt NTNU passord på flere tjenester. I tabellen under beskrives svarene til datasettet vi skal analysere.

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
Bruker NTNU e-post til jobbrelaterte tjenester	Under 2	6	1.50	.548	.224	.93	2.07	1	2
	2-4	6	1.67	.516	.211	1.12	2.21	1	2
	5-9	9	1.33	.500	.167	.95	1.72	1	2
	10-15	14	1.14	.363	.097	.93	1.35	1	2
	Over 15	35	1.29	.458	.077	1.13	1.44	1	2
	Total	70	1.31	.468	.056	1.20	1.43	1	2
Bruker NTNU e-post til private tjenester	Under 2	5	2.00	.000	.000	2.00	2.00	2	2
	2-4	6	1.83	.408	.167	1.40	2.26	1	2
	5-9	9	1.56	.527	.176	1.15	1.96	1	2
	10-15	15	1.67	.488	.126	1.40	1.94	1	2
	Over 15	35	1.29	.458	.077	1.13	1.44	1	2
	Total	70	1.50	.504	.060	1.38	1.62	1	2
Har blitt lurt av phishing før	Under 2	6	1.67	.516	.211	1.12	2.21	1	2
	2-4	5	1.80	.447	.200	1.24	2.36	1	2
	5-9	8	1.88	.354	.125	1.58	2.17	1	2
	10-15	14	1.79	.426	.114	1.54	2.03	1	2
	Over 15	34	1.88	.327	.056	1.77	2.00	1	2
	Total	67	1.84	.373	.046	1.74	1.93	1	2
Bruker NTNU passord på flere tjenester	Under 2	6	1.83	.408	.167	1.40	2.26	1	2
	2-4	6	1.33	.516	.211	.79	1.88	1	2
	5-9	9	1.33	.500	.167	.95	1.72	1	2
	10-15	15	1.53	.516	.133	1.25	1.82	1	2
	Over 15	36	1.42	.500	.083	1.25	1.59	1	2
	Total	72	1.46	.502	.059	1.34	1.58	1	2

Figur 51: Descriptive av år ved NTNU mot passord-, e-post- og andre brukervaner

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Bruker NTNU e-post til jobbrelaterte tjenester	Between Groups	1.395	4	.349	1.656	.171
	Within Groups	13.690	65	.211		
	Total	15.086	69			
Bruker NTNU e-post til private tjenester	Between Groups	3.968	4	.992	4.765	.002
	Within Groups	13.532	65	.208		
	Total	17.500	69			
Har blitt lurt av phishing før	Between Groups	.299	4	.075	.521	.720
	Within Groups	8.895	62	.143		
	Total	9.194	66			
Bruker NTNU passord på flere tjenester	Between Groups	1.225	4	.306	1.232	.306
	Within Groups	16.650	67	.249		
	Total	17.875	71			

Figur 52: ANOVA av år ved NTNU mot passord-, e-post- og andre brukervaner

Siden det er signifikans på de som bruker NTNU e-post til private tjenester ($\alpha \leq 0,05$), ble en post-hoc test kjørt for å se om det var noen ytterligere signifikans mellom gruppene. Grunnet plassbesparelse er bare de variablene som inkluderte signifikans tatt med i rapporten.

Multiple Comparisons

LSD

Dependent Variable	(I) ÅrBinær	(J) ÅrBinær	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Bruker NTNU e-post til jobbrelaterte tjenester	Under 2	2-4	-.167	.265	.532	-.70	.36
		5-9	.167	.242	.493	-.32	.65
		10-15	.357	.224	.116	-.09	.80
		Over 15	.214	.203	.295	-.19	.62
	2-4	Under 2	.167	.265	.532	-.36	.70
		5-9	.333	.242	.173	-.15	.82
		10-15	.524*	.224	.022	.08	.97
		Over 15	.381	.203	.065	-.02	.79
	5-9	Under 2	-.167	.242	.493	-.65	.32
		2-4	-.333	.242	.173	-.82	.15
		10-15	.190	.196	.335	-.20	.58
		Over 15	.048	.172	.782	-.29	.39
	10-15	Under 2	-.357	.224	.116	-.80	.09
		2-4	-.524*	.224	.022	-.97	-.08
		5-9	-.190	.196	.335	-.58	.20
		Over 15	-.143	.145	.329	-.43	.15
	Over 15	Under 2	-.214	.203	.295	-.62	.19
		2-4	-.381	.203	.065	-.79	.02
		5-9	-.048	.172	.782	-.39	.29
		10-15	.143	.145	.329	-.15	.43

Figur 53: Post-hoc av år ved NTNU mot passord-, e-post- og andre brukervaner, del 1

Bruker NTNU e-post til private tjenester	Under 2	2-4	.167	.276	.548	-.39	.72
		5-9	.444	.254	.085	-.06	.95
		10-15	.333	.236	.162	-.14	.80
		Over 15	.714*	.218	.002	.28	1.15
	2-4	Under 2	-.167	.276	.548	-.72	.39
		5-9	.278	.240	.252	-.20	.76
		10-15	.167	.220	.452	-.27	.61
		Over 15	.548*	.202	.008	.14	.95
	5-9	Under 2	-.444	.254	.085	-.95	.06
		2-4	-.278	.240	.252	-.76	.20
		10-15	-.111	.192	.566	-.50	.27
		Over 15	.270	.171	.118	-.07	.61
	10-15	Under 2	-.333	.236	.162	-.80	.14
		2-4	-.167	.220	.452	-.61	.27
		5-9	.111	.192	.566	-.27	.50
		Over 15	.381*	.141	.009	.10	.66
	Over 15	Under 2	-.714*	.218	.002	-1.15	-.28
		2-4	-.548*	.202	.008	-.95	-.14
		5-9	-.270	.171	.118	-.61	.07
		10-15	-.381*	.141	.009	-.66	-.10

*. The mean difference is significant at the 0.05 level.

Figur 54: Post-hoc av år ved NTNU mot passord-, e-post- og andre brukervaner, del 2

I post-hoc testen i figur 53 og 54 ser vi at når det kommer til jobbrelaterte tjenester er forskjellen signifikant mellom de som har vært ved NTNU i 2-4 år og 10-15 år. Når det kommer til private tjenester er forskjellen signifikant mellom under 2 år og over 15, 2-4 år og over 15, og mellom 10-15 år og over 15. Vi ser at det er en relasjon mellom hvor mange år ved NTNU de og om de bruker NTNU e-post på andre tjenester. Jo lenger de er der, jo mer sannsynlig er det at de bruker e-posten på flere tjenester.

ANOVA på alder mot passord-, e-post- og andre brukervaner

Siden det ble funnet signifikans på antall år ved NTNU og bruk av NTNU e-post på private tjenester, kunne det være sannsynlig at dette også korrelerte med alder. Det er logisk å

tro at jo lenger tid en har tilbringet ved NTNU, jo eldre er personen. Derfor ble det kjørt en korrelasjonstest på alder og antall år ved NTNU for å teste dette. I tabellen under kan vi se at det er en sterk positiv korrelasjon ($\alpha \leq 0,01$) mellom alder og tid ved NTNU.

Correlations

		Alder	År ved NTNU
Alder	Pearson Correlation	1	,621**
	Sig. (2-tailed)		,000
	N	72	72
År ved NTNU	Pearson Correlation	,621**	1
	Sig. (2-tailed)	,000	
	N	72	72

**. Correlation is significant at the 0.01 level (2-tailed).

Figur 55: Korrelasjon mellom alder og antall år ved NTNU

Basert på resultatene er det grunnlag for å tro at siden jo eldre respondenten som har fått sin konto kompromittert er, jo mer sannsynlig er det at personen har benyttet e-posten på private tjenester, basert på resultatene i figur 52 i forrige seksjon.

7.4.9 Independent sample t-test på de som har delt passord mot hvor ofte de bytter passord

Selv om det bare er åtte personer som har sagt at de har delt sitt NTNU passord er dette åtte personer for mye. I IT-reglementet står det at dersom du har mistanke om at noen kan passordet, skal du bytte det med en gang [7]. Derfor var det relevant å se hvor ofte de som har delt passordet sitt bytter passord. Variabelen "ByttePassordBinær" går fra 1-4 der 1 er bytte av passord hver sjette måned og 4 er hvert andre år.

Group Statistics

	DeltPassordBinær	N	Mean	Std. Deviation	Std. Error Mean
ByttePassordBinær	Ja	8	4,00	,000	,000
	Nei	64	3,22	,899	,112

Figur 56: Group statistics av de som har delt passord mot hvor ofte de bytter

Statistikken i figur 56 over viser at alle de som har delt passordet sitt, bytter passord sjeldnere enn hvert andre år. Dette er bekymringsfullt i og med at passordene er kjent av andre over lengre tid. I figur 57 sjekker vi om disse tallene er signifikante.

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
BytteP assordBinær	Equal variances assumed	25,585	,000	2,442	70	,017	,781	,320	,143	1,419
	Equal variances not assumed			6,951	63,000	,000	,781	,112	,557	1,006

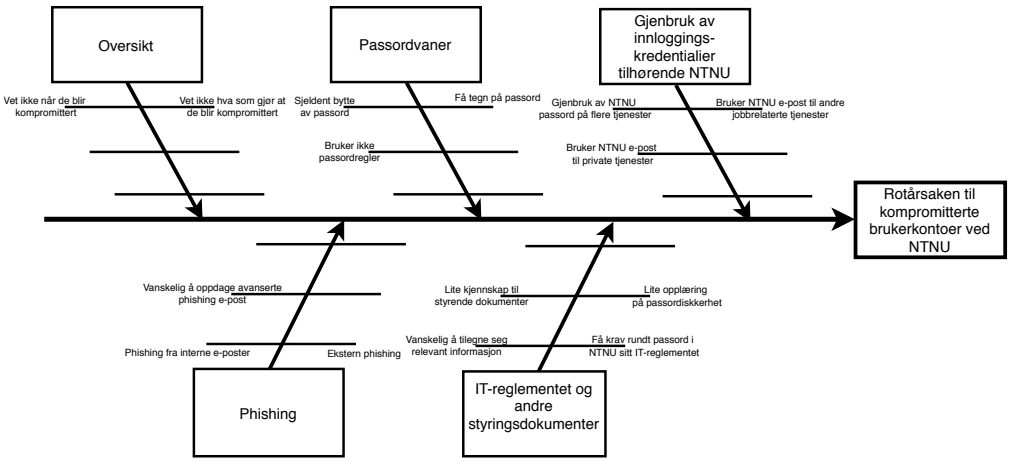
Figur 57: Independent t-test av de som har delt passord mot hvor ofte de bytter

Vi kan se at $\alpha = 0,017$, som betyr at resultatet er statistisk signifikant.

7.5 Rotårsaksidentifisering

7.5.1 Årsak-virkningsdiagram

Innledningsvis ble problemet beskrevet som rotårsaken til kompromitterte kontoer ved NTNU. Hovedkategoriene som ble undersøkt for å finne svar på dette var gjenbruk av innloggingskredentialier tilhørende NTNU, IT-reglementet og andre styringsdokumenter, passordvaner, phishing og oversikt over situasjonen. Både hovedkategoriene og årsakene under disse er i hovedsak basert på dataanalysen, mens noe er basert på kreativ idémyldring.



Figur 58: Fiskebeindiagram over hovedkategorier og årsaker til kompromitterte kontoer

Vi har kommet frem til at rotårsaken til kompromitterte kontoer er sammensatt av flere faktorer. Et passord på mellom åtte til elleve tegn i seg selv er ikke nok for at kontoen skal bli kompromittert, men sammen med at de bytter sjeldnere enn hvert andre år gjør at dette blir et problem. I tillegg til dette bruker flertallet NTNU e-posten til andre tjenester, enten til jobbrelatert eller til privat bruk. De bruker også samme NTNU passord på flere tjenester. Dette er noe en burde unngå til enhver tid, og er noe av det vi anser å være blant det mest kritiske.

Respondentene hadde også liten kjennskap til IT-reglementet og andre styringsdokumenter. De svarte også at de har fått lite opplæring på passordsikkerhet. Vi har lest gjennom IT-reglementet og andre styringsdokumenter, og har kommet frem til at IT-reglementet har for få krav til passord. Det var vanskelig å tilegne seg all informasjon på de forskjellige styringsdokumentene da IT-reglementet ikke henviste til noen av retningslinjene. I retningslinjer for behandling av brukernavn, passord og andre autentiserings-

data [21] står det at passordet skal byttes hver 12 måned. Denne retningslinjen er ikke nevnt i IT-reglementet at du skal gjøre deg bekjent med.

Sammenlagt så viste det oss at respondentene hadde dårlige passordvaner, gjenbruk av innloggingskredentialier tilhørende NTNU og lite kunnskap til IT-reglementet og andre styrende dokumenter. Phishing er også en relevant årsak til kompromitterte kontoer. Phishing e-poster har blitt såpass sofistikerte at det er vanskelig å skille mellom falske og legimite e-poster. [22]. Rotårsakene er derfor som følger:

- Mistet kontodetaljer av phishing
- E-post og passordgjenbruk på andre tjenester
- Liten kjennskap til IT-reglement og andre styrende dokumenter
- Dårlige passordvaner

7.5.2 5 Whys

Det ble fremhevet fem årsaker som skulle analyseres. Fire av disse kom fra fiskebeindiagrammet over, og en fra idémyldring. Tabellene under viser resultatene fra gjennomføringen.

Årsak:	Mistet kontodetaljer av phishing
Why?	Fordi e-posten kom fra en intern e-postadresse
Why?	Fordi kontoen var blitt kompomittert
Why?	Fordi kontodetaljene ble phishet fra en ekstern e-postadresse
Why?	Fordi brukeren var ikke oppmerksom på at det var en phishing e-post
Why?	Fordi brukeren hadde ikke fått tilstrekkelig opplæring i deteksjon av phishing e-post

Tabell 6: 5 Whys på mistet kontodetaljer av phishing

Å miste kontodetaljer av en phishing e-post kan skje fra enten interne eller eksterne e-postadresser. I 5 Whys over kom vi frem til at dette skjer fordi en ikke er oppmerksom på tvilsomme e-poster. Årsaken til det kan være fordi brukerne ikke har fått tilstrekkelig opplæring i deteksjon av phishing e-post.

Årsak:	E-post og passordgjenbruk på andre tjenester
Why?	Fordi det er vanskelig å huske mange unike brukerdetaljer
Why?	Fordi det ikke brukes passordmanager
Why?	Fordi de ikke vet hva det er
Why?	Fordi det ikke gis informasjon om det i retningslinjene
Why?	-

Tabell 7: 5 Whys på e-post og passordgjenbruk på andre tjenester

Årsaken til at mange velger å benytte samme kredentialer flere steder er som regel at de synes det er vanskelig å huske mange brukerdetaljer, og motsatt, enkelt å huske få. Noe som kan gjøre dette lettere er å bruke en passordmanager, men dette informeres det ikke om i styringsdokumentene eller andre steder.

Årsak:	Liten kjennskap til IT-reglement og andre styrende dokumenter
Why?	Fordi det er vanskelig å tilegne seg informasjon
Why?	Fordi informasjonen er spredt på mange sider og dokumenter
Why?	Fordi det ikke er et overordnet ISMS
Why?	-
Why?	-

Tabell 8: 5 Whys på liten kjennskap til IT-reglement og andre styrende dokumenter

En mulig årsak til at det er liten kjennskap til disse dokumentene er at det er vanskelig å tilegne seg informasjonen. Det blir ofte mye for en person å forholde seg til, spesielt når informasjonen er spredt utover mange forskjellige sider og dokumenter. Et overordnet ISMS kunne hjulpet med å standardisere sikkerhetsstyringen, og kanskje sentralisere informasjonen.

Årsak:	Dårlige passordvaner
Why?	Fordi de er lite bevisste på sikkerhet
Why?	Fordi de tenker det ikke er så viktig
Why?	Fordi det er ingen tydelige krav rundt passord i NTNU sitt IT-reglement
Why?	Fordi IT-reglementet ikke henviser til de relevante dokumentene
Why?	-

Tabell 9: 5 Whys på dårlige passordvaner

Mange har dårlige passordvaner, fordi de er lite bevisste på sikkerhet, og at de ikke tenker det er så viktig. Mulig årsak til dette kan være fordi det ikke er noen tydelige krav rundt passord i NTNU sitt IT-reglement. IT-reglementet henviser ikke til de dokumentene som nevner passordrutiner [7], og det er bare IT-reglementet brukerne er pliktig å sette seg inn i og skrive under på [23].

Årsak:	Lukrativt for trusselaktører
Why?	Fordi de tjener og sparer penger på å kompromittere kontoer
Why?	Fordi de får tilgang til forskningsdatabaser
Why?	Fordi det er for enkelt å få tilgang til brukerkontoene
Why?	Fordi det er utilstrekkelig tilgangskontroll på brukerkontoene
Why?	-

Tabell 10: 5 Whys på lukrativitet for datakriminelle

Det er lukrativt for datakriminelle å prøve å kompromittere brukerkontoer fordi det er for god kost-nytte effekt. De kan tjene penger på å selge kontoene, eller spare penger ved å laste ned forskningsartikler. Her kom vi frem til at utilstrekkelig tilgangskontroll kan være en rotårsak til at det er så høy kost-nytteverdi for trusselaktørene.

7.6 Rotårsakseliminering

7.6.1 Systematisk Innovativ Tenkning (SIT)

Alle komponenter som eksisterer i problemets naturlige omgivelser listes under:

- E-postadresse
- Brukernavn
- Autentisering
- IT-reglement
- Retningslinjer for behandling av brukernavn, passord og andre autentiseringsdata
- Prinsipper for informasjonssikkerhet (inkludert Policy)
- Påloggingssystem
- E-post filter

Når komponentene er gjort rede for, vil de fem SIT prinsippene brukes sekvensielt på komponentene for å utvikle løsninger på problemene. Ikke alle SIT-prinsipper finner løsninger som er gjennomførbare for alle komponenter. I disse tilfellene vil det stå: "Ikke gjennomførbart". Resultatene fremheves under.

E-post

- **Attributtavhengighet** Ikke gjennomførbart.
- **Komponentkontroll** Bevisstgjøringskampanje for god e-postskikk.
- **Erstatning** Gi folk kurs og hjelp til å ordne private e-postadresser.
- **Forkastning** Ikke gjennomførbart.
- **Oppdeling** Gi folk en egen epost adresse som bare skal brukes til privat bruk.

Brukernavn

- **Attributtavhengighet** Ikke gjennomførbart.
- **Komponentkontroll** Ikke gjennomførbart.
- **Erstatning** Ha mer tilfeldig brukernavn som er vanskeligere å gjette.
- **Forkastning** Ikke la e-postadressen kunne brukes som brukernavn.
- **Oppdeling** Ikke gjennomførbart.

Autentisering

- **Attributtavhengighet** Krav om sterkere passord.
- **Komponentkontroll** Bruke passordmanager for å behandle passord.
- **Erstatning** Ikke gjennomførbart.
- **Forkastning** Ikke gjennomførbart.
- **Oppdeling** Gå over til 2-faktor autentisering.

IT-reglement

- **Attributtavhengighet** Utbedre IT-reglementet med tydeligere krav rundt passord.
- **Komponentkontroll** Henvise til de andre styringsdokumentene.
- **Erstatning** Ikke gjennomførbart.
- **Forkastning** Ikke gjennomførbart.
- **Oppdeling** Ikke gjennomførbart.

Retningslinjer for behandling av brukernavn, passord og andre autentiseringsdata

- **Attributtavhengighet** Ikke gjennomførbart.
- **Komponentkontroll** Bevisstgjøringskampanje.
- **Erstatning** Legge retningslinjene inn i IT-reglementet.
- **Forkastning** Ikke gjennomførbart.
- **Oppdeling** Ikke gjennomførbart.

Prinsipper for informasjonssikkerhet

- **Attributtavhengighet** Ikke gjennomførbart.
- **Komponentkontroll** Integrere det i et ISMS
- **Erstatning** Ikke gjennomførbart.
- **Forkastning** Ikke gjennomførbart.
- **Oppdeling** Ikke gjennomførbart.

Påloggingssystem

- **Attributtavhengighet** Øk minimum antall tegn på passord fra 8 til 10.
- **Komponentkontroll** Overholde kravet om å bytte passord hver 12. måned.
- **Erstatning** Ikke gjennomførbart.
- **Forkastning** Ikke gjennomførbart.
- **Oppdeling** Enhetskontroll på nye innlogginger.

E-post filter

- **Attributtavhengighet** Forbedre e-post filter.
- **Komponentkontroll** Ikke gjennomførbart.
- **Erstatning** Ikke gjennomførbart.
- **Forkastning** Ikke gjennomførbart.
- **Oppdeling** Ikke gjennomførbart.

Vi sorterer og beskriver de mest relevante idéer til videre utdyping:

Bevisstgjøringskampanje for god e-postskikk Med god e-postskikk så mener vi at brukerene er bevisste på om e-post er legitim eller ikke, og at NTNU e-post ikke skal bli benyttet til andre tjenester.

Gi folk kurs og hjelp til å ordne private e-postadresser Det er et problem at folk bruker sin NTNU e-post til andre tjenester. Dette kan være fordi de ikke har en egen privat e-post de kan bruke til dette. Dette tiltaket vil hjelpe de med å anskaffe en privat e-post, så de ikke bruker NTNU e-posten på andre ting en det den er ment for.

Ikke la e-postadressen kunne brukes som brukernavn Dersom e-postadressen er brukt på andre tjenester med samme passord som NTNU, kan trusselaktørene også kompromittere NTNU kontoen. Hvis ikke e-postadressen lar seg bruke som brukernavn, vil det senke risikoen for at de får logget seg på.

Krav om sterkere passord Krav om sterkere passord i form av økt minimumslengde til 10 tegn.

Overholde kravet om å bytte passord hver 12. måned I retningslinjene for behandling av autentiseringsdata er det krav om å bytte passord hver 12. måned. Dette blir ikke håndhevet. Et mulig tiltak er derfor å automatisk kreve endring av passord hver 12. måned.

Gå over til 2-faktor autentisering For å hindre at kontoen blir kompromittert dersom passordet ble det kan man benytte seg av 2-faktor autentisering. Dette skaper ekstra redundans dersom kredentialiene går tapt.

Bruke passordmanager for å behandle passord Det blir lettere å behandle lange, kompliserte og unike passord med en passordmanager.

Utbedre IT-reglementet med tydeligere krav rundt passord Per nå er det eneste som står i IT-reglementet rundt passord at man skal bytte passord dersom man har mistanke om at noen vet det. Dette mener vi ikke er nok, og burde utbedres, for eksempel ved å referere til retningslinjer for behandling av autentiseringsdata.

Henvise til de andre styringsdokumentene Per nå er det lite henvisning til andre styringsdokumenter som gjør det vanskelig og tungvint for brukerene å lete igjennom dokumentene. Dette burde samles på ett sted og henvise til hverandre.

Bevisstgjøringskampanje rundt autentiseringsdata Bevisstgjøringskampanjen skal få frem at passordet til NTNU kontoen skal ikke bli brukt til andre tjenester for å sikre at uvedkommende ikke får tilgang til kontoen.

Integrere Prinsipper for informasjonssikkerhet i et ISMS Etter hva vi har fått av informasjon fra oppdragsgiver har ikke NTNU et skikkelig ISMS. Dette er noe som før eller siden bør være på plass.

Enhetskontroll på nye innlogginger En mulig måte å gjennomføre dette på er å sende en e-post eller SMS om å autorisere enheten når det er første gang du logger på, på den enheten. Eventuelt validere den for 30 dager av gangen før dette må gjøres på nytt.

7.6.2 Tiltaksplan

Etter å ha brukt de fem SIT-prinsippene på hver komponent, og filtrert de, sitter vi igjen med et par idéer. I denne delen fremhever vi idéer i en tiltaksplan som vi anbefaler å implementere. Under beskrives de ulike tiltakene:

Bevisstgjøringskampanje for god e-postskikk og behandling av autentiseringsdata Denne bevisstgjøringskampanjen vil inkludere opplæring i deteksjon av phishing e-post, beste praksis innen behandling av brukernavn, passord og andre autentiseringsdata, og innsikt i eksisterende dokumentasjon som NTNU har på informasjonssikkerhet.

Krav om strengere passordkontroll Dette tiltaket vil inkludere en økning av minimum passordlengde til 10 tegn, og innføre en automatisk funksjon som pålegger deg å bytte passord hver 12. måned, slik det er krav om i retningslinjene.

Implementer 2-faktor autentisering Tiltaket går ut på å implementere 2-faktor autentisering for hver innlogging. Vi anbefaler å bruke SMS, som gir deg en kode du kan logge inn med. Dette er ikke nødvendigvis den sikreste 2-faktor løsningen, men det er en av de enkelere.

Enhetskontroll og informering på nye innlogginger Dette tiltaket går på å ha en enhetskontroll der ansvarlig bruker får SMS når noen logger inn fra en ny enhet. Dersom dette var et legitimt påloggingsforsøk fra brukeren kan han eller hun validere enheten for en gitt periode. Vi anbefaler 30 dager av gangen, men dette kan også spesifiseres av brukeren selv.

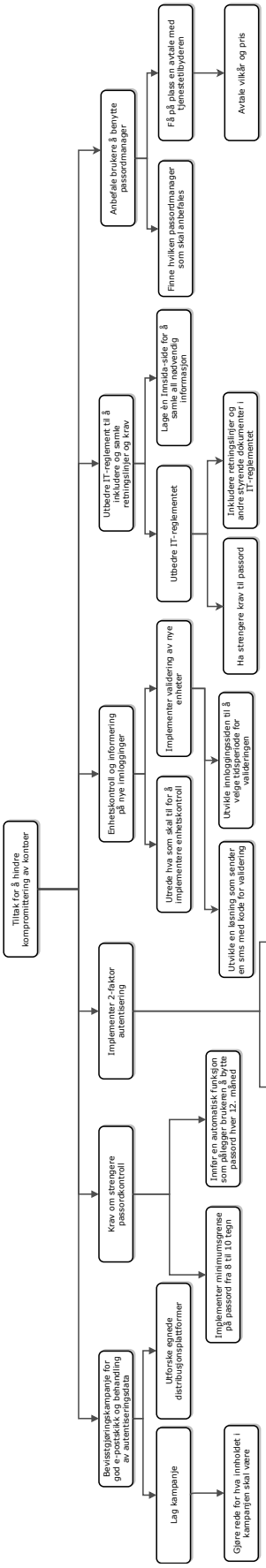
Utbedre IT-reglement til å inkludere og samle retningslinjer og krav Dette tiltaket går på å utbedre passordkrav i tillegg til å henvise retningslinjer og andre styrende dokumenter. Dette burde samles på èn Innsida-side slik at det er lett å finne frem de nødvendige dokumentene til informasjonssikkerhet.

Anbefale brukere å benytte passordmanager Dette tiltaket går på å inkludere passordmanager som et anbefalt verktøy på samlesiden til IT-reglementet, retningslinjer og andre styrende dokumenter

7.7 Løsningsimplementering

7.7.1 Trediagram

For å få en oversikt over hva som må gjøres for å implementere tiltaksplanen bruker vi Trediagram til å dele opp aktivitetene og bestemme rekkefølgen. Diagrammet viser hovedtiltakene og underaktivitetene som må gjøres for å fullføre implementeringen.



Figur 59: Trediagram av tiltak mot kompromitterte kontoer

7.8 Kostnad-nytte-analyse

Denne seksjonen tar for seg en kostnad-nytte-analyse av nytteverdien til bruk av rotårsaksanalyse for case 2.

7.8.1 Kostnad for gjennomføring

I denne analysen definerer vi kostnad som tid brukt på en iterasjonen av metoden. Vi definerer en skala for kostnad fra 1 til 5 der nivåene tilsvarer følgende tidsbruk:

1. Under 50 timer
2. 50-150 timer
3. 150-250 timer
4. 250-400 timer
5. Over 400 timer

Tabell 11 under viser tidsbruken i enkeltfasene i dette caset. Dette inkluderer tid brukt til å dokumentere alt som har med de enkelte fasene å gjøre.

Tabell 11: Tidsbruk i de ulike fasene i case 2

Case 2		
Fase	**Verktøy brukt**	**Timer totalt**
Problemforståelse	Kritiske hendelser	14-18t
Idémyldring	Idemyldring	14-18t
Datainnsamling	Sampling og spørreundersøkelse	70-90t
Datanalyse	Analyseverktøy	90-110t
Rotårsaksidentifisering	Årsak-virkningsdiagram og 5 Whys	18-22t
Rotårsakseliminering	SIT	14-18t
Løsningsimplementering	Trediagram	8-10t
Sum		**228-286t**

Dersom kosten på caset går over flere nivåer regner vi med medianen til ytterpunktene for å plassere kostnaden. Basert på kostnadsnivåene vi definerte over, plasseres tidsbruken på case 2 til:

$$\mathrm{Kostnad} = 4$$

7.8.2 Nytte av resultatene

I denne analysen definerer vi nytten som egen oppfatning av hvor gode resultatene fra caset var. Det vurderes ut fra om vi tror det kan finnes andre underliggende årsaker, og hvorvidt vi mener problemet blir løst dersom rotårsakene fjernes. Nytten defineres på en skala fra 1 til 5.

I dette caset kom vi frem til at rotårsakene var spredt over flere årsaker. Hovedårsakene var gjenbruk av kredentialier på flere tjenester, phishing og utilstrekkelig tilgangskontroll på brukerkontoene. Vi er sikre på at hvis disse årsakene fjernes, vil brorparten av problemet løses. Vi definerer derfor nytten til:

$$\mathrm{Nytte} = 5$$

7.8.3 Total nytteverdi

Når vi regner ut kostnad-nytte deler vi kostnaden på nytteverdien.

$$\frac{\mathit{Kostnad}}{\mathit{Nytte}} = \mathit{Totalnytteverdi}$$

I dette caset blir regnestykket slik:

$$\frac{4}{5} = 0,8$$

Svarene på regnestykket kan bli fra 0,2 til 5. Jo lavere denne nytteverdien er, jo bedre fungerte metoden til caset.

8 Resultater og analyse fra Case 3: Misbruk av NTNU sin infrastruktur til utvinning av kryptovaluta

I dette kapittelet fremlegger vi våre resultater i alle fasene i case 3.

8.1 Problemforståelse

8.1.1 Ytelsesmatrise

Variablene som ble vurdert til å kunne hjelpe til å redusere utvinning av kryptovaluta hos NTNU er som følger:

Adgangskontroll på HPC klynger: Klynger av tilkoblet maskinvare som sammen utgir svært høy ytelse. Er også kjent som superdatamaskiner. Disse er godt beskyttet med streng adgangskontroll og logging av alt som blir gjort.

Adgangskontroll på kritiske servere: Adgangskontroll til servere som har en funksjonskritisk og/eller virksomhetskritisk rolle i driften av NTNU, som for eksempel DNS og DHCP servere.

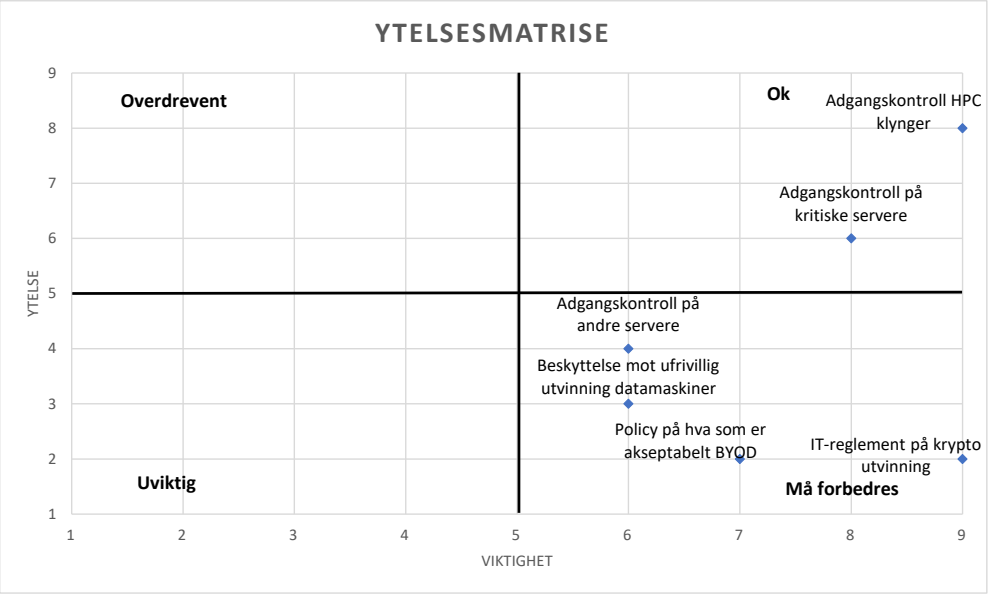
Adgangskontroll på andre servere: Adgangskontroll til alle servere som ikke har en kritisk rolle i NTNU, men som fortsatt kan bli misbrukt. Inkluderer servere som står åpent ut mot nettet.

Beskyttelse mot ufrivillig utvinning på datamaskiner: Beskyttelse mot at personer får tilgang til din datamaskin gjennom nettleseren og bruker den til å utvinne kryptovaluta.

Policy på hva som er akseptabelt som BYOD: Definerer hva som er lov å ta med av BYOD.

IT-reglement på kryptoutvinning: IT-reglementet spesifiserer per i dag bare at det å misbruke universitetets ressurser til kommersiell virksomhet ikke er greit. Det kan være vanskelig for folk å skjønne at strøm er en slik ressurs og at utvinning av kryptovaluta kan regnes som kommersiell virksomhet. Slik som IT-reglementet er idag er det heller ikke noen gode sanksjonsmuligheter mot folk som utvinner kryptovaluta.

Under ser vi hvor de ulike ressursene, eller aktiva, er plassert i henhold til de tidligere nevnte områdene.



Figur 60: Resultater fra ytelsesmatrisen

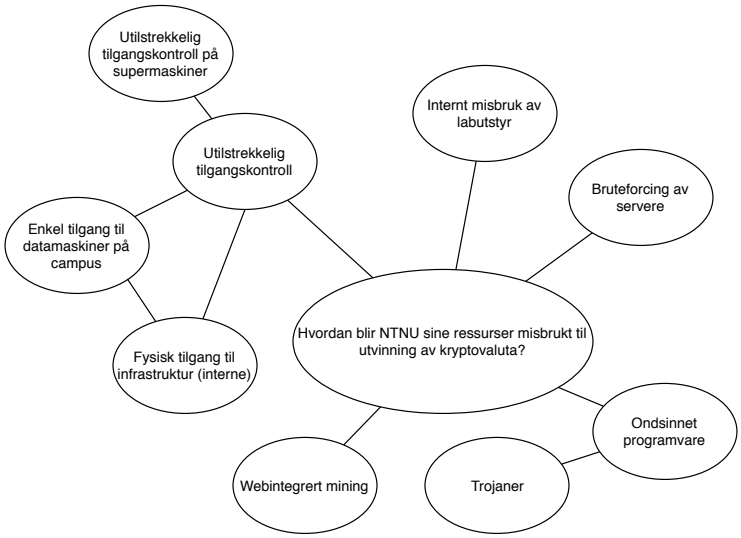
Det er mest kritisk å vurdere de variablene som havner under "må forbedres". Selv om noen havner under "ok", bør de fortsatt vurderes, men de vil ha lavere prioritet enn de nevnt over. Variabler som er uviktig eller overdrevent trenger man ikke vurdere nøye. Matrisen viser følgende prioriteringsgrunnlag til utbedring:

1. IT-reglement på kryptoutvinning
2. Policy på hva som er akseptabelt som BYOD
3. Beskyttelse mot ufrivillig utvinning på datamaskiner
4. Adgangskontroll på andre servere
5. Adgangskontroll på kritiske servere
6. Adgangskontroll på HPC klynger

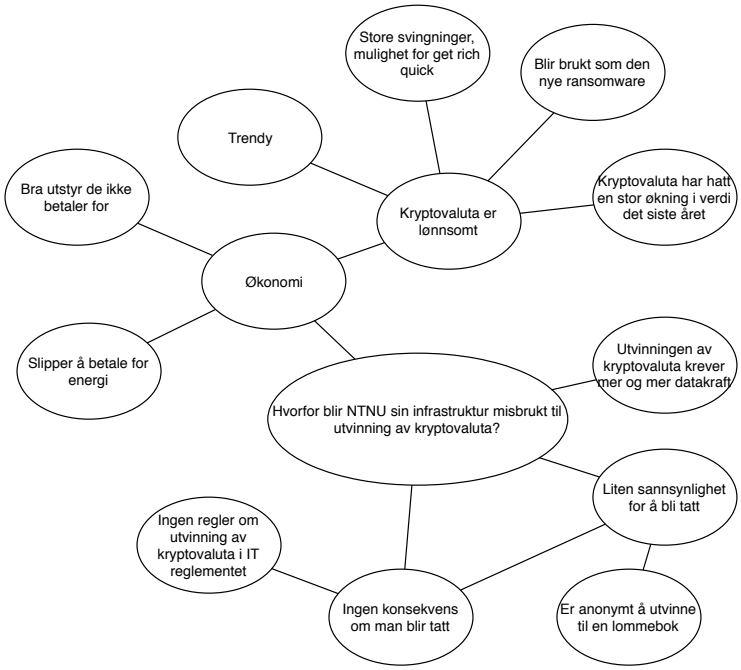
8.2 Idémyldring

8.2.1 Idémyldring

Etter at idémyldringsøkten var ferdig ble det gjort en vurdering av hvilke momenter som hørte sammen eller hadde likhetstrekk. Disse ble gruppert sammen, se figur 61 og 62 under.



Figur 61: Resultater og gruppering av Hvordan



Figur 62: Resultater og gruppering av Hvorfor

Resultatene er gruppert inn i 4 hovedkategorier:

Ondsinnet programmvare Er i stor grad trojanere i form av javascript.

Utilstrekkelig tilgangskontroll Tilganskontroll på diverese datamaskiner rundt på campus, som kan utnyttes.

Økonomi Er i stor grad motivasjonen til aktørene, der det er stor økonomisk vinning med kryptovaluta.

Ingen konsekvens om man blir tatt Det står lite i IT-reglementet om at kryptoutvinning ikke er lov.

8.2.2 NGT

Etter at hvert gruppemedlem hadde gitt ut sine 15 poeng satt vi igjen med 4 idéer som stakk seg ut med hvor mange poeng de fikk. Disse vises i fet skrift i tabell 12.

	Årsak	Poeng
A	Bra utstyr de ikke betaler for	5
B	Bruteforce av servere	0
C	Enkel tilgang til datamaskiner på campus	0
D	**Ingen regler om utvinning av kryptovaluta i IT-reglementet**	11
E	**Internt misbruk av labutstyr**	8
F	Kryptovaluta har hatt en stor økning i verdi det siste året	0
G	Liten sannsynlighet for å bli tatt	2
H	**Ondsinnet programvare som utvinner**	16
I	Slipper å betale for energi	0
J	Store svingninger, mulighet for “get rich quick"	0
K	Utilstrekkelig tilgangskontroll på supermaskiner	0
L	Utvinningen av kryptovaluta krever mer og mer datakraft	4
M	**Kryptoutvinner integrert i nettleser**	14

Tabell 12: Oversikt over prioritering av idéer ved hjelp av NGT

Disse fire årsakene er de vi kommer til å fokusere på i dette caset. De fire fokuspunktene kan deles etter de to problemstillingene “hvordan og hvorfor”.

De to årsakene knyttet til “hvorfor” går ut på at det ikke er ulovlig med kryptoutvinning i henhold til gjeldende regelverk [7]. De faller derfor i en gråsone der en ikke får noen represalier for å holde på med kryptoutvinning, annet enn å bli kastet av nettet. Konsekvensene får man hvis en utnytter NTNU sine ressurser til egen vinning.

De neste årsakene går ut på hvilke aktører som bruker universitetet sine ressurser til utvinning av kryptovaluta, og hvordan de bruker ressursene. Internt misbruk av labutstyr går ut på at studenter eller ansatte har tilgang til diverse labber og PCer som kan brukes til utvinning av kryptovaluta. Både ondsinnet programvare som utvinner kryptovaluta og kryptoutvinnere integrert i nettleser brukes av eksterne trusselaktører. Pengene som tjenes her går til kriminelle. Utvinning av kryptovaluta har blitt mer utbredt som et alternativ til løsepengevirus, der løsepengevirus har blitt mindre lønnsomt den siste tiden [24].

8.3 Datainnsamling

8.3.1 Spørreundersøkelse

Før intervjuet fikk vi et utdrag av alarmer som SOCen får av de kjente signaturene som omhandler kryotoutvinning. Disse alarmene stammer fra kryptoutvinnere som folk har fått lagt inn på PCene sine, kryptoutvinnere i nettleser som er lagt inn på diverse nettsteder eller trojanere.

Vi hadde noen hypoteser når vi utformet intervjuspørsmålene, disse var:

- Det er tekniske løsninger som kan brukes til å fikse store deler av problemet.

- Det er begrenset handlingsrom for hva som kan bli gjort mot interne som utvinner.
- Lite bevissthet rundt regelverket til NTNU angående bruk av universitetets ressurser.
- Utviklingen av utvinning følger kryptovalutaen sin verdi.
- Dataer blir kompromittert gjennom de vanlige formene, phishing og wateringholes.

Spørsmål
Hva er de typiske angrepsvektorene?
Tar det lang tid å oppdage trojanere i nettverket?
Hva gjør Seksjon for Digital Sikkerhet når de oppdager trojanere?
Hvordan fant dere ut om HPC clusterne blir misbrukt?
Hvordan fant dere ut at det var internt misbruk?
Har dere andre tiltak enn å stenge internett til de som miner?
hva er grunnen til at dere ikke har implementert noe slike tiltak?
Hva tror du er oppfatningen blant dine kolleger er angående utvinning. Vet folk det er ulovlig eller har de ikke tenkt så mye over det og utvinner fordi det er en trend?
Hva er måten dere for du snakket tidligere om at dere så mange av de lommebøkene som ble brukt var fra mørke siden av nettet?
Hvordan ser dere at de går til disse lommebøkene?
Hvordan skal dere implementere kryptoutvinning i neste IT-reglement?
Tenker folk over at det ikke er lov til å utvinne kryptovaluta i henhold til IT-reglementet?
Har dere noen tiltak på utvinning på nettsider?
Er det like stor økning nå som det var før jul?
Økningen er det gjort av de profesjonelle aktørene eller er det folk som setter frivillig opp utvinnere?
Dere hadde ikke sett noe tilfeller av bruteforcede PCer og servere som ble installert kryptominere på, etter at de ble bruteforcet?
Er det noen regler på hva ansatte får lov til å legge på serverne?
Har dere noen tilfeller av PCer på datalabber der studenter har installert kryptoutvinning?

Tabell 13: Spørsmål til intervju case 3

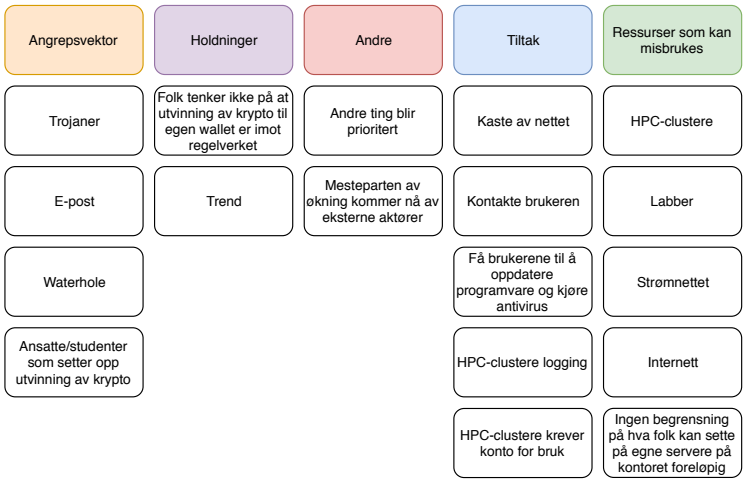
Under intervjuet ble det tatt lydopptak, slik at vi lett kunne gå tilbake til svarene for å få det mest mulig nøyaktig til neste fase. Når intervjuet var ferdig ble det transkribert. Transkripsjonen finnes i vedlegg K.

8.4 Dataanalyse

8.4.1 Affinitetsdiagram

Affinitetsdiagram brukes til å analysere data som det ikke er mulig å nummerere, eksempelvis meninger eller idéer. Affinitetsdiagram grupperer data og finner de underliggende korrelasjoner og likhetstrekk i gruppen.

Analysen ble gjennomført med å ta transkripsjon av intervjuet og stykke den opp i fem hovedgrupper.



Figur 63: Hvordan fungerer utvinning av kryptovaluta ved NTNU?

Affinitetsdiagrammet deles inn i hovedkategoriene: angrepsvektor, holdninger, ressurser som kan misbrukes, tiltak og andre. Blant disse er mulige årsaker til problemet og anbefalte tiltak som kan løse det.

8.5 Rotårsaksidentifisering

8.5.1 5 whys

Det ble fremhevet fem årsaker som skulle analyseres. Fire av disse kom fra fiskebeindiagrammet over, og en fra idémyldring. Tabellene under viser resultatene fra gjennomføringen.

Årsak:	Ansatte og studenter utvinner kryptovaluta med universitetet sine ressurser
Why?	Lønnsomhet
Why?	Har ingen utgifter
Why?	Bruker strøm og infrastrukturen til universitetet
Why?	Det er en gråsone i regelverket
Why?	Ikke spesifisert godt nok i IT-reglementet

Tabell 14: 5 Whys på ansatte og studenter utvinner kryptovaluta med universitetet

Det å utvinne kryptovaluta på universitetet sine ressurser er alt fra å kjøre en kryptoutvinner på en PC til å sette opp maskinvare ment for kryptoutvinning. I 5 Whys over kom vi frem til at lønnsomhet er primærgrunnen til at de driver med kryptoutvinning, men årsaken til at ansatte og studenter utvinner på universitet er at det ikke er spesifisert godt nok i IT-reglementet.

Årsak:	Eksterne trusselaktører utvinner kryptovaluta med universitetet sine ressurser
Why?	Lønnsomhet
Why?	Enkelt å spre minere
Why?	Folk går inn på waterholes og trykker på phishingmail
Why?	Brukeren var ikke oppmerksom nok på e-post eller siden de gikk på
Why?	Brukere har ikke fått nok opplæring i hvordan dette unngås

Tabell 15: 5 Whys Eksterne trusselaktører utvinner kryptovaluta med universitetet sine ressurser

Årsaken til at eksterne trusselaktører utvinner kryptovaluta med universitetet sine ressurser er fordi det er en lønnsom affære som koster lite å distribuere og som det er liten sannsynlighet å bli tatt for. Dette virker i kombinasjon med at brukere ikke er oppmerksom på hva de trykker på. Rotårsaken til at de ikke er oppmerksomme er at de ikke har fått nok opplæring.

Årsak:	Utvinnere som implementert inn i nettsider
Why?	God fortjeneste
Why?	Fordi de når en stor menge folk som utvinner kryptovaluta for dem
Why?	Mange har ikke en annonseblokkering som også stopper utvinnere på nett
Why?	På grunn av lite eller ingen opplæring til denne typen programvare
Why?	Ikke prioritert
Why?	Fordi det ikke er nok folk/ressurser

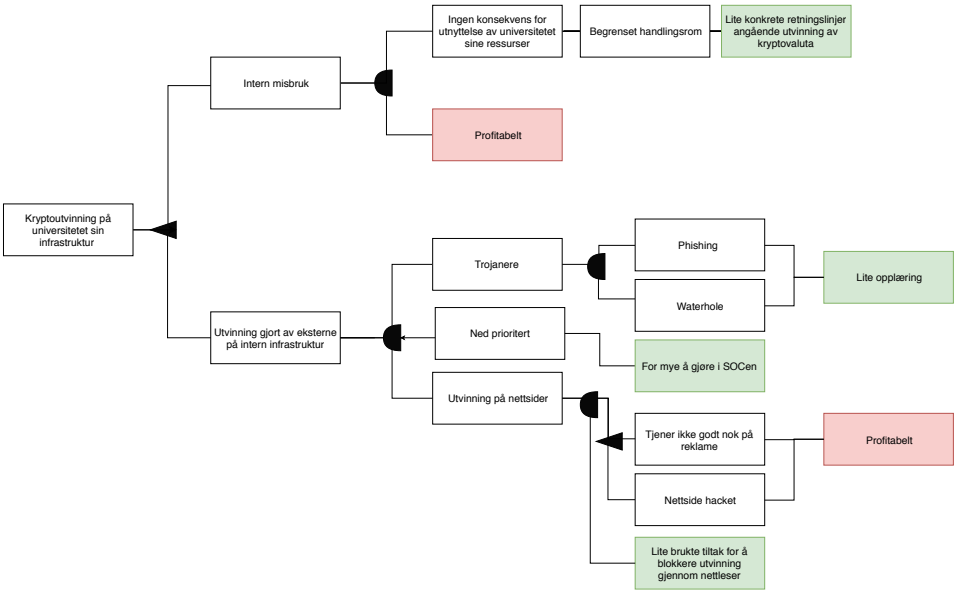
Tabell 16: 5 Whys på ansatte og studenter utvinner kryptovaluta med universitetet sine ressurser

Utvinning på nettsider blir mer utbredt fordi det er profitabelt og en god erstatning til reklame. Dette kan bli stoppet med annonseblokkering eller blokkering av DNS adresser. Dette blir ikke gjort fordi det ikke er en prioritet fra Seksjon for Digital Sikkerhet.

8.5.2 Feiltreanalyse

Feiltreanalyse tar for seg alle mulige årsaker i et diagram og identifiserer mulige relasjoner. Analysen bygger på hva som ble gjort i 5 Whys.

Vi har kommet fram til fire hovedgrunner til at kryptoutvinning på NTNU forekommer. Rotårsaken er sammensatt av årsakene definert i figur 64. I dette caset er problemet delt inn i to deler: de interne og de eksterne. Det er to forskjellige typer årsaker, der interne går mer på regelverk og eksterne er mer teknisk.



Figur 64: Feiltreanalyse

I figur 64 over representerer trekanter “eller” og halvsirkelen “og”. De røde boksene er de årsakene vi ikke kan gjøre noe med, mens de grønne kan det gjøres noe med.

8.6 Rotårsakseliminering

8.6.1 SIT

Alle komponenter som eksisterer i problemets naturlige omgivelser listes under:

- IT-reglement
- Annonseblokker
- Internett
- SOCen
- Brannmur
- Servere og datamaskiner
- Datalabber
- HPC-cluster
- Bring your own device (BYOD)
- Strøm

Når komponentene er gjort rede for, vil de fem SIT prinsippene brukes sekvensielt på komponentene for å utvikle løsninger på problemene. Ikke alle SIT-prinsipper finner løsninger som er gjennomførbare for alle komponenter. I disse tilfellene vil det stå: “Ikke gjennomførbart”. Resultatene fremheves under.

IT-reglement

- **Attributtavhengighet** Legge til et større fokus på utvinning av kryptovaluta.
- **Komponentkontroll** Gjennomføre en informasjonskampanje for å sette fokus på hva som er misbruk.
- **Erstatning** Ikke gjennomførbart.

- **Forkastning** Ikke gjennomførbart.
- **Oppdeling** Ikke gjennomførbart.

Annonseblokker

- **Attributtavhengighet** Legge til blokkering av kryptoutvinning
- **Komponentkontroll** Passe på at alle ansatte har annonseblokker installert som også stopper utvinning av kryptovaluta.
- **Erstatning** Ikke gjennomførtbart
- **Forkastning** Ikke gjennomførtbart
- **Oppdeling** Ikke gjennomførtbart.

Internett

- **Attributtavhengighet** Blokkere kryptoutvinning
- **Komponentkontroll** Automatisere at alle datamaskiner som utvinner kryptovaluta blir kastet av nettet.
- **Erstatning** Ikke gjennomførtbart.
- **Forkastning** Ikke gjennomførtbart.
- **Oppdeling** Ikke gjennomførtbart.

SOC

- **Attributtavhengighet** Øke antall ansatte.
- **Komponentkontroll** Økt prioritet til kryptovaluta.
- **Erstatning** Ikke gjennomførtbart.
- **Forkastning** Ikke gjennomførtbart.
- **Oppdeling** Gi forslag til implementering av tiltak til bachelorgrupper.

Servere og datamaskin

- **Attributtavhengighet** Strengere adgangskontroll.
- **Komponentkontroll** Ikke gjennomførtbart.
- **Erstatning** Ikke gjennomførtbart.
- **Forkastning** Ikke gjennomførtbart.
- **Oppdeling** Ikke gjennomførtbart.

Datalabber

- **Attributtavhengighet** Strengere adgangskontroll.
- **Komponentkontroll** Logging.
- **Erstatning** Svakere maskinvare på labbene.
- **Forkastning** Slutte å tilby labber, som kan brukes i sammenheng med kryptoutvinning.
- **Oppdeling** Ikke gjennomførbart.

HPC-clustere

- **Attributtavhengighet** Øke tilgangskontrollen ytterligere.
- **Komponentkontroll** Ikke gjennomførbart.
- **Erstatning** Ikke gjennomførbart.
- **Forkastning** Ikke gjennomførbart.
- **Oppdeling** Ikke gjennomførbart.

Bring your own device (BYOD)

- **Attributtavhengighet** Ikke gjennomførbart.
- **Komponentkontroll** Kaste datamaskiner som ikke tilhører NTNU-personell av nettet slik at de manuelt må koble seg på igjen.
- **Erstatning** Ikke gjennomførbart.
- **Forkastning** Ikke gjennomførbart.
- **Oppdeling** Ikke gjennomførbart.

Strøm

- **Attributtavhengighet** Ikke gjennomførtbart
- **Komponentkontroll** Strømkvotering, overstiges kvoten må vedkommende betale for strømmen
- **Erstatning** Ikke gjennomførtbart
- **Forkastning** Ikke gjennomførtbart
- **Oppdeling** Ikke gjennomførtbart

Vi sorterer og beskriver de mest relevante idéer til videre utdyping:

Gjennomføre en informasjonskampanje om kommersielt misbruk av NTNU sin infrastruktur Kampanjen skal få frem at det å bruke NTNU sine ressurser til kommersiell virksomhet bryter IT-reglementet. I NTNU sine ressurser inkluderer strøm og internett.

Legge til et større fokus på utvinning av kryptovaluta i IT-reglementet Gi IT-reglement et større fokus på kryptoutvinning og gi klarere retningslinjer på hva som ikke er akseptabelt.

Legge til annonseblokker som stopper utvinning Aktivere blokkering av utvinningsprotokoll på annonseblokkere og passe på at alle har en annonseblokkeringstjeneste installert.

Blokkere kryptoutvinning Med dette mener vi å gjøre et eller flere tiltak som å blokkere DNS-forespørsler som omhandler kryptoutvinning.

Øke antall personell i SOC SOC har mange oppgaver som er mer kritiske enn kryptoutvinning. Derfor foreslår vi å ansette flere, kanskje i kombinasjon med bachelor-oppgaver.

Strengere adgangskontroll Begrenser tilgang til datalabber.

Logging Øke bruk av logging i datalabbene.

Kaste datamaskiner som ikke er kritisk infrastruktur av nettet Ved midnatt blir alle datamaskiner eller servere som ikke er kritisk infrastruktur koblet av nettet og må manuelt koble seg på nettet igjen.

8.6.2 Tiltaksplan

Etter å ha brukt de fem SIT-prinsippene på hver komponent og filtrert de, sitter vi igjen med et par idéer. I denne delen fremhever vi idéer i en tiltaksplan som vi anbefaler å implementere. Under beskrives de ulike tiltakene:

Gjennomføre en informasjonskampanje om kommersielt misbruk av NTNU sin infrastruktur Utvinning av kryptovaluta er en ny ting, hvor mange ikke er klar over hvordan universitetet sitt regelverk håndterer temaet. Vår anbefaling er å ha en kampanje der universitet informerer om hva som regnes som NTNU sine ressuser og hvordan disse ikke skal brukes til kommersiell virksomhet.

Legge til et større fokus på utvinning av kryptovaluta i IT-reglementet Endre IT-reglementet slik at det blir tydelig at kryptoutvinning ikke er lovlig bruk av NTNU sine ressurser.

Blokkere kryptoutvinning Dette tiltaket går ut på å blokkere DNS-forespørsler tilknyttet kryptoutvinning. Slik at PCer som blir brukt i utvinning ikke kan hente nye oppgaver å løse. De velkjente DNS-ene blokkeres. Videre kan loggen bli benyttet for å legge nye domener inn i en svarteliste, eller justere de gamle DNS-ene.

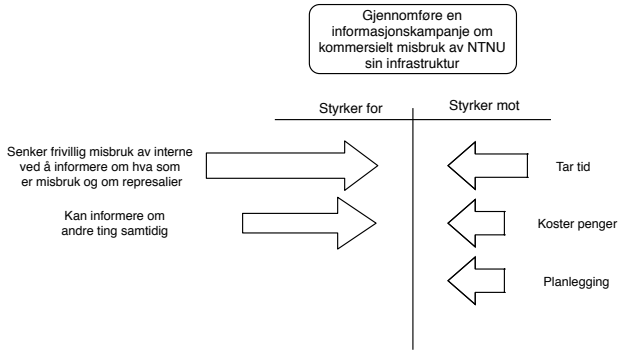
Øke antall personell i SOC SOCen kan ikke prioritere å stoppe utvinning av kryptovaluta. Derfor anbefaler vi å enten øke mengden personell i SOCen, eller gi utvikling av et teknisk forslag til implementasjon som en bacheloroppgave.

8.7 Løsningsimplementering

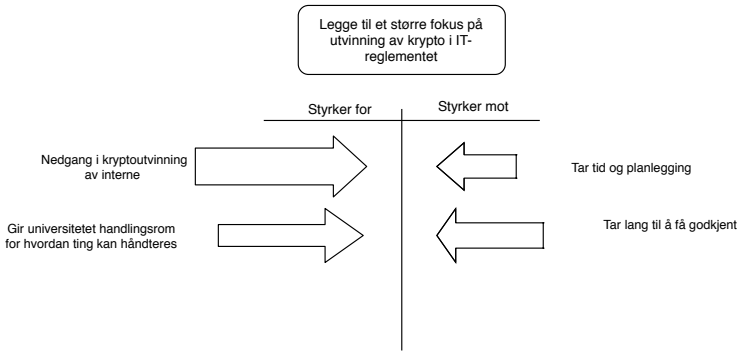
8.7.1 Kraftfeltsanalyse

Kraftfeltsanalyse blir brukt for å få en oversikt over hvilke styrker som er for og hvilke styrker som er mot implementering av tiltakene. Dette verktøyet gir en plan over hvilke tiltak som er lettest å gjennomføre.

Informasjonskampanjen og endringen i IT-reglementet bør gjøre i kombinasjon med hverandre. Der IT-reglementet får klartgjort at selv om kryptoutvinning ikke ulovlig i henhold til norsk lov, er det imot NTNU sitt IT-reglement så fremt det ikke er søkt om. Når endringen er gjort, gjennomføres informasjonskampanjen. Under, i tabell 65 og 66, viser resultatene fra kraftfeltsanalysen på informasjonskampanje og endring i IT-reglementet.

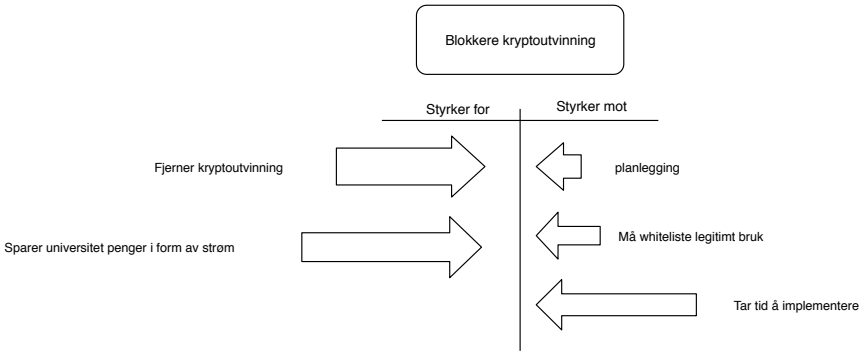


Figur 65: Oversikt over informasjonskampanjen



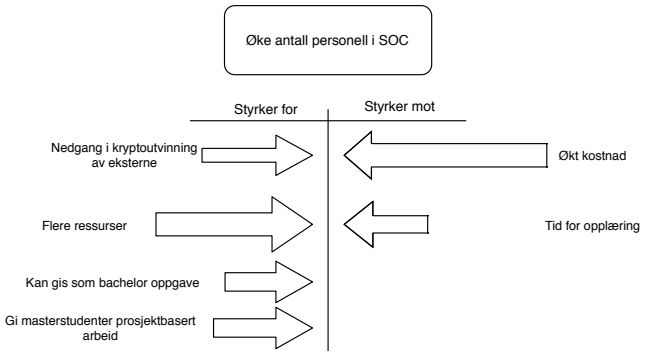
Figur 66: Endring i IT-reglementet

Fra dataanalysen kom vi frem til at selv om det finnes tekniske løsninger, har ikke SOCen hatt mulighet til å implementere DNS blokkering på bakgrunn av mangel på ressurser. Figur 67 og 68 viser hva som skal til for å blokkere DNS og hva som må til for å øke ressursene til SOCen. Vi estimerer at den største kraften mot implementering av dette kommer til å være tidsbruk og kostnadene rundt tidsbruk.



Figur 67: Blokkering av DNS forespørsel

Ved å øke antall ansatte i SOCen estimerer vi at kosten av en ny ansatt vil være største kraften mot. Det er vanskelig å si om vedkommende vil ha nok arbeidsoppgaver til at det er verdt ansettelsen. Det bør vurderes å gi prosjekter til bachelor- og masterstudenter.



Figur 68: Øke andel ansatte i SOC

Figurene viser våres antakelser på hvilke krefter som jobber for implementeringen og hvilke som jobber mot, samt estimater på styrken til kreftene. Lengden på pilene indikerer antatt styrke.

8.8 Kostnad-nytte-analyse

Denne seksjonen tar for seg en kostnad-nytte-analyse av nytteverdien til bruk av rotårsaksanalyse for case 3.

8.8.1 Kostnad for gjennomføring

I denne analysen definerer vi kostnad som tid brukt på en iterasjonen av metoden. Vi definerer en skala for kostnad fra 1 til 5 der nivåene tilsvarer følgende tidsbruk:

1. Under 50 timer
2. 50-150 timer
3. 150-250 timer
4. 250-400 timer
5. Over 400 timer

Tabell 17 under viser tidsbruken i enkeltfasene i dette caset. Dette inkluderer tid brukt til å dokumentere alt som har med de enkelte fasene å gjøre.

Tabell 17: Tidsbruk i de ulike fasene i case 3

Case 3		
Fase	**Verktøy brukt**	**Timer totalt**
Problemforståelse	Ytelsesmatrise	16-20t
Idémyldring	Idémyldring og NGT	16-20t
Datainnsamling	Intervju	20-30t
Datanalyse	Affinitetsdiagram	15-20t
Rotårsaksidentifisering	5 whys og feil-tre diagram	25-30t
Rotårsakseliminering	SIT	15-20t
Løsningsimplementering	Kraftfeltsdiagram	10-15t
Sum		**117-155t**

Dersom kosten på caset går over flere nivåer regner vi med medianen til ytterpunktene for å plassere kostnaden. Basert på kostnadsnivåene vi definerte over, plasseres tidsbruken på case 3 til:

$$\mathrm{Kostnad} = 2$$

8.8.2 Nytte av resultatene

I denne analysen definerer vi nytten som egen oppfatning av hvor gode resultatene fra caset var. Det vurderes ut fra om vi tror det kan finnes andre underliggende årsaker, og hvorvidt vi mener problemet blir løst dersom rotårsakene fjernes. Nytten defineres på en skala fra 1 til 5.

I dette caset kom vi frem til at rotårsakene var uklarhetet i IT-reglement når det kommer til utvinning av kryptovaluta, samt for lite ressurser på Seksjon for Digital Sikkerhet for å gjøre noe med tekniske løsninger. Caset ble preget av svakt datagrunnlag, så vi har grunn til å tro at det kan være flere rotårsaker. Tiltakene vi kom frem til vil kunne hjelpe med å begrense konsekvensene til problemet, men vil trolig ikke fjerne det helt.

Vi definerer derfor nytten til:

$$Nytte = 2$$

8.8.3 Total nytteverdi

Når vi regner ut kostnad-nytte deler vi kostnaden på nytteverdien.

$$\frac{Kostnad}{Nytte} = Totalnytteverdi$$

I dette caset blir regnestykket slik:

$$\frac{2}{2} = 1$$

Svarene på regnestykket kan bli fra 0,2 til 5. Jo lavere denne nytteverdien er, jo bedre fungerte metoden til caset.

9 Diskusjon

Utgangspunktet i denne drøftingen er hvorvidt rotårsakene vi kom frem til i hvert case er reelle rotårsaker som, hvis fjernet, vil fjerne symptomene helt. I tillegg ser vi på hvordan erfaringen fra de tre casene viser hvor godt rotårsaksanalyse fungerer innen informasjonssikkerhet, om det lønner seg å bruke og hvilke verktøy som fungerer best innen informasjonssikkerhet.

9.1 Hva er rotårsaken til at studenter laster ned opphavsrettsbeskyttet materiale?

Rotårsak: Dårligere utvalg på alternative tjenester i Norge

Ut fra vår analyse viser det seg at dette er hovedårsaken til at studenter laster ned ulovlig. Siden Netflix og de andre strømmetjenestene har inntatt markedet har filmer og serier blitt fordelt mellom tjenestene. Tjenestene ønsker også flest mulig orginale serier som bare finnes hos dem. Dette gjør at tilgjengeligheten på filmer og serier går ned, med mindre man abonnerer på alt. Men selv da får man ikke tilgang på alt. Mange filmer og serier er geografisk blokkert i Norge, som gjør tilgjengeligheten til et enda større problem. I musikkstrømmingsmiljøet er problemet noe mindre. Selv om ulovlig musikknedlasting ikke er borte, har det blitt redusert [25]. Noe av grunnen til dette er at musikkbransjen er mer sentralisert i hvem som eier rettighetene, også kjent som et oligopol. Dette gjør det lettere for strømmetjenestene å skaffe lisenser for musikk, og kan tilby det folk trenger på ett sted. Det er også mye mindre orginalt innhold i disse tjenestene i forhold til strømmetjenester for filmer og serier.

Rotårsak: Tjenestene er ikke verdt prisen

Jo flere tjenester det blir, jo mer må man betale for å få tilgang på mer materiale. Filmer og serier blir spredt utover markedet på flere tjenester som så og si koster det samme. Dette fører til at hver enkelt tjeneste blir mindre verdt pengene man må betale for å få tilgang. Det skal sies at strømming er en revolusjonerende løsning i forhold til å kjøpe hver enkelt film for seg selv, men hvis man må betale for fem forskjellige strømmetjenester for å få tilgang til det man har lyst på, hvorfor ikke bare laste ned gratis? Analysen vår viste at det å betale for tjenester ikke var noe problem for studentene; problemet var at de ikke føler de får det de betaler for.

Rotårsak: Håndheving og kommunisering av lovene knyttet til ulovlig fildeling blir ikke prioritert

Det eksisterer allerede regler på ulovlig nedlasting på universitetsnettet. Problemet er derimot at det er vanskelig å håndheve de. Andre arbeidsoppgaver har heller blitt prioritert. Enkelte tiltak har heller ikke vært lovlige for NTNU å gjennomføre for å stoppe de som driver med ulovlig fildeling. For eksempel er det ikke lov å overvåke enkeltboliger hos Sit, og heller ikke straffe enkeltpersoner dersom de laster ned, siden det blir regnet som inngrep i den private sfæren. Dette har datatilsynet fortalt Seksjon for Digital

Sikkerhet [1].

9.2 Hva er rotårsaken til at brukerkontoer ved NTNU blir kompromittert?

Rotårsak: Gjenbruk av brukerkredentialier på tredjepartssider

Vi har vurdert gjenbruk av brukerkredentialier på andre tjenester som den mest relevante rotårsaken til at NTNU sine brukerkontoer blir kompromittert. Dette gjør vi på bakgrunn av at det var over halvparten som hadde svart at de hadde brukt sine NTNU kredentialier på flere tjenester. Dette betyr ikke nødvendigvis at det er den rotårsaken en bør frykte mest. I en studie gjort på oppdrag fra Google – som tok utgangspunkt i e-postadresser – viste det seg at selv om studien fastslo at det var desidert flest som var blitt kompromittert av datainnbrudd på andre tjenester, hadde flere hadde byttet passord siden de var blitt kompromittert, sammenlignet med de som hadde blitt kompromittert av phishing [26]. Likevel viser studien også den store mengden kontoer som blir kompromittert som følger av datainnbrudd ved andre tjenester, som bekrefter at det fortsatt er et stort problem.

Rotårsak: Phishing

Phishing var en av årsakene som ble belyst, og det viste seg at brukerne ikke hadde fått tilstrekkelig opplæring i deteksjon av phishing e-post. Phishing er, og har lenge vært en stor årsak til kompromitterte kontoer [22]. Phishing skjer også svært hyppig; undersøkelsen vår viste at de aller fleste hadde lagt merke til flere hendelser med phishing på sin NTNU e-post. Phishing kan være vanskelig å gjøre noe med. Vår formening er at det alltid vil være en risiko, uansett hva slags tiltak en implementerer. På en side kan både tekniske og bevissthetsmessige tiltak hjelpe, men disse vil aldri fjerne rotårsaken helt.

Rotårsak: For dårlig kjennskap til styrende dokumenter

Det er alltid en vanskelig oppgave å gjøre de ansatte oppmerksom på beste praksis innen informasjonssikkerhet. Dette gjelder også NTNU siden det i resultatene våre ble fremhevet at de ansatte hadde liten kjennskap til reglementer, retningslinjer og prinsipper knyttet til IT og informasjonssikkerhet. Det er imidlertid en pågående debatt om det i det hele tatt er verdt tiden og pengene i å forsøke å trene opp ansatte. Mange mener disse pengene kan bli bedre brukt på andre vis. Bruce Schneider skriver i sin blogg at dette er bortkastet tid og penger [27]. Mange er enige med han, men det er også mange eksperter som mener det er nyttig. Vi mener derimot det er nyttig, men at ressursbruken på dette burde holdes forholdsvis lav.

Rotårsak: Utilstrekkelig tilgangskontroll på brukerkontoer

Vi har kommet frem til at dette er et problem som kan løse mange av symptomene ved hjelp av tilgangskontroll. 2FA med SMS er noe av det som blir anbefalt av oss siden det er en av de enklere å implementere. Dersom 2FA blir benyttet vil det hindre de fleste kontoer i å bli kompromittert, selv om kredentialiene blir kjent for trusselaktørene. Det er imidlertid mange som mener at SMS-meldinger er en usikker løsning på 2FA, siden SMS-meldinger er relativt enkelt å avlytte [28]. De fleste anbefaler enten autentisering gjennom applikasjon eller fysisk kodebrikke. Disse metodene er dessverre noe vanskeligere å implementere, og det er heller ikke alle som har en smarttelefon som kan bruke

[1] Informasjon fra oppdragsgiver

applikasjonene som kreves. Et annet tiltak som blir mye brukt er å validere brukerkontoen for spesifikke maskiner når en bruker logger på enheten for første gang. Tiltaket kan også gi beskjed om ny innlogging fra et annet sted slik at brukeren blir oppmerksom på at kontoen kan være kompromittert. Disse brukes av flere tjenester for å informere om og hindre kontoer fra å bli kompromittert. Google gir deg både beskjed når nye innlogginger finner sted, og gir deg muligheten til å legge til klarerte enheter [29]. Dette fungerer ofte som en erstatning til 2FA hver gang du logger på. Siden dette har vært effektivt i andre sammenhenger ser vi ingen grunn til at dette ikke vil fungere bra hos NTNU, annet enn den ekstra anstrengelsen for brukerne når de logger på.

9.3 Hva er rotårsaken til misbruk av NTNU sin infrastruktur til utvinning av kryptovaluta?

Rotårsak: Uklarhet i IT-reglementet angående kryptoutvinning

Vi har vurdert uklarhet i IT-reglementet som hovedårsaken bak kryptoutvinning hos de ansatte og studenter, der de utnytter universitetets ressurser. Dette gjør vi fordi IT-reglementet ikke nevner utvinning av kryptovaluta eksplisitt, og fordi kryptovaluta har vært en trend den siste tiden [2]. Siden kryptoutvinning ikke er ulovlig og har blitt betegnet som den nye måten å bli rik på, tenker nok flere ikke over at personlig vinning ikke er lov i henhold til IT-reglement. Her er det informasjonskampanjen kommer inn. Den vil gjøre at folk blir oppmerksom på hva de gjør og hvilke represalier som kan forekomme. Det er en svakhet til løsningen for misbruk av NTNU sine ressurser. Informasjonskampanje vil ikke nødvendigvis endre oppførselen til de som allerede er klar over regelbruddet, men vil kunne hjelpe til å stoppe de som ikke er klar over det.

Rotårsak: Seksjon for Digital Sikkerhet har ikke nok ressurser til å prioritere håndtering av kryptoutvinning

En vanlig måte for eksterne aktører å utvinne kryptovaluta på, er med datamaskiner i et botnett [30]. Botnett er datamaskiner infisert av skadevare som lar den eksterne aktøren utnytte maskinene til deres eget formål. Siden dette er en utbredt måte å angripe på, anser vi det som et godt tiltak å blokkere DNS-adressene til som blir mest brukt. Dette tar derimot tid og er ressurskrevende. Siden det er ressurskrevende er ikke utvinning noe SOCen prioriterer per nå.

Hvis NTNU hadde brukt mer ressurser til å implementere forbyggende tiltak, ville dette kunne senke lukrativiteten på å utvinne med universitetet sin maskinvare. Så hvis vi stopper det utvinning fra å være mulig, vil det stoppe utvinning fra å foregå på NTNU. Det å ansette noen nye bare for å bekjempe utvinning av kryptovaluta er trolig ikke kostnadseffektivt, men om dette ansvarsområdet kombineres med andre kan det kanskje bli verdt det.

9.4 Hvor godt fungerer rotårsaksanalyse innen informasjonssikkerhet?

Det er fortsatt få studier som prøver å sette lys på nytteverdien ved bruk av rotårsaksanalyse innen informasjonssikkerhet. I løpet av dette prosjektet har vi gjort oss en erfaring basert på verktøybruken, men for å fremskaffe empirisk grunnlag for å mene hvor godt

[2] Informasjon fra oppdragsgiver

det fungerer, må det gjerne gjøres mer enn én gang.

På den ene siden vet vi ikke helt hvor godt rotårsaksanalyse har fungert før tiltakene er implementert, og det er kontrollert at symptomene minker eller forsvinner helt. På den andre siden har et tidligere bachelorprosjekt kommet frem til at nytteverdien er stor. De stilte blant annet spørsmål om hvor godt det fungerer på case med lite tid og ressurser, samt mye tid og ressurser [8]. Det ble i begge sammenhenger konkludert med at det ga gode resultater. Vi mener at nytteverdien kommer an på hvor god tilgang en har på relevant informasjon. I de to første casene fikk vi et godt datagrunnlag som ga oss gode muligheter til å avdekke rotårsakene, mens spesielt i det tredje caset slet vi med svakt datagrunnlag. Vi anser dette å være kritisk for hvor god nytteverdien er. I tidligere nevnte bacheloroppgave ble det også erfart at ved hjelp av rotårsaksanalyse er det mulig å oppdage problemer som ikke belyses av andre verktøy [8]. Vi hadde også noen resultater som kom noe overraskende på oppdragsgiver, spesielt at økonomi ikke var så viktig som først antatt på caset om ulovlig fildeling.

Vi har erfart at den strukturerte tilnærmingen til casene som rotårsaksanalyse gir oss er nyttig for å forstå problemet i detalj, og foreslå tiltak som hjelper på det faktiske problemet. Om det fungerer godt er en ting, men om det lønner seg å bruke rotårsaksanalyse innen informasjonssikkerhet er en annen, og dette diskuteres nærmere i neste seksjon.

9.5 Lønner det seg å benytte rotårsaksanalyse i informasjonssikkerhetssammenheng?

Vi har i alle tre casene dokumentert tidsbruken i de ulike fasene av metodikken. Det er tidsbruken sammenlignet med resultatene vi tar utgangspunkt i når det drøftes om det lønner seg å benytte rotårsaksanalyse innen informasjonssikkerhet. Tidsbruken og tilhørende kostnad-nytte-analyse i henholdsvis case 1, 2 og 3, kan sees i seksjon 3, 11 og 17. Det er relativt lik tidsbruk på de to første casene, mens den tredje casen ble gjort raskt. Grunnen var en blanding av at det tredje caset ikke var så omfattende, og at det var liten tid til disposisjon. Likevel fikk vi resultater, selv om disse ikke var like detaljerte som i foregående caser. I det første caset var det vanskelig å nå noen endelig løsning siden rotårsaken til problemet er større enn det universitetet kan løse. Det ble likevel utredet noen gjennomførbare tiltak som kan hjelpe med å senke risikoen, men ikke fjerne rotårsaken. Det er mulig at dette kunne blitt gjort like godt med en risiko- og sårbarhetsanalyse. Det negative med det er at man kan gå glipp av en dypere forståelse av årsaken til fildelingen, og kanskje hatt mindre fokus på å fjerne problemet. En rapport som baserte seg på en tidligere bacheloroppgave som undersøkte bruk av RCA i informasjonssikkerhet kom frem til at RCA ofte burde brukes sammen med en ISRA for å komplimentere hverandre [4]. Ved bruk av RCA fikk vi uansett et dypere innblikk i problemet, og det ble funnet resultater som ikke oppdragsgiver forventet. I caset om kompromitterte kontoer fungerte det veldig bra. Tidsbruken speilet ganske godt de resultatene vi fikk, og nytteverdien her mener vi var best blant casene som ble utført, som vist i seksjon 7.8. Til tross for liten tid og svakt datagrunnlag på case 3, kom vi frem til noen resultater, selv om vi ikke vet om det finnes ytterligere rotårsaker. Det hjalp at caset var lite og håndterbart. Dersom det hadde vært et større og mer komplekst case hadde det gått mye dårligere med så liten tid. En tidligere bacheloroppgave undersøkte hvordan rotårsaksanalyse fungerer på caser med både god og dårlig tid [8]. Denne kom frem til at lang tidsbruk på analysen faktisk fører

til andre resultater enn en normal risikovurdering av problemet. De konkluderte derfor med at resultatene rettferdiggjorde tidsbruken. Kort tidsbruk viste også å lønne seg til en viss grad. De kom frem til forslag til tiltak som ikke hadde blitt vurdert eller implementert tidligere. I en annen rapport som tok utgangspunkt i den tidligere bacheloroppgaven om bruk av rotårsaksanalyse innen informasjonssikkerhet, ble det konkludert mer spesifikt. De konkluderte med at rotårsaksanalyse fungerer best i kompliserte case, men det må gjøres en vurdering på forhånd om problemet er kostbart nok til å være verdt tidsbruken [9].

9.6 Hvilke verktøy som ofte brukes i rotårsaksanalyse, fungerer best innen informasjonssikkerhet?

På bakgrunn av erfaringer vi har tilegnet oss gjennom bruk av rotårsaksanalyse i de tre casene, har vi laget en veiledning for bruk av rotårsaksanalyse innen informasjonssikkerhet. I tillegg til egen erfaring ble også den tidligere bacheloroppgaven [8] tatt i betraktning, men den ble vektet svakere enn egne erfaringer. Veiledningen finnes i kapittel 10.

9.7 Kritikk av oppgaven

Til tross for engasjerende casestudier var case 1 en hard nøtt å knekke. Rotårsakene vi kom frem til var vanskelige å fjerne helt. Dette var muligens på grunn av type case.

Når det kommer til case 3 burde datagrunnlaget vært bedre. Dette kommer av flere ting, blant annet at caset var noe høytflytende og at det var liten tid. Likevel fikk det konsekvenser for resten av oppgaven.

Et annet stort problem for oppgaven var at vi hadde et svakt teorigrunnlag. Med bare én bok som beskrev metodikken og et par rapporter fra én tidligere bacheloroppgave, hadde vi ikke mye å ta utgangspunkt i. Dette kommer litt av at det er lite materiell som beskriver rotårsaksanalyse med utgangspunkt i informasjonssikkerhet.

Det ble også litt kort tid til å skrive veilederen, så den ble noe udetaljert.

10 Veileder i bruk av rotårsaksanalyse innen informasjonssikkerhet

Veilederen er skrevet slik at de kan bli benyttet uten bacheloroppgaven. Derfor vil noe av det som er gjennomgått i bacheloroppgaven bli gjentatt.

10.1 Formål og bakgrunn

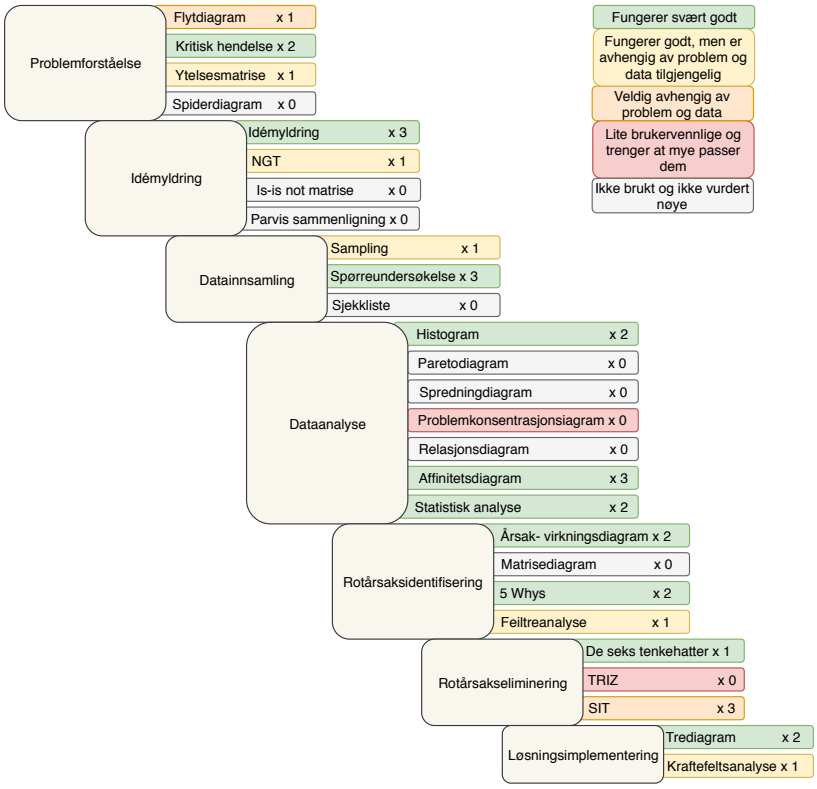
Formålet med dette dokumentet er å gi leseren en veileder for anvendelse av rotårsaksanalyse. Veilederen beskriver anvendelse av rotårsaksanalyseverktøyene beskrevet i boken "Root Cause Analysis: Simplified Tools and Techniques - second edition" av Bjørn Andersen og Tom Fagerhaug [1] i forhold til informasjonssikkerhet. Vi anbefaler denne boken som samlet metodikk. Boken beskriver godt hva som skal til for å komme frem til rotårsaken til et problem.

Dette dokumentet ble skrevet i forbindelse med bacheloroppgave i informasjonssikkerhet der det ble gjennomført tre caser. Veilederene er derfor basert på funn fra disse casene, om hvordan metoden og verktøyene fungerte.

Dette dokumentet vil ikke beskrive verktøyene, men valg av de. Beskrivelsen til verktøyene står i boken til Fagerhaug og Andersen [1].

10.2 Valg av verktøy

Boken beskriver 7 faser i rotårsaksanalyse. Disse må bli fulgt stegvis ettersom hver fase bygger på resultater fra foregående. Verktøyene beskrevet i boken til Fagerhaug og Andersen [1] er generelle verktøy som er ofte brukt i rotårsaksanalyse. Vi har sett på et utvalg av disse verktøyene og hvordan disse fungerer innen informasjonssikkerhet. Figur 69 under viser verktøyene i metodikken, og er fargekodet ut i fra hva vi anbefaler.



Figur 69: De syv fasene i rotårsaksanalyseprosessen

10.2.1 Problemforståelse

Problemforståelse går ut på å få en solid forståelse for problemet en ønsker å løse. Det kan også hjelpe med å skape enighet i teamet rundt hva problemet egentlig omfatter. Det er også viktig for å passe på at ressursene som benyttes for analysen brukes effektivt videre. Verktøyene vi anbefaler til denne fasen er:

Kritiske hendelser

Kritiske hendelser er et godt verktøy å bruke når man har mye data som kan gi et innblikk i hva som går galt. Etter vår erfaring kan man bruke logger til å finne de kritiske hendelsene, hvilket passer utmerket i et informasjonssikkerhetsperspektiv. For kritiske hendelser i informasjonssikkerhet anbefaler vi at det utføres slik:

Steg 1: Logg tilgjengelig Bruk informasjon fra hendelseslogger til å finne informasjon om kritiske hendelser.

Steg 1: Informasjon ikke i logg Om hendelsene ikke er logget, kan informasjon hentes fra personell som jobber med hendelsene, eller samles inn selv.

Steg 2: Sorter hendelsene etter frekvens.

Steg 3: Bruk de mest kritiske hendelsene som startpunkter for analysen.

10.2.2 Ytelsesmatrise

Ytelsesmatrise er et godt verktøy for å få oversikt over hvilke tiltak og kontrollere som blir brukt og hvor godt disse fungerer per nå. Bruk dette verkøyet når du vil undersøke

viktigheten og ytelsen til problemområder, og trenger et prioriteringsgrunnlag.

Steg 1: Lag en tom matrise fra en til ni med horisontal linje som viktighet og den vertikale aksen skal ha nåværende ytelse.

Steg 2: Bestem problemer og variabler som skal analyseres, og estimer viktighet og nåværende ytelse til hver variabel.

Steg 3: Plasser disse på matrisen etter viktighet og ytelse.

Steg 5: Tegn opp fire like områder i matrisen og gi disse følgende navn: Ok (ytelse:5-9, viktighet:5-9), Overdrevent (ytelse:5-9, viktighet:1-5), må forbedres (ytelse:1-5, viktighet:5-9) og uviktig (ytelse:1-5, viktighet:1-5).

Steg 6: Dersom variablene er overrepresentert i en eller to av kvadratene, kan skillelinjene justeres for å jevne ut.

Det som kommer nederst i "må forbedres" prioriteres først for et startpunkt for videre analyse. De andre prioriteres etter dette. Det som kommer under "Ok", bør også vurderes dersom du har nok ressurser.

10.2.3 Idémyldring

Målet med idémyldring er å generere så mange idéer som mulig om et gitt emne. I rotårsaksanalyse er målet stort sett å generere en liste over problemområder som kan forbedres, identifisere mulige konsekvenser, generere en liste over mulige årsaker til problemet og oppmuntre til å tenke på løsninger som kan eliminere problemet. Verktøyene vi anbefaler til denne fasen er:

Idémyldring

Idémyldring gir mange idéer om mulige rotårsaker. Vi brukte idémyldring på våres tre caser og fant verktøyet til å fungere strålende. Skulle det være noen i gruppen som dominerer myldringen, anbefales heller idéskriving. Dette verktøyet fungerer på samme måte som idémyldring, men istedenfor å si idéene høyt, blir de skrevet ned og samlet inn før de skrives på tavlen.

Steg 1: Skriv opp problemstillingen en ønsker å ta utgangspunkt i på en tavle og la personene i gruppen komme med idéer. Husk på å ikke kritisere idéene til hverandre. Prosessen burde la seg dø ut en gang før man tar en runde til, for å sørge for at alle idéer er nevnt.

Steg 2: Sorter alle idéene i grupper og gå videre med de mest lovende idéene.

Nominell gruppe teknikk

Dette verktøyet gir en liste over hva en burde prioritere mest i datainnsamling for å gi ett mer målrettet datagrunnlag for å finne rotårsaken. Vi anbefaler å bruke dette verktøy som et supplement, skulle man ha mange idéer fra idémyldringen og trenger å prioritere.

Steg 1: Gi hver idé fra idémyldringen hver sin bokstav.

Steg 2: Gi alle gruppemedlemene hvert sitt stemmeark, med alle bokstavene på.

Steg 3: Gi fem idéer et tallpoeng fra 1-5 der 5 selvfølgelig er høyest.

Steg 4: Tell opp poengsummene. De idéene med flest poeng prioriteres videre i prosessen.

10.2.4 Datainnsamling

Datainnsamling er et steg i prosessen der man skal være strukturert og samle inn så mye relevant informasjon om problemstillingen som mulig. En god datainnsamling er sentralt for gode resultater i senere faser. Vi anbefaler følgende verktøy:

Sampling Sampling er et godt verktøy for å begrense datainnsamling til en utvalgt del av en større gruppe. Brukes ofte i kombinasjon ble spørreundersøkelser eller sjekklister.

Spørreundersøkelser Spørreundersøkelser er et godt verktøy for å få data fra de berørte personene.

10.2.5 Dataanalyse

I denne fasen blir dataene analysert og visualisert. Hovedmålet er å avklare mulige rotårsaker som har innvirkning på problemet, og hvilke av de som har størst innflytelse. Under beskrives de ulike verktøyene som ble brukt for å analysere dataene. Når det gjelder histogram vil vi ikke skrive noe om stegene som må tas, da det kommer an på hva programvare som brukes. Verktøyene vi anbefaler til denne fasen er:

Histogram Histogram fungerer veldig godt for å skape en visuell forståelse av dataene, som kan gjøre det lettere å se korrelasjoner mellom variabler. Det gir også en tilfredstillende fremstilling av dataen.

Statistisk analyse

Statistisk analyse er ikke i boken, men er en analyse metode som fungerer veldig godt for å se korrelasjoner. Dette fungerer også ved å se på signifikansen.

Steg 1: Gjør om alle svar til numerisk form

Steg 2: Gjennomfør en bivariate korrelasjon på alle svarene

Steg 3: På de som korrelerer, gjennomfør en One-Way ANOVA eller en uavhengig t-test avhengig om det er 2 eller flere grupper i den uavhengige variabelen.

Steg 4: Lag gjerne et histogram på de som har signifikans for å visualisere korrelasjonen.

Affinitetsdiagram

Affinitetsdiagram passer veldig godt med spørreundersøkelser, der det er kortsvar- eller langsvaroppgaver. Den gir mulighet for å gruppere etter innhold i svarene.

Steg 1: Bruk data fra forrige fase til å komme fram til overordnede svar.

Steg 2: Skriv svarene på post-it lapper.

Steg 3: Grupper svarene. Ofte må lappene flyttes flere ganger før gruppene blir funnet. Det bør ikke overstige 5-10 grupper

Steg 4: Lag tittel på gruppene og lag grafikk.

10.2.6 Rotårsaksidentifisering

De foregående fasene skal ha generert en liste over mulige rotårsaker og målet i denne fasen er å identifisere de faktiske årsakene.

Verktøyene vi anbefaler til denne fasen er:

Årsak-virkning diagram

Som årsak-virkning anbefaler vi å benytte fiskebeindiagram. Ved å bruke fiskebeindiagram får en en visuell fremstilling av rotårsaken til problemet.

Steg 1: Definer tydelig hva problemstilingen er.

Steg 2: Bruke Draw.io eller et annet tegneprogram til tegne fiskebeindiagramet. Kan også bruke penn og papir.

Steg 3: Identifiser hovedkategoriene for årsakene og tegn de opp som greiner.

Steg 4: Idémyldre alle årsaker som kan knyttes til hovedkategoriene.

Steg 5: Analyser årsakene for å identifisere det som mest sannsynlig er rotårsaken

5 Whys

Hvis det er mistanke om høyere nivå av årsaker bak de identifiserte årsakene kan 5 Whys gi en bekreftelse på om årsakene som er identifisert er faktisk rotårsaken og ikke lav-nivå årsaker. Det kan kreve flere iterasjoner for å finne rotårsaken(e).

Steg 1: Identifiser årsakene du ønsker å undersøke

Steg 2: Spør hvorfor til hver årsak, og spør igjen for hver nye årsak som du kommer med.

Steg 3: Hvis det ikke er noen annen forklaring på årsaken enn Gud, da har du funnet rotårsaken.

Det kan ta både mindre eller mer enn fem “hvorfor” for å komme til rotårsaken, men det er en tommelfingerregel å utføre fem iterasjoner.

Feiltreanalyse

Kan brukes etter 5 Whys for å få en visuell presentasjon på hvordan de forskjellige rotårsakene man kom frem til i 5 Whys henger sammen.

10.2.7 Rotårsakseliminering

Denne fasen innebærer å komme med mulige løsninger til problemet for å eliminere rotårsaken. Boken til Fagerhaug og Andersen [1] beskriver to mulige tilnærminger til denne fasen. En tilnærming for å stimulere kreativitet når man leter etter løsninger, som benytter verktøyet seks tenkehatter. Den andre for å konstruere og utvikle løsninger, som benytter TRIZ eller SIT. Vi vil i denne fasen primært anbefale å bruke de seks tenkehatter med de modifikasjonene vi har gjort istedenfor å bruke SIT.

Verktøyene vi anbefaler til denne fasen er:

De seks tenkehatter

Seks tenkehatter fungerer godt for å idéemyldre løsninger når all dataen er klar og kreative løsninger trengs. Seks tenkehatter er også den måten vi tror passer best i infromasjonssikkerhetssammenheng.

Hvit hatt skal være kald, nøytral og objektiv, personen skal fokusere på fakta.

Rød hatt skal representere sinne, og skal bare fokusere på mageføelelsen og egne følelser.

Svart hatt skal være pessimistisk og negativ, og fokusere på hvorfor idéen er dårlig.

Gul hatt er optimistisk og positiv, og skal fokusere på hvorfor idéen er bra og vil fungere.

Grønn hatt representerer gresset, fruktbarhet og vekst, og skal fokusere på å vøre kreativ og komme på nye idéer.

Blå hatt er koblet til himmelen, og skal fokusere på å se tingene fra et høyere perspektiv.

Steg 1: Tildel hatter til diskusjonsgruppen.

Steg 2: Start diskusjonen ved at hvit hatt presenterer fakta om problemet som skal løses

Steg 3: Grønn hatt presenterer idéer på hvordan problemet kan løses

Steg 4: Diskuter de mulige løsningene, der gul hatt fokuserer på fordeler og svart på ulemper (alle kan delta i tillegg)

Steg 5: Rød hatt skal lokke frem gruppens mageføelelse på løsningene

Steg 6: Blå hatt oppsummerer diskusjonen og stopper møtet

SIT

Vi prøvde SIT i hver av casene våres for å se hvordan det fungerte. Vi kom fram til at SIT er et tungvint verktøy å starte, der mange av SIT-prinsippene ikke godt lar seg overføre til informasjonssikkerhet. Resten av stegene går bra og gir gode resultater i form av forslag på en tiltaksplan.

Steg 1: Ideelt sett bør man bruk et team som består av personer som innehaver all mulig informasjon om problemet. Er mulig uten, men blir langt vanskeligere å gjøre.

Steg 2: List alle komponenten og sørg for å ta med de som virker irrelevant.

Steg 3: Bruk de fem SIT-prinsippene til å finne på løsninger:

Attributtavhengighet vurderer å endre en nøkkelvariabel i et produkt for å skape forbedring.

Komponentkontroll ser på hvordan et produkt er knyttet til omgivelsene.

Erstatning handler om å erstatte en del av et produkt med noe annet fra produktets omgivelser.

Forkastning vurderer å forbedre problemet ved å fjerne en komponent.

Oppdeling har som mål å splitte et produkts attributter i to, som for eksempel splittelsen av sjampo fra balsam.

Steg 4: Velg de idéer som er best egnet for videre utdyping

Steg 5: Forsett å utdype idéene og kom opp med en eller flere løsninger for å gå videre til en tiltaksplan.

10.2.8 Løsningsimplementering

I den siste fasen er målet å implementere løsningene som ble funnet i foregående fase. Implementeringen inkluderer blant annet organisering, utvikling av en implementeringsplan, skape et konsensus om de nødvendige endringene og selvfølgelig implementeringen. Implementeringen av løsningen kan sies å være en suksess når symptomene forsvinner.

Verktøyet vi anbefaler til denne fasen er:

Trediagram

Trediagram fungerer veldig bra for å lage en plan over hva som må gjøres for at tiltaket skal bli implementert.

Steg 1: Lag en liste over gjøremål for å implementere løsningen(e)

Steg 2: Disse skal grupperes og settes opp i en trestruktur, i rekkefølgen som skal til for å få løsningen implementert. Aktivitetene skal plasseres i

I dette steget er det ikke nødvendig å bruke noe verktøy, men det kan være lurt å benytte trediagram for å få en plan over løsningimplementering.

11 Konklusjon

Rotårsaksanalyse er ikke en standardisert metodikk. Det finnes mye som blir kalt rotårsaksanalyse, men dette prosjektet tok utgangspunkt i metodikken til Fagerhaug og Andersen [1]. Hovedformålet med prosjektet var å undersøke om rotårsaksanalysemetodikk har bruksområder innen informasjonssikkerhet. Tilnærmingen var gjennom tre caser der målet var å finne rotårsaken og gi forslag til tiltak som kunne eliminere disse. Ut fra disse kriteriene ble det definert noen forskningsspørsmål. Tre av de var å finne rotårsaken til: ulovlig fildeling ved universitetsnettet, kompromitterte kontoer ved NTNU og misbruk av NTNU sine ressurser til utvinning av kryptovaluta. De siste forskningsspørsmålene gikk på å vurdere hvor godt rotårsaksanalyse fungerer innen informasjonssikkerhet, om det er lønnsomt å bruke det og hvilke verktøy som fungerer best innen informasjonssikkerhet.

Rotårsaken til ulovlig fildeling viste seg i hovedsak å være tilgjengeligheten, eller mangelen på den. En mindre årsak var at de følte ikke tjenestene var verdt det de måtte betale. En siste årsak ble funnet, nemlig at håndhevingen og kommuniseringen av lovene knyttet til ulovlig fildeling er utilstrekkelig og blir ikke prioritert. Tiltak vi har foreslått for å løse dette problemet er å tilby produkter fra selskaper som sender mest notifikasjoner om brudd på opphavsrett, å ha et kurs for studenter i bruk av universitetets nettverk, at Sit regelrett bytter ISP slik at problemet blir overført til andre og tilslutt at alt materiale blir tilgengelig på ett sted. Det siste tiltaket er urealistisk, men vil fjerne rotårsaken helt.

Når det kommer til kompromitterte kontoer konkluderer vi med at både gjenbruk av kredentialier og phishing er de største rotårsakene. I tillegg resulterte analysen også i at folk som har blitt kompromittert kjenner svært dårlig til styrende dokumenter på IT, informasjonssikkerhet og behandling av autentiseringsdata. Vi kom også frem til at det var utilstrekkelig tilgangskontroll på brukerkontoene da vi mener brukernavn og passord ikke er nok. For å løse dette anbefaler vi en rekke tiltak, som inkluderer: en bevisstgjørelseskampanje for god e-postskikk og behandling av autentiseringsdata, krav om strengere passordkontroll, implementere 2-faktor autentisering, klarere enheter for en viss periode gjennom 2-faktor autentisering og informering om innlogginger fra andre maskiner, utbedre IT-reglementet til å inkludere retningslinjer og krav, og til slutt å anbefale eller pålegge brukere å benytte seg av passordmanager. Av disse anbefaler vi spesielt å klarere enheter med 2-faktor autentisering i en viss periode av gangen, og i tillegg gi informasjon når det logges på fra en ny maskin.

På caset om misbruk av ressurser til kryptoutvinning kom vi frem til at rotårsaken av en blanding av uklarheter i IT-reglementet angående kryptoutvinning og at Seksjon for Digital Sikkerhet ikke har ressurser til å prioritere problemet. For å løse problemet anbefaler vi å gjennomføre en informasjonskampanje om kommersielt misbruk av NTNU sin infrastruktur, gjøre IT-reglementet klarere på misbruk av ressursene spesifikt når det kommer til kryptoutvinning, DNS blokkering av kryptoforespørsler og tilsutt øke antall

personell i seksjonen, enten i form av faste ansatte eller flere bacheloroppgaver.

Basert på erfaring fra utføringen av casestudiene kan vi konkludere med at rotårsaksanalyse fungerer godt innen informasjonssikkerhet. Dette kommer selvfølgelig helt an på hvor god datainnsamlingen er. Det kommer også an på hva slags case det benyttes på, da noen har en rotårsak som ikke kan fjernes. Rotårsaksanalyse gir også mulighet for forskjellige resultater da rotårsaken ofte ikke er den du ser med første øyekast. For å konkludere endelig med hvor godt det fungerer må tiltakene innføres. Deretter kan man se om de fjerner problemet eller ikke.

Rotårsaksanalyse er en strukturert problemløsningsmetode som egner seg godt ved lengre tidsbruk, men også helt greit over kortere tid. Det er spesielt viktig å ikke velge et for komplisert case hvis det er liten tid, da rotårsaksanalysen kan fort bli oppstykket og uferdig. Den største styrken ved rotårsaksanalyse er evnen den gir til å sette seg dypt inn i en problemstilling. Dette er nyttig uansett om det er mulig å fjerne rotårsaken eller ikke. I visse situasjoner kan det være mer fordelaktig å utføre en risiko- og sårbarhetsanalyse, men da kan du miste den dype forståelsen av bakgrunnen til problemet. Tidsbruken gjenspeilet stort sett resultatene vi fikk. Inkludert har vi også en veiledning som skal hjelpe med å veilede personer som ønsker å utføre rotårsaksanalyser på caser som omhandler informasjonssikkerhet. Dette dokumentet beskriver hvilke verktøy en bør bruke i ulike sammenhenger. Veiledningen finnes i kapittel 10.

11.1 Videre arbeid

Vi anbefaler at videre arbeid blir å gjennomgå tiltaksforslagene våre, og se om noen av disse er fornuftige å implementere, samt om de er verdt kostnadene. Ulovlig fildeling på universitetnettet er et veldig vanskelig problem å fjerne rotårsaken til, siden tilgjengelighet er den store drivkraften bak nedlasting. Det kan også være nyttig å undersøke hvilke opphavsrettshavere som sender notifikasjoner, for å se om universitetet kan tilby tjenester hvis de fleste kommer fra ett sted. Videre arbeid kan også inkludere en risikoanalyse for å underbygge problemstillingen knyttet til ulovlig fildeling på universitetsnettet.

Siden vi bare tok et sample fra de som tidligere hadde blitt kompromittert kan det være interessant å undersøke hele NTNU når det kommer til passordvaner, e-post, kjennskap til retningslinjer osv. Deretter kan resultatene sammenlignes og se om det er noen forskjeller som bør tas i betraktning. Annet videre arbeid kan være å undersøke keylogging som en mulig årsak til kompromitterte kontoer. Vi gikk ikke så mye inn på det i denne rapporten, men det kan være interessant å se på i forlengelse av ondsinnet programvare.

Siden datagrunnlaget vårt var noe snevert på case 3 kan det være interessant å hente inn mer data, for å se om det er andre underliggende rotårsaker vi ikke fant. Retningslinjer for bruk utvinning av kryptovaluta burde i teorien få alle ansatte eller studenter til å slutte å utvinne. Men de er mennesker så det kan være greit å se etter flere tekniske løsninger som hinder uautorisert utvinning av kryptovaluta.

Siden estimatene på nytten i kostnad-nytte-analysen var vage, kan videre arbeid være å utføre en ny kostnad-nytte-analyse basert på mer konkrete verdier, etter tiltakene er implementert.

videre arbeid på veiledninger Veilederen inneholder kun fremgangsmåte til verktøy vi har gjennomgått. Derfor vil videre arbeid innen veilederen være å utføre nye rotårsaksanalyser som tar for seg nye verktøy og se hvordan de fungerer innen informasjonssikkerhet. Hvis de fungerer godt, må de innarbeides inn i veilederen med en stegvis forklaringsmetode av verktøyet.

Bibliografi

[1] Andersen, B. & Fagerhaug, T. 2006. *Root Cause Analysis: Simplified Tools and Techniques. 2nd edition*. ASQ Quality Press.

[2] Wikipedia. 2016. Statistisk signifikans. [På internett; besøkt 09-mai-2018]. URL: https://no.wikipedia.org/w/index.php?title=Statistisk_signifikans&oldid=16295760.

[3] Wikipedia. 2016. Konfidensintervall. [På internett; besøkt 09-mai-2018]. URL: https://no.wikipedia.org/w/index.php?title=Konfidensintervall&oldid=16137183.

[4] Hellesen, N., Torres, H., & Wangen, G. 2018. Empirical case studies of the root-cause analysis method in information security. *International Journal On Advances in Security*, 11(1&2).

[5] Krebs, B. 2017. The market for stolen account credentials. URL: https://krebsonsecurity.com/2017/12/the-market-for-stolen-account-credentials/.

[6] 11. mai 2018. List of cryptocurrencies. URL: https://web.archive.org/web/20180513093427/https://en.wikipedia.org/wiki/List_of_cryptocurrencies.

[7] NTNU. 2005. NTNUs IT-reglement. URL: https://bas.ntnu.no/docs/ITreglement.pdf.

[8] Torres, H. M. N., Hellesen, N., & Brækken, E. L. *Bruk av rotårsaksanalyse i informasjonssikkerhet*. Gjøvik: NTNU i Gjøvik, 2016.

[9] Hellesen, N., Torres, H., Brækken, E., & Wangen, G. 2017. An empirical study of root-cause analysis in information security management.

[10] Scheid, J. Besøkt: 30. April 2018. How has the root cause analysis evolved since inception? URL: https://web.archive.org/web/20180430113417/https://www.brighthubpm.com/risk-management/123244-how-has-the-root-cause-analysis-evolved-since-inception/.

[11] Surveymonkey. Sitert 30. Mars 2018. Kvantitative vs. kvalitative undersøkelser. URL: https://web.archive.org/web/20180424213158/https://no.surveymonkey.com/mp/quantitative-vs-qualitative-research/.

[12] Wikipedia. 2015. Prøvetaking. [På internett; besøkt 10-mai-2018]. URL: https://no.wikipedia.org/w/index.php?title=Pr%C3%B8vetaking&oldid=15168038.

[13] Wikipedia. Besøkt: 24. April 2018. Variansanalyse. URL: https://no.wikipedia.org/w/index.php?title=Variansanalyse&oldid=16370460.

[14] Lærd statistics. Besøkt: 08. Mai 2018. Independent t-test using spss statistics. URL: https://statistics.laerd.com/spss-tutorials/independent-t-test-using-spss-statistics.php.

[15] Wikipedia contributors. 2018. Fault tree analysis — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Fault_tree_analysis&oldid=840272418. [På internett; besøkt 10-mai-2018].

[16] Draw.io. URL: https://draw.io.

[17] Østby, E. B., Skari, B. H., & Berglind, C. *Konsekvenser av sikkerhetshendelser og mørketall på NTNU*. Gjøvik: NTNU i Gjøvik, 2018.

[18] NTNU. Besøkt: 30. April 2018. Fakta om ntnu. URL: https://web.archive.org/web/20180430113103/https://www.ntnu.no/tall-og-fakta.

[19] SurveySystem. Brukt: 04. Mai 2018. Sample size calculator. URL: https://www.surveysystem.com/sscalc.htm.

[20] NTNU. 2010. Prinsipper for informasjonssikkerhet ved ntnu.

[21] NTNU. 2008. Retningslinjer for behandling av brukernavn, passord og andre autentiseringsdata.

[22] Williams, E. & Ashenden, D. Besøkt: 05. Mai 2018. Phishing scams are becoming ever more sophisticated – and firms are struggling to keep up. URL: https://web.archive.org/web/20180505113540/https://theconversation.com/phishing-scams-are-becoming-ever-more-sophisticated-and-firms-are-struggling-to-keep-up-

[23] Sitert 15. Mai 2018. It-sikkerhet. URL: https://innsida.ntnu.no/wiki/-/wiki/Norsk/IT-sikkerhet.

[24] 2017. Proliferation of mining malware signals a shift in cybercriminal operations. URL: https://go.recordedfuture.com/hubfs/reports/cta-2017-1011.pdf.

[25] IFPI. Sitert 13. Mai 2018. Norske totalmarkedet - 2017. URL: http://www.ifpi.no/statistikk/162-norske-totalmarkedet-2017.

[26] Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., Markov, Y., Comanescu, O., Eranti, V., Moscicki, A., Margolis, D., Paxson, V., & Bursztein, E., eds. *Data breaches, phishing, or malware? Understanding the risks of stolen credentials*, 2017.

[27] Schneider, B. Sitert 11. Mai 2018. Security awareness training. URL: https://www.schneier.com/blog/archives/2013/03/security_awaren_1.html.

[28] Raphael, J. Sitert 12. Mai 2018. What is two-factor authentication (2fa)? how to enable it and why you should. URL: https://www.csoonline.com/article/3239144/password-security/what-is-two-factor-authentication-2fa-how-to-enable-it-and-why-you-should.html.

[29] Nick. Sitert 12. Mai 2018. Add or remove trusted computers. URL: https://support.google.com/accounts/answer/2544838?hl=en.

[30] Spring, T. 2018 [Sitert 12. mai 2018]. Massive smominru cryptocurrency botnet rakes in millions. URL: https://web.archive.org/web/20180512145343/https://threatpost.com/massive-smominru-cryptocurrency-botnet-rakes-in-millions/129726/.

A Spørreundersøkelse case 1

Spørreundersøkelse

Vi er fire bachelorstudenter som har fått i oppgave å finne rotårsaken til at personer, som bor i studenthyblene til SiT Bolig, laster ned og deler opphavsrettsbeskyttet materiale gjennom torrenting og fildeling. Denne oppgaven er gitt av NTNU Seksjon for Digital Sikkerhet for å kartlegge omfanget av ulovlig fildeling. Spørreundersøkelsen er anonym, og info som blir hentet inn her skal ikke brukes for å identifisere enkeltpersoner.

Når det snakkes om nedlastning og fildeling mener vi nedlastning ved bruk av Torrents.

Spørreundersøkelsen vil ta ca 3-5 minutter.

Denne undersøkelsen skal undersøke omfanget til fildeling på skolenettet ved de forskjellige studentbyene ved NTNU i Gjøvik. Den skal også se på årsaker til nedlasting og hvordan dette kan stoppes.

*Må fylles ut

1. **Hvilket fakultet tilhører du?** *
   Markér bare én oval.
   - ◯ Fakultet for arkitektur og design
   - ◯ Fakultet for informasjonsteknologi og elektroteknikk
   - ◯ Fakultet for ingeniørvitenskap
   - ◯ Fakultet for medisin og helsevitenskap
   - ◯ Fakultet for økonomi
   - ◯ Andre: _____

2. **Alder** *
   Markér bare én oval.
   - ◯ Under 20
   - ◯ 20-25
   - ◯ 26-30
   - ◯ 31-35
   - ◯ Over 35

3. **Kjønn** *
   Markér bare én oval.
   - ◯ Mann
   - ◯ Kvinne

4. **Hvilken studentby bor du i?** *
   Markér bare én oval.
   - ◯ Sørbyen
   - ◯ Nordbyen
   - ◯ Kallerud
   - ◯ Sentrum
   - ◯ Jeg bor ikke i noen studentby *Stopp å fylle ut dette skjemaet.*

5. **Har du lastet ned opphavsrettsbeskyttet materiale i hybelen?** *
Markér bare én oval.

- ◯ Ja *Hopp til spørsmål 6.*
- ◯ Nei *Hopp til spørsmål 16.*

6. **Hva slags opphavsrettsbeskyttet materiale har du lastet ned etter du flyttet inn i SIT bolig? (du kan velge flere)**
Merk av for alt som passer

- ☐ Filmer og serier som kom ut i år eller i fjor
- ☐ Eldre filmer og serier
- ☐ Skolebøker
- ☐ Programvare til skolebruk
- ☐ Programvare til bruk utenom skole
- ☐ Bøker og tegneserier til bruk utenom skole
- ☐ Spill
- ☐ Musikk
- ☐ Andre: _____

7. **Hvor mye opphavsrettsbeskyttet materiale har du lastet ned den siste måneden? (antall torrents)** *
Markér bare én oval.

- ◯ Ingenting
- ◯ 1-3
- ◯ 4-6
- ◯ 7-9
- ◯ 10+

Hvor godt stemmer disse påstandene:

Vi kommer med 6 påstander, hvor godt stemmer de med din situasjon

8. **Jeg laster ned fordi jeg føler jeg ikke har råd til alternativer.**
Markér bare én oval.

	1	2	3	4	5	
Liten grad	◯	◯	◯	◯	◯	Stor grad

9. **Jeg laster ned fordi det jeg vil ha ikke er tilgjengelig på tjenester i Norge.**
Markér bare én oval.

	1	2	3	4	5	
Liten grad	◯	◯	◯	◯	◯	Stor grad

10. **Når jeg laster ned på skolenettet føler jeg meg mer anonym enn ellers.**
Markér bare én oval.

	1	2	3	4	5	
Liten grad	◯	◯	◯	◯	◯	Stor grad

11. **Jeg laster ned fordi det er lav sannsynlighet for å bli tatt.**
Markér bare én oval.

	1	2	3	4	5	
Liten grad	◯	◯	◯	◯	◯	Stor grad

12. **Jeg laster ned fordi jeg synes kvaliteten på strømmetjenester er for dårlig.**
Markér bare én oval.

	1	2	3	4	5	
Liten grad	◯	◯	◯	◯	◯	Stor grad

13. **Jeg laster ned fordi jeg ikke ønsker å støtte selskapet som eier opphavsretten.**
Markér bare én oval.

	1	2	3	4	5	
Liten grad	◯	◯	◯	◯	◯	Stor grad

14. **Jeg laster ned av en annen grunn.**

_____

15. **Fortsetter du å dele filer over lengre tid etter nedlastingen er ferdig?**
Markér bare én oval.

- ◯ Ja
- ◯ Nei
- ◯ Over en kortere periode
- ◯ Andre: _____

16. **Har du tilgang til betalte videostrømmingstjenester? (Eksempelvis Netflix, HBO Nordic, Viaplay osv..)** *
Markér bare én oval.

- ◯ Ja *Hopp til spørsmål 17.*
- ◯ Nei *Hopp til spørsmål 18.*

17. **Hvor mange slike tjenester har du tilgang til?**
Markér bare én oval.

- 1 *Hopp til spørsmål 18.*
- 2 *Hopp til spørsmål 18.*
- 3 *Hopp til spørsmål 18.*
- 4+ *Hopp til spørsmål 18.*

18. **Har du tilgang til betalte musikkstrømmetjenester? (Eksempelvis Spotify, Tidal, osv..)**
Markér bare én oval.

- Ja
- Nei

19. **Kjenner du til konsekvenser ved brudd på opphavsrett**
Markér bare én oval.

- Ja
- Nei

20. **Hvor kjent er du med IT-reglementet til NTNU?**
Markér bare én oval.

	1	2	3	4	5	
Liten grad						Stor grad

21. **Hva skal til for at du stopper med nedlastning?**

B Spørreundersøkelse case 2 (norsk og engelsk)

NTNU
Kunnskap for en bedre verden

Spørreundersøkelse angående årsaken til stjålne brukerkontoer ved NTNU

Page 1

Hjelp oss i å hjelpe andre. Å få sin konto kompromittert er aldri noe en ønsker, og sammen med flere hundre andre har du i denne sammenhengen vært spesielt uheldig. Seksjon for Digital Sikkerhet jobber med å finne årsaken til kompromitterte kontoer ved NTNU. Med en kompromittert konto mener vi når noen har stjålet brukernavn og passord. Siden du var så uheldig sitter du nå på verdifull kunnskap og er i en unik posisjon til å hjelpe andre. Vi ønsker derfor din hjelp til å finne årsaken til at dette skjer, og hindre at flere blir rammet på samme måte. All data vi samler inn vil bli håndtert anonymt.

Spørreundersøkelsen består av 23 spørsmål, og det tar omtrent 4-5 minutter å svare.

NTNU
Kunnskap for en bedre verden

Spørreundersøkelse angående årsaken til stjålne brukerkontoer ved NTNU

Page 2

Demografi

1. Din alder?*
   - Under 20
   - 20-29
   - 30-39
   - 40-49
   - 50-59
   - 60-69
   - 70 eller over

2. Ditt kjønn?*
   - Mann
   - Kvinne
   - Ønsker ikke oppgi

3. Hva er din primærrolle ved NTNU?*
   - Ansatt
   - Student

4. I hvilken by jobber/studerer du primært?*
   - Gjøvik
   - Trondheim
   - Ålesund

5. Hvor mange år har du jobbet/studert ved NTNU eller de tidligere høgskolene? (HiG, HiST, HiÅ)*
   - Under 2
   - 2-4
   - 5-9
   - 10-15
   - Over 15

NTNU
Kunnskap for en bedre verden

Spørreundersøkelse angående årsaken til stjålne brukerkontoer ved NTNU

Page 3

Generelle spørsmål

6. Når fant du ut at kontoen var blitt kompromittert?*
   - ○ Når Seksjon for Digital Sikkerhet kontaktet deg
   - ○ Før Seksjon for Digital Sikkerhet kontaktet deg
   - ○ Vet ikke

7. Har du noen formening om hvor lang tid kontoen var kompromittert før Seksjon for Digital Sikkerhet kontaktet deg? (la det være blankt hvis du ikke vet)
   - ○ Mindre enn tre måneder
   - ○ Tre til seks måneder
   - ○ Seks til tolv måneder
   - ○ Ett til to år
   - ○ Mer enn to år

8. Har du noen formening om hvordan kontoen din ble kompromittert?*

9. Bruker du din NTNU e-post til å registrere deg på ulike tjenester på nett i forbindelse med jobben/studiet? (f.eks. Dropbox, Trello, Slack, osv.)*
   - ○ Ja
   - ○ Nei
   - ○ Vet ikke

10. Bruker du din NTNU e-post til å registrere deg på tjenester på nett til privat bruk? (f.eks. Netflix, Facebook, Adobe, nettavis, Reddit, osv.)*
    - ○ Ja
    - ○ Nei
    - ○ Vet ikke

11. På en skala fra 1-6, der 1 er lite bevisst og 6 er svært bevisst, hvor bevisst er du på sikkerhet når du...*

	1	2	3	4	5	6
besøker nettsider?	○	○	○	○	○	○
lager passord?	○	○	○	○	○	○
sjekker e-post?	○	○	○	○	○	○

12. Har du i din tid hos NTNU lagt merke til phishing-forsøk mot deg på din NTNU e-post? (phishing er når noen prøver å lure deg til å oppgi personlig informasjon som for eksempel brukernavn og passord)*
    - ○ Ja, en gang
    - ○ Ja, flere ganger

- Nei
- Vet ikke

13. Har du blitt lurt av phishing på din NTNU e-post?*
    - Ja
    - Nei
    - Vet ikke

14. Har du i løpet av din tid ved NTNU eller de andre høgskolene, oppdaget virus eller annen skadevare på maskinen din?*
    - Ja
    - Nei
    - Vet ikke

NTNU
Kunnskap for en bedre verden

Spørreundersøkelse angående årsaken til stjålne brukerkontoer ved NTNU

Page 4

Spørsmål om passordbruk

15. Bruker du ditt NTNU passord på flere tjenester?*
    - Ja
    - Nei

16. Brukte du regler til å generere ditt NTNU passord? (f.eks. "lisa-gikk-til-facebook", "lisa-gikk-til-NTNU", "lisa-gikk-til-linkedin" eller en kombinasjon av personlige detaljer)*
    - Ja
    - Nei

17. Er ditt NTNU passord tilfeldig sammensatt av bokstaver, tall og/eller spesialtegn?*
    - Ja
    - Nei

18. Hvor mange tegn består ditt NTNU passord av?*
    - Under 8
    - 8-11
    - 12-15
    - 16-20
    - Over 20

19. Har du i løpet av din tid ved NTNU delt NTNU passordet ditt med andre?*
    - Ja
    - Nei

20. Omtrent hvor ofte bytter du ditt NTNU passord?*
    - Oftere enn hver sjette måned
    - Hver sjette måned
    - Hvert år
    - Hvert andre år
    - Sjeldnere enn hvert andre år

21. Bruker du en passordmanager? (f.eks. LastPass, Dashlane, osv...)*
    - Ja
    - Nei
    - Nei, men har brukt det før
    - Nei, men har vurdert det
    - Vet ikke hva en passordmanager er

NTNU
Kunnskap for en bedre verden

Spørreundersøkelse angående årsaken til stjålne brukerkontoer ved NTNU

Page 5

Spørsmål om policy og retningslinjer

22. På en skala fra 1 til 6, der 1 er lite kjent og 6 er godt kjent, hvor godt kjent er du med...*

	1	2	3	4	5	6
NTNU sine retningslinjer for behandling av brukernavn, passord og andre autentiseringsdata?	○	○	○	○	○	○
IT reglementet til NTNU?	○	○	○	○	○	○
NTNU sine prinsipper for informasjonssikkerhet?	○	○	○	○	○	○

23. Har du fått opplæring i passordsikkerhet fra NTNU?*

- ○ Ja
- ○ Nei
- ○ Vet ikke

NTNU
Kunnskap for en bedre verden

Survey regarding the cause of stolen user accounts at NTNU

Page 1

We would appreciate it if you could help us in helping others. The Digital Security Section is working to find the cause of compromised accounts at NTNU. A compromised account means that someone has stolen a username and password. No one wishes for their account to be compromised, and you have along with hundreds of others, been particularly unfortunate. There is, however, a silver lining, you are now in the possession of valuable knowledge and in a unique position to help others. We therefore hope that you may help us find the cause of this, and thus prevent more people from experiencing the same as you have. All data we collect will be handled anonymously.

The survey consists of 23 questions, and it will take about 4-5 minutes to complete.

(PS: The next- and back buttons at the bottom of the page are unfortunately in Norwegian. "Neste" means "next", and "tilbake" means "back". Sorry for the inconvenience.)

NTNU
Kunnskap for en bedre verden

Survey regarding the cause of stolen user accounts at NTNU

Page 2

Demographics

1. Your age?*
   - Younger than 20
   - 20-29
   - 30-39
   - 40-49
   - 50-59
   - 60-69
   - 70 or older

2. Your gender?*
   - Male
   - Female
   - Prefer not to answer

3. What is your primary role at NTNU?*
   - Employee
   - Student

4. In which city do you primarily work/study?*
   - Gjøvik
   - Trondheim
   - Ålesund

5. How many years have you been an employee/student at NTNU? (including former university colleges)*
   - Less than 2
   - 2-4
   - 5-9
   - 10-15
   - More than 15

NTNU
Kunnskap for en bedre verden

Survey regarding the cause of stolen user accounts at NTNU

Page 3

General questions

6. When did you realise that your NTNU account had been compromised?*
   - ○ When the Digital Security Section contacted you
   - ○ Before the Digital Security Section contacted you
   - ○ I don't know

7. Do you have an idea about how long your NTNU account had been compromised before the Digital Security Section contacted you? (leave it blank if you don't know)
   - ○ Less than three months
   - ○ Three to six months
   - ○ Six to twelve months
   - ○ One to two years
   - ○ More than two years

8. Do you have an idea about how your NTNU account was compromised?*

9. Do you use your NTNU e-mail to sign up to various work related online services? (e.g. Dropbox, Trello, Slack, etc.)*
   - ○ Yes
   - ○ No
   - ○ I don't know

10. Do you use your NTNU e-mail to sign up for online services for private use? (e.g. Netflix, Facebook, Adobe, Reddit, online newspapers, etc.)*
    - ○ Yes
    - ○ No
    - ○ I don't know

11. On a scale from 1 to 6, where 1 is not aware and 6 is very aware, how aware are you regarding security when...*

	1	2	3	4	5	6
browsing websites?	○	○	○	○	○	○
creating passwords?	○	○	○	○	○	○
checking your e-mail?	○	○	○	○	○	○

12. Have you, while working/studying at NTNU or the former university colleges, noticed phishing attempts against you on your NTNU e-mail?*
    - ○ Yes, once
    - ○ Yes, multiple times
    - ○ No
    - ○ I don't know

13. Do you think you have been fooled by phishing on your NTNU e-mail?*
    - Yes
    - No
    - I don't know

14. Have you, while working/studying at NTNU or the former university colleges, noticed any viruses or malware on your computer?*
    - Yes
    - No
    - I don't know

NTNU
Kunnskap for en bedre verden

Survey regarding the cause of stolen user accounts at NTNU

Page 4

Questions about password use

15. Do you use your NTNU password on multiple services?*
    - Yes
    - No

16. Do you make password phrases when generating new NTNU passwords? (e.g. "Old-macdonald-had-a-farm-at-NTNU'',"Old-macdonald-had-a-farm-at-facebook" or a combination of personal details)*
    - Yes
    - No

17. Is your NTNU password randomly comprised of letters, numbers and/or special characters?*
    - Yes
    - No

18. How many characters does your NTNU password consist of?*
    - Less than 8
    - 8-11
    - 12-15
    - 16-20
    - More than 20

19. Have you shared your NTNU credentials with others during your time at NTNU or the former university colleges?*
    - Yes
    - No

20. About how often do you change your NTNU password?*
    - Less than every sixth months
    - Every sixth months
    - Each year
    - Every two years
    - More than every two years

21. Do you use a password manager?*
    - Yes
    - No
    - No, but I have used one before
    - No, but I have considered it
    - I don't know what a password manager is

NTNU
Kunnskap for en bedre verden

Survey regarding the cause of stolen user accounts at NTNU

Page 5

Questions about policy and guidelines

22. On a scale from 1-6, where 1 is not familiar and 6 is very familiar, how familiar are you with...*

	1	2	3	4	5	6
NTNU's guidelines for handling usernames, passwords, and other authentication data?	○	○	○	○	○	○
NTNU's IT policy?	○	○	○	○	○	○
NTNU's guidelines for information security?	○	○	○	○	○	○

23. Have you received training in password security from NTNU?*

- ○ Yes
- ○ No
- ○ I don't know

C Spørreundersøkelse case 2 resultater (norsk og engelsk)

Hide/Show Print Tools

Spørreundersøkelse angående årsaken til stjålne brukerkontoer ved NTNU

Respondents: 92 displayed, 92 total **Status:** Closed

Launched Date: 22.04.2018 **Closed Date:** 28.04.2018

1. Din alder?

	Response Total	Response Percent	Points	Avg
Under 20	2	2%	n/a	n/a
20-29	4	5%	n/a	n/a
30-39	14	18%	n/a	n/a
40-49	29	36%	n/a	n/a
50-59	12	15%	n/a	n/a
60-69	11	14%	n/a	n/a
70 eller over	8	10%	n/a	n/a
Total Respondents	80	100%		
(skipped this question)	12			

2. Ditt kjønn?

	Response Total	Response Percent	Points	Avg
Mann	33	41%	n/a	n/a
Kvinne	47	59%	n/a	n/a
Ønsker ikke oppgi	0	0%	n/a	n/a
Total Respondents	80	100%		
(skipped this question)	12			

3. Hva er din primærrolle ved NTNU?

	Response Total	Response Percent	Points	Avg
Ansatt	71	89%	n/a	n/a
Student	9	11%	n/a	n/a
Total Respondents	80	100%		
(skipped this question)	12			

4. I hvilken by jobber/studerer du primært?

	Response Total	Response Percent	Points	Avg
Gjøvik	1	1%	n/a	n/a
Trondheim	77	96%	n/a	n/a
Ålesund	2	2%	n/a	n/a
Total Respondents	80	100%		
(skipped this question)	12			

5. Hvor mange år har du jobbet/studert ved NTNU eller de tidligere høgskolene? (HiG, HiST, HiÅ)

	Response Total	Response Percent	Points	Avg
Under 2	9	11%	n/a	n/a
2-4	6	8%	n/a	n/a
5-9	7	9%	n/a	n/a
10-15	16	20%	n/a	n/a
Over 15	42	52%	n/a	n/a
Total Respondents	80	100%		
(skipped this question)	12			

6. Når fant du ut at kontoen var blitt kompromittert?

	Response Total	Response Percent	Points	Avg
Når Seksjon for Digital Sikkerhet kontaktet deg	47	67%	n/a	n/a
Før Seksjon for Digital Sikkerhet kontaktet deg	14	20%	n/a	n/a
Vet ikke	9	13%	n/a	n/a
Total Respondents	70	100%		
(skipped this question)	22			

7. Har du noen formening om hvor lang tid kontoen var kompromittert før Seksjon for Digital Sikkerhet kontaktet deg? (la det være blankt hvis du ikke vet)

	Response Total	Response Percent	Points	Avg
Mindre enn tre måneder	37	86%	n/a	n/a
Tre til seks måneder	2	5%	n/a	n/a
Seks til tolv måneder	2	5%	n/a	n/a
Ett til to år	0	0%	n/a	n/a
Mer enn to år	2	5%	n/a	n/a
Total Respondents	43	100%		
(skipped this question)	49			

8. Har du noen formening om hvordan kontoen din ble kompromittert?

Total Respondents	69
(skipped this question)	23

9. Bruker du din NTNU e-post til å registrere deg på ulike tjenester på nett i forbindelse med jobben/studiet? (f.eks. Dropbox, Trello, Slack, osv.)

	Response Total	Response Percent	Points	Avg
Ja	45	65%	n/a	n/a
Nei	22	32%	n/a	n/a
Vet ikke	2	3%	n/a	n/a
Total Respondents	69	100%		
(skipped this question)	23			

10. Bruker du din NTNU e-post til å registrere deg på tjenester på nett til privat bruk? (f.eks. Netflix, Facebook, Adobe, nettavis, Reddit, osv.)

	Response Total	Response Percent	Points	Avg
Ja	35	51%	n/a	n/a
Nei	32	46%	n/a	n/a
Vet ikke	2	3%	n/a	n/a
Total Respondents	69	100%		
(skipped this question)	23			

11. På en skala fra 1-6, der 1 er lite bevisst og 6 er svært bevisst, hvor bevisst er du på sikkerhet når du...

	1	2	3	4	5	6	Response Total	Response Average
besøker nettsider?	5,88% (4)	7,35% (5)	27,94% (19)	32,35% (22)	19,12% (13)	7,35% (5)	68	3,74
lager passord?	4,35% (3)	2,9% (2)	14,49% (10)	28,99% (20)	31,88% (22)	17,39% (12)	69	4,33
sjekker e-post?	7,46% (5)	4,48% (3)	14,93% (10)	22,39% (15)	28,36% (19)	22,39% (15)	67	4,27
Total Respondents							69	
(skipped this question)							23	

12. Har du i din tid hos NTNU lagt merke til phishing-forsøk mot deg på din NTNU e-post? (phishing er når noen prøver å lure deg til å oppgi personlig informasjon som for eksempel brukernavn og passord)

	Response	Response	Points	Avg

	Total	Percent		
Ja, en gang	2	3%	n/a	n/a
Ja, flere ganger	51	74%	n/a	n/a
Nei	14	20%	n/a	n/a
Vet ikke	2	3%	n/a	n/a
Total Respondents	69	100%		
(skipped this question)	23			

13. Har du blitt lurt av phishing på din NTNU e-post?

	Response Total	Response Percent	Points	Avg
Ja	10	14%	n/a	n/a
Nei	54	78%	n/a	n/a
Vet ikke	5	7%	n/a	n/a
Total Respondents	69	100%		
(skipped this question)	23			

14. Har du i løpet av din tid ved NTNU eller de andre høgskolene, oppdaget virus eller annen skadevare på maskinen din?

	Response Total	Response Percent	Points	Avg
Ja	20	29%	n/a	n/a
Nei	42	61%	n/a	n/a
Vet ikke	7	10%	n/a	n/a
Total Respondents	69	100%		
(skipped this question)	23			

15. Bruker du ditt NTNU passord på flere tjenester?

	Response Total	Response Percent	Points	Avg
Ja	36	53%	n/a	n/a
Nei	32	47%	n/a	n/a
Total Respondents	68	100%		
(skipped this question)	24			

16. Brukte du regler til å generere ditt NTNU passord? (f.eks. “lisa-gikk-til-facebook”, “lisa-gikk-til-NTNU”, “lisa-gikk-til-linkedin” eller en kombinasjon av personlige detaljer)

	Response Total	Response Percent	Points	Avg
Ja	13	19%	n/a	n/a
Nei	55	81%	n/a	n/a
Total Respondents	68	100%		
(skipped this question)	24			

17. Er ditt NTNU passord tilfeldig sammensatt av bokstaver, tall og/eller spesialtegn?

	Response Total	Response Percent	Points	Avg
Ja	41	60%	n/a	n/a
Nei	27	40%	n/a	n/a
Total Respondents	68	100%		
(skipped this question)	24			

18. Hvor mange tegn består ditt NTNU passord av?

	Response Total	Response Percent	Points	Avg
Under 8	2	3%	n/a	n/a
8-11	61	90%	n/a	n/a
12-15	3	4%	n/a	n/a
16-20	0	0%	n/a	n/a
Over 20				

	2	3%	n/a	n/a
Total Respondents	68	100%		
(skipped this question)	24			

19. Har du i løpet av din tid ved NTNU delt NTNU passordet ditt med andre?

	Response Total	Response Percent	Points	Avg
Ja	8	12%	n/a	n/a
Nei	60	88%	n/a	n/a
Total Respondents	68	100%		
(skipped this question)	24			

20. Omtrent hvor ofte bytter du ditt NTNU passord?

	Response Total	Response Percent	Points	Avg
Oftere enn hver sjette måned	0	0%	n/a	n/a
Hver sjette måned	2	3%	n/a	n/a
Hvert år	13	19%	n/a	n/a
Hvert andre år	13	19%	n/a	n/a
Sjeldnere enn hvert andre år	40	59%	n/a	n/a
Total Respondents	68	100%		
(skipped this question)	24			

21. Bruker du en passordmanager? (f.eks. LastPass, Dashlane, osv...)

	Response Total	Response Percent	Points	Avg
Ja	3	4%	n/a	n/a
Nei	51	75%	n/a	n/a
Nei, men har brukt det før	0	0%	n/a	n/a
Nei, men har vurdert det	2	3%	n/a	n/a
Vet ikke hva en passordmanager er	12	18%	n/a	n/a
Total Respondents	68	100%		
(skipped this question)	24			

22. På en skala fra 1 til 6, der 1 er lite kjent og 6 er godt kjent, hvor godt kjent er du med...

	1	2	3	4	5	6	Response Total	Response Average
NTNU sine retningslinjer for behandling av brukernavn, passord og andre autentiseringsdata?	26,47% (18)	30,88% (21)	22,06% (15)	8,82% (6)	10,29% (7)	1,47% (1)	68	2,5
IT reglementet til NTNU?	25% (17)	30,88% (21)	20,59% (14)	13,24% (9)	8,82% (6)	1,47% (1)	68	2,54
NTNU sine prinsipper for informasjonssikkerhet?	25,37% (17)	32,84% (22)	25,37% (17)	7,46% (5)	7,46% (5)	1,49% (1)	67	2,43
Total Respondents							68	
(skipped this question)							24	

23. Har du fått opplæring i passordsikkerhet fra NTNU?

	Response Total	Response Percent	Points	Avg
Ja	5	7%	n/a	n/a
Nei	53	78%	n/a	n/a
Vet ikke	10	15%	n/a	n/a
Total Respondents	68	100%		
(skipped this question)	24			

Hide/Show Print Tools

Survey regarding the cause of stolen user accounts at NTNU

Respondents: 6 displayed, 6 total **Status:** Closed

Launched Date: 22.04.2018 **Closed Date:** 28.04.2018

1. Your age?

	Response Total	Response Percent	Points	Avg
Younger than 20	0	0%	n/a	n/a
20-29	0	0%	n/a	n/a
30-39	3	75%	n/a	n/a
40-49	1	25%	n/a	n/a
50-59	0	0%	n/a	n/a
60-69	0	0%	n/a	n/a
70 or older	0	0%	n/a	n/a
Total Respondents	4	100%		
(skipped this question)	2			

2. Your gender?

	Response Total	Response Percent	Points	Avg
Male	1	25%	n/a	n/a
Female	3	75%	n/a	n/a
Prefer not to answer	0	0%	n/a	n/a
Total Respondents	4	100%		
(skipped this question)	2			

3. What is your primary role at NTNU?

	Response Total	Response Percent	Points	Avg
Employee	3	75%	n/a	n/a
Student	1	25%	n/a	n/a
Total Respondents	4	100%		
(skipped this question)	2			

4. In which city do you primarily work/study?

	Response Total	Response Percent	Points	Avg
Gjøvik	0	0%	n/a	n/a
Trondheim	4	100%	n/a	n/a
Ålesund	0	0%	n/a	n/a
Total Respondents	4	100%		
(skipped this question)	2			

5. How many years have you been an employee/student at NTNU? (including former university colleges)

	Response Total	Response Percent	Points	Avg
Less than 2	0	0%	n/a	n/a
2-4	1	25%	n/a	n/a
5-9	3	75%	n/a	n/a
10-15	0	0%	n/a	n/a
More than 15	0	0%	n/a	n/a
Total Respondents	4	100%		

(skipped this question) 2

6. When did you realise that your NTNU account had been compromised?

	Response Total	Response Percent	Points	Avg
When the Digital Security Section contacted you	0	0%	n/a	n/a
Before the Digital Security Section contacted you	2	50%	n/a	n/a
I don't know	2	50%	n/a	n/a
Total Respondents	4	100%		

(skipped this question) 2

7. Do you have an idea about how long your NTNU account had been compromised before the Digital Security Section contacted you? (leave it blank if you don't know)

	Response Total	Response Percent	Points	Avg
Less than three months	3	100%	n/a	n/a
Three to six months	0	0%	n/a	n/a
Six to twelve months	0	0%	n/a	n/a
One to two years	0	0%	n/a	n/a
More than two years	0	0%	n/a	n/a
Total Respondents	3	100%		

(skipped this question) 3

8. Do you have an idea about how your NTNU account was compromised?

Total Respondents	4
(skipped this question)	2

9. Do you use your NTNU e-mail to sign up to various work related online services? (e.g. Dropbox, Trello, Slack, etc.)

	Response Total	Response Percent	Points	Avg
Yes	3	75%	n/a	n/a
No	1	25%	n/a	n/a
I don't know	0	0%	n/a	n/a
Total Respondents	4	100%		

(skipped this question) 2

10. Do you use your NTNU e-mail to sign up for online services for private use? (e.g. Netflix, Facebook, Adobe, Reddit, online newspapers, etc.)

	Response Total	Response Percent	Points	Avg
Yes	0	0%	n/a	n/a
No	4	100%	n/a	n/a
I don't know	0	0%	n/a	n/a
Total Respondents	4	100%		

(skipped this question) 2

11. On a scale from 1 to 6, where 1 is not aware and 6 is very aware, how aware are you regarding security when...

	1	2	3	4	5	6	Response Total	Response Average
browsing websites?	0% (0)	25% (1)	0% (0)	50% (2)	25% (1)	0% (0)	4	3,75

creating passwords?	0% (0)	0% (0)	25% (1)	25% (1)	50% (2)	0% (0)	**4** **4,25**
checking your e-mail?	0% (0)	50% (2)	0% (0)	25% (1)	25% (1)	0% (0)	**4** **3,25**

Total Respondents **4**

(skipped this question) 2

12. Have you, while working/studying at NTNU or the former university colleges, noticed phishing attempts against you on your NTNU e-mail?

	Response Total	Response Percent	Points	Avg
Yes, once	**0**	**0%**	**n/a**	**n/a**
Yes, multiple times	**2**	**50%**	**n/a**	**n/a**
No	**1**	**25%**	**n/a**	**n/a**
I don't know	**1**	**25%**	**n/a**	**n/a**
Total Respondents	**4**	**100%**		
(skipped this question)	2			

13. Do you think you have been fooled by phishing on your NTNU e-mail?

	Response Total	Response Percent	Points	Avg
Yes	**1**	**25%**	**n/a**	**n/a**
No	**3**	**75%**	**n/a**	**n/a**
I don't know	**0**	**0%**	**n/a**	**n/a**
Total Respondents	**4**	**100%**		
(skipped this question)	2			

14. Have you, while working/studying at NTNU or the former university colleges, noticed any viruses or malware on your computer?

	Response Total	Response Percent	Points	Avg
Yes	**0**	**0%**	**n/a**	**n/a**
No	**2**	**50%**	**n/a**	**n/a**
I don't know	**2**	**50%**	**n/a**	**n/a**
Total Respondents	**4**	**100%**		
(skipped this question)	2			

15. Do you use your NTNU password on multiple services?

	Response Total	Response Percent	Points	Avg
Yes	**3**	**75%**	**n/a**	**n/a**
No	**1**	**25%**	**n/a**	**n/a**
Total Respondents	**4**			
(skipped this question)	2			

16. Do you make password phrases when generating new NTNU passwords? (e.g. “Old-macdonald-had-a-farm-at-NTNU’’,”Old-macdonald-had-a-farm-at-facebook” or a combination of personal details)

	Response Total	Response Percent	Points	Avg
Yes	**0**	**0%**	**n/a**	**n/a**
No	**4**	**100%**	**n/a**	**n/a**
Total Respondents	**4**			
(skipped this question)	2			

17. Is your NTNU password randomly comprised of letters, numbers and/or special characters?

	Response Total	Response Percent	Points	Avg
Yes	**2**	**50%**	**n/a**	**n/a**
No	**2**	**50%**	**n/a**	**n/a**
Total Respondents	**4**			
(skipped this question)	2			

18. How many characters does your NTNU password consist of?

	Response Total	Response Percent	Points	Avg
Less than 8	0	0%	n/a	n/a
8-11	4	100%	n/a	n/a
12-15	0	0%	n/a	n/a
16-20	0	0%	n/a	n/a
More than 20	0	0%	n/a	n/a
Total Respondents	4	100%		
(skipped this question)	2			

19. Have you shared your NTNU credentials with others during your time at NTNU or the former university colleges?

	Response Total	Response Percent	Points	Avg
Yes	0	0%	n/a	n/a
No	4	100%	n/a	n/a
Total Respondents	4			
(skipped this question)	2			

20. About how often do you change your NTNU password?

	Response Total	Response Percent	Points	Avg
Less than every sixth months	0	0%	n/a	n/a
Every sixth months	0	0%	n/a	n/a
Each year	1	25%	n/a	n/a
Every two years	3	75%	n/a	n/a
More than every two years	0	0%	n/a	n/a
Total Respondents	4	100%		
(skipped this question)	2			

21. Do you use a password manager?

	Response Total	Response Percent	Points	Avg
Yes	1	25%	n/a	n/a
No	1	25%	n/a	n/a
No, but I have used one before	0	0%	n/a	n/a
No, but I have considered it	0	0%	n/a	n/a
I don't know what a password manager is	2	50%	n/a	n/a
Total Respondents	4	100%		
(skipped this question)	2			

22. On a scale from 1-6, where 1 is not familiar and 6 is very familiar, how familiar are you with...

	1	2	3	4	5	6	Response Total	Response Average
NTNU's guidelines for handling usernames, passwords, and other authentication data?	25% (1)	75% (3)	0% (0)	0% (0)	0% (0)	0% (0)	4	1,75
NTNU's IT policy?	25% (1)	75% (3)	0% (0)	0% (0)	0% (0)	0% (0)	4	1,75
NTNU's guidelines for information security?	25% (1)	75% (3)	0% (0)	0% (0)	0% (0)	0% (0)	4	1,75
Total Respondents							4	
(skipped this question)							2	

23. Have you received training in password security from NTNU?

	Response Total	Response Percent	Points	Avg

D Vedlegg: Plakat

Figur 70: Plakat som ble brukt i forbindelse med promotering av spørreundersøkelsen

E Vedlegg: Frekvenstabeller case 1

Kjønn				
	Frequency	Percent	Valid Percent	Cumulative Percent
Kvinne	27	27.8	27.8	27.8
Mann	70	72.2	72.2	100.0
Total	97	100.0	100.0	

Tabell 18: Frekvenstabell av kjønn

Alder				
	Frequency	Percent	Valid Percent	Cumulative Percent
Under 20	9	9.3	9.3	9.3
20-25	72	74.2	74.2	83.5
26-30	11	11.3	11.3	94.9
31-35	4	4.1	4.1	99.0
Over 35	1	1.0	1.0	100.0
Total	97	100.0	100.0	

Tabell 19: Frekvenstabell av alder

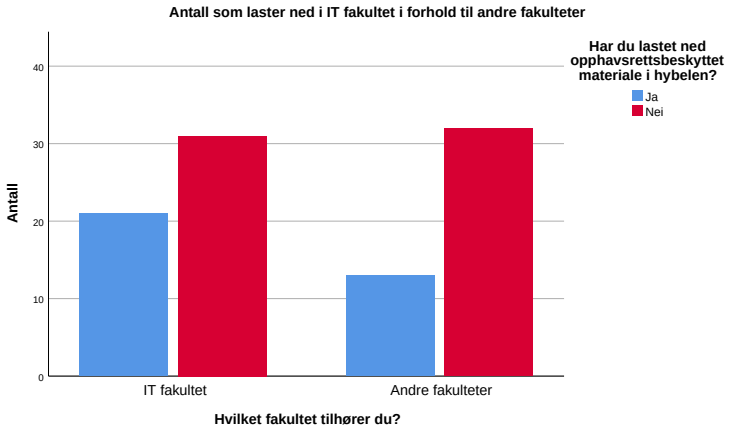
Studentby				
	Frequency	Percent	Valid Percent	Cumulative Percent
Kallerud	49	50.5	50.5	50.5
Nordbyen	13	13.4	13.4	63.9
Sentrum	11	11.3	11.3	75.3
Sørbyen	24	24.7	24.7	100.0
Total	97	100.0	100.0	

Tabell 20: Frekvenstabell av studentby

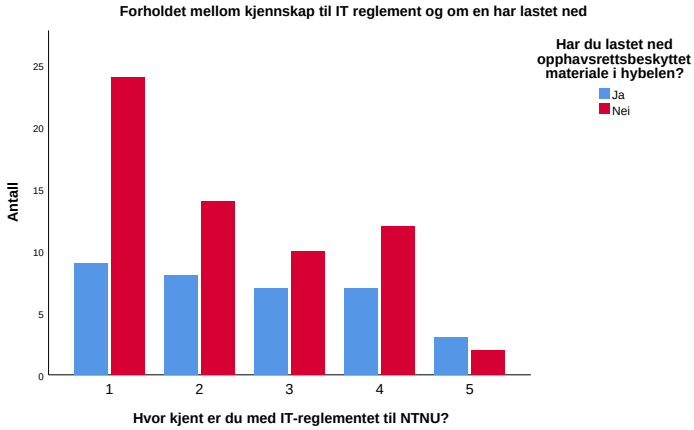
Fakultet				
	Frequency	Percent	Valid Percent	Cumulative Percent
Fakultet for arkitektur og design	15	15.5	15.5	15.5
Fakultet for informasjonsteknologi og elektroteknikk	52	53.6	53.6	69.1
Fakultet for ingeniørvitenskap	13	13.4	13.4	82.5
Fakultet for medisin og helsevitenskap	11	11.3	11.3	93.8
Fakultet for økonomi	6	6.2	6.2	100.0
Total	97	100.0	100.0	

Tabell 21: Frekvenstabell av fakultet

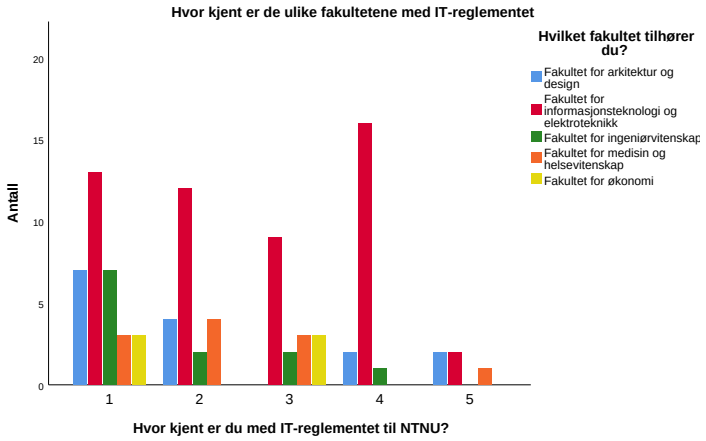
F Vedlegg: Diverse histogrammer fra case 1



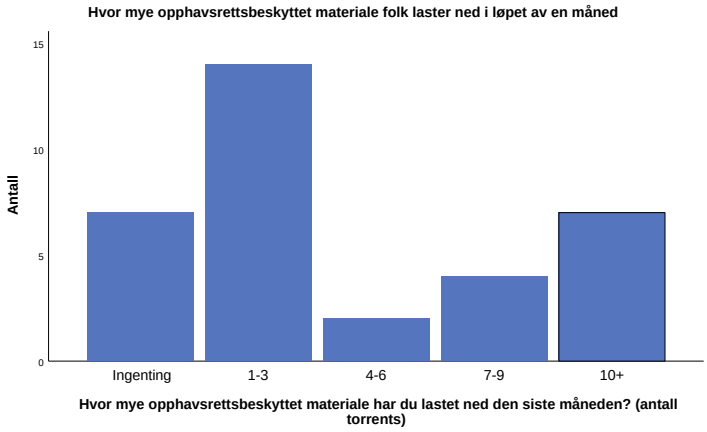
Figur 71: Forholdet mellom IT studier og andre når det kommer til nedlasting



Figur 72: Forholdet mellom kjennskap til IT-reglement og om en laster ned

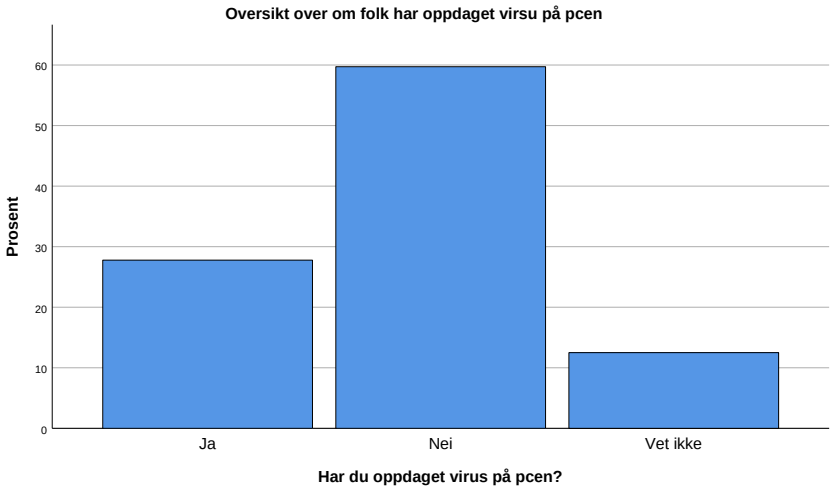


Figur 73: Hvor godt kjennskap de ulike fakultetene har med IT-reglementet

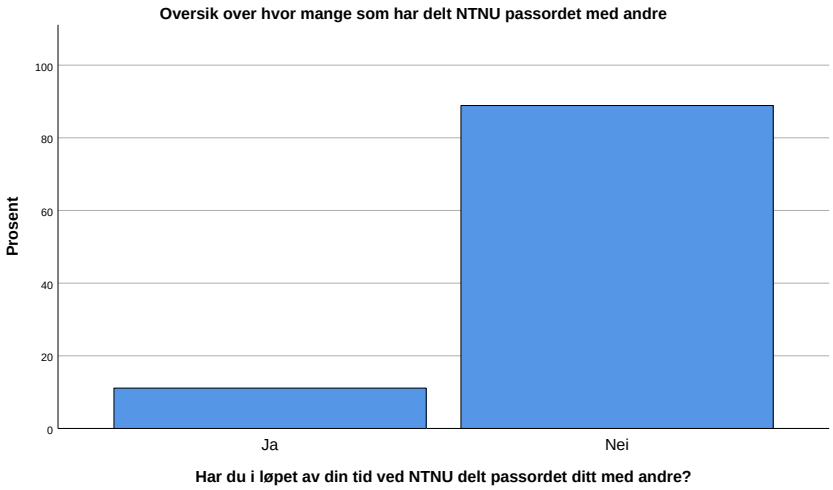


Figur 74: Hvor mange torrents folk laster ned i løpet av en måned

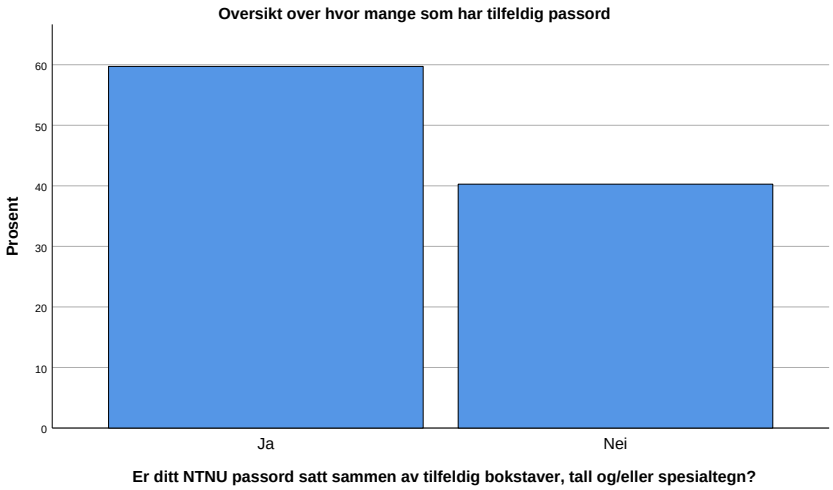
G Vedlegg: Diverse histogrammer fra case 2



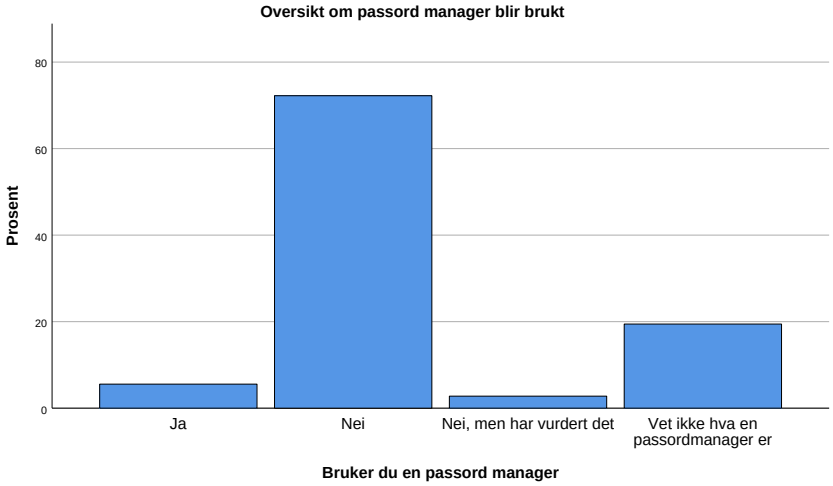
Figur 75: Oversikt over hvor mange som oppdaget virus på datamaskinen



Figur 76: Viser hvor mange som har delt sitt NTNU passord før



Figur 77: Viser hvor mange som bruker tilfeldig sammensatt passord



Figur 78: Viser hvor mange som bruker passord manager

H Vedlegg: Statistisk analyse case 2

År ved NTNU mot bevissthet på sikkerhet og kjennskap til retningslinjer

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean Lower Bound	95% Confidence Interval for Mean Upper Bound	Minimum	Maximum
Bevisst på sikkerhet når nettsider besøkes	Under 2	6	3.83	1.472	.601	2.29	5.38	1	5
	2-4	6	4.67	.816	.333	3.81	5.52	4	6
	5-9	9	3.67	1.414	.471	2.58	4.75	1	5
	10-15	15	3.47	1.246	.322	2.78	4.16	1	6
	Over 15	35	3.71	1.202	.203	3.30	4.13	1	6
	Total	71	3.75	1.239	.147	3.45	4.04	1	6
Bevisst på sikkerhet når passord lages	Under 2	6	4.83	1.941	.792	2.80	6.87	1	6
	2-4	6	4.17	1.472	.601	2.62	5.71	2	6
	5-9	9	4.11	.782	.261	3.51	4.71	3	5
	10-15	15	4.07	1.486	.384	3.24	4.89	1	6
	Over 15	36	4.47	1.055	.176	4.12	4.83	1	6
	Total	72	4.35	1.235	.146	4.06	4.64	1	6
Bevisst på sikkerhet når epost sjekkes	Under 2	6	4.67	1.966	.803	2.60	6.73	1	6
	2-4	6	4.50	1.378	.563	3.05	5.95	2	6
	5-9	9	3.67	1.225	.408	2.73	4.61	2	5
	10-15	15	4.07	1.486	.384	3.24	4.89	1	6
	Over 15	34	4.32	1.492	.256	3.80	4.84	1	6
	Total	70	4.23	1.476	.176	3.88	4.58	1	6
Kjennskap til retningslinjer for behandling av autentiseringsdata	Under 2	6	3.00	1.673	.683	1.24	4.76	1	5
	2-4	6	1.33	.516	.211	.79	1.88	1	2
	5-9	9	2.56	1.014	.338	1.78	3.33	1	4
	10-15	15	2.13	1.060	.274	1.55	2.72	1	5
	Over 15	36	2.67	1.414	.236	2.19	3.15	1	6
	Total	72	2.46	1.310	.154	2.15	2.77	1	6

Figur 79: Descriptive av tid ved NTNU mot bevissthet på sikkerhet og kjennskap til retningslinjer, del 1

Kjennskap til NTNU sitt IT reglement	Under 2	6	3.00	1.673	.683	1.24	4.76	1	5
	2-4	6	1.50	.837	.342	.62	2.38	1	3
	5-9	9	2.56	1.130	.377	1.69	3.42	1	4
	10-15	15	2.33	1.234	.319	1.65	3.02	1	5
	Over 15	36	2.64	1.334	.222	2.19	3.09	1	6
	Total	72	2.50	1.300	.153	2.19	2.81	1	6
Kjennskap til NTNU sine prinsipper for informasjonssikkerhet	Under 2	6	2.83	1.722	.703	1.03	4.64	1	5
	2-4	6	1.50	.837	.342	.62	2.38	1	3
	5-9	9	2.22	.972	.324	1.48	2.97	1	4
	10-15	14	2.50	1.225	.327	1.79	3.21	1	5
	Over 15	36	2.47	1.230	.205	2.06	2.89	1	6
	Total	71	2.39	1.224	.145	2.10	2.68	1	6

Figur 80: Descriptive av tid ved NTNU mot bevissthet på sikkerhet og kjennskap til retningslinjer, del 2

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Bevisst på sikkerhet når nettsider besøkes	Between Groups	6.394	4	1.598	1.044	.391
	Within Groups	101.043	66	1.531		
	Total	107.437	70			
Bevisst på sikkerhet når passord lages	Between Groups	3.858	4	.965	.619	.651
	Within Groups	104.461	67	1.559		
	Total	108.319	71			
Bevisst på sikkerhet når epost sjekkes	Between Groups	5.135	4	1.284	.575	.682
	Within Groups	145.208	65	2.234		
	Total	150.343	69			
Kjennskap til retningslinjer for behandling av autentiseringsdata	Between Groups	12.586	4	3.147	1.929	.116
	Within Groups	109.289	67	1.631		
	Total	121.875	71			
Kjennskap til NTNU sitt IT reglement	Between Groups	8.639	4	2.160	1.299	.279
	Within Groups	111.361	67	1.662		
	Total	120.000	71			
Kjennskap til NTNU sine prinsipper for informasjonssikkerhet	Between Groups	6.597	4	1.649	1.107	.361
	Within Groups	98.361	66	1.490		
	Total	104.958	70			

Figur 81: Anova av tid ved NTNU mot bevissthet på sikkerhet og kjennskap til retningslinjer

Multiple Comparisons

LSD

Dependent Variable	(I) ÅrBinær	(J) ÅrBinær	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Bevisst på sikkerhet når nettsider besøkes	1	2	-.833	.714	.248	-2.26	.59
		3	.167	.652	.799	-1.14	1.47
		4	.367	.598	.542	-.83	1.56
		5	.119	.547	.828	-.97	1.21
	2	1	.833	.714	.248	-.59	2.26
		3	1.000	.652	.130	-.30	2.30
		4	1.200*	.598	.049	.01	2.39
		5	.952	.547	.086	-.14	2.04
	3	1	-.167	.652	.799	-1.47	1.14
		2	-1.000	.652	.130	-2.30	.30
		4	.200	.522	.703	-.84	1.24
		5	-.048	.462	.918	-.97	.88
	4	1	-.367	.598	.542	-1.56	.83
		2	-1.200*	.598	.049	-2.39	-.01
		3	-.200	.522	.703	-1.24	.84
		5	-.248	.382	.519	-1.01	.51
	5	1	-.119	.547	.828	-1.21	.97
		2	-.952	.547	.086	-2.04	.14
		3	.048	.462	.918	-.88	.97
		4	.248	.382	.519	-.51	1.01
Kjennskap til retningslinjer for behandling av autentiseringsdata	1	2	1.667*	.737	.027	.19	3.14
		3	.444	.673	.511	-.90	1.79
		4	.867	.617	.165	-.36	2.10
		5	.333	.563	.556	-.79	1.46
	2	1	-1.667*	.737	.027	-3.14	-.19
		3	-1.222	.673	.074	-2.57	.12
		4	-.800	.617	.199	-2.03	.43
		5	-1.333*	.563	.021	-2.46	-.21
	3	1	-.444	.673	.511	-1.79	.90
		2	1.222	.673	.074	-.12	2.57
		4	.422	.539	.436	-.65	1.50
		5	-.111	.476	.816	-1.06	.84
	4	1	-.867	.617	.165	-2.10	.36

Figur 82: Post-hoc av tid ved NTNU mot bevissthet på sikkerhet og kjennskap til retningslinjer, del 1

		2	.800	.617	.199	-.43	2.03
		3	-.422	.539	.436	-1.50	.65
		5	-.533	.392	.179	-1.32	.25
	5	1	-.333	.563	.556	-1.46	.79
		2	1.333*	.563	.021	.21	2.46
		3	.111	.476	.816	-.84	1.06
		4	.533	.392	.179	-.25	1.32
Kjennskap til NTNU sitt IT reglement	1	2	1.500*	.744	.048	.01	2.99
		3	.444	.679	.515	-.91	1.80
		4	.667	.623	.288	-.58	1.91
		5	.361	.568	.527	-.77	1.50
	2	1	-1.500*	.744	.048	-2.99	-.01
		3	-1.056	.679	.125	-2.41	.30
		4	-.833	.623	.185	-2.08	.41
		5	-1.139*	.568	.049	-2.27	.00
	3	1	-.444	.679	.515	-1.80	.91
		2	1.056	.679	.125	-.30	2.41
		4	.222	.544	.684	-.86	1.31
		5	-.083	.480	.863	-1.04	.88
	4	1	-.667	.623	.288	-1.91	.58
		2	.833	.623	.185	-.41	2.08
		3	-.222	.544	.684	-1.31	.86
		5	-.306	.396	.443	-1.10	.49
	5	1	-.361	.568	.527	-1.50	.77
		2	1.139*	.568	.049	.00	2.27
		3	.083	.480	.863	-.88	1.04
		4	.306	.396	.443	-.49	1.10

*. The mean difference is significant at the 0.05 level.

Figur 83: Post-hoc av tid ved NTNU mot bevissthet på sikkerhet og kjennskap til retningslinjer, del 2

Kjønn mot bevissthet på sikkerhet og kjennskap til retningslinjer

Group Statistics

	Kjønn	N	Mean	Std. Deviation	Std. Error Mean
Bevisst på sikkerhet når nettsider besøkes	Mann	26	3.73	1.218	.239
	Kvinne	45	3.76	1.264	.188
Bevisst på sikkerhet når passord lages	Mann	27	4.67	1.240	.239
	Kvinne	45	4.16	1.205	.180
Bevisst på sikkerhet når epost sjekkes	Mann	26	4.50	1.476	.290
	Kvinne	44	4.07	1.469	.221
Kjennskap til retningslinjer for behandling av autentiseringsdata	Mann	27	2.52	1.424	.274
	Kvinne	45	2.42	1.252	.187
Kjennskap til NTNU sitt IT reglement	Mann	27	2.56	1.340	.258
	Kvinne	45	2.47	1.290	.192
Kjennskap til NTNU sine prinsipper for informasjonssikkerhet	Mann	27	2.26	1.163	.224
	Kvinne	44	2.48	1.267	.191

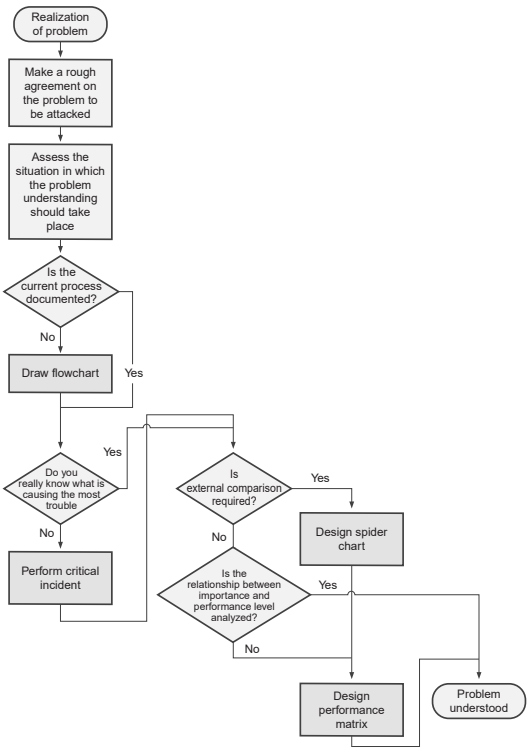
Figur 84: Gruppestatistikk av kjønn mot bevissthet på sikkerhet og kjennskap til retningslinjer

Independent Samples Test

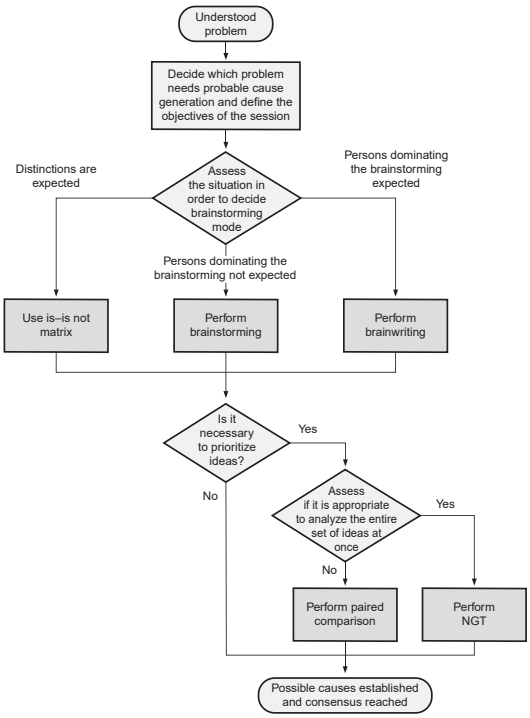
		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Bevisst på sikkerhet når nettsider besøkes	Equal variances assumed	.098	.755	-.081	69	.936	-.025	.307	-.638	.588
	Equal variances not assumed			-.081	53.916	.935	-.025	.304	-.635	.585
Bevisst på sikkerhet når passord lages	Equal variances assumed	.000	.987	1.723	70	.089	.511	.297	-.080	1.103
	Equal variances not assumed			1.711	53.631	.093	.511	.299	-.088	1.110
Bevisst på sikkerhet når epost sjekkes	Equal variances assumed	.066	.798	1.186	68	.240	.432	.364	-.295	1.158
	Equal variances not assumed			1.185	52.381	.242	.432	.365	-.300	1.163
Kjennskap til retningslinjer for behandling av autentiseringsdata	Equal variances assumed	1.400	.241	.300	70	.765	.096	.321	-.544	.737
	Equal variances not assumed			.290	49.423	.773	.096	.332	-.570	.763
Kjennskap til NTNU sitt IT reglement	Equal variances assumed	.682	.412	.279	70	.781	.089	.319	-.546	.724
	Equal variances not assumed			.276	53.232	.783	.089	.322	-.556	.734
Kjennskap til NTNU sine prinsipper for informasjonssikkerhet	Equal variances assumed	.014	.905	-.726	69	.470	-.218	.300	-.817	.381
	Equal variances not assumed			-.741	58.777	.462	-.218	.294	-.807	.371

Figur 85: Independent t-test av kjønn mot bevissthet på sikkerhet og kjennskap til retningslinjer

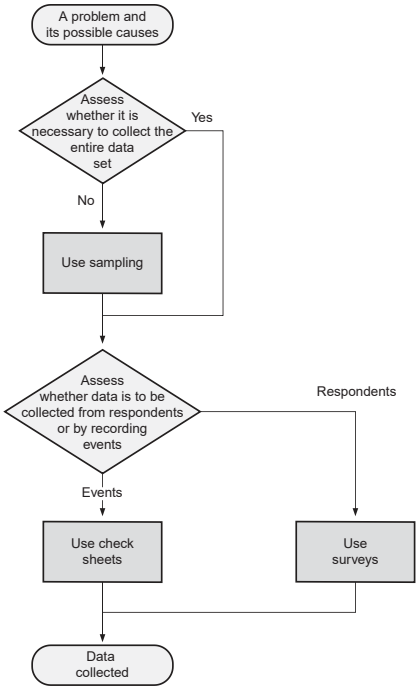
I Vedlegg: Flytdiagrammer for verktøyvalg



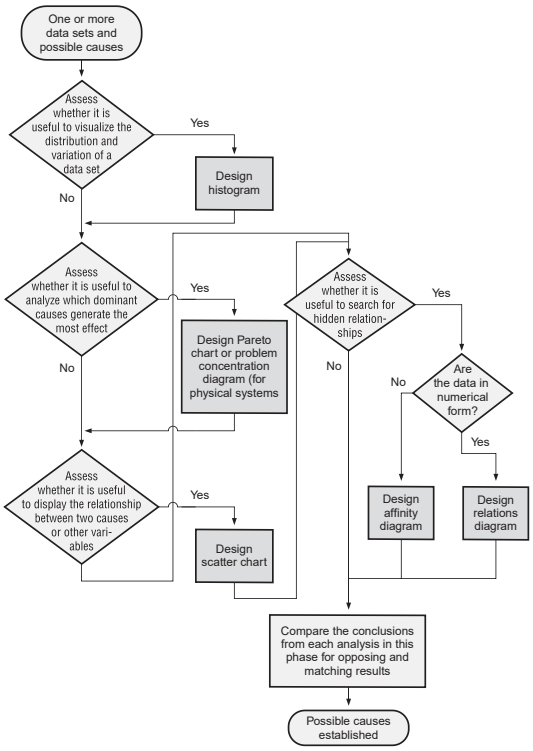
Figur 86: De ulike verktøyene boken anbefaler i problemforståelse ut fra spesifikke kriterier



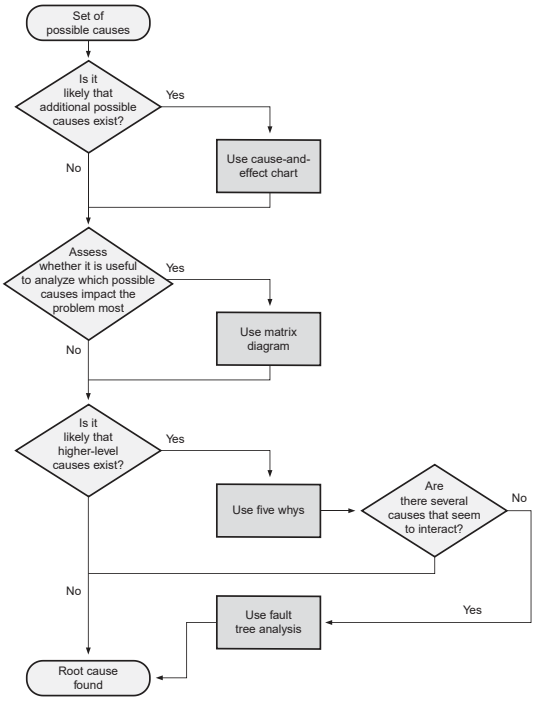
Figur 87: De ulike verktøyene boken anbefaler i idémyldring ut fra spesifikke kriterier



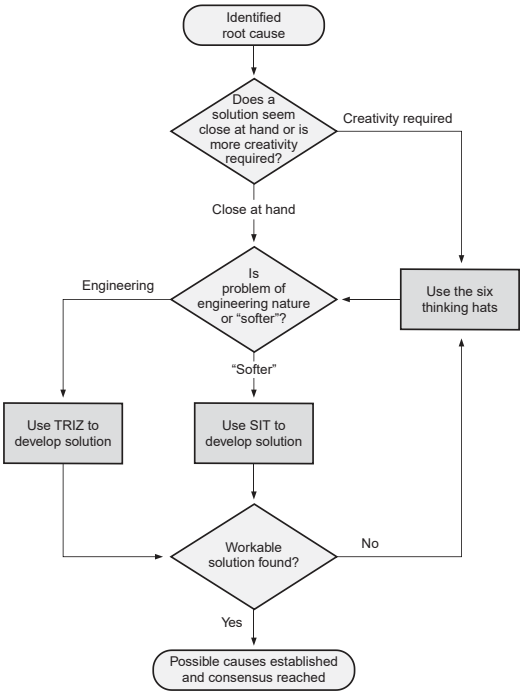
Figur 88: De ulike verktøyene boken anbefaler i datainnsamling ut fra spesifikke kriterier



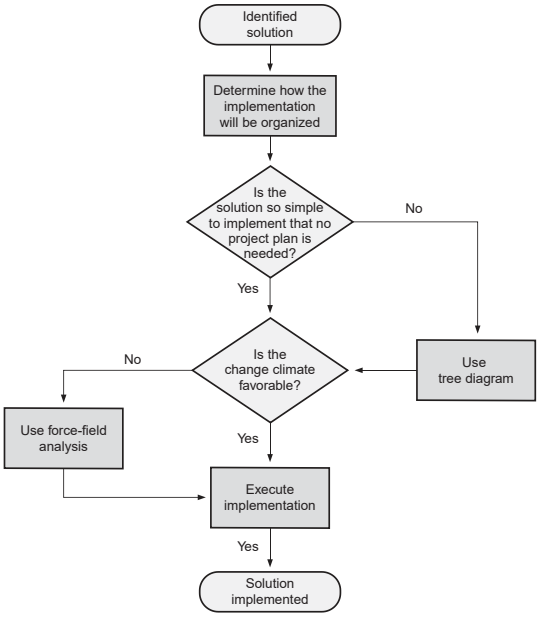
Figur 89: De ulike verktøyene boken anbefaler i dataanalyse ut fra spesifikke kriterier



Figur 90: De ulike verktøyene boken anbefaler i rotårsaksidentifisering ut fra spesifikke kriterier



Figur 91: De ulike verktøyene boken anbefaler i rotårsakseliminering ut fra spesifikke kriterier



Figur 92: De ulike verktøyene boken anbefaler i løsningsimplementering ut fra spesifikke kriterier

J Vedlegg: Møtereferater

Generelt oppsett på

Veiledermøte xx.xx.xxxx (dato)

Gjennomgang av arbeid fra siste uke

Her skriver vi notater fra tilbakemeldinger vi får på rapportskriving.

Spørsmål og svar

Her listes spørsmålene vi stilte, og notater fra svarene vi fikk er notert under hvert spørsmål

Veiledermøte 03.05.2018

Gjennomgang av arbeid

Case 2

Datainnsamling

- Ønsket utbytte: Mer om hva slags personer vi får info om, om de har blitt kompromittert det siste året.
- Gjennomførelse: data→ Informasjon
    - bestemt/definert
- Må sjekke kjønn, kanskje til og med ansatt/student
- "Noen" → flertallet/under
- 11 eller færre tegn
- "Sjeldent" sjeldnere enn x?

Dataanalyse

- Ønsket utbytte: Hvilke verktøy vi bruker til hvilke ting
- Antall over, og prosent
- Litt forsiktig, kvinner kan være mer lojale, spør om antall kvinner i 157
- Ansatte og studenter, kan spørre om antall i 157
- År ved NTNU interessant mot totalpopulasjon
- CHECK Nesten → tilnærmet
- Sjekk om de som visste det fra før er de som sa at de var blitt phishet
- Er de få som har kjennskap de som lager lange passord?

Case 3

- Problemforståelse: Hvor mange av hver ressurs, og ressurskraft
    - Ta med andre servere sammen med datamaskiner i konklusjon
- Idémyldring: Formulering på "hvordan", hva som gjør at det blir tilgjengelig for misbruk
- Datainnsamling: Hvem, hvordan, når og hypoteser
- Dataanalyse: Diskuter skjevhetstendensen

Spørsmål og svar

Hvordan kan vi være sikre på at resultatene vi fikk fra kjønn er riktige?

- Sjekk om samplen er representativt ved å sjekke andel kjønn som ble sendt ut til i forhold til andel på NTNU totalt

Generelt oppsett på

Oppdragsgivermøte xx.xx.xxxx (dato)

Gjennomgang av hva oppdragsgiver ønsker fra oppgaven

Notater…

Fremvisning og gjennomgang av teknisk arbeid

Notater…

Spørsmål og svar på teknisk veiledning

Notater…

Oppdragsgivermøte 05.04.2018

Gjennomgang av hva oppdragsgiver ønsker fra oppgaven

- spørreundersøkelse til et sample av de som har blitt kompromittert
- nevne etikken i å kontakte folk som har gjort en tabbe

Fremvisning og gjennomgang av teknisk arbeid

- Passord management
    - ikke håndhevet
    - dårlig formulerte regler
- Viste de at de ble kompromittert?
- Hvor ofte bytter de NTNU passord?
- Nedskrevne passord, kanskje ikke en årsak?

Spørsmål og svar på teknisk veiledning

- Backup til spørreundersøkelse
    - gå bredere ut
    - spør alle ntnu ansatte
    - fjerne spm om kompromitterte kontoer
- Bruteforcing av servere
- Remote desktop RDP

K Vedlegg: Transkripsjon fra møte med senior sikkerhetsanalytiker på NTNU SOC

Transcript

P. Starte litt opp med litt praktisk angående den statistikken du sendte oss, for der står det jo sånn om ETPRO TROJANER og alt mulig sånt. Er det sånn at dette er malware som er på pcene?
C. Når det står at det er trojaner så er det jo malware, da er det bevist malware
P. Er bevist malware ja, alt er bare en felles betegnelse på malware?
C. Nei men type trojaner, malware type trojaner.
P. har dere noen formening på hvordan disse trojanerne kommer på pcene til folk?
C. Vi har ikke dokumentert det, men sånn tipper det er enten via epost eller waterhole nettsider som sprer de. Stort sett de angrepsvektorene som brukes, uten at vi har registrert det da, men det er utifra hva leverandører og de som forsker på trussel etterretning de sier at det er stort sett sånn de ser de kommer inn. Så vil det jo være rart at de kommer inn på noen annen måte hos oss.
P. hvor lenge ca. er det de pleier å være på pcene før dere oppdager de?
C. Nei så fort de er på merkes de i trafikken som synes i statistikken dere har fått der
P. Og da går dere bare kjapt og sier nå må vi (Philip Lager lyd og tegn signaliserer kastes ut)
C. Hiver de av nett og kontakter brukeren det kommer helt ann på hvordan maskinen er, altså om det er maskin vi har kontroll på eller ikke om det er en server eller om det er en klient. Om det er en bring your own device eller drifta klient. Her er det litt mer komplisert linje å gå
P. Ok så hva er det dere gjør hvis det er en klient liksom, altså booter dere de av nettet liksom eller er det mer?
C. Spørs om det er bring your own device eller om det er drift av klient. Drifta klient har vi mulighet til å gå inn og sjekke det. Bring your own device har vi ikke noen annen mulighet enn kaste de av nett. Men som regel når det er coinmining varsler vi brukeren. Ber de kjøre noe antivirus programmer eller oppdatere maskinen deres

P. Unike signaturer fra dette er signatur fra den malware?
C. Det er forskjellige unike så har du jo de signaturene som har coinminer eller i seg og da er da antall. Så dette er da de unike signaturene vi ser og så har du da antall hver signatur har trigga på.
P. Men de antallet er det antallet med pc liksom eller om det?
C. Nei det er antall ganger den signaturen har trigget
P. men har dere noe tall på hvor mye ofte klienter eller hvor mange klienter som er, stadig blir brukt til mining på en måte?
C. Da må e hent ut ny statistikk, men ja du kan se det. Vi kan ta sortering på unike ip adresser
P. Har dere noe på hvor stort antall privat bruk av det og hvor mye som er liksom dette her er malware som?
C. det kan vi ikke skille på per nå
P. Men har dere noe tanker sånn cirka, sånn cirka hva fordelingen er?
C. Nei ikke per nå som jeg tør å si. Da må jeg sjekke datasettet først

P. Ja men. Ja men det er fult lovlig det ja
T. Ja det var hpc clusterne
C. Ja
T. Hvordan var det dere fant ut den ble misbrukt?
C. Kombinasjon av at hpc som lurte om vi kunne se på det og det var signatur som var trigga.
P. Ja ok, Hvordan fant derre ut at det var noen interne?
C. Det var jo lett, det er jo scheduling og det er jo logg på hpc cluster som kjører. Så da kan se hvem som starta prosess og da spore tilbake hvilken node den prosessen har gått på og så videre og videre
P. Og da har vedkommende sagt jeg gjorde det eller lignende?
C. Det utaler meg ikke noe om
P. Er det noe måte for dere å blokkere folk annet enn kaste de av nettet, fra kunne kjøre cryptominer på pc sine?
C. Kan gjøre grep i nettet, blokkere f.eks dns adresser som brukes til å rapportere ting og så videre også videre. Ting vi kan gjøre, men når det gjelder private utstyr så det jo litt begrensa. Annet enn å begrense nette deres
P. Hva er grunnen til at dere ikke har implementert noe slike tiltak?
C Fordi det er andre ting som brenner mer
P. Ja ok
C Så miner litt bitcurrent, det er ikke høyest på lista over problemmer
P. Hva tror du er oppfatningen blant dine kollega angående mining, er det folk vet det er ulovlig på en måte eller er det har ikke tenkt så mye over det og miner bare fordi det?
T. Trend eller?
C. Tro det er en trend folk hiver seg på ja, ihvertfall når det gjelder de som setter opp sjølv. Det er jo ikke ulovlig etter når du snakker ulovlig så er jo norsk lover, men brudd på regelverk tror jeg det ikke er mange som har tenkt over
P. Hva er måten dere for du snakket tidligere om at dere så mange av de walletsa som ble brukt var fra mørke siden av nettet?
C. der har du jo de som går etter trojan
P ja og der fordi hvordan ser dere at de går til disse walletsa. Er det bare fordi disse kjente malware sender til?
C. Altså du kan jo se hvilken wallet det sendes til og innholdet denne walleten er jo offentlig informasjon i hvert fall på bitcoin. Så kan se alle transaksjoner som går inn og ut av en wallet
P. Ja ok har dere noen tanker hvordan dere skal implemiter kryptomining i neste IT-reglement?
C. ja det er allerede, det er ikke spesifikt sagt noe om det, men det står svart på hvitt i reglement at det ikke får lov til å bruke NTNU infrastruktur til kommersiell virksomhet. Så lenge du tjener penger på det er det kommersiell virksomhet.
P. Er det noe folk tenker over?
C. Nei må må nok kjøre en liten innsida sak eller noe sånt få en liten kampanje rundt det på awarensen. Så reglemente dekker det det skal dekke
P. Har dere noen tiltak på mining på nettsider. Det er jo noe som ser ut som blir brukt en del?
T. Hvis du liksom stopper med reklame og så begynner med mining istedenfor

C. Der kan man gjøre ting på klienten og blokkere de javascriptene, selv en drifta client er det mange måter vi kan gjøre det på. Selve nettet kan blokkere de filene som lastes ned. Så får ikke kjørt den javascript fil på klienten
P. Igjen det blir nedprioritert fordi de ikke såpass spennende?
C Per nå ja
P. Er det like stor økning nå som det var før jul eller har det dabba en del av?
C. Det fortsetter
P. Det gjør det?
C Det øker ikke så veldig mye mer, men det fortsetter
T. Den økninga er det da gjort av den profesjonelle aktørene eller det folk setter frivillig opp minere?
C. Det er jo mest på den profesjonelle du ser den da, men ja det er nok en litt økning på som setter opp sjølv på grunn alt alle vg artiklene kan man vel si da. Hvordan bli rik på cryptomining, merker at folk prøver.
P. Dere hadde ikke sett noe tilfeller av brutforce på pc og server som ble installert cryptominere på etter de ble brutforca?
C Ikke som jeg kan huske nei
T. Ja er det noen regler på hva ansatt får lov å legge på serverne de f.eks har stående på kontoret sitt slike ting?
C. Nei ikke spesifikt som jeg kommer på så du har et sett med retningslinjer, men de er ikke ferdig vedtatt av styre enda. Og så er det da
P. Kommersiell bruk biten
T. Så det er liksom forsker på crypto
C. Vi har folk som forsker på crypto
T. Men det er sann at de satt de opp av nysgjerrighet og så glemte de at den var satt opp?
C. det skjer hele tiden, det er ikke bare med kryptominere
P. Har dere hadd noen tilfeller av type pcer på ciscolab at studenter har slengt cryptominere på de og bare latt de stå og gå?
C. Kan ikke huske at det har hvert noen på ciscolabe, men det er eksempel på det
P. Det er det ja
T. Har du lyst å komme med et eksempel eller?
C. Trenger ikke henge ut noen faggrupper
P. Sykepleierne?
C. Spesielt de, nei da
P. Fungerer adgangskontroll på de forskjellige clusterene deres bare visse folk som kan bruke det?
C. Må få en konto på de av de som administrer dette
P. Har du noe estimat på hvor mye penger det har kostet skolen?
C. Nei