NTNU
Norwegian University of
Science and Technology

Bruk av rotårsaksanalyse i informasjonssikkerhet

Forfattere
Henrik Miguel N. Torres
Niclas Hellesen
Erlend Lundsvoll Brækken

Bachelor i informasjonssikkerhet
20 ECTS
Avdeling for informatikk og medieteknikk
Norges teknisk-naturvitenskapelige universitet,

18.05.2016

Veileder Ph.D. student Gaute Bjørklund Wangen,
Avdeling for informatikk og medieteknikk, NTNU i Gjøvik

Sammendrag av Bacheloroppgaven

Tittel:	**Bruk av rotårsaksanalyse i informasjonssikkerhet**
Dato:	18.05.2016
Deltakere:	Henrik Miguel N. Torres Niclas Hellesen Erlend Lundsvoll Brækken
Veiledere:	Ph.D. student Gaute Bjørklund Wangen, Avdeling for informatikk og medieteknikk, NTNU i Gjøvik
Oppdragsgiver:	Professor Einar Arthur Snekkenes, Avdeling for informatikk og medieteknikk, NTNU i Gjøvik
Kontaktperson:	Einar Arthur Snekkenes, einar.snekkenes@ntnu.no, Tlf.: 61 13 52 52
Nøkkelord:	Rotårsaksanalyse, Informasjonssikkerhet, Case Study, Kostnytteanalyse, Norway, Norsk
Antall sider:	192
Antall vedlegg:	
Tilgjengelighet:	Åpen

Sammendrag:

Tilnærming til problemer i informasjonssikkerhet (IS) er å identifisere risiko og velge et risikoreduserende tiltak basert på en risikovurdering (RV), eller hendelseshåndtering for problemer som forekommer hyppig. Tilnærmingene har sine begrensninger.Rapporten benyttet rotårsaksanalyse (RCA) på tre caser innen IS for å grave dypere ned i problemet med mål om å eliminere det i sin helhet. Vi besvarer forskningsspørsmålet: *Hvor stor nytteverdi har RCA innenfor fagfeltet informasjonssikkerhet?*, og underspørsmål: (i) Er det kostnadseffektiv å bruke RCA innen informasjonssikkerhet? (ii) Hvordan fungerer RCA på et tabletop case? (iii) Hvordan fungerer RCA med mye ressurser og tid? (iv) Hvordan fungerer RCA med begrenset ressurser og tid? RCA er lite brukt innen IS som er bakgrunnen for denne oppgaven. Vi konkluderte at RCA fungerer bra som en læringsprosess på tabletop, kun teknisk dokumentasjon er ikke tilstrekkelig, da kontakt med nøkkelpersoner er kritisk for analysen. RCA med mye tid og ressurser ga ekstra innsikt i problemet og førte til svært forskjellige tiltak samenliknet med risikovurdering. Når vi gjennomførte RCA med begrenset tid og ressurser ga det resultater, men vi fant at RCA ikke ble utnyttet til sitt fulle. Vi så at RCA ga resultater i form av rotårsaker for DDoS-caset, disse var mer på den administrative siden. Arbeidet vårt belyste RCAs begrensninger i forhold til de tekniske aspektene av IS.

Summary of Graduate Project

Title:	**Bruk av rotårsaksanalyse i informasjonssikkerhet**
Date:	18.05.2016
Authors:	Henrik Miguel N. Torres Niclas Hellesen Erlend Lundsvoll Brækken
Supervisor:	Ph.D. student Gaute Bjørklund Wangen, Avdeling for informatikk og medieteknikk, NTNU i Gjøvik
Employer:	Professor Einar Arthur Snekkenes, Avdeling for informatikk og medieteknikk, NTNU i Gjøvik
Contact Person:	Einar Arthur Snekkenes, einar.snekkenes@ntnu.no, Tlf.: 61 13 52 52
Keywords:	Root Cause Analysis, Information Security, Case Study, Cost benefit analysis, Norway, Norwegian
Pages:	192
Attachments:	
Availability:	Open

Abstract:

Common approach to problems in information security (IS) is to identify risk and choose risk reducing measures based on risk assessment. This report used root cause analysis (RCA) on three IS case studies to dig deeper into the issue with the goal of eliminating it entirely. We answer the following research questions: *How usefull is root cause analysis in the field of information security?*, and the following sub-questions: (i) Is it cost effective to use root cause analysis in information security? (ii) How well works root cause analysis on a tabletop case? (iii) How well works root cause analysis on a case with a lot of resources and time? (iv) How well works root cause analysis on a case with limited resources and time? Root cause analysis is rarely used in IS which is the main basis for this task. We conclude that RCA works well as learning prosess on tabletop, but only technical is not sufi-cent far a full prosess since contact with key persons is critical. RCA with a lot of resources gave oss extra insight in the problem and lead to different measures compared to risk assessment. When we completed the RCA with limited time and resources we got results, but we found that RCA hadn't been used to its full potensial. We also found that RCA gave results in the form of root causes for the the DDoS case, these where more adminastrative related. Our work also highlited RCAs limitations in relation to the technical aspects of IS.

Forord

Prosjektet var en spennende prosess hvor vi fikk satt oss inn i rotårsaksanalyse og tre forskjellige caser.

Oppgaven om å undersøke rotårsaksanalyse innen informasjonssikkerhet ble gitt av Einar Arthur Snekkenes til bachelorgruppen høsten 2015. Vi syntes oppgaven har vert veldig spennende og det har vert gøy å føle at vi har kunnet bidra med ny informasjon på området.

Vi ønsker å rette en spesiell takk til Gaute Bjørklund Wangen for hjelp og veiledning igjennom arbeidet med prosjektet.

Takk til oppdragsgiver Einar Arthur Snekkenes for å ha gitt oss oppgaven.
Takk til Christoffer V Hallstensen og Stian Husemoen fra IT-tjenesten og Vidar Sandland fra slettmeg.

Vi ønsker også å rette en takk til alle som stilte opp på intervju og bidro til å gjøre denne oppgaven mulig.

Innhold

Figurer

Tabeller

executive summary

Rotårsaksanalyse er lite brukt innen informasjonssikkerhet som har vert hovedgrunnlaget for denne oppgaven. Vanligvis håndteres problemsituasjoner innen informasjonssikkerhet ved at det gjennomføres en rissiko analyse. En risikoanalyse tar for seg potensielle problemer som kan oppstå, hvor man ser på sannsynligheten for at trusselen inntreffer samt hva som vil være konsekvens, og hva som vil være preventive og reaktive mottiltak. Vi i vår bachelor ser på rotårsaksanalyse som er en systematisk metode for å finne de underliggende årsaker til feil eller svikt. En rotårsaksanalyse gjøres i etterkant av hendelsesforløpet, som står i kontrast med risikoanalyse som behandler tenkte situasjoner i fremtiden. For å konkretisere problemet ønsker vi å undersøke hoved forskningsspørsmålet *Hvor stor nytteverdi har rotårsaksanalyse innenfor fagfeltet informasjonssikkerhet?*, med følgende underspørsmål:

1. Er det kostnadseffektiv å bruke rotårsaksanalyse innen informasjonssikkerhet?
2. Hvordan fungerer rotårsaksanalyse på et tabletop case?
3. Hvordan fungerer rotårsaksanalyse på en case med mye ressurser og tid?
4. Hvordan fungerer rotårsaksanalyse på en case med begrenset ressurser og tid?

For å besvare forskningsspørsmålene hadde vi tre caser. Først tok vi en tabletop øvelse på Carbanak angrepet og baserte oss på tilgjengelig dokumentasjon. Dereter fikk vi en case av IT-tjenesten som gikk ut på å undersøke rotårsaker til kortlån på skolen, hvor vi brukte mye ressurser og tid. Tilslutt fikk vi en case av slettmeg hvor vi undersøkte et DDoS tilfelle med lite tid og ressurser.

Vi mener at rotårsaksanalyse har nytteverdi innen informasjonssikkerhet. Det gir forskjellige resultater enn andre verktøy. Det kan lønne seg å anvende rotårsaksanalyse til å håndtere problemer som oppstår.

Gjennomføring av rotårsaksanalyse på Carbanak caset viste seg å være vanskelig på områder der informasjonen ikke var tilgjengelig. Derimot fremstår øvelsen som et nyttig lærings verktøy. For personer som lærer seg rotårsaksanalyse gir dette et godt læringsutbytte.

Rotårsaksanalyse fungerte godt på case om adgangskort låning fra IT-tjeneste hvor vi hadde mye ressurser og tid. Vi kom frem til andre resultater enn risiko analysen skolen hadde gjort. I tillegg ble våre forslag til tiltak svært annerledes enn de som ble foreslått av IT-tjenesten.

I caset hvor ressurser og tid var begrenset ga RCA resultater, men problemsituasjonen bør ikke være for stor eller kompleks i forhold til antall personer inkludert i analysen og deres tid og ressurs begrensninger.

Utifra nytteverdien av RCA innen informasjonssikkerhet ser vi at de syv RCA stegene vi anvendte i våre analyser dekker problemløsningen på en strukturert måte fra å forstå problemet til å implementere en løsning. Det er viktig med god forståelse av problemet og tilgang til nøkkelpersoner. Ut i fra rotårsaksanalysene våres gir RCA resultater, selv med begrenset tid og ressurser. Vi har erfart at ved hjelp av rotårsaksanalyse er det mulig oppdage problemsituasjoner som med andre verktøy brukt innen informasjonssikkerhet ikke er synlige.

1 Introduksjon

Introduksjonskapittelet inneholder informasjon om hele bacheloroppgaven. Det er en beskrivelse av formålet med oppgaven, hvem prosjektet er utført for, våre forskningsspørsmål, resultatmål samt effektmål. Vi tar for oss rammer og avgrensninger vi har satt for oppgaven.

1.1 Bakgrunn og Formål

Risikovurdering et verktøy som er svært utbredt innenfor informasjonssikkerhet og personvern. Det anvendes til å kartlegge trusler en bedrift kan støte på. De fleste bedrifter har utarbeidet egne planer for hendelseshåndtering om en trussel inntreffer. Rotårsaksanalyse er en metodikk hvor man går gjennom en rekke steg for å komme til roten av et problem. Det vi ønsker å undersøke i bacheloroppgaven vår er om rotårsaksanalyse (RCA - Root Cause Analysis) kan anvendes på problemer som oppstår innen informasjonssikkerhet, og om det kan være en god og effektiv fremgangsmetode, som enda ikke er fullstendig utnyttet.

Vi skal se på forskjellige verktøy som i dag blir brukt i sammenheng med rotårsaksanalyse. Rotårsaksanalyse blir brukt innen andre fagfelt men vi vil anvende disse til feltet informasjonssikkerhet for å besvare underspørsmålene til forskningsspørsmålet.

1.2 Problemstilling

Problemet vi adresserer i denne oppgaven er å finne ut om rotårsaksanalyse har nytteverdi innen feltet informasjonssikkerhet. Utfordringer vi ser for oss er om det finnes verktøy som passer og hvordan de kan implementeres eller anvendes innen informasjonssikkerhet. Normalt sett anvendes risikovurdering som en måte å analysere sannsynligheter og konsekvenser av forutsette problemer bedriften står ovenfor. En slik vurdering baserer seg på potensielle trusler og sårbarheter som kan føre til tap for bedriften i fremtiden. I kontrast til dette behandler rotårsaksanalyse tilfeller som har inntruffet, og forsøker å identifisere og behandle den underliggende årsaken til ett eller flere problemer. Fordelen med rotårsaksanalyse er at du blir kvitt problemet i sin helhet, i motsetning til risikovurdering hvor hovedmålet er å redusere risiko til et akseptabelt nivå. Faglitteraturen innen informasjonssikkerhet viser at rotårsaksanalyse ikke har vært benyttet i særlig stor grad.

1.3 Forskningsspørsmål

For å konkretisere problemet ønsker vi å undersøke hovedforskningsspørsmålet:
Hvor stor nytteverdi har rotårsaksanalyse innenfor fagfeltet informasjonssikkerhet?
Med følgende underspørsmål:

1. Er det kostnadseffektivt å bruke rotårsaksanalyse innen informasjonssikkerhet?

2. Hvordan fungerer rotårsaksanalyse på et tabletop case?
3. Hvordan fungerer rotårsaksanalyse på et case med mye ressurser og tid?
4. Hvordan fungerer rotårsaksanalyse på et case med begrenset ressurser og tid?

Med ressurser tenker vi på personer som er tilgjengelige for å gjennomføre analysen.

1.4 Effektmål

Ved å svare på de fire underspørsmålene vil vi oppnå disse effektmålene:

- Finne ut om det er fordeler ved å bruke rotårsaksanalyse.
- Øke interesse og forståelse for bruk av rotårsaksanalyse innen informasjonssikkerhet.
- Gjøre det enklere å utføre rotårsaksanalyse innen informasjonssikkerhet.
- Tilfør informasjonsikerhetsmiljøet mer kunnskap om nytten av rotårsaksanalyse.

1.5 Resultatmål

Da vi er ferdig med hele rapporten ønsker vi å oppnå disse resultatmålene:

- Bruke rapporten som en veiledning og gi en innføring i teknikker som kan bedre arbeidet med å identifisere rotårsaker til hendelser.
- Finne rotårsak ved bruk av verktøy for rotårsaksanalyse i minst 2 case innen informasjonssikkerhet.
- Kartlegge muligheter og begrensninger for bruk av rotårsaksanalyse innen informasjonssikkerhet.

1.6 Avgrensning

Det finnes en rekke metoder og verktøy innen rotårsaksanalyse, men vi blir nødt til å begrense antall metoder vi utfører eller videreutvikler grunnet tidsbegrensninger. Vi velger ut noen metoder vi mener er relevante for hver enkel problemstillingen i casene.

1.7 Målgruppe

Vår målgruppe for denne bacheloroppgaven er oppdragsgiver, veileder og generelt alle som arbeider med problemløsning, risikovurdering og hendelsehåndtering og de som har interesse for faget informasjonssikkerhet. Denne prosjektoppgaven kan fungere som en veileder for de som ønsker å utføre rotårsaksanalyse innen informasjonssikkerhet.

1.8 Oppgavebeskrivelse

Det kan ofte være vanskelig å identifisere underliggende årsaker til et problem, samt identifisere riktige tiltak som bør gjøres for å håndtere rotårsaken til en hendelse.
Ved å identifisere rotårsaken og ikke kun symptomene skal det være mulig å finne tiltak som forbedrer prosessen samt hindre en uønsket effekt over tid. Det vi ønsker å gjøre i

denne bacheloroppgaven er å veilede samt gi en innføring i teknikker som kan bedre arbeidet med å identifisere rotårsaker til hendelser. Rotårsaksanalyse kan hjelpe med å finne løsninger på hendelser ved å bruke strukturerte og visuelle tilnærminger samt trekke konklusjoner. Primært vil rotårsaksanalyse brukes til å identifisere tilhørende løsningsforslag og rotårsaken til et problem[4].
Det skal også gis en strukturert forståelse i forholdet mellom mulige kategorier av hovedårsaker og tjene som en visuell fremstilling av årsakene til en hendelse. Det vil involvere medarbeidere som har best forutsetninger til å løse hendelsene og hjelpe medarbeiderne med å kommunisere med hverandre og resten av organisasjonen.

1.8.1 Prosjektgruppens bakgrunn

Gruppens medlemmer tar bachelor i Informasjonssikkerhet på Høgskolen i Gjøvik, hvor siste halvåret er under NTNU etter HiG ble fusjonert med NTNU i 2016. I utdanningsforløpet har vi tilegnet oss kunnskaper vi kan dra nytte av til oppgaven, først og fremst fra "Sikkerhetsplanlegging og Hendelseshåndtering" og "Risikostyring". Vi har fått en bedre forståelse av hvordan trusler i næringslivet bør tas hånd om og hvordan rangere disse truslene. I faget "Systemutvikling" fikk vi erfaring med forskjellige systemutviklingsmodeller og praktisk anvendelse med prosjektarbeid. Dette ga grunnlaget for valg av utviklingsmodell som blir brukt i denne rapporten. Ingen hadde kompetanse innen rotårsaksanalyse eller statistikk derfor brukte vi mye tid på å lære dette.

1.9 Rammer

Prosjektet skal være ferdig og levert innen 18.mai. Datainnsamling til case skal hovedsakelig være utført av gruppen. Rapporten vil bli skrevet via ShareLaTeX
med backup på GitHub. Vi legger arbeidsoppgaver inn i www.trello.com der kan vi selv sette tidsfrister på arbeid som må gjøres og hver enkelt person i gruppen kan hente ut arbeid han selv vil gjøre.

1.10 Arbeidsmetode

I rotårsaksanalysen vi bruker, er det 7 forskjellige faser der man har forskjellige verktøy til de ulike fasene. Vi gjør hver fase ferdig før vi går videre til neste. Fremdriften for vårt prosjekt er lineær og vi har da ingen grunn om å gå tilbake for å endre på ting i de enkelte fasene etter at de er fullført. Vi ser derfor for oss at fossefalls modellen vil være ideell for vårt prosjekt, og vi referer til Software Engineering 9, side 29 til 32[5].

1.11 Rapportstruktur

I kapittel 2 forklares forskjell på rotårsaksanalyse og risikoanalyse, i tillegg til ulike nivåer av årsaker og verktøy brukt innen rotårsaksanalyse. Det blir til slutt sett på tidligere arbeid. Kapittel 3 omhandler valg av metoder for å løse forskningsspørsmålene. I kapittel 4 presenterer vi resultater fra våre caser. I kapittel 5 diskuterer vi oppgavens resultat og mål og hvordan vi kom frem til svarene på våre forskningsspørsmål. I kapittel 6 oppsummerer vi og gjør en konklusjon av oppgaven basert på forskningsspørsmålene våre.

2 Beskrivelse av rotårsaksanalyse og tidligere arbeid

Dette kapittelet er basert på boken "Root Cause Analysis: Simplified Tools and Techniques" [1] s.4-7 og vil forklare hva rotårsaksanalyse er og de forskjellige stegene vi må gå igjennom for å fullføre rotårsaksanalysen. Vi forklarer hva som er forskjell på rotårsaksanalyse og risikoanalyse, hvorfor man bør anvende rotårsaksanalyse og ulike nivåer av årsaker samt verktøy man bruker innen rotårsaksanalyse. Det er også sett på tidligere arbeid innen fagområdene rotårsaksanalyse og informasjonssikkerhet.

2.1 Rotårsaksanalyse kontra risikoanalyse

En risikoanalyse tar for seg potensielle problemer som kan oppstå. Der ser man på sannsynligheten for at trusselen inntreffer, samt mulige konsekvenser, og hva som vil være mulige preventive og reaktive mottiltak [6]. Rotårsaksanalyse/RCA er en systematisk metode for å finne de underliggende årsaker til feil eller svikt. En rotårsaksanalyse gjøres i etterkant av hendelsesforløpet, som står i kontrast med risikoanalyse som behandler tenkte situasjoner i fremtiden.

2.2 Hvorfor bruke rotårsaksanalyse

Grunnen til å utføre en rotårsaksanalyse er å kunne identifisere en eller flere rotårsaker. Når disse er identifisert og løsningsforslag er implementert, bør symptomet/symptomene som var konsekvens av problemene opphøre. Dersom de ikke opphører kan dette være et tegn på at man ikke har funnet rett årsak, eller at det er flere rotårsaker til problemet. Det er ikke en vanlig metodikk å bruke rotårsaksanalyse innenfor informasjonssikkerhet. Vi så at dette ga oss en stor mulighet til å kunne anvende kjente rotårsaksanalyse-verktøyer vi kjenner, og observere hvordan de passet til den gitte situasjonen.

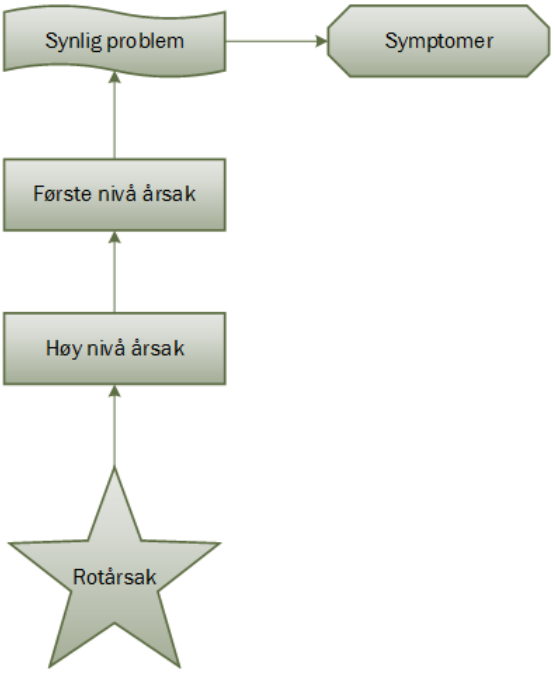
2.3 Ulike nivåer av årsaker

Et problem kommer ofte som et resultat av flere årsaker på ulike nivåer. Dette betyr at noen årsaker påvirker andre årsaker, som igjen kan gi synlige problemer, se figur 1. Årsaker kan klassifiseres som et av de følgende punkter [1]:

- Symptomer: Disse regnes ikke som faktiske årsaker, men snarere som et tegn på eksisterende problemer.
- Første nivå årsak: Årsaker som direkte fører til et problem.
- Høy nivå årsak: Årsaker som kan føre til første nivå årsakene. Selv om de ikke direkte er årsak til problemet, lager høy nivå årsakene ledd i kjeden av årsaker og virkninger på relasjoner som til slutt skaper problemet.

Noen problemer har ofte sammensatte årsaker, hvor ulike faktorer til sammen forårsaker problemet.

Det høyeste problemnivået vi tar for oss er det vi kaller for rotårsak. I Fig:1 viser vi veien fra rotårsak til høy nivå årsak, første nivå årsak, det synlige problemet som oppstår etterfulgt av symptomene som konsekvens av rotårsaken.

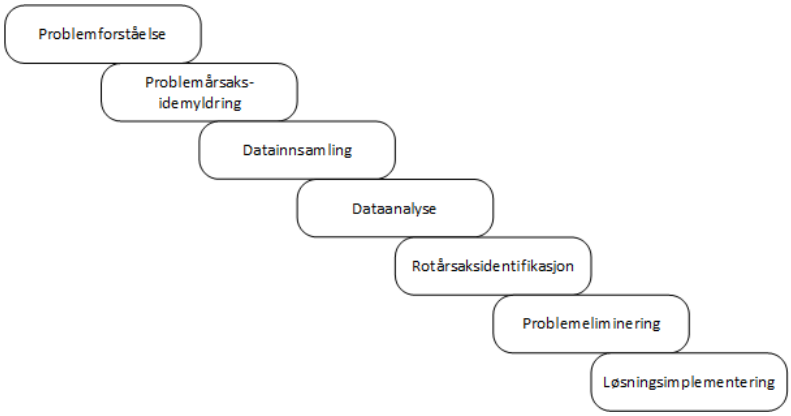


Figur 1: Veien fra rotårsak til symptomer basert på Root cause analysis simplified tools and techniques[1] s.5

Om man kun fjerner symptomene, kan situasjonen bli verre. Problemet vil fortsatt være tilstede, men det vil ikke lenger være et lett gjenkjennelige symptom som kan overvåkes. Eliminerer man første- eller høy nivå årsakene kan man midlertidig eliminere problemet, men årsaken vil til slutt finne en annen måte å manifestere seg på i form av et annet problem. Når man har klart å finne riktig rotårsak og fjernet den, skal man overvåke symptomer for å bidra til å sikre at problemet ikke vil gjenoppstå. Først da vet man at man har funnet og eliminert rett rotårsak til problemet.

2.3.1 Rotårsaksanalyseprosessen

I rotårsaksanalyseprosessen gikk vi gjennom syv forskjellige faser som vist i Fig: 2, her brukte vi flere forskjellige verktøy som vi mener var eget for de ulike fasene.



Figur 2: Rotårsaksanalyseprosessen basert på bilde i Root cause analysis simplified tools and techniques[1] s.7

De forskjellige fasene som er illustrert i fossefallsmodelen er beskrevet under:

- **Problemforståelse:** Mange problemer er ikke like synlige for alle og det er ikke alltid like lett å forstå hva som egentlig er problemet. Når et case ble mottatt var det essensielt at vi klarte å forstå det virkelige problemet. For at dette skulle være mulig måtte vi kaste lys på miljøet problemet befant seg i, og først da kunne vi se situasjonen som et faktisk problem. Det var viktig at alle involverte i caset hadde samme problemforståelse.
  Det finnes verktøy innenfor årsaksanalyse som er utviklet for å gi analytikerne innsikt i problemet som for eksempel Flowchart, Critical Incident og Performance Matrix.
- **Problemårsaksidemyldring:** Først da gruppen forstod problemet kunne vi starte idemyldringen. Her gjorde vi antagelser om problemenes symptomer og konsekvenser. Det kan være nyttig å inkludere flere personer med ulik kunnskap innad i organisasjonen for å få flest mulige synsvinklinger inn i bildet, blant annet personer med god erfaring fra miljøet problemet oppsto i. Vi har blant annet sett på verktøyet Brainstorming, her var det viktig å passe på under utførelsen at alles meninger kom frem og ikke blir avbrutt eller kommentert selv om det er positivt eller negativt.
- **Datainnsamling:** Dette var den fasen som var mest kritisk. Her var det viktig at vi fikk inn mest mulig anvendbar data vi trengte for å løse problemene. Hadde vi fått ukorrekt data ville det vært svært vanskelig å komme frem til riktig rotårsak om ikke umulig. Datainnsamlingen bestemte kvaliteten for selve analysen som har blitt vurdert. Gruppen har nøye planlagt hvordan dataene skal samles inn for å gjøre en best mulig analyse, og hvilke hensyn vi må ta. Noe informasjon krever spesiell håndtering av hensyn til personvern.
- **Dataanalyse:** Dette steget i prosessen baserer seg på å gjøre analyse og visualisering av dataene som ble samlet inn. Det finnes en rekke diagrammer som kan anvendes på dette området som Pareto Chart og Affinity Diagram. Pareto Chart er et effektivt verktøy for visualisering av årsakenes viktighet og Affinity Diagram kan

brukes til å gruppere relaterte årsaker inn i forskjellige klasser.

- **Rotårsakidentifikasjon:** Om vi hadde funnet riktig rotårsak skulle symptomene opphøre. Eksempler på to verktøy som hører til i denne delen av rotårsaksanalysen er Fishbone diagram og Five Whys. Fishbone diagram baserer seg på visualiseringen av hvilke problemer som resulterer i overliggende problemer og Five Whys går ut på å stille spørsmål til årsaken av et problem gjentatte ganger helt til den underliggende rotårsaken er identifisert.
- **Problemeliminering:** I denne fasen bestemte vi tiltak som skal eliminere rotårsaken. Vi så på de ulike verktøyene og bestemte oss for et verktøy vi mente passet caset best.
- **Løsningsimplementering:** Under løsningsimplementeringen er det er par krav som er viktig at oppfylles. Først og fremst må implementeringen foregå organisert og det må være utviklet en plan for gjennomføring. Verktøy som er naturlig å anvende på dette området beskrives, men vi vil ikke utføre det i denne rapporten, da vi ikke har muligheten til å gjennomføre implementeringen.

2.4 Stegene i problemløsningsprosessen

I boken Root Cause Analysis: Simplified Tools and Techniques [1] s.8 er disse stegene for å løse problemene beskrevet i en detaljert liste som vist under:

1. Erkjenne at det er et problem. Hvis du oppfatter situasjonen som normal, vil det aldri bli bedre.
2. Navngi problemet. Alle som er berørt eller behandler problemet må være enige om definisjonen av problemet.
3. Grundig forståelse av problemets natur, da dette danner grunnlaget som til slutt vil løse det.
4. Finne rotårsaken.
5. Ta tak i og fjerne årsaken, dermed hindre at problemet oppstår igjen.
6. Verifisere at problemet er løst ved å bekrefte at symptomene er borte.

2.5 Verktøy for rotårsaksanalyse

Det finnes utallige verktøy for rotårsaksanalyse. Vi vil gå igjennom de vi har brukt i vår rapport. Alle verktøyene vi har brukt er fra bøkene: **Root Cause Analysis Simplified Tools and Techniques**[1], **The Root Cause Analysis Handbook: A Simplified Approach to Identifying, Correcting, and Reporting Workplace Errors** [7], **Root Cause Analysis: The Core of Problem Solving and Corrective Action**[8]. Alle disse bøkene beskriver hvordan man skal utføre rotårsaksanalyse, men da det kom til utførelse av verktøyene følte vi at **Root cause analysis simplified tools and techniques** skilte seg ut. Her var alle verktøyene godt beskrevet trinn for trinn, man hadde en sjekkliste og det stod beskrevet hva man kunne forvente seg ved bruk av verktøyet. Swim Lane Flowchart var beskrevet i boken The Basics of Process Mapping 2nd Edition på side 6 [9].

2.6 Verktøy for problemforståelse

Problemforståelse er det aller første steget man begynner å jobbe med innen rotårsaksanalyse. Verktøyene i problemforståelsen er ment å gi en bedre forståelse av selve problemet og hvilke aspekter i saken man burde titte nærmere på. For å vite hvilket verktøy man skal bruke på problemet og at man behandler riktig problem, er det viktig at man først forstår hva som er selve problemet. Verktøy vi brukte for å hjelpe oss med dette var:

2.6.1 Swim Lane Flowchart

Swim Lane Flowchart viser flyten av hendelser igjennom et tidsløp og viser forbindelser mellom hendelsene. Diagrammet er delt opp i aktører, hvor hver aktør har sin horisontale bane.

2.6.2 Critical Incident

Hovedformålet med Critical Incident verktøyet er å forstå hva som er de mest plagsomme symptomene i en problematisk situasjon. Ved bruk av Critical Incident skal man få en bedre forståelse av hvilke aspekter av problemet som må løses, samt innse problemets natur og dets konsekvenser. Som med de fleste verktøyene innen rotårsaksanalyse er de best anvendt av et team for å finne årsaken til problemet. For å fungere, krever det en atmosfære av tillit, åpenhet og ærlighet som oppfordrer folk til å røpe viktig informasjon uten å frykte konsekvensene. Dette gjelder alle verktøy men spesielt Critical Incident da denne kan bringe frem potensielt ubehagelige situasjoner.

2.6.3 Performance Matrix

Performance Matrices blir brukt til å illustrere nåværende ytelse og viktighet på samme tid. Dette hjelper med en oppfatning av prioritet. Det brukes til å illustrere problemer eller årsaker i form av hvilken del av problemet som det er det viktigste å angripe samt hvilke problemer, dersom fjernet, vil redusere flest symptomer.

2.7 Verktøy for problemårsaksidemyldring

Denne fasen av rotårsaksanalysen er med på å samle forslag til mulige årsaker av caset. Forslag diskuteres og nye ideer vil kunne bli dannet i løpet av prosessen. Når forslag til et problem blir diskutert og analysert, blir sannsynligheten for at fokus som blir brukt på feil problemer reduseres.

2.7.1 Brainstorming

Brainstorming kan foregå på forskjellige måter, strukturert eller ustrukturert brainstorming og Brain Writing. En strukturert brainstorming baserer seg på at medlemmene etter tur kommer med forslag for å forsikre at ikke en person dominerer prosessen. Ustrukturert brainstorming tillater spontane svar fra hvem som helst i gruppen til enhver tid. Brain Writing kan utføres på to måter. Gruppemedlemmene skriver ned ideene sine på såkalte idekort, eller på en tavle. Under brainstorming er det viktig at ideer og forslag

ikke kritiseres før helt til slutt da alle ideene og forslagene skal gjennomgås.

2.8 Verktøy for datainnsamling

Datainnsammlingsfasen er med på å gjøre søkene etter problemer mer treffsikre. Tilfeldig problemløsning har en tendens til å resultere i antagelser og gjetting mens strukturert rotårsaksanalyse er basert på en systematisk innsamling av gyldige og pålitelige data som er et viktig steg i rotårsaksanalyse. Det er derfor viktig å planlegge nøye hvilke verktøy som en kan tenke seg å anvende.

2.8.1 Intervjuer

Intervjuer anvendes for å få en verbal tilbakemelding fra intervjuobjekt. Det er viktig å være imøtekommende for de som skal intervjues. En god ide kan være å anvende samme stemme under intervjuspørsmålene som under introduksjonen. Når spørsmål stilles bør ikke spørsmålene kunne besvares med bare ja eller nei dersom dette ikke er ønsket. Ha også en intervjuguide ferdiglaget på forhånd. Da har en bedre tid til å passe på at spørsmålene ikke blir tvetydige.

2.8.2 Check Sheet

Check Sheet brukes til å systematisere registrert data som er samlet inn. Hovedformålet er å sikre at alle data som er samlet inn stemmer med virkeligheten. Kan brukes til å registrere frekvensen av hendelser som antas å forårsake problemer.

2.9 Verktøy for dataanalyse

Formålet i denne fasen er å avklare mulige årsaker før man forsøker å løse problemet i siste forberedende stadium. Hvordan er de mulige årsaker knyttet til problematikken, og hva er det som gjør mest skade? Formålet med dataanalysefasen i det siste forberedende stadium før man forsøker å løse problemet, er å avklare mulige årsaker. Det er viktig å se på hvordan forskjellige aspekter av problemet er koblet sammen. I dataanalyse kan følgende verktøy anvendes:

2.9.1 Histogram

Et histogram, også kalt et søyle/stolpediagram, brukes for å vise fordeling og variasjon av et datasett. Dataene kan være skalarer som lengde, diameter, varighet, kostnader, holdninger, etc. Hovedformålet med histogrammet er å synliggjøre presentasjonen av data. Man kan presentere den samme informasjonen i en tabell. Presentasjonformatet er vanligvis det som gjør det lettere å se sammenhenger med dette verktøyet.

2.9.2 Relasjonsdiagram

Relasjonsdiagram er et verktøy som brukes til å identifisere logiske sammenhenger mellom ulike ideer eller problemer i en kompleks og forvirrende situasjon. I slike tilfeller

så er styrken til relasjonsdiagrammet dens evne til å visualisere slike forbindelser. Et relasjonsdiagrams viktigste formål er å bidra til å identifisere forhold som ikke er lett gjenkjennelig.

2.9.3 Affinity Diagram

Et Affinity Diagram hjelper med å korrelere tilsynelatende urelaterte ideer, betingelser, betydninger og årsaker, slik at de kollektivt kan bli utforsket videre. Når man skal analysere kvalitative data så er Affinity Diagram nyttig da den grupperer data og funn av underliggende forhold koblet sammen i grupper.

2.9.4 Statistical Package for the Social Sciences (SPSS)

SPSS (opprinnelig Statistical Package for the Social Sciences) er en kommersiell programvarepakke med grafisk grensesnitt for statistiske beregninger [10]. Vi har brukt brukt versjon 23 for statistisk analyse.

2.10 Verktøy for rotårsakidentifikasjon

Fra listen over mulige årsaker man har opprettet og analysert i løpet av de foregående fire stadier, er man nå klar til å identifisere rotårsaken. Med rotårsaksidentifisering er poenget å utarbeide løsninger som vil fjerne symptomene og dermed eliminere problemet. Når det gjelder varighet og kompleksitet, er dette stadiet sjelden det vanskeligste eller lengste. Med grundig forberedelse, kan man normalt gå gjennom dette stadiet raskt.

2.10.1 Five Whys

Five Whys går ut på å identifisere et problem deretter spørre hvorfor dette er et problem. Da man kommer til et svar så spør man igjen hvorfor. Dette repeteres vanligvis fem ganger til man klarer å komme til rotårsaken.

2.10.2 Fishbone

Fishbone er et verktøy som analyserer et forhold mellom et problem og dets årsaker. Det innehar aspekter fra brainstorming og systematisk analyse for å skape en virkningsfull teknikk. Verktøyets viktigste formål er å forstå hva som forårsaker et problem. Det kan brukes til å utvikle samt gruppere årsaker til et problem. Det vurderer også systematisk årsaker og finner ut hvilke rotårsaker som er mest sannsynlige.

2.11 Verktøy for problemeliminering

Problemeliminering handler om å finne løsninger på problemet ved å fjerne rotårsaken. Fjerner man riktig rotproblem(er) vil symptomene forsvinne sammen med problemet, og ikke gjenoppstå.

2.11.1 Countermeasures Matrix

Countermeasures Matrix er en metode for hjelpe deg å prioritere hvilke tiltak som skal utføres. Prioritet blir etablert ved rangering basert på effekten og gjennomførbarheten av anbefalte tiltak.

2.11.2 Systematic Inventive Thinking (SIT)

SIT baserer seg på å undersøke ett eller flere problemers komponenter. Alle komponentene skal så vurderes ved hjelp av de fem SIT prinsippene[1]. Disse prinsippene er som følger:

1. *Attribute dependency*: vurder om en endring i komponenten vil føre til forbedring.
2. *Component control*: undersøk hvordan komponenten er forbundet med miljøet rundt seg.
3. *Replacement*: bytt ut noe i komponenten med noe fra komponentens omgivelse.
4. *Displacement*: vurder om komponenten kan få økt ytelse ved at en del av komponenten fjernes.
5. *Division*: vurder om splitting av en komponent eller et produkts attributter kan gi forbedring.

2.12 Verktøy for løsningsimplementering

Løsningsimplementering fokuserer på gjennomføringsfasen. Dette steget inkluderer hvordan man bør organisere gjennomføringen av løsningsimplementeringen og hvordan utvikle en implementeringsplan. Vi har ikke kunnet utført løsningsimplementasjoner i vår oppgave, men vi har kommet med forslag til utføring av verktøyene som boken henviser til.

2.12.1 Tree Diagram

Implementeringsprosesser kan være komplisert, men for å bryte ned og organisere arbeidet brukes Tree Diagram til å strukturere aktivitetene. Det er et verktøy som er lett å bruke for å bryte ned større oppgaver i virksomheten til håndterbare størrelser. Tree Diagram er rett og slett en måte å representere en sekvens av hendelser.

2.13 Verktøy vi vurderte, men ikke brukte

Det er veldig mange verktøy man kan bruke innen rotårsaksanalyse men vi har ingen mulighet til å gå gjennom alle disse. På de to første casene vi gjorde, valgte vi selv hvilke verktøy vi mente passet caset og fasen best. For case 3 fulgte vi bokens flowchart. Her brukte vi de verktøyene boken mente var best egnet ut fra informasjon vi hadde. For de casene vi valgte verktøy selv var det også andre verktøy som ble evaluert/diskutert om de egnet seg. Disse er kort beskrevet under:

2.13.1 Spider Chart

Dette er et verktøy noen av gruppemedlemmene hadde jobbet med før i faget "Risikostyring: metodikk og standarder". Et Spider Chart er et godt verktøy der man ser etter ekstern sammenligning. Dette verktøyet er ment å bruke i problemforståelsesfasen. Hovedformålet med Spider Chart er å gi en grafisk fremstilling av resultatene av problemområder sammenlignet med andre organisasjoner. I rotårsaksanalyse er dets viktigste anvendelser å finne ut hva som er det mest kritiske problemet og sammenligne alvorlighetsgraden av problem og årsaker.

2.13.2 Is - Is not Matrices

Is - Is not verktøyet er ment for bruk i fasen for problemårsaksidemyldring. Dens skal hjelpe brukeren å se forskjeller og avklare hva problemet handler om. Hensikten er å gi brukeren en forståelse av mulige problemårsaker samt identifisere problemer som definitivt ikke er relatert til problemet. Ved å sammenligne "Is" med "Is not" kan man raskere finne ut hvilke områder man bør se nærmere på.

2.13.3 Nominal Group Technique (NGT)

NGT som brukes i fasen problemårsaksidemyldring og er en strukturert metode for brainstorming. Den hjelper der det er personer som dominerer. Faren ved at enkeltpersoner dominerer brainstormingen er at de samme personene kan også dominere da ideene skal diskuteres hva som er relevant eller ikke å ta med. Det kan føre til at gruppen kommer frem til minoritetens beslutninger. Den nominelle gruppeteknikken skal legge til rette for en form for brainstorming der alle deltakerne har samme stemme ved valg av løsninger. Dens oppgave er å generere ideer ved å ta med hele gruppen. Og få en samlet oppfatning på hvilke ideer å forfølge videre gjennom analysen.

2.13.4 Paired Comparisons

Paired Comparisons som brukes i fasen problemårsaksidemyldring er et verktøy som tar sikte på å komme til enighet når det gjelder prioritering. Dette gjør den ved å sammenligne f.eks løsninger parvis. Det er ofte enklere å velge mellom et lite antall enn om du samler alle løsningene for så å bestemme hvilken løsning man bør gå for. Verktøyet kan brukes i de tillfeller man må prioritere forskjellige alternativ til problemet eller årsaker.

2.13.5 Surveys

Survey er et verktøy som brukes i datainnsamlingsfasen, dette verktøyet er nyttig da man samler inn data om f.eks folks holdninger, meninger, følelser etc. Hovedformålet med en Survey er å samle inn data fra respondenter. Dette verktøyet er ofte brukt for å samle inn kundetilfredshet relatert til et problem.

2.13.6 Concentration Diagram

Concentration Diagram blir brukt i dataanalysefasen for å avdekke mønstre av et problems forekomst i tilfeller hvor problem oppstår i fysiske systemer og anlegg.

2.13.7 Fault Tree Analysis

Fault Tree Analysis blir brukt i fasen for rotårsakidentifikasjon og er nyttig da man skal portrettere alle mulige årsaker i et diagram og identifisere slike koblinger. Formålet med dette verktøyet er å få en klar oversikt over mulige årsaker som er identifisert samt det å se sammenhengen mellom årsaker eller identifiserte grupper av relaterte årsaker.

2.13.8 Six Thinking Hats

Six Thinking Hats brukes i fasen for rotårsakseliminerings går ut på å oppmuntre folk til å se forskjellige aspekter av et problem. Her har 6 forskjellige personer forskjellige roller ("hatter") de tar på seg som representerer en holdning/synspunkt, som f.eks med den svarte hatten på skal personen være pessimistisk og negativ kontra den som har den den gule hatten som skal være optimistisk og positiv og fokusere hvordan ideen vil fungere og hvordan man skal komme seg forbi utfordringene. Denne teknikken hjelper til med å gjenkjenne hva slags tanker du bruker og oppfordrer deg til å tenke på en annerledes måte. I rotårsaksanalyse brukes dette verktøyet for å vise problemer og løsninger fra ulike perspektiver samt å sike at beslutninger er nøye vurdert før man tar en beslutning.

2.14 Tidligere arbeid med rotårsaksanalyse og informasjonssikkerhet

Innenfor tidligere informasjonssikkerhetsarbeid med rotårsaksanalyse fant vi et fåtall tidligere studier: Vi finner rotårsaksanalyse nevnt i Williams [11] sin modenhetsskala for organisasjoner, hvor han foreslår rotårsaksanalyse som et verktøy for svært erfarene sikkerhetsorganisasjoner, men studien inneholder ingen eksperimenter eller analyser av rotårsaksanalyse-verktøy. Når det kommer til effekt av rotårsaksanalyse, så fant vi en studie utført av Julisch [12]. Hvor forfatteren anvender rotårsaksanalyse til forbedring av beslutningsprosessen for håndtering av alarmer fra intrusion detection systemer. Resultatene i studien viser at det er noen få rotårsaker som utløser over 90 % av alarmene og ved å løse disse så klarte forfatterene å effektivisere håndteringen av alarmer. I denne sammenhengen var rotårsaksanalyse et positivt bidrag, men studien benytter ikke rotårsaksanalyse-verktøy som er foreslått i nyere litteratur og selve rotårsaksanalyse aspektet er nedtonet i studien. I tillegg er dette en svært teknisk studie, hvor den nåværende rotårsaksanalyse litteraturen (for eksempel Andersen og Fagerhaug[1]) er fokusert mot de menneskelige aspekter av en problemårsak, og ikke så mye de tekniske årsakene. I en nyere studie utført av Collmann og Cooper[13] anvendte de rotårsaksanalyse på et informasjonssikkerhetscase som omhandlet brudd på konfidensialitet og integritet i helsesektoren. Basert på den kvalitative tilnærmingen finner forfatterne ut hva som er rotårsaken til en hendelse og foreslår tiltak. Collmann og Coopers resultater viser en klar nytte av å anvende rotårsaksanalyse for å finne frem til rotårsaken. En av ulempene med

deres RCA-tilnærming er at den virker å ikke være standardisert, hvor metodebeskrivelsen er noe fraværende og i stor grad basert på siteringer av tidligere publiserte studier. Wangen [14] benyttet rotårsaksanalyse for å analysere en hendelse relatert til fagfellevurderingsprosessen, hvor en forfatter klarte å utnytte en sårbarhet i prosessen slik at han vurderte sine egne vitenskapelige bidrag. Denne hendelsen ble analysert ved å kombinere rotårsaksanalyse verktøy og «Conflicting Incentives Risk Analysis» for å forstå de forskjellige aktørers underliggende insentiver, samt det å velge mottiltak som adresserer risiko. Vi anser CIRA RCA[14] som en lett modifisert versjon av rotårsaksanalyse, i motsetning til denne oppgaven som vil måle kost-nytte effekten av en fullverdig og standardisert rotårsaksanalyse.

Vår litteraturgjennomgang viser at tidligere arbeid innen rotårsaksanalyse og informasjonssikkerhet er manglende. I tillegg er det et gap i litteraturen når det kommer til å eksperimentere med RCA verktøy for å løse informasjonssikkerhetsproblemer. Denne rapporten sikter seg derfor inn på om standardisert rotårsaksanalyse kan gi en langsiktig løsning for informasjonssikkerhetsproblemer, og om det kan forsvares fra et kost-nytte perspektiv.

3 Valg av metode

Dette kapittelet omhandler valg av metode for å løse de definerte forskningsspørsmålene i kapitel 1. Vi begynner med overordnet vitenskapelig tilnærming til problemene før vi går i dybden for å løse de forskjellige spørsmålene.

3.1 Forskningsspørsmål 1, kost-nytte vurdering

For å løse forskningsspørsmål 1, *Er det kostnadseffektivt å bruke rotårsaksanalyse innen informasjonssikkerhet?* så har vi brukt kost-nytte. Slik som det er vanskelig å fastslå verdien av informasjon, kan det også være vanskelig å bestemme prisen for å beskytte den. Når vi har sett på kost-nytte har vi brukt beskrivelsene av Whitman og Mattord s. 315-316 [15], og tilpasset den til prosjektet. Vi har vurdert kost-nytte basert på kostnad for gjennomføring, tiden det tar å lære seg rotårsaksanalyse samt verktøyene, planleggingen rundt verktøyene og timebruk som er blitt loggført på hvert verktøy.

3.2 Forskningsspørsmål 2, Tabletop

For å løse forskningsspørsmål 2, *Hvordan fungerer rotårsaksanalyse på tabletop øvelse?*, har vi valgt en overordnet kvalitativ tilnærming. Med dette mener vi at vi gjennomfører en tabletop-øvelse hvor vi vurderer kost-nytte. Tabletop vil si at rotårsaksanalysen gjennomføres internt i gruppen basert på innsamlet teknisk dokumentasjon om et case. Caset vi utførte forskningsspørsmål 2 på er: “Carbanak” et avansert angrep utført av en organisert gruppe. Angrepet gikk ut på å få kontroll over nettverket til en finansiell institusjon og deretter tappe dem for penger. Vi tenker oss at vi kommer inn i etterkant av hendelsen og gjør en rotårsaksanalyse for å finne ut om det er underliggende problemer som bidro til at institusjonene ble rammet.

Vi vurderte kost-nytte basert på tid brukt på å gjennomføre hele analysen i tillegg til en kvalitativ nyttevurdering av resultatene.

3.2.1 Case 1, Rotårsaksanalyse metodikk

Vi baserte oss på tilgjengelig teknisk dokumentasjon om caset [16, 17, 18, 19, 20]. Hele caset var basert på åpne kilder. Rapportene ga ikke et fullstendig bilde, så når det var nødvendig gjorde vi antagelser.

Gjennomføring av Swim Lane Flowchart [2.6.1]

Vi startet med å tegne opp et Swim Lane Flowchart. Med dette ønsket vi å få en oversikt over hendelsesforløpet via en grafisk fremstilling. Det ble anvendt brainstorming under utførelsen og den nye informasjonen ble synliggjort hvor den tilhører i tidsperspektivet gjennom hendelsesforløpet.

Gjennomføring av Critical Incident[2.6.2]

Det var ikke mulig å fremskaffe en konkret numerisk frekvens. Derfor ble de numeriske verdiene substituert med variablene Høy, Medium og Lav frekvens. Vi gikk så sammen om

å liste opp det vi så på som sikkerhetshendelser og antok en frekvens på disse hendelsene. Det ble gjort antagelser basert på følgende argumenter:

- Lav frekvens når det skjer månedlig eller sjeldnere.
- Medium frekvens, det skjer ukentlig.
- Høy frekvens, det skjer daglig.

Gjennomføring av Brainstorming [2.7.1]

Her satt gruppen seg ned for å gjøre en idemyldring. Det var viktig å avgjøre om det skulle være ren verbal gjennomførelse eller skriftlig. De tilstedeværende genererte forslag på hva som kunne være problemårsaker og disse ble så listet opp på en tavle.
Da alle forslagene var listet opp var det nødvendig å gruppere enten via tema eller i rekkefølge der rangeringen går fra høyere til lavere potensiale til problemene. Vi valgte å rangere ideene våre fra høyere til lavere potensiale.

Gjennomføring av Intervjuer [2.8.1]

Det var ikke mulig å utføre intervju men vi valgte å skissere det opp sånn som vi så for oss at vi burde gjort det. Vi fant ut av hva vi ønsket å ha data om og hva vi ville spurt om. Vi ville valgt å intervjue rundt 20 personer, av disse burde 4-5 personer være med administrasjonsrettigheter eller andre i lederposisjoner. Vi regnet med at intervjuene ville tatt omlag en time per intervju. Vi ville etterspurt logger bedriften sitter på.

Gjennomføring av Relasjonsdiagram [2.9.2]

Det ble tegnet en stor sirkel på tavlen. Deretter begynte vi å liste opp elementer vi så på som viktige og overordnede nok og plasserte disse rundt sirkelen. Deretter tegnet vi relasjonene mellom elementer ved piler basert på informasjonen vi hadde hentet inn fra de to tidligere fasene. Vi ser på det som naturlig at det er diskusjon under utførelsen av dette verktøyet.

Gjennomføring av Affinity Diagram [2.9.3]

Under gjennomførelsen av Affinity Diagram, ble en rekke punkter generert ut fra de to tidligere fasene, og disse ble diskutert grundig. Punktene var fysisk plassert på en tavle under diskusjon, og ble så ført inn i et dataprogram hvor det var virtuelle lapper på en tavle. Kolonner som ikke var navngitt fra starten ble fylt tilfeldig med punktene vi genererte på tavlen. Så kunne hver person på sin egen maskin flytte disse lappene rundt til alle var enige om plasseringene. Deretter fikk gruppene navn ut fra hvilke lapper som befant seg i hver av dem.

Gjennomføring av Five Whys [2.10.1]

Vi avgjorde startpunktet for analysen. I vårt tilfelle startet vi med “Hvorfor spytter minibanken ut penger?”. Vi skrev dette opp på tavlen og brukte verktøyet Brainstorming for å finne årsaken til startpunktet. Her er poenget å spørre hvorfor? Vi genererte et svar vi mente var sannsynlig, og igjen spurte hvorfor. Dette ble repetert til vi fant fram til en rotårsak, det tar vanligvis rundt fem “hvorfor?” før man finner en rotårsak. Dette er kun en antagelse siden vi ikke hadde noen personer fra det aktuelle caset å spørre.

Gjennomføring av Countermeasures Matrix [2.11.1]

Vi tok utgangspunkt i funn fra tidligere faser og plasserte disse så inn i en matrise for å kunne anta effekt og gjennomførbarhet. Vi antar effekt og gjennomførbarhet på vektene 1 til 5 hvor 1 er lav og 5 er høy basert på funn fra tidligere faser i analysen.

Vektene i matrisen beregnes slik: $\mathtt{Effekt} \times \mathtt{Gjennomførbarhet} = \mathtt{Total}$
Dersom totalen er mer enn 10, blir det sett på som et godt alternativ for implementering.

Gjennomføring av Tree Diagram [2.12.1]

Først genererte vi en liste over aktiviteter som måtte utføres for å implementere løsningen. Vi skrev ned hver aktivitet, i form av et verb etterfulgt av et substantiv. Deretter rangerte vi aktivitetene i logiske undergrupper med aktiviteter som utføres i rekkefølgen de plasseres. Det siste vi gjorde var å sette sammen undergrupper i en samlet sekvens for å illustrere hele planen av Tree Diagram.

3.3 Forskningspørsmål 3, mye ressurser og tid

For å løse forskningsspørsmål 3, *Hvordan fungerer rotårsaksanalyse på et case med mye ressurser og tid?*, har vi valgt en overordnet kvalitativ tilnærming med en hybrid variant av kvantitativ + kvalitativ datainnsamling og på analysen ble det brukt statistikk. Med dette mener vi at vi gjennomfører et case vi fikk av IT-tjenesten der vi har mye ressurser og tid. Mye tid og ressurser vil si at vi gjennomfører alle stegene selv internt i gruppa, vi samler inn all data og analyserer med SPSS. Det vil ikke bli gjort antagelser. Caset vi utførte på forskningsspørsmål 3 er: Hvorfor deler ansatte og studenter adgangskortet sitt.

Vi vurderte kost-nytte basert på tid brukt på å gjennomføre hele analysen i tillegg til en kvalitativ nyttevurdering av resultatene.

3.3.1 Case 2, rotårsaksanalyse metodikk

Vi baserte oss på informasjon som vi selv hentet ut med verktøyene fra rotårsaksanalyse.

Gjennomføring av Performance Matrix [2.6.3]

Her pratet vi med IT-Tjenesten om nåværende ytelser og viktigheten av ytelsene, for å vite hvilken del av problemet det var viktigst å angripe først og hvilket problem som vil redusere flest symptomer. Da vi hadde fått informasjonen vi trengte fra IT-Tjenesten startet vi på stegene som beskrevet i nedenfor:

1. Først lagde vi tomt et diagram ved å plassere viktigheten på den horisontale aksen og nåværende ytelse på den vertikale aksen som hver er delt opp i ni like segmenter.
2. Deretter bestemte vi hvilke faktorer å analysere.
3. Vi plasserte hver faktor i diagrammet i henhold til sin posisjon langs de to aksene, ved hjelp av symboler for å identifisere hver faktor. Det å plassere faktorene inn på rette plass bør gjøres av noen som kjenner til problemet godt fra før. I vårt tilfelle gjorde vi dette selv før vi gikk til IT-Tjenesten for å bekrefte om vi hadde oppfattet rett. Etter IT-Tjenesten fikk se verdiene i diagrammet vi hadde så ble de justert.
4. Etter at alle faktorer var plottet inn i diagrammet, delte vi diagrammet i fire kvadranter omtrent på midten av hver akse. Hvert kvadrat fikk et eget navn: Overdrevet,

Uviktig, Ok og Må forbedres. Hvis mange faktorer var samlet på ett område, plasserte vi linjene litt lenger til en side.

5. Til slutt bestemte vi hvilke faktorer som var innenfor rett kvadrat.

Gjennomføring av brainstorming [2.7.1]

En ustrukturert brainstorming ble utført på mulige årsaker til at personer ved skolen ønsker å låne og låne bort kort til andre, og hvilken konsekvens dette har. Hvert gruppemedlem kunne til enhver tid komme med forslag som ble notert på en tavle. Når ingen var i stand til å utarbeide flere forslag, ble forslagene gjennomgått. Vi fjernet forslag vi mente ikke var relevante. Alle forslagene ble sortert i 2 grupper, "årsaker" og "konsekvenser".

Gjennomføring av Intervjuer [2.8.1]

Intervjuer ble gjort med 36 ansatte og studenter ved NTNU i Gjøvik. Intervjuene ble gjennomført på grupperom eller på intervjuobjektenes kontor. Foruten IT-Tjenesten og management var utvelgelsen av intervjuobjekter vilkårlig. Innenfor de to førstnevnte valgte vi ut nøkkelpersonell i form av beslutningstagere, policy-forfattere og ansvarspersoner i drift av adgangskontroll. Vi knyttet spørsmålene vi stilte til vår "Performance Matrix". Dette er beskrevet i detalj i resultatkapittel **??**.

Gjennomføring av Histogram [2.9.1]

Da vi analyserte intervjuene satt vi svarene inn i SPSS som genererte histogram slik at vi kunne se forskjeller mellom de ulike intervjuobjektene.

Gjennomføring av statistisk analyse [2.9.4]

IBM SPSS ble brukt for dataanalyse og baserte seg på metodikken beskrevet i "An Initial Insight Into InfoSec Risk Management Practices" [21]. Dataen vi samlet inn ble plottet inn i IBM SPSS som er en programvare for statistisk analyse. Vi brukte en rekke statistiske dataanalyseverktøy de verktøyene vi benyttet i denne forskningen er som følger: Når vi utførte Descriptive (beskrivende) analyse har vi vurdert distribusjon inkludert intervall og standardavvik. På graderte svar, brukte vi mål for sentraltendens (gjennomsnitt), median og modus. Vi har også utført univariat analyse av enkeltspørsmål, og bivariat analyse av to variabler, for å se hvordan de kan sammenlignes og samhandler (gjennomsnitt og standardavvik). Vi har brukt Statistisk inferens for å forutsi og bestemme betydning. Analysen har operert med et 95% standard konfidensintervall på ANOVA for testing av statistisk signifikans. Vi har utført post hoc tester av typen Turkey for å analysere videre statistisk signifikante resultater mellom par og avdekke sammenhenger mellom variabler.

Intervjuene hadde også flere åpne spørsmål. Disse har vi behandlet ved å liste og kategorisere svarene. Videre telte vi forekomsten av hvert emne og oppsummerte svarene.

Gjennomføring av Affinity Diagram [2.9.3]

Da vi spurte intervjuobjektene om forslag til tiltak for å redusere låning fikk vi mange forskjellige svar, disse ble gjort uniforme og samlet i 26 kategorier. Videre brukte vi Affinity Diagram verktøyet for å kategorisere forslagene inn i 6 hovedgrupper.

Gjennomføring av Fishbone diagram [2.10.2]

Hovedproblemets årsaker skal undersøkes, og hva som skaper disse årsakene skal identifiseres. Deretter sorteres og grupperes årsakene til tilhørende problemer. Fishbone Diagramet utførte vi i 3 steg der:
Steg 1: Problemet beskrives ved at adgangskort blir lånt mellom ansatte, studenter og mellom disse to gruppene.
Steg 2: Brainstorming der fokuset var å finne mulige årsaker.
Steg 3: Her gikk gruppen sammen om å velge forslag vi mente burde være med videre i prosessen. Hovedkategoriene ble tegnet i Fishbone diagrammet.

Gjennomføring av SIT[2.11.2]

SIT ble utført i 5 steg:
Steg 1: Samlet inn personell med relevant kunnskap. Dette var ikke gjennomførbart for oss og vi fortsatte derfor med vår gruppe.
Steg 2: Listet og grupperte komponenter. Her skrev vi ned rotårsakene fra rotårsaksidentifiseringen Da dette var gjort listet vi alle elementer som tilhørte problemet og sorterte de i grupper hvor hver gruppe fikk et eget navn.
Steg 3: Brukte vi de fem SIT prinsippene. Alle komponenter fra steg 2 ble kandidater for videre undersøkelse.
Steg 4: Diskuterte vi hvilke alternativer som er realistiske å anta at kan gjennomføres.
Steg 5: Utdypet de mest lovende ideene og utviklet løsninger.

Gjennomføring av Tree Diagram [2.12.1]

Tree Diagram ble utført i 4 steg, stegene var:
Steg 1: Genererte liste over aktiviteter som må utføres for å få gjennomført løsningen.
Steg 2: Skrev ned aktivitetene helst via ett verb og ett substantiv (Verktøyet er beskrevet på engelsk, og derfor kan det bli vanskelig å følge reglene ordrett på steg 2.)
Steg 3: Arrangerte aktivitetene i naturlige undergrupper som viser hvordan implementeringen skulle utføres i sekvens innad i gruppene.
Steg 4: Plasserte de arrangerte undergruppene i diagrammet.

3.4 Forskningsspørsmål 4, begrenset med ressurser og tid?

For å løse forskningsspørsmål 4, *Hvordan fungerer rotårsaksanalyse på en case med begrenset ressurser og tid?*, har vi valgt en overordnet kvalitativ tilnærming, med dette mener vi at vi gjennomfører et case med begrenset tid og ressurser til rådighet hvor vi vurderer kost-nytte. På dette forskningsspørsmålet brukte vi case 3 som vi mottok fra slettmeg.no der de hadde opplevd et DDoS angrep. Dette førte til at sider som slettmeg.no, norsis.no, sikkert.no og idtyveri.info ble utilgjengelig under angrepet. Vi vurderte kost-nytte basert på tid brukt på å gjennomføre hele analysen i tillegg til en kvalitativ nyttevurdering av resultatene.

3.4.1 Case 3: Rotårsaksanalyse metodikk

Vi baserte oss i hovedsak på Flow Chart fra boken Root Cause Analysis Simplified Tools and Techniques [1] i kapitel 10 som heter “How to select the right tool”

Gjennomføring av Swim Lane Flowchart [2.6.1]

Vi startet med å tegne opp et Swim Lane Flowchart. Her ble anmeldelsen av tjenestenektangrepet fra NorSIS brukt til utførelsen av Swim Lane Flowchart.

Gjennomføring av Critical Incident [2.6.2]

Verktøyet var beskrevet i 5 steg i hovedlitteraturen.
Steg 1 : Fortalte oss at nøkkelpersoner skal delta.
Steg 2 : Forteller videre at deltagerne skal sekvensielt skrive ned lapper med hva som var vanskeligst å behandle samt hva som var de største problemene. Grunnet begrenset tid lagde vi heller noen spørsmål som vi stilte dem og mottok verbale svar på.
Steg 3 : Svarene på lappene analyseres ut fra frekvens. Det var ikke mulig å telle frekvens.
Steg 4 : Var å gi en grafisk fremstilling, hvor vi valgte å fremstille de tre punktene i listeformat.
Steg 5 : Anvendte de hendelsene med høyest frekvens videre i analysen. Vi tok derfor med oss informasjonen om hva som var viktigst for slettmeg.no videre i vår analyse.

Gjennomføring av Performance Matrix [2.6.3]

Her snakket vi med vår kontaktperson hvor vi utarbeidet punkter på nåværende ytelse og viktighet hos slettmeg.no.

Gjennomføring av brainstorming [2.7.1]

Vi brukte ustrukturert brainstorming. Gruppen anvender en tavle til å skrive ned ideene på. Det ble generert en liste med mulige årsaker til problemet som igjen ble gjennomgått og kategorisert etter viktighet.

Gjennomføring av Check Sheet [2.8.2]

En brainstorming fase ble anvendt til å generere problemer og problemsituasjoner som hendte under angrepet og i etterkant. Punktene ble diskutert med vår kontaktperson hos slettmeg.no. Vanskeligheten med å rangere problemene i listen ble løst med diskusjon av hvert punkt og må derfor fremstilles med en kvalitativ presentasjon fremfor en kvantitativ frekvens av hendelsene.

Gjennomføring av SIT[2.11.2]

Her blir stegene for gjennomførelsen av rotårsaken beskrevet. Gruppen trengte å samle nøkkelpersoner men det var ikke gjennomførbart i vårt tilfelle. Deretter listes komponenter til problemet. Hver komponent som var realistiske å behandle videre i analysen ble valgt. Deretter anvendes de 5 SIT prinsippene på hver av komponentene som ble valgt. Ideene som virker best egnet til videre arbeid ble valgt ut. De utvalgte ideene utdypes deretter valgte vi ut de mest lovende komponentene og genererte løsningsforslag.

4 Resultater

I dette kapittelet presenterer vi våre resultater ved å beskrive caset og vise til hvilket forskningsspørsmål som caset svarer til. Resultatene fra hvert av de 7 stegene i fossefallsmodellen modellen, figur 2, presenteres for hver av de tre casene: (i) Tabletop case: Carbanak, (ii) Adgangskort case, (iii) Slettmeg DDoS case.

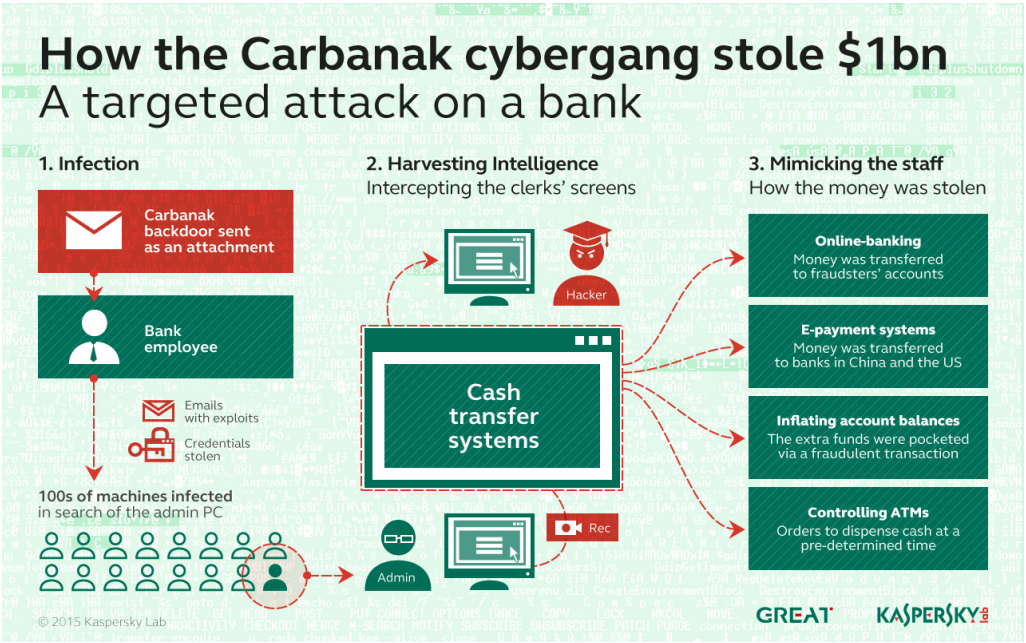
4.1 Case 1 - Carbanak

Caset ble gjennomført som en tabletop oppgave for å kunne gi svar til forskningsspørsmålet: *Hvordan fungerer rotårsaksanalyse på tabletop øvelse?*

Caset omhandlet Carbanak som er et avansert angrep utført av en organisert gruppe. Angrepet går ut på å få kontroll over nettverket til en finansiell institusjon og deretter tappe dem for penger. Vi baserte oss på informasjon fra Kaspersky[16], to artikkler fra Brian Krebs[17][18], artikkelen Anunak: APT against financial institutions [19] samt YouTube klipp[20]. Hele caset ble basert på åpne kilder. Kildene ga ikke et fullstendig bilde, så når det var nødvendig gjorde vi antagelser for å fylle gapene. Vi har presisert hvor vi har gjort antagelser i caset. Vi tenkte at vi kom inn i etterkant av hendelsen og gjorde en rotårsaksanalyse for å finne ut om det er noen underliggende problemer som bidro til at institusjonene ble rammet av angrepet.

De fleste av ofrene var lokalisert i Russland ifølge Carbanak the Great Bank Robbery av Kaspersky Labs [16] side 4. Videre forteller Kaspersky i sin rapport at bankene som var utsatte hadde kumulativt tap på opptil en milliard dollar, og at angriperne oppfører seg som en Advanced Persistent Threat (APT) [22]. Bankansattes arbeidsstasjoner ble overvåket ved at tastetrykk ble logget og skjermbilder ble tatt hvert tjuende sekund [16] som ble sendt til angriperne. Angrepet var basert på spear phishing [18] via e-post med infiserte dokumenter som utnyttet sårbarheter i Microsoft Office. Det eksisterte patcher som ikke var lagt inn [17].

Bildet viser oversikt over utførelsen av angrepet 3 og er hentet fra The Great Bank Robbery: the Carbanak APT [2].



Figur 3: Bilde er laget av Kaspersky [2]

4.1.1 Problemforståelse

For å få bedre problemforståelse så valgte vi Swim Lane Flowchart [2.6.1] som skal gi en oversikt over hendelsesforløpet. Critical Incident [2.6.2] ble anvendt for å finne det mest problematiske symptomet.

Swim Lane Flowchart

Ønsket utbytte var å synliggjøre flyt mellom hendelser og avsløre forbindelser mellom elementer i diagrammet som ikke ellers ville vært lett synlig.

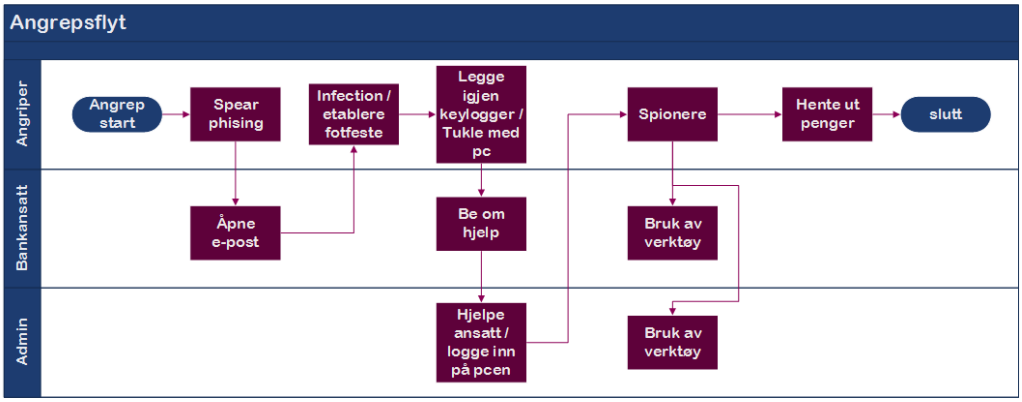
Resultatet ble et diagram delt inn i 3 forskjellige baner med rollene angriper, vanlig bruker som er en typisk bankansatt og til slutt administrator som i diagrammet er kalt admin. Utførelsen av verktøyet viste at angrepet var introdusert inn i banken via spearphising e-post, og handlingsmønsteret mellom angripere, typiske ansatte og administratorer.

Elementene i Swim Lane Flowchart

Her følger en beskrivelse av elementene i Fig: 4.

1. *Login* Her ser vi for oss at angriperne allerede har fått malware lastet inn på en av maskinene til banken og er i stand til å aksessere en brukerkonto.
2. *PC* Dette er en av arbeidsstasjonene og er bankens eiendel. Det er her ansatte åpner infiserte e-poster.

3. *E-post* Her tenker vi på e-poster generelt, hvor angriperens infiserte e-postvedlegg befinner seg.
4. *Verktøy* Administrative verktøy som anvendes av ansatte. Dette inkluderer ikke bare bankens generelle brukere men også administratorer sine verktøy.
5. *Generell administrasjon* Er en anvendelsen av verktøy eller ren administrering av bankansattes oppgaver.
6. *Minibank* Dette er både minibankene som fysisk er lokalisert rundt om i landene samt programvaren som administrerer minibankene.
7. *Penger* Pengene som er i flyt fra banken og i retning angriperne.
8. *Angriper* Carbanaks bakmenn.



Figur 4: Carbanak illustrert i form av et Swim Lane Flowchart

Critical Incident

Verktøyet ble brukt i jakten på å finne de mest problematiske hendelsene i en problem situasjon. I diagrammet ble hendelser målt på frekvens.

Ønsket utbytte var en visuell fremstilling av rangering etter frekvens for å få et riktig inntrykk av viktighetsgraden til elementene.

Under følger en beskrivelse av rangeringen anvendt i tabell: 1.

1. *Høy* Inntreffer daglig.
2. *Medium* Ukentlig.
3. *Lav* Månedlig eller sjeldnere.

Vi fant ut at hendelser som foregikk oftest var mistenkelig trafikk, overvåking av maskiner, åpning av e-post vedlegg og brudd på regelverk.

4.1.2 Problemårsaksidemyldring

Målet var å generere en liste med problemer som kunne forbedres og identifisere mulige konsekvenser som stammet fra problemet som ble analysert.

Hendelse	Frekvens
Mistenkelig trafikk	Høy
Overvåking av maskiner	Høy
Åpning av e-post vedlegg	Medium
Brudd på regelverk	Medium
Utro tjenere	Lav
Angripere har tilgang på servere	Lav
Ikke oppdaget infeksjon på IT systemer	Lav
Uvitenhet om spionprogramvare	Lav
Uopplærte medarbeidere	Lav

Tabell 1: Tabell som viser Critical Incident for Carbanak

Brainstorming

Grupperingen ga oss muligheter til å kunne gjøre antagelser på hvilke elementer som ga konsekvenser innenfor samme problemområde. Fordeler ved bruk av dette verktøyet var derfor å finne, samt å få en oversikt over problemene.
Kunnskapen om hvilke elementer som hadde relasjoner med hverandre ble skapt.

1. Opplæring og oppfølging av ansatte.
    - Manglende sett med retningslinjer eller manglende oppfølging av disse.
    - Mangelfull opplæring av ansatte.
    - Dårlig oppfølgelse av opplæring.
    - For skjedent bytte av passord.
2. Svakheter.
    - Manglende oppdatering av programvare/patching.
    - Manglende etablering av baseline.
    - Manglende varsling på mistenkelig aktivitet.
    - Sen reaksjon på at minibanker ble tømt for penger.
    - Virus eller malware (skadelig programvare).
3. System-og nettverksovervåking.
    - Tillatt ukjent inn/ut trafikk av nettverket.
    - Lite overvåking av nettverkstrafikk (inn/ut).
    - For lite gjennomgang loggføring.
    - For liten kontroll av ressursbruk på IT systemer.
    - Dårlig segregering av maskiner i nettverk.
    - Vedlegg blir ikke filtrert godt nok.
4. Bedriftstrusler.
    - Utro ansatte.
    - Bedriftspionasje.
    - Fysisk tilgang til maskiner og minibanker.
    - Særs ressurssterk angriper.

4.1.3 Datainnsamling

Ønsket utbytte var informasjon om:

1. Bedriftens indre miljø.
2. Informasjon som kan avdekke utro ansatte eller korrupsjon.
3. Bankenes rutiner og etterfølgelse av disse.
4. Installerte versjoner av programvare da malwaren utnyttet sårbarheter som ikke var oppdaterte.

Intervju

Det var ikke mulighet å gjennomføre intervjuer da vi ikke hadde tilgang til nøkkelpersoner som var involvert i caset. I rapporten [appendix A 6.3] ble det generert lister over data vi ville hentet ut, hvilke spørsmål vi ville spurt administratorer og spørsmål vi ville stilt til andre ansatte.

4.1.4 Dataanalyse

Relasjonsdiagram og Affinity Diagram [2.9.3] ble anvendt til å analysere dataene som var innsamlet.

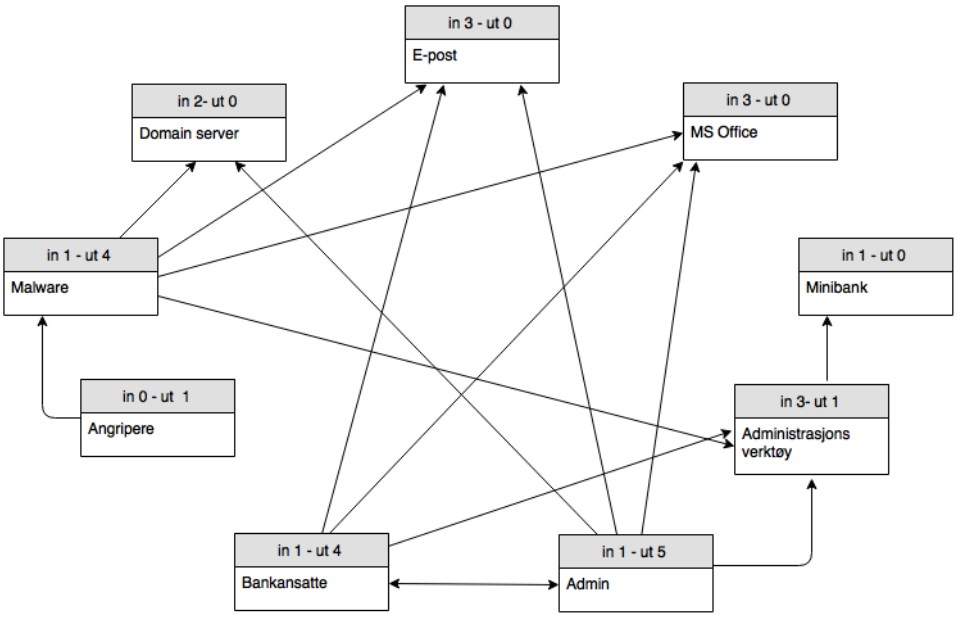
Relasjonsdiagram

Relasjonsdiagrammet 5 viser relasjoner mellom viktige elementer i angrepets tidsløp. Elementene er utarbeidet fra de tidligere fasene.

Elementene vi kom frem til var:

1. Angripere.
2. Malware.
3. Domain server.
4. E-post.
5. MS Office.
6. Minibank.
7. Administrasjonsverktøy.
8. Admin.
9. Bankansatte.

Punktene ble valgt da de representerer hovedsettet med elementer som inngår i angrepet.

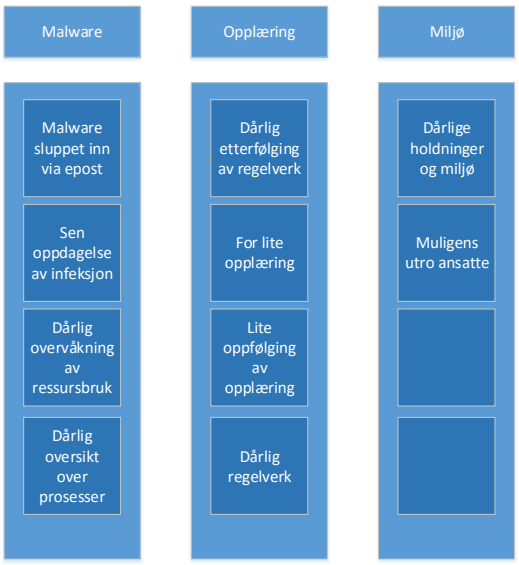


Figur 5: Relasjon mellom angriper og interne elementer

Resultatet var en tydeligere visualisering over hvilke maskiner og mennesker som har forbindelser med hverandre, i motsetning til Swim Lane Flowchart som viser hendelsesforløpet over tid.

Affinity Diagram

Affinity Diagrammet 6 viser tre overordnede grupper hvor problemene har blitt fordelt inn under.



Figur 6: Affinty diagram som viser grupperte årsaker.

Verktøyet gjorde det mulig å få et nytt og bedre bilde av situasjonen og alle elementene vi hadde generert og samlet inn. Informasjonen vi endte opp med var mer redusert og raffinert enn den vi satt med fra tidligere faser. Ut fra dette var det ikke stor endring i vår forståelse av situasjonen. En bedre oversikt ble oppnådd da vi fikk gruppert relaterte årsaker inn i klassene “Malware”, “Opplæring” og “Miljø”.

4.1.5 Rotårsaksidentifikasjon

Her ble det brukt Five Whys vist i figur 2 [2.10.1] til å lete etter rotårsak.

Five Whys

Spørsmålet det ble startet med var “Hvorfor spytter minibanken ut penger?”
I tabellen er hvert spørsmål vist til venstre, og svar vist til høyre.

Minibanken spyttet ut penger.	
Hvorfor?	Fordi systemet var kompromittert
Hvorfor?	Fordi angriperene utnyttet en exploit da ansatte åpent mail
Hvorfor?	Fordi programvaren ikke var up to date.
Hvorfor?	Fordi banken hadde dårlige/mangelfulle rutiner på oppdatering.
Hvorfor?	Ble ikke vurdert til å være kritisk nok

Tabell 2: Five Whys, startende med hvorfor spyttet minibanken ut penger.

Vi var i stand til å lande på det vi mener er en rotårsak. Det er ikke synlig om andre årsaker kan være rotårsaker. Verktøyet fungerte svært effektivt og det tok kort tid å nå et resultat.

4.1.6 Rotårsakseliminering

En Coutermeasure Matrix vist i figur 3 [2.11.1] blir anvendt til å å finne hva som best eliminerer årsakene til problemene samtidig som kostnad og risiko blir tatt hensyn til.

Countermeasures Matrix

Vektene i matrisen regnes slik: $\mathtt{Effektivitet x Gjennomførbarhet} = \mathtt{Total}$
Dersom vekten er mer enn 10, blir det sett på som et godt alternativ for implementering.

Tiltak	Effektivitet	x Gjennomførbarhet	= Total	Utføre tiltak
Oppdatering	4	5	20	Ja
Patching	4	5	20	Ja
Auto-updates	4	2	8	Nei
Opplæring	2	5	10	Ja
Baseline	4	3	12	Ja
Monitorering	4	4	16	Ja
Stenge banken midlertidig	2	1	2	Nei
Spore angrep tilbake	2	1	2	Nei
Oppgradere legacy systemer	5	2	10	Nei
Sandboxing	3	3	9	Nei
Test miljø	4	3	12	Ja
Gjennomgang av logg	3	5	15	Ja
Scan av e-post	3	4	12	Ja

Tabell 3: Countermeasures Matrix som viser mulige løsninger på problemet.

Selv om resultatet av tiltaket *Oppgradere legacy systemer* var på 10 valgte vi å sette "Nei" for å utføre dette tiltaket. Dette fordi vi ikke ser det som realistisk når det kan medbringe konsekvenser på nærliggende systemer ved at deler av bankens programmer blir skiftet ut.
Vi hadde ingen mulighet til å gå inn å monitorere effekten hos bankene eller se om problemet ble løst. Derfor ble de neste stegene av verktøyet som beskrevet i The Root Cause Analysis Handbook [7] ikke gjennomførbare:

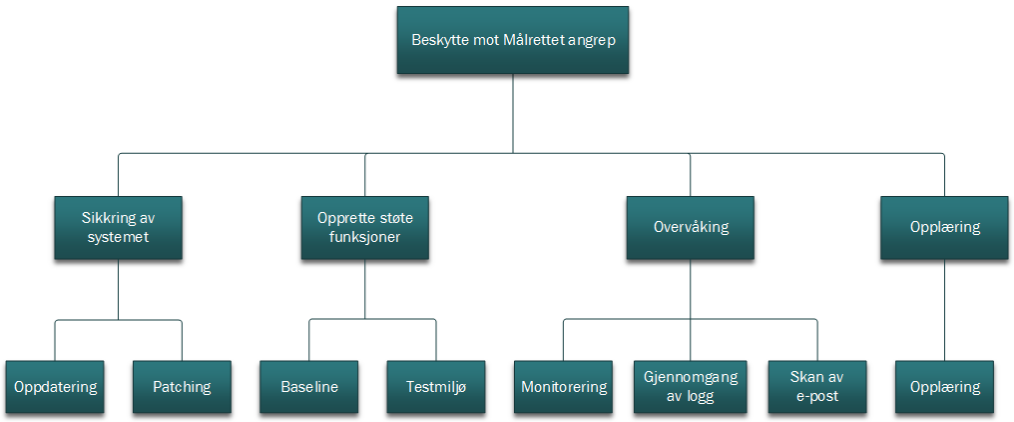
1. Report recommended corrective action(s), as appropriate.
2. Standardize to prevent the problem from recurring.
3. Communicate results, as appropriate.
4. Take additional actions as appropriate.

4.1.7 Løsningsimplementering

I løsningsimplementeringen ble det brukt et Tree Diagram 7 for å lage en struktur av oppgavene som skulle utføres for å implementere vårt løsningsforslag. Vi håpet å vise linker mellom det som skulle gjøres og hvilken aktivitet det ble forbundet med. Tree Diagram er beskrevet i kapittel 2.12.1.

Tree diagram

Aktivtetene som skulle gjennomføres er listet opp i form av et verb etterfulgt av et substantiv. Disse er plassert i grupper:



Figur 7: Carbanak Tree Diagram som viser en plan for å gjennomføre tiltak.

4.1.8 Case 1 tidsbruk

Den totale tiden brukt på case 1 er omtrent 100 timer per person (300 timer).

Tidsbruk

Tabell 4: Loggføring

Loggføring av tidsbruk på verktøyene		
Fase	**Verktøy**	**Tidsbruk t=timer m=minutter**
Forberedende fase	Læring av RCA	150 timer
Forberedende fase	Innsamling og kartlegging av data	100 timer
Forberedende fase	Testing og valg av verktøy	24 timer
Problemforståelse	Critical Incident	3t15m
Problemårsaksidemyldring	Brainstorming	2t30m
Datainnsamling	Interjuv	3t
Dataanalyse	Relasjons Diagram	6t
	Affinity Diagram	4t
Rotårsaksidentifisering	Five Whys	1t
Løsningsimplementering	Countermeasures Matrix	3t
Problemeliminering	Tree Diagram	3t30m
		Total 26t 15m

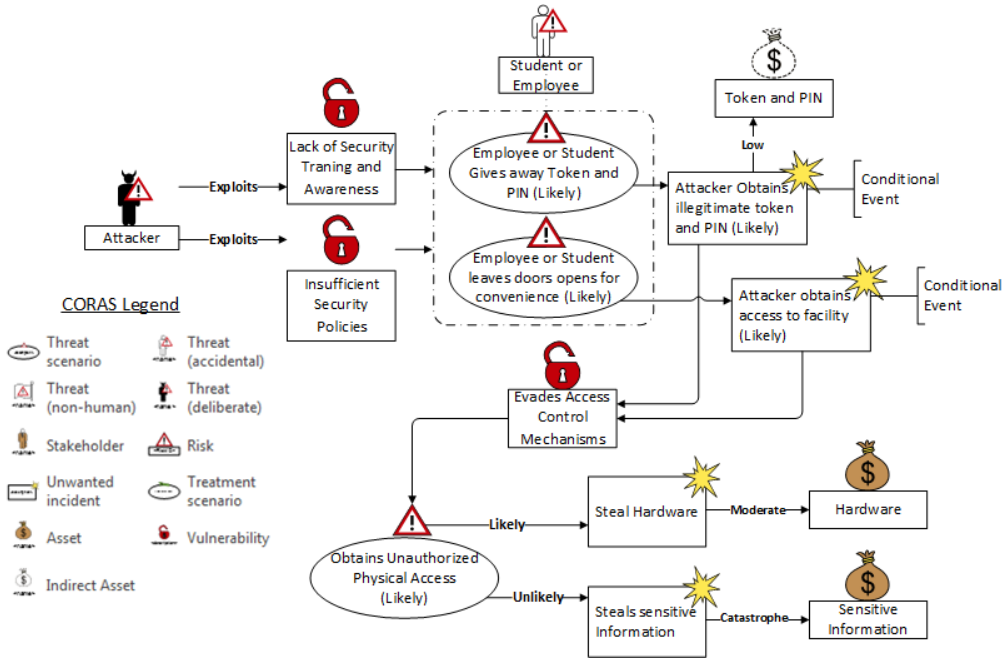
4.2 Case 2 - Adgangskort

I dette caset har vi sett på hvorfor ansatte og elever låner bort adgangskortet sitt, samt om det er mulig å finne en rotårsak som kan fjerne behovet for å bruke andres adgangskort. Oppgaven har vi fått av IT-tjenesten ved NTNU i Gjøvik og er:
"PIN og adgangskort skal være privat, men det hender ofte at studenter og ansatte allikevel deler disse med familie, venner, kolleger og andre studenter. Dette fører til at urettmessig tilgang blir gitt til NTNU i Gjøviks fasiliteter. Dette er et gjentagende problem som forekommer flere ganger i året, og IT-tjenesten har fått rapportert inn hendelser relatert til dette. Det er også sannsynlig at det er flere uoppdagede risiko trusler relatert til dette."

Caset er ment for å hjelpe oss med å gi svar på forsknings spørsmålet: *Hvordan fungerer rotårsaksanalyse på en case med mye ressurser og mye tid?*.

Oversikt over situasjon

Vi så på situasjonen som illustrert i figure number 8; en angriper utnytter at en student eller ansatt låner bort kort og pin eller de etterlater en dør åpen. Dette kan skyldes mangel på sikkerhetstrening eller kjennskap til policy samt at policy ikke nødvendigvis tydelig nok viser til at dette ikke er akseptabelt. Dersom student eller ansatt gir bort kort og pin eller glemmer å lukke dører, vil angriper kunne unngå byggets innebygde sikkerhetstiltak og få adgang til maskinvare eller sensitiv informasjon.



Figur 8: Oversikt over situasjonen. Tegningen er laget i samarbeid med vår veileder. Laget med CORAS [3]

4.2.1 Problemforståelse

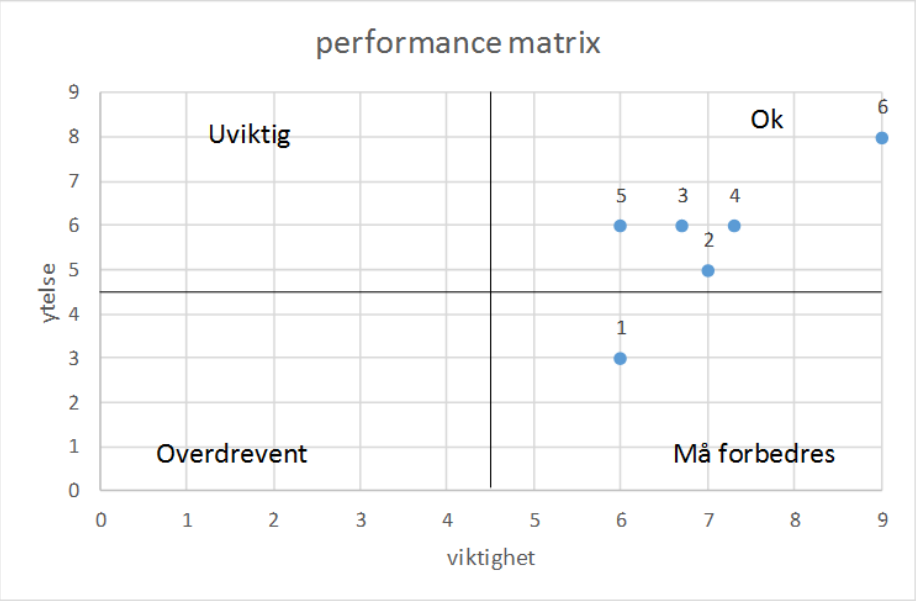
For å få bedre problemforståelse så valgte vi Peformance Matrix [2.6.3] som skal hjelpe med å finne ut hvilke problemer som er viktig å angripe.

Performance Matrix

Spørsmålene vi stilte til IT-tjenesten er listet under. Svarene er gradert fra 1 til 9 hvor 1 er lavt rangert og 9 er høyt rangert.

1. Teoretisk sikkerhetspolicy (hvor godt kjent er folk med policy: gammel og ny).
    1. Viktigheten: Hvor viktig er det at folk er kjent med den? Svar: 6.
    2. Nåværende ytelse: Hvor mange kjenner til den? Svar: 3.
2. Praktisk sikkerhetspolicy (hvor godt den er implementert i organisasjonen).
    1. Viktigheten: Hvor viktig er den? Svar: 7.
    2. Nåværende ytelse: Hvordan fungerer den nå? Svar: 5.
3. Sanksjoner/konsekvenser på brudd på policy.
    1. Viktigheten: Hvor viktig er sanksjoner/konsekvenser? Svar: 7.
    2. Nåværende ytelse: Hvor godt fungerer sanksjoner/konsekvenser? Svar: 6.
4. Sikkerhetskultur.
    1. Viktigheten: Hvor viktig er det med god sikkerhetskultur? Svar: 7.
    2. Nåværende ytelse: Hvor bra sikkerhetskultur er det? Svar: 6.
5. Reserveløsninger for kortutdeling ved glemt kort/besøkende.
    1. Viktigheten: Hvor viktig er det med reserveløsninger? Svar: 6.
    2. Nåværende ytelse: Hvor godt er det fungerende? Svar: 6
6. Kortutdeling ved nyansettelse.
    1. Viktigheten: Hvor viktig blir dette sett på? Svar: 9.
    2. Nåværende ytelse: Hvor godt fungerende er det? Svar: 8.

I figur 9 er nummereringen til punktene tilsvarende spørsmålene i listen over.



Figur 9: Performance Matrix som viser viktighet og ytelse.

4.2.2 Problemårsaksidemyldring

I denne fasen av rotårsaksanalysen måtte vi samle forslag til mulige årsaker av caset. Verktøyet vi benyttet oss av var brainstorming 2.7.1.

4.2.3 Brainstorming

Årsaker til at ansatte/studenter ved NTNU i Gjøvik velger å låne bort adgangskort med eller uten pin:

Årsak til lån av adgangskort	
"Privilage escalation" for å komme seg inn på rom.	Spionasje, sabotasje, planting av bakdører, kjennskap til infrastruktur
Glemt kortet.	Stoler på vedkommende.
Gi venner og bekjente tilgang til treningsrom.	Flaut/vanskelig å si nei.
Låne til kopimaskin.	Ta eksamen for andre.
Bruk av ansatt-toalett.	Hente ting.
Tilgang til utstyr.	
Tilgang til låste dører der man ikke har adgang	

Tabell 5: Oppsumering av årsaker som fremkom av Brainstorming prosessen.

Konsekvens på lån av adgangskort	
Policy brudd.	Tap av rykte.
Tyveri.	Tapt arbeid.
Terrorisme eller spionasje mot CCIS, NISlab, NorSIS, ol.	Studweb pga. samme pin. (meldes av fag).

Tabell 6: Konsekvenser vi anså ved låning av kort.

4.2.4 Datainnsamling

I denne fasen ble datainnsamling gjort med intervjuer.

Intervjuer

Intervjuer ble gjort av 36 ansatte og studenter ved NTNU i Gjøvik.

De forskjellige organisatoriske instansene vi intervjuet var Management, IT-Tjenesten, A-IMT, HOS, TØL og eksterne. Innenfor de forskjellige instansene intervjuet vi førsteamanuensiser, postdoktor, lektorer, avdelingsledere, professorer, dekaner, PhD-stipendiater, master studenter, renholdsansatte, statsbyggansatt, IT-Tjenesten og management.

Ut fra dette laget vi 6 grupper. De forskjellige gruppene var:

- Management: Denne gruppen inneholder alle dekaner og middle management vi har intervjuet
- IT-Tjenesten: Denne gruppen besto av to personer fra IT-Tjenesten med lederroller og sikkerhet vi har intervjuet
- Akademisk personell: Denne gruppen inneholder alle førsteamanuensiser, postdoktor, lektorer, avdelingsledere, professorer vi har intervjuet
- PhD: Denne gruppen inneholder alle PhD-stipendiater vi har intervjuet
- Student: Denne gruppen inneholder alle mastergradsstudenter vi har intervjuet
- Ekstern: Denne gruppen inneholder alle ansatte fra renhold og statsbygg vi har intervjuet

Under selve intervjuprosessen erfarte vi fort at spørsmålene vi hadde laget ikke var tilstrekkelige. Dermed valgte vi å tilpasse de og la til spørsmål for IT-Tjenesten og management. Et eksempel er når vi spurte ansatte om de har lest skolens sikkerhets policy, spurte vi IT-Tjenesten i tillegg om hvor stor andel av skolens ansatte de trudde hadde lest policyen angående adgangskort.

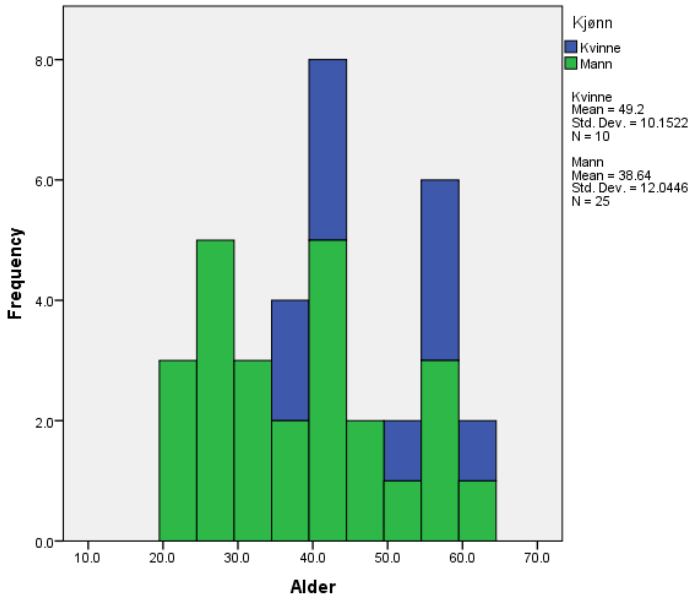
Vi klarte å avdekke holdninger rundt adgangskort hos ansatte og fikk mange relevante svar. Vi så også at noen spørsmål ikke ga oss den relevante dataen som var ønsket.

4.2.5 Dataanalyse

Viktige resultater fra analysen innebærer demografi, resultater på spørsmål, kategorisk analyse og kvalitativ analyse blir presentert her.

Demografi

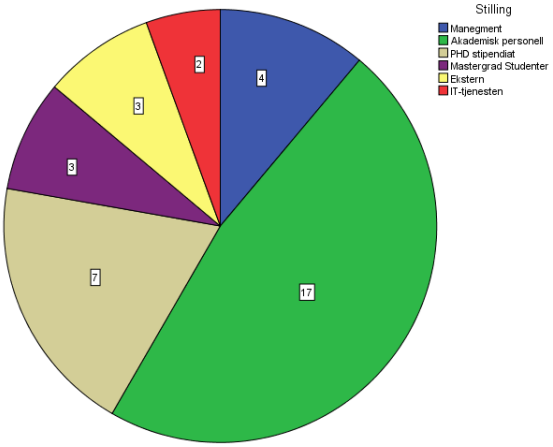
I figur 10 vises til fordelingen av kjønn og alder på intervjuobjektene.



Figur 10: Histogram: Kjønn og alder på de vi intervjuet.

Intervjudelen under gjennomførelse ble det vist til hvilke grupper som ble interjuvet og hvilke yrkestitler som inngikk. Avdelingene A-IMT og HOS har flest respondenter i vår undersøkelse. Avdelingene som deltok var IT-tjenesten, A-IMT, HOS og TØL i tillegg til ansatte i renhold og Statsbygg. Det ble ikke sett noen signifikant forskjell mellom alder og svar på intervju spørsmålene.

Fig.11 viser fordelingen av stillinger på de vi har spurt.



Figur 11: Pie graph av stillingene til de vi har spurt.

Spørsmål og svar

Når intervjuobjektene fikk spørsmål med skalar alternativer ble tallet 1 satt som minimum og 6 som maksimum, slik at ikke det eksisterte et heltall midt i mellom. Dersom

Nr	Spørsmål spurt til ansatte/studenter
1.	Hvilken nasjonalitet har du?
2.	Hvilket organisatorisk fagområde tilhører du? (F.eks A-IMT, TØL, HOS)
3.	Har du lest den gamle sikkerhetspolicyen?
4.	Nå som vi har fusjonert med NTNU, har du lest den nye sikkerhetspolicyen?
5.	Fra en skala fra 1 til 6, hvor 1 er "ikke i det heletatt" og 6 er "igjennom hele prosessen" føler du at ansatte som følger policyene skal få være med på å forme policyene?
6.	Vet du om det er lov eller ikke å byttelåne adgangskort?
7.	Kunnedu sagt oss hva IT-Tjenestens syn på kortlåning er?
8.	På en skala fra 1 til 6 der 1 er mindre alvorlig og 6 er veldig alvorlig, hvor alvorlig tror du skolen ser på byttelåne av adgangskort?
9.	Vet du hva konsekvensene vil være om skolen finner ut at personer byttelåner adgangskort?
10.	På en skala fra 1 til 6, hvor 1 er lite sannsynlig og 6 er svært sannsynlig, hvor sannsynlig tror du det er at ansatte innrømmer byttelåne av adgangskort kort?
11.	Tror du det er en lavere terskel for å låne bort adgangskort til familiemedlemmer?
12.	Hvor ofte tror du adgangskort blir lånt på skolen? Aldri, Årlig, Månedlig, Ukentlig, Daglig
13.	Hva kan du tenke deg er årsaker til at folk velger å låne bort adgangskort og pin?
14.	Bør det være lov å låne bort adgangskort og pin til personer som har samme romtilgang?
15.	Kjenner du til om noen har fått konsekvenser av lån/bortlån av adgangskort?
16.	Hva tror du er det verste som kan skje ved kortlåning?
17.	Hva føler du er kultur rundt kortdeling på NTNU Gjøvik?
18.	Vet du om tilfeller der det har vært lånt ut adgangskort mellom ansatte og studenter? a. Hvis ja: Husker du årsaken?
19.	Har du blitt spurt av noen om de kan låne ditt adgangskort? a. Hvis ja: Hadde de noen begrunnelse på hvorfor de trengte å låne adgangskortet?
20.	Har du noen gang følt behovet for å skulle spør noen om å låne deres adgangskort? Aldri, Årlig, Månedlig, Ukentlig, Daglig
21.	Vet du om det finnes noen reserveløsning dersom du har glemt adgangskortet ditt?
22.	Har du noen formening om hvilken avdeling som som byttelåner mest?
23	Tror du nasjonalkultur kan ha påvirkning på holdninger når det gjelder lån og bortlån av adgangskort?
24.	Fra en skala fra 1 til 6. Der 1 er veldig lang tid og 6 er hadde tilgang da jeg startet: Fikk du tilgang til alle rommene du trengte med en gang?
25.	Hva ser du for deg som mulige mottiltak for å forebygge lån og bortlån av adgangskort og pin mellom ansatte/studenter?

Tabell 7: Spørsmål stilt til ansatte/studenter under datainnsamling

Nr	Spørsmål spurt til IT-Tjenesten
1.	Er det viktig for IT avdelingen at ansatte har lest skolens policyer?
2.	På en skala fra 1 - 6 der 1 er ingen og 6 er alle. Hvor mange ansatte trur du har lest policyen ang.adgangskort?
3.	Tror du alle vet at det ikke er lov å låne eller låne bort adgangskort?

Tabell 8: Spørsmål som kun ble gitt til IT-Tjenesten

alternativet var fra 1 til 10 antok vi at det kunne være en enkel løsning å svare 5.

Her er listen over spørsmålene som ble stilt ansatte og studenter. Dette er ikke de samme spørsmålene som ble stilt Management eller IT-Tjenesten. Disse spørsmålene ble ikke lest inn av intervjuobjektene men stilt av oss muntlig.

Spørsmål til IT-Tjenesten var nesten de samme spørsmålene som ansatte fikk, de spørsmålene som kun IT-Tjenesten fikk er vist i tab.8. IT-Tjenesten ble ikke spurt disse spørsmålene: *"Vet du om det er lov eller ikke å byttelåne kort?"*, *"Bør det være lov å låne bort kort og pin til personer som har samme romtilgang?"*, Fra en skala fra 1 til 6. *"Der 1 er veldig lang tid og 6 er hadde tilgang da jeg startet: Fikk du tilgang til alle rommene du trengte med en gang?"*

Management fikk de samme spørsmålene som ansatte/studenter men de fikk også tilleggs spørsmål som kun ble spurt til dem som du kan se i tabell 9

I spørsmål nummer 25, har alle svarene fra intervju objektene blitt gjort uniforme og

Nr	Spørsmål spurt til management
1.	Må du ofte gi ut nye kort til ansatte eller studenter som kommer å spør?
2.	Har du oversikt over om IT eller Student Torget leverer ut nye kort til studenter eller ansatte?

Tabell 9: Spørsmål som kun ble gitt til management

deretter kategorisert inn i grupper i Affinity Diagram 12 og hver gruppe er representert i tabellen 10 fra gruppe nummer 1 til 6. I spørsmål 3, 4 og 7 er alternativ for ja lik 1, nei lik 2 og vet ikke lik 3. Std. Deviation står for standard avvik og beskriver hvor stor spredning det er mellom svarene som er gitt.

Descriptive Statistics

Spørsmål	N	Minimum	Maximum	Mean	Std. Deviation
Nr. 3	36	1,00	3,00	2,0833	,96732
Nr. 4	36	1,00	3,00	2,7778	,59094
Nr. 5	34	3	6	4,50	1,108
Nr. 7	35	1,00	3,00	1,4571	,78000
Nr. 8	34	1,0	6,0	4,000	1,7581
Nr. 10	35	1,0	6,0	3,457	1,5213
Nr. 12	35	2,00	5,00	3,9143	,91944
Nr. 20	32	1,00	2,00	1,4688	,50701
Nr. 21	31	1,00	4,00	2,0645	1,15284
Nr. 25	33	1	6	4,67	1,652
Valid N (listwise)	10				

Tabell 10: Tabell av spørsmål behandlet i SPSS

Kategorisk analyse

Analysen viser at det er tydelig forskjell mellom svar fra menn og kvinner på spørsmål 8 og 10 i intervju runden. Kvinner ser på situasjoner med låning av kort blandt ansatte som mer alvorlig enn menn. Kvinner mener også at det er større sannsynlighet for at ansatte innrømmer kortlåning enn det menn tror. Hvis man ser på tallverdiene [11] så er det en henholdsvis 1.42 forskjell i mean på Nr. 8 og 1.32 på Nr. 10. Begge har en lav p verdi 0,03 og 0,018, som vil si at begge er statisisk relevante [11].

Descriptives

		N	Mean	Std.Dev.	Std.Er.	95% C.I.		Min	Max	Anova sig.
						LB	UB			
Nr. 8	Mann	24	3,583	1,7673	,3607	2,837	4,330	1,0	6,0	
	Kvinne	10	5,000	1,3333	,4216	4,046	5,954	2,0	6,0	
	Total	34	4,000	1,7581	,3015	3,387	4,613	1,0	6,0	,030
Nr. 10	Mann	25	3,080	1,4978	,2996	2,462	3,698	1,0	5,0	
	Kvinne	10	4,400	1,1738	,3712	3,560	5,240	3,0	6,0	
	Total	35	3,457	1,5213	,2571	2,935	3,980	1,0	6,0	,018

Tabell 11: Descriptive til ANOVA på kjønn.

Det er stor forskjell på svarene fra IT-Tjenesten når det kommer til involvering i policy. På mean diffrence så har de største verdiene. Dersom ANOVA verdien er under 0.05 er det signifikans. Hva ansatte trodde angående hvor alvorlig skolen anså låning var det antydninger til relevanse og signifikans verdien her var på 0.339 og post hoc testen mellom eksterne og PhD stipendiater var på 0.242. Her var de på motsatte siden av skalaen, med PhD-stipendiaten på den lave enden og eksterne på den høye. Her er det forskjeller på hvor alvorlig folk tror situasjonen er. De som hadde minst tro på at ansatte ville innrømme å at de hadde lånt kort var de eksterne. Det var jevnt hvor ofte de forskjellige gruppene hadde følt behovet på å låne kort. ANOVA testen viste at det var en sig på 0.028 på hvor lang tid det tok for ansatte å få tilgang. Her var det de med høyere stilling som mente det tok mindre tid. Dette kan tyde på at det er de som har mer å si som blir tatt vare på først. IT-tjenesten er ikke nevnt her siden det er dem som har kontroll over systemet.

Descriptives

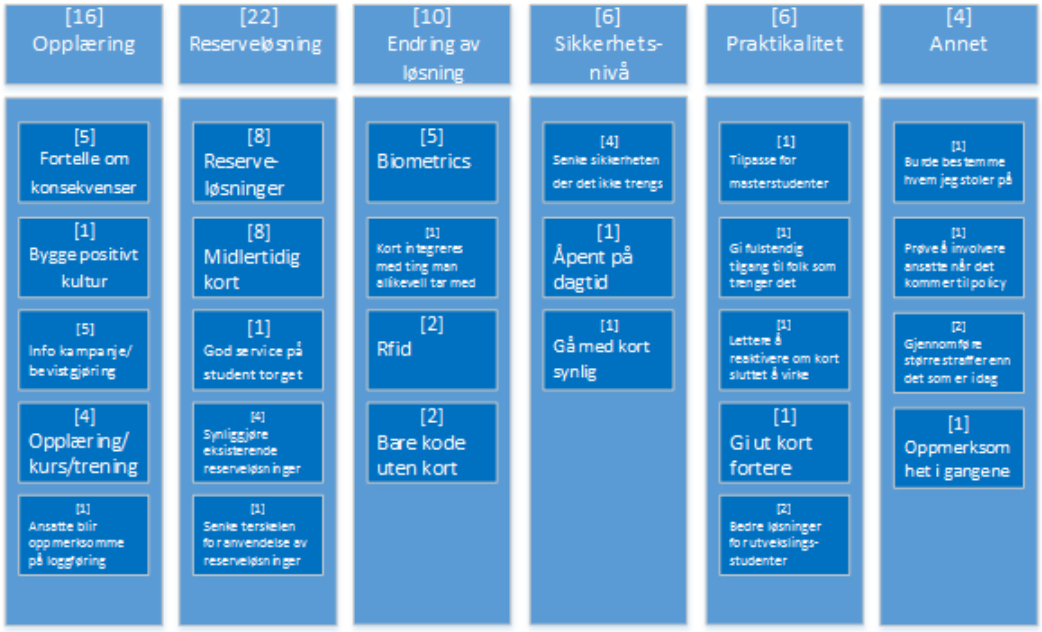
		N	Mean	Std.Dev.	Std.Er.	95% C.I.		Min	Max	Anova sig.
						LB	UB			
Fra en skala fra 1 til 6, hvor 1 er "ikke i det heletatt" og 6 er "igjennom hele prosessen" føler du at ansatte som følger policyene skal få være med på å forme policyene?	Manegment	3	5,00	1,732	1,000	,70	9,30	3	6	
	Akademisk personell	16	4,56	1,031	,258	4,01	5,11	3	6	
	PhD stipendiat	7	4,29	1,380	,522	3,01	5,56	3	6	
	Mastergradsstudenter	3	4,67	,577	,333	3,23	6,10	4	5	
	Ekstern	3	4,67	1,155	,667	1,80	7,54	4	6	
	IT-tjenesten	2	3,50	,707	,500	-2,85	9,85	3	4	
	Total	34	4,50	1,108	,190	4,11	4,89	3	6	,776
På en skala fra 1 til 6 der 1 er mindre alvorlig og 6 er veldig alvorlig, hvor alvorlig tror du skolen ser på byttelåne av adgangskort?	Manegment	4	4,500	1,9149	,9574	1,453	7,547	2,0	6,0	
	Akademisk personell	17	3,824	1,9117	,4636	2,841	4,806	1,0	6,0	
	PhD stipendiat	5	2,800	1,6432	,7348	,760	4,840	1,0	4,0	
	Mastergradsstudenter	3	4,333	1,1547	,6667	1,465	7,202	3,0	5,0	
	Ekstern	3	5,667	,5774	,3333	4,232	7,101	5,0	6,0	
	IT-tjenesten	2	4,500	,7071	,5000	-1,853	10,853	4,0	5,0	
	Total	34	4,000	1,7581	,3015	3,387	4,613	1,0	6,0	,339
På en skala fra 1 til 6, hvor 1 er lite sannsynlig og 6 er svært sannsynlig hvor sannsynlig tror du det er at ansatte innrømmer byttelåne av adgangskort kort?	Manegment	4	4,250	1,7078	,8539	1,532	6,968	2,0	6,0	
	Akademisk personell	16	3,688	1,5370	,3843	2,868	4,507	1,0	6,0	
	PhD stipendiat	7	3,000	1,7321	,6547	1,398	4,602	1,0	5,0	
	Mastergradsstudenter	3	3,333	1,5275	,8819	-,461	7,128	2,0	5,0	
	Ekstern	3	2,333	1,1547	,6667	-,535	5,202	1,0	3,0	
	IT-tjenesten	2	3,500	,7071	,5000	-2,853	9,853	3,0	4,0	
	Total	35	3,457	1,5213	,2571	2,935	3,980	1,0	6,0	,615
Har du noen gang følt behovet for å skulle spør noen om å låne deres adgangskort? Aldri, Årlig, Månedlig, Ukentlig, Daglig	Manegment	4	4,0000	,81650	,40825	2,7008	5,2992	3,00	5,00	
	Akademisk personell	16	4,0625	,99791	,24948	3,5307	4,5943	2,00	5,00	
	PhD stipendiat	7	3,7143	,75593	,28571	3,0152	4,4134	3,00	5,00	
	Mastergradsstudenter	3	3,3333	1,15470	,66667	,4649	6,2018	2,00	4,00	
	Ekstern	3	3,6667	1,15470	,66667	,7982	6,5351	3,00	5,00	
	IT-tjenesten	2	4,5000	,70711	,50000	-1,8531	10,8531	4,00	5,00	
	Total	35	3,9143	,91944	,15541	3,5984	4,2301	2,00	5,00	,727
Fra en skala fra 1 til 6. Der 1 er veldig lang tid og 6 er hadde tilgang da jeg startet: Fikk du tilgang til alle rommene du trengte med en gang?	Manegment	3	6,00	0,000	0,000	6,00	6,00	6	6	
	Akademisk personell	17	5,18	1,286	,312	4,52	5,84	2	6	
	PhD stipendiat	7	4,29	1,799	,680	2,62	5,95	1	6	
	Mastergradsstudenter	3	3,00	2,000	1,155	-1,97	7,97	1	5	
	Ekstern	3	3,00	1,732	1,000	-1,30	7,30	1	4	
	IT-tjenesten	0								
	Total	33	4,67	1,652	,288	4,08	5,25	1	6	,028

Tabell 12: Descriptive på stilling.

Affinity Diagram

Forslagene fra intervjuene ble gjort uniforme og samlet inn i 26 grupper. Videre brukte vi Affinity Diagram 2.9.3 verktøyet for å kategorisere forslagene inn i 6 hovedgrupper som vist i fig.12. Ønsket formål er å danne en oversikt over hvilke kategorier folk viste interesse for. I tillegg gir dette også fordeler ved at det blir lettere å presentere dataene i et Histogram da søylene presenterer 6 kategorier istedenfor 26 grupper med forslag.

Dersom en person har sagt mer enn ett alternativ, har hvert alternativ personen nevnte fått 1 "stemme".



Figur 12: Affinity Diagram: Forslag til reserveløsninger.

Histogram

Histogrammet 2.9.1 i fig.13 viser fordeling av antall personer opp mot antall forslag vi mottok og er basert på gruppene fra Affinity Diagram 12.

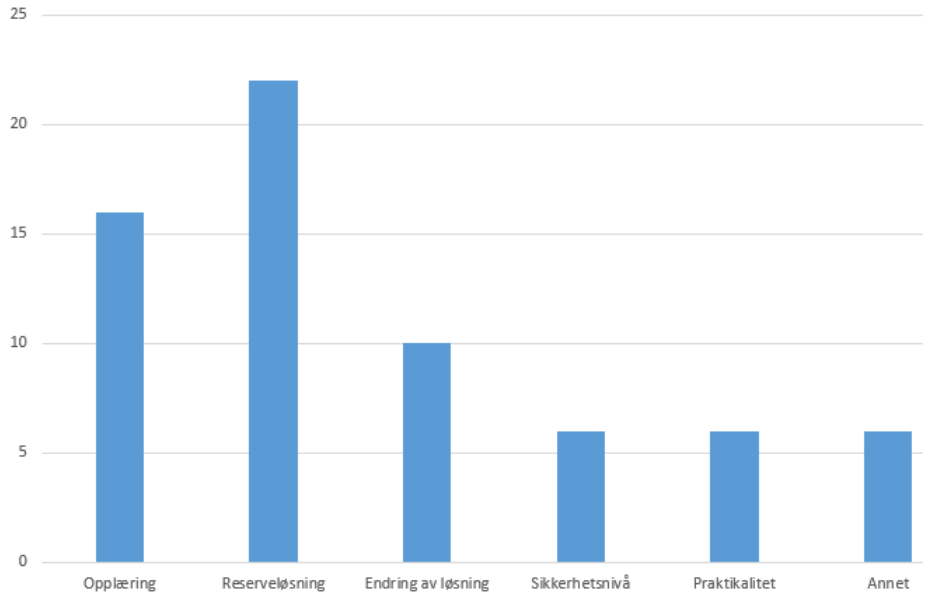
Kvalitativ analyse

Management

Alle hadde lest den gamle policyen da vi var HiG, men ingen hadde lest den nye etter skolen var blitt fusjonert med NTNU. Halvparten mente at det var viktig å ha med de som skal følge policyen til å utforme policyen igjennom hele prosessen. Da vi spurte denne gruppen om hva de så på som det verste scenariet, hadde denne gruppen ganske like meninger. Dataen vi samlet inn viser at de var bekymret for tap av informasjon, kompromittering og juridiske aspekter. Når vi spurte om ansatte ville svart ærlig på om de hadde lånt bort kortet sitt til andre var meningene ganske splittet. Det ble også sagt av 2 stykker i denne gruppen at de ikke fikk den servicen eller som de forventet av IT-Tjenesten. 3 av 4 hadde også til felles at de mente sikkerhetskulturen på NTNU i Gjøvik var bra mens 1 sa at den var tungvinn.

IT-Tjenesten

Her hadde alle vi spurte lest både gammel og ny policy og ser på det som svært viktig at ansatte og studenter også leser policyen. De mener i større grad at adgangskort lånes ut oftere enn andre grupper, og at A-IMT er den avdelingen som låner bort adgangskort mest siden det er flere kortlesere i A-bygget. De har også gitt en lavere score enn de andre gruppene på om ansatte bør involveres i policy.



Figur 13: Histogram: antall i hver gruppe fra Affinity.

Akademisk personell

Vi oppfatet under intervjuene at denne gruppen hadde flest og mest spredte meninger. Her svarte folk helt forskjellig. Men en av de tingene som ble sagt rundt spørsmål angående policy var at det verken var sikkerhetsavdelingen eller IT-Tjenesten som skulle stå for sikkerhets policyen. Det var organisasjonen som skulle stå for hva som stod i policyen og ikke være i veien for arbeid som må gjøres. Det handlet om virksomhetens mål og om oppdragets betydning overgår den potensielle skade man opplever at bytte vil ha, altså at policyen bør utformes med bedre risikoforståelse. Det ble også poengtert at ansatte skal til en hvert tid ha tilgang til rommene sine. IT-Tjenesten måtte gjerne skrive en policy rundt selve kortbruken, men skille mellom det som er den overordnede policy. Det var flere som sa at om kort ikke ble lånt bort til ansatte ville det være svært problematisk dersom det ikke eksisterte reserveløsninger. De savnet gode reserveløsninger om man hadde glemt adgangskortet sitt. Alle i denne gruppen svarte at det ikke var lov å dele kort selv om mer en halvparten ikke hadde lest gammel policy, og ingen hadde lest gjeldene policy etter fusjonen.

Ph.D-Stipendiat

5 av 7 vi spurte i denne kategorien hadde fått adgangskort relativt raskt, mens 2 andre hadde det tatt mye lenger tid. Det var en som svarte at han måte vente veldig lenge med å få tilgang til alt han trengte. Dette kan være en årsak til at man blir nødt å låne andre sine kort. Dette var også noe som ble nevnt av management gruppen, de nevte at det kunne ta lenger tid å verifisere utenlandskstudenter og de ønsket bedre løsninger på dette. Vi ble også fortalt at da Ph.D-stipendiatene av og til jobbet tett med mastergradstudenter var det mange mastergradstudenter som trengte romtilgang der de ikke adgang. Da måtte Ph.D-stipendiatene enten fysisk åpne dører for mastergradstudenter eller låne vekk kortene sine så de fikk gjort jobben de var satt til. Stipendiatene mente det burde være bedre løsninger enn det som eksisterer i dag. Ingen hadde lest den gjeldene policyen for

NTNU og kun en hadde lest gammel policyen. De fleste antok at det ikke var lov å låne bort adgangskortene sine men 2 sa de ikke visste. Når vi spurte om sikkerhetskulturen på NTNU i Gjøvik var svarene splittede, 2 svarte at de ikke vet, 1 mente at sikkerheten var bra, 1 sa at folk stoler på hverandre, 1 sa at den var slapp, 1 sa at folk viste at man ikke skulle låne det vekk mens siste sa at av praktiske årsaker lånes kort bort.

Studenter

Kun 1 av 3 studeter hadde lest gammel og ny policy. Studentene vi pratet med visste heller ikke om tilfeller der det var lånt vekk kort men 2 av 3 hadde blitt spurt om de kunne låne bort kortet sitt. De hadde ingen spesiell oppfatning om sikkerhetskulturen blant ansatte eller elever.

Eksterne

I gruppen for de eksterne inngår renhold og Stats Bygg. Ingen av dem hadde lest gjeldene policy, og kun en hadde lest gammel. Alle mente at det ikke var lov å låne kort, og at skolen så på dette som ganske alvorlig. De fleste hadde ikke hatt behov å låne andre sine kort. Her var det en som svarte at han følte behov årlig for å låne kort.

Forskjell på svar fra menn og kvinner

Vi la under intervjuene merke til at det var stor forskjell på menn og kvinners syn på hvordan skolen reagerte på låning av kort. De fleste av kvinnene vi pratet med mente at skolen så på dette mer alvorlig enn det menn gjorde som vist i tabell 11. Da vi spurte dette spørsmålet skulle de rangere på en skala fra 1 til 6, der 1 var mindre alvorlig og 6 var veldig alvorlig. Flere kvinner rangerte dette til 6 enn menn. Vi spurte også om hvor sannsynlig er det at folk innrømmer låning av adgangskort, med samme rangering. Dataene viser at kvinnene har mer tillit til at folk innrømmer låning av adgangskort enn det menn gjorde. Her var den laveste scoren blant kvinnene 3, mens 10 menn hadde rangert dette til 2 eller lavere.

4.2.6 Rotårsaksidentifisering

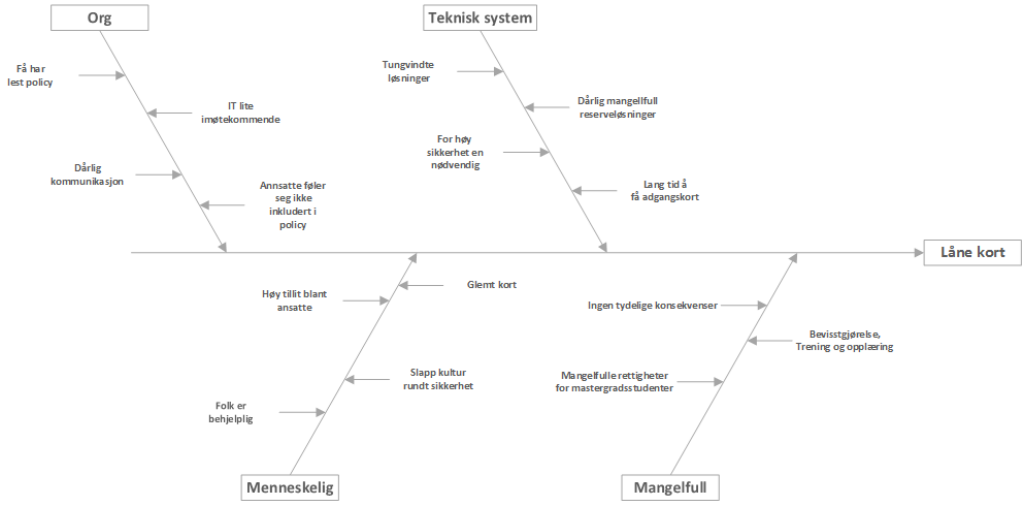
I rotårsaksidentifiseringen blir det anvendt et Fishbone diagram 14 for å vise problemer som fører til at personer velger å låne kort. 4 rotårsaker ble funnet.

Fishbone

Det har vært utført flere steg i dette verktøyet, og gjennomføringen kan leses i rapporten i appendix 6.3 og verktøyet er beskrevet i 2.10.2. Vi mener her at det er flere rotårsaker som må forbedres for at symptomene til problemet skal kunne elimineres. Rotårsaker vi har funnet er listet nedenfor:

1. Litt manglende/utydlige reserveløsninger.
2. Dårlig kommunisering av reserveløsningene som eksisterer.
3. Arbeiderenes effektivitet er ikke likestilt med IT-Tjenestens ønske om sikkerhet.
4. Lave sanksjoner av å låne bort adgangskort.

I Fishbone diagrammet 14 vises problemer som fører til hovedproblemet med at kort blir lånt.



Figur 14: Fishbone diagram over problemer som fører til hovedproblem.

4.2.7 Rotårsakseliminering

Systematic Inventive Thinking (SIT) 2.11.2 ble anvendt til å komme frem til løsningsforslag for eliminering.

SIT

Resultatene av fullført SIT er følgende:

Policy

(Attribute dependency): Tydeliggjøre straff ved brudd på policy og la ansatte få lov til å være med på forming av policy.
Vi foreslår at alle grupper får i tilstrekkelig grad være med på innvirkning i policy, om det innebærer fysisk tilstedeværelse eller mulighet til å gi tilbakemeldinger. Muligheten for å kunne komme med tilbakemeldinger må være godt nok kommunisert slik at det ikke er tvil om at personene kjenner muligheten. Eksempel kan være sticky e-poster, som vil vises på toppen i innboksen, muligens ha egen konvoluttfarge som er uslettbar i en viss periode.
(Conponent control): Gjøre policy lettere tilgjengelig.
På intranettsidene til NTNU “Innsida” bør det være lett å finne gjeldende bestemmelser og policy. De bør også være lett søkbare.

Antagelser/uklarheter

(Attribute dependencey): Tydliggjøre og bevisstgjøre.
Forsøke å unngå å gjøre antagelser på sikkerhetsrestriksjoner på bygget og dets rom. Avklare med de ansatte om hvilke sikkerhetsbehov som er nødvendige for å unngå at de implementerte sikkerhetstiltakene reduserer de ansattes produktivitet.
(Component control): Hvis mulig og ikke for mye bry - spør istedenfor å anta.
Det er lett å gjøre antagelser, som kan bidra til feil. Derfor er det være viktig å maksimere kommunikasjonen for å få stilt spørsmål, selv om en ville følt seg trygg på å gjøre en antakelse i situasjonen. Vise skjønn.

Byggets sikkerhetsnivåer

(Attribute dependency): Se over/revurdere sikkerhetsnivåer.
Forhindre at sikkerhetsnivåer er overdrevent i forhold til rommets bruk. For høyt sikkerhetsnivå gjør at de ansatte tyr til snareveier.
(Component control): Kontrollere at verdier i rom tilsvarer sikkerhetsnivå.

IT-Tjenesten

(Component control): Sjekke med omgivelsene om løsningene fungerer. Kommunisere med de ansatte om løsningene som er implementert fungerer. Dette fordi de ansatte er brukerene og kan formidle sine brukeropplevelser som kan bli tatt i betraktning av IT tjenesten.

Nettsider

(Attribute dependency): Tilføye hjelpeside for adgangskort.
Opprette en nettside på ntnu.no domenet som gjør det mulig å lese støttelitteratur om problemer rundt adgangskort samt hvilke reserveløsninger som eksisterer og hvordan å utnytte dem.

Reservekort/adgangskort

(Attribute dependency): Tilpasset tilgang på rom (adekvat).
Gi administratorer bedre muligheter til å tilpasse romtilganger med hovedfokus på å kunne gi reservekort som har adekvat og spesifikk romtilgang. Dette vil si å unngå å gi generell romtilgang på reservekort som ikke er tilstrekkelig for alle.

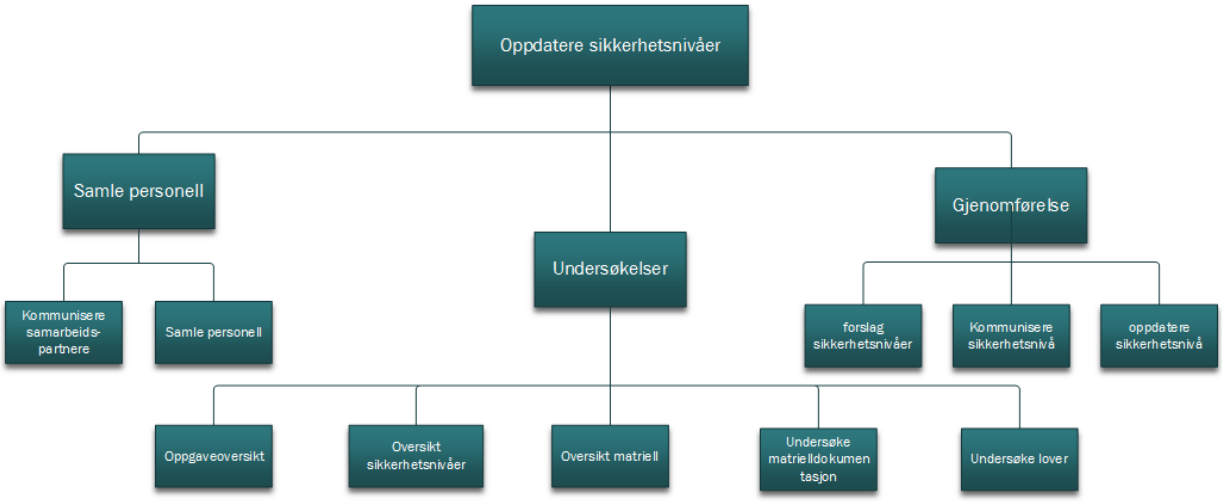
4.2.8 Løsningsimplementering

Implementeringen av løsningsforslag vil bli organisert av IT-Tjenesten og relevant nøkkelpersonell i de forskjellige avdelingene. Det var brukt et Tree Diagram 2.12.1 for å representere resultatet av stegene og rekkefølgen disse skal løses i.

Tree Diagram

I dette kapittelet ble det gitt et eksempel på hvordan planlegging av løsningsimplementering kan utføres. Det var vanskelig for oss som ikke er personell i IT-tjenesten å komme med noe annet enn forslag, derfor viste vi til et eksempel på hvordan det kan løsningsimplementeringen kan gjennomføres. Vi valgte å bruke byggets sikkerhetsnivåer 4.2.7 for dette eksemplet.

Her ønsket vi å lage en strukturert plan som kan følges i kronologisk rekkefølge for å oppnå ferdig løsningsimplementering 15 . Alt som ble gjennomgått i stegene for å utføre verktøyet kan leses om i case 2 i appendix 6.3. For å traversere treet startes det nederst til venstre fra undergruppen Samle personell, deretter gjøres det undersøkelser og til slutt gjennomførelse.



Figur 15: Case 2 Tree Diagram over løsningsimplementering

4.2.9 Case 2 Tidsbruk

4.2.10 Tidsbruk

Den totale tiden brukt på case 2 er omtrent 220 timer per person (660 timer).

Tabell 13: Loggføring

Loggføring av tidsbruk på verktøyene		
Fase	**Verktøy**	**Tidsbruk t=timer m=minutter**
Forberedende fase	Innsamling og kartlegging av data	100 timer
Forberedende fase	Testing og valg av verktøy	72 timer
Problemforståelse	Performance Matrix	3,25 timer
Problemårsaksidemyldring	Brainstorming	1,23 timer
Problemårsaksidemyldring	Planlegge intervju	150 timer
Datainnsamling	Gjennomføre Intervju	100 timer
Dataanalyse	Kvalitativ og kvantitativ analyse, SPSS	220 timer
Rotårsaksidentifisering	Fishbone	6,4 timer
Rotårsakseliminering	SIT	7,1 timer
Løsningsimplementering	Tree	1,2 timer
		Total 660 timer.

4.3 Case 3 - DDoS

I dette caset vi fikk av slettmeg så vi på et DDoS angrep som inntraff 7.mai 2015. Her anvendte vi verktøy for å se på hva som var årsaken til at slettmeg ble utilgjengelig under angrepet. Dette er muligens kjent for slettmeg men det ga oss grunnlag for å bruke RCA verktøyene og levere resultat. Slettmeg kan forvente resultater på kunnskap om verktøyene vi forsøkte i caset. Vi diskuterte erfaringer vi satt igjen med etter arbeidet var gjort og håper at slettmeg vil kunne finne disse anvendbare. Dette vil inkludere struktur på utførelsen av verktøy og muligens fallgruver. Vi så kun på angrepet som inntraff 7.mai 2015 og på hvilken beskyttelse de hadde denne datoen.

Begrensninger

Under datainnsamling hadde vi ikke tilgang til logger. Derimot hadde vi tilgang til politianmeldelsen. Det var utført møter med kontaktperson som ble gjennomført i forbindelse problemforståelsen og datainnsamlingen. Slettmeg fortalte oss at de ønsket at vi skulle i en stor grad skulle se bort i fra tekniske aspekter som hvordan å unngå DDoS fra et teknisk synspunkt og hvilke type DDoS det var. Vi forsøkte å se om det å gjøre rotårsaksanalyse kunne hjelpe slettmeg med å finne en rotårsak de selv ikke var klar over. Vi så også på om løsningsforslagene som er implementert til dags dato svarer på alle problemene eller om noen problemer gjenstår.

Caset er ment for å hjelpe oss med å gi svar på forsknings spørsmålet: *Hvordan fungerer rotårsaksanalyse på en case med lite ressurser og lite tid?*.

4.3.1 Problemforståelse

Før vi startet med dette caset hadde vi en samtale med Vidar Sandland fra slettmeg om hendelsesforløpet og fikk en kopi av anmeldelsen som ble levert til Gjøvik politikammer. Her er det god tidslinje av forløpet noe som gir oss en mulighet å bruke verktøyet flowchart (vi valgte å lage et Swim Lane Flowchart 2.6.1).

Swim Lane Flowchart

Det vi ønsket som utbytte er var tydelig visning av flyten gjennom utførelser og hendelser.

Her følger en beskrivelse av elementene i Fig: 16.

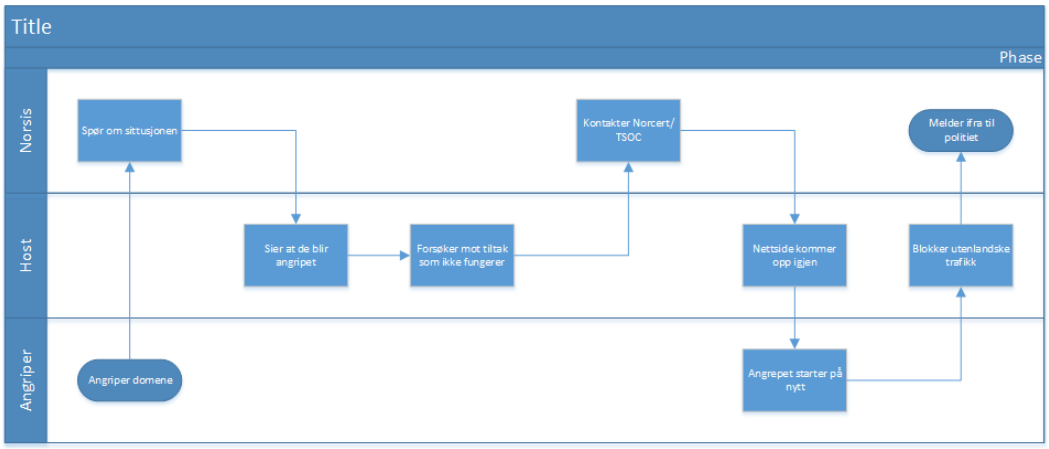
7.mai 2015

1. *kl.14:30* NorSIS varsles via ekstern tjeneste om at NorSIS' nettsier er utilgjengelige.
2. *kl.15:45* NorSIS kontakter tjenesteleverandøren sin, og blir informert om at de jobber med saken.
3. *kl.16:16* NorSIS blir kontaktet av sin tjenesteleverandør, som informerer at det er snakk om et tjenestenektangrep (DDoS)
4. *kl.19:50* NorSIS blir kontaktet av sin tjenesteleverandør som forklarer at NorSIS' nettsider mottar kontinuerlig mellom 40 og 60000 forespørsler fra utenlandske IP-addresser, og kneler som følge av overbelastning. Det ble forsøkt å sperre for utenlands trafikk, men grunnet utfordringer hos tjenesteleverandørs nett-leverandør lot ikke dette seg gjøre.
   Det ble da forsøkt å bytte IP-adresse på NorSIS' webserver og oppdatere DNS på domenet norsis.no. Dette fungerte i 15-20 minutter.
5. *Ettermiddag/kveld* NorSIS informerer NorCERT og TSOC om tjenestenektangrepet. NorCERT får også oversendt loggene fra angrepet.

8.mai 2015

1. *kl.08:00* Alle NorSIS' nettsider fortsatt utilgjengelige.
2. *kl.08:10* Alle nettsidene blir tilgjengelige igjen
3. *kl.10:15* Angrepet starter på nytt, med det resultat at alle nettsidene igjen blir utilgjengelige.
4. *kl.12:24* Tjenesteleverandør informerer om at de nå blokkerer trafikk fra utlandet, og nettsidene blir gradvis tilgjengelige for norske og skandinaviske besøkende

5. *kl.12:30* Politiet på Gjøvik blir kontaktet for bistand i saken.



Figur 16: Swim Lane Flowchart av hendelsesforløpet

Critical Incident

For å forsikre oss om at vi forstod hva som virkelig lagde mest problemer var det viktig å høre hva slettmeg selv mente om akkurat dette og her ble det brukt Critical Incident 2.6.2.

Spørsmålene samt svarene vi fikk av slettmeg.

1. Hva er det mest negative ved at siden deres er nede?
2. Hvordan beskriver dere problemet med å forhindre DDoS mot slettmeg.no? (Teknisk og prioriterings basert).
3. Hvor mange ganger utsettes dere for DDoS angrep i året?

Slettmeg forteller at det som var det mest problematiske med at nettsiden deres var nede var at folk ikke fikk tak i selvhjelp. Det var ved den datoen ikke tilstrekkelige mottiltak mot DDoS. De kunne ikke helt svare på hvor mange ganger de ble utsatt for DDoS i løpet av et år da host ikke alltid fortalte om det, men heller automatisk utførte rutiner med blokkering av IP'er fra utlandet. Disse rutinene var ikke tilstede under DDoS angrepet 7.Mai 2015. Det største problemet med DDoS er derfor at folk ikke lengre har tilgang til selvhjelp siden som slettmeg tilbyr.

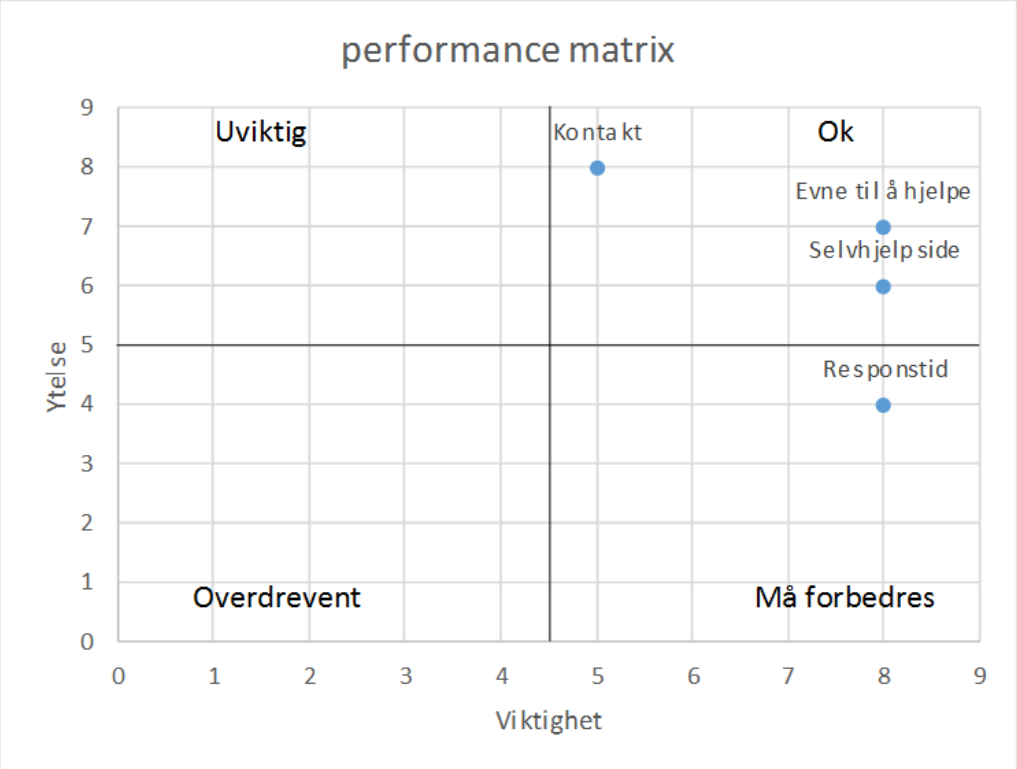
Vi var ikke i stand til å utføre verktøyet akkurat slik hvert steg var da vi ikke hadde mulighet til å samle alle som jobbet på slettmeg og gjennomføre gruppeaktiviteter.

Performance Matrix

Det ble anvendt Performance Matrix 17 beskrevet i kapittel 2.6.3 for å finne ut hva som var viktig for slettmeg og hvordan de mente at ting fungerte.

Disse punktene ble utarbeidet i sammen med kontaktperson i slettmeg.

1. Evne til å hjelpe (oppetid (kapasitet til forespørsler)).
    1. *(Importance)* Hvor viktig er oppetiden på nettsidene? Svar: 8
    2. *(Performance)* Hvor god er oppetiden på nettsidene? Svar: 7
2. Kontakt muligheter.
    1. *(Importance)* Hvor viktige for dere er det at klienter får lett kontakt med dere via tlf. og mail eller sosiale medier? Svar: 5
    2. *(Performance)* Hvor godt fungerer kontaktmulighetene til dere via tlf. og mail eller sosiale medier? Svar: 8
3. Responstid.
    1. *(Importance)* Hvor viktig er responstid? Svar: 8
    2. *(Performance)* Hvordan faktiske responstiden er? Svar: 4
4. Selvhjelp side.
    1. *(Importance)* Hvor viktig for dere er det at dere kan tilby selvhjelp? Svar: 8
    2. *(Performance)* Hvor godt tilgjengelig er selvhjelpen dere tilbyr? Svar: 6



Figur 17: Performance Matrix av ytelse og viktighetsgrad

Vi ble fortalt at antallet henvendelser til slettmeg var stort og at det kan være vanskelig å henvende seg til alle innen kort tid og samtidig gi god hjelp. Deres selvhjelp og dermed også nettside oppetid rangeres høyt da det er et sterkt ønske fra slettmeg at selvhjelpen skal bidra med at flesteparten som oppsøker hjelp er i stand til å få løst sine problemer

via selvhjelp.

4.3.2 Problemårsaksidemyldring

Her brukte vi ustrukturert brainstorming 2.7.1 med ønske om at gruppen som analyserer har en samlet oversikt med konsensus på hva som blir sett på som problemårsaker.

Brainstorming

Ønsket utbytte er en liste med antatte konsekvenser og årsaker til problemet eller de problemer som bygger opp til de synlige symptomene. Listene er gruppert etter viktighet.

Identifiserte mulige konsekvenser av problemet:

1. Mindre tilgjengelighet for klienter/brukere av tjenesten.
2. Nedsatt rykte.
3. Dersom slettmeg ikke er i stand til å drifte selvhjelp vil de ha økonomiske problemer.

Mulige årsaker til problemet:

1. Tjeneste leverandør hadde ingen testet plan for behandling av situasjonen.
2. Ikke gode nok kunnskaper hos de som hoster om hvordan å behandle situasjonen.
3. slettmeg setter seg i kryss ild mellom individers problemsituasjoner.
4. Angriperene kan være utenfor norsk jord.
5. Ingen tydelig avskrekking for DDoS angrep på siden.
6. DDoS av slettmeg.no ikke vurdert kritisk nok.
7. Manglende/utilstrekkelig risikovurdering.
8. For lite ressurser brukt på server-kraft.

Problemområder som kan forbedres er beskrevet i Performance Matrix 17, hvor punkter på “performance” kan økes til ønskede verdier.

4.3.3 Datainnsamling

Slettmeg har innført DDoS beskyttelse, slik at vi nå antar at alle de tekniske aspektene ved slike angrep blir tatt hånd om av de som står bak denne tjenesten. Dette innebærer at tjeneren av DDoS beskyttelsen har kunnskaper om hvordan å behandle en slik situasjon og at slettmeg blir informert dersom siden allikevel er nede slik at slettmeg så kan informere sine brukere. I Check Sheet verktøyet blir det sett på situasjonen slik den var under angrepet, og hvordan situasjonen er i ettertid.

Check Sheet

Da det ble bestemt at i dette caset skulle litteraturen strengt etterfølges, ble flowchartene i tool selection seksjonen i Root Cause Analysis Simplified Tools and Techniques side 174 til 186 [1] anvendt til verktøy valg. Det var ikke gjennomførbart å tegne noen grafiske Check Sheets 2.8.2 i vårt tilfelle.

Ønskede utbytte er å oppnå en prioritering eller en rangering på elementene som skal analyseres. Eventuelt om dette er gjennomførbart. En del av det ønskede utbytte er å

erfare verktøyet og evaluere dets tilpasning til situasjonen.

En brainstormingfase ble anvendt til å generere problemer og problemsituasjoner som hendte under angrepet og i etterkant ved rapportering til myndigeter. Punktene ble diskutert med vår kontaktperson hos slettmeg. Vanskeligheten med å rangere problemene i listen ble løst med diskusjon av hvert punkt. Vi kan derfor fremstille våre data med en kvalitativ presentasjon fremfor en kvantitativ frekvens av hendelsene.

Politiet kikket ikke på bevismateriale

Bevisene ble samlet inn i form av logger, og loggene ble deretter kryptert og gitt ett passord. NorSIS anmeldte så angrepet til politiet og sendte den krypterte filen med loggene og skrev at politiet kunne kontakte NorSIS for å motta passordet til filen. Politiet kontaktet dem aldri for å få åpnet filen og henla saken.

Kontakt med tjenesteleverandør

Slettmeg sin nettside leverandør hadde ingen prosedyrer på hvordan å håndtere situasjonen, og kontaktet sin nettleverandør som ikke umiddelbart kunne bistå. Tiden det tok for å opprette kontakt var relativt kort. Slettmeg opplever det som et viktig aspekt av denne situasjonen at kontakttiden er svært lav og at de selv får vite at det er problemer med tjenestene de blir levert.

Måtte finne ut hvordan de skulle håndtere situasjonen på stedet

Leverandør av webtjenestene var ikke trente på slike situasjoner, og kunne ikke håndtere den da angrepet inntraff. De kontaktet derfor sin nettverksleverandør og foreslo at de skulle blokkere trafikken som kom fra utenlandske adresser da angrepet ikke stammet fra i fra Norge. Nettverksleverandøren var heller ikke i stand til å øyeblikkelig etterfølge dette ønsket. NorSIS selv hadde ikke gjennomført noen øvelser på DDoS situasjoner da det ofte ikke er annet å gjøre enn å blokkere trafikk, vente angrepet ut og opprette en beskjed via en annen leverandør som forteller situasjonen til brukerne, DDoS Proactive and Reactive measures [**?**] side 31.

Host fikk ikke blokkert utenlandsk trafikk øyeblikkelig

Host hadde ikke ordninger på plass for å stenge av nettverkstrafikk fra utlandet. Dermed måtte de kontakte ISP'en de brukte som heller ikke hadde noe løsning på plass. Det gikk dermed unødvendig mye tid med på å få nettverkstrafikk fra utlandet stengt.

Skapte uante problemer for resten av organisasjonen

Angrepet på slettmeg var rettet mot domenet og ikke IP adressen. Trafikken slo ut alle webtjenester som NorSIS hadde.

Unødvendig mye ressurser gått bort på å behandle situasjonen

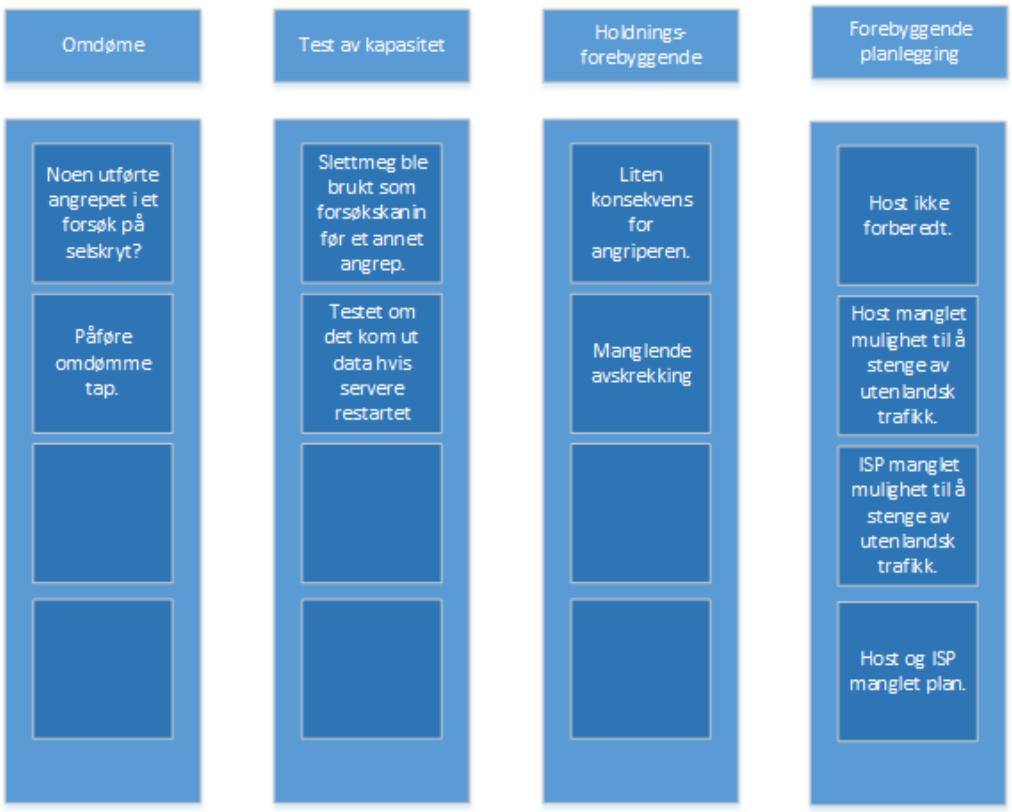
Angrepet førte også til at personer i NorSIS måtte omprioritere oppgavene sine og deres normale arbeid ble utsatt. Ansatte hos web host og ISP måtte også bruke tid av sine ansatte til å behandle situasjonen. Anmeldelsen som ble skrevet ble det satt av en halv dag til på en ansatt, slik at strukturen og fremgangsmåten kan anvendes på nytt ved liknende situasjoner og av andre enn NorSIS.

4.3.4 Dataanalyse

I denne delen analyserte vi dataene som ble innhentet. Svært få verktøy passet vårt case. Derimot var det gjennomførbart å lete etter skjulte sammenhenger i dataene som ble samlet inn. Et Affinity Diagram 18 ble forsøkt anvendt da dataene ikke var numeriske. Verktøyet er beskrevet i kapittel 2.9.3.

Affinity Diagram

Ønsket er å lete etter skulte sammenhenger i dataene som ble samlet inn.



Figur 18: Affinity Diagram som viser om det er skjulte sammenhenger

4.3.5 Rotårsaksidentifisering

Diskusjon av årsaker

Da det ble bestemt at hovedlitteraturens flowcharts for forslag til verktøyvalg skulle anvendes på hvert av de 7 stegene forotårsaksanalyse, har dette vist seg å være vanskelig på rotårsaks identifiserings steget.

Vi konkluderte med at det ikke kunne eksistere bare en rotårsak. Hver rotårsak blir diskutert:

Nr 1, Angriperens motivasjon og intensjon

Angriperen er motivert til å utføre et angrep av flere forskjellige årsaker. Noen av årsakene kan forekomme ut av arbeidet slettmeg gjør med sine klienter. Det kan også eksistere motivasjoner som ikke skyldes slettmeg sitt arbeid men kan være at angriper skryter av egne handlinger. Skryt omhandler også hacktivister som er motivert av publisitet og berømmelse. Det kan ligge prestisje i å ta ned slettmeg.no som er under NorSIS og DDoS er et enkelt valg av verktøy da det er lett å gjennomføre og med riktige tiltak er det vanskelig å avsløre angriperen.

nr 2, Lav risiko

Når det kommer til avskrekking og redusering av motivasjon hos angriper er det svært vanskelig å avgjøre hva som motiverer dem. Eksempler på motivasjon kan være ingen konsekvens, føler seg uretferdig behandlet eller ikke liker det slettmeg gjør og skryt.

nr 3, Lett å iverksette

DDoS angrep er veldig lett å iverksette. Selv med liten kunnskap kan du bruke verktøy som gjør mesteparten for deg, eller kjøpe tjenesten av noen. Det at såkalte "amplifikation attacks" er lett å gjennomføre medvirker til en skjev fordeling av styrke mellom angriper og de som beskytter mot angrepet.

Nr 4, Mangel på forberedelser

Mangel på forberedelse mot angrep. Host til NorSIS var ikke foreberedt på å behandle DDoS angrep. Selv med de beste forberedelsene, så kan angriperene komme på nye teknikker for å unngå forsvarsmetodikkene. Det er derfor viktig å være forberedt.

Nr 5, Mangel på kontroll

Mangel på kontroll over situasjonen. NorSIS delegerte bort ansvaret for situasjonen uten å kontrollere at hosten var i stand til å håndtere slike situasjoner.

1. Rotårsak nummer 1 er det ikke mye vi tror kan gjøres med da angriperenes motivasjon er uforutsigbar. Det kan være interessant i videre arbeid å forsøke å kartlegge motivasjoner for angrep.
2. Rotårsak nummer 2 blir ikke behandlet her da NorSIS har valgt å outsource DDoS beskyttelse.
3. Rotårsak nummer 3 blir tatt med videre i analysen.

Ut fra flowchart på verktøyvalg for rotårsaksidentifisering i tool selection seksjonen i Root Cause Analysis Simplified Tools and Techniques side 182 til 183 [1] , var ingen av alternativene passende. Derimot ble rotårsakene diskutert og argumentert for. Vi ser på dette som et funn.

4.3.6 Rotårsakseliminering

SIT

Ønsket utbytte var kunnskap om hvilke problemårsaker fra rotårsaksidentifiseringen det trengs å implementere løsninger til.

Problemet vi tok for oss er: Mangel på kontroll. Her listes komponenter til problemet, og iht. verktøybeskrivelse 2.11.2 tok vi med forslag på komponenter selv om de kunne virke irrelevante.

1. Ansvarsperson
2. Prosedyre
3. Leverandør (riktig ord?)
4. Kunnskap og erfaringer til leverandøren
5. Rykte/omdømme (ryktet leverandøren har på seg).
6. Kontrakt
7. Kommunikasjon mellom leverandør og klient

Hver komponent som vi så på som realistisk å behandle videre i analysen ble valgt ut og de 5 SIT prinsippene 2.11.2 ble brukt på hver av komponentene. Flere av prinsippene viste seg at ikke var gjennomførbare på komponenten, og i våres tilfelle valgte vi å la de være blanke. Under utførelsen av et SIT prinsipp har vi beskrevet et forslag til forbedring utifra prinsippets formål.

Den første som ble valgt er *Ansvarsperson*.
Component control: Forsikre at kontrollperson er knyttet til miljøer med faglig kunnskap.

Nummer to er *Prosedyre*:
Attribute dependency: Ilegge større kontroll på de det kjøpes tjenester av.
Component control: Sammenligne egne prosedyrer med andres.

Nummer tre er *Kontrakt*:
Attribute dependency: Kontrakten bør beskrive tydelig tjenerens ansvarsområder. Component control: Passe på at kontrakten tilsvarer miljøet den anvendes i.

Løsningsforslagene:

Prosedyre

Dersom en sammenlikner sine prosedyrer med andres kan man oppdage svakheter i sin egen og få nye ideer på hvordan problemer kan løses. Ved å undersøke tjenesteleverandøren nøye på forhånd kan en forsøke å redusere mulige problemsituasjoner i fremtiden.

Kontrakt

Dersom det er realistisk at kontrakten hadde holdt tjenesteleverandør ansvarlig, kunne det vært mulig for slettmeg å fått kompensasjon for tapt arbeidstid som ble påført av omorganisering av arbeidsoppgaver under og etter angrepet. Kontrakt kan også spesifisere at leverandøren må ha kunnskaper om hvordan slike situasjoner skulle behandles.

4.3.7 Forslag til Løsningsimplementasjons

Som beskrevet i introduksjonskapittelet ble det valgt å følge hovedlitteraturens flowcharts på valg av verktøy på dette caset. Flowcharten[1] på side 186 starter med å spørre

om løsning på problemet er funnet. Vi har presentert forslag om forbedring på prosedyre og kontrakt. Videre skal skal det bestemmes hvordan implementeringen skal organiseres. Verktøyene for løsningsimplementasjon som er tilgjengelig hjelper til med å forklare hvordan organiseringen skal være. Deretter er spørsmålet om det trengs et verktøy til å veilede, organisere og strukturere gjennomføringen. Dersom implementasjonen er stor eller uoversiktlig, blir det anbefalt å bruke et Tree Diagram 2.12.1. Vi ser fra tidligere analyser som er utført at tre diagrammet har en strukturert gjennomgang, som vist i adgangskort case for adgangskort delkapittel 4.2.8 og DDoS case 1 delkapittel 4.1.7. Når det er aktuelt å gjøre sammenlikninger med andre organisasjoner, kan det anvendes et Spider Chart som beskrevet i kapittel 2.13.1.

4.3.8 Case 3 Tidsbruk

Den totale tiden brukt på case 3 er omtrent 75 timer per person (150 timer).

Tabell 14: Loggføring

Loggføring av tidsbruk på verktøyene		
Fase	**Verktøy**	**Tidsbruk t=timer**
Forberedende fase	Innsamling og kartlegging av data	100 timer
Forberedende fase	Testing og valg av verktøy	25 timer
Problemforståelse	Swim Lane Flowchart	1,20 timer
Problemforståelse	Critical Incident	2.73 timer
Problemforståelse	Performance Matrix	3,05 timer
Problemårsaksidemyldring	Brainstorming	1.53 timer
Problemårsaks datainnsamling	Check Sheets	9,53 timer
Problemårsaks dataanalyse	Affinity diagram	1.85 timer
Rotårsaks identifisering	Diskusjon av rotårsaker	2 timer
Rotårsaks eliminering	SIT	1.1 timer
Løsningsimplementering	Beskrivelse av alternativer	2,05 timer
		Total: 150

5 Diskusjon

Her diskuter vi oppgavens resultat og mål og hvordan vi kom frem til svar på vårt forskningsspørsmål. Vi velger å gå gjennom forskningsspørsmålene sekvensielt. Vi vil også gi kritikk av oppgaven der vi mener vi kunne utført punktene bedre samt hva som kan gjøres i videre arbeid.

5.1 Er det kostnadseffektivt å bruke rotårsaksanalyse innen informasjonssikkerhet?

Som man kan se av antall steg i en systematisk tilnærming til problemløsning, kan prosessen ta tid og ressurser for å oppnå ønsket mål. Problemer av mindre betydning, eller av en slik art at de trolig forsvinner av seg selv etter en gitt tid, bør ikke være gjenstand for omfattende innsats. Det er det rett og slett ikke verdt. Det er uproduktivt å bruke en komplisert problemløsningprosess til hverdagslige problemer vi allerede vet hvordan vi kan løse. Når du imidlertid oppfatter problemet som viktig, og ikke vet dets natur eller årsak, angrip det systematisk for å sikre at du finner årsaken og til slutt eliminer problemet for godt. I slike tilfeller er problemløsningprosessen fornuftig. Det som vanligvis blir brukt i situasjoner innen informasjonssikkerhet er en risikoanalyse. En slik prosess kan fort bli veldig komplisert og stort, ganske likt det en rotårsakanalyse hadde blitt. Det du kommer frem til er tiltak som er ment til å redusere sannsynligheten for at en hendelse inntreffer samt redusere skaden ved denne hendelsen. I motsetning til rotårsaksanalyse der du har en annen tilnærming, du er ute etter å stoppe det som skaper problemet. Siden de to forskjellige metodene har ulik hensikt, så er det viktig at de som har tenkt å utføre prosessen vet formålet med prosessen. Vi ser på kostnatt utifra tidsbruk. Vi opplever at tiden brukt på å utføre RCA verktøy blir mindre når gruppens medlemmer får mer erfaring.

Når vi utførte case 1 som var en tabletop-øvelse var det utfordrende å samle inn informasjonen vi trengte fra dokumentasjon, dette førte til at vi måte gjøre antagelser. Vi utførte ikke vår egen datainnsamling under trinnet for datainnsamling som er et essensielt steg i rotårsaksanalyse. I rotårsaksanalyse er det viktig at vi har tilgang til nøkkelpersoner under analysen. Det var ingen informasjon i dokumentasjonen vi fant, som gjorde at vi greide å gjøre nye funn ved videre analyse. Vi opplever at tabletop-øvelsen ga oss god læring i bruk av verktøyene, noe som kan være nyttig for andre som forsøker å lære seg rotårsaksanalyse.

Å ha tilgjengelig mye tid og resurser i case 2, gjorde at vi kunne gjennomføre stegene grundig. Her hadde vi tilgang på nøkkelpersoner, en bedre problemforståelse, vi fikk hentet inn dataene vi mente var nødvendige og analyserte resultatene selv. Dette ga oss en mye bedre oversikt over problemstillingen vi fikk fra IT-tjenesten. Da var vi også mye bedre i stand til å sette opp tiltak vi mente var realistiske å gjennomføre. Dette gjør oss tryggere på resultatene vi kom frem til. Våre resultater i motsetning til IT-Tjenesten som gjorde en risikovurdering ble helt anderledes. De mente at kameraovervåkning var et tiltak som skulle gjøres, mens vi mente at kommunikasjonen må bedres mellom av-

delingene ved å tydeliggjøre konsekvensene av kortlån og forklare hvorfor kortlån er et problem for IT-tjenesten. De bør også tydeliggjøre de reserveløsningene de har, eller eventuelt utbedre dem.

Det å gjøre en grundig rotårsaksanalyse hjelper med å komme frem til andre tiltak enn tradisjonelle metoder. Organisasjoner må veie kost-nytte opp mot problemet for å avgjøre om de ønsker å utføre en rotårsaksanalyse eller ikke. Rotårsaksanalyse har sine fordeler men prosessen kan være krevende. Vi mener det er verdt å gjennomføre en rotårsaksanalyse der kost-nytten tilsier det.

Vi merket at det å ha begrenset med tid og ressurser på analysen av DDoS angrepet var veldig krevende da vi kun var to personer og kun hadde to uker å gjennomføre analysen på. Her ville flere personer avdekket flere mulige problemer under brainstorming fasen, og det blir vanskeligere å avdekke feil og mangler tidlig i fasene. Det å være få gjorde at det var vanskelig å oppdage problemer som igjen førte til at det var mer jobb å rette opp. Tidspresset ble større og valg av verktøy måtte gjøres raskere samt at vi hadde redusert tilgang til nøkkelpersonell. Selv med begrenset tid og ressurser har vi kommet frem til et resultat, men det er ikke sikkert vi hadde klart det samme om problemet var mer komplekst. Det kan tenkes at med mer erfaring så vil det være lettere å jobbe med begrensninger.

5.2 Hvordan fungerer rotårsaksanalyse på tabletop øvelse?

Det å utføre en rotårsaksanalyse i form av en tabletop øvelse på en kjent hendelse er ikke lett. Dette fordi det ikke er vanlig for bedrifter å dele mye informasjon om sikkerhetsrelaterte hendelser. Vi hadde ingen mulighet å kontakte de involverte i hendelsen for å etterspørre mer informasjon. Når en rotårsaksanalyse krever at du har den nødvendige informasjonen er det vanskelig å få fullført en tabletop analyse uten antagelser. Mer informasjonsdeling kunne ført til at en slik øvelse var enklere. Videre kunne dette gitt et større læringsutbytte for alle involverte. I Carbanak caset utførte vi en tabeltop øvelse, der kom vi fram til at rotårsaken var at situasjonen ikke var vurdert kritisk nok. Vi utførte dette caset med bare dokumentasjonen som var offentlig. Det førte til at vi måtte gjøre antagelser, særlig på de verktøyne som krevde frekvens. Dette er noe som er vanskelig å unngå med en slik type øvelse.

Etter vi hadde gjennomført Five Whys følte vi oss ikke helt sikre på at vi hadde oppdaget alle rotårsakene. Måten den er beskrevet på i litteraturen gir ingen sjekk for om man har gått glipp av rotårsaker. Vårt funn tyder på at noen av bankene som var utsatt for dette angrepet ikke var forbredt på situasjonen. Det er vanskelig å stoppe en APT da de kan angripe så mange sårbarheter i organisasjonen at det er veldig ressurskrevende å håndtere. Derfor blir det vanskelig å løse alle disse sårbarhetene med en rotårsaksanalyse. Mot en APT er det mulig at implementering av løsningsforslag på rotproblemer bare er med på å redusere risikoen for nye vellykkede angrep. Vi mener at vi ikke får utnyttet rotårsaksanalyse til sitt fulle potensiale på et slikt case. Vi fikk derimot innsikt i at rotårsaksanalyse krever mye informasjon. Som læringsutbytte fungerte dette bra og var derfor verdt tiden vi brukte på det.

5.3 Hvordan fungerer rotårsaksanalyse på et case med mye ressurser og mye tid?

Vi fikk et case av IT-tjensten der vi fullførte en rotårsaksanalyse på hvorfor ansatte og elever lånte adgangskort. Her brukte vi mye tid på å fullføre en grundig undersøkelse. Det vi erfarte med Peformance Matrix er at det er viktig å inkludere nøkkelpersoner for å få et bra resultat. Antagelsene vi hadde gjort var forskjellig fra det IT-tjenesten selv mente. Dette kunne ført til fokus på feil sted.

Datainnsamlingen gikk fortere en det vi antok, og vi fikk gjort flere intervjuer enn først antatt. Vi kunne ha styrt intervjuene mer da det var et par ganger intervjuene sporet av. Det at det var noen spørsmål som viste seg å være irrelevante var å forvente, men vi kunne gjerne stilt flere spørsmål. Vi kunne også ha utformet spørsmålene slik at det hadde vært lettere a samenligne svarene. Analyseprosessen tok lengre tid på grunn av manglende forkunnskaper. Vi måtte sette oss inn i verktøye vi skulle bruke. Her merket vi at det kunne være ønskelig med mer data, særlig spørsmål der svar kunne vert rangert på en skala.

Vår utførelse av rotårsaksidentifiseringen var utfordrende. Der valgte å utføre Fishbone på en måte som gjorde at vi brukte lengre tid enn en annen alternativ måte å utføre det på.

Da IT-Tjenesten utførte sin risikovurdering av problemet, var deres tiltak kameraovervåking. Vår analyse har derimot helt andre tiltak en det IT-Tjenesten har kommet fram til. Her kan vi se at det å bruke forskjellig metodikk på et problem kan gi veldig ulike resultat. Løsningen de kom med prøver å redusere problemet, mens vi forsøker å løse rotårsaken. Dette viser at ved å gjennomføre en grundig rotårsaksanalyse så kan du komme fram til andre tiltak en det man ville ha funnet med en risikovurdering. Her mener vi at det å utføre en rotårsaksanalyse med mye ressurser og tid vil gi resultater som er brukbare og gir forskjellige resultat en det andre metoder ville gitt, for eksempel resultater fra en risikoanalyse. Utifra tiden vi har brukt på caset har vi fått mye erfaring og skapt bedre innsikt i problemet. Vi fikk avdekket holdninger om kortlåning, kjennskap om reserveløsninger og manglende involvering i policy blant ansatte. Vi ser også at det eksisterer forbedringspotensiale innen reserveløsninger og at det ikke er tydelige nok sanksjoner. Vi mener derfor at resultatene rettferdiggjør tidsbruken.

5.4 Hvordan fungerer rotårsaksanalyse på et case med begrenset ressurser og lite tid?

I dette tilfellet utførte vi et case på DDoS angrep mot slettmeg. Her hadde vi begrenset med tid og tilgang til ressurser. Vi hadde kun en kontakt person innad i slettmeg som begrenset mengden med informasjon vi fikk inn. Da vi gjorde datainnsamlingen hadde vi lyst til å prøve Check Sheets. Vi kunne ikke telle opp hvor ofte et problem inntraff, og heller ikke observere problemene under hendelsesforløpet. Det vi valgte å prøve da, var å rangere de forskjellige problematiske hendelsene, og når det viste seg å være vanskelig valgte vi heller å diskutere rundt punktene vi hadde valgt. Vi erfarte at det hadde vært lettere å gjennomføre et intervju under datainnsamlingen. Punktene over problematiske hendelser som vi hadde lagd fungerte bra som spørsmål og var relevante. Selv om vi ikke fikk det til slik som vi hadde tenkt, greide vi å hente data inn alikvel.

Resultatet vi kom frem til viser at det å gjennomføre en rotårsaksanalyse kan gi en

bedre forståelse av situasjonen selv med begrenset ressurser. Vi kom frem til forslag på endringer som slettmeg ikke hadde gjort i etterkant av hendelsen.

5.5 Hvor stor nytteverdi har rotårsaksanalyse innenfor fagfeltet informasjonssikkerhet?

Vi har erfart at ved hjelp av rotårsaksanalyse er det mulig oppdage problemsituasjoner som med andre verktøy brukt innen informasjonssikkerhet ikke er synlige. Vi mener at ved å følge de 7 stegene vi har anvendt i våre analyser, dekkes problemløsningen på en strukturert måte fra å forstå problemet til å implementere en løsning. Innen informasjonssikkerhet kan det være vanskelig å få nok informasjon om problemer da viljen til å dele informasjon kan være begrenset. Da det er vanskelig å utføre en rotårsaksanalyse uten tilstrekkelig informasjon er det viktig med tilgang til nøkkelpersoner og kunnskap om problemet.

Vår erfaring med å bruke rotårsaksanalyse på problemer med mye ressurser og tid og med begrensede ressurser og tid er at under begge tilfellene greide vi å komme frem til et resultat. Dette viser at det er mulig å sette av tid og ressurser ut fra viktigheten til problemet og allikevel oppnå resultater.

6 Konklusjon

Her vil vi gjøre en konklusjon av oppgaven basert på våre forskningsspørsmål.

6.1 Konklusjon

Gruppen er godt fornøyd med å ha gjennomført bacheloroppgaven innen rotårsaksanalyse. Den har vært utfordrende, spennende og vi har tilegnet oss mye ny kunnskap innen dette feltet. Det at rotårsaksanalyse ikke har vært mye brukt innen informasjonssikkerhet har hele tiden vært en driv som vi syns det var spennende å jobbe med, og det ble en ekstra motivasjon for oss til å komme fram til et bra resultat. Det gjorde det samtidig vanskelig å finne litteratur innenfor feltet rotårsaksanalyse i sammenheng med informasjonssikkerhet så det meste av det vi har hatt behov for måtte vi skaffe oss selv.

Vi har lært mye om hva verktøyene i rotårsaksanalyse inneholder og hvordan disse skal brukes. Vi har også sett at det å jobbe med verktøyene flere ganger har gjort at vi jobbet raskere og mer effektivt enn det vi klarte den første gangen vi skulle prøve ut verktøyene. Årene gjennom studieløpet har lært oss mange tekniske ferdigheter, disse har vi ikke hatt stort behov for å bruke da vi jobbet med prosjektet. Imidlertid har fag som “Sikkerhetsplanlegging”, “Hendelseshåndtering”, “Risikostyring” og “Systemutvikling” hjulpet oss underveis i prosjektet.

Vi har lært mye om rotårsaksanalyse, og hvor det er godt anvendbart. Vi håper at våre resultater kan gi bedre innsikt i rotårsaksanalyse og at det viser seg at det er anvendbart innenfor informasjonssikkerhet.

Vår overordnede konklusjon er at vi har fått svart tilstrekkelig på forskningsspørsmålene.

Vi konkluderer med at i form av tabletop-øvelse er det god trening men vi får ikke utnyttet rotårsaksanalyse til sitt fulle potensiale. Dette siden rotårsaksanalyse krever mye tilgang til data og nøkkelpersoner. Det var vanskelig å gå videre på nye funn, da det ikke var mulig å undersøke i etterkant om funnene var reelle, men øvelsen fremstår som et nyttig læring. For personer som lærer seg rotårsaksanalyse gir dette et godt læringsutbytte.

Vi hadde et stort læringsutbytte på caset med mye ressurser og tid. Her lønner det seg å ha forhåndskunnskaper om rotårsaksanalyse for å få fullt utbytte. Vi konkluderer med at der vi hadde mye ressurser og tid, er vi trygge på resultatene våres. Da IT-Tjenesten utførte sin risikovurdering av problemet, var deres tiltak kameraovervåking. Vår analyse har derimot helt andre tiltak en det IT-Tjenesten har kommet fram til. Her kan vi se at det å bruke forskjellig metodikk på et problem kan gi helt ulike resultat. Vi kan heller ikke si med sikkerhet at personer som låner bort adgangskort er grunnen til at hærverk og tyveri har oppstått. Det resultatene våre viser til er at det har vært dårlig kommunikasjon mellom de forskjellige avdelingene på skolen. Vi ser også ut fra dataen vi samlet inn at ansatte ikke vet hva som kan være konsekvens av at kort blir lånt bort. Om ansatte ikke forstår problematikken rundt at adgangskort blir lånt bort er det viktig at dette blir tatt

tak i. Skolen er ansvarlig for at alle ansatte har fått den trening og opplæring som kreves av skolen.

Vi konkluderer også med at et case med begrensede ressurser og tid gir resultater, men problemsituasjonen bør ikke være for stor eller kompleks i forhold til antall personer inkludert i analysen og deres tids begrensninger. Løsningene i vår case er hovedsakelig utenfor Slettmeg.no kontroll da angriperens motivasjon er et hovedmoment. Dersom angriper har tilstrekkelig motivasjon kan de finne en måte å utføre et vellykket angrep på. De løsningsforslagene vi har kommet med baserer seg på prosedyre innad i slettmeg og kontrakt med tjenesteleverandør. Prosedyren dikterer prosessen på hvordan slettmeg bestemmer leverandør. Her menes det sjekk av leverandørs historikk, erfaring som leverandør og kunnskap om hvordan å behandle kjente problemsituasjoner. Vi foreslår at kontrakter med tjenesteleverandører bestemmer at leverandørene skal ha kunnskaper om håndtering av kjente problemsituasjoner og er i stand til å tilby en løsning, som for eksempel blokkering av IP områder.

De 7 rotårsaksanalyse stegene vi anvendte i våre analyser dekker problemløsningen på en strukturert måte fra å forstå problemet til å implementere en løsning. Det er viktig med god forståelse av problemet og tilgang til nøkkelpersoner. Ut fra våre rotårsaksanalyser gir bruk av verktøyne resultater, selv med begrenset tid og ressurser. Vi konkluderer at hvis rotårsaksanalyse skal ha stor nytteverdi, så krever det mye datatilgang og tilgang til nøkkelpersoner. Vi fant ikke ny informasjon vedrørende problemet å tilføye basert på å gjøre RCA på tabletop-øvelse, men øvelsen fremstår som et nyttig læringsverktøy. I tillegg så fant vi at RCA ga resultater i form av rotårsaker for DDoS-caset også, disse var mer på den administrative siden. Arbeidet vårt kastet også lys på RCAs begrensninger i forhold til de tekniske aspektene.

6.2 Kritikk av oppgaven

Det er alltid en læringsprosess å gjøre et så stort proskjekt for første gang, og i etterkant har vi merket noen ting vi ville gjort anderledes. Til å begynne med burde vi ha lagt mer vekt på planlegging selv om vi i utgangspunktet mente vi hadde vert nøye, og prøvd å følge den bedre. Dette ville gitt oss bedre utnyttelse av tiden. Vi skulle gjerne vært flinkere med logføring av vår tidsbruk.

På case 2 kunne vi ha planlagt oppgaven først, hvordan vi skulle gjennomføre den fra start til slutt i tilleg til hvilke data vi kunne trengt. Vi kunne testet intervjuspørsmålene før vi brukte dem, i form av rollespill innad i gruppen. Selv om intervjuene gikk forholdsvis smertefritt, ser vi at det kunne vert en fordel å øvd på intervjuer på forhånd. Vi kunne hatt en større spredning på intervjuobjekter. Vi kunne ha styrt intervjuene mer siden det var et par ganger intervjuene sporet av.

6.3 Veien videre

Innen rotårsaksanalyse er det mye som kan gjøres siden så liten del av rotårsaksanalyse er utforsket i sammenheng med informasjonssikkerhet. Her kan man finne ut hvordan man kan måle kvalitet på resultat som er gjort. Det kan også være interessant å sammenligne våre resultat der man ser på resultatene av forskningsspørsmålene for å se om man kan finne avvik. Man kan også se om man kan bruke bachelor oppgaven vår som en veiledning for å finne rotårsak til et problem samt se på flere verktøy som eksisterer innenfor

denne sjangeren. Her er det en del verktøy vi ikke fikk gått gjennom og utprøvd.

Bibliografi

[1] Andersen, B. & Fagerhaug, T. 2006. *Root cause analysis: Simplified tools and techniques*. ASQ Quality Press, second edition.

[2] The great bank robbery: the carbanak apt. (Visited May 2016). URL: https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/.

[3] den Braber, F., Hogganvik, I., Lund, M. S., Stølen, K., & Vraalsen, F. 2007. Model-based security analysis in seven steps - a guided tour to the coras method. *BT Technology Journal*, 25(1), 101–117.

[4] Wikipedia. 2015. Root cause analysis. [Online; accessed 22-Jan-2016]. URL: https://en.wikipedia.org/w/index.php?title=Root_cause_analysis&oldid=695507624.

[5] Sommerville, I. 2011. *Softwareengineering*. pearson, 9th edition.

[6] Lars Arne Sand, Gaute Bjørklund Wangen, A. S. F. 2010. Hendelseshåndtering i små og mellomstore bedrifter.

[7] Ammerman, M. 1998. *The root cause analysis handbook: A simplified approach to identifying, correcting, and reporting workplace errors*. SteinerBooks, first edition.

[8] Okes, D. 2009. *Root cause analysis: The core of problem solving and corrective action*. ASQ Quality Press, first edition.

[9] Damelio, R. 2011. *The Basics of Process Mapping*. CRC Press, 2nd edition.

[10] Wikipedia. 2015. Spss. URL: https://no.wikipedia.org/w/index.php?title=SPSS&oldid=15194736.

[11] Williams, P. 2001. Information security governance. *Information security technical report*, 6(3), 60–70.

[12] Julisch, K. 2003. Clustering intrusion detection alarms to support root cause analysis. *ACM transactions on information and system security (TISSEC)*, 6(4), 443–471.

[13] Collmann, J. & Cooper, T. 2007. Breaching the security of the kaiser permanente internet patient portal: the organizational foundations of information security. *Journal of the American Medical Informatics Association*, 14(2), 239–243.

[14] Wangen, G. 2015. Conflicting incentives risk analysis: A case study of the normative peer review process. *Administrative Sciences*, 5(3), 125. URL: http://www.mdpi.com/2076-3387/5/3/125, doi:10.3390/admsci5030125.

[15] Whitman, M. E. & Mattord, H. J. 2010. *Management of information security*. CengageBrain. com.

[16] Kaspersky. 2015. Carbanak apt the great bank robbery. URL: https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf.

[17] Krebs, B. 2015. The great bank heist, or death by 1,000 cuts. [Online; accessed 24-Feb-2016]. URL: https://krebsonsecurity.com/2015/02/the-great-bank-heist-or-death-by-1000-cuts.

[18] Krebs, B. 2015. Gang hacked atms from inside banks. [Online; accessed 24-Feb-2016]. URL: http://krebsonsecurity.com/2014/12/gang-hacked-atms-from-inside-banks.

[19] Group IB, F. Anunak: Apt against financial institutions.

[20] video youtube. 2015. Jornt van der wiel: How did the carbanak cybergang steal $1 billion from banks? (1/3). [Online; accessed 22-Feb-2016]. URL: https://www.youtube.com/watch?v=csc9VDuHBNU.

[21] Wangen, G. B. 2015. An initial insight into infosec risk management practices.

[22] Wikipedia. 2016. Advanced persistent threat. [Online; accessed 13-May-2016]. URL: https://en.wikipedia.org/w/index.php?title=Advanced_persistent_threat&oldid=717116198.

NTNU i Gjøvik

Vår dato 09.05.2016
Deres dato

Vår referanse IT-tjenesten, Gjøvik
Deres referanse

Notat

Til:	Ansatte og studenter
Kopi til:	
Fra:	Viserektor
Signatur:	JW

Kameraovervåkning på NTNU i Gjøvik

Frist for innspill: 1. juni 2016

Sendes til: christoffer.hallstensen@ntnu.no

Dessverre har NTNU i Gjøvik observert en økende trend av hærverk og tyveri siste året hvor verdier for 500 000 kr har blitt enten stjålet eller ødelagt, dette er midler som kunne vært brukt til å gjøre campus et bedre sted å være for studenter og ansatte. Vi har i tillegg også observert at adgangskort lånes ut, deles og oftere havner på avveie. På grunn av økt antallet tyverier, hærverk og lav oppklaringsprosent ser vi nå oss nødt til å sette opp overvåkningskameraer som et mottiltak. Erfaringer fra NTNU i Trondheim viser til betydelig mindre saker og økt oppklaringsprosent. Innføring av kameraovervåkning er også i tråd med retningslinjer og praksis på NTNUs campuser i Trondheim.

NTNU i Gjøvik har lenge prøvd å unngå så langt det lar seg gjøre å samle inn mer informasjon enn nødvendig om våre ansatte og studenter, dette har latt seg synes ved at det meste stort sett er åpent på dagtid og at man ikke trenger å benytte adgangskort til å komme inn i labber og undervisningsrom innenfor åpningstid.

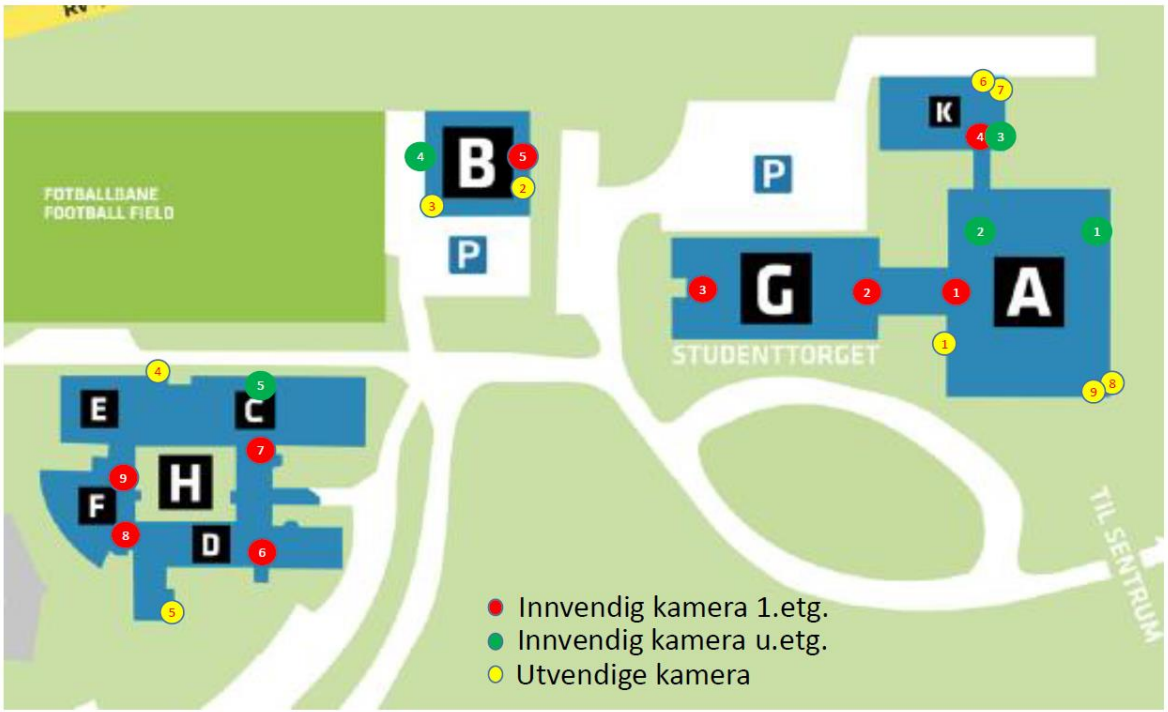
Kameraovervåkning reguleres etter Personopplysningslovens kapittel 7, og defineres som:

«vedvarende eller regelmessig gjentatt personovervåking ved hjelp av fjernbetjent eller automatisk virkende overvåkningskamera eller annet lignende utstyr som er fastmontert.»

Postadresse | **Org.nr. 974 767 880** | **Besøksadresse** | **Telefon** | **Saksbehandler**
Christoffer V. Hallstensen
Tlf: 611 35145

All data i fra kameraovervåkning (definisjonen over) er ansett som sensitive personopplysninger. Utstyret og opptakene vil lagres på IT-tjenestens sikre maskinrom, hvor kun et fåtall personer har tilgang. All tilgang til dette rommet loggføres elektronisk og kun et begrenset antall på IT-tjenesten har mulighet til å komme i kontakt med utstyret. Kun enkeltpersoner på Driftsavdelingen og IT-tjenesten vil ha tilgang til brukergrensesnittet på systemet som vil isoleres fra øvrig infrastruktur. IT-tjenesten drifter i dag den fysiske adgangskontrollen på campus, og samme regime vil opprettholdes for kameraovervåkning. Alle opptak som gjøres på anlegget vil slettes innen 7-dager i tråd med Personopplysningsforskriften[1] dersom det ikke er en juridisk gyldig grunn from å lagre lengre.

Kameraplasseringene blir som vist på denne tegningen:



Før installering av kameraer iverksettes, inviterer viserektor ansatte og studenter til å komme med innspill i saken.

Til orientering har de ansattes fagforeninger v/ Lokalt samarbeidsorgan (LOSAM) gitt sin støtte til beslutningen om kameraovervåking, samt plassering av kameraene som vist på tegningen.

[1] http://lovdata.no/forskrift/2000-12-15-1265/§8-4

Case 1: Carbanak

Henrik Torres, Erlend Brækken, Niclas Hellesen

May 17, 2016

Contents

List of Figures

List of Tables

Executive summary

Vi har tatt en titt på carbanak som er et avansert angrep som ble utført mot banker. Her har vi brukt rotårsaksanalyse, en metodikk som går over syv steg for å avdekke opprinnelsen til problemet. Til å begynne med lagde vi et swimlane-diagram for å få en bedre forståelse av problemet og hvordan handlinger henger sammen. Critical incident ble også brukt for å finne andre relevante problemer som var verdt å undersøke. Videre brukte vi brainstorming for å genere en liste med potensielle problemer som skal undersøkes videre. I dette caset fikk vi ikke utført reel data innsamling, og gjorde gjorde en tabletop øvelse. For å forstå caset bedre brukte vi både relasjon og affinity digram for å kunne visualisere relasjoner bedre. For å komme frem til en rotårsak brukte vi five whys der vi kom fram til at oppdatering av systemet ikke var vurdert kritisk nok. Vi brukte countermesure matrix til å bestemme hvilke tiltak som skal gjøres, og med et tree diagram så får vi fremstilt hvilken rekfølge tiltakene bør utføres i.

1 Introduksjon

Årsaksanalyse kan anvendes for å finne hovedårsakene til at ett eller flere problemer inntraff. En rotårsaksanalyse gjøres i etterkant av hendelsesforløpet, som står i kontrast med risikohåndtering som behandler tenkte situasjoner i fremtiden. Gevinsten av å utføre en rotårsaksanalyse er å kunne finne en eller flere rotårsaker. Når disse er identifisert og løsningsforslag er implementert bør problemer som var konsekvens av problemer opphøre. Dersom de ikke opphører, betyr dette at det ikke var rotårsaken som ble behandlet, eller at det er flere rotårsaker som alene er i stand til å gi konsekvenser.

Vi så at det ikke var anvendt rotårsaksanalyse-verktøy i rapportene som vi anvendte i studiet av Carbanak caset. Dette ga oss en stor mulighet til å kunne anvende rotårsaksanalyse-verktøyene vi kjenner, og observere hvordan de passet til situasjonen.

Denne rapporten er en del av vårt bachelorprosjekt hvor vi ser på rotårsaksanalyse i bruk på informasjonssikkerhet.

Strukturen i dokumentet er delt opp i syv overordnede steg. Hvert steg er en hovedoperasjon av rotårsaksanalyse. I hvert steg er det anvendt en eller flere metodikker som vi kaller verktøy. Vi vil også prøve å nevne andre verktøy enn de som ble anvendt på hvert steg for å henvise til hvilke som eksisterer samt argumentere for de vi valgte. Vi vil så ha underkapitler hvor vi beskriver ønsket utbytte. Dette gjør vi utifra forventningene vi har til verktøyet etter å ha studert Root Cause Analysis Simplified Tools and Techniques Second Edition [1], The Root Cause Analysis Handbook[2] og Root Cause Analysis The Core of Problem Solving and Corrective Action [3]. Gjennomførelsen blir så dokumentert i neste underkapittel. Vi vil så diskutere om verktøyet ga den nytten vi

ønsket i ikke-modifisert tilstand. I det siste underkapittelet til hver metodikk vil vi diskutere om det var noen informasjon om verktøyet vi kunne ønsket å ta med oss. Under idémyldring og diskusjonsprosessen ble det noen ganger forsøkt å la et gruppemedlem ta på seg en rolle som bankansatt, angriper e.l. Vi hadde som håp at dette kunne være med på å øke kreativ tenkning ved at vi så situasjonen med andre øyne. Idéen var inspirert av artikkelen Case Study Role Play for Research and Training[4], men ble utført på en veldig enkel og uformell måte. Rapporten beskriver et verktøy for bruk i situasjoner der informasjon kan være vanskelig å skaffe.

Hovedpunktene i dokumentet følger utførelsen i vår rotårsaksanalyse gjennom sitt naturlige løp med sterke likheter til systemutvikklingsmodellen Fossefall, startende med problemforståelse og ender med løsnings implementasjon. Hvert kapittel begynner med en introduksjon til selve steget i analysen hvor vi forklarer hva det går ut på.

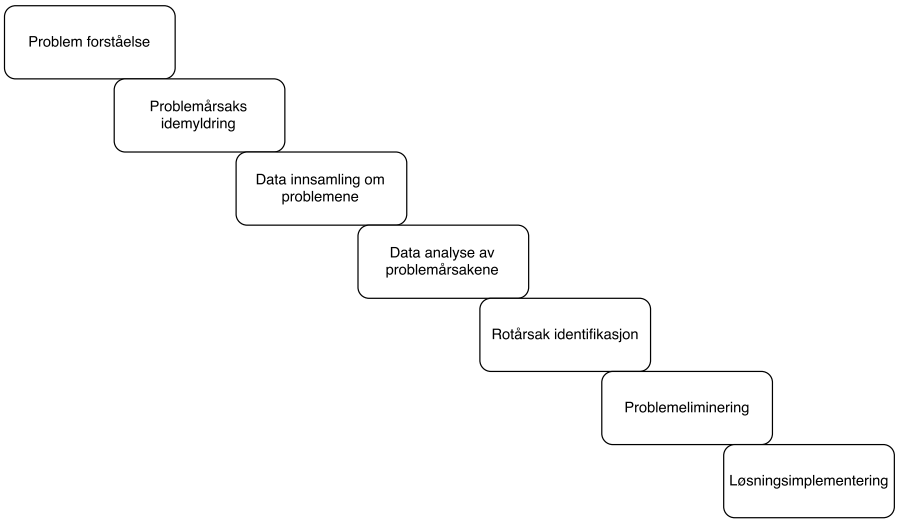


Figure 1: Waterfall

2 Problemforståelse

Carbanak er et avansert angrep utført av en organisert gruppe. Angrepet går ut på å få kontroll over nettverket til en finansiell institusjon og derretter tappe dem for penger. Vi kommer til å basere oss på informasjon fra Kaspersky[5], to artikkler fra Brian Krebs[6][7], artikkelen Anunak: APT against financial institutions [8] samt youtube klipp[9] har gitt ut om hendelsen. Hele caset er basert på åpne kilder. Rapportene gir ikke et fullstendig bilde, så når det er nødvendig vil vi gjøre antagelser. Vi tenker at vi kommer inn i etterkant av hendelsen og gjør en rotårsaksanalyse for å finne ut om det er noen underliggende problemer som bidro til at institusjonene ble rammet av angrepet.

Bildet viser en oversikt over utførelsen av angrepet 2 og er hentet ifra The Great Bank Robbery: the Carbanak APT [10].

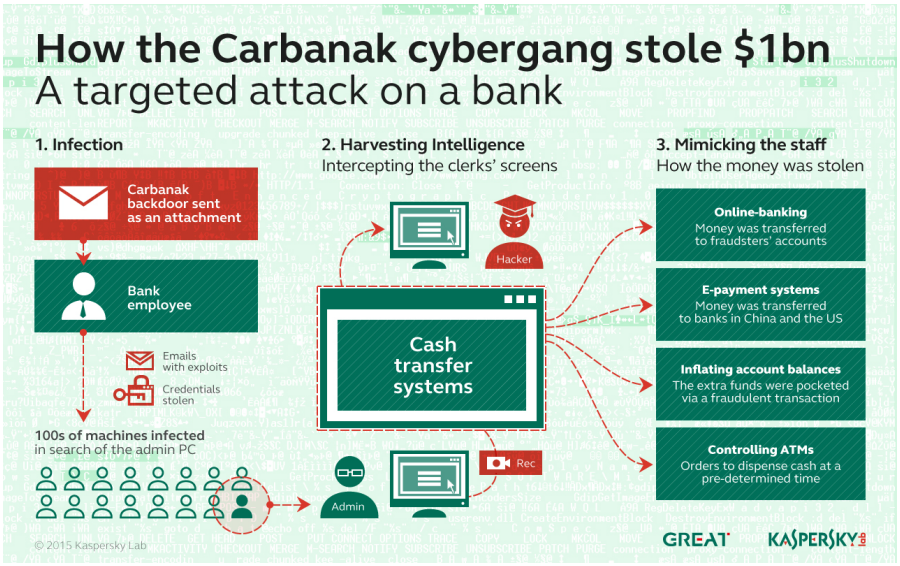


Figure 2: Bilde er laget av Caspersky

2.1 Swim Lane Flowchart

En ansatt i banken vil logge seg inn på sin arbeidsstasjon. Personen vil så oppdage e-posten fra angriperene som er maskert som en autentisk e-post. Vedlegget til e-posten åpnes og maskinen kan regnes som infisert. Vi kan ikke se bort fra at ansatte kan ha åpnet flere infiserte e-poster fra angriperene bak Carbanak. Når angriperene nå har tilgang til maskinen, er de på innsiden av nettverket. Her er det beskrevet i Kaspersky sin rapport[5] at angriperene overvåket de ansattes bruk av IT systemer. Dette ga dem kunnskap om hvordan IT systemene fungerte og de lærte seg hvordan de kunne utføre administrative

oppgaver. Denne kunnskapen kunne brukes til å manipulere databaser for å endre pengeverdier på bankkunders konto. De tre største metodene som ble brukt i dette angrepet var tømming av minibanker, overføring via SWIFT [1] og manipulasjon av pengebeløp på bankkontoer.

Ønsket utbytte av Swim Lane flowchart verktøy

Det vi ønsker som utbytte er en tydelig visning av flyten gjennom utførelser og hendelser. Forhåpentligvis kan det vise veier av flyt som ikke var synlig uten grafisk fremtstilling. Ønsket utbytte er å få en økt detaljforståelse og avdekke forbindelser mellom elementene vi ikke like lett kunne oppdaget.

Gjennomførelse av verktøy

Vi startet med å tegne opp et Swim Lane flowchart. Det blir anvendt brainstorming under utførelsen av Swim Lane flowchart, og den nye informasjonen bør kunne bli synliggjort på hvor den tilhører i tidsperspektivet gjennom hendelsesforløpet. Med dette ønsket vi å få en oversikt over hendelsesforløpet via en grafisk fremstilling som vist i figur 3.

[1] Society for Worldwide Interbank Financial Telecomminucation er en en samarbeidsorganisasjon banker og andre livssynsorganisasjoner rundt om i hele verden. Bankene i Norge benytter i dag SWIFT's formidlingssystem for å kunne gjennomføre betalingsoppdrag, hovedsakelig betalinger til og fra utlandet.[11]

Elementene i Swim Lane flowchart

Her følger en beskrivelse av elementene i Fig: 3.

1. *Login* Her ser vi for oss at angriperene allerede har fått malware lastet inn på en av maskinene til banken og er i stand til å aksessere en brukerkonto.

2. *PC* Dette er en av arbeidsstasjonene som er en av bankens eiendeler. Det er her ansatte åpner infiserte e-poster.

3. *E-post* Her tenker vi på e-poster generelt, hvor angriperenes infiserte e-postvedlegg befinner seg.

4. *Verktøy* Administrative verktøy som anvendes av ansatte. Dette inkluderer ikke bare bankens generelle brukere men også administratorer sine verktøy.

5. *Generell administrasjon* Er en anvendelsen av verktøy eller ren administrering av bankansattes oppgaver.

6. *Minibank* Dette er både minibankene som fysisk er lokalisert rundt om i landene samt programvaren som administrerer minibankene.

7. *Penger* Pengene som er i flyt fra banken og i retning angriperene.

8. *Angriper* Carbanaks bakmenn.

Vi har nå fått tegnet opp et hendelsesforløp slik som vi kan se det for oss, tatt i betraktning den informasjonen vi har hatt tilgjengelig.

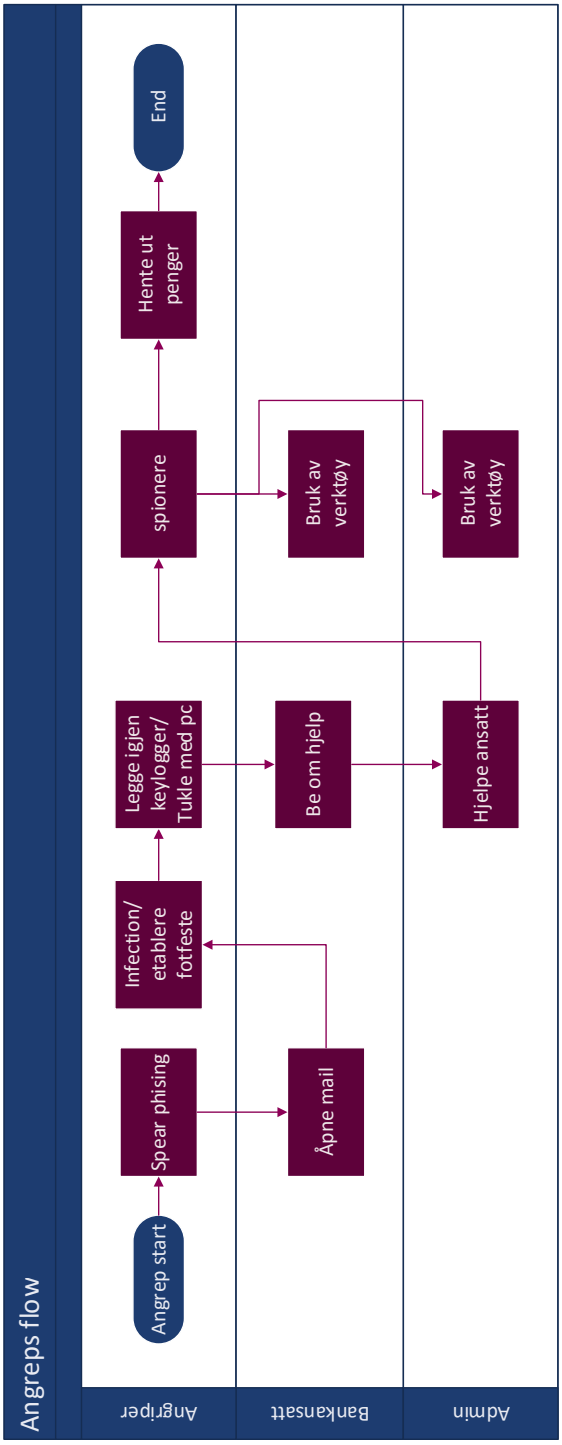


Figure 3: Carbanak swimlane

2.2 Critical incident

Hovedformålet med critical incident verktøyet er å forstå hva de mest plagsomme symptomene er i en problematisk situasjon. Ved bruk av critical incident skal man få en bedre forståelse på hvilke aspekter av problemet som må løses, samt innse problemets natur og dens konsekvenser. Som med de fleste verktøyene innen årsaksanalyse er de best anvendt av et team for å finne årsaken til problemet. For å fungere, krever det en atmosfære av tillit, åpenhet og ærlighet som oppfordrer folk til å røpe viktig informasjon uten å frykte konsekvensene. Dette gjelder alle verktøy men spesielt critical incident da denne kan bringe frem potensielt pinlige situasjoner.

Ønsket utbytte Vi er nå ute etter å få laget en liste med hendelser som har skjedd og rangere disse etter frekvens i håp om å få et bilde av hvor ofte hendelsene forekommer. Vi vil se på om en visuell fremstilling av rangering etter frekvens kan være med på å gi et riktig inntrykk av viktighetsgraden til elementene.

Utførelse Under utførelse av critical incident verktøyet så vi at vi ikke var i stand til å anskaffe frekvens verdiene. Vi ble derfor nødt til å gjøre noen logiske antagelser basert på den informasjonen som vi hadde tilgjengelig.

Navn	Frekvens
Mistenkelig trafikk	Høy
Overvåking av maskiner	Høy
Åpning av e-post vedlegg	Medium
Brudd på regelverk	Medium
Utro tjenere	Lav
Angripere har tilgang på servere	Lav
Ikke oppdaget infeksjon på IT systemer	Lav
Uvitenhet om spionprogramvare	Lav
Uopplærte medarbeidere	Lav

Table 1: Carbanak Critical Incident table

Beskrivelse av vektene

Under følger en beskrivelse av vektene anvendt i Table: 1.

1. *Høy* Inntreffer daglig.
2. *Medium* Ukentlig.
3. *Lav* Månedlig eller sjeldnere.

Vi gikk så sammen om å liste opp det vi så på som sikkerhetshendelser og antok en frekvens. Vi gjorde disse antagelsene basert på følgende argumenter: Lav frekvens når det skjer månedlig eller sjeldnere. Medium frekvens, det skjer ukentlig. Høy frekvens, det skjer daglig.

Mistenkelig trafikk
Malwaren på bankenes infiserte maskiner kommuniserer med C2 (command and control) serverene. Her antar vi at denne type trafikk er høy siden angriperene hele tiden hadde tilgang til banksystemene.

Overvåking av maskiner
Maskinene har blitt overvåket gjennom hele hendelsesforløpet. Spesifikt under læringsprosessen hvor angriperene studerte verktøyene bankene brukte samt at de lærte hvordan å utføre en rekke administrative handlinger.

Åpning av e-post vedlegg
Her ser vi på hendelser hvor ansatte åpner e-post vedlegg der avsenderene var Carbanak angriperene. Vi gjør en forutsetning at dette kan ha hendt mer enn en gang. Angriperene kan ha brukt infiserte maskiner til å sende e-poster med ekte avsenderadresse til andre brukere i systemet. Målet med dette er å komme seg dypere inn i IT infrastrukturen.

Utro tjenere
Vi kan bare gjøre en forutsetning at det finnes utro tjenere i bankene under denne perioden som var med på gjennomføringen av Carbanak angrepene. Vi har derfor heller ingen dokumentert frekvens på dette, men i forhold til de andre hendelsene som er tatt, vil vi anta en lav frekvens i betraktning.

2.3 Konklusjon av verktøyene

Konklusjonen vår ang. swim lane flowchart så ga denne oss et visuelt bilde der vi kan se flyten på angrepet som ble gjennomført som igjen gir oss en større detaljforståelse av hvordan angrepet ble utført.

Når det gjelder critical incident så er dette basert på antagelser vi hadde etter å ha lest rapportene. Her skulle den egentlige utførelsen ha numerisk data noe som gjorde det litt problematisk siden vi ikke fikk utført verktøyet slik det var ment å brukes. Allikevel mener vi det greit å anslå verdiene som Høy, Medium og Lav. Det ga oss ikke et korrekt visuelt bilde på hvor frekvensen var høyest, men kun antagelser vi følte var logiske.

2.3.1 Ga verktøyet oss den nytten vi ville i ikke-modifisert tilstand?

Swim Lane Flowchart
Anvendelsen av swim lane flowchart har gitt oss det visuelle overblikket som

var ønsket. Samtidig ga dette oss muligheten til å se alternative ruter angrepet kunne ta igjennom systemer og prosesser i banken. Under anvendelsen av dette verktøyet fikk vi et endret syn på hendelsesforløp og diskutert oss imellom. En enighet om flyten fra start til slutt av infeksjon og utnyttelsesforløpet ble oppnådd, og dette ser vi på i etterkant som svært viktig for senere arbeid.

Critical incident

Selv om vi manglet numeriske data for å kunne utfylle verktøyets krav fullstendig, var vi i stand til å substituere disse dataene med generelle subjektive verdier som Høy, Medium og Lav. Dette kan naturlighvis gjøre det litt utydelig på hvor stort skille det er mellom elementer innenfor samme rangering. Vi ser at når informasjonen mangler en del numeriske data, slik som de fleste dokumentene vi studerte gjorde, ga denne generaliseringen oss mulighet til å allikevel høste inn noen av fordelene til verktøyet.

Endringer som vi ser som nyttige er ikke en endring i seg selv, men heller et tillegg. Innen informasjonssikkerhet er det ikke nødvendigvis alle som kan frigjøre detaljerte data uten å åpne seg selv for sårbarheter. Derfor er det ikke alltid like praktisk at et verktøy gjør krav på eksplisitte numeriske data for å kunne utføres. Variabler som rangeres innenfor definerte rammer kan anvendes istedenfor numeriske frekvenser, men dette vil redusere klarheten i hvilke elementer på tabellen innenfor samme ramme som skal plasseres over eller under hverandre. Det gir også et nytt krav til bruken av verktøyet, disse variablene som brukes som frekvenser defineres, og at elementene i tabellene får en forklaring på hvorfor de er plassert der de er.

3 Problemårsaks idemyldring

I problemårsaks idemyldring finnes det en del generiske verktøy som kan brukes på ulike stadier i analysen. De vi har sett på er brainstorming, brainwriting, is - is not, nominell gruppeteknikk og parvise sammenligninger. For eksempel så bidrar brainstorming til å generere ideer om mulige årsaker. Siden analysen normalt gjennomføres i grupper er metoder som hjelper med å komme til enighet også nyttige.

3.1 Brainstorming

Her finnes det flere verktøy å velge. Det vi velger i dette tilfellet er ustrukturert brainstorming, siden det passer gruppen og siden ingen dominerer prosessen. I ustrukturert brainstorming kan alle som er med fritt komme med forslag og ideer spontant, dette kan gi andre deltagere nye idéer de selv ikke ville klart å kommet på. Dette tillater alle gruppemedlemmene å komme med forslag på hvordan tilfellene i problemforståelsen kan forekomme. Her er det viktig at man ikke kommenterer, positivt eller negativt kommentarer til forslagene, men lister opp flest mulig forslag før de blir finkjemmet og kategorisert.

3.1.1 Ønsket utbytte

Målet er å generere en liste med problemer som kan forbedres og identifisere mulige konsekvenser som stammer fra problemet som blir analysert. Det har også som hensikt å generere mulige årsaker til problemet samt oppfordre til tenking som kan eliminere årsakene.

3.1.2 Gjennomførelse

Her setter gruppen seg ned for å gjøre en idemyldring. Det er viktig å avgjøre om det skal være ren verbal gjennomførelse eller en som foregår skriftlig. De tilstedeværende genererer forslag til hva som kan være problemårsaker og disse blir så visuelt presentert på en tavle eller via en projektor. Vi anvendte brainstorming verbalt på tavle.

I vårt tilfelle ble disse punktene generert etter ca 20 min med 3 personer til stede.

1. Manglende oppdatering av programvare/patching.
2. Manglende sett med retningslinjer eller manglende oppfølging av disse.
3. Sen reaksjon på at minibanker ble tømt for penger.
4. For liten kontroll på ressursbruk på IT systemer.
5. Mangelfull opplæring av ansatte.
6. Tillot ukjent inn/ut-trafikk av nettverket.
7. Utro ansatte.
8. Vedlegg blir ikke filtrert godt nok.
9. Bedriftspionasje.
10. For sjeldent bytte av passord.
11. Dårlig segregering av maskiner i nettverk.
12. Dårlig videreoppfølging av opplæring.
13. Lite overvåking av nettverkstrafikk (ut/inn).
14. Etablere baseline (manglende).
15. Manglende varsling på mistenkelig aktivitet.
16. Manglende loggføring.
17. Virus eller malware (skadelig programvare).
18. Fysisk tilgang til maskiner og minibanker.
19. Uvanlig ressurssterk angriper

Etter vi har listet opp alle forslagene er det nødvendig å evaluere ideene i grupper enten via tema eller i rekkefølge der rangeringen går fra høyere til lavere potensiale. Vi velger å rangere ideene våre etter høyere til lavere potensiale.

1. Manglende oppdatering av programvare/patching.
2. Manglende sett med retningslinjer eller manglende oppfølging av disse.
3. Etablere "baseline" (manglende)
4. Tillot ukjent inn/ut-trafikk av nettverket.
5. For sjeldent bytte av passord
6. Manglende varsling på mistenkelig aktivitet
7. Utro ansatte
8. For liten kontroll på ressursbruk på IT systemer.
9. Mangelfull opplæring av ansatte.
10. Dårlig videreoppfølging av opplæring
11. Vedlegg blir ikke filtrert godt nok
12. Lite overvåking av nettverkstrafikk (ut/inn)
13. For lite gjennomgang loggføring
14. Dårlig segregering av maskiner i nettverk
15. Fysisk tilgang til maskiner og minibanker
16. Virus eller malware (skadelig programvare)
17. Sen reaksjon på at minibanker ble tømt for penger.
18. Bedriftspionasje

Etter å ha sortert listen, valgte vi å gruppere listens elementer i grupper de naturlig tilhører.

1. Opplæring og etterfølging av ansatte.
    - Manglende sett med retningslinjer eller manglende oppfølging av disse.
    - Mangelfull opplæring av ansatte.
    - Dårlig videreoppfølging av opplæring.
    - For lite bytte av passord.
2. Svakheter.
    - Manglende oppdatering av programvare/patching.

- Manglende etablering av baseline.
- Manglende varsling på mistenkelig aktivitet.
- Sen reaksjon på at minibanker ble tømt for penger.
- Virus eller malware (skadelig programvare).

3. System og nettverksovervåking.
    - Tilatt ukjent inn/- ut trafikk av nettverket.
    - Lite overvåking av nettverkstrafikk (ut/inn).
    - For lite gjennomgang loggføring.
    - For liten kontroll på ressursbruk på IT systemer.
    - Dårlig segregering av maskiner i nettverk.
    - Vedlegg blir ikke filtrert godt nok.
4. Bedrifts trusler.
    - Utro ansatte.
    - Bedrift spionasje.
    - Fysisk tilgang til maskiner og minibanker.
    - Særs ressurssterk angriper

3.1.3 Konklusjon av verktøyet

Vi var i stand til å generere en liste med elementer som trenger forbedring. Ved å gruppere disse elementene inn i grupper blir det også øyeblikkelig mer forståelig for leserene. Grupperingen gir oss muligheter til å kunne gjøre antagelser på hvilke elementer som gir konsekvenser innenfor samme problemområde. Utførelsen og utbytte sto til forventningene. Fordeler ved bruk av dette verktøyet er derfor å finne, samt å få en oversikt over problemene. Kunnskap om hvilke elementer som har relasjoner med hverandre blir skapt.

4 Problemårsaks datainnsamling

Datainnsammlingsfasen er med på å gjøre søkene etter problemer mer treff sikkre. Det er derfor viktig å planlegge nøye hvilke verktøy som en kan tenke seg å anvende. Verktøyet som er anvendt her er beskrevet under, samt en liten beskrivelse av hvilke andre verktøy som også kan anvendes til datainnsamling.

4.1 Intervjuer

Det er viktig å være imøtekommende for de som skal intervjues. En god ide kan være å anvende samme stemme under intervju spørsmålene som under introduksjonen. Når spørsmål stilles bør ikke spørsmålene kunne svares på med bare ja eller nei dersom dette ikke er ønsket. Ha også en del spørsmål ferdig laget på forhånd. Da har en bedre tid til å passe på at spørsmålene ikke blir tvetydige.

Det finnes andre verktøy som kunne vært anvendt på dette steget. Tre eksempler på andre verktøy er sampling, surveys og check sheets. Sampling fungerer ved at en henter ut informasjon fra en mindre gruppe mennesker som representerer en større gruppe. Surveys er en spørreundersøkelse hvor alle som er inkludert i interessegruppen mottar et spørreskjema. I spørreundersøkelsen er man i stand til å hente ut den enkeltes personlige meninger. Check sheet er et verktøy for å registrere data etterhvert som de er samlet inn. Dette er en god måte å strukturere dataene på.

4.1.1 Ønsket utbytte

Ved å gjennomføre intervjuer håper vi å få en forståelse av bedriftens indre miljø og muligens informasjon som kan hjelpe til med å avdekke utro ansatte eller korrupsjon. Vi ønsker kunnskaper om deres rutiner og hvor god etterfølgelse av rutinene er. Det er viktig å få informasjon om hvilken versjon av softwaren er på da malware angrep utnytter sårbarheter i programvare som enda ikke er blitt oppdatert.

4.1.2 Gjennomførelse

I tillegg til intervju, ville vi spurt om logger bedriften sitter på. Intervjuet kunne verdt gjort med omtrent 20 personer og helst minst fire til fem administratorer eller andre høyere ansatte. Det virker rimelig å anta at det vil ta én time per intervju.

Hva ville vi hatt tilgang til om vi skulle hentet inn data selv?

1. Logger
2. E-post
3. Overvåkingsbilder
4. Datatrafikk
5. Verktøy
6. Versjonskontroll
7. Prosessorer som kjører
8. Nettverkskart
9. Liste over ansatte

Intervju med admin/manager

1. Hvor ofte bytter dere passord?
2. Har dere god nok oversikt over trafikk som går inngående og utgående?
3. Filtrerer dere spam/e-post, i så fall hvordan?

4. Blir loggene gått gjennom, hvor langt tilbake logger dere? Finnes det automatisering på dette?
5. Hvordan er IDS, IPS, antivirus og firewall konfigurert.
6. Hvor lang tid etter oppsigelse blir brukerkontoer/nøkkelkort terminert.
7. Hvordan er rettighetene pr. brukerkonto satt opp.
8. Hvor ofte merker dere mistenkelig trafikk?
9. Er alt oppdatert og "patchet" så fort som overhodet mulig?
10. Hvordan er oppdateringsrutiner?
11. Har ansatte fått tilstrekkelig opplæring?
12. Har dere eksterne som leverer systemet?

Intervju til ansatt

1. Hvor ofte bytter dere passord?
2. Hvilke rettigheter har dere?
3. Hva slags rutiner har du for åpning av e-post?
4. Hvordan er varslingssystemet dere har?
5. Har dere tilgang til ekstern oppkobling?

4.1.3 Konklusjon av verktøyet

Med hensyn til at dette blir sett på i retrospektiv perspektiv, ville vi ellers potensielt kunnet hentet ut mengder med god informasjon. Dette er et verktøy som krever tilgang til personer under etterforskning eller i etterkant dersom det gjøres forskning på tidligere hendelser. Det vil ikke kunne være noe problem å bruke verktøyet i etterkant så lenge en ikke ønsker å hente ut informasjon fra personer som er for detaljert, eller som er informasjon mennesker ikke kan lagre over lengre perioder.

Istedenfor å gjøre en modifikasjon på selve verktøyet kunne det vært mulig å inkludere andre verktøy, som en kombinasjon av intervju over telefon samt spørreskjema i etterkant som henviste til telefonintervju med mennesker som deltok aktivt under hendelsesforløpet.

Summert opp kan vi si at verktøyet ikke ga oss den informasjonen vi trengte siden vi arbeidet fra utsiden uten tilgang til nødvendig informasjon. Vi mener verktøyet er godt egnet til datainnsamlingen da "face to face" kommunikasjon kan være en god kilde til informasjon gitt at en har tilgang til ansatte. Denne metodikken bruker derimot lang tid for de som intervjuer, samt at antall personer som kan behandles iløpet av en dag er basert på antall intervjuer. Verktøyet er lett å anvende da det hovedsakelig baserer seg på å samle inn informasjon gjennom å stille spørsmål og lytte til svar. Derimot er det viktig å ta hensyn til metoder som gjør intervjuene mye mer effektive. Det inkluderer måten personen som intervjuer opptrer på, hvilke spørsmål som stilles og hvordan de blir stilt.

5 Problemårsaks dataanalyse

Det er viktig å se på hvordan forskjellige aspekter av problemet er koblet sammen. Her anvender vi noen verktøy for å oppnå akkurat dette. Det som er viktig i denne sammenheng er hvordan ting henger sammen. Dermed så har vi prøvd å bruke to forskjellige verktøy til å vise relasjoner, der den første er et relasjonsdiagram.

5.1 Relasjonsdiagram

Relasjonsdiagram er et verktøy som brukes til å identifisere logiske sammenhenger mellom ulike ideer eller problemer i en kompleks og forvirrende situasjon. I slike tilfeller så er styrken til relasjonsdiagrammet dens evne til å visualisere slike forbindelser. Et relasjondiagrams viktigste formål er å bidra til å identifisere forhold som ikke er lett gjenkjennelig.

5.1.1 Ønsket utbytte

For å forstå sammenhengen mellom det som skjer, så har vi valgt å lage et relasjons diagram. Med dette håper vi å belyse hva som påvirker hva og kunne avdekke relasjoner som ikke var oppdaget i tidligere fase.

5.1.2 Gjennomførelse

Det ble tegnet en stor sirkel på tavlen. Deretter begynte vi å liste opp elementer vi så på som viktige og overordnede nok til å kunne begynne å tegne relasjonene seg imellom. Ut fra den informasjonen vi hadde hentet inn fra de to tidligere fasene, kunne vi avgjøre hvilke elementer som det skulle tegnes piler mellom. Vi ser på det som naturlig at det er diskusjon under utførelsen av dette verktøyet.

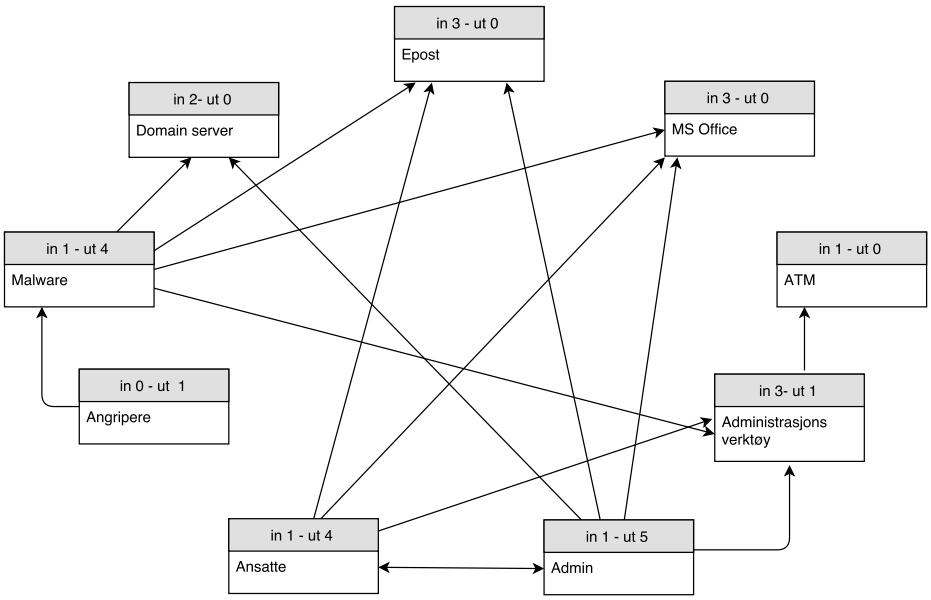


Figure 4: Relation Diagram

5.1.3 Ga verktøyet oss den nytten vi ville i ikke-modifisert tilstand?

Vi oppdaget ingen relasjoner som vi ikke tidligere hadde sett for oss. Det hjalp oss å få en visualisering om at angriperenes kommunikasjon gikk ene og alene gjennom malware, som kan virke som en selvfølge på et teknisk nivå, men er ikke nødvendigvis like lett synlig for alle som ikke har gode IT ferdigheter og kunnskaper.

Vi konkluderer derfor med at verktøyet er lett å anvende, åpner for diskusjon mellom gruppemedlemmer og gjør relasjoner synlig og tilgjengelig selv om det skulle være manglende tekniske kunnskaper hos noen av medlemmene.

5.2 Affinity diagram

Et affinity diagram hjelper med å korrelere tilsynelatende urelaterte ideer, betingelser, betydninger og årsaker, slik at de kan kollektivt bli utforsket videre. Når man skal analysere kvalitative data så er affinity diagram nyttig da den grupperer data og funn av underliggende forhold som kobles sammen i grupper.

5.2.1 Ønsket utbytte

Vårt ønskede utbytte ved å bruke dette verktøyet er å kunne redusere ned funn fra brainstorming i problemårsaks idemyldring og dataene fra problemårsaks data innsamlingsfasen og få gruppere forslagene inn i nye naturlige grupper.

Dette gjør det mulig å få et nytt og bedre bilde av situasjonen og alle elementene vi har generert og samlet inn.

5.2.2 Gjennomførelse

Under gjennomførelsen av affinity diagram, ble en rekke punkter generert ut fra de to tidligere fasene, og disse ble diskutert grundig. Punktene var fysisk plassert på en tavle under diskusjon, og ble så ført inn i et dataprogram hvor det var virtuelle lapper på en tavle. Kolonner som ikke var navngitt fra starten ble fylt tilfeldig med punktene vi genererte på tavlen. Så kunne hver person på sin egen maskin flytte disse lappene rundt til alle var enige om plasseringene. Deretter fikk gruppene navn ut fra hvilke lapper som befant seg i hver av dem.

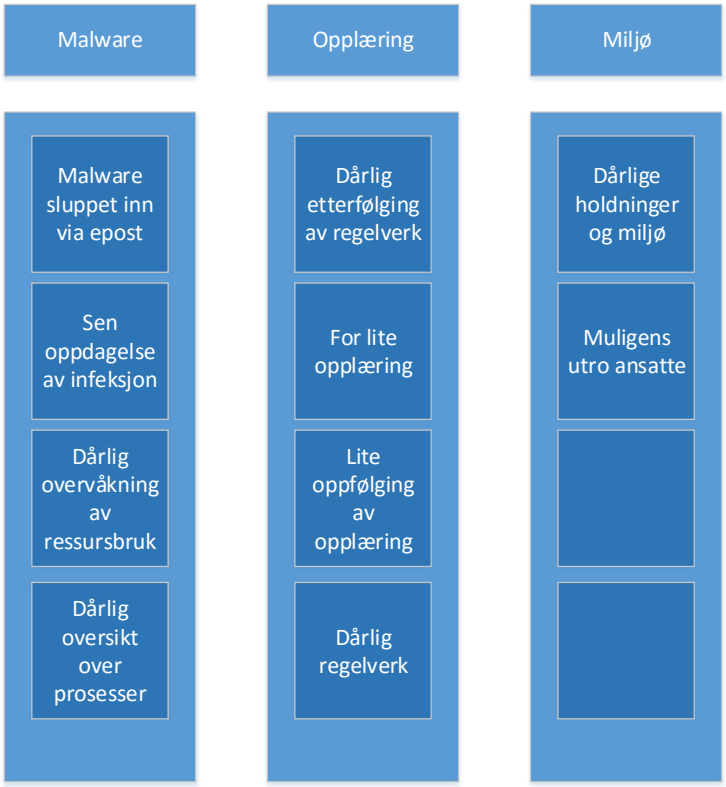


Figure 5: Affinity Diagram

5.2.3 Ga verktøyet oss den nytten vi ville i ikke-modifisert tilstand?

Informasjonen vi endte opp med var mer redusert og raffinert enn den vi satt med fra tidligere faser. Ut fra dette var det ikke stor endring i vår forståelse av situasjonen. En bedre oversikt har blitt oppnådd da vi har fått gruppert relaterte årsaker inn i klasser.

5.2.4 Hvilken informasjon om verktøyet kan vi ta med oss til senere bruk?

Verktøyet hadde mange likheter med andre verktøy, som for eksempel brainstorming i problemårsaks idemyldring fasen hvor ideer ble listet og kategorisert i grupper.

6 Rotårsaksidentifisering

Under rotårsaksidentifisering er poenget å utarbeide løsninger som vil fjerne årsaken og dermed eliminere problemet.

6.1 Five whys

Når vi kommer til Rotårsaks identifisering er vi nesten ferdig med analysen. Det er her vi skal kunne komme med en aktuell rotårsak for problemet. I vårt tilfelle velger vi å bruke et verktøy som heter five whys. Poenget med dette er å dykke dypere inn i nivåer til årsakene og dermed få et bredere spekter av årsaksanalysen. Hovedformålet er å stadig spørre "Hvorfor?" når en sak har blitt identifisert og dermed gå igjennom nivåene i årsaken.

Five whys går ut på å identifisere et problem deretter spørre hvorfor dette er et problem. Da man kommer til et svar så spør man igjen hvorfor. Dette repeteres vanligvis fem ganger til man klarer å komme til rotårsaken, men det kan også ta færre eller flere ganger.

6.1.1 Ønsket utbytte

Vårt ønskede utbytte var å gjøre et dypdykk i informasjonen vi hadde tilgjengelig for å søke etter en eller flere rotårsaker. Ved å anvende denne teknikken håper vi på å komme dypt nok til at de problemene vi lander på er de faktiske rotårsakene. Ønsket utbytte vil også være å avdekke mer enn en enkel rotårsak. Vi ser for oss at når en rotårsak avdekkes, vil det være psykologisk fristende å lande de andre seriene med five whys på samme rotårsak da vi vet at den allerede eksisterer.

6.1.2 Gjennomførelse

Vi avgjør startpunktet for analysen, enten et problem eller en identifisert rotårsak som vi mener bør analyseres grundigere. I vårt tilfelle startet vi med "Hvorfor spytter minibanken ut penger?". Vi skrev dette opp på whiteboard

Table 2: Five whys

Hvorfor spyttet minibanken ut penger?	
Fordi systemet var kompromitert	
Hvorfor?	Fordi angriperene utnyttet en exploit da ansatte åpent mail
Hvorfor?	Fordi programmvaren ikke var up to date.
Hvorfor?	Fordi banken hadde dårlige/mangelfulle rutiner på oppdatering.
Hvorfor?	Ble ikke vurdert til å være kritisk nok

og brukte teknikken Idemyldring for å finne årsaken til startpunktet. Her er poenget å spørre hvorfor er dette årsak til det orginale problemet. Det vi kom fram til etter vi hadde utført five whys var at systemet til bankene ikke var oppdatert grunnet dårlig/mangelfulle rutiner. Dette er kun en antagelse da vi ikke vet med sikkerhet.

6.1.3 Konklusjon av verktøyet

Vi var i stand til å lande på en rotårsak. Det er ikke synlig om andre årsaker kan være rotårsaker. Verktøyet fungerte svært effektivt og det tok kort tid å nå et resultat.

6.1.4 Ga verktøyet oss den nytten vi ville i ikke-modifisert tilstand?

Det kan gjøres en antagelse om at verktøyet kan være litt isolerende på rotårsaken dersom det bare anvendes en gang.

6.1.5 Hvilke endringer kunne vi tenke oss å gjøre på verktøyet for å få det til å passe bedre?

En kunne tenke seg å modifisere det slik at det kjørte forskjellige iterasjoner på et minimum antall hovedspørsmål dersom de er tilgjengelige, for å forhindre at brukerene føler seg tilfreds med bare å kjøre verktøyet på ett spørsmål.

6.1.6 Hvilken informasjon om verktøyet kan vi ta med oss til senere bruk?

Vi ser at det kan lønne seg å generere noen flere hovedspørsmål og kjøre verktøyet på disse fremfor bare å kjøre ett, som vi gjorde i vårt eksempel med "Hvofor spyttet minibanken ut penger?". Dette er for å forsøke å landet på flere rotårsaker.

7 Problemeliminering

7.1 Countermeasures Matrix

7.1.1 Ønsket utbytte

Vårt ønskede utbytte er å finne hva som best eliminerer årsakene til problemene samtidig som kostnad og risiko blir tatt hensyn til.

7.1.2 Gjennomførelse

Action Plan

Vi tok utgangspunkt i funn fra tidligere faser og vi plasserte disse så inn i en countermeasure matrix for å kunne anta effekt og gjennomførbarhet. Vi antar effekt og gjennomførbarhet på vektene 1 til 5 hvor 1 er lav og 5 er høy basert på funn fra tidligere faser i analysen.

Ved bruk av standardvariabler så kommer det ikke frem potensielle risiko og bivirkninger ved å gjennomføre en løsning, som kan føre til, feks. at gjennomføring av forslag blir urealistisk. Det å prøve å bruke flere eller forskjellige variabler hjalp heller ikke siden det førte til mer krøll og usikkerhet en det den presiserte.

Vektene i matrisen regnes slik: $Effekt \cdot Gjennomførbarhet = Produkt$
Det ble bestemt at dersom sum blir mer enn 10, er det et godt alternativ for implementering.

Assess Effectiveness

Vi får ikke gått inn og sett på effekten av tiltakene, da vi ikke har tilgang til slik informasjon eller systemene til bankene.

Table 3: Countermeasures Matrix

Mottiltak	**Effektivitet**	**x Gjennomførbarhet**	**= Sum**	**Action**
Oppdatering	4	5	20	Ja
Patching	4	5	20	Ja
Auto-updates	4	2	8	Nei
Opplæring	2	5	10	Ja
Baseline	4	3	12	Ja
Monitorering	4	4	16	Ja
Stenge banken midlertidig	2	1	2	Nei
Trace angrep tilbake	2	1	2	Nei
Upgrade legacy systemer	5	2	10	Nei
Sandboxing	3	3	9	Nei
Test miljø	4	3	12	Ja
Gjennomgang av logg	3	5	15	Ja
Scan av e-post	3	4	12	Ja

Hvordan skal effekten monitoreres
Vi har ingen mulighet til å kunne gå inn å monitorere effekten hos bankene.

Confirm Corrective Action(s) are Solving the Problem
Vi har ikke muligheten til å kunne gå inn å se om problemet ble løst, og derfor blir det ikke mulig å fullføre disse punktene i verktøyet heller:

1. Report Recommended Corrective Action(s), as Appropriate.
2. Standardize to Prevent the Problem From Recurring.
3. Take Additional Actions as Appropritate.
4. Formiddle resultatene som nøvendig.

7.1.3 Konklusjon av verktøyet

Klare definisjoner hjelper veldig under anvendelsen av dette verktøyet. Verktøyet er ikke i stand til å ta i betraktning hvilken konsekvens et mottiltak kan ha. Vekter på mottiltakenes effektivitet og gjennomførbarhet kan være med på å skape oversikt dersom noen personer har lettere for å forholde seg til numeriske data. Matrisen synliggjør hva som er viktig for bedriften eller organisasjonen ved å ha tiltakene presentert visuelt rangert.

7.1.4 Hvilken informasjon om verktøyet kan vi ta med oss til senere bruk?

Som nevnt i konklusjonen av verktøyet er det veldig viktig å bare anvende verktøyet dersom definisjoner av elementene som skal inn i matrisen er nøye definert.

8 Løsningsimplementering

8.1 Tree diagram

8.1.1 Ønsket utbytte

Vårt ønskede utbytte var en struktur av oppgavene som skulle utføres. Vi håpet å vise linker mellom det som skulle gjøres og hvilke aktivitet det ble forbundet med.

8.1.2 Gjennomførelse

Først genererte vi en liste over aktiviteter som må utføres for å implementere løsningen. Vi skrev ned hver aktivitet, i form av et verb etterfulgt av et substantiv. Deretter rangerte vi aktivitetene i logiske undergrupper med aktiviteter som utføres i rekkefølgen de plasseres. Det siste vi gjorde var å sette sammen undergrupper i en samlet sekvens for å illustrere hele planen av tree diagram.

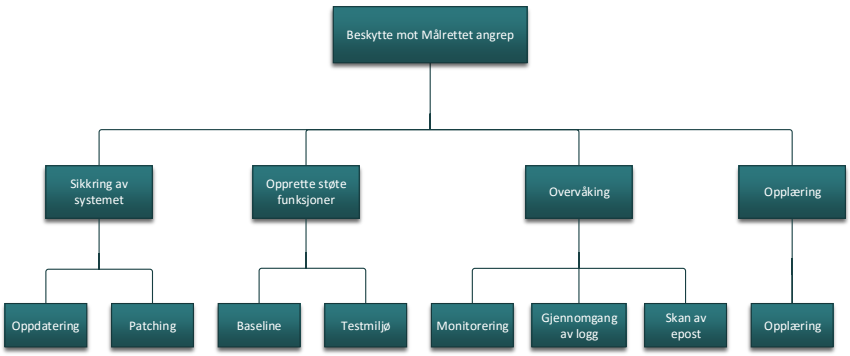


Figure 6: Tree Diagram

8.1.3 Konklusjon av verktøyet

Ved bruk av verktøyet fikk vi den oversikten vi forventet. Det er nå mulig for oss å vise grafisk hvilke tiltak som tilhører hvilke grupper. Vi fikk vist linker mellom det som skulle gjøres og aktivitetene de ble forbundet med, rekkefølgen aktivitetene utføres i ble synlig.

8.1.4 Ga verktøyet oss den nytten vi ville i ikke-modifisert tilstand?

En modifisering som var nødvendig var å utelate dato på tree diagramet. Dette fordi vi kom inn i situasjonen i etterkant samtidig som den blir observert fra utsiden. Vi har derfor ikke tilgang på disse dataene.

9 Diskusjon og konklusjon

Et kort sammendrag av rapporten og resultater.

9.1 Tidsbruk

Den totale tiden brukt på case 1 er omtrent 100 timer per person (300 timer).

Tabellen under viser bare den konsentrerte tiden brukt på selve verktøyene iløpet av vellykket forsøk, men inkluderer ikke tiden brukt på diskusjon av valg og testing av verktøy og rapport skriving.

Table 4: Loggføring

Loggføring av tidsbruk på verktøyene		
Fase	**Verktøy**	**Tidsbruk t=timer m=minutter**
Problemforståelse	Critical Incident	3t15m
Problemårsaksidemyldring	Brainstorming	2t30m
Problemårsaks datainnsamling	Interjuv	3t
Problemårsaks dataanalyse	Relasjons diagram	6t
	Affinity diagramm	4t
Rotårsaks identifisering	Five whys	1t
Løsningsimplementering	Countermeasures Matrix	3t
Problem eliminering	Tree Diagram	3t30m
		Total 26t 15m

9.2 Resultater

Vi vil liste opp resultatene av rapporten i følgende underkapitler.

9.2.1 Problemforståelse

Carbanak er malware brukt mot banker. Angriperene hadde tilgang til bankenes IT systemer, og kunne overvåke ansatte samt hente penger ut fra banken. Angrepet er av en skala som likner på hva en APT kunne stått bak. I forsøk på å forstå problemet ble swimlane flowchart og critical incident anvendt.

Swim lane flowchart ble valgt ovenfor en mer generell flowchart da vi fikk sett på handlingsflyten mellom forskjellige aktører (admin, angriper ol.). Resultatet viste at angrepet var introdusert inn i banken via spearphising e-post, og handlingsmønsteret mellom angripere, typiske ansatte og administratorer.

Critical incident ble anvendt for å få oversikt over hendelser som har skjedd og i hvilken frekvens. Vi hadde ikke mulighet til å komme opp med numeriske data, og måtte derfor supplementere med variable frekvensnavn. De to hendelsene med høyest frekvens var mistenkelig trafikk og overvåkning av maskiner.

9.2.2 Probemårsaksidemyldring

Her ønsket vi først og fremst å generere en liste med problemer som kan være konsekvens av rotproblemet Carbanak, med et håp om at disse skulle kunne lede til hvor rotproblemet var i vår senere analyse. Muntlig brainstorming ble anvendt. Utførelse av verktøyet er svært enkelt å utføre praktisk. Mange forslag på svakheter ble generert og deretter gruppert. Disse resultatene blir så videre raffinert i de neste fasene av analysen.

9.2.3 Problemårsaks datainnsamling

Under innsamlingsprosessen ble det foreslått bruken av intervjuer. Det var ikke mulig for oss å utføre intervjuene da vi ikke har tilgang til ansatte i bankene og sikkerhetsselskapene. Det ble laget en liste med spørsmål som vi antok ville vært svært hjelpsomme å kunne fått besvart, som rutiner og etterfølgelse av disse, hvilken softwareversjoner de hadde mm. Valget av intervju baserer seg også på ønske om å kunne avdekke bedriftens indre miljø. Med informasjon om miljøet blir det lettere å skulle se på muligheter for utro ansatte.

9.2.4 Problemårsaks dataanalyse

Her var vi primært ute etter å se på hvordan aspekter av problemet er koblet sammen. Derfor var det et naturlig valg å starte med å tegne et relasjons diagram. Relasjons diagrammet utførtes i plenum via en idemyldring hvor gruppemedlemmene foreslo sine argumenter på hvordan de hadde forstått at problemets elementer hang sammen. Diagrammet viste hvilke forbindelser og i hvilken retning forbindelsen gikk imot. Vi tilegnet oss ikke noen ny kunnskap, annet enn at det vi allerede var klar over, nå var visuelt fremstilt og lettere fordøyelig.

Affinity diagrammet ble anvendt for å redusere ned sårbarhets og svakhets-funn fra tidligere faser til mer målrettede og grupperte funn. De nye gruppene ble malware, opplæring og miljø. Utførelse kan gjøres på en tavle i plenum.

9.2.5 Rotårsaks identifisering

Her er vi på selve identifiseringen av rotårsakene. Ønsket her er å finne minst en rotårsak. Verktøyet som ble anvendt var five whys. Vi oppfattet verktøyet som svært effektivt til å finne en enkelt rotårsak. Derimot ble det ikke synlig om det kunne være flere rotårsaker. Rotårsaken vi kom frem til var at bankene ikke hadde sett på sårbarhetene som kritiske nok til at det var kost-nytte-effektivt

nok til å forbedre. Verktøyet er lett å utføre og trenger ingen trening på forhånd for å mestre.

9.2.6 Problemeliminering.

I jakten på løsninger ble det anvendt countermeasure matrix. Flere av stegene her var ikke gjennomførbare siden vi ser på problemet fra utsiden. I matrisen ble mottiltak numerisk målt via antatt effektivitet multiplisert med gjennomførbarhet. Dersom produktet ble 10 eller mer, vil mottiltaket bli anbefalt. Implementering av et mottiltak kan ha risiko for å føre til implikasjoner med andre systemer. Derfor diskuterte vi muligheten av å legge til en kolonne for risiko ved implementering av mottiltaket. Resultatet av diskusjonen endte med enighet om at det ville bli for mye krøll og usikkerhet rundt endring av verktøyet. To av hovedtiltakene med høyest numerisk verdi vi kom frem til var oppdatering og patching.

9.2.7 Løsningsimplementering

En liste over aktiviteter som må til for å implementere en løsning på problemet ble grafisk fremstil i naturlig rekkefølge for utførelse. Dette ble gjort via et tree diagram figur 6. I diagrammet vises løsningsrekkefølgen fra nederst til venstre mot høyre.

9.3 Diskusjon

Gjennomføring av rotårsaksanalyse på Carbanak caset viste seg å være vanskelig på områder der informasjonen ikke var tilgjengelig og der vi ikke hadde mulighet til å kunne komme i kontakt. Det fantes verktøy som var utviklet for situasjoner innen risiko håndering og annet sikkerhets arbeid der informasjon ikke er tilgjengeligjort forskerene. Dette kan være forårsaket av at bedrifter og organisasjoner ikke ønsker å vise til sårbarheter de har eller har hatt. Vi ser at verktøyene som var i litteraturen som vi anvendte ikke var designet for informasjonssikerhet men andre fagfelt, og dette ga grunnlag for vår bachelor oppgave, hvor denne rapporten er en del av. Det er godt mulig at vi kunne funnet litteratur som dekte vårt felt, men med begrenset tid og ressurser anvendte vi 5 bøker ved siden av artiklene om Carbanak caset. Vårt håp er at del-rapportene samt hovedrapporten vi produserer kan være anvendbar for videre forskning på rotårsaksanalyse for informasjonssikkerhet, uansett hvilken vei resultatene peker. Vi tror at å følge analyseprosessen i klare planlagte faser med stort varierende verktøysett kan gi gode resultater i søket etter rotårsaker. Vi kom frem til antagelsen om at mangelfulle rutiner på oppdatering var en årsak til infeksjonen, som igjen var en konsekvens av at det ikke ble vurdert kritisk nok til å behandles. Det kan være tre synsvinkler å se problemet på. Den føreste, som vi tok tak i, var å se på hvordan å behandle situasjonen slik at den ikke oppstår igjen ved å redusere angrepsvinklene. To andre synsvinkler er

å se på hvorfor de ikke ble vurdert kritisk nok på oppdateringer, eller hvordan å finne løsninger som gjør at de vil se anderleder på det i fremtiden.

References

[1] Andersen, B. & Fagerhaug, T. 2006. *Root cause analysis: Simplified tools and techniques*. ASQ Quality Press, second edition.

[2] Ammerman, M. 1998. *The root cause analysis handbook: A simplified approach to identifying, correcting, and reporting workplace errors*. Steiner-Books, first edition.

[3] Okes, D. 2009. *Root cause analysis: The core of problem solving and corrective action*. ASQ Quality Press, first edition.

[4] Rajbhandari, L. *Risk Analysis Using "Conflicting Incentives" as an alternative notion of Risk*. PhD thesis, Gjøvik University College, 2013.

[5] Kaspersky. 2015. Carbanak apt the great bank robbery. URL: https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf.

[6] Krebs, B. 2015. The great bank heist, or death by 1,000 cuts. [Online; accessed 24-Feb-2016]. URL: https://krebsonsecurity.com/2015/02/the-great-bank-heist-or-death-by-1000-cuts.

[7] Krebs, B. 2015. Gang hacked atms from inside banks. [Online; accessed 24-Feb-2016]. URL: http://krebsonsecurity.com/2014/12/gang-hacked-atms-from-inside-banks.

[8] Group IB, F. Anunak: Apt against financial institutions.

[9] video youtube. 2015. Jornt van der wiel: How did the carbanak cybergang steal $1 billion from banks? (1/3). [Online; accessed 22-Feb-2016]. URL: https://www.youtube.com/watch?v=csc9VDuHBNU.

[10] The great bank robbery: the carbanak apt. (Visited May 2016). URL: https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/.

[11] Hva er swift. (Visited Feb 2016). URL: https://www.sparebank1.no/ostfold-akershus/kort-og-betaling/utland/iban-og-swift/.

Case 2: Adgangskort

Henrik Miguel Torres, Erlend Brækken, Niclas Hellesen

May 17, 2016

Contents

List of Figures

List of Tables

Executive summary

Vi har fått i oppdrag av IT tjenesten for å se på hvorfor kort blir lånt bort, og hva som kan gjøres for å redusere dette. Her har vi brukt rotårsaksanalyse, en metodikk som går over 7 steg for å avdekke opprinnelsen til problemet. Til å begynne med utførte vi en performance matrix for å få en bedre forståelse av problemet og hvordan handlinger henger sammen. Deretter utførte vi en brainstorming for å komme på relevante problemer som var verdt å undersøke. Datainnsammlingen gikk ut på å utføre intervjuer på ansatte og studenter som vi deretter analyserte for å finne sammenhenger og særtrekk fra forskjellige organisatoriske felt på skolen. Vi behandlet dataene i verktøy som kvalitativ analyse, kvantitativ analyse og SPSS. Vi grupperte mottiltak fra intervjuobjektene inn i et affinity diagram for at vi skulle kunne visualisere relasjoner bedre. For å komme frem til en rotårsak brukte vi verktlyet fishbone diagram, ut fra dette fant vi ut at problemene er

1. Litt manglende/utydlige reserveløsninger.
2. Dårlig kommunisering om reserveløsningene som eksisterer.
3. Arbeiderenes effektivitet er ikke likestilt med IT-Tjenestens ønske om sikkerhet.
4. Lave sanksjoner av å låne bort adgangskort.

Deretter brukte vi SIT på å bestemme hvilke tiltak som skal gjøres og et tree diagram for å beskrive rekkefølgen på utførelsen. Til slutt kommer vi med en konklusjon etterfulgt av en diskusjon av analysen.

1 Introduksjon

Årsaksanalyse kan anvendes for å finne hovedårsakene til at ett eller flere problem inntraff. En rotårsaksanalyse gjøres i etterkant av hendelsesforløpet, som står i kontrast til risikohåndtering som behandler tenkte situasjoner i fremtiden. Gevinsten av å utføre en rotårsaksanalyse er å kunne finne underliggende årsaker. Ved å løse disse årsakene vil man forhindre at de skal skape flere problemer.

Denne rapporten er en del av vårt bachelorprosjekt hvor vi ser på `rotårsaksanalyse` brukt innen informasjonssikkerhet.

Oppgavebeskrivelse
I denne casen har vi sett på hvorfor ansatte og elever låner bort adgangskortet sitt, samt om det er mulig å finne en rotårsak som kan fjerne behovet for å bruke andre sine adgangskort. Oppgaven har vi fått av IT-tjenesten og er: "PIN og adgangskort skal være privat, men det hender ofte at studenter og ansatte allikevel deler disse med familie, venner, kolleger og andre studenter. Dette fører til at urettmessig tilgang blir gitt til NTNU i Gjøviks fasiliteter. Dette er et gjentagende problem som forekommer flere ganger i året, og IT-tjenesten har fått rapportert inn hendelser relatert til dette. Det er også sannsynlig at det er flere uoppdagede risiko trusler relatert til dette."

Det har vært konkrete tilfeller av tyveri av svært dyrt utstyr på skolen og konsekvenser kan også være utnyttelse av privilegie escalation samt brudd på policy. Privilegie escalation i kontekst av vårt case er når noen øker sin tilgang til ressurser som en ikke skal ha tilgang til. Ved at en elev eller ansatt låner adgangskort av noen som har tilgang til flere rom og ressurser, vil nå låntakeren ha økt sin egen tilgang forbi det personen var ment å ha.

Struktur
Strukturen i dokumentet er delt opp i syv overordnede steg. Hvert steg er en hovedoperasjon av rotårsaksanalysen. I hvert steg er det anvendt en eller flere metodikker som vi kaller verktøy. Vi vil så ha underkapitler hvor vi beskriver ønsket utbytte. Dette gjør vi utifra forventningene vi har til verktøyet etter å ha studert Root Cause Analysis Simplified Tools and Techniques Second Edition [1], The Root Cause Analysis Handbook[2] og Root Cause Analysis The Core of Problem Solving and Corrective Action [3]. Gjennomførelsen er så dokumentert i neste underkapittel. Deretter ser vi om verktøyet ga den nytten vi ønsket og til slutt diskuterer vi om det var noe informasjon om verktøyet vi kunne ønsket å ta med oss.

Vi håper å avdekke hvorfor dette skjer og hva som er rotårsak til denne type misbruk.

Målet med studien er å validere etablerte rotårsaksanalyse (RCA) verktøy for informasjonssikkerhet. Gruppen RCA-NTNU har utført en rotårsaksanalyse med den hensikt å avdekke rotårsakene til dette problemet. Gruppen begrenset sin undersøkelse til PhD-stipendiater, akademisk personell, management, IT-Tjenesten, studenter og eksterne aktører.

Hovedpunktene i dokumentet følger utførelsen i vår rotårsaksanalyse gjennom sitt naturlige løp med sterke likheter til systemutviklingsmodellen Fossefall, startende med problemforståelse og ender med løsningsimplementasjon. Hvert kapittel begynner med en introduksjon til selve steget i analysen hvor vi forklarer hva det går ut på.

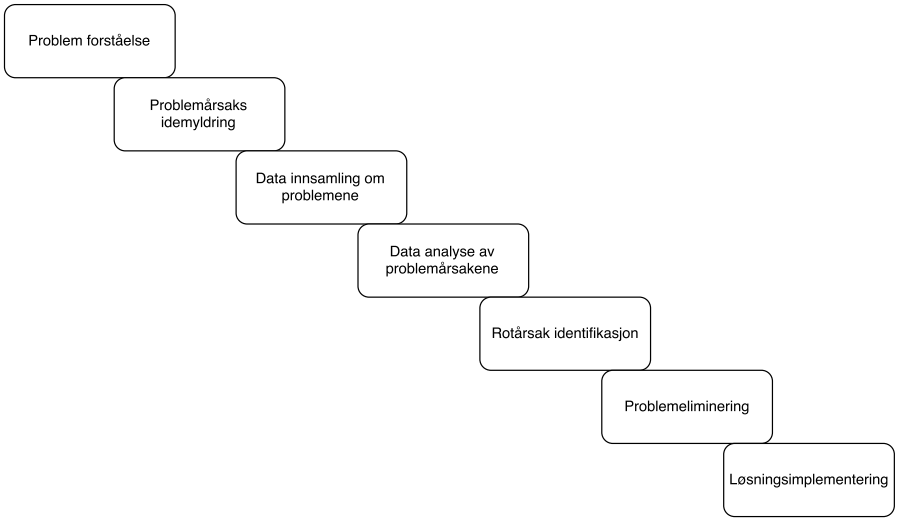


Figure 1: RCA prossesen som skrevet av Andersen og Fagerli [1]

2 Problemforståelse

Da vi fikk casen fra IT-Tjenesten om å se på hvorfor PIN og adgangskort på NTNU i Gjøvik blir delt er det viktig at vi forstår hele aspektet av oppgaven vi skal begi oss ut på. Vi må være sikker på at vi virkelig forstår hva IT-Tjenesten har gitt oss i oppgave. Derfor er det viktig at vi med sikkerhet forstår selve problemet før vi i det hele tatt kan begynne å tenke på hva som kan være årsak.

Verktøyene i problemforståelsen er ment for å gi en bedre forståelse på selve oppgaven og på hvilke aspekter i saken man burde titte nærmere på. I dette caset vil vi bruke Preformance Matrices som verktøy under problemforståelse. Stegene i verktøyet preformance matrice er hentet fra boken Root Cause Analysis Simplified Tools and Techniques Second Edition [1].

2.1 Performance Matrix

Performance Matrices blir brukt til å illustrere nåværende ytelse og viktighet på samme tid. Dette hjelper med å komme frem til en oppfatning av prioritet. Performance Matrices brukes til å illustrere problemer eller årsaker i form av:

- Hvilken del av problemet er det viktigst å angripe?
- Hvilke problem, dersom fjernet, vil redusere flest symptomer?

De to punktene over stammer i fra Root Cause Analysis Simplified Tools and Techniques [1].

Ønsket utbytte
Her ønsket vi å finne ut nåværende ytelse og viktighet på samme tid for å vite hvilken del av problemet det var viktigst å angripe først og hvem problem som vil redusere flest symptomer. Her ønsket vi å inkludere IT-Tjenesten ved at de svarte på noen spørsmål om hvor viktig policyen er for dem, hvordan den fungerte, hvordan sikkerhetskulturen er og diverse andre spørsmål. Spørsmålene er presisert og definert i beskrivelsen av gjennomførelsen av verktøyet.

Gjennomførelse av verktøy
Da vi hadde fått informasjonen vi trengte fra IT-Tjenesten startet vi på stegene som beskrevet i boken:

1. Først konstruerte vi tomt et diagram ved å plassere "importance" på den horisontale aksen og "current performance" på den vertikale aksen som hver er delt opp i ni like segmenter.
2. Deretter bestemte vi hvilke faktorer å analysere.

3. Vi plasserte hver faktor i diagrammet i henhold til sin posisjon langs de to aksene, ved hjelp av symboler for å identifisere hver faktor. Det å plassere faktorene inn på rette plass bør gjøres av noen som kjenner til problemet godt fra før. I vårt tilfelle gjorde vi dette selv før vi gikk til IT-Tjenesten for å bekrefte om vi hadde oppfattet rett. Etter at IT-Tjenesten fikk se verdiene vi hadde satt faktorene inn i, ble de justert.

4. Etter at alle faktorer er plottet inn i diagrammet, delte vi diagrammet i fire kvadranter omtrent på midten av hver akse. Hvert kvadrat fikk et eget navn: Overdrevet, Uviktig, Ok og Må forbedres. Hvis mange faktorer var samlet i ett område, plasserte vi linjene litt lenger til en side.

5. Til slutt bestemte vi hvilke faktorer som var innenfor rett kvadrat.

Spørsmålene til IT-tjenesten er listet under. Svarene er gradert på en skalar fra 1 til 9 hvor 1 er lavt rangert og 9 er høyt rangert.

1. Teoretisk sikkerhetspolicy (hvor godt kjent er folk med policy: gammel og ny).
   (a) Importance: Hvor viktig er det at folk er kjent med den? Svar: 6.
   (b) Performance: Hvor mange kjenner til den? Svar: 3.
2. Praktisk sikkerhetspolicy (hvor godt den er implementert i organisasjonen).
   (a) Importance: Hvor viktig er den? Svar: 7.
   (b) Performance: Hvordan fungerer den nå? Svar: 5.
3. Sanksjoner/konsekvenser på brudd på policy.
   (a) Importance: Hvor viktig er sanksjoner/konsekvenser? Svar: 7.
   (b) Performance: Hvor godt fungerer sanksjoner/konsekvenser? Svar: 6.
4. Sikkerhetskultur.
   (a) Importance: Hvor viktig er det med god sikkerhetskultur? Svar: 7.
   (b) Performance: Hvor bra sikkerhetskultur er det? Svar: 6.
5. Reserveløsninger for kortutdeling ved glemt kort/besøkende.
   (a) Importance: Hvor viktig er det med reserveløsninger? Svar: 6.
   (b) Performance: Hvor godt er det fungerende? Svar: 6
6. Kortutdeling ved nyansettelse.
   (a) Importance: Hvor viktig blir dette sett på? Svar: 9.
   (b) Performance: Hvor godt fungerende er det? Svar: 8.

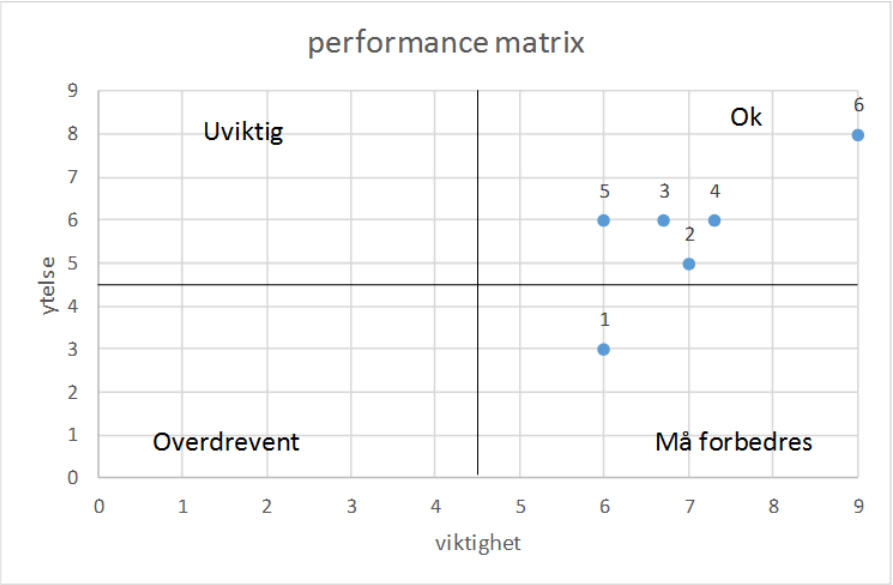


Figure 2: Performance Matrix

Y Aksen representerer "nåværende ytelse" og X aksen representerer "viktighet".

2.1.1 Konklusjon av verktøyet

Da vi antok verdier og pratet med IT-Tjenesten i ettertid for å bekrefte resultatene, var det store forskjeller fra våre forslag og IT-Tjenestens. Dette viser at man bør ha med noen som kjenner til den daglige driften når man utfører en preformance matrice. Verktøyet ga oss svar på viktigheten til problemene og det ga oss en start på hvor vi skulle starte å angripe problemet. Det hjalp oss også med å forstå problemet bedre.

2.2 Oversikt over situasjon

Vi ser på situasjonen som illustrert i figuren 3, at en angriper utnytter at en student eller ansatt låner bort kort og pin eller etterlater en dør åpen. Dette kan skyldes mangel på sikkerhets trening eller kjennskap til regelverk samt at regelverk ikke nødvendig vis tydelig nok viser til at dette ikke er akseptabelt. Dersom student eller ansatt gir bort kort og pin eller glemmer å lukke dører vil angriper kunne unngå byggets innebygde sikkerhets tiltak og få aksess til maskinvare eller sensitiv informasjon.

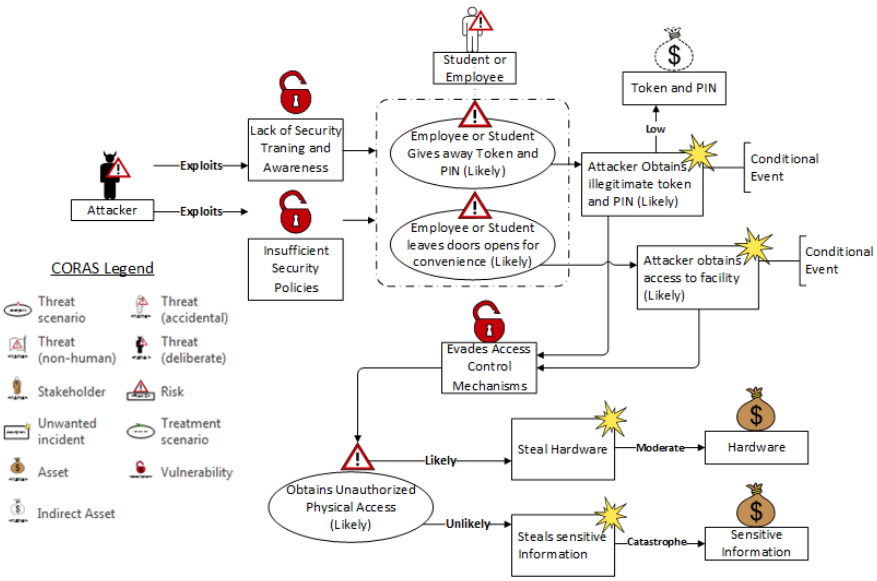


Figure 3: Oversikt over situasjonen. Tegningen er laget i samarbeid med vår veileder

3 Problemårsaks idemyldring

Denne fasen av rotårsaksanalysen er med på å samle forslag til mulige årsaker av caset. Forslag diskuteres og nye ideer vil kunne bli dannet i løpet av prosessen. Når forslag til et problem blir diskutert og analysert ser vi for oss at sannsynligheten for at fokus som blir brukt på feil problemer reduseres.

3.1 Brainstorming

Brainstorming kan foregå på forskjellige måter, strukturert eller ustrukturert brainstorming og brain writing [1]. En strukturert brainstorming baserer seg på at medlemmene etter tur kommer med forslag for å forsikre at ikke en person dominerer. Ustrukturert brainstorming tillater spontane svar fra hvem som helst i gruppen til enhver tid. Brain writing kan utføres på to måter [1]. Gruppemedlemmene skriver ned ideene sine på såkalte idekort, eller på en tavle.

Vår gruppe har gode erfaringer med brainstorming, og vet at det kan anvendes som del av andre verktøy, og kan brukes til å få gruppen i gang dersom medlemmene føler de står fast. Under en brainstorming runde er det viktig at ideer og forslag ikke kritiseres før helt til slutt da alle ideene og forslagene skal gjennomgås.

3.1.1 Ønsket utbytte

Her var det ønskede utbytte å komme opp med flest mulige årsaker til at personer ved skolen ønsker å låne kort av andre og hvilken konsekvens dette får. Det å høre andres forslag hjalp oss med å komme på nye punkter.

3.1.2 Gjennomførelse

En ustrukturert brainstorming ble utført. Hvert gruppemedlem kunne til enhver tid komme med forslag som ble notert på en tavle. Når ingen var i stand til å utarbeide flere forslag, ble forslagene gjennomgått. Vi fjernet forslag vi mente at ikke var relevante. Alle forslagene ble så sortert over i 2 grupper, årsaker og konsekvenser, listet under.

Årsak til lån av adgangskort

1. "Privilage escalation" for å komme seg inn på rom.
2. Glemt kortet sitt et eller annet sted.
3. Gi venner og bekjente tilgang til treningsrom.
4. Låne til printing.
5. Bruk av ansatttoalett.

6. Tilgang til utstyr.
7. Tilgang til låste dører der man ikke har adgang.
8. Stoler på vedkommende.
9. Flaut/vanskelig å si nei.
10. Ta eksamen for andre.
11. Spionasje, sabotasje, planting av bakdører, kjennskap til infrastruktur.
12. Hente ting.

Konsekvens

1. Policy brudd.
2. Tyveri.
3. Tapt arbeid.
4. Studweb pga samme pin. (meldes av fag).
5. Tap av rykte.
6. Terrorisme eller spionasje mot CCIS, NISlab, NorSIS, ol.

3.1.3 Konklusjon av verktøyet

Ved å utføre en brainstorming fikk vi ett raskt overblikk over potensielle årsaker til hva som kan være grunnlag for kortlåning og hvilke konsekvenser dette påfører skole, personell og studenter. Vi kan konkludere med at gruppen blir mer enstemt og samkjørt etter en slik prosess og at verktøyet derfor har en positiv virkning på gruppen i seg selv.

4 Datainnsamling og analyse

I dette kapitelet vil vi gå nermere på verktøy vi brukte for datainnsamling, analyse samt komme med en konklusjon av hva rotårsaken kan være.

4.1 Problemårsaks datainnsamling

Datainnsamlingsfasen er med på å gjøre søket etter problemer mer treffsikre. Det er derfor viktig å planlegge nøye hvilke verktøy en kan tenke seg å anvende. Vi valgte å bruke intervju i denne fasen. Litteraturen vi brukte er fra The Root Cause Analysis Handbook[2] og Root Cause Analysis The Core of Problem Solving and Corrective Action [3].

4.2 Intervjuer

Intervjuer ble gjort med 36 ansatte og studenter ved NTNU i Gjøvik.

4.2.1 Ønsket utbytte

Vårt ønskede utbytte er å avdekke holdninger samt kultur vedrørende adgangskort hos interessentene. Vi undersøkte om ansatte hadde lest policyen og om de hadde noen meninger angående i hvilken grad de skulle få være med på utformingen av policyer. Det var viktig for oss å finne ut om ansatte så på policyen som et hinder eller om de var fornøyde. Vi knyttet spørsmålene vi stilte til "Performance Matricen" vi utførte i kapittelet for problemforståelsen.

4.2.2 Gjennomførelse

Intervjuene ble gjennomført på grupperom eller på intervjuobjektenes kontor. Forutenom IT-tjenesten og manegment var utvelgelsen av intervjuobjekter var vilkårlig. Innenfor de to sistnevnte valgte vi ut nøkkelpersonell i form av beslutningstagere, policy-forfattere og ansvarspersoner i drift av adgangskontroll.

De forskjellige organisatoriske instansene vi intervjuet var Management, IT-Tjenesten, A-IMT, HOS, TØL og eksterne. Innenfor de forskjellige instansene intervjuet vi førsteamanuensiser, postdoktor, lektorer, avdelingsledere, professorer, dekaner, PhD-stipendiater, master studenter, renholds ansatte, statsbygg ansatt, IT-Tjenesten og management.

Utifra dette laget vi 6 grupper. De forskjellige gruppene var:

- Management: Denne gruppen inneholder alle dekaner og middle management vi har intervjuet
- IT-Tjenesten: Denne gruppen inneholder alle på IT-Tjenesten med lederroller og sikkerhet vi har intervjuet
- Akademiskpersonel: Denne gruppen inneholder alle førsteamanuensiser, postdoktor, lektorer, avdelingsledere, professorer vi har intervjuet
- PhD: Denne gruppen inneholder alle PhD-stipendiater vi har intervjuet
- Student: Denne gruppen inneholder alle mastergrad studenter vi har intervjuet
- Ekstern: Denne gruppen inneholder alle ansatte fra renhold og statsbygg vi har intervjuet

4.2.3 Læringsutbytte etter intervjuene

Under selve intervjuprosessen erfarte vi fort at spørsmålene vi hadde laget ikke var tilstrekkelige. Dermed valgte vi å tilpasse de videre og la til spørsmål for IT-Tjenesten og management. Et eksempel er når vi spør ansatte om de har lest skolens sikkerhets policy, spør vi da IT-Tjenesten tjenesten i tillegg om hvor stor andel av skolens ansatte de trur har lest policyen angående adgangskort.

4.2.4 Konklusjon av verktøyet

Vi fikk en god respons på de fleste spørsmål. Vi klarte å avdekke holdninger rundt adgangskort hos ansatte og fikk mange relevante svar. Vi så også at noen spørsmål ikke ga oss den relevante dataen som var ønsket.

Tanker vi tar med oss om verktøyet

Vi har selv fått mye erfaringer ut ifra dette. En av de viktigeste erfaringene vi tar med oss er å gjennomgå spørsmålene svert nøye innad i gruppen. Generer så mange spørsmål som mulig, og i etterkant se om noen spørsmål er overflødige. Dersom det er forskjellige interessegrupper som skal intervjues, tenk igjennom om disse skal få like spørsmål eller om det er spesifikk informasjon disse gruppene sitter på. Gjerne bruk rollespill og still spørsmålene innad i gruppen, for å se om en slik prosess kan kaste nytt lys på utformingen av spørsmålene som skal brukes i intervjuene.

4.3 Problemårsaks dataanalyse

Etter at datainnsamlingen var ferdig var det nødvendig å gå over daten vi hadde samlet inn, her anvendte vi en rekke årsaksanalyseverktøy samt programvaren SPSS til å analysere resultatene fra datainnsamlingsfasen.

Det finnes flere verktøy som kan behandle data som er kategoriserte og uniforme. Dette er verktøy som lar deg liste dataene, som et regneark, og verktøy som lar deg tegne ønskede grafer og illustrasjoner. Verktøyene vi valgte å bruke, samt rekkefølge og hvorfor blir beskrevet i dette kapittelet.

Intervjuene ble behandlet og klargjort for statistisk analyse i et regneark, hvorav selve analysen ble utført i SPSS.

4.4 Demografi

Introduksjon

I intervju delen under gjennomførelse ble det vist til hvilke grupper som ble interjuvet og hvilke yrkestitler som inngikk. Ut ifra disse gruppene er antall deltagere fremstilt grafisk og deres svar summert og fremstilt i de neste delkapitlene. Avdelingene A-IMT og HOS har flest respondenter i vår undersøkelse. Avdelingene som deltok var IT-tjenesten, A-IMT, HOS og TØL i tillegg ansatte i renhold og Statsbygg. Det ble ikke sett noen signifikant forskjell mellom alder og svar på intervju spørsmålene.

Fig.4 viser fordelingen av stillinger på de vi har spurt.

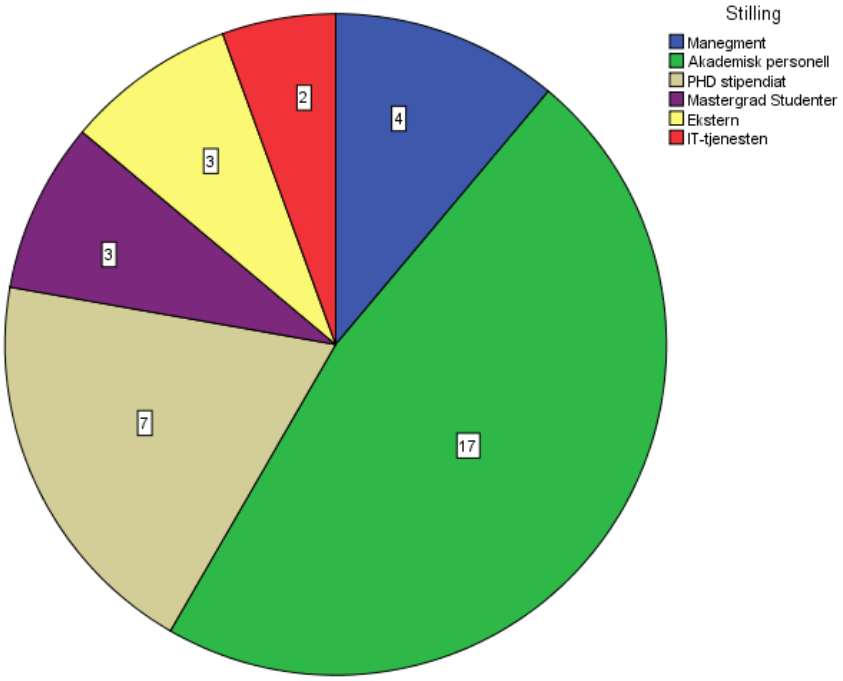


Figure 4: Pie graph av stillingene til de vi har spurt

Som man kan se i fig.5 fikk vi ikke en optimal kjønnsfordeling, men dette basert på sammensetningen av ansatte så anser vi dette som bra nok.
Alderen ble rangert i aldersgrupper som har et intervall på 5 år. Altså fra 20-24, 25-29, 30-34 etc. Det vi ønsket å finne ut ved å kategorisere data på alder, kjønn og interessegrupper var å se om det var noen likhetstrekk innenfor de kategoriserte dataene som kunne være relevant i analysen.

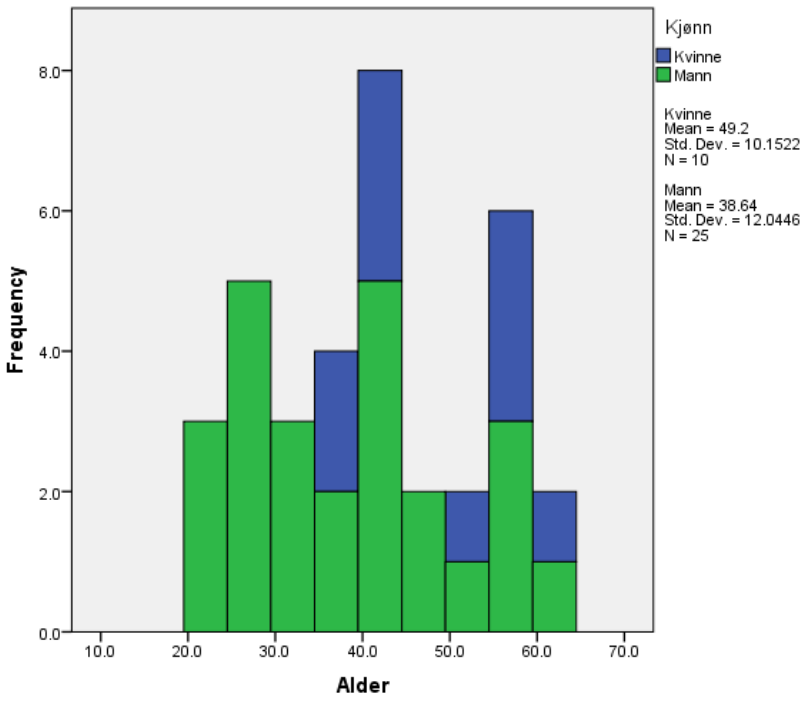


Figure 5: Histogram som illustrerer kjønn og alder over de vi intervjuet

4.5 Kvantitativ analyse

I kvantitativ analyse vil vi se på de numeriske verdiene vi har samlet inn. Dataen grupperes i grupper for presentasjon og diskusjon.

Som vist i tab.1 har vi valgt ut de spørsmålene som ga oss mest mening for selve analysen og fokuserte på disse. Spørsmålene som i hovedsakt blir analysert er vist i tabellen under. N verdien beskriver antall gyldige svar vi mottok per spørsmål. Minimum og maksimum verdiene er det minste og største tallene som er besvart og mean er gjennomsnitts verdien. Std. Deviation står for Standard Diviation og beskriver hvor stor spredning det er mellom svarene som er gitt.

Spørsmål listet i apendix[9]

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Nr. 3	36	1,00	3,00	2,0833	,96732
Nr. 4	36	1,00	3,00	2,7778	,59094
Nr. 5	34	3	6	4,50	1,108
Nr. 7	35	1,00	3,00	1,4571	,78000
Nr. 8	34	1,0	6,0	4,000	1,7581
Nr. 9	36	1,00	4,00	1,4167	,76997
Nr. 10	35	1,0	6,0	3,457	1,5213
Nr. 12	35	2,00	5,00	3,9143	,91944
Nr. 20	32	1,00	2,00	1,4688	,50701
Nr. 21	31	1,00	4,00	2,0645	1,15284
Nr. 25	33	1	6	4,67	1,652
Valid N (listwise)	10				

Table 1: Liste av spørsmål behandlet i spss

4.5.1 Sikkerhetspolicy

I sikkerhetspolicyen til NTNU, under seksjon 4 i Informasjonssikkerhet knyttet til ansatte, innleid personell, studenter og tredjeparter i prinsipper for informasjonssikkerhet ved NTNU punkt 4.3 står det [4]:

Alle brukere av NTNUs informasjonssystemer skal få tilstrekkelig opplæring og oppdatering i NTNUs prinsipper for informasjonssikkerhet og tilhørende rutiner herunder sikkerhetsansvar og roller.

Vi spurte kun ett av intervjuobjektene om dette og vedkommende kunne bekrefte at dette ikke var gjort.

Om vi ser på histogrammet i fig.6 så kan vi se at svært få av de vi har intervjuet har lest den gamle policyen som var gjeldene for HiG.

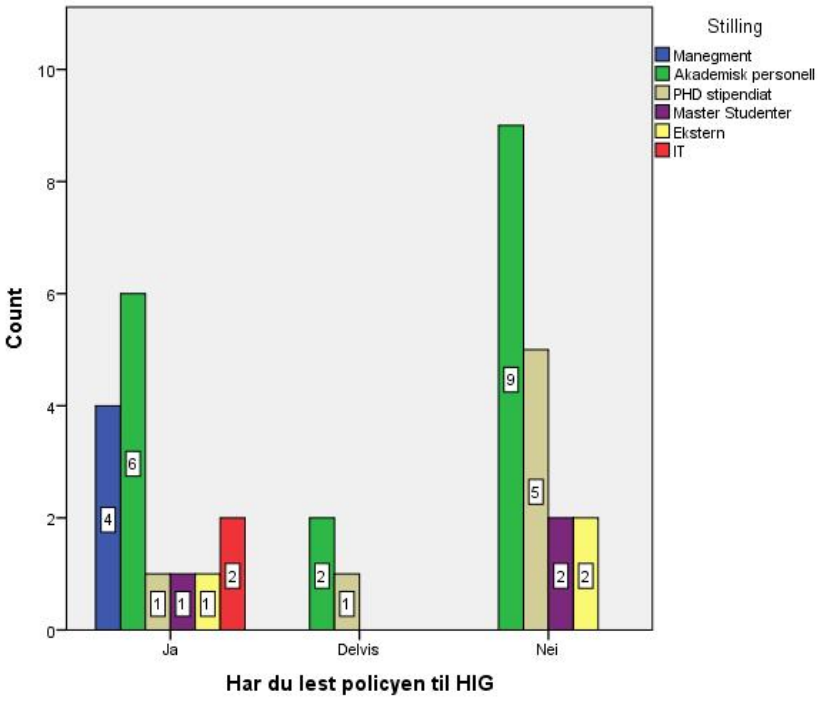


Figure 6: Hvem har lest gammel policy (HIG)

Videre i histogrammet til fig.7 har enda færre lest den nye gjeldene policyen til NTNU.

Som vi kan se så har 15 av de intervjuobjektene vi har spurt lest den gamle policyen og 3 har lest den nye. Når kun et så lite antall ansatte/studenter har lest den nye sikkerhets policyen, kan dette tyde på at det enten har vært for lite informasjon gitt rundt den nye policyen eller et at den ikke har vært synlig nok for ansatte/studenter.

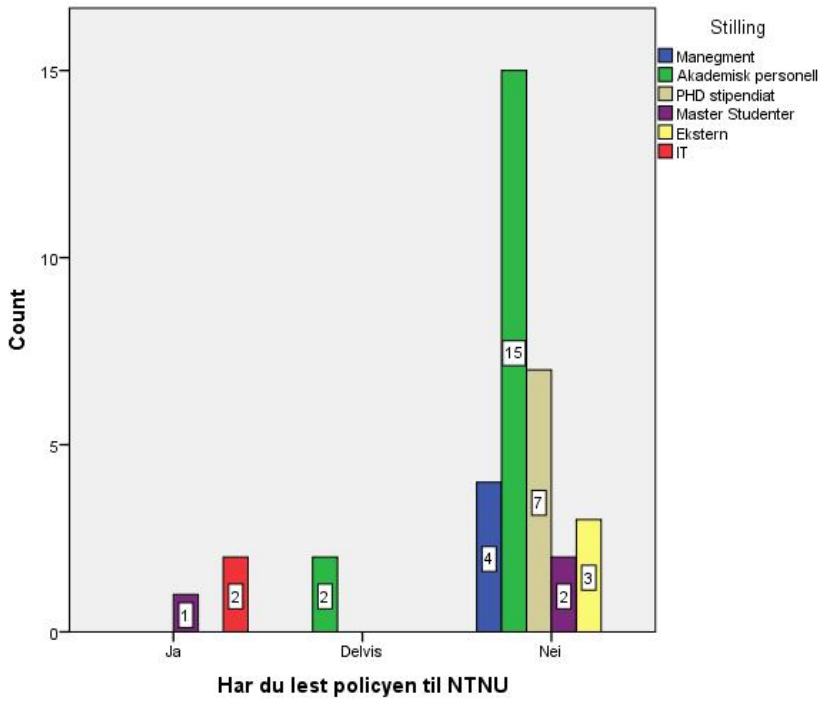


Figure 7: Hvem har lest ny policy (NTNU)

De forskjellige gruppene som ble intervjuet ble også spurt om i hvilken grad ansatte skal få være med på utforming av policy (ref. til table 2). Intervjuobjektene fikk alternativene 1 til 6, hvor 1 tilsier at ansatte på ingen måte skal få delta og 6 tilsier at ansatte skal igjennom hele prosessen få delta i formingen av policy. Her er det forskjeller i hvilken grad de forskjellige gruppene mener ansatte skal delta i utformenging av policyen. Alle mente at de ansatte skulle kunne få si hva de mente og management er de som mente det burde være størst involvering gjennom prosessen. PhD-stipendiatene og akademiske personellet ville ikke være like mye involvert i prosessen, men ville ha muligheten til å få fremme sine meninger. Her var det IT-tjenesten som ga den laveste scoren på at ansatte skulle få lov å være involvert gjennom hele prosessen.

Involvert i Policy

Stillingnr	Mean	N	Std. Deviation
Manegment	5,00	3	1,732
Akademisk personell	4,56	16	1,031
PhD stipendiat	4,29	7	1,380
Master Studenter	4,67	3	,577
Ekstern	4,67	3	1,155
IT-tjenesten	3,50	2	,707
Total	4,50	34	1,108

Table 2: Deltagelse på utforming av policy

4.5.2 Sanksjoner og brudd på policy

Som vi kan se ut ifra histogrammet i fig.8 er det så å si ingen som har kontroll på hva som er konsekvensen av brudd på policy. De som hadde mest oversikt var IT-Tjenesten, men noe usikkert pga. nye ordninger ved fusjonen med NTNU.

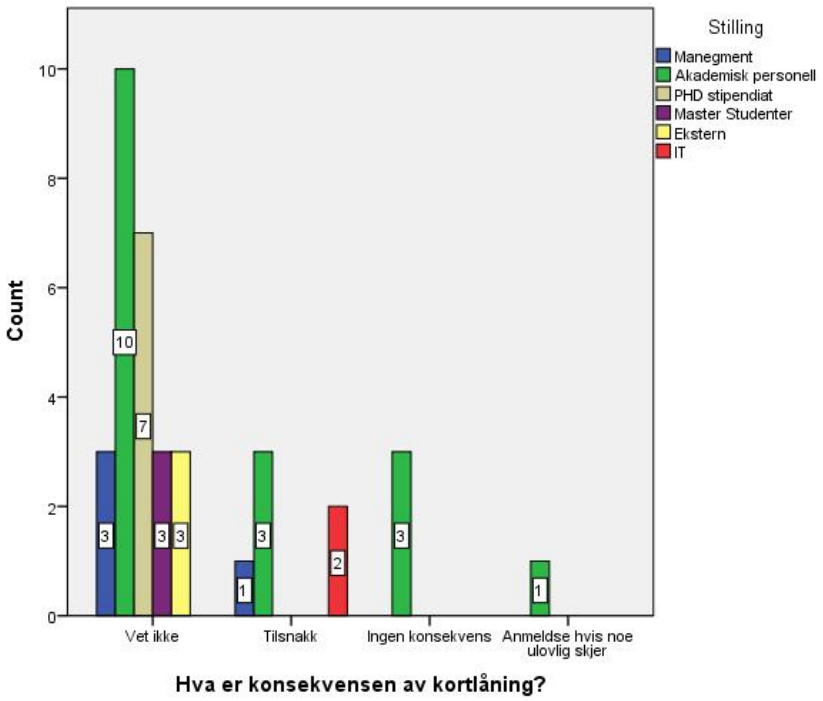


Figure 8: Vet ansatte hva konsekvensen er ved policy brdd

4.5.3 Sikkerhetskultur

Da var delte meninger rundt hvordan sikkerhetskulturen rund kortdeling var. De fleste mente det var en god kultur etter fulgt av de som ikke visste, lavest var de som mente den ikke var god som vist i fig.9.

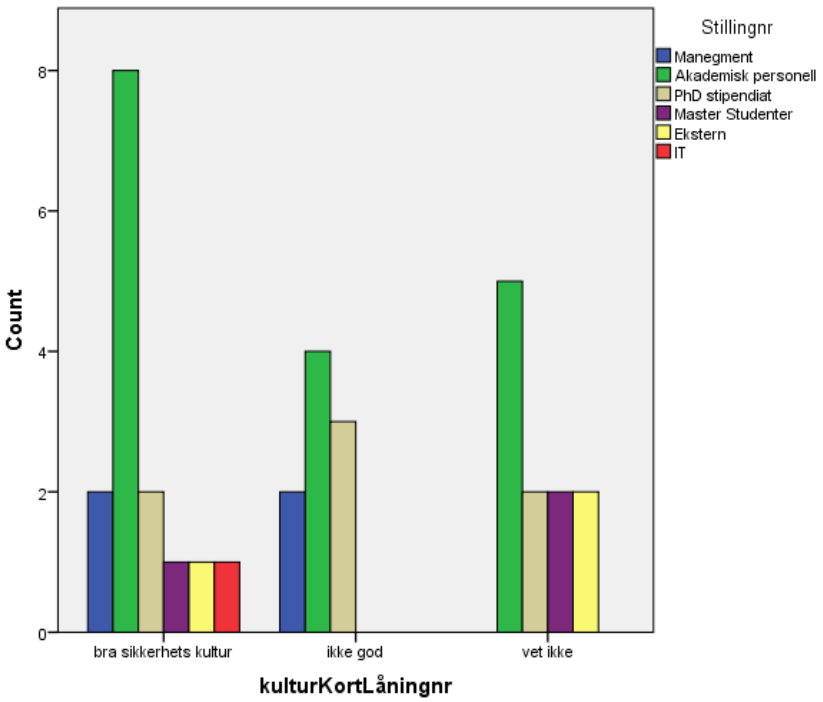


Figure 9: Tanker rundt sikkerhets kulturen på campus

4.5.4 Reserveløsninger for kortutdeling og mottiltak

Kjenner til reserveløsninger

Under i fig.10 presenteres et diagram over kjennskap til reserveløsninger. Her var det 31 av 36 som ga et gyldig svar. Her ser vi at 14 av 31 ikke vet om det faktisk eksisterer en reserveløsninger de kan benytte seg av om de f.ex skulle glemme kortet sitt hjemme.

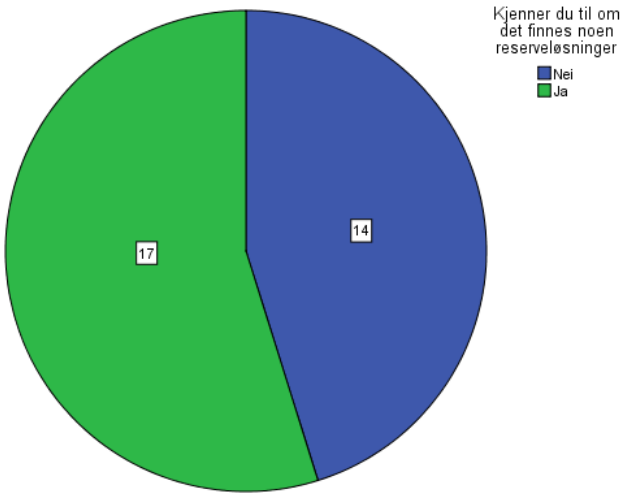


Figure 10: Ansatte/studenter som kjenner til reserveløsninger

Forslag til reserveløsninger

Forslagene fra intervjuene ble gjort uniforme og samlet inn i 26 grupper. Videre brukte vi affinity diagram verktøyet for å videre kategorisere forslagene inn i 6 hovedgrupper som vist i fig.11. Ønsket formål er å danne en oversikt over hvilke kategorier folk viste interesse for. I tillegg gir dette også fordeler ved at det blir lettere å presentere dataene i et histogram format da søylene presenterer 6 kategorier istedenfor 26 grupper med forslag.

Dersom en person har sagt mer enn ett alternativ, har hvert alternativ personen nevnte fått 1 "stemme".

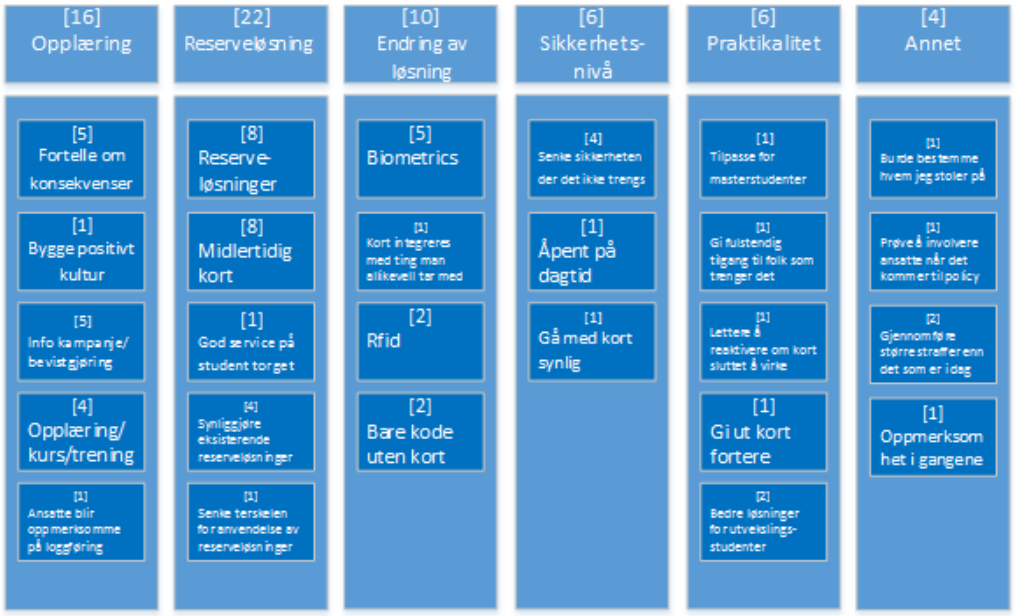


Figure 11: Affinity diagram over forslag til reserveløsninger

Histogrammet i fig.12 viser fordeling av antall personer opp mot antall forslag vi mottok.

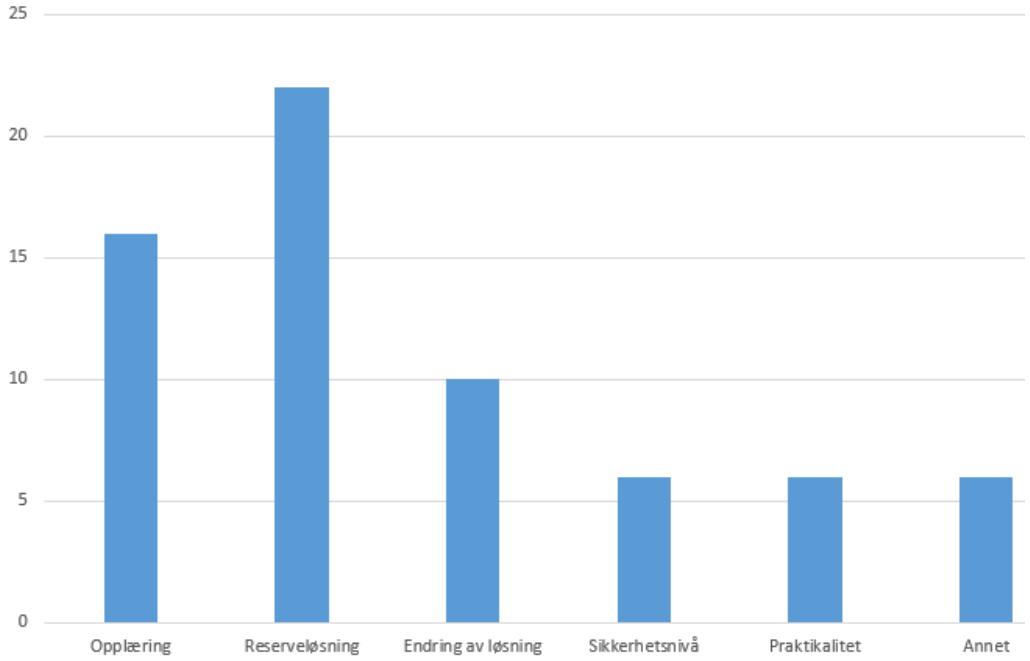


Figure 12: Histogramm

4.5.5 Kortutdeling

Da vi spurte IT-tjenesten om de trudde ansatte/studenter visste at det ikke var lov å låne bort adgangskort svarte 1 av personen vi spurte nei og den andre svarte at innerst inne vet alle at det ikke er lov. Dataen vi samlet inn viser i fig.13 at alle bortsett fra 2 vet at det ikke er lov å låne bort adgangskort. De 2 som ikke visste om det var lov var begge PhD-stipendiater.

Figure 13: Her ble det spurt om "Vet du om det er lov eller ikke å låne bort adgangskort?"

Totalt var det 17 av 32 personer vi spurte som svarte at de har følt behov for å låne noen sitt adgangskort som vist i fig.14. Om man setter dette opp mot at ikke alle vet om det eksisterer reserveløsningen kan dette være med på å bidra til at ansatte velger å gå for løsninger som er enkle for dem men som kan være i strid med policyen.

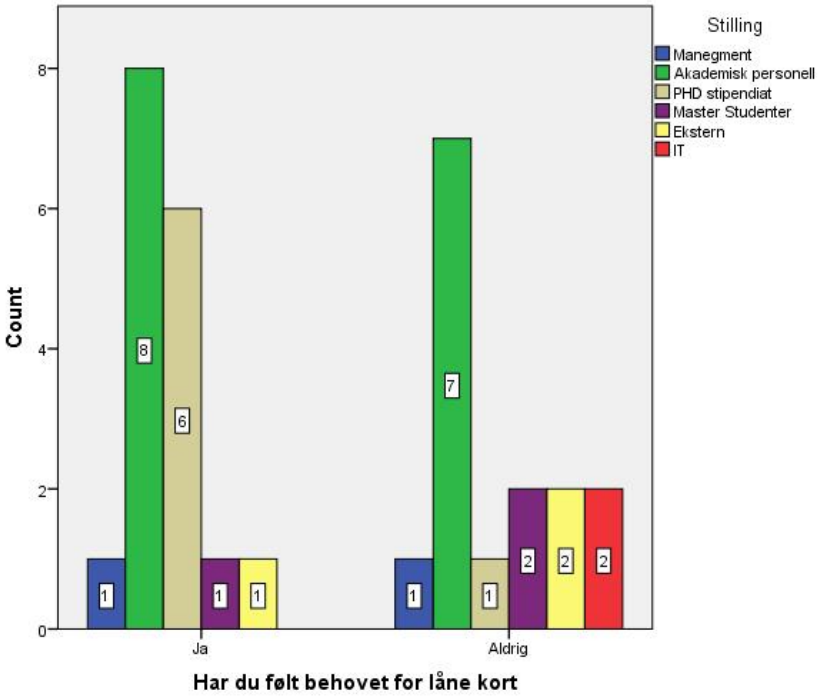


Figure 14: Har følt behovet for å låne adgangskort

Vi spurte intervjuobjektene om de noen gang hadde blitt spurt om å låne bort adgangskortene sine. Her var det 17 av 35 stykker som har blitt spurt som svarte ja som vist i fig.15. Dette kan tyde på at personer som føler behovet og ikke har kjennskap til reserveløsninger velger å spør andre om å få låne deres kort.

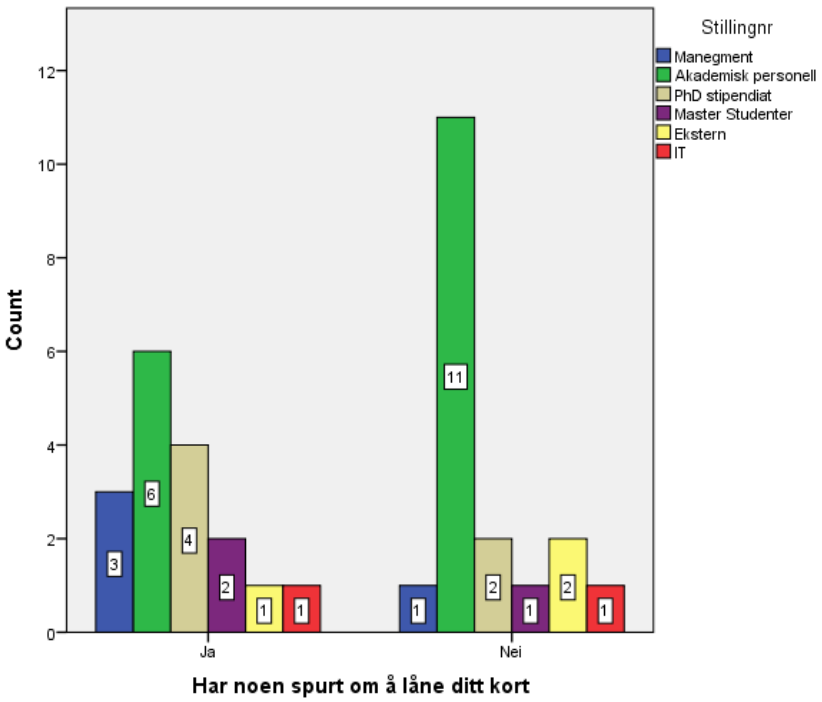


Figure 15: Antall personer som har blitt spurt om låne bort deres adgangskort.

Da vi stilte intervjuobjektene om de kjente til om kort var blitt lånt bort svarte 19 av 36 ja, som vist i fig.16. De to gruppene som skiller seg ut her akademisk personell og IT-tjenesten der større andel av de gruppene kjente til tilfeller. Dette kan være pga. at de har vært her lengre enn de andre grupenne.

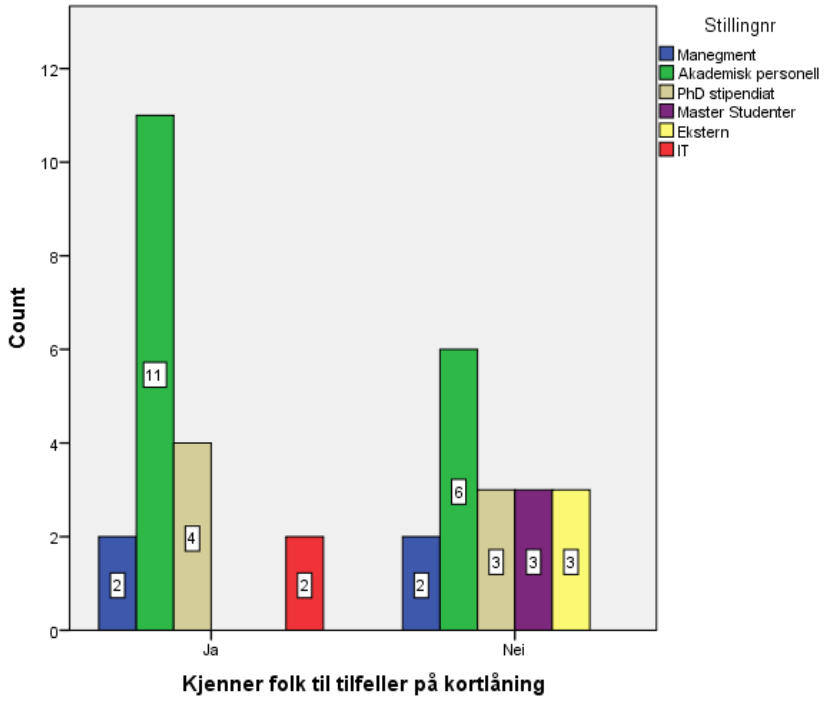


Figure 16: Kjenner tilfeller hvor adgangskort har blitt lånt bort

4.5.6 Anova

Anova testen skjekker om det er signifikans i gruppen og derretter kan det gjøres en posthoc test for å se om det er noe relevans mellom enkelte grupper. Vi tok å gjorde anova test på gruppen stilling, alder og kjønn.

Under er descriptive av anovan i som kan sees i tab.3. Anova testen i tab. 4. Post hoc testen vises i tab. 5 og 6

Her skiller den yngste grupen seg ut med at de vil være minst involvert i policyen. Her var sig på anova 0.230 og post hocen hadde en gi 0.282 melleom gruppen 20-29 og 20-29.

På de andre spørsmålene som er tatt med i anovaen så hadde aldersgruppen meninger som var lik nok til at det ikke var noe som skilte seg ut her. Hverken anova eller post hoc testen ga oss noe relevant for disse spørsmålene.

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% C.I. for Mean		Min	Max
						LB	UB		
Fra en skala fra 1 til 6,	20-29	8	3,88	,991	,350	3,05	4,70	3	5
hvor 1 er "ikke i det heletatt"	30-39	7	5,00	1,291	,488	3,81	6,19	3	6
og 6 er "igjennom hele prosessen"	40-49	10	4,50	,972	,307	3,80	5,20	3	6
føler du at ansatte som følger	50-59	7	4,43	1,134	,429	3,38	5,48	3	6
policyene skal få være med	60-69	2	5,50	,707	,500	-,85	11,85	5	6
på å forme policyene?	Total	34	4,50	1,108	,190	4,11	4,89	3	6
På en skala fra 1 til 6	20-29	7	3,857	1,4639	,5533	2,503	5,211	1,0	5,0
der 1 er mindre alvorlig	30-39	7	3,714	1,7043	,6442	2,138	5,291	1,0	6,0
og 6 er veldig alvorlig,	40-49	9	3,444	1,7401	,5800	2,107	4,782	1,0	6,0
hvor alvorlig tror du skolen	50-59	9	4,556	2,1279	,7093	2,920	6,191	1,0	6,0
ser på byttelåne av adgangskort?	60-69	2	5,500	,7071	,5000	-,853	11,853	5,0	6,0
	Total	34	4,000	1,7581	,3015	3,387	4,613	1,0	6,0
På en skala fra 1 til 6,	20-29	8	3,000	1,4142	,5000	1,818	4,182	1,0	5,0
hvor 1 er lite sannsynlig	30-39	7	3,857	1,0690	,4041	2,868	4,846	2,0	5,0
og 6 er svært sannsynlig	40-49	10	3,400	1,7127	,5416	2,175	4,625	1,0	6,0
hvor sannsynlig tror du det	50-59	8	3,500	2,0000	,7071	1,828	5,172	1,0	6,0
er at ansatte innrømmer	60-69	2	4,000	0,0000	0,0000	4,000	4,000	4,0	4,0
byttelåne av adgangskort kort?	Total	35	3,457	1,5213	,2571	2,935	3,980	1,0	6,0
Har du noen gang følt behovet	20-29	8	3,6250	,74402	,26305	3,0030	4,2470	2,00	4,00
for å skulle spør noen om å	30-39	7	4,2857	,95119	,35952	3,4060	5,1654	3,00	5,00
låne deres adgangskort?	40-49	10	4,0000	1,05409	,33333	3,2459	4,7541	3,00	5,00
Aldri, Årlig, Månedlig,	50-59	9	3,7778	,97183	,32394	3,0308	4,5248	2,00	5,00
Ukentlig, Daglig	60-69	1	4,0000					4,00	4,00
	Total	35	3,9143	,91944	,15541	3,5984	4,2301	2,00	5,00
Fra en skala fra 1 til 6.	20-29	7	4,14	1,676	,634	2,59	5,69	1	6
Der 1 er veldig lang tid	30-39	6	4,33	2,251	,919	1,97	6,70	1	6
og 6 er hadde tilgang da jeg startet:	40-49	9	4,67	1,732	,577	3,34	6,00	1	6
Fikk du tilgang til alle	50-59	9	5,33	1,118	,373	4,47	6,19	3	6
rommene du trengte med en gang?	60-69	2	4,50	2,121	1,500	-14,56	23,56	3	6
	Total	33	4,67	1,652	,288	4,08	5,25	1	6

Table 3: Descriptive på Alder

ANOVA

		Sum of Sq.	df	Mean Sq.	F	Sig.
Fra en skala fra 1 til 6, hvor 1 er "ikke i det heletatt" og 6 er "igjennom hele prosessen" føler du at ansatte som følger policyene skal få være med på å forme policyene?	Between Groups	6,911	4	1,728	1,492	,230
	Within Groups	33,589	29	1,158		
	Total	40,500	33			
På en skala fra 1 til 6 der 1 er mindre alvorlig og 6 er veldig alvorlig, hvor alvorlig tror du skolen ser på byttelåne av adgangskort?	Between Groups	10,770	4	2,692	,856	,502
	Within Groups	91,230	29	3,146		
	Total	102,000	33			
På en skala fra 1 til 6, hvor 1 er lite sannsynlig og 6 er svært sannsynlig hvor sannsynlig tror du det er at ansatte innrømmer byttelåne av adgangskort kort?	Between Groups	3,429	4	,857	,342	,848
	Within Groups	75,257	30	2,509		
	Total	78,686	34			
Har du noen gang følt behovet for å skulle spør noen om å låne deres adgangskort? Aldri, Årlig, Månedlig, Ukentlig, Daglig	Between Groups	1,884	4	,471	,526	,717
	Within Groups	26,859	30	,895		
	Total	28,743	34			
Fra en skala fra 1 til 6. Der 1 er veldig lang tid og 6 er hadde tilgang da jeg startet: Fikk du tilgang til alle rommene du trengte med en gang?	Between Groups	6,643	4	1,661	,576	,682
	Within Groups	80,690	28	2,882		
	Total	87,333	32			

Table 4: Anova på alder

Multiple Comparisons

Tukey HSD

Dependent Variable			Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Nr. 5	20-29	30-39	-1,125	,557	,282	-2,74	,49
		40-49	-,625	,510	,738	-2,11	,86
		50-59	-,554	,557	,856	-2,17	1,07
		60-69	-1,625	,851	,335	-4,10	,85
	30-39	20-29	1,125	,557	,282	-,49	2,74
		40-49	,500	,530	,878	-1,04	2,04
		50-59	,571	,575	,856	-1,10	2,24
		60-69	-,500	,863	,977	-3,01	2,01
	40-49	20-29	,625	,510	,738	-,86	2,11
		30-39	-,500	,530	,878	-2,04	1,04
		50-59	,071	,530	1,000	-1,47	1,61
		60-69	-1,000	,834	,752	-3,42	1,42
	50-59	20-29	,554	,557	,856	-1,07	2,17
		30-39	-,571	,575	,856	-2,24	1,10
		40-49	-,071	,530	1,000	-1,61	1,47
		60-69	-1,071	,863	,728	-3,58	1,44
	60-69	20-29	1,625	,851	,335	-,85	4,10
		30-39	,500	,863	,977	-2,01	3,01
		40-49	1,000	,834	,752	-1,42	3,42
		50-59	1,071	,863	,728	-1,44	3,58
Nr. 8	20-29	30-39	,1429	,9481	1,000	-2,613	2,899
		40-49	,4127	,8938	,990	-2,186	3,011
		50-59	-,6984	,8938	,934	-3,297	1,900
		60-69	-1,6429	1,4221	,776	-5,777	2,491
	30-39	20-29	-,1429	,9481	1,000	-2,899	2,613
		40-49	,2698	,8938	,998	-2,328	2,868
		50-59	-,8413	,8938	,878	-3,440	1,757
		60-69	-1,7857	1,4221	,719	-5,919	2,348
	40-49	20-29	-,4127	,8938	,990	-3,011	2,186
		30-39	-,2698	,8938	,998	-2,868	2,328
		50-59	-1,1111	,8361	,676	-3,542	1,319
		60-69	-2,0556	1,3865	,582	-6,086	1,975
	50-59	20-29	,6984	,8938	,934	-1,900	3,297
		30-39	,8413	,8938	,878	-1,757	3,440
		40-49	1,1111	,8361	,676	-1,319	3,542
		60-69	-,9444	1,3865	,959	-4,975	3,086
	60-69	20-29	1,6429	1,4221	,776	-2,491	5,777
		30-39	1,7857	1,4221	,719	-2,348	5,919
		40-49	2,0556	1,3865	,582	-1,975	6,086
		50-59	,9444	1,3865	,959	-3,086	4,975

Table 5: Post hoc tuckey på alder pt.1

Multiple Comparisons

Tukey HSD

Dependent Variable			Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
Nr. 20	20-29	30-39	-,8571	,8197	,832	-3,235	1,521
		40-49	-,4000	,7513	,983	-2,579	1,779
		50-59	-,5000	,7919	,969	-2,797	1,797
		60-69	-1,0000	1,2521	,929	-4,632	2,632
	30-39	20-29	,8571	,8197	,832	-1,521	3,235
		40-49	,4571	,7805	,976	-1,807	2,721
		50-59	,3571	,8197	,992	-2,021	2,735
		60-69	-,1429	1,2699	1,000	-3,826	3,541
	40-49	20-29	,4000	,7513	,983	-1,779	2,579
		30-39	-,4571	,7805	,976	-2,721	1,807
		50-59	-,1000	,7513	1,000	-2,279	2,079
		60-69	-,6000	1,2268	,988	-4,159	2,959
	50-59	20-29	,5000	,7919	,969	-1,797	2,797
		30-39	-,3571	,8197	,992	-2,735	2,021
		40-49	,1000	,7513	1,000	-2,079	2,279
		60-69	-,5000	1,2521	,994	-4,132	3,132
	60-69	20-29	1,0000	1,2521	,929	-2,632	4,632
		30-39	,1429	1,2699	1,000	-3,541	3,826
		40-49	,6000	1,2268	,988	-2,959	4,159
		50-59	,5000	1,2521	,994	-3,132	4,132
Nr. 24	20-29	30-39	-,190	,944	1,000	-2,94	2,56
		40-49	-,524	,856	,972	-3,02	1,97
		50-59	-1,190	,856	,638	-3,68	1,30
		60-69	-,357	1,361	,999	-4,32	3,61
	30-39	20-29	,190	,944	1,000	-2,56	2,94
		40-49	-,333	,895	,996	-2,94	2,27
		50-59	-1,000	,895	,796	-3,61	1,61
		60-69	-,167	1,386	1,000	-4,20	3,87
	40-49	20-29	,524	,856	,972	-1,97	3,02
		30-39	,333	,895	,996	-2,27	2,94
		50-59	-,667	,800	,918	-3,00	1,66
		60-69	,167	1,327	1,000	-3,70	4,03
	50-59	20-29	1,190	,856	,638	-1,30	3,68
		30-39	1,000	,895	,796	-1,61	3,61
		40-49	,667	,800	,918	-1,66	3,00
		60-69	,833	1,327	,969	-3,03	4,70
	60-69	20-29	,357	1,361	,999	-3,61	4,32
		30-39	,167	1,386	1,000	-3,87	4,20
		40-49	-,167	1,327	1,000	-4,03	3,70
		50-59	-,833	1,327	,969	-4,70	3,03

Table 6: Post hoc tuckey på alder pt.2

Under er descriptive av anovan i som kan sees i tab.7. Anova testen i tab. 8. Post hoc testen vises i tab. 9 og 10

Når det kommer til innvolvering i policyen så er det IT-tjenesten som størst forskjell fra hva de andre mener. På mean diffrance så har de største verdiene. Her er det IT-tjenestensom er med NTNU i Trondheim med på å skrive policyen. Det hadde kunne hjulpet at de hadde ett syn som reflekterte det resten av

organisasjonen mente til å skape ett mer velyket policy. Hverken anova eller post hoc testen ga oss noe relevant.

Hva ansaatte trodde angående hvor alvorlig skolen anså låning var det antydninger til relevanse. Sig verdien her var på 0.339 og post hoc testen mellom externe og PhD stipendiater var på 0.242. Her var de på motsatte siden av skallaen, med PhD-stipendiaten på den lave enden og eksterne på den høye. Her er det forskjeller på hvor alvorlig folk tror situasjonen er.

De som hadde minst tro på at ansatte ville innrøme å at de hadde lånt kort var de eksterne. Resten var nærme med sine meninger. Hverken anova eller post hoc testen ga oss noe relevant.

Det var jevnt hvor ofte de forskjellige gruppene hadde følt behovet på å låne kort. Hverken anova eller post hoc testen ga oss noe relevant.

Anova testen viste at det var en sig på 0.028 på hvor lang tid det tok for ansatte å få tilgang. Her var det de med høyere stilling som mente det tok mindre tid. Dette kan tyde på at det er de som har mer å si som blir tatt vare på først. IT-tjenesten er ikke nevnt her siden det er dem som har kontroll over systemet.

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% C.I. for Mean		Min	Max
						LB	UB		
Fra en skala fra 1 til 6,	Manegment	3	5,00	1,732	1,000	,70	9,30	3	6
hvor 1 er "ikke i det heletatt"	Akademisk personell	16	4,56	1,031	,258	4,01	5,11	3	6
og 6 er "igjennom hele prosessen"	PhD stipendiat	7	4,29	1,380	,522	3,01	5,56	3	6
føler du at ansatte som følger	Mastergrads Studenter	3	4,67	,577	,333	3,23	6,10	4	5
policyene skal få være med	Ekstern	3	4,67	1,155	,667	1,80	7,54	4	6
på å forme policyene?	IT-tjenesten	2	3,50	,707	,500	-2,85	9,85	3	4
	Total	34	4,50	1,108	,190	4,11	4,89	3	6
På en skala fra 1 til 6	Manegment	4	4,500	1,9149	,9574	1,453	7,547	2,0	6,0
der 1 er mindre alvorlig	Akademisk personell	17	3,824	1,9117	,4636	2,841	4,806	1,0	6,0
og 6 er veldig alvorlig,	PhD stipendiat	5	2,800	1,6432	,7348	,760	4,840	1,0	4,0
hvor alvorlig tror du skolen	Mastergrads Studenter	3	4,333	1,1547	,6667	1,465	7,202	3,0	5,0
ser på byttelåne av adgangskort?	Ekstern	3	5,667	,5774	,3333	4,232	7,101	5,0	6,0
	IT-tjenesten	2	4,500	,7071	,5000	-1,853	10,853	4,0	5,0
	Total	34	4,000	1,7581	,3015	3,387	4,613	1,0	6,0
På en skala fra 1 til 6,	Manegment	4	4,250	1,7078	,8539	1,532	6,968	2,0	6,0
hvor 1 er lite sannsynlig	Akademisk personell	16	3,688	1,5370	,3843	2,868	4,507	1,0	6,0
og 6 er svært sannsynlig	PhD stipendiat	7	3,000	1,7321	,6547	1,398	4,602	1,0	5,0
hvor sannsynlig tror du det	Mastergrads Studenter	3	3,333	1,5275	,8819	-,461	7,128	2,0	5,0
er at ansatte innrømmer	Ekstern	3	2,333	1,1547	,6667	-,535	5,202	1,0	3,0
byttelåne av adgangskort kort?	IT-tjenesten	2	3,500	,7071	,5000	-2,853	9,853	3,0	4,0
	Total	35	3,457	1,5213	,2571	2,935	3,980	1,0	6,0
Har du noen gang følt behovet	Manegment	4	4,0000	,81650	,40825	2,7008	5,2992	3,00	5,00
for å skulle spør noen om å	Akademisk personell	16	4,0625	,99791	,24948	3,5307	4,5943	2,00	5,00
låne deres adgangskort?	PhD stipendiat	7	3,7143	,75593	,28571	3,0152	4,4134	3,00	5,00
Aldri, Årlig, Månedlig,	Mastergrads Studenter	3	3,3333	1,15470	,66667	,4649	6,2018	2,00	4,00
Ukentlig, Daglig	Ekstern	3	3,6667	1,15470	,66667	,7982	6,5351	3,00	5,00
	IT-tjenesten	2	4,5000	,70711	,50000	-1,8531	10,8531	4,00	5,00
	Total	35	3,9143	,91944	,15541	3,5984	4,2301	2,00	5,00
Fra en skala fra 1 til 6.	Manegment	3	6,00	0,000	0,000	6,00	6,00	6	6
Der 1 er veldig lang tid	Akademisk personell	17	5,18	1,286	,312	4,52	5,84	2	6
og 6 er hadde tilgang da jeg startet:	PhD stipendiat	7	4,29	1,799	,680	2,62	5,95	1	6
Fikk du tilgang til alle	Mastergrads Studenter	3	3,00	2,000	1,155	-1,97	7,97	1	5
rommene du trengte med en gang?	Ekstern	3	3,00	1,732	1,000	-1,30	7,30	1	4
	IT-tjenesten	0							
	Total	33	4,67	1,652	,288	4,08	5,25	1	6

Table 7: Descreptive på stilling

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
InvolvertPolicy	Between Groups	3,301	5	,660	,497	,776
	Within Groups	37,199	28	1,329		
	Total	40,500	33			
AlvorligLåne	Between Groups	17,896	5	3,579	1,192	,339
	Within Groups	84,104	28	3,004		
	Total	102,000	33			
AnsatteInrømmer	Between Groups	8,665	5	1,733	,718	,615
	Within Groups	70,021	29	2,415		
	Total	78,686	34			
HvorOfteLåneNr	Between Groups	2,543	5	,509	,563	,727
	Within Groups	26,199	29	,903		
	Total	28,743	34			
TilgangTid	Between Groups	27,434	4	6,859	3,206	,028
	Within Groups	59,899	28	2,139		
	Total	87,333	32			

Table 8: Anova på stilling

Multiple Comparisons

Tukey HSD

Dependent Variable			Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Nr. 5	Manegment	Akademisk personell	,438	,725	,990	-1,78	2,65
		PhD stipendiat	,714	,795	,944	-1,72	3,14
		Mastergrads Studenter	,333	,941	,999	-2,54	3,21
		Ekstern	,333	,941	,999	-2,54	3,21
		IT-tjenesten	1,500	1,052	,712	-1,72	4,72
	Akademisk personell	Manegment	-,438	,725	,990	-2,65	1,78
		PhD stipendiat	,277	,522	,994	-1,32	1,87
		Mastergrads Studenter	-,104	,725	1,000	-2,32	2,11
		Ekstern	-,104	,725	1,000	-2,32	2,11
		IT-tjenesten	1,063	,864	,819	-1,58	3,70
	PhD stipendiat	Manegment	-,714	,795	,944	-3,14	1,72
		Akademisk personell	-,277	,522	,994	-1,87	1,32
		Mastergrads Studenter	-,381	,795	,997	-2,81	2,05
		Ekstern	-,381	,795	,997	-2,81	2,05
		IT-tjenesten	,786	,924	,955	-2,04	3,61
	Mastergrads Studenter	Manegment	-,333	,941	,999	-3,21	2,54
		Akademisk personell	,104	,725	1,000	-2,11	2,32
		PhD stipendiat	,381	,795	,997	-2,05	2,81
		Ekstern	0,000	,941	1,000	-2,88	2,88
		IT-tjenesten	1,167	1,052	,874	-2,05	4,38
	Ekstern	Manegment	-,333	,941	,999	-3,21	2,54
		Akademisk personell	,104	,725	1,000	-2,11	2,32
		PhD stipendiat	,381	,795	,997	-2,05	2,81
		Mastergrads Studenter	0,000	,941	1,000	-2,88	2,88
		IT-tjenesten	1,167	1,052	,874	-2,05	4,38
	IT-tjenesten	Manegment	-1,500	1,052	,712	-4,72	1,72
		Akademisk personell	-1,063	,864	,819	-3,70	1,58
		PhD stipendiat	-,786	,924	,955	-3,61	2,04
		Mastergrads Studenter	-1,167	1,052	,874	-4,38	2,05
		Ekstern	-1,167	1,052	,874	-4,38	2,05
Nr. 8	Manegment	Akademisk personell	,6765	,9631	,980	-2,267	3,620
		PhD stipendiat	1,7000	1,1626	,690	-1,853	5,253
		Mastergrads Studenter	,1667	1,3237	1,000	-3,878	4,212
		Ekstern	-1,1667	1,3237	,948	-5,212	2,878
		IT-tjenesten	0,0000	1,5009	1,000	-4,587	4,587
	Akademisk personell	Manegment	-,6765	,9631	,980	-3,620	2,267
		PhD stipendiat	1,0235	,8817	,851	-1,671	3,718
		Mastergrads Studenter	-,5098	1,0853	,997	-3,826	2,807
		Ekstern	-1,8431	1,0853	,544	-5,160	1,473
		IT-tjenesten	-,6765	1,2956	,995	-4,636	3,283
	PhD stipendiat	Manegment	-1,7000	1,1626	,690	-5,253	1,853
		Akademisk personell	-1,0235	,8817	,851	-3,718	1,671
		Mastergrads Studenter	-1,5333	1,2657	,828	-5,401	2,334
		Ekstern	-2,8667	1,2657	,242	-6,734	1,001
		IT-tjenesten	-1,7000	1,4500	,846	-6,131	2,731
	Mastergrads Studenter	Manegment	-,1667	1,3237	1,000	-4,212	3,878
		Akademisk personell	,5098	1,0853	,997	-2,807	3,826
		PhD stipendiat	1,5333	1,2657	,828	-2,334	5,401
		Ekstern	-1,3333	1,4151	,932	-5,658	2,991
		IT-tjenesten	-,1667	1,5821	1,000	-5,001	4,668
	Ekstern	Manegment	1,1667	1,3237	,948	-2,878	5,212
		Akademisk personell	1,8431	1,0853	,544	-1,473	5,160
		PhD stipendiat	2,8667	1,2657	,242	-1,001	6,734
		Mastergrads Studenter	1,3333	1,4151	,932	-2,991	5,658
		IT-tjenesten	1,1667	1,5821	,975	-3,668	6,001
	IT-tjenesten	Manegment	0,0000	1,5009	1,000	-4,587	4,587
		Akademisk personell	,6765	1,2956	,995	-3,283	4,636
		PhD stipendiat	1,7000	1,4500	,846	-2,731	6,131
		Mastergrads Studenter	,1667	1,5821	1,000	-4,668	5,001
		Ekstern	-1,1667	1,5821	,975	-6,001	3,668

Table 9: Post hoc tuckey på stilling del 1

Multiple Comparisons

Tukey HSD

Dependent Variable			Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
		Akademisk personell	,5625	,8686	,986	-2,086	3,211
		PhD stipendiat	1,2500	,9739	,791	-1,719	4,219
	Manegment	Mastergrads Studenter	,9167	1,1868	,970	-2,701	4,535
		Ekstern	1,9167	1,1868	,596	-1,701	5,535
		IT-tjenesten	,7500	1,3457	,993	-3,352	4,852
		Manegment	-,5625	,8686	,986	-3,211	2,086
		PhD stipendiat	,6875	,7042	,922	-1,459	2,834
	Akademisk personell	Mastergrads Studenter	,3542	,9776	,999	-2,626	3,334
		Ekstern	1,3542	,9776	,735	-1,626	4,334
		IT-tjenesten	,1875	1,1654	1,000	-3,365	3,740
		Manegment	-1,2500	,9739	,791	-4,219	1,719
		Akademisk personell	-,6875	,7042	,922	-2,834	1,459
	PhD stipendiat	Mastergrads Studenter	-,3333	1,0723	1,000	-3,602	2,935
		Ekstern	,6667	1,0723	,988	-2,602	3,935
Nr. 10		IT-tjenesten	-,5000	1,2459	,999	-4,298	3,298
		Manegment	-,9167	1,1868	,970	-4,535	2,701
		Akademisk personell	-,3542	,9776	,999	-3,334	2,626
	Mastergrads Studenter	PhD stipendiat	,3333	1,0723	1,000	-2,935	3,602
		Ekstern	1,0000	1,2687	,967	-2,868	4,868
		IT-tjenesten	-,1667	1,4185	1,000	-4,491	4,158
		Manegment	-1,9167	1,1868	,596	-5,535	1,701
		Akademisk personell	-1,3542	,9776	,735	-4,334	1,626
	Ekstern	PhD stipendiat	-,6667	1,0723	,988	-3,935	2,602
		Mastergrads Studenter	-1,0000	1,2687	,967	-4,868	2,868
		IT-tjenesten	-1,1667	1,4185	,961	-5,491	3,158
		Manegment	-,7500	1,3457	,993	-4,852	3,352
		Akademisk personell	-,1875	1,1654	1,000	-3,740	3,365
	IT-tjenesten	PhD stipendiat	,5000	1,2459	,999	-3,298	4,298
		Mastergrads Studenter	,1667	1,4185	1,000	-4,158	4,491
		Ekstern	1,1667	1,4185	,961	-3,158	5,491
		Akademisk personell	-,06250	,53134	1,000	-1,6823	1,5573
		PhD stipendiat	,28571	,59575	,997	-1,5304	2,1018
	Manegment	Mastergrads Studenter	,66667	,72595	,939	-1,5464	2,8797
		Ekstern	,33333	,72595	,997	-1,8797	2,5464
		IT-tjenesten	-,50000	,82315	,990	-3,0093	2,0093
		Manegment	,06250	,53134	1,000	-1,5573	1,6823
		PhD stipendiat	,34821	,43073	,964	-,9648	1,6613
	Akademisk personell	Mastergrads Studenter	,72917	,59800	,824	-1,0938	2,5522
		Ekstern	,39583	,59800	,985	-1,4272	2,2188
		IT-tjenesten	-,43750	,71287	,989	-2,6107	1,7357
		Manegment	-,28571	,59575	,997	-2,1018	1,5304
		Akademisk personell	-,34821	,43073	,964	-1,6613	,9648
	PhD stipendiat	Mastergrads Studenter	,38095	,65590	,992	-1,6185	2,3804
		Ekstern	,04762	,65590	1,000	-1,9519	2,0471
nr. 20		IT-tjenesten	-,78571	,76209	,904	-3,1089	1,5375
		Manegment	-,66667	,72595	,939	-2,8797	1,5464
		Akademisk personell	-,72917	,59800	,824	-2,5522	1,0938
	Mastergrads Studenter	PhD stipendiat	-,38095	,65590	,992	-2,3804	1,6185
		Ekstern	-,33333	,77607	,998	-2,6992	2,0325
		IT-tjenesten	-1,16667	,86767	,758	-3,8117	1,4784
		Manegment	-,33333	,72595	,997	-2,5464	1,8797
		Akademisk personell	-,39583	,59800	,985	-2,2188	1,4272
	Ekstern	PhD stipendiat	-,04762	,65590	1,000	-2,0471	1,9519
		Mastergrads Studenter	,33333	,77607	,998	-2,0325	2,6992
		IT-tjenesten	-,83333	,86767	,927	-3,4784	1,8117
		Manegment	,50000	,82315	,990	-2,0093	3,0093
		Akademisk personell	,43750	,71287	,989	-1,7357	2,6107
	IT-tjenesten	PhD stipendiat	,78571	,76209	,904	-1,5375	3,1089
		Mastergrads Studenter	1,16667	,86767	,758	-1,4784	3,8117
		Ekstern	,83333	,86767	,927	-1,8117	3,4784

Table 10: Post hoc tuckey på stilling del 2

Analysen viser at det er tydelig forskjell mellom svar fra menn og kvinner på spørsmål 8 og 10 i spørreundersøkelsen [9]. Kvinner ser på situasjoner med låning av kort mellom ansatte som mer alvorlig enn menn. Kvinner mener også at det er større sannsynlighet for at ansatte innrømmer kortlåning enn det menn trur. Vis man ser på tall verdiene [11] så er det en henholdsvis 1.42 forskjell i mean på Nr. 8 og 1.32 på Nr. 10.. Begge har en lav sig value 0,03 og 0,018, som vil si at begge er statisisk relevante [12].

Descriptives

		N	Mean	Std. Dev.	Std. Error	95% C.I. for Mean		Min	Max
						LB	UB		
Nr. 8	Mann	24	3,583	1,7673	,3607	2,837	4,330	1,0	6,0
	Kvinne	10	5,000	1,3333	,4216	4,046	5,954	2,0	6,0
	Total	34	4,000	1,7581	,3015	3,387	4,613	1,0	6,0
Nr. 10	Mann	25	3,080	1,4978	,2996	2,462	3,698	1,0	5,0
	Kvinne	10	4,400	1,1738	,3712	3,560	5,240	3,0	6,0
	Total	35	3,457	1,5213	,2571	2,935	3,980	1,0	6,0

Table 11: Descripve til anova på kjønn

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Nr. 8	Between Groups	14,167	1	14,167	5,161	,030
	Within Groups	87,833	32	2,745		
	Total	102,000	33			
Nr. 10	Between Groups	12,446	1	12,446	6,200	,018
	Within Groups	66,240	33	2,007		
	Total	78,686	34			

Table 12: Anova på kjønn

4.6 Forskjell på gruppene og særtrekk

Etter analysen var gjort så vi det var forskjell samt særtrekk på de forskjellige gruppene. Nedenfor går vi inn på de forskjellige gruppene og tar ut informasjon vi mener er viktig og relevant.

4.6.1 Management

Alle hadde lest den gamle policyen da vi var HiG, men ingen hadde lest den nye etter skolen var blitt fusjonert med NTNU. Halvparten mente at det var viktig å ha med de som skal følge policyen til å utforme policyen igjennom hele prosessen. Da vi spurte denne gruppen om hva de så på som det verste scenariet, hadde denne gruppen ganske like meninger. Dataen vi samlet inn viser at de var bekymret for tap av informasjon, kompromittering og juridiske aspekter. Når vi spurte om ansatte ville svart ærlig på om de hadde lånt bort kortet sitt til andre var meningene ganske splittet. Det ble også sagt av 2 stykker i denne gruppen at de ikke fikk den servicen eller som de forventet av IT-Tjenesten. 3 av 4 hadde også til felles at de mente sikkerhetskulturen på NTNU i Gjøvik var bra mens 1 sa at den var tungvinn.

4.6.2 IT-Tjenesten

Her hadde alle vi spurte lest både gammel og ny policy og ser på det som svært viktig at ansatte og studenter også leser policyen. De mener i større grad at adgangskort lånes ut oftere enn andre grupper, og at A-IMT er den avdelingen som låner bort adgangskort mest siden det er flere kortlesere i A-bygget. De har også gitt en lavere score enn de andre gruppene på om ansatte bør involveres i policy.

4.6.3 Akademiskpersonel

Vi oppfatet under intervjuene at denne gruppen hadde flest og mest spredte meninger. Her svarte folk helt forskjellig. Men en av de tingene som ble sagt rundt spørsmål angående policy var at det verken var sikkerhetsavdelingen eller IT-Tjenesten som skulle stå for sikkerhets policyen. Det var organisasjonen som skulle stå for hva som stod i policyen og ikke være i veien for arbeid som må gjøres. Det handlet om virksomhetens mål og om oppdragets betydning overgår den potensielle skade man opplever at bytte vil ha, altså at policyen bør utformes med bedre risikoforståelse. Det ble også poengtert at ansatte skal til en hvert tid ha tilgang til rommene sine. IT-Tjenesten måtte gjerne skrive en policy rundt selve kortbruken, men skille mellom det som er den overordnede policy. Det var flere som sa at om kort ikke ble lånt bort til ansatte ville det være svært problematisk dersom det ikke eksisterte reserveløsninger. De savnet gode reserveløsninger om man hadde glemt adgangskortet sitt. Alle i denne gruppen svarte at det ikke var lov å dele kort selv om mer en halvparten ikke hadde lest gammel policy, og ingen hadde lest gjeldene policy etter fusjonen.

4.6.4 PhD-Stipendiat

5 av 7 vi spurte i denne kategorien hadde fått adgangskort relativt raskt, mens 2 andre hadde det tatt mye lenger tid. Det var en som svarte at han måte vente veldig lenge med å få tilgang til alt han trengte. Dette kan være en årsak til at man blir nødt å låne andre sine kort. Dette var også noe som ble nevnt av management gruppen, de nevte at det kunne ta lenger tid å verifisere utenlandskstudenter og de ønsket bedre løsninger på dette. Vi ble også fortalt at da PhD-stipendiatene av og til jobbet tett med mastergradstudenter var det mange mastergradstudenter som trengte romtilgang der de ikke adgang. Da måtte PhD-stipendiatene enten fysisk åpne dører for mastergradstudenter eller låne vekk kortene sine så de fikk gjort jobben de var satt til. Stipendiatene mente det burde være bedre løsninger enn det som eksisterer i dag. Ingen hadde lest den gjeldene policyen for NTNU og kun en hadde lest gammel policyen. De fleste antok at det ikke var lov å låne bort adgangskortene sine men 2 sa de ikke visste. Når vi spurte om sikkerhetskulturen på NTNU i Gjøvik var svarene splittede, 2 svarte at de ikke vet, 1 mente at sikkerheten var bra, 1 sa at folk stoler på hverandre, 1 sa at den var slapp, 1 sa at folk viste at man ikke skulle låne det vekk mens siste sa at av praktiske årsaker lånes kort bort.

4.6.5 Studenter

Kun 1 av 3 studeter hadde lest gammel og ny policy. Studentene vi pratet med visste heller ikke om tilfeller der det var lånt vekk kort men 2 av 3 hadde blitt spurt om de kunne låne bort kortet sitt. De hadde ingen spesiell oppfatning om sikkerhetskulturen blant ansatte eller elever.

4.6.6 Eksterne

I gruppen for de eksterne inngår renhold og Stats Bygg. Ingen av dem hadde lest gjeldene policy, og kun en hadde lest gammel. Alle mente at det ikke var lov å låne kort, og at skolen så på dette som ganske alvorlig. De fleste hadde ikke hatt behov å låne andre sine kort. Her var det en som svarte at han følte behov årlig for å låne kort.

4.6.7 Forskjell på svar fra menn og kvinner

Vi la under intervjuene merke til at det var stor forskjell på menn og kvinners syn på hvordan skolen reagerte på låning av kort. De fleste av kvinnene vi pratet med mente at skolen så på dette mer alvorlig enn det menn gjorde som vist i tabell 11. Da vi spurte dette spørsmålet skulle de rangere på en skala fra 1 til 6, der 1 var mindre alvorlig og 6 var veldig alvorlig. Flere kvinner rangerte dette til 6 enn menn. Vi spurte også om hvor sannsynlig er det at folk innrømmer låning av adgangskort, med samme rangering. Dataene viser at kvinnene har mer tillit til at folk innrømmer låning av adgangskort enn det menn gjorde. Her var den laveste scoren blant kvinnene 3, mens 10 menn hadde rangert dette til 2 eller lavere.

4.7 Konklusjon av dataanalysen

Etter at alt var ferdig analysert sitter vi igjen med data rundt våre funn.

4.7.1 Usikkerhet rundt reserveløsninger

Det vi la klart merke til var usikkerheten rundt det med reserveløsninger. 14 av de 31 som svarte var usikre på om det faktisk eksisterte, og sa at de ønsket bedre reserveløsninger. 17 mente at det eksisterte reserveløsninger men av de som sa det fantes var det også ulike meninger om hvem man kunne henvende seg til om de hadde glemt kort. Det var 6 som mente de kunne gå til IT-Tjenesten, 3 til studenttorget, resterende svarte management eller be enn venn bruke sitt adgangskort. Det er tydelig at de ansatte er usikre på om det faktisk eksisterer reserveløsninger og eventuelt hvor de skal henvende seg. Selv innen IT-Tjenesten så var svarene sprikende. Av de vi spurte om det eksisterte en reserveløsning og eventuelt hva den var, så var det ingen som sa lik reserveløsning. Av de vi spurte sa den ene personen at reserveløsningen var å komme innom IT-Tjenesten eller studenttorget, og at de hadde mulighet for utlånskort. En anen sa at reserveløsningen var å gå til management som har reserve kort samt mulighet å skrive ut nytt kort.

4.7.2 Ubehag ved benyttelse av reserveløsninger

Det ble også nevnt av 2 personer som hadde vært innom IT-Tjenesten pga. de ikke hadde kort tilgjengelig, at de hadde opplevd situasjonen med IT-Tjenesten som svært ubehagelig. De hadde ikke fått den servicen de følte de hadde krav på. De nevnte også at de følte de ble sett ned på da de faktisk kom for å spørre om et lånekort. Om man vil at ansatte skal bruke en tjeneste så er det viktig at de ansatte ikke skal oppfatte den som ubehagelig, for da vil de heller ty til andre metoder, noe som igjen kan føre til policybrudd.

4.7.3 Sikkerhetspolicy i konflikt med arbeid?

Det viktigste for de ansatte er å gjøre jobben sin, og at policyen om å låne kort ikke må bli et hinder i å utfør sitt arbeid. Derfor kan man tenke seg til at om ansatte ikke er sikre på om det finnes en reserveløsning vil de spørre andre kolleger låne kort. Om de hadde visst om reserveløsning kan det være mulig de hadde brukt denne istedenfor. Også en av årsakene til at de ansatte spurte kolleger var at det var en rask og enkel måte å gjøre det på, så om man skulle hatt en annen reserveløsning og man vil at den skulle bli brukt så måtte mann tenkt på at den skulle vært rask og effektiv og så lite smertefull som mulig.

4.7.4 For høy sikkerhet?

Vi la merke til at svært mange syns det var i overkant mange kortlesere inne på A-bygget. Flere trudde den størst årsak til lån av kort var å gå på do. Mange innrømmet å ha lånet bort kortet til ansatte og gjester siden man ikke trengte

å gi vekk pinkoden. De kunne ikke forstå hvorfor man skulle ha en kortleser på dette området. Dette senker terskelen til å gi fra seg kortet noe som kan senke sikkerhetskulturen.

4.7.5 Mangel på risikoforståelse og konsekvenser

De ansatte var veldig usikre på hva som ville skje om det ble oppdaget at kort var blitt lånt ut. Noen trodde det ikke var en konsekvens mens andre visste ikke. Når vi spurte management om de kunne svare på, eller visste hva konsekvensen ville være, sa alle personene her nei. Hos IT-Tjenesten så virket usikkerheten på konsekvens like stor. De sa de ikke visste hva konsekvensen ville bli, men i praksis var det kun tilsnakk. Det var en som sa at dem ikke visste, den personen sa at konsekvensen ville være tilsnakk, og at hva avdelingene gjør med det etter at det har blitt rapportert, er opp til hver enkelt avdelingene. Det var ingen av de som ble intervjuet som kjente til om noen hadde fått konsekvens av å låne eller låne bort adgangskortet sitt bortsett fra en som sa at det har skjedd. Men det var ansatte som faktisk ønsket strengere og tydeligere straff på brudd av sikkerhetspolicyen.

5 Rotårsaksidentifisering

I dette steget vil vi identifisert en eller flere rotårsaker til problemet med kortlåning ved bruk av verktøyet fishbone ut i fra stegene vi har gjort ovenfor.

Forhånds antagelser

Før vi anvender årsaksanalyse verktøy til å identifisere rotårsaken, har vi gjort noen antagelser på hva som kan være rotårsaker etter dataanalysen. Dette gir oss muligheten til å se på forskjellen med våre antagelser nå, og hva vi faktisk kommer frem til etter at dette steget er utført. Vi har gjort antagelse at dårlig kommunikasjon med IT-Tjenesten samt for mye sikkerhet på noen plasser, som toaletter kan være rotårsaker til problemet. En annen faktor vi tar med er at management fortalte oss at prosessen med å gi adgangskort til utenlandske er mer tungvint en med norske. Dette er også noe vi mener kan være relevant til problemet.

5.1 Risikoforståelse

Da kort blir lånt ut blant studenter og ansatte er det ikke kun et policybrudd dette medfører men det øker også risiko for at hendelser kan inntreffe. Ved start av dette caset hadde vi et møte med IT-Tjenesten hvor de sa at identitet på avveie er noe av det mest kritiske med låning av kort. Når ansatte/studenter velger å låne vekk adgangskort blir også adgangsloggen kompromittert noe som kan gjøre det vanskelig å stille hvem som er ansvarlig til en gitt hendelse. Her er det viktig at alle ansatte/studenter vet hvilken risiko byttelåning av adgangkort faktisk utgjør. Dette kan vi si med sikkerhet, for da vi stillet sprøsmålet ”Hva

tror du er det værste som kan skje ved kortlåning?" mottok vi svar som: "Ingen ting i Norge", "Advarsel", "Tap av kort", "Prat med avdelingsleder", "Vet ikke" og "Kort blir ødelagt". Her er det viktig at skolen tar tak i dette problemet og underretter de som har adgangskort om konsekvenser.

5.2 Fishbone

Fishbone diagram er et verktøy som analyserer forholdet mellom et problem og dens årsaker. Det innehar aspekter fra brainstorming og systematisk analyse for å skape en kraftfull teknikk. Verktøyets viktigste formål er å forstå hva som forårsaker et problem og kan brukes til å utvikle samt gruppere årsaker til et problem. Den vurderer også systematisk årsaker og finner ut hvilke rotårsaker som mest sannsynlige.

5.2.1 Ønsket utbytte

Hovedproblemets årsaker skal undersøkes, og hva som skaper disse årsakene skal identifiseres. Deretter sorteres og grupperes årsakene til tilhørende problemer. Vi ønsket et diagram som viser et bilde av situasjonen og utifra denne identifisere rotårsaken.

5.2.2 Gjennomførelse

Steg 1 Problemet beskrives ved at adgangskort blir lånt mellom ansatte, studenter og mellom disse to gruppene.

Steg 2 Her ble det gjennomført brainstorming som tidligere. Hvor fokuset var å finne mulige årsaker. Forslagene vi kom opp med er i tab.13

Table 13: Resultat av brainstormingen

1. Dårlig kommunikasjon.	13. Ingen bra gjeldende policy.
2. Ikke kommunisert med ansatte at ny policy er gjeldende.	14. Mangelfulle rettigheter for for mastergradstudenter som jobber med PhD-stipendiater.
3. Låst ute av rom.	15. Trenger kort for å gå på do.
4. Dårlig/mangelfull reserveløsning.	16. IT-tjenesten ikke inkluderende når de lager policy.
5. IT-Tjenesten ikke inkluderende når de lager policy.	17. Lang tid å få adgangskort for noen ansatte.
6. IT-Tjenesten lite imøtekommende	18. Mangelfull bevistgjøring/trening/opplæring.
7. Ingen tydelig/synlig konsekvens.	19. Dårlig kultur rundt sikkerhet.
8. IT-Tjenesten begrunnelse på valg av løsninger er ikke formidlet godt nok.	20. Få har lest policy.
9. Glemt kort.	21. Høy tillit blandt ansatte.
10. Ansatte føler de ikke er inkludert i å forme policy.	22. Folk er for behjelplige
11. Tungvinne løsninger for eksterne.	23. Tungvinne løsninger.
12. IT-Tjenesten tar ikke hensyn til andres arbeid.	

Steg 3 Gruppering

Her gikk gruppen sammen om å velge forslag vi mente burde være med videre i prosessen. Forslaget som "trenger kort for å gå på do" ble byttet ut med "Høyere sikkerhet enn nødvendig". Videre ble hovedkategoriene tegnet på fishbone diagrammet som vist i fig.17.

Under datainnsamlingen fant vi ut at ansatte vil i større grad være med å forme policyen, her mener IT-tjenesten at de er inkluderende ved å sende ut policyene til høring før de blir vedtatt. Derfor har punktene "Ansatte føler seg ikke inkludert i å forme policy" og "IT-tjenesten ikke inkluderende når de lager policy" blitt slått sammen til "Ansatte føler seg ikke inkludert i formingen av policyer". Dersom ansatte ikke får delta i utformingen av policyer føler de mindre eierskap og dermed mindre forpliktelser.

Vidre kan vi se i tab.14 hvem elementener vi ønsket å ta med videre i prosessen.

Table 14: Filtrert liste

1. Dårlig kommunikasjon.	9. Mangelfulle romtilgangs rettigheter for master studenter som jobber med PhD.
2. Dårlige/mangelfulle reserveløsninger for ansatte, studenter og gjester/eksterne.	10. Lang tid for å få adgangskort for noen ansatte.
3. Høyere sikkerhet enn nødvendig.	11. Mangelfull bevistgjøring/trening/opplæring.
4. IT er lite imøtekommende.	12. Slapp kultur rundt sikkerhet.
5. Ingen tydelige/synlig konsekvenser.	13. Få har lest policy.
6. Glemt kort.	14. Høy tillit blant ansatte.
7. Ansatte føler seg ikke inkludert i formingen av policyer.	15. Folk er behjelpelige.
8. Tungvinne løsninger.	

I tab.15 kan man se hvordan vi grupperte listen.

Table 15: Gruppert liste

Organisatorisk	**Menneskelig**
1. Dårlig kommunikasjon.	1. Glemt kort.
2. IT-Tjenesten er lite imøtekommende.	2. Slapp kultur rundt sikkerhet.
3. Ansatte føler seg ikke inkludert i formingen av policyer.	3. Høy tillit blant ansatte.
4. Få har lest policy.	4. Folk er behjelpelige.
Teknisk system	**Mangler**
1. Dårlige/mangelfulle reserveløsninger for ansatte, studenter og gjester/eksterne.	1. Ingen tydelige/synlig konsekvenser.
2. Høyere sikkerhet enn nøvendig.	2. Mangelfulle romtilgangs rettigheter for master studenter som jobber med PhD.
3. Tungvinne løsninger.	3. Mangelfull bevistgjøring/trening/opplæring.
4. Lang tid for å få adgangskort for noen ansatte.	

Steg 4 identifisere årsaker, og steg 5, analysere rotårsaker

I dette steget kommer vi frem til hva rotårsakene av analysen er, vi mener her at det er flere rotårsaker som må forbedres for at symptomene til problemet skal kunne elimineres. Rotårsaker vi har funnet ut av er listet nedenfor:

1. Litt manglende/utydlige reserveløsninger.
2. Dårlig kommunisering om reserveløsningene som eksisterer.
3. Arbeiderenes effektivitet er ikke likestilt med IT-Tjenestens ønske om sikkerhet.
4. Lave sanksjoner av å låne bort adgangskort.

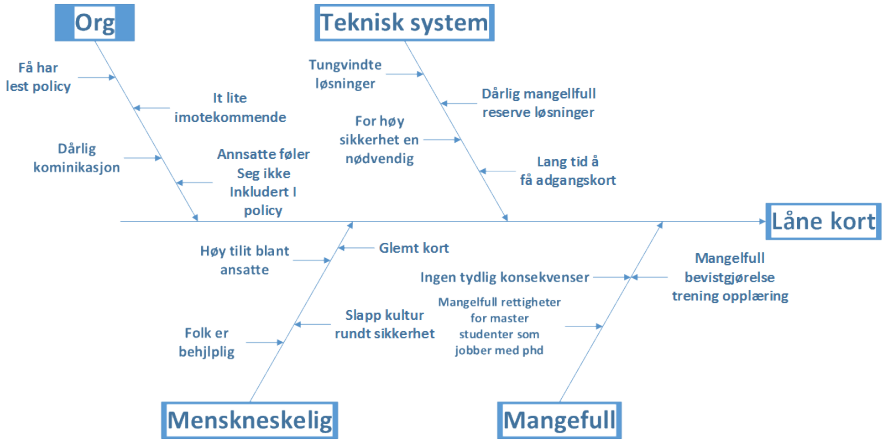


Figure 17: Fishbone

5.2.3 Konklusjon av verktøyet

Det var vanskelig å lage gode og relevante grupper på fishbone diagrammet når det ikke var helt klart definerte grupper på forhånd. Verktøyet er i stand til å gi en god visualisering av hvor alle elementene hører til. Dersom vi ser bort fra grupperinger, gikk det relativt smertefritt. Med verktøyet var vi i stand til å komme frem til det vi mener er rotårsakene til problemet.

5.2.4 Hvilken informasjon om verktøyet kan vi ta med oss til senere bruk?

Det burde vært definerte grupper føre verktøyet ble tatt i bruk, slik at det er lettere å gjennomføre. Det hadde også hjulpet oss å hatt mer erfaringer og vert mer innenforstått med verktøyet før det ble anvendt på et case. Her mener vi at jo mer man arbeider med ting som dette jo bedre og lettere vil det være å jobbe med dette videre.

6 Rotårsaks eliminering

I dette kapittelet går vi gjennom vårt løsningsforslag på problemet. Hvilke verktøy vi brukte og hvoran vi gjennomførte problemelimineringen.

6.1 SIT

Systematic Inventive Thinking baserer seg på å undersøke et eller flere problemers komponenter. Alle komponentene skal så vurderes ved hjelp av de fem SIT prinsippene[1]. Disse prinsippene er som følger:

1. *Attribute dependency*: vurder om en endring i komponenten vil føre til forbedring.
2. *Component control*: undersøk hvordan komponenten er forbundet med miljøet rundt seg.
3. *Replacement*: bytt ut noe i komponenten med noe fra komponentens omgivelse.
4. *Displacement*: vurder om komponten kan få økt ytelse ved at en del av komponenten fjernes.
5. *Division*: vurder om splittelse av en komponent eller et produkts attributter kan gi forbedring.

6.1.1 Ønsket utbytte

Kunnskap om hvilke problemårsaker fra rotårsaksidentifiseringen som trengs å implementere løsninger til for at alle problemene skal opphøre. Ved å anvende SIT håper vi å finne kreative løsninger, noe verktøyet er kjent for å bidra til.

6.1.2 Gjennomførelse

Steg 1 baserer seg på å samle inn personell med relevant kunnskap. Dette var ikke gjennomførbart for oss og vi fortsatte derfor med vår gruppe.

Steg 2 listes og grupperes komponenter. Her skrev vi ned rotårsakene fra rotårsaksidentifiseringen i forrige kapittel. Da dette var gjort listet vi alle elementer som tilhørte problemet og sorterte de i grupper hvor hver gruppe fikk et eget navn som vist i tab.16 og tab.17.

Table 16: Gruppering av elementer

Mangelfull/utydelige reserveløsninger	Dårlig kommunikasjon
Studenttorget	Antagelser/uklarheter
IT-Tjenesten	Nettsider
Manegement	Søkefelt
Antagelser/uklarheter	Kommunikasjons parter
Kortprinter	Mennesker
Reservekort	Policy
Adgangskort	Email
	Telefon

Table 17: Gruppering av elementer

Lave sanksjoner på lån av kort	Arbeidernes effektivitet ikke likestilt med IT-tjenestens fokus på sikkerhet
Policy	Organisasjonens mål
Straffbar handling	Avdelingens mål
IT-Tjenesten	Kortpin og lesere
Vurdering av straff	Byggets sikkerhetsnivåer
Utførelse av straff	Enkeltpersons arbeidsoppgaver
Presedens	Arbeidsområder
Adgangskort	Kritisk materiale
Arbeidsmiljøloven	Mennesker
	Policy

Steg 3 skal de fem SIT prinsippene anvendes. Alle komponenter fra steg 2 ble kandidater for videre undersøkelse. Ikke gjennomførbart tilsvarer mangel på mulighet til å anvende SIT prinsipp på punktet.

Policy:
(Attribute dependency): Tydeliggjøre straff på brudd på policy og la ansatte få lov til å være med på forming av policy.
(Conponent control): Gjøre policy lettere å få tak i.
(Replacement): Ikke gjennomførbart
(Displacement): Ikke gjennomførbart
(Division): Ikke gjennomførbart

Antagelser/uklarheter:
(Attribute dependencey): Tydliggjøre og bevistgjøre.
(Component control): Spør istedenfor å anta.
(Replacement): Ikke gjennomførbart
(Displacement): Identifisere og eliminere antagelser.

(Division): Ikke gjennomførbart

Byggets sikkerhetsnivåer:
(Attribute dependency): Se over/revurdere sikkerhetsnivåer.
(Component control): Kontrollere at verdisaker i rom tilsvarer sikkerhetsnivå.
(Replacement): Biometri.
(Displacement): Unødvendige kortlesere.
(Division): Ikke gjennomførbart

IT-Tjenesten:
(Attribute dependency): Bytte ut ansatte.
(Component control): Sjekke med omgivelsene om løsningene fungerer.
(Replacement): Bytte mellom IT-Tjenesten, management eller studenttorg.
(Displacement): Dersom IT-Tjenesten har for mange ansvarsområder.
(Division): Splitte mellom tydlige grupper innad i IT-Tjenesten.

Nettsider:
(Attribute dependency): Tilføye hjelpeside for adgangskort.
(Component control): Kontrollere tilgjengelighet på hjelp via søk ol. og kontrollere at det er satt gode metadata.
(Replacement): Ikke gjennomførbart
(Displacement): Ikke gjennomførbart
(Division): Ikke gjennomførbart

Reservekort/adgangskort:
(Attribute dependency): Tilpasset tilgang på rom (adekvat).
(Component control): Tilgjengelighet i alle bygg.
(Replacement): Ikke gjennomførbart
(Displacement): Ikke gjennomførbart
(Division): Ikke gjennomførbart

Steg 4 diskuterte vi hvilke alternativer som er realistiske å anta at kan gjennomføres. Ideene vi satt igjen med blir så listet under.

Policy:
(Attribute dependency): Tydliggjøre straff på brudd på policy og la ansatte få lov til å være med på forming av policy.
(Conponent control): Gjøre policy lettere tillgjenglig.

Antagelser/uklarheter:
(Attribute dependencey): Tydliggjøre og bevisstgjøre.

(Component control): Hvis mulig og ikke for mye bry: spør istedenfor å anta.

Byggets sikkerhetsnivåer:
(Attribute dependency): Se over/revurdere sikkerhetsnivåer.
(Component control): Kontrollere at verdier i rom tilsvarer sikkerhetsnivå.

IT-Tjenesten:
(Component control): Sjekke med omgivelsene om løsningene fungerer.

Nettsider:
(Attribute dependency): Tilføye hjelpeside for kort.

Reservekort/adgangskort:
Attribute dependency): Tilpasset tilgang på rom (adekvat).

Steg 5 Her skal diskusjonen om hvilke ideer som er best å implementere fortsette, samtidig som ett eller flere løsningsforslag genereres hvor detalj skal bli tatt hensyn til.

Policy
(Attribute dependency): Tydeliggjøre straff ved brudd på policy og la ansatte få lov til å være med på forming av policy.
Vi foreslår at alle grupper får i tilstrekkelig grad være med på innvirkning i policy, om det innebærer fysisk tilstedeværelse eller mulighet til å gi tilbakemeldinger. Muligheten for å kunne komme med tilbakemeldinger må være godt nok kommunisert slik at det ikke er tvil om at personene kjenner muligheten. Eksempel kan være sticky eposter, som vil vises på toppen i innboksen, muligens ha egen konvolutt farge og er uslettbar i en viss periode.

(Conponent control): Gjøre policy lettere tilgjengelig. I innsida bør det være lett å finne en side over gjeldende bestemmelser og policy som også kommer tydelig frem på søk.

Antagelser/uklarheter
(Attribute dependencey): Tydliggjøre og bevisstgjøre. Forsøke å unngå å gjøre antagelser på sikkerhets restriksjoner på bygget og dets rom. Avklare med de ansatte om hvilke sikkerhetsbehov som er nødvendige for å unngå at de implementerte sikkerhets tiltakene reduserer de ansattes produktivitet.

(Component control): Hvis mulig og ikke for mye bry: spør istedenfor å anta. Det er mange feil som oppstår dersom en gjør antagelser, og samtidig er det lett å gjøre antagelser. Derfor er det være viktig å maksimere kommunikasjonen for å få stilt spørsmål, selv om en ville følt seg trygg på å gjort en antakelse i situasjonen. Vise skjønn.

Byggets sikkerhetsnivåer
(Attribute dependency): Se over/revurdere sikkerhetsnivåer. Forhindre at sikkerhetsnivåer er overdrevent i forhold til rommets bruk. For høyt sikkerhetsnivå skaper snarevei-løsninger hos de ansatte.

(Component control): Kontrollere at verdier i rom tilsvarer sikkerhetsnivå.

IT-Tjenesten
(Component control): Sjekke med omgivelsene om løsningene fungerer.Kommunisere med de ansatte om løsningene som er implementert fungerer. Dette fordi de ansatte er brukerene og kan formidle sine brukeropplevelser som kan bli tatt i betraktning av IT tjenesten.

Nettsider
(Attribute dependency): Tilføye hjelpeside for adgangskort. Opprette en nettside på ntnu.no domenet som gjør det mulig å lese støttelitteratur om problemer rundt adgangskort samt hvilke reserveløsninger som eksisterer og hvordan å utnytte dem.

Reservekort/adgangskort
(Attribute dependency): Tilpasset tilgang på rom (adekvat). Gi administratorer bedre muligheter til å tilpasse romtilganger med hovedfokus på å kunne gi reservekort som har adekvat og spesifikk romtilgang. Dette vil si å unngå å gi generell romtilgang på reservekort som ikke er tilstrekkelig for alle.

6.1.3 Konklusjon av verktøyet

Verktøyet ga godt utbytte. Gjennomførelsen var tung og det ble mange småkomponenter. Gjennomførelsen av behandling på småkomponentene var tidskrevende og det var lett å gjøre feil. Utførelsen av steg 2 var ikke helt optimalt men krevende i forhold til tid. Større problemer med flere komponenter vil bli nesten eksponentielt tyngre å bruke verktøyet på.

6.1.4 Hvilken informasjon om verktøyet kan vi ta med oss til senere bruk?

Ha god oversikt over problemet og miljøet problemet befinner seg i. Verktøyet kan bli tidskrevende, og det er derfor viktig å ha satt av nok tid til å gjennomførelsen.

7 Løsningsimplementering

Implementeringen av løsningsforslag vil bli organisert av IT-Tjenesten og relevant nøkkelpersonell i de forskjellige avdelingene.

Før man begynner å anvende verktøyet er det viktig at personell med riktig kunnskap på områdene inkluderes. Dette gjelder spesielt når nettside skal lages, og byggets sikkerhetsnivåer skal gjennomgås/revurderes.

I dette kapittelet vil vi gi et eksempel på hvordan planlegging av løsningsimplementering kan utføres. Det er vanskelig for oss som sitter utenfor å komme med noe annet enn forslag, derfor viser vi et eksempel på hvordan det kan gjøres. Vi har da valgt å bruke "byggets sikkerhetsnivåer" for dette eksemplet.

7.1 Verktøyet

Diagrammet åpner for muligheten til å gruppere arbeidsoppgavene og deres underkomponenter inn i et hierarkisk løsningsforslag. Løsningsforslaget følges fra venstre til høyre og fra nederst i diagrammet til øverst.

7.1.1 Ønsket utbytte

Lage en strukturert plan som kan følges i kronologisk rekkefølge for å oppnå ferdig løsningsimplementering.

7.1.2 Gjennomførelse

Steg 1 generer liste med aktiviteter som må utføres for å få gjennomført løsningen. Denne kan ses i tab.18

Table 18: My caption

Samle inn kunnskapspersonell.	Kommunisere med samarbeidspartnere (skolens tredjeparter).
Få oversikt over nivåer som eksisterer.	Oppdatere seg på lover og regelverk.
Få oversikt over arbeidsoppgaver som utføres på området.	Lage forslag til nye sikkerhetsnivå.
Få oversikt over materiell som oppbevares på området.	Kommunisere forslag på nye sikkerhets
Undersøke dokumentasjon på materiell som oppbevares på området.	Oppdatere sikkerhetsnivåene på områdene.

Steg 2 Skrive ned aktivitetene helst via ett verb og ett substantiv (Verktøyet er beskrevet på engelsk, og derfor kan det bli vanskelig å følge reglene ordrett på steg 2. Før verktøyet anvendes, ta kontakt med nøkkelpersoner slik at de er i stand til å bidra når verktøyet er bestemt at skal anvendes.):

1. -samle personel
2. -oversikt sikkerhetsnivåer

3. -oversikt oppgave
4. -oversikt matriell
5. -undersøke matrielldokumentasjon
6. -kommunisere samarbeidspartnere
7. -undersøke lover
8. -forslag sikkerhetsnivåer
9. -kommunisere sikkerhetsnivå
10. -oppdatere sikkerhetsnivå

Steg 3 Arrangerte aktivitetene i naturlige undergrupper som skal utføres i sekvens innad i disse gruppene:

1. Samle personell
   (a) Kommunisere samarbeidspartnere
   (b) Samle personell.
2. Undersøkelser
   (a) Oversikt oppgave .
   (b) Oversikt sikkerhetsnivåer.
   (c) Oversikt matriell.
   (d) Undersøke matrielldokumentasjon.
   (e) Undersøke lover.
3. Gjennomførelser
   (a) Forslag sikkerhetsnivåer
   (b) Kommunisere sikkerhetsnivå
   (c) Oppdatere sikkerhetsnivå

Steg 4 plasserte vi de arrangerte undergruppene i tre diagrammet som vist i fig.18

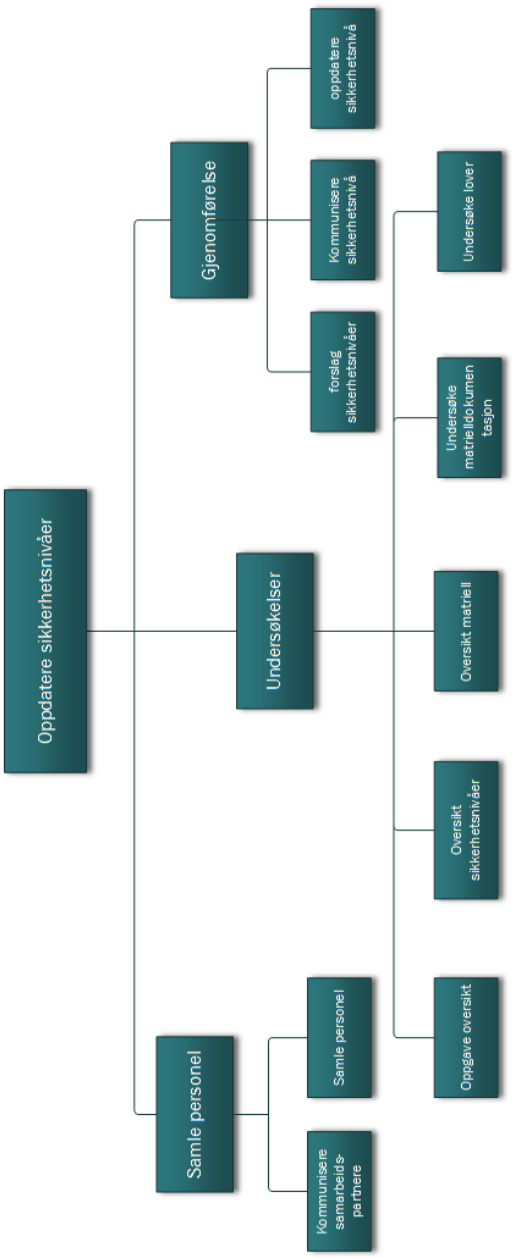


Figure 18: Tree

7.1.3 Konklusjon av verktøyet

Det vi har fått gjort er forslag, og derfor kan vi ikke anslå kostnadder, tidsbruk eller hvem som må være tilknyttet hver oppgave.
Verktøyet er veldig godt organisert til å vise hvilken oppgave som skal utføres til hvilken tid, og hvilken oppgave som må utføres før en annen oppgave kan påbegynnes.

7.1.4 Hvilken informasjon om verktøyet kan vi ta med oss til senere bruk?

Verktøyet er beskrevet på engelsk, og derfor kan det bli vanskelig å følge reglene ordrett på steg 2. Før verktøyet anvendes, ta kontakt med nøkkelpersoner slik at de er i stand til å bidra når verktøyet er bestemt at skal anvendes.

8 Diskusjon og konklusjon

Her vil vi se på og diskutere effekten vi mener rotårsaksanalysen har har og om vi mener rotårsaksanalyse er anvendbart innen informasjonssikkerhets samt diskutere kost-nytte effekt.

8.1 Resultater

8.1.1 Datainnsammling og analyse

Igjennom intervju fasen ble 36 personer intervjuet, hvor valget av intervju objekter var basert på hvilke avdelinger de tilhørte skolen. Det ble funnet at det var forskjeller mellom kvinner og menn på hvor alvorlig de trodde skolen så på byttelåning av kort, der kvinner trodde det var mer alvorlig enn det menn gjorde. Videre ble det funnet at svært få hadde lest den nye eller den gamle sikkerhets policyen.

8.1.2 Rotårsaksidentifisering

Det var totalt 4 rotårsaker vi kom frem til, der alle vi mener alle bør behandles.Rotarsakene vi kom frem til var:

1. Litt manglende/utydlige reserveløsninger.
2. Dårlig kommunisering om reserveløsningene som eksisterer.
3. Arbeiderenes effektivitet er ikke likestilt med IT-Tjenestens ønske om sikkerhet.
4. Lave sanksjoner av å låne bort adgangskort.

Eliminering

Grunnet tidsbegrensninger ble det utarbeidet løsningsforslag på en rotårsak, hvor gjennomføringen ble beskrevet og verktøyet ble konkludert basert på erfaringene vi fikk ved å anvende det. Løsningsimplementeringen i kapittel 7 - "løsningsimplementering", kunne ikke praktisk gjennomføres av oss da vi jobber analytisk med caset. SIT er et komplisert verktøy og alle ideene som ble laget i rotårsakselimineringen var:

1. Policy
2. Antagelser/uklarheter
3. Byggets sikkerhetsnivåer
4. IT-tjenesten
5. Nettsider
6. Reservekort/adgangskort

Løsningsforslaget

Vårt løsningsforslag ble utarbeidet på resultatet i kapittel 5 rotårsakseliminering, som ble laget med verktøyet SIT i steg 5 "byggets sikkerhetsnivåer". Resultatet er i trediagrammet i fig.18 som viser utføringen av vårt forslag i kronologisk rekkefølge, startende fra nederst til venstre i diagrammet. Hovedpunktene er først og fremst samling av personell med kunnskap om problemområdet, deretter utføre vi undersøkelser som innebærte blant annet sikkerhets nivåer, materiell dokumentasjon og lovverk. Siste hovedpunktet er gjennomførelse av forslag til nye sikkerhetsnivåer, kommunisere de nye sikkerhetsnivåene og oppdatere nåværende nivåer.

8.2 Diskusjon

Vi begynte med å forstå problemet ved å utføre en performance matrix. Resten av analysen ble forsøkt knyttet opp mot resultatene fra performance matrixen. I vårt tilfelle fungerte det bra å bruke hovedpunktene i performance matrixen som egne kapitler i analyse delen av kapittel 4.

Gruppen merket under utførelsen at vi hadde liten erfaring og at dette førte til at ting tok lengre tid enn antatt. Videre førte dette til at vi ikke fikk kommunisert det vi ville fordi vi ikke forstod det helt og manglet noe kontroll.

Vi antok at datainnsamlingen ville være mer problematisk og ta lengre tid enn det den faktisk gjorde. Dersom vi hadde hatt mer tid ville vi samlet inn flere intervjuer med større spredning på organisatorisk felt og kjønn. En av de viktigeste erfaringene vi tar med oss er å gjennomgå spørsmålene mer grundig innad i gruppen. Det var ganger vi ønsket at vi hadde stilt flere spørsmål som vi savnet å ha med i analysen. Svarene intervjuobjektene ga virker veldig ærlige, men en ting vi tar i betraktning er at vi kunne styrt intervjuene mer slik at svar ble mer uniforme. De spørsmålene med rangering på en skala var mye raskere samt lettere å analysere enn de der intervjuobjektene hadde mer frihet til å svare hva de ville.

I rotårsakseliminering brukte vi verktøyet fishbone, dette var nytt for oss da ingen av oss hadde jobbet med dette før. Her hadde boken "Root cause analysis: Simplified tools and techniques[[1]] s.119" to fremgangsmåter å velge mellom "Dispersion analysis" eller "Cause enumeration"

Hovedforskjellen er at "Cause enumeration" starter med brainstorming hvor "Dispersion analysis" fyller fishbone diagrammet direkte med data. Resultatmessing er det ingen forskjell.

I rotårsaks eliminering opplevde vi SIT som komplisert å forstå, og her kunne erfaring ha hjulpet oss til å være mer effektive til å gjennomføre, samtidig som

gruppen opplevde prosessen som veldig langtekkelig.

Vi opplevde løsingsimplementeringen som en enkel og rett frem metode.

Da resultatene er basert på data fra intervjuer, gir de et innsyn i hva personell på skolen har som meninger. Ideene generert i løsningsimplementeringen baserer seg derfor på å løse problemene som ble avdekket i intervju svarene. Her er det viktig at skolen tar ansvar og formiddler informasjon om konsekvenser og reserveløsninger.

8.2.1 Videre arbeid

Veien på videre arbeid kan være å følge boken mer slavisk og punktvis en det vi har valgt å gjøre på dette caset. Man kan samle inn større mengder med data og prøve andre verktøy en det vi har brukt på flere oppgaver med måling av resultater. Dette kan være viktig i forskningen av verktøyenes effekt og videreutvikling. Man kan også involvere nøkkelpersoner mye mer enn det vi vært i stand til i form av f.ex workshops. Verktøyene er egentlig ment for bruk av personer som kjenner til bedriften og prosessene bedre. Dette vil mest sannsynlig redusere tiden på selve gjennomførelsen av analysen.

8.3 Tidsbruk

Den totale tiden brukt på case 2 er omtrent 220 timer per person (660 timer).

Tabellen under viser bare den konsentrerte tiden brukt på selve verktøyene iløpet av vellykket forsøk, men inkluderer ikke tiden brukt på diskusjon av valg og testing av verktøy og rapport skriving.

Table 19: Loggføring

Loggføring av tidsbruk på verktøyene		
Fase	**Verktøy**	**Tidsbruk t=timer m=minutter**
Problemforståelse	Performance Matrix	3,25 timer
Problemårsaksidemyldring	Brainstorming	1,23 timer
Problemårsaks datainnsamling	Intervju	10,85 timer
Problemårsaks dataanalyse	Kvalitativ og kvantitativ analyse, SPSS	13,5 timer
Rotårsaks identifisering	Fishbone	6,4 timer
Rotårsaks eliminering	SIT	7,1 timer
Løsningsimplementering	Tree	1,2 timer
		Total 43,53 timer.

9 Appendix

1. Blir det ført logger på hvilke kort som bruker hvor og når?
2. Ligger for det meste problemene ved byttelåning av kort i “privilegie escalation”, eller er det problematikk i at personer på samme sikkerhetsnivå byttelåner også kort?
3. Om nøkkelkort blir lånt bort er det kun et prudd på policy eller er det flere konsekvenser?
4. Er det like ille å at studenter låner kort av hverandre, ansatte låner av hverandre eller at ansatta og elever låner mellom hverandre?
5. Ofte jobber master studenter for phd og de trenger tilgang til rom. Er det forståelig at disse låner bort kort?
6. Hem bestemmer rom tilgang?
7. Er det noe estimat på tap med tanke på innbrudd?
8. Sier dere ifra til personer dere mistenker etter å ha sett på logg med tanke på tyveri og hva blir konsekvensen?
9. Hvordan vet dere at folk låner bort kort?
10. Hvor trenge er dere på å gjennomføre konsekvenser mot personene?
11. Er det nye sikkerhets policyer som tar over for de som HiG hadde, og er det noen mulighet at vi kan få kikke på de som er relevante for adgangskort?
12. Hva ser dere på som de største problemene, og har dere estimater på hvor ofte det lånes ut?
13. Hvem står for kort produksjonen?
14. Hvis studenten er kastet ut av skolen hvor lang tid tar det før adgangskortet blir deaktivert?
15. Har dere noen form for kort som kan lånes?
16. Hva ser dere på som det mest kritiske når det kommer til uretmessig låning av kort?
17. Hvor mange ansatte er det på gjøvik?
18. Hvilken avdeling mener dere deler mest nøkkelkort?
19. Hvem har hovedansvar for nøkkelkort?
20. Kan policy være en årsak til at folk låner bort kort?

Her er en liste over spørsmålene som ble stilt til ansatte og studenter. Dette er ikke de samme spørsmålene som ble stilt til Management eller IT-Tjenesten. Disse spørsmålene ble ikke lest av intervjuobjektene men stilt av oss muntlig.

Mann/kvinne: Alder:

1. Hvilken nasjonalitet har du?
2. Hvilket organisatorisk fagområde tilhører du? (F.ex A-IMT, TØL, HOS)
3. Har du lest den gamle sikkerhetspolicyen?
4. Nå som vi har fusjonert med NTNU, har du lest den nye sikkerhetspolicyen?
5. Fra en skala fra 1 til 6, hvor 1 er "ikke i det heletatt" og 6 er "igjennom hele prosessen" føler du at ansatte som følger policyene skal få være med på å forme policyene?
6. Vet du om det er lov eller ikke å byttelåne adgangskort?
7. Kunne du sagt oss hva IT-Tjenestens syn på kortlåning er?
8. På en skala fra 1 til 6 der 1 er mindre alvorlig og 6 er veldig alvorlig, hvor alvorlig tror du skolen ser på byttelåne av adgangskort?
9. Vet du hva konsekvensene vil være om skolen finner ut at personer byttelåner adgangskort?
10. På en skala fra 1 til 6, hvor 1 er lite sannsynlig og 6 er svært sannsynlig hvor sannsynlig tror du det er at ansatte innrømmer byttelåne av adgangskort kort?
11. Tror du det er en lavere terskel for å låne bort adgangskort til familiemedlemmer?
12. Hvor ofte tror du adgangskort blir lånt på skolen? Aldri, Årlig, Månedlig, Ukentlig, Daglig
13. Hva kan du tenke deg er årsaker til at folk velger å låne bort adgangskort og pin?
14. Bør det være lov å låne bort adgangskort og pin til personer som har samme romtilgang?
15. Kjenner du til om noen har fått konsekvenser av lån/bortlån av adgangskort?
16. Hva tror du er det verste som kan skje ved kortlåning?
17. Hva føler du er kultur rundt kortdeling på NTNU Gjøvik?
18. Vet du om tilfeller der det har vært lånt ut adgangskort mellom ansatte og studenter?
    a. Hvis ja: Husker du årsaken?
19. Har du blitt spurt av noen om de kan låne ditt adgangskort?
    a. Hvis ja: Hadde de noen begrunnelse på hvorfor de trengte å låne adgangskortet?
20. Har du noen gang følt behovet for å skulle spør noen om å låne deres adgangskort? Aldri, Årlig, Månedlig, Ukentlig, Daglig
21. Vet du om det finnes noen reserveløsning dersom du har glemt adgangskortet ditt?
22. Har du noen formening om hvilken avdeling som som byttelåner mest?
23. Tror du nasjonalkultur kan ha påvirkning på holdninger når det gjelder lån og bortlån av adgangskort?
24. Fra en skala fra 1 til 6. Der 1 er veldig lang tid og 6 er hadde tilgang da jeg startet: Fikk du tilgang til alle rommene du trengte med en gang?
25. Hva ser du for deg som mulige mottiltak for å forebygge lån og bortlån av adgangskort og pin mellom ansatte/studenter?

Dette er de spørsmålene som ble stilt til IT-Tjenesten

Mann/kvinne: Alder:

1. Hvilken nasjonalitet har du?
2. Hvilket organisatorisk fagområde tilhører du? (F.ex A-IMT, TØL, HOS)
3. Har du lest den gamle sikkerhetspolicyen?
4. Nå som vi har fusjonert med NTNU, har du lest den nye sikkerhetspolicyen?
    a. Hvem har laget gjeldene policy
5. Er det viktig for IT avdelingen at ansatte har lest skolens policyer?
    a. På en skala fra 1 - 6 der 1 er ingen og 6 er alle. Hvor mange ansatte trur du har lest policyen ang. adgangskort?
6. Fra en skala fra 1 til 6, hvor 1 er “ikke i det heletatt” og 6 er “igjennom hele prosessen”: i hvilken grad mener du at de ansatte skal kunne få være med på å forme policyene?
7. Tror du alle vet at det ikke er lov å låne eller låne bort adgangskort?
8. Kunne du sagt oss hva IT-Tjenestens syn på kortlåning er?
9. På en skala fra 1 til 6 der 1 er mindre alvorlig og 6 er veldig alvorlig, hvor alvorlig er skolens syn på lån av adgangskort blant ansatte og studenter?
10. Vet du hva konsekvensene vil være om skolen finner ut at personer byttelåner adgangskort?
11. På en skala fra 1 til 6, hvor 1 er lite sannsynlig og 6 er svært sannsynlig hvor sannsynlig tror du det er at ansatte innrømmer byttelåne av adgangskort kort?
12. Tror du det er en lavere terskel for å låne bort adgangskort til familiemedlemmer?
13. Hvor ofte tror du adgangskort blir lånt på skolen? Aldri, Månedlig, Ukentlig, Daglig
14. Hva kan du tenke deg er årsaker til at folk velger å låne bort adgangskort og pin?
15. Kjenner du til om noen har fått konsekvenser av lån/bortlån av adgangskort?
16. Hva tror du er det verste som kan skje ved kortlåning?
17. Hva føler du er kultur rundt kortdeling på NTNU Gjøvik?
18. Vet du om tilfeller der det har vært lånt ut adgangskort mellom ansatte og studenter?
    a. Hvis ja: Husker du årsaken?
19. Har du blitt spurt av noen om de kan låne ditt adgangskort?
    a. Hvis ja: Hadde de noen begrunnelse på hvorfor de trengte å låne adgangskortet?
20. Har du noen gang følt behovet for å skulle spør noen om å låne andres adgangskort? Aldri, Årlig, Månedlig, Ukentlig, Daglig
21. Vet du om det finnes noen reserveløsning dersom du har glemt agnagskortet ditt?
22. Har du noen formening om hvilken avdeling som som byttelåner mest?
23. Tror du nasjonalkultur kan ha påvirkning på holdninger når det gjelder lån/bortlån av adgangskort?
24. Hva ser du for deg som mulige mottiltak for å forebygge lån og utlån av adgangskort og pin mellom ansatte?

Dette er de spørsmålene som ble stilt til Management

Mann/kvinne: Alder:

1. Hvilken nasjonalitet har du?
2. Hvilket organisatorisk fagområde tilhører du? (F.ex A-IMT, TØL, HOS)
3. Har du lest den gamle sikkerhetspolicyen?
4. Nå som vi har fusjonert med NTNU, har du lest den nye sikkerhetspolicyen?
5. Fra en skala fra 1 til 6, hvor 1 er "ikke i det heletatt" og 6 er "igjennom hele prosessen": i hvilken grad mener du at de ansatte skal kunne få være med på å forme policyene?
6. Vet du om det er lov eller ikke å låne eller låne bort adgangskort?
7. Kunne du sagt oss hva IT-Tjenestens syn på kortlåning er?
8. På en skala fra 1 til 6 der 1 er mindre alvorlig og 6 er veldig alvorlig, hvor alvorlig tror du skolen ser på byttelåne av adgangskort?
9. Vet du hva konsekvensene vil være om skolen finner ut at personer byttelåner adgangskort?
10. På en skala fra 1 til 6, hvor 1 er lite sannsynlig og 6 er svært sannsynlig hvor sannsynlig tror du det er at ansatte innrømmer byttelåne av adgangskort?
11. Tror du det er en lavere terskel for å låne bort adgangskort til familiemedlemmer?
12. Hvor ofte tror du adgangskort blir lånt på skolen? Aldri, Månedlig, Ukentlig, Daglig
13. Hva kan du tenke deg er årsaker til at folk velger å låne bort adgangskort og pin?
14. Bør det være lov å låne bort kort og pin til personer som har samme romtilgang?
15. Kjenner du til om noen har fått konsekvenser av lån/bortlån av adgangskort?
16. Hva tror du er det verste som kan skje ved kortlåning?
17. Hva føler du er kultur rundt kortdeling på NTNU Gjøvik?
18. Vet du om tilfeller der det har vært lånt ut adgangskort av andre ansatte?
    a. Hvis ja: Husker du årsaken?
19. Har du blitt spurt av noen om de kan låne ditt adgangskort?
    a. Hvis ja: Hadde de noen begrunnelse på hvorfor de trengte å låne adgangskortet?
20. Har du noen formening om hvilken avdeling som som byttelåner adgangskort mest?
21. Tror du nasjonalkultur kan ha påvirkning på holdninger når det gjelder lån/bortlån av adgangskort?
22. Fra en skala fra 1 til 6. Der 1 er veldig lang tid og 6 er hadde tilgang da jeg startet: Fikk tilgang til alle rommene du trengte med en gang?
23. Hva ser du for deg som mulige mottiltak for å forebygge lån/utlåne av adgangskort og pin mellom ansatte?
24. Må du ofte gi ut nye adgangskort til ansatte eller studenter som kommer å spør?
25. Har du oversikt over om IT-Tjenesten eller Student Torget leverer ut nye adgangskort til studenter eller ansatte?

References

[1] Andersen, B. & Fagerhaug, T. 2006. *Root cause analysis: Simplified tools and techniques*. ASQ Quality Press, second edition.

[2] Ammerman, M. 1998. *The root cause analysis handbook: A simplified approach to identifying, correcting, and reporting workplace errors*. Steiner-Books, first edition.

[3] Okes, D. 2009. *Root cause analysis: The core of problem solving and corrective action*. ASQ Quality Press, first edition.

[4] NTNU. 2010. Prinsipper for informasjonssikkerhet ved ntnu. [Online; accessed 26-APR-2016]. URL: https://innsida.ntnu.no/c/wiki/get_page_attachment?p_l_id=22780&nodeId=24647&title=Informasjonssikkerhet&fileName=Prinsipper_versjon1_00.pdf.

Case 3: DDoS

Henrik Miguel Torres, Erlend Brækken, Niclas Hellesen

May 17, 2016

Contents

List of Figures

List of Tables

.

Executive summary

Vi har fått i oppdrag fra slettmeg å utføre en rotårsaksanalyse på et DDOS angrep. Her har vi brukt en metodikk som går over 7 steg for å avdekke opprinnelsen til problemet som foreslått av Anders og Fagerhaug 2008 [1].

For å forstå problemet ble følgende 3 verktøy anvendt.
Swim lane flowchart ble brukt for å få en tydelig visning av flyten gjennom utførelser og hendelser og få en økt detaljforståelse. Deretter utførte vi en critical incident for å forstå hvilke aspekter av problemet som må bli løst. Til slutt ble det anvendt en performance matrix for å forstå hva slettmeg mente var viktige aspekter av deres arbeid og hvilken ytelse hvert aspekt hadde.

Det ble utført en problemårsaks idemyldring hvor en ustrukturert brainstorming ble anvendt for å lage en liste med antatte årsaker til problemet eller de problemer som bygger opp til de synlige symptomene.

Datainnsamlingen baserte seg på samtaler med kontaktperson i slettmeg. Her ble det forsøkt anvendelse av verktøyet check sheets, som viste seg å ikke passe situasjonen godt og et resultat ble oppnådd via samtale med kontaktperson. Når dataene skulle analyseres var det få verktøy som passet og valget falt dermed på affinity diagram. Vårt ønskede utbytte med verktøyet var å lete etter skjulte sammenhenger i dataene. Ingen skjulte sammenhenger ble funnet men en god fremstilling av data ble oppnådd.

I rotårsaks identifisering og eliminering ble rotårsakene identifisert ved diskusjon da ingen verktøy passet situasjonen. Rotårsakene vi fant var angriperens motivasjon, mangel på forberedelser og mangel på kontrol. I rotårsaks elimineringen ble det anvendt Systematic Inventive Thinking til å identifisere hvilke problemårsaker det var nødvendig og realistisk å implementere løsninger til. Våres løsningsforslag var bedringer i prosedyre og kontrakt. Vi var ikke i stand til å komme med forslag til løsningsimplementasjon, men beskrev forslag rundt løsning av problemene.

1 Introduksjon

Årsaksanalyse kan anvendes for å finne hovedårsakene til at ett eller flere problemer inntraff. En rotårsaksanalyse gjøres i etterkant av hendelsesforløpet, som står i kontrast med risikohåndtering som behandler tenkte situasjoner i fremtiden. Gevinsten av å utføre en rotårsaksanalyse er å kunne finne en eller flere rotårsaker. Når disse er identifisert og løsningsforslag er implementert bør symptomene som var konsekvens av problemer opphøre. Dersom de ikke opphører, betyr dette at det ikke var rotårsaken som ble behandlet, eller at det er flere rotårsaker som er i stand til å gi symptomer.

Denne rapporten er en del av vårt bachelorprosjekt hvor vi ser på `rotårsaks-analyse` i bruk innen informasjonssikkerhet.

Struktur
Strukturen i dokumentet er delt opp i syv overordnede steg. Hvert steg er en hovedoperasjon av rotårsaksanalysen. I hvert steg er det anvendt en eller flere metodikker som vi kaller verktøy. Vi vil så ha underkapitler hvor vi beskriver ønsket utbytte. Dette gjør vi utifra forventningene vi har til verktøyet etter å ha studert Root Cause Analysis Simplified Tools and Techniques Second Edition [1] som vi ser på som hoved litteraturen, The Root Cause Analysis Handbook[2] og Root Cause Analysis The Core of Problem Solving and Corrective Action [3]. Gjennomførelsen blir så dokumentert i neste underkapittel. Deretter diskuterer vi om verktøyet ga den nytten vi ønsket og til slutt diskuterer vi om det var noe informasjon om verktøyet vi kunne ønsket å ta med oss.

Oppgavebeskrivelse
Vi fulgte boken systematisk i vår anvendelse av verktøy på dette caset. Her brukte vi kapittel 10: "How to select the right tool" fra boken Root Cause Analysis Simplified Tools and Techniques Second Edition[1] i større grad enn det vi har gjort på de andre casene. I dette caset vi fikk av slettmeg så vi på et DDOS angrep som inntraff 7.Mai 2015. Her anvendte vi verktøy for å se på hva som var årsaken til at slettmeg ble utilgjengelig under angrepet. Dette er muligens kjent for slettmeg men det ga oss grunnlag for å gjøre studier på verktøyene og levere resultat. Slettmeg kan forvente resultater på kunnskap om verktøyene vi forsøkte i caset. Vi diskuterte erfaringer vi satt igjen med etter arbeidet var gjort og håper at slettmeg vil kunne finne disse anvendbare. Dette vil inkludere struktur på utførelsen av verktøy og muligens fallgruver. Vi så kun på angrepet som traff 7.Mai 2015 og på beskyttelsen som eksisterte denne datoen.
Konsekvensene av DDoS angrepet var at alle nettsidene til NorSIS samt slettmeg.no, sikkert.no og idyveri.info var utilgjengelige fra 7.Mai frem til 8.Mai

Målet med studien er å validere etablerte rotårsaksanalyse (RCA) verktøy for informasjonssikkerhet.

Hovedpunktene i dokumentet følger utførelsen i vår rotårsaksanalyse gjennom sitt naturlige løp med sterke likheter til systemutvikklingsmodellen Fossefall, startende med problemforståelse og ender med løsnings implementasjon. Hvert kapittel begynner med en introduksjon til selve steget i analysen hvor vi forklarer hva det går ut på.

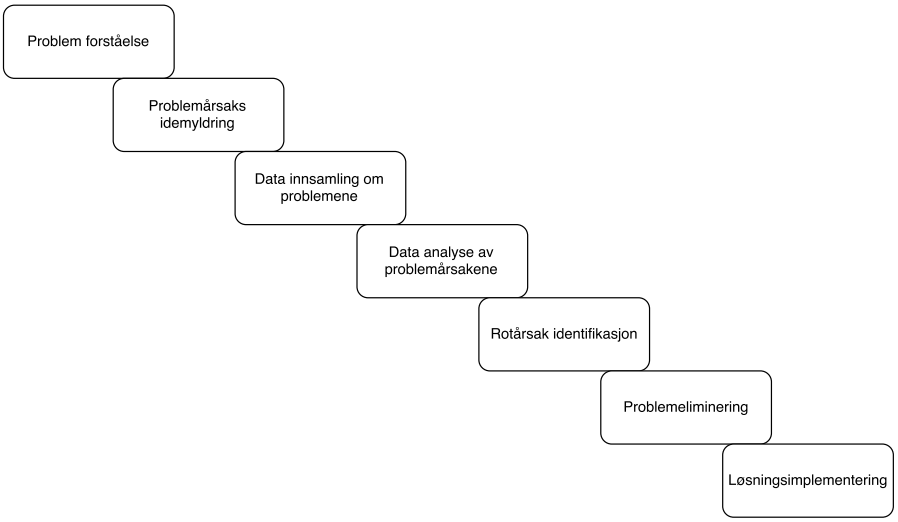


Figure 1: Waterfall

Liste over anvendte verktøy:

1. I problemforståelse ble det brukt Swim Lande Flowchart, Critical Incident og Performance Matrix.
2. I problemårsaks idemyldring ble det brukt Brainstorming.
3. I problemårsaks datainnsamling ble det brukt Check Sheet.
4. I problemårsaks data analyse ble det brukt Affinity Diagram.
5. Under rotårsaks identifisering ble det brukt diskusjon.
6. Under rotårsaks eliminering ble det brukt Systematic Inventive Thinking (SIT).
7. I løsnings implementering ble det henvist til Tree Diagram og Spider Chart.

1.1 Begrensninger

Under datainnsamling hadde vi ikke tilgang til logger. Derimot hadde vi tilgang til anmeldelsen som ble analysert i kapittel 2 Problemforståelse. Det var utført møter med veileder som ble gjennomført i forbindelse problemforståelsen og datainnsamlings kapittelet. Slettmeg har fortalt oss at de ønsker at vi skal i en stor grad se bort i fra tekniske aspekter som hvordan å unngå DDOS fra et teknisk synspunkt og hvilke type DDOS det var. Vi forsøkte å se om det å gjøre rotårsaks analyse kan hjelpe slettmeg med å finne en rotårsak de selv ikke så. Vi så også på om løsningsforslagene som er implementert til den dags dato svarer på alle problemene eller om noen problemer gjenstår i diskusjons kapittelet.

2 Problemforståelse

Verktøyene i problemforståelsen er ment for å gi en bedre forståelse på selve oppgaven og på hvilke aspekter i saken man burde titte nærmere på. Før vi startet med dette caset hadde vi en samtale med Vidar Sandland om hendelsesforløpet og fikk en kopi av anmeldelsen som ble levert til Gjøvik politikammer. Her er det god tidslinje av forløpet noe som gir oss en mulighet å bruke verktøyet flowchart(vi valgte å lage en swim lane flowchart).

2.1 Swim Lane Flowchart

Swim lane flowchart er et visuelt verktøy som brukes i flytskjemaer. Swim lane flowchart skiller seg fra andre flowcharts med at prosesser og beslutninger er gruppert visuelt ved å plassere dem i baner(lanes). Parallelle linjer deler diagrammet i baner, med ett kjørefelt for hver person, gruppe eller delprosess. Lanes er merket for å vise hvordan diagrammet er organisert. Swim lane kan ordnes enten horisontalt eller vertikalt.

Ønsket utbytte av Swim Lane flowchart verktøy

Det vi ønsker som utbytte er en tydelig visning av flyten gjennom utførelser og hendelser. Forhåpentligvis kan det vise veier av flyt som ikke var synlig uten grafisk fremtstilling. Ønsket utbytte er å få en økt detaljforståelse og avdekke forbindelser mellom elementene vi ikke like lett kunne oppdaget.

Gjennomførelse av verktøy

Vi startet med å tegne opp et Swim Lane flowchart. Her ble anmeldelsen av tjenestenektangrepet fra NorSIS brukt til utførelsen av Swim Lane flowchart. Med dette ønsket vi å få en oversikt over hendelsesforløpet via en grafisk fremstilling som vist i figur 2. Ønsket utbytte var å få en økt detaljforståelse for å kunne avdekke forbindelser mellom elementene vi ellers ikke ville oppdaget.

Elementene i Swim Lane flowchart

Her følger en beskrivelse av elementene i Fig: 2.

7 Mai 2015

1. *kl.14:30* NorSIS varsles via ekstern tjeneste om at NorSIS' nettsier er utilgjengelige.

2. *kl.15:45* NorSIS kontakter tjenesteleverandøren sin, og blir informert om at de jobber med saken.

3. *kl.16:16* NorSIS blir kontaktet av sin tjenesteleverandør, som informerer at det er snakk om et tjenestenektangrep (DDoS)

4. *kl.19:50* NorSIS blir kontaktet av sin tjenesteleverandør som forklarer at NorSIS' nettsider mottar kontinuerlig mellom 40 og 60000 forespørsler fra utenlandske IP-addresser, og kneler som følge av overbelastning. Det ble forsøkt å sperre for utenlands trafikk, men grunnet utfordringer hos tjenesteleverandørs nett-leverandør lot ikke dette seg gjøre.

   Det ble da forsøkt å bytte IP-adresse på NorSIS' webserver og oppdatere DNS på domenet norsis.no. Dette fungerte i 15-20 minutter.

5. *Ettermiddag/kveld* NorSIS informerer NorCERT og TSOC om tjenestenektangrepet. NorCERT får også oversendt loggene fra angrepet.

8 Mai 2015

1. *kl.08:00* Alle NorSIS' nettsider fortsatt utilgjengelige.
2. *kl.08:10* Alle nettsidene blir tilgjengelige igjen
3. *kl.10:15* Angrepet starter på nytt, med det resultat at alle nettsidene igjen blir utilgjengelige.
4. *kl.12:24* Tjenesteleverandør informerer om at de nå blokkerer trafikk fra utlandet, og nettsidene blir gradvis tilgjengelige for norske og skandinaviske besøkende
5. *kl.12:30* Politiet på Gjøvik blir kontaktet for bistand i saken.

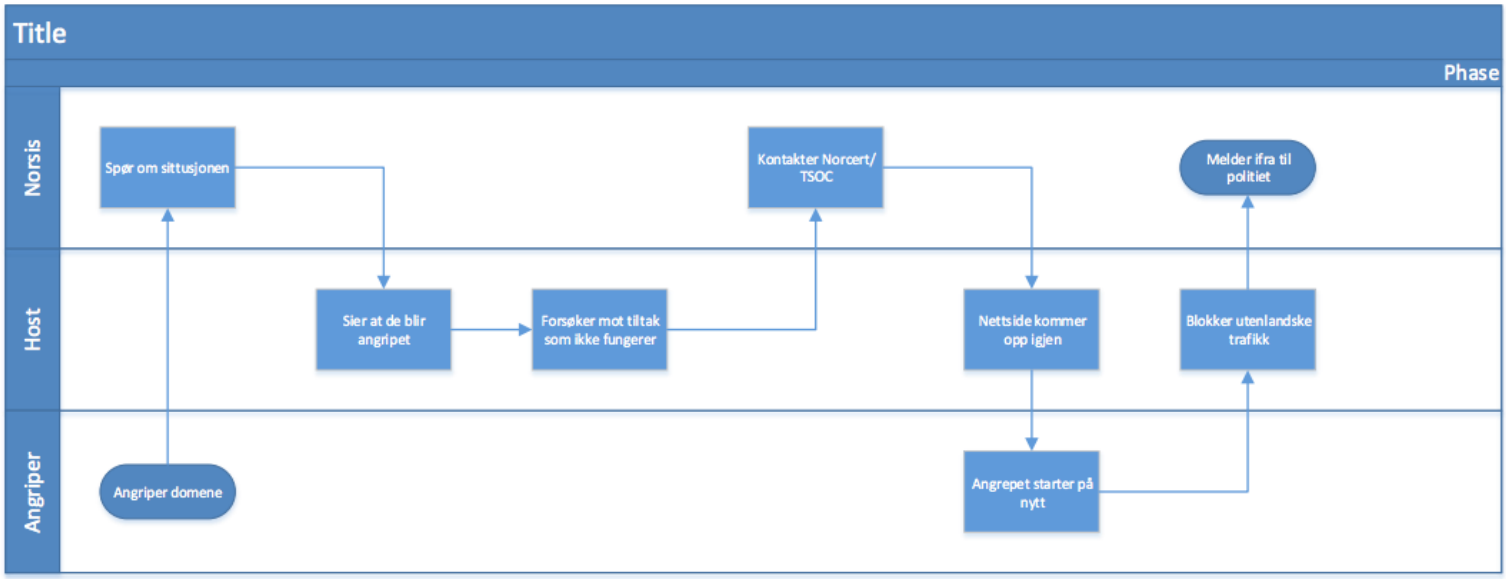


Figure 2: Swim lane av hendelsesforløpet

2.1.1 Konklusjon av verktøyet

Vi opplevde at verktøyet ga et godt visuelt bilde over flyten i hendelsesforløpet. Det er raskt å utføre dersom alle dataene som skal anvendes er tilgjengelig. Hver aktør kan plasseres i en egen lane/bane som vil gi informasjon om når aktøren ble påvirket av en hendelse eller aktivt var årsak til en hendelse.

2.2 Critical Incident

For å forsikre oss om at vi forstod hva som virkelig lagde mest problemer var det viktig å høre hva slettmeg selv mente om akkurat dette.

2.2.1 Ønsket utbytte

Forstå hvilke aspekter av problemet som må bli løst, og forstå innholdet av problemet og dets konsekvenser. Dette dekkes av formålsbeskrivelsen av verktøyet i RCA Simplified Tools and Techniques[1] side 36.

2.2.2 Gjennomførelse

Verktøyet er beskrevet i 5 steg i hovedlitteraturen. Steg 1 forteller at nøkkelpersoner skal delta. Steg 2 forteller videre at deltagerene skal i en sekvens skrive ned på lapper hva som var vanskeligest å behandle samt hva som var de største problemene. Grunnet begrenset ressurser lagde vi heller noen spørsmål som vi stilte dem og mottok verbale svar på. I steg 3 skal svarene på lappene analyseres utifra frekvens. Det var ikke mulig å telle frekvens. Steg 4 er å gi en grafisk fremstilling, hvor vi valgte å fremstille de tre punktene i liste format. Steg 5 er å anvende de hendelsene med høyest frekvens videre i analysen. Vi tar derfor med oss informasjonen om hva som var viktigst for slettmeg videre i vår analyse.

Spørsmålene
Spørsmålene samt svarene vi fikk av slettmeg.

1. Hva er det mest negative ved at siden deres er nede?
2. Hvordan beskriver dere problemet med å forhindre DDOS mot slettmeg.no? (Teknisk og prioriterings basert).
3. Hvor mange ganger utsettes dere for DDOS angrep i året?

Slettmeg forteller at det som var det mest problematiske med at nettsiden deres var nede var at folk ikke fikk tak i selvhjelp. Det var ved den datoen ikke tilstrekkelige mottiltak mot DDOS. De kunne ikke helt svare på hvor mange ganger de ble utsatt for DDOS i løpet av et år da host ikke alltid fortalte om det, men heller automatisk utførte rutiner med blokkering av IP'er fra utlandet. Disse rutinene var ikke tilstede under DDoS angrepet 7.Mai 2015.
Det største problemet med DDOS er derfor at folk ikke lengre har tilgang til selvhjelp siden som slettmeg tilbyr.

2.2.3 Konklusjon av verktøyet

Verktøyet ga oss informasjonen om hva som skapte mest problemer.

2.2.4 Hvilken informasjon om verktøyet kan vi ta med oss til senere bruk?

Vi var ikke i stand til å utføre verktøyet akkurat slik hvert steg var da vi ikke hadde mulighet til å samle alle som jobbet på slettmeg og gjennomføre gruppeaktiviteter. Derfor mener vi det er viktig at nøkkelpersoner kontaktes på forhånd. Dersom deltagerene ikke kan møte til samme tid, kan eventuelt spørsmålene sendes til dem, og svarene behandles av de som utfører rotårsaks analysen til slutt, noe som var umulig å gjennomføre for oss på grunn av tidsrestriksjoner.

2.3 Performance Matrix

Performance Matrices blir brukt til å illustrere nåværende ytelse og viktighet på samme tid. Dette hjelper med å komme frem til en oppfatning av prioritet. Performance Matrices brukes til å illustrere problemer eller årsaker i form av:

- Hvilken del av problemet er det viktigste å angripe?
- Hvilke problem, dersom fjernet, vil redusere flest symptomer?

De to punktene over stammer i fra Root Cause Analysis Simplified Tools and Techniques [1].

2.3.1 Ønsket utbytte

Vi ønsket å finne ut hva som var viktig for slettmeg og hvordan de mente at ting fungerte.

2.3.2 Gjennomførelse

Disse punktene ble utarbeidet i sammen med kontaktperson i slettmeg.

1. Evne til å hjelpe (oppetid (kapasitet til forespørsler)).
   (a) *(Importance)* Hvor viktig er oppetiden på nettsidene? Svar: 8
   (b) *(Performance)* Hvor god er oppetiden på nettsidene? Svar: 7
2. Kontakt muligheter.
   (a) *(Importance)* Hvor viktige for dere er det at klienter får lett kontakt med dere via tlf. og mail eller sosiale medier? Svar: 5
   (b) *(Performance)* Hvor godt fungerer kontaktmulighetene til dere via tlf. og mail eller sosiale medier? Svar: 8
3. Responstid.
   (a) *(Importance)* Hvor viktig er responstid? Svar: 8

(b) *(Performance)* Hvordan faktiske responstiden er? Svar: 4

4. Selvhjelp side.

   (a) *(Importance)* Hvor viktig for dere er det at dere kan tilby selvhjelp? Svar: 8

   (b) *(Performance)* Hvor godt tilgjengelig er selvhjelpen dere tilbyr? Svar: 6

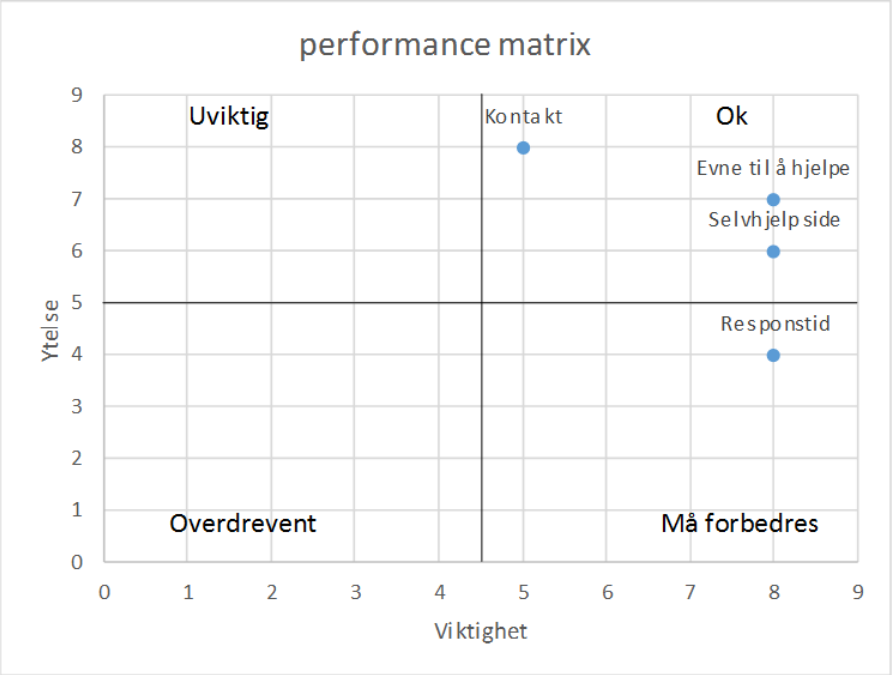


Figure 3: Performance matrix

2.3.3 Konklusjon av verktøyet

Verktøyet gir et godt innblikk i hva slettmeg ser på som viktig, og viste at responstiden er høyt prioritert, og vi ble fortalt at antallet henvendelser var stort og at det kan være vanskelig å henvende seg til alle innen kort tid og samtidig gi god hjelp. Deres selvhjelp og dermed også nettside oppetid rangeres høyt da det er et sterkt ønske fra slettmeg at selvhjelpen skal bidra med at flesteparten som oppsøker hjelp er i stand til å få løst sine problemer via selvhjelp.

2.3.4 Hvilken informasjon om verktøyet kan vi ta med oss til senere bruk?

Vi merket her hvor stor viktigheten av tydelig kommunikasjon fra vår side var. Med kommunikasjon menes det vår evne til å forklare hva vi var ute etter i en oversiktlig og kronologisk rekkefølge som var tydelig. Hvis vi hadde vert bedre på kommunikasjonen våres, hadde verktøyet blitt lettere og raskere å gjennomføre.

3 Problemårsaks idemyldring

Introduksjon
Problemårsaks idemyldring som er steg 3 i rotårsaks analysen skal gi dypere problemforståelse. Her studeres antatte årsaker til problemet som blir samlet strukturert og listet opp. Formål med steg 3 i analysen er at gruppen som analyserer har en samlet oversikt med konsensus på hva som blir sett på som problemårsaker.

3.1 Brainstorming

Her brukte vi ustrukturert brainstorming. Her følger vi verktøyet slik som beskrevet i Root Cause Analysis Simplified Tools and Techniques [1] side 46.

3.1.1 Ønsket utbytte

Ønsket utbytte er en liste med antatte konsekvenser og årsaker til problemet eller de problemer som bygger opp til de synlige symptomene.

3.1.2 Gjennomførelse

Gruppen anvender en tavle til å skrive ned ideene på.

Steg 1
Her skal problemet defineres. Problemet er "Selvhjelp ikke tilgjengelig".

Steg 2 til 5
Identifiserte mulige konsekvenser av problemet og skrev de ned:

1. Mindre tilgjengelighet for klienter/brukere av tjenesten.
2. Nedsatt rykte.
3. Dersom slettmeg ikke er i stand til å drifte selvhjelp vil de ha økonomiske problemer.

Det ble generert en liste med mulige årsaker til problemet, og denne blir presentert i steg 6 hvor den er gruppert etter viktighet.

Med punktet "slettmeg setter seg i kryss ild mellom individers problemsituasjoner" mente vi at det kan eksistere muligheter for at noen klienter kan føle frustrasjon over situasjonen sin og oppleve motivasjon for opprørsk holdning. Utfall av dette kan være DDoS mot slettmeg.

Punktet "angriperene kan være utenfor norsk jord" ble laget på grunn av at datatrafikken kom fra utenlandske adresser. Det er vanskelig å avgjøre hvor angriperene faktisk er fra og hvem de er. Det å skulle straffeforfølge dem kan

bli komplisert.

Med punktet "ingen tydelig avskrekking" mente vi at personer som har motivasjon for å utføre DDoS angrep mot slettmeg ikke utsetter seg for en stor risiko da politiet får vanskeligheter med å avdekke hvor de er og hvem de er. Det kan også være at det ikke er en tydelig konsekvens for angriperene.

Steg 6
Steget går ut på å gruppere elementene funnet i steg 2 til 5.
Det ble valgt å gruppere etter viktighet.
Gruppering av konsekvens:
Punktene i konsekvens beholder rekkefølgen de er skrevet i.
Gruppering av mulige årsaker til problemet:

1. Tjeneste leverandør hadde ingen testet plan for behandling av situasjonen.
2. Ikke gode nok kunnskaper hos de som hoster om hvordan å behandle situasjonen.
3. slettmeg setter seg i kryss ild mellom individers problemsituasjoner.
4. Angriperene kan være utenfor norsk jord.
5. Ingen tydelig avskrekking for DDoS angrep på siden.
6. DDoS av slettmeg.no ikke vurdert kritisk nok.
7. Manglende/utilstrekkelig risikovurdering.
8. For lite ressurser brukt på server-kraft.

Problemområder som kan forbedres er beskrevet i performance matrix, hvor punkter på "performance" kan økes til ønskede verdier.

3.1.3 Konklusjon av verktøyet

Verktøyet ga rask oversikt over elementer av problemet samtidig som grupepringer viser viktigheten til elementene raskt da leseren starter med å lese de første punktene som er i lister. Gruppen blir samtstemt da alle får delta i idemyldringen og hvert medlem får bedre forståelse av problemet.

4 Problemårsaks-data-innsamling og analyse

I denne seksjonen blir datainnsamling gjennomført og analyse av de innsamlede dataene gjort.

Når slettmeg var under angrep var det ikke tilstede noen DDOS beskyttelse, og det var heller ikke gjennomført noen trening på hendelseshåndtering av slike situasjoner.

Slettmeg har innført DDOS beskyttelse, slik at vi nå antar at alle de tekniske aspektene ved slike angrep blir tatt hånd om av de som står bak denne tjenesten. Dette innebærer at tjeneren av DDOS beskyttelsen har kunnskaper om hvordan å behandle en slik situasjon og at slettmeg blir informert dersom siden allikevel er nede slik at slettmeg så kan informere sine brukere. I check sheet verktøyet blir det sett på situasjonen slik den var under angrepet, og hvordan situasjonen er i ettertid.

4.1 Check sheet

Verktøyet brukes til å registrere frekvenser på hvor ofte problemer inntreffer [1]. Da det ble bestemt at i dette caset skulle litteraturen strengt etterfølges, ble flowchartene i tool selection seksjonen i Root Cause Analysis Simplified Tools nd Techniques side 174 til 186 [1] anvendt til verktøy valg. Det var ikke gjennomførbart å tegne noen grafiske chacksheets i vårt tilfelle.

4.1.1 Ønsket utbytte

Ønskede utbytte er å oppnå en prioritering eller en rangering på elementene som skal analyseres. Eventuelt om dette er gjennomførbart. En del av det ønskede utbytte er å erfare verktøyet og evaluere dets tilpasning til situasjonen.

4.1.2 Gjennomførelse

En brainstorming fase ble anvendt til å generere problemer og problemsituasjoner som hendte under angrepet og i etterkant ved rapportering til myndigeter. Punktene ble diskutert med vår kontaktperson hos slettmeg. Vanskeligheten med å rangere problemene i listen ble løst med diskusjon av hvert punkt. Vi kan derfor fremstille våre data med en kvalitativ presentasjon fremfor en kvantitativ frekvens av hendelsene.

4.1.3 Resultater

Politiet kikket ikke på bevismateriale

Bevisene ble samlet inn i form av logger, og loggene ble deretter kryptert og gitt ett passord. NorSIS anmeldte så angrepet til politiet og sendte den krypterte filen med loggene og skrev at politiet kunne kontakte NorSIS for å

motta passordet til filen. Politiet kontaktet dem aldri for å få åpnet filen og henla saken.

Kontakt med tjenesteleverandør
slettmeg sin nettside leverandør hadde ingen prosedyrer på hvordan å håndtere situasjonen, og kontaktet sin nettleverandør som ikke umiddelbart kunne bistå. Tiden det tok for å opprette kontakt var relativt kort. NorSIS opplever det som et viktig aspekt av denne situasjonen at kontakt tiden er svært lav og at de selv får vite at det er problemer med tjenestene de blir levert.

Måtte finne ut hvordan de skulle håndtere situasjonen på stedet
Leverandør av web tjenestene var ikke trente på slike situasjoner, og kunne ikke håndtere den da angrepet inntraff. De kontaktet derfor sin nettverksleverandør og foreslo at de skulle blokkere trafikken som kom fra utenlandske adresser da angrepet ikke originerte i fra Norge. Nettverksleverandøren var heller ikke i stand til å øyeblikkelig etterfølge dette ønsket. NorSIS selv hadde ikke gjennomført noen øvelser på DDOS situasjoner da det ofte ikke er annet å gjøre enn å blokkere trafikk, vente angrepet ut og opprette en beskjed via en annen leverandør som forteller situasjonen til befolkningen, DDoS Proactive and Reactive measures [4] side 31.

Host fikk ikke blokkert utenlandsk trafikk øyeblikkelig
Host hadde ikke ordninger på plass for å stenge av nettverkstrafikk fra utlandet. Dermed måtte de kontakte ISP'en de brukte som også ikke hadde noe løsning på plass. Det gikk dermed unødvendig mye tid med på å få nettverkstrafikk fra utlandet stengt.

Skapte uante problemer for resten av organisasjonen
Angrepet på slettmeg var rettet mot domenet og ikke IP adressen. Trafikken slo ut alle web tjenester som NorSIS hadde.

Unødvendig mye ressurser gått bort på å behandle situasjonen
Angrepet førte også til at personer i NorSIS måtte omprioritere oppgavene sine og deres normale arbeid ble utsatt. Ansatte hos web host og ISP måtte også bruke tid av sine ansatte til å behandle situasjonen. Anmeldelsen som ble skrevet ble det satt av en halv dag til på en ansatt, slik at strukturen og fremgangsmåten kan anvendes på nytt ved liknende situasjoner og av andre enn NorSIS.

4.1.4 Konklusjon av verktøyet

Verktøyets krav om frekvens var ikke oppnåelig da måling av frekvens ikke var gjennomførbart på punktene vi kom frem til. Selv om vi prøvde å få det til som en check sheet ble gjennomførelsen tilsvarende en intervju. Dette var fordi det

var vanskelig å sette tall på frekvenser på enkelt hendelser. Dermed så stilte vi heller spørmål rundt problemene vi hadde listet. Vi fikk dermed i det minste noe å gå på, selv om det ikke var det vi hadde hadde sett for oss.

4.1.5 Hvilken informasjon om verktøyet kan vi ta med oss til senere bruk?

Vite at frekvens kan være svært vanskelig å måle i situasjoner som befinner seg i retroperspektiv.

4.2 Affinity diagram

I denne delen analyserte vi dataene som ble innhentet. Svært få verktøy passet vårt case. Derimot var det gjennomførbart å lete etter skjulte sammenhenger i dataene som ble samlet inn. Et affinity diagram ble forsøkt anvendt da dataene ikke var numeriske.

Et affinity diagram hjelper med å korrelere tilsynelatende urelaterte ideer, betingelser, betydninger og årsaker, slik at de kan kollektivt bli utforsket videre. Når man skal analysere kvalitative data så er affinity diagram nyttig da den grupperer data og funn av underliggende forhold som kobles sammen i grupper.

4.2.1 Ønsket utbytte

Lete etter skulte sammenhenger i dataene som ble samlet inn.

4.2.2 Gjennomførelse

Stegne i gjennomførelsen er hentet i fra Root Cause Analysis Simplified Tools and Techniques [1] side 111. Stegene fører gjennomgangen av verktøyet på en sekvensiell måte hvor vi beskrev hva som hovedsakelig skal gjøres på hvert at stegene..

Steg 1
Gruppen ble samlet og emnet ble skrevet på en tavle. Deretter ble elementer brainstormet. Dette steget er med på å initialisere prosessen med verktøyet.

Steg 2
Gruppen genererte punkter som ble plassert på tavlen i tilfeldig rekkefølge som omhandler årsaker til at noen velger å angripe slettmeg og punkter som kan være årsaker til at angrep ble gjennomførbart.

Årsaker til angrep.

1. Noen har noe imot slettmeg?

2. Noen utførte angrepet i et forsøk på selskryt?
3. Slettmeg ble brukt som forsøkskanin før et annet angrep.
4. Testet om det kom ut data hvis servere restartet: smokescreen.
5. Påføre omdømme tap.
6. Liten konsekvens for angriperen ved DDOS angrept.
7. Manglende avskrekking/deterrence.

Årsaker til gjennomførbarhet på engrep.

1. Norsis overlot ansvar til host.
2. Host ikke forberedt.
3. Host kunne ikke stenge av utenlandsk trafikk til å begynne med.
4. ISP kunne ikke stenge av utenlandsk trafikk til å begynne med.
5. Host og ISP måtte under problemets løp finne ut av hvordan å behandle situasjonen.

Steg 3, 4 og 5

Ideene generert i steg 2 ble gruppert for økt oversikt, som tilsvarer steg 3. En slik gruppering gjør at det blir lettere å tegne histogram på dataene skulle dette være ønsket hvis svært mange elementer er generert. Grunnet plassen det tar å notere ned stegene, ble steg 4 og 5 gjort sammen med steg 3. Steg 4 omhandler diskusjon av resultatet hittil, og tillater små endringer. Steg 5 omhandler navngiving til gruppene som er med på å fortelle konteksten til hele gruppen.

På grunn av størrelsen til diagrammet, har disse punktene blitt omformet:

"Host kunne ikke stenge av utenlandsk trafikk til å begynne med" er omformet til "Host manglet mulighet til å stenge av utenlandsk trafikk".

"ISP kunne ikke stenge av utenlandsk trafikk til å begynne med" er omformet til "ISP manglet mulighet til å stenge av utenlandsk trafikk".

"Host og ISP måtte under problemets løp finne ut av hvordan å behandle situasjonen" er omformet til "Host og ISP manglet plan".

Elementet "Norsis overlot ansvar til host" var ikke i stand til å passe gruppene, og er derfor ikke representert grafisk i affinity diagrammet.

1. Omdømme

(a) Noen utførte angrepet i et forsøk på selskryt?

(b) Påføre omdømme tap.

2. Test av kapasitet

   (a) Slettmeg ble brukt som forsøkskanin før et annet angrep.

   (b) Testet om det kom ut data hvis servere restartet: smokescreen.

3. Holdningsforebyggende

   (a) Liten konsekvens for angriperen ved DDOS angrept.

   (b) Manglende avskrekking/deterrence.

4. Forebyggende planlegging

   (a) Host ikke forberedt.

   (b) Host manglet mulighet til å stenge av utenlandsk trafikk.

   (c) ISP manglet mulighet til å stenge av utenlandsk trafikk.

   (d) Host og ISP måtte under problemets løp finne ut av hvordan å behandle situasjonen.

Steg 6

Tegning av det grafiske diagrammet.

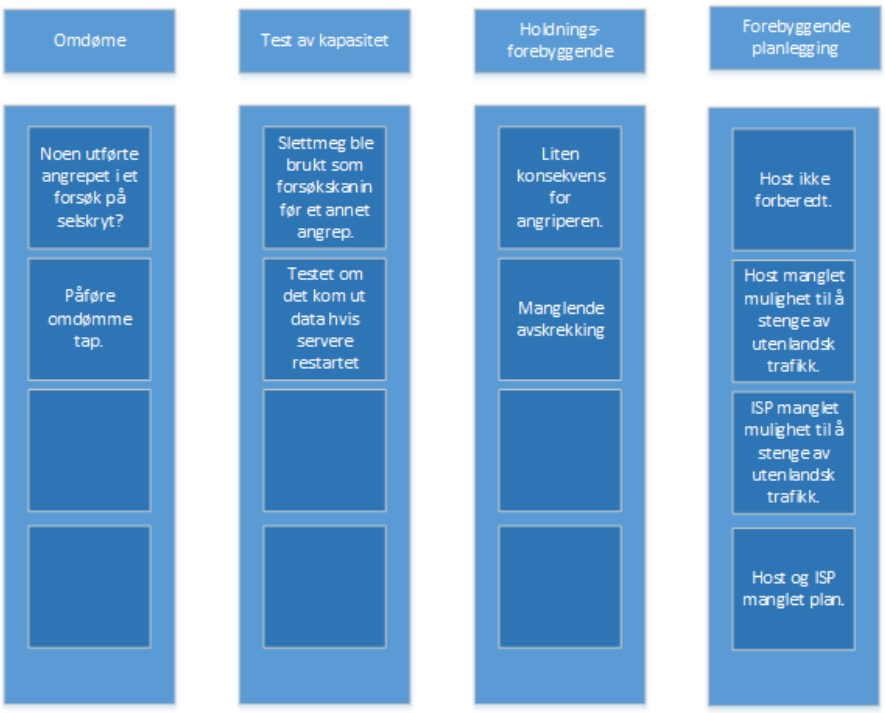


Figure 4: Affinity diagram som viser om det er skjulte sammenhenger

Steg 7

Gruppene blir sett på i sin helhet, og utifra den etterfølgende rotårsaksanalyse vil elementene bli tatt hensyn til utifra gruppene de er plassert i.

4.2.3 Konklusjon av verktøyet

Verktøyet i denne sammenhengen avslørte ikke skjulte sammenhenger, men det ga en tydelig oversikt for oss og forhåpentlig vis leserene av rapporten til analysen over komponenter til problemet og deres tilhørigheter og sammenheng.

4.2.4 Hvilken informasjon om verktøyet kan vi ta med oss til senere bruk?

Vi ønsker å ta med oss som videre kunnskap at gruppering av så få elementer ikke er nødvendig og derfor ikke gir en tilstrekkelig god kost-nytte effekt.

5 Rotårsaks identifisering

Da det ble bestemt at hovedlitteraturens flowcharts for forslag til verktøy valg skulle anvendes på hvert av de 7 rotårsaks analyse stegene, har dette vist seg å være vanskelig på rotårsaks identifiserings steget.

Vi konkluderte med at det ikke kunne eksistere bare en rotårsak. Hver rotårsak blir diskutert:

Nr 1, Angriperens motivasjon og intensjon
Angriperen er motivert til å utføre ett angrep av flere forskjellige årsaker. Noen av årsakene kan forekomme ut av arbeidet slettmeg gjør med sine klienter. Det kan også eksistere motivasjoner som ikke skyldes slettmeg sitt arbeid, og som er nevnt i analyse fasen i kapittel 4 som skryt. Skryt omhandler også hacktivister som er motivert av publisitet og berømmelse. Det kan ligge presitsje i å ta ned slettmeg.no som er under NorSIS og DDoS er et enkelt valg av verktøy da det er lett å gjennomføre og med riktige tiltak er det vanskelig å avsløre angriperen.

nr 2, Lav risiko Når det kommer til avskrekking og redusering i motivasjon hos angriper er det svært vanskelig å avgjøre hva som motiverer dem. Eksempler på motivasjon kan være ingen konsekvens, føler seg uretferdig behandlet eller ikke liker det slettmeg gjør og skryt.

nr 3, Lett å iverksette DDOS angrep er veldig lett å iverksette. Selv med liten kunnskap så kan du bruke verktøy som gjør mesteparten for deg, eller kjøpe tjenesten av noen. Det at såkalte "amplifikation attacks" er lett å gjenomføre medvirker til en skjev fordeling av styrke mellom angriper og de som beskytter mot angrepet.

Nr 4, Mangel på forberedelser
Mangel på forberedelse mot angrep. Host til slettmeg var ikke foreberedt på å behandle DDOS angrep. Selv med de beste forberedelsene, så kan angriperene komme på nye tekniker for å unngå forsvarsmetodikkene. Det er derfor viktig å være forberedt.

Nr 5, Mangel på kontroll
Mangel på kontroll over situasjonen. slettmeg delegerte bort ansvaret for situasjonen uten å kontrollere at hosten var i stand til å håndtere slike situasjoner.

Rotårsak nummer 1 er det ikke mye vi tror kan gjøres med da angriperenes motivasjon er uforutsigbar. Det kan være interessant i videre arbeid å forsøke å kartlegge motivasjoner for angrep. Rotårsak nummer 2 blir ikke behandlet her da NorSIS har valgt å outsource DDOS beskyttelse. Rotårsak nummer 3 blir tatt med videre i analysen.

5.1 Konklusjon på rotårsaks identifisering

Utifra flowchart på verktøy valg for rotårsaks identifisering, var ingen av alternativene passende. Derimot ble rotårsakene diskutert og argumentert for. Vi ser på dette som et funn.

6 Rotårsaks eliminering

I dette kapittelet går vi gjennom vårt løsningsforslag på problemet. Hvilke verktøy vi brukte og hvoran vi gjennomførte problemelimineringen. Verktøyet som brukes er beskrevet i boken på side 151 [1].

6.1 SIT

SIT står for Systematic Inventive Thinking og baserer seg på å undersøke et eller flere problemers komponenter. Alle komponentene skal så vurderes ved hjelp av de fem SIT prinsippene. Disse prinsippene er som følger:

1. *Attribute dependency*: vurder om en endring i komponenten vil føre til forbedring.
2. *Component control*: undersøk hvordan komponenten er forbundet med miljøet rundt seg.
3. *Replacement*: bytt ut noe i komponenten med noe fra komponentens omgivelse.
4. *Displacement*: vurder om komponten kan få økt ytelse ved at en del av komponenten fjernes.
5. *Division*: vurder om splittelse av en komponent eller et produkts attributter kan gi forbedring.

6.1.1 Ønsket utbytte

Kunnskap om hvilke problemårsaker fra rot årsaksidentifiseringen som trengs å implementere løsninger til. Ved å anvende SIT håper vi å finne kreative løsninger, noe verktøyet er kjent for å bidra til.

6.1.2 Gjennomførelse

Her blir stegene for gjennomførelsen beskrevet.

Steg 1
Her skal gruppen samles med nøkkelpersoner, helst 10 til 12. Dette er ikke gjennomførbart for vår tilfelle.

Steg 2
Problemet er: Mangel på kontroll. Her listes komponenter til problemet, og det er viktig å inkludere ideer om komponenter på dette steget selv om de virker irrelevante.

1. Ansvars person
2. Prosedyre

3. Leverandør (riktig ord?)
4. Kunnskap og erfaringer til leverandøren
5. Rykte/omdømme (ryktet leverandøren har på seg).
6. Kontrakt
7. Kommunikasjon mellom leverandør og klient

Steg 3

Hver komponent som er realistiske å behandle videre i analysen velges ut. Deretter anvendes de 5 SIT prinsippene på hver av komponentene som ble valgt. Flere av prinsippene vil vise seg at ikke er gjennomførbare på komponenten, og i våres tilfelle valgte vi å la de være blanke. Under utførelsen av et SIT prinsipp blir det beskrevet et forslag til forbedring utifra prinsippets formål.

Den første som ble valgt er "Ansvars person".
Attribute dependency:
Component control: Forsikkre at kontroll person er knyttet til miljøer med faglig kunnskap.
Replacement:
Displacement:
Division:

Prosedyre:
Attribute dependency: Ilegge større kontroll på de det kjøpes tjenester av.
Component control: Sammenlikne egne prosedyrer med andres.
Replacement:
Displacement:
Division:

Kontrakt:
Attribute dependency: Kontrakten bør beskrive tydelig tjenerens ansvarsområder.
Component control: Passe på at kontrakten tilsvarer miljøet den anvendes i. Replacement:
Displacement:
Division:

Steg 4 og 5

I steg 4 skal de ideene som virker best egnet til vidre arbeid velges ut. Her valgte vi Prosedyre og Kontrakt.
I steg 5 skal de utvalgte ideene utdypes og dersom det er mange av dem, velg ut de mest lovende komponentene og generer løsningsforslag.

Løsningsforslag

Prosedyre
Dersom en sammenlikner sine prosedyrer med andres kan man oppdage svakheter i sin egen og få nye ideer på hvordan problemer kan løses. Ved å undersøke tjeneste leverandøren nøye på forhånd kan en forsøke å redusere mulige problemsituasjoner i fremtiden.

Kontrakt
Dersom det er realistisk at kontrakten hadde holdt tjenesteleverandør ansvarlig, kunne det vert mulig for slettmeg å fått kompensasjon for tapt arbeidstid som ble påført av omorganisering av arbeidsoppgaver under og etter angrepet. Kontrakt kan også uttale at leverandøren måtte ha kunnskaper om hvordan slike situasjoner skulle behandles.

6.1.3 Konklusjon av verktøyet

Verktøyet hjalp oss med å gå systematisk igjennom situasjonen, og oppdage komponenter vi tidligere ikke hadde lagt merke til.

7 Løsnings implementasjon

Kapittelet baserer seg på å anvende ett verktøy for implementering av løsningsforslaget i fra kapittel 7 løsnings implementering. Et løsnings implementerings verktøy bør bidra med en strukturert gjennomførelse som deler oppgaven i deler slik at ikke oppgaven blir sett på som en stor og uoversiktlig operasjon.

7.1 Verktøy

Som beskrevet i introduksjons kapittelet ble det valgt å følge hovedlitteraturens flowcharts på valg av verktøy på dette caset. Flowcharten[1] på side 186 starter med å spør om løsning på problemet er funnet. Vi har presentert forslag om forbedring på prosedyre og kontrakt. Videre skal skal det bestemmes hvordan implementeringen skal organiseres. Løsnings implementasjons verktøyene som er tilgjengelig hjelper til med å stå for hvordan organiseringen skal være. Deretter er spørsmålet om det trengs et verktøy til å veilede, organisere og strukturere gjennomføringen. Dersom implementasjonen er stor eller uoversiktlig, blir det anbefalt å bruke et tre diagram.

Tre diagrammet baserer seg på at en liste med aktiviteter som skal utføres, og at disse aktivitetene grupperes i undergrupper med oppgaver som må utføres i sekvens. Når en så utfører løsningsforslaget vil en kunne bevege seg i fra nederst til venstre i treet og utføre en undergruppe av gangen.

Løsningsforslaget krever minimalt med personer og ressurser. Å anvende et tre diagram for løsningsimplementasjon ble anslått som unødvendig.

Da løsningsforslaget på prosedyren innebærer å sammenlikne med andres prosedyrer, finnes det et verktøy kalt Spider Chart. Dette verktøyet stammer i fra problemforståelse steget, som tilhører verktøysettet til steg 1 i fossefalls modellen som vi har anvendt. Verktøyet går ut på å sammenlikne ytelse med andres ytelse, eller for å se at andre har klart å løse et problem, som viser at det er gjennomførbart. Verktøyet gir også en grafisk fremstilling av sammenlikningen i et kiviat format. Vi har ikke tilgang til interne prosedyrer, og kan ikke gjennomføre en slik sammenlikning.

7.2 Konklusjon av implementasjon

Vår konklusjon er at løsningsforslaget ikke er komplisert nok til at et tre diagram kan anvendes.

8 Diskusjon og konklusjon

Dette caset er en del av vår bachelor oppgave og er til for å svare på ett av våres forskningsspørsmål: Hvordan fungerer RCA på en case med lite ressurser og lite tid?
Ressursene blir sett på som medlemmer i gruppen og datatilgjengelighet. Bachelor gruppen utførte dette caset med 2 av sine medlemmer, og dataene som var tilgjengelig var anmeldelsen til slettmeg og samtaler med kontaktperson i slettmeg.

Vi oppdaget ved å utføre SIT i rotårsaks elimineringen at rotårsaken "mangel på kontroll" kan diskuteres om er bygget opp under to andre årsaker, "prosedyre" og "kontrakt". Hvor igjen antatte mangler i prosedyre og krav i kontrakt kan diskuteres at skyldes "mangel på kontroll". Vi har gått utifra at "prosedyre" og "kontrakt" er komponenter til rotårsaken "mangel på kontroll". Vi ønsker å legge til at dersom "prosedyre" og "kontrakt" ble forstått som rotårsakene til "mangel på kontroll", ville det vert nødvendig å gått tilbake til steg 5 rotårsaks identifikasjon og anvendt verktøyet Five Whys.

8.1 Konklusjon

Rotårsakene vi kom frem til var angriperens motivasjon, mangel på forberedelser og mangel på kontroll.

Beskrivelse på rotårsaker
Angriperens motivasjoner kan innebære frustrasjon mot slettmegs arbeid, eller annet utenfor slettmegs kontroll som skryt. Det er vanskelig å avgjøre hva som motiverer angriperen, men at liten konsekvens for DDOS forsterker problemet.

Mangel på forberedelser var et aktuelt problem da ingen øvelse på håndtering av hendelse var utført i forkant. Selv med god forberedelse kan en ikke sikkre seg mot DDOS angrep.

Kontroll NorSIS delegerte bort ansvaret for situasjonen uten å kontrollere at hosten var i stand til å håndtere slike situasjoner.

Løsninger
Løsninger er hovedsakelig utenfor slettmegs kontroll da angriperens motivasjon er et hovedmoment. Dersom angriper har tilstrekkelig motivasjon kan de finne en måte å utføre et vellykket angrep på. De løsningsforslagene vi har kommet med baserer seg på prosedyre innad i slettmeg og kontrakt med tjeneste leverandør. Prosedyren dikterer prosessen på hvordan slettmeg bestemmer leverandør. Her menes det sjekk av leverandørs historikk, erfaring som

leverandør og kunnskap om hvordan å behandle kjente problemsituasjoner. Vi foreslår at kontrakter med tjeneste leverandører dikterer at leverandørene skal ha kunnskaper om håndtering av kjente problemsituasjoner og er i stand til å tilby en løsning, som for eksempel blokkering av IP ranges.

8.2 Diskusjon

Her har vi diskutert resultat i forhold til tid og data ressurser. Deretter diskutert resultat i forhold til hvilke rotårsaker vi har valgt å lage løsningsforslag til.

Denne analysen er en del av vårt bachelor prosjekt og baserer seg på ett av våres forskningsspørmål: Hvordan fungerer RCA på en case med lite ressurser og lite tid?
Det eksistert også limitasjoner på dataene vi kunne få tak i. Dette på grunn av at logger fra DDOS angrep innehold personidentifiserende data. Det er vanskelig å sette seg inn i angriperens situasjon og tankegang, men det er mulig å gjøre antagelser på hva som kan virke som motivasjon. Det kan derfor være lurt å ta i betraktning limitasjonene i forhold til våre resultater, og at dersom analysen hadde vert utført av nøkkelpersoner innad i organisasjonen som sitter på erfaringer med klienters tankegang og følelsessett ville resultatet kunne blitt et mer siktet på angriperen.

Da vi hadde liten tid, var det ikke mulighet til å ha flere kontaktpersoner innad i NorSIS, som kan føre til at noen sider av problemer og noen nyanser av dataene ikke blir synlige for oss.

Det var problematikk i å få verktøy til å passe situasjonene vi sto ovenfor. I noen tilfeller eksisterte det ikke et verktøy i vår litteratur som kunne behandle situasjonen. I de tilfeller ble diskusjon anvendt til å løse problemet. Vi ser på slike situasjoner som funn og mener at dette åpner for videre arbeid med å gjøre rotårsaksanalyse mer anvendbar innen IT.

Med de tiltak som eksisterte, mener vi at slettmeg var sårbar for DDOS angrep. Vi forstår det slik at situasjonen ikke var høyt prioritert på grunn av kost-nytte effekt. I nyere tid har det blitt innført beskyttelse mot slike angrep. Denne beskyttelsen er på et rent teknisk nivå og gjør sannsynligheten for et vellykket angrep mindre men stopper ikke folk i å forsøke å angripe.

8.3 Tidsbruk

Den totale tiden brukt på case 3 er omtrent 75 timer per person (150 timer).

Tabellen under viser bare den konsentrerte tiden brukt på selve verktøyene iløpet av vellykket forsøk, men inkluderer ikke tiden brukt på diskusjon av valg og testing av verktøy og rapport skriving.

Table 1: Loggføring

Loggføring av tidsbruk på verktøyene		
Fase	**Verktøy**	**Tidsbruk t=timer**
Problemforståelse	Swimlane Flowchart	1,20 timer
Problemforståelse	Critical Incident	2.73 timer
Problemforståelse	Performance Matrix	3,05 timer
Problemårsaksidemyldring	Brainstorming	1.53 timer
Problemårsaks datainnsamling	Check Sheets	9,53 timer
Problemårsaks dataanalyse	Affinity Diagram	1.85 timer
Rotårsaks identifisering	Diskusjon av rotårsaker	2 timer
Rotårsaks eliminering	SIT	1.1 timer
Løsningsimplementering	Beskrivelse av alternativer	2,05 timer
		Total: 25,05

Check Sheets var problematisk da verktøyet ikke var godt egnet, men det eneste alternativet utifra verktøy utvalgs flowchart fra hovedlitteraturen side 178 [1], og mye tid ble brukt på å forsøke å anvende det.

References

[1] Andersen, B. & Fagerhaug, T. 2006. *Root cause analysis: Simplified tools and techniques.* ASQ Quality Press, second edition.

[2] Ammerman, M. 1998. *The root cause analysis handbook: A simplified approach to identifying, correcting, and reporting workplace errors.* Steiner-Books, first edition.

[3] Okes, D. 2009. *Root cause analysis: The core of problem solving and corrective action.* ASQ Quality Press, first edition.

[4] Impe, K. V. 15 October 2015. Ddos proactive and reactive measures. [Online; accessed 09-MAI-2016]. URL: https://www.cert.be/files/DDoS-proactive-reactive.pdf.