UNIVERSITETET I OSLO

Institutt for informatikk

Hackere / Crackere

Masteroppgave

(60 studiepoeng)

Ørjan Nordvik

1. februar 2006

Sammendrag

Denne masteroppgaven går kort sagt ut på å finne ut hva som karakteriserer *hackere* og *crackere*. Det er viktig å klargjøre så tidlig som mulig i oppgaven hvordan jeg tolker disse to termene. I kapittel tre vil jeg gå grundig igjennom dette, men først vil jeg her kort oppsummere hvordan jeg kommer til å bruke begrepene hacker og cracker. Hackere er dataeksperter som holder seg på den riktige siden av loven, mens crackere er de som bryter loven.

For å kunne diskutere de sentrale begrepene har jeg gjort en litteraturstudie som resulterte i kapittel tre, samt en empirisk undersøkelse ved å intervjue dataeksperter, hackere og crackere. Det er den empiriske undersøkelsen som består av en rekke kvalitative intervjuer, og data fra sekundærlitteraturen som danner datagrunnlaget i denne oppgaven.

Hackere og crackere er etter min mening ikke homogene grupper som lett lar seg beskrive med få setninger. Det finnes et utall av motiver som ligger bak deres handlinger enten de er hacker eller cracker. Måten de arbeider på avhenger ofte av hvilket ferdighetsnivå de har. Det klassiske bilde av hackere som kvisete, coladrikkende fjortisser med tykke briller er en myte. Hackere og crackere finnes i alle samfunnslag og er like gjerne 30 som 15 år.

Forord

Denne masteroppgaven inngår som en del av mastergraden min ved Institutt for Informatikk, Universitetet i Oslo våren 2006. Området for forskningen er innen Informasjonssystemer oppgaven fokuserer på karakteristikker av hackere og crackere. Oppgaven er av «lang» type og gir 60 studiepoeng.

Jeg vil veldig gjerne rette en stor takk til veilederen min Gisle Hannemyr for konstruktiv og god veiledning. En stor takk går også til alle jeg har intervjuet og ellers alle andre som har bidratt med hjelp til denne oppgaven.

Oslo, 1. februar 2006

Ørjan Nordvik

Innhold

Figurer

1. Introduksjon

Samfunnet blir stadig mer avhengige av IKT-systemer (Informasjons- og kommunikasjonsteknologi) for å fungere, noe som også kan øke samfunnets sårbarhet. I dagens samfunn med stadig utvikling av ny teknologi, er det viktig å ta datasikkerheten på alvor. Det finnes i dag godt over 350 millioner vertsmaskiner tilknyttet Internett og dette tallet vokser raskt (Internet Systems Consoritum 2005). Ikke bare kobles det nye maskiner på nettet, men i tiden fremover vil vi se at også biler, kjøleskap og andre innretninger i hjemmet kobler seg på Internett.

Jeg vil begynne denne masteroppgaven med å referere til Nærings- og handelsdepartementet sin rapport «Samfunnets sårbarhet som følge av avhengighet til IT» fra år 2000 (Nærings- og handelsdepartementet 2000). Den sier at informasjons- og kommunikasjonsteknologien har gitt mennesket store muligheter, gitt økonomisk vekst og nye kanaler for informasjon. Men det er ikke bare positive sider med den nye teknologien, den kan også medføre ulemper. Problemet er at dagens økonomi, og samfunn generelt, er blitt avhengig av teknologien for å kunne fungere. Teknologien er blitt en integrert del av systemene vi omgir oss med og som er med på å sikre vår velferd. Omfattende svikt i IKT-systemer og infrastruktur kan nå forstyrre vitale samfunnsfunksjoner på en måte som få av oss kan forutse.

Som rapporten sier lever vi i et sårbart samfunn. Utviklingen av ny teknologi går fort og det er ikke alltid like lett å følge med. Men hvordan kan vi sikre

systemene våre mot uønskede hendelser? Når det snakkes om informasjonssikkerhet og sikring av systemer dukker ord som hackere og crackere opp. Det er disse menneskene denne masteroppgaven handler om. Hackere og crackere blir grundig forklart i kapittel tre hvor jeg vil presentere teori.

1.1 Problemstilling

Jeg ønsker å gjøre nærmere undersøkelser av hva som karakteriserer hackere og crackere. Som en del av dette vil jeg også prøve å finne motivasjoner til denne typen aktivitet, samt metodene de benytter.

Min innfallsvinkel til dette emnet er formulert som følgende enkle problemstilling:

Hva karakteriserer hackere og crackere og hva er deres motivasjon og metoder?

I kapittel tre vil jeg gjøre rede for hva jeg mener med ordene *hacker og cracker* i tillegg til andre definisjoner som jeg finner relevante for oppgaven. Målsetningen med oppgaven er, ved hjelp av kvalitative forskningsmetoder, å finne frem til konklusjoner på min problemstilling. Svarene jeg kommer frem til er basert på min datainnsamling og sekundærlitteratur.

1.2 Motivasjon og bakgrunn

Min motivasjon for å velge å skrive en masteroppgave om hackere og crackere, begrunnes med den økende interessen for sikring av datasystemer. Oftere og oftere hører man i media om «hackerangrep» og «svindelforsøk», og om dataeksperten som oppfordrer oss til å installere antivirusprogrammer, brannmurer og å oppdatere operativsystemene. Det finnes noe «mystisk» over hackerbegrepet som fascinerer meg og som jeg ønsker å finne mer ut av. Min nysgjerrige side iver etter å finne ut hvem som står bak crackerangrep, hvorfor de bedriver dette og ikke minst hvordan de får det til.

1.3 Avgrensing

Under arbeidet med denne masteroppgaven har jeg vært nødt til å foreta en rekke valg, for ikke å gape over for mye. Jeg vil av den grunn ikke gå i dybden på hvilke teknikker som benyttes eller hvordan personer teknisk kompromitterer et system. Det som jeg heller skal legge vekt på er hvorfor personer ønsker å gjøre dette.

Jeg har av praktiske grunner kun snakket med norske informanter rett og slett fordi de er lettere tilgjengelig. Det er lettere å intervjue informanter som befinner seg i samme geografiske område som en selv. Det blir selvfølgelig litt annerledes når man snakker med informanter på nettet, men jeg har konsekvent snakket med nordmenn og for eksempel kun holdt meg på IRC-kanaler der jeg vet det befinner seg mange fra Norge.

1.4 Organisering av oppgaven

Denne oppgaven består av syv kapitler i tillegg til referanser og vedlegg som kommer helt til slutt i oppgaven.

Kapittel 1 – Introduksjon

Dette kapitlet forklarer hva oppgaven omhandler. Problemstillingen og fokuset i oppgaven blir presentert, samt en forklaring bak motivasjonen for å velge denne problemstillingen.

Kapittel 2 – Informantene

I dette kapittelet presenterer jeg kort informantene som jeg har intervjuet, samt litt om sekundærlitteraturen jeg har benyttet meg av.

Kapittel 3 – Teorigjennomgang

Her presenteres teorien fra feltene jeg belyser i oppgaven. Kapittelet beskriver aktuell teori som danner grunnlaget for analysen i kapittel fem. I dette kapittelet gir jeg en kort historisk beskrivelse av hackerbegrepet, hvordan det oppstod og hvordan det har utviklet seg opp igjennom tiden. Her forklarer jeg også en del ord og uttrykk som er relevant videre i oppgaven.

Kapittel 4 - Metode

Metodekapittelet skal gi en oversikt over hvilke metoder jeg har benyttet for å samle inn data. Hvordan jeg har brukt de, hvorfor jeg har valgt akkurat disse metodene og hva som er styrkene og svakhetene ved dem.

Kapittel 5 – Analyse og diskusjon

I kapittel fem presenterer og diskuterer jeg de spørsmålene jeg stilte innledningsvis i problemdefineringen med bakgrunn i det teoretiske rammeverket og empirien jeg har presentert.

Kapittel 6 - Konklusjon

Kort konklusjon og oppsummering av de viktigste funnene.

Kapittel 7 – Erfaringer

I dette kapittelet presenterer jeg mine refleksjoner fra arbeidet med masteroppgaven. Hvilke tanker jeg har hatt når det gjelder kvalitative metoder, datainnsamling og analyse, samt erfaringene mine fra det å skrive masteroppgave. I slutten av dette kapittelet nevner jeg andre sider av problemstillingen som kunne være brukt i videre arbeid.

Referanser

Alfabetisk liste over referansene som er brukt.

Vedlegg

Intervjuavtaler og intervjuguide.

2. Informantene

I dette kapittelet vil jeg presentere informantene som jeg har intervjuet, samt si litt generelt om hvilke sekundærkilder jeg har brukt for å supplere primærdataene.

Mitt utgangspunkt for valg av informanter var at jeg ville ha samtaler med både hackere, crackere og ressurspersoner med god kjennskap til temaet som jeg har valgt. Intervjupersonene er delt inn i to utvalg, hvor utvalg A består av personer med kunnskap om hacking og cracking og utvalg B som består av (anonyme) crackere.

Når det gjelder min utvelgelse av informanter i utvalg A, så er dette offentlige personer som har stor kunnskap fra dette temaet ved at de enten har jobbet mot dette miljøet eller har skrevet om det. Personer som jeg har intervjuet er Stein Møllerhaug, Svein Willassen, Tron Øgrim, Christer Berg Johannesen, Christopher Birkeland, Are Garnåsjordet og Knut Borge. Siden utvalg B er anonymisert, vil jeg ikke gjengi personopplysninger fra dette utvalget. Disse personer har jeg kommet i kontakt med gjennom personer jeg kjenner, media og/eller IRC-miljøer. Dette utvalget består av tre personer som jeg har anonymisert under navnene Cracker#1, Cracker#2 og Cracker#3. Under følger en kort presentasjon av personene i utvalg A og B.

2.1 Presentasjon av informantene

2.1.1 Utvalg A

Stein Møllerhaug

Stein Møllerhaug er sikkerhetskonsulent i Symantec Security Services. Han begynte å jobbe med IT-sikkerhet i 1986 og har tidligere jobbet som sikkerhetssjef i Digital, og fulgte med over til Compaq etter at de ble kjøpt opp. Møllerhaug er en kjent figur innen IT og sikkerhet og er forfatter av flere teknothrillere med fokus på IT-kriminalitet.

Møllerhaug har bred kompetanse innen IT-sikkerhet og jobber med store virksomheter og organisasjoner. Han har ekspertise innen feltene informasjonssikkerhet, respons planer, sikkerhetsanalyser, trender og samfunn. Han har mange ganger vært foredragsholder på seminarer og han er også kjent for mange gjennom tv, radio og tidsskrifter.

Svein Y. Willassen[1]

Svein Y. Willassen er utdannet sivilingeniør i informasjonssikkerhet ved Norges Teknisk Naturvitenskapelige Universitet (NTNU). Etter studiene har Willassen jobbet som konsulent ved Initio IT-løsninger AS og som spesialetterforsker ved Datakrimteamet i ØKOKRIM. Her har han utført etterforskning av datainnbruddssaker, samt sikring og analyse av databevis i

[1] Info hentet fra http://www.willassen.no/

alle typer straffesaker. Han har også deltatt i oppbyggingen av Politiets Datakrimsenter. Gjennom jobben i ØKOKRIM har Willassen deltatt i internasjonalt arbeid, blant annet som medforfatter av Interpol Computer Crime Manual, samt utarbeidelse av retningslinjer for sikring og analyse av databevis i regi av International Organization on Computer Evidence.

Willassen har også vært ansatt i Ibas AS. Her ledet han oppbyggingen av det nye forretningsområdet sikring og analyse av databevis. Som dataetterforskningssjef var Willassen ansvarlig for et stort antall undersøkelser i sivile tvister i hele Europa, og bygget også opp kursvirksomhet i dataetterforskning. Willassen er i dag forsker ved NTNU der han gjennomfører det første forskningsprosjektet innen dataetterforskning i Norden.

Svein Y. Willassen er mye benyttet som foredragsholder, som konsulent og som sakkyndig i straffesaker og sivile saker der elektronisk informasjon står sentralt.

Tron Øgrim

Tron Øgrim er journalist, forfatter og foredragsholder. Yrkeskarrieren har blant annet bestått av ti år i industrien, forfatter og freelance journalist for diverse blader og tidskrifter. Øgrim har lang erfaring fra databransjen og skriver mye om data, samfunn og fremtiden.

Tron Øgrim har deltatt i debatten om data og samfunn siden 70-tallet, og har siden den gang skrevet artikler og spalter for datapressen. Han har blant annet vært fast spaltist for PCWorld i over 10 år. Siden 1990 har han vært mye brukt som foredragsholder for næringsliv, departementer, universiteter og høyskoler.

Christopher Birkeland

Christopher Birkeland er leder for Varslingssystemer for Digital Infrastruktur (VDI) som er et samarbeidsprosjekt mellom EOS-tjenestene (Forsvarets Etterretningstjeneste, Politiets Sikkerhetstjeneste, og Nasjonal Sikkerhetsmyndighet) og noen offentlige etater og private bedrifter som samlet presenterer samfunnskritisk infrastruktur.

Birkeland er utdannet ved NTNU med fagfelt innenfor industriell matematikk og numerikk. Han har også en doktorgrad i fysikk.

Christer Berg Johannesen

Christer Berg Johannesen driver datasikkerhetsselskapet LOOP i Bergen. LOOP leverer tjenester innenfor informasjons- og kommunikasjonssikkerhet, herunder kvalitetssikring, risikoanalyse og utarbeidelse av rutiner, tilgangskontroll og konstruksjon av tilhørende rapportverktøy. Johannessen omtaler seg selv som hacker.

Are Garnåsjordet

Are Garnåsjordet er leder for *Windows operativsystemgruppe* ved *Universitetets senter for Informasjonsteknologi.* Denne gruppen er blant annet ansvarlig for drift av Universitetets Windows-baserte infrastruktur innenfor områder som Active Directory, serverdrift, sikkerhet, klientdrift og printertjenester.

Knut Borge

Knut Borge er leder for *Seksjon for system- og applikasjonsdrift* og er ansatt ved *Universitetets senter for Informasjonsteknologi.* SAPP har ansvaret for drift, overvåking og utvikling av felles IT-tjenester på UIO. Seksjonen har ansvaret for drift av flere hundre tjenermaskiner og databaser, drift/utvikling av infrastruktur som for eksempel UIOs e-postsystem, brukerdatabase, gruppevare, katalogtjeneste, mellomvare og drift av sentrale webservere og applikasjoner.

2.1.2 Utvalg B

Cracker#1

Personen som klarte å komme seg inn i et norsk firma sitt billettsystem og skrev ut falske billetter. Skaffet seg tilgang til personopplysninger til passasjerene som skulle reise. Cracker#1 studerer Informatikk på universitetsnivå.

Cracker#2

Cracker#2 er medlem av en gruppe på fem personer som utvikler egne exploits/tools. Personen har tatt kontroll over et stort antall datamaskiner enten alene eller som i et samarbeid med de andre i gruppen. Cracker#2 er 25 år og student.

Cracker#3

Cracker som blant annet *uncappet*[2] kabelmodemer for å kunne nyte fordeler som bedre båndbredde. Personen har også brutt seg inn i datamaskiner og tatt kontroll over disse ved å utnytte kjente hull i operativsystemer. Bruker ferdiglagde exploits for å utnytte eksisterende svakheter.

2.2 Sekundærlitteratur

Jeg har hentet inn en del sekundærlitteratur da jeg ikke fikk tak i like mange informanter som jeg hadde ønsket. Jeg har blant annet brukt Jon Johansen, Richard Stallmann og Eugene Spafford som sekundærkilder, hvor jeg refererer til skriftlige kilder de selv har skrevet eller informasjon fra intervjuer av dem. Under vil jeg gjøre en kort presentasjon av dem.

[2] Uncapping, når det er snakk om kabelmodemer, er en rekke aktiviteter som ulovlig endrer innstillinger i kabelmodemet til en Internet-tjeneste-tilbyder (ISP). Som oftest for å øke båndbredden, endre identiteten til modemet eller andre konfigurerbare innstillinger som et DOCSIS modem kan tilby (Wikipedia 2005p).

Jon Lech Johansen

Jon Lech Johansen, «DVD-Jon», ble verdenskjent da han sammen med noen andre var med på å knekke koden som beskytter DVD-plater gjennom programmet DeCSS. I 2002 ble han stilt for retten siktet for brudd på både straffeloven og åndsverkloven ved å ha gjort det mulig å omgå denne sperren. Han ble imidlertid frifunnet av Oslo Tingrett. Dommen ble anket av Økokrim, men han ble på nytt frikjent på alle punkter av lagmannsretten i desember 2003. Økokrim valgte å ikke anke saken videre, og en lang rettssak var over for Johansen. Saken fikk stor oppmerksomhet og dataentusiaster over hele verden jublet over Jon Johansens seier i lagmannsretten.

Johansen er kjent for mer enn bare DeCSS programmet. Like før han skulle møte i retten i 2003 lanserte han programmet QTFairUse, som omgår DRM[3]-systemet på Apples musikkformat iTunes. Dette skapte selvfølgelig mer overskrifter, og Johansen viste med dette at DVD-saken ikke var en tilfeldighet, men at det var motivasjonen for å omgå kopisperrer som drev han.

DVD-Jon har vært i omtalt i media for flere saker. Sammen med to andre utviklet han programmet PyMusique som gjør det mulig å kjøpe musikk fra Apples musikknedlastningstjeneste, iTunes Music Store (iTMS), uten at den er utstyrt med kopisperre eller DRM. Dette var noe Apple ikke var særlig begeistret for.

[3] Digital Rights Management.

Johansen har lovet en lang kamp mot proprietære systemer og i den senere tid har han tatt sikte på å knekke kopisperren AACS som vil bli å finne på det nye DVD-formatet Blu-ray.

Richard Stallmann

Stallmann er en av de tidlige hackerne som på slutten av 70-tallet ville skape et helt sett av fri programvare som alle kunne bruke. I stedet for å kjøpe lukkede, proprietære programmer fra store selskaper som Microsoft, ønsket han at alle kunne bruke, videreutvikle og dele programmer fritt. Stallmann er initiativtakeren til GNU («GNU's Not Unix») som, foruten kjernen, er et komplett ikke-proprietært operativsystem. Linux er kjernen i operativsystemet og navnet blir da GNU/Linux. I tillegg startet han i 1985 FSF («Free Software Foundation») som er en organisasjon som har som visjon at all programvare skal være fri. Jeg vil komme tilbake til Richard Stallmann i kapittel 3.1.7.

Spafford

Dr. Eugene Spafford er professor i dataforskning ved Purdue University i Indiana i USA. Spafford er en erfaren og velkjent person innen datafaget. Han har jobbet som rådgiver og konsulent for store virksomheter som for eksempel Microsoft, Intel og FBI (Federal Bureau of Investigation), hvor han har delt sin kunnskap om datasikkerhet, nettkriminalitet og risikoer i forbindelse med datasystemer. Jeg har brukt artikkelen «Are Computer Hacker Break-ins Ethical?» (Spafford 1992) som en sekundærkilde.

3. Teorigjennomgang

I dette kapittelet vil jeg presentere en del teorier og begreper som danner rammeverket for min analyse av det empiriske materialet. Jeg vil først gi en gjennomgang av hackerbegrepet og dets historie, samt en oppklaring av forvirringen rundt begrepene hacker og cracker. Jeg vil så presentere hvordan jeg vil bruke termene i oppgaven, for deretter å gå igjennom forskjellige hacker- og crackervarianter og ulike metoder de bruker. Til slutt i dette kapittelet vil jeg si litt om hvilke trusler og trender som finnes på Internett i dag, samt presentere noen crackingteknikker.

3.1 Hackerbegrepet

Er en hacker en innesluttet ungdom som bare er ute etter å drive digitalt hærverk eller en godhjertet person som ønsker å avdekke sikkerhetsfeil? Som en innledning til oppgaven vil jeg først prøve å få rydde opp i en del begreper rundt dette temaet og forsøke å fremstille en historisk utvikling av dette begrepet fra ordets opprinnelse fram til i dag.

Hackerbegrepet kan oppfattes på flere måter og det er ikke i alle sammenhenger det er like lett å skjønne hva folk mener når de bruker dette ordet. Det finnes flere måter å forstå ordet på, noe som lett kan føre til forvirring. Forskjellige kilder definerer termen forskjellig og den sammenblandes ofte med crackerbegrepet. Opprinnelig ble ordet hacker brukt om en person som likte å finne ut alt om datamaskiner uten å forårsake skade,

i motsetning til en cracker. Men fra slutten av 80-tallet fikk hacker en ny betydning, hvor en hacker nå var en som brøt seg inn og saboterte datasystemer. Jeg vil nå prøve å definere hacker- og crackertermen og følge opp dette med å gi en beskrivelse av de forskjellige hackergenerasjonene.

3.1.1 Hvordan defineres hackere og crackere

Hvis vi ser på hvordan ordet brukes innen hackermiljøene så finnes det i *The Hacker's Dictionary: a guide to the world of computer wizard*s (Steele jr. et al. 1983) en rekke definisjoner. Dette er en bok basert på *The Jargon File* (Finkel 1975) som er en fil som samler ord og utrykk fra de tidlige hackermiljøene. Boken forteller at opprinnelig er en hacker en som lager møbler med øks, altså en person som skaper noe. Men i dataverdenen definerer *The Hacker's Dictionary* en hacker som en person som elsker å utforske detaljer i programmerbare systemer og som liker å utvide mulighetene i systemene, i motsetning til de fleste andre som bare ønsker å lære det mest nødvendige. Videre beskriver *The Hacker's Dictionary* en hacker som en som programmerer entusiastisk (nærmest besatt), eller en som liker å programmere fremfor å lære teorien om programmering. En hacker er også en person som er i stand til å verdsette *hack value* (ibid), som er motivasjon for å jobbe mot et unyttig mål. I tillegg er det en som kan programmere raskt og som er ekspert på et bestemt program/system.

Slik jeg ser det er disse definisjonene stort sett varianter over samme tema, hvor det gjennomgående forklares med at en hacker er en med særlig kunnskap om datateknologi, en ekspert. Men *The Hacker's Dictionary* tar også med en negativ beskrivelse hvor en hacker er en ondsinnet eller nysgjerrig

person som forsøker å skaffe seg informasjon ved å snoke rundt. Som vi kan se har en og samme kilde flere definisjoner på samme begrep, noe som ikke er uvanlig for kilder som definerer hackere og crackere.

The Jargon File ble påbegynt allerede i 1975 hvor en rekke personer bidro med å fylle filen med hackersjargong. Etter filen ble publisert som boken *The Hacker's Dictionary* i 1983 stoppet filen å vokse. Men en ny versjon ble påbegynt i 1990 av Eric S. Raymond med støtte av Guy Steele, som var redaktør for den opprinnelige filen. Filen ligger tilgjengelig på Raymonds nettside (Raymond 2005b) hvor den negative definisjonen har blitt lagt til, men den er utgitt på bokform i boken *The New hacker's dictionary* (Raymond 1993).

Boken gir blant annet en mer vid definisjon av hackere. Den sier blant annet at en hacker kan være en ekspert eller entusiast av et eller annet slag (for eksempel kan man være en astronomi hacker), eller det kan være en som liker den intellektuelle utfordringen ved å være kreativ og omgå begrensninger.

En viktig forskjell fra *The hacker's dictionary* til *The New hacker's dictionary* er at den negative beskrivelsen av en hacker i *The hacker's dictionary* nå blir omtalt som en *cracker* i *The New hacker's dictionary.* Ordet *cracker* fantes ikke i den originale boken, men ble først tatt i bruk i 1985 av hackere som ønsket å differensiere seg fra personer som drev uønsket virksomhet. En *cracker* er i *The New hacker's dictionary* de personer som bryter seg inn i datasystemer for å stjele eller ødelegge data.

Bokmålsordboka til Dokumentasjonsprosjektet ved Universitetet i Oslo har en litt annen definisjon av en hacker. Ved oppslag på verbet hacke, beskrives dette slik: «***hacke*** *v1 (utt hække; av hacker) skaffe seg tilgang til datasystemer og datanettverk på ulovlig vis (ved å knekke koder el. passord)*» (Wangensteen et al. 2004). Substantivet hacker beskrives slik: «***hacker*** *m2 (utt hækker; eng., av hack 'hakke (på tastatur)') person som hacker, datasnok*» (ibid).

Slår man opp på ordet *cracker*, blir vi i Bokmålsordsboka henvist videre til ordet *krakke* som forklares på denne måten; «*krakke v1 (eng. crack 'knuse') spalte, knuse (våtgass) molekyler*». Ordet er ikke direkte relatert til dataverdenen her, men beskriver noe nedbrytende, som det engelske verbet «to crack» som betyr å knuse eller ødelegge noe. Bokmålsordboka bruker altså *hacker* som en nedsettende beskrivelse om en som bryter seg inn i systemer, og har ikke engang *cracker* oppført i ordboken. Dette viser at forskjellige kilder bruker forskjellige definisjoner på hackere og crackere. Etter min mening er det greit at Bokmålsordboka bruker ordet hacker, og ikke cracker, om datakriminelle, men da mener jeg også at de burde ha beskrevet hva som var den opprinnelige betydningen av ordet, slik Caplex og Store Norske Leksikon gjør (jf. kapittel 3.1.2).

Ser man på enda en kilde som definerer hacker, omtaler Wikipedia hackere på to måter; nedsettende eller komplimenterende (Wikipedia 2005g). Wikipedia sier at i media omtales hackerne generelt som datainntrengere eller datakriminelle, mens i datamiljøet omtales hackerne som spesielt briljante programmerere eller tekniske eksperter. Linus Torvalds som er skaperen av kjernen i Linux er et eksempel på en slik briljant hacker. Det er den siste

definisjonen som er sagt å være den «riktige» bruken av ordet, slik det også er definert i *The Jargon File.*

Ved å kikke på definisjonene over kan vi se at forskjellige kilder definerer hackere på ulike måter. *The Jargon File* har en positiv og komplimenterende beskrivelse av en hacker, mens Bokmålsordboka gir en negativ karakteristikk og kaller hackerne kriminelle. Begge disse kildene gir en definisjon på en hacker, i motsetning til Wikipedia som gir oss to hoveddefinisjoner på en hacker.

Dette viser at man ikke er helt enige i hvordan man skal definere og bruke ordet, og at det pågår en debatt om hva som er den riktige bruken. Uansett hvordan man velger å bruke ordet er det viktig å være konsekvent og gi klart utrykk for hva man mener med ordet. Jeg vil komme tilbake til hvordan jeg velger å bruke ordet i avsnittet om *Min bruk av termene* i kapittel 3.1.4.

3.1.2 Forvirringen rundt hackerbegrepet

Det har lenge vært litt forviklinger rundt hackerbegrepet. Spesielt snakkes det mye om forskjellen på en hacker og en cracker. Som jeg forklarte i forrige subkapittel ble ordet hacker opprinnelig brukt om en person som liker å finne ut alt om datamaskiner uten å forårsake skade. Et sentralt kjennetegn ved de tidlige hackerne var at de var aktive deltakere av utviklingen av digitale artefakter.

Dessverre for mange av de opprinnelige hackere, ble populariteten av ordet en katastrofe. Levy (Levy 1994) forklarer at hackerbegrepet på slutten av 80-tallet fikk en negativ betydning. Han forteller at det hele startet med at en gjeng ungdommer ble arrestert for å ha brutt seg inn i offentlige datasystemer. Dette var arrestasjoner som var tett fulgt av media og journalistene som dekket disse historiene refererte til disse kjeltringene som hackere. Det var jo dette ungdommene kalte *seg selv.* På denne måten ble ordet raskt synonymt med en *digital inntrenger.* En kombinasjon av at en undergrunn på slutten av 80-tallet adopterte ordene *hacker* og *hacking* og medias fascinasjon for ting som er spektakulære og ødeleggende har ført til at det er den negative versjonen som er blitt framtredende.

Bruken av ordene i media har nok også hatt en innvirking på hvordan folk i gata bruker ordene. Siden ordet *hacker* stort sett brukes om en person som driver datakriminalitet, er det dette vanlige folk tenker på når de hører eller leser dette ordet. Det er etter hvert blitt et godt innarbeidet ord i den norske befolkningen. Det samme er ordet *cracker* som omtales som en person som lager små programkoder som gjør det mulig å bruke piratkopiert programvare eller spill som på en eller annen måte er kopibeskyttet.

Noe av forvirringen omkring bruken av termer kan skyldes at ordet *cracker* (engelsk låneord) ikke finnes på norsk. Dette oppdager vi raskt hvis man slår opp i diverse leksikon og ordbøker. Som jeg allerede har nevnt fantes ikke *cracker* i Bokmålsordboka, men heller ikke i kompaktleksikonet Caplex (Skagmo og Wikström 2004) eksisterer dette ordet. Det samme gjelder for det største norske leksikonet Store Norske Leksikon (Henriksen og Eriksen 2005) hvor man heller ikke finner dette ordet (i en datakontekst vel å merke).

Årsaken til at cracker ikke nevnes i disse oppslagsverkene er at det er et engelsk ord. Leksikonene har valgt å likestille hacker med datasnok. Det som oppslagsverkene kaller hacker eller datasnok, er etter mine definisjoner en cracker. Mine definisjoner finnes i kapittel 3.1.4.

I tillegg til å definere hacker som en som bryter seg inn i datasystemer og nettverk som vedkommende ikke har lovlig tilgang til, gir Store Norske Leksikon også en forklaring på forviklingen rundt hackerbegrepet. Leksikonet sier at; «*Opprinnelig ble betegnelsen brukt om personer som fordypet seg i dataprogrammering og informasjonsteknologi, og den brukes fortsatt i positiv forstand om personer som er opptatt av å plukke programsystemer fra hverandre for å finne ut av hvordan de virker*» (ibid). Med denne forklaringen mener jeg at leksikonet gir et klart uttrykk for at hackerbegrepet har fått en ny betydning, men at den opprinnelige definisjonen fremdeles brukes.

3.1.3 Hacker – Cracker

Jeg mener det ikke er noe stort skille på en hacker og en cracker hvis en ser på metoder og fremgangsmåter. Derimot mener jeg at skille er stort hvis man ser på holdninger og moral som disse menneskene besitter. Både hackere og crackere kan bryte seg inn i datasystemer, forskjellen ligger i at hackerne kun bryter seg inn på egne systemer eller på systemer hvor systemeier har gitt tillatelse. Crackerne bryr seg ikke om de har tillatelse eller ikke. Dette har med etikk å gjøre, som er viktig å komme inn på når man skal se på hvilke motivasjoner hackerne og crackerne har. Jeg vil drøfte hackernes og crackernes etikk i kapittel 3.2.8.

Andre mener det er et klart skille mellom en hacker og en cracker også utover etikken. Mange som karakteriserer seg for hackere, ønsker ikke å bli assosiert med en cracker og tar avstand fra crackernes handlinger. De fleste hackerne mener crackerne er uintelligente eller ukompetente, i hvert fall når det gjelder dybdekunnskap til datasystemer. En av disse som mener det er Eric S. Raymond som forteller i nettartikkelen «How To Become A Hacker» (Raymond 2005a) at «ekte» hackere ikke ønsker å ha noe med crackere å gjøre. Han mener at hackere bygger ting, mens crackerne ødelegger dem.

Årsakene til forvirringen rundt «hacker»-ordet kan i følge Gisle Hannemyr komme av at det er anvendt i minst tre forskjellige miljøer; datakyndige som arbeider etter bestemte verdier og en felles kultur; aktivister som ser på datamaskinen som et instrument for politisk maktutøvelse; og digitale vandaler som bryter seg inn i datasystemer fordi det er moro eller fordi de på en eller annen måte tjener på det *(Hannemyr 1998).*

I denne artikkelen ønsker Hannemyr å fokusere på det første miljøet der han mener at det har fått mindre oppmerksomhet enn det fortjener. Hannemyr sier at hackerne har stått for en stor del av programvareutviklingen, men at metodene som brukes er lite nevnt i litteraturen. Han mener også at hacking eller hacking-lignende metoder kan være med på å bedre kvaliteten på utviklingsprosessene og sluttproduktene.

Hannemyr mener hackertermen er temmelig missforstått, full av fordommer, folklore og mytologi (Hannemyr 1999). Han mener deler av misforståelsen stammer fra spesielle interessegrupper, som spenner seg fra digitale vandaler

til neoklassiske økonomiske liberalister, som forsøkte å kapre termen. Men det er imidlertid mulig å se forbi misforståelsen og bli oppmerksom på miljøet som deler en holding til en metode for å konstruere dataartefakter, en holding som har vært konstant siden 60-tallet.

Hannemyr mener at hacking fortjener å bli satt på kartet som en levedyktig metode for å skape og konstruere informasjonssystemer og programvareartefakter, noe jeg vil si meg enig i. Hacking burde vært studert ved siden av andre systemutviklingsmetoder og systemutviklere burde være oppmerksomme på dens anvendbarhet og være i stand til å utnytte hackingens arbeidsmetoder når det passer.

3.1.4 Min bruk av termene

I denne masteroppgaven kommer jeg til å gjøre et skille mellom hackere og crackere. Jeg kommer til å omtale hackere som datakyndige personer som ikke er involvert i noen form for kriminelle handlinger, og crackere som personer som oppnår eller prøver å oppnå uautorisert tilgang til systemer og informasjon. Jeg definerer hackerne som de «etiske» og lovlydige, mens crackerne blir de «uetiske» og kriminelle.

Jeg vil også omtale hackeren/crackeren som «han» fordi de fleste hackere/crackere er menn og fordi det vil være tungvint å skrive «han eller henne» gjennom hele oppgaven. I tillegg til ord som hacker og cracker vil jeg også benytte ord som *hacktivist, white hat hacker, black hat hacker, cyberpunk,*

phreaker, scriptkiddie og social engineer hvor det vil være naturlig. En beskrivelse av disse begrepene kommer i kapittel 3.2.

3.1.5 Hackergenerasjonene

Hackermiljøene har, som mye annet, gjennomgått en utvikling opp igjennom årene. Levy snakker om tre generasjoner av hackere; «True hackers», «Hardware hackers» og «Game hackers» (Levy 1994).

True hackers (første generasjon): De opprinnelige hackerne var dataspesialister som, på 60-tallet, adopterte ordet *hack* som et synonym på dataarbeid. De er fagkyndige personer som liker å lære absolutt alt om datasystemer. Gjennom dyktig programmering fikk de systemene til å yte maksimalt. Mer om denne generasjonen i kapittel 3.1.6; *De opprinnelige hackerne.*

Hardware hackers (andre generasjon): På 70-tallet oppstod det diverse tekno-hipper som ønsket å gjøre datamaskiner og datasystemer tilgjengelig og brukbare for allmennheten. De ønsket å komme et skritt videre fra stormaskinene, og utviklet mindre maskiner slik at en person kunne ha sin egen maskin.

Game hackers (tredje generasjon): Spillhackerne, som opplevde en voldsom respons på sine spill på 80-tallet. Dette ble de første programmererne som tjente store penger på sine *hacks*.

Måten begrepet *hacker* brukes på i dag vil i følge Taylor (Taylor 1999, s. 5) legge til enda en generasjon av hackere;

Hacker (fjerde generasjon): På slutten av 80-tallet fikk *hack* og *hacker* en ny betydning. For undergrunnen innen data, betydde nå «to hack» å bryte seg inn og sabotere datasystemer. En *hacker* var aktøren bak disse aktivitetene.

Til den fjerde generasjonen mener også Taylor at det kan legges til en ny gruppe. «The microserfs»[4], som jeg oppfatter som «samlebåndsprogrammerere» som ikke får utløp for kreativitet og frihet. Det er en generasjon som fra midten av 90-tallet ble satt til å utvikle programmer for den kommersielle databransjen.

Levys bok *Hackers* er opprinnelig fra 1984 og beskriver følgende bare utviklingen av hackerkulturen fram til det. Men hackermiljøene har utviklet seg siden det. Boken kom i en ny utgave i 1994 hvor Levy har lagt til etterord i slutten av boken hvor han forteller om utviklingen de siste ti årene. Og i dette kapittelet kommer det frem hvordan hackerbegrepet nå har fått en negativ

[4] Fra Douglas Couplands novelle med samme navn.

betydning. Så i tillegg til Levys opprinnelige tre generasjoner av hackere, beskriver han i 1994 utgaven av boken en ny generasjon som *digitale inntrengere.*

Levy og Taylor beskriver altså fire generasjoner av hackere i sine bøker. Hannemyr beskriver tre generasjoner i artikkelen *The art and craft of hacking (Hannemyr 1998)*. Han forteller om hackere i tre forskjellige miljøer; datakyndige personer som arbeider etter bestemte verdier og en felles kultur; aktivister som ser på datamaskinen som et instrument for politisk maktutøvelse; og digitale vandaler som bryter seg inn i datasystemer fordi det er moro eller fordi de på en eller annen måte tjener på det. Første og siste miljø som Hannemyr beskriver samsvarer bra med det Levy og Tylor definerer med første og fjerde generasjon hackere. Men istedenfor *hardware- og gamehackers* har Hannemyr en generasjon av aktivister. Dette viser i grove trekk at det er en felles oppfatning av hvordan hackerne opprinnelig var og hvordan hackerne nå oppfattes. Men at det likevel kan være forskjellige måter å dele opp den historiske utvikingen av hackerne på.

3.1.6 De opprinnelige hackerne

Levy forteller at de første hackermiljøene oppstod på universitetsområdet til Massachusetts Institute of Technology (MIT) på sekstitallet. De opprinnelige hackerne var dataspesialister som adopterte ordet «hack» som et synonym for dataarbeid. De begynte å bruke ordet «hacker» om dyktige personer som fant glede i og var stolte av det arbeidet de gjorde. Det var i «Tech Model Railroad Club» (TMRC) på MIT det hele startet. Klubbens «System and Power»-

avdeling (S&P) tok seg av jernbanens tekniske funksjoner. Dette var et komplekst system som gjorde det mulig for flere brukere å utvikle og kontrollere ulike deler av jernbanen samtidig.

Et «hack» var et ord som svirret rundt på MIT og som studentene i TMRC tok til seg. Levy forklarer ordet på følgende måte;

> «Det er en stilig, teknisk innovasjon eller forbedring av et system for dens egen skyld og er en slags eksperimentering eller utforskning gjort med stor glede fordi det er interessant eller gøy. Det ikke primært utført med tanke på eksterne, nyttige formål» .
>
> (Levy 1994, s. 23)

På jakt etter nye nyttige jernbane-hacks oppdaget studentene i S&P en IBM maskin som umiddelbart fascinerte dem. Men tilgangen til maskinen var både overvåket og begrenset av byråkratiske regler, i tillegg var regnetid dyrt. Etter hvert skaffet de seg regnetid om nettene, som gjorde at de fikk mye tid til å utforske stormaskinen fra IBM.

Etter å ha deltatt på det første datakurset ved MIT, ble de gradvis integrert i den like ferske avdelingen for Artificial Intelligence (AI). Her utviklet hackerne programvare, kompilatorer, dataspill og flerbrukeroperativsystemer. Fordi hackerne ikke likte den såkalte «batch»-programmeringen som IBM foretrakk, gjorde hackerne maskinene mer interaktive. De mulig gjorde dermed en mindre sentralisert bruk av datamaskinene. De hacket maskinvare og koblet sammen maskinene ved hjelp av ledninger.

Hackernes sosiale struktur var flat og samarbeid var viktig. Det ble sett på som en selvfølge å hjelpe hverandre og utveksle informasjon og erfaringer. Programmenes kildekode ble fritt distribuert og alle kunne komme med kommentarer og forbedringer. Dette er det som er blitt opphavet til hackeretikken. (Jf. kapittel 3.18).

Synspunktene om deling av informasjon og ressurser var grunnleggende verdier innen hackerkulturen. Her brukes begrepet hackerkulturen i den opprinnelige betydningen slik Levy brukte det da han beskrev kulturen rundt Institute of Technology sin AI lab på 60-tallet. (ibid). Hackeretikken står sentralt når Levy definerer de første hackerne. Han bruker hacker som en hedersbetegnelse om en person som viser sin dyktighet i programmering og som i tillegg føler seg forpliktet til hackeretikken.

3.1.7 Richard Stallmann / Free software

Richard Stallmann er en av de opprinnelige hackerne, en førstegenerasjons hacker som er kjent verden over for sitt engasjement for utvikling og spredning av fri programvare. Stallmann er en av motstanderne mot proprietære systemer og har blant annet vært i Norge og snakket om sine syn og meninger flere ganger. Jeg vil i dette kapittelet bruke Stallmann som et konkret eksempel på hva de første hackerne stod for og gi en beskrivelse av hvem han er og hva som er viktig for han i den forbindelse.

Stallmann er initiativtakeren av GNU-prosjektet (Stallmann 2005c) og Free Software Foundation (Stallmann 2005b). Etter å ha jobbet en stund ved Artificial Intelligence laboratoriet ved MIT sluttet han her pga. han var uenig i hvordan informasjonssystemer ble utviklet og brukt. Han var blitt bedt om å skrive under på en «non-disclosure agreement», en avtale som forhindrer han i å dele sin kunnskap om virkemåten til dataprogrammer med andre. Dette kunne ikke Stallmann godta. Han lanserer da prosjektet GNU, som er et fullstendig åpent datasystem. «GNU» er et akronym dannet fra forbokstavene i setningen; «GNU`s Not Unix».

Stallmann ønsket å utvikle et Unix-lignende system (kunne ikke bruke Unix siden det er et proprietært system) som fritt kunne distribueres til alle som ønsket det. Men hva mener Richard Stallmann egentlig med *Fri programvare*?

> «'Free software' is a matter of liberty, not price. To understand the concept, you should think of 'free' as in 'free speech', not as in 'free beer'».
>
> (Stallmann 2005a)

Det Stallmann mener er altså at programvare bør kunne distribueres fritt, ikke nødvendigvis at all programvare skal være gratis. Han mener det er helt greitt at man tar seg betalt for programvaren man utvikler så lenge den kan modifiseres og distribueres videre. I følge Free Software Foundation gir fri programvare følgende friheter (ibid);

1. Friheten til å kjøre programmet, uansett hensikt.
2. Friheten til å studere hvordan programmet virker, og tilpasse det til dine behov.
3. Friheten til å redistribuere kopier så du kan hjelpe din neste.
4. Friheten til å forbedre programmet, og gi det ut med dine forbedringer til offentlig eie, slik at hele samfunnet kan få utbytte av det.

En programvarelisens som ofte er brukt til fri programvare er GNU General Public License (GPL). Dette er en lisens av typen Copyleft som er en egenskap ved fri programvare som innebærer at dersom noen forandrer programvaren, må disse forandringene også være fri programvare. *Friheten* følger altså programvare ettersom den spres rundt. Stallmann mener at *frihet* handler om at det skal være mulig å kopiere programvare, at det skal kunne utvikles modifiserte versjoner og at den enkelt skal kunne distribueres til alle. Han har ingenting til gode for proprietær programvare, som for eksempel Microsoft utvikler. Stallmann mener da at solidariteten og fellesskapet mellom programmererne og folk flest blir ødelagt.

Et par ting som er viktig for Stallmann å poengtere, og som ofte er misforstått, er at *fri* programvare ikke betyr *gratis*. Han mener det er greitt å selge programvare man selv har utviklet, så lenge man ikke lager hindringer for andre. Stallmann mener også at Linux for ofte har fått æren hvor det egentlig har vært snakk om GNU/Linux. Linux, som Linus Torvalds står bak, er en operativsystemkjerne og GNU er applikasjonene rundt denne kjernen. Sammen utgjør de GNU/Linux.

Programvare som en felles ressurs har vært et gode i hackermiljøene siden begynnelsen av sekstitallet. På denne tiden ble programvare utviklet og delt mellom de som ønsket det. Det eksisterte ikke noe marked for programvare hvor programvare ble solgt og lisensiert. Programmerere kunne utvikle og forbedre programvare og i etterkant fritt distribuere produktet til alle andre.

Etter hvert utviklet dette seg til en kommersiell industri hvor programvareprodusentene ønsket å lisensiere og ta betalt for programvaren de laget. Mange hackere likte ikke denne utviklingen og Richard Stallmann beskriver i *The GNU Manifesto* hvorfor denne utviklingen er feil;

> «Many programmers are unhappy about the commercialization of system software. It may enable them to make more money, but it requires them to feel in conflict with other programmers in general rather than feel as comrades. The fundamental act of friendship among programmers is the sharing of programs; marketing arrangements now typically used essentially forbid programmers to treat others as friends. The purchaser of software must choose between friendship and obeying the law. Naturally, many decide that friendship is more important. But those who believe in law often do not feel at ease with either choice. They become cynical and think that programming is just a way of making money».

(Stallmann 2005d)

Det er altså den kommersielle dataindustrien Stallmann tar et kraftig oppgjør med. Han er imot de store aktørene som for eksempel Microsoft og Apple fordi de låser sin teknologi til bestemte produkter. Det Stallmann forsøker å få til med GNU prosjektet er å motarbeide og ødelegge for industrien som bruker hemmelige eller proprietære dataformater. Han ønsker å stoppe denne

utviklingen i programvarebransjen hvor det er de store markedskreftene som styrer. Han mener at kontrollen bør ligge hos programmererne. Dette har også vært et hett tema i Norge de siste par årene da den nye åndsverksloven har vært diskutert. Diskusjonen rundt den nye åndsverkloven er et konkret eksempel på hvilke saker hackere som Richard Stallmann kjemper imot. (Mer om åndsverksloven i kapittel 3.4.2).

3.1.8 Hackeretikken

Første generasjons hackere levde gjerne etter en etikk, hackeretikken. Deres drivkraft var vanligvis deres fascinasjon for teknologi. Hackerne hadde en ideologi som gikk ut på at all programvare og digital informasjon skulle være et universelt gode som burde være tilgjengelig for alle; *hackeretikken*. Den består av seks elementer:;

1. Tilgangen til datamaskiner - og hva som helst som kan lære deg noe om hvordan verden virker - bør være ubegrenset og total. Gi aldri opp med å prøve og feile («Always yield to the Hands-On Imperative»).
2. All informasjon bør være fritt tilgjengelig.
3. Ha mistro til autoriteter - du bør fremme desentralisering.
4. Hackere bør vurderes etter deres hacking, ikke etter tvilsomme kriterier som grad, alder, rase eller posisjon.
5. Du kan lage kunst og skjønnhet på en datamaskin.
6. Datamaskiner kan forandre ditt liv til det bedre.

(Levy 1994, kap. 3)

Når disse prinsippene og godene de er ment for å fremme, er truet, blir hackerne ofte politiske. De fokuserer på enhvers rett til å ha internettilgang og på menneskelige rettigheter, slik som ytringsfriheten. Electronic Frontier Foundation[5] (EFF) og Access for All[6] er eksempler på slike politiske hackerorganisasjoner.

En ting som jeg mener er verdt å merke seg er at hackeretikken inneholder de samme verdiene som Stallmann og Free Software Foundation lister opp som fire typer av frihet. Både hackeretikken og prinsippene om frihet bringer det samme budskapet om at all informasjon bør deles og være fritt tilgjengelig for alle. Det er tankene om en bedre verden som står sentralt bak disse punktene. Det er kanskje ikke så rart at Stallmann har kommet med akkurat disse ytringene om hvordan programvare bør utvikles, da han selv har levd etter hackeretikkens prinsipper.

Mange av dagens hackere og crackere følger hackeretikkens «regler» og Jon Johansen er et eksempel på dette. Jeg mener Johansen kan sammenlignes med de opprinnelige hackerne som levde etter prinsippene i hackeretikken. Både hackerne fra 60-tallet og Johansen er opptatt av at informasjon skal være fritt tilgjengelig og at det skal være fri konkurranse på markedet. Når disse prinsippene blir truet blir hackerne ofte politiske, slik vi har sett Stallmann med GNU og FSF og Johansen med sine gjentatte krumspring mot den kommersielle dataindustrien.

[5] http://www.eff.org/

[6] http://www.xs4all.org/

3.2 Hacker- og crackervarianter

Så langt i oppgaven har jeg forklart hva som menes med ordene hackere og crackere. Jeg vil nå gå ned et abstraksjonsnivå og gå igjennom forskjellige typer av hackere og crackere. Begrepene jeg nå vil gå igjennom brukes ofte om hverandre så jeg vil prøve å få klart frem hva som skiller de forskjellige variantene fra hverandre, samt hva som er karakteristiske for de ulike begrepene.

Som jeg tidligere har nevnt oversettes cracker med datasnok på norsk, noe jeg har valgt å ikke gjøre i denne oppgaven. Årsaken til at jeg velger å benytte den engelske varianten, er fordi det ikke finnes norske ord for de andre hacker- og crackervariantene som jeg omtaler. Dessuten er tittelen på oppgaven min hackere/crackere som jeg synes tar seg bedre ut enn hackere/datasnoker.

Likevel syns jeg datasnok bør nevnes i en oppgave som denne. En datasnok er en som forsøker å snoke til seg data og informasjon som han eller hun ikke har rett til å se (Hannemyr 2003). Som jeg tidligere har nevnt i kapittel 3.1.2 oversetter flere leksikon ordet *hacker* med ordet *datasnok*. Siden jeg har valgt å skille på hackere og crackere kan ikke jeg gjøre samme oversettelsen. I motsetning til leksikonene vil da min definisjon av en datasnok være cracker og IKKE hacker. Uansett om man velger å bruke datasnok eller cracker, er denne personen like uetisk med tanke på personens handlinger.

3.2.1 White hat hacker

En *white hat hacker* er en etisk hacker som kun bryter seg inn i datasystemer eller nettverk han selv administrerer eller hvor tillatelse til slik aktivitet er gitt. Intensjonen til denne typen hackere er å finne svakheter i systemer og utbedre disse. De tar avstand fra innbrudd og misbruk av datasystemer. Mange white hat hackere jobber som sikkerhetskonsulenter og har utvikling og testing av datasystemer som arbeidsfelt. (Wikipedia 2006c)

Begrepet «hvite» hackerne brukes noen ganger om personer som angriper systemer eller nettverk med det formål å hjelpe systemeieren med å sikre systemene sine. Slike personer velger jeg å definere som crackere. Selv om de har gode intensjoner bryter de seg inn i systemer som de ikke har rettigheter til, og dermed vil jeg si de er uetiske.

White hat hacker er en motsetning til *black hat hackers* som jeg omtaler i kapittel 3.2.3. Termene er hentet fra gamle Western filmer, der heltene ofte hadde hvite hatter og forbryterne hadde svarte.

3.2.2 Hacktivist

Nettsiden *the Hacktivist* definerer *hacktivisme* som en blanding av hacking og aktivisme; teknologi og politikk. *Hacktivisme* er beskrevet som hacking for politiske grunner. En *hacktivist* er en som utfører disse handlingene (The Hacktivist 2005).

I dokumentarfilmen «Hackere», som er vist på National Geograpic Channel, viser lederen for hacktivistgruppen *Electronic Disturbance Theater*, Ricardo Dominguez, hvordan hans gruppe uttrykker politiske meninger online. Dominguez har samordnet angrep mot Det Hvite Hus, Pentagon, Frankfurt-børsen og Mexicos regjering. Via Internett protesterer gruppen hans blant annet mot undertrykkingen av Chiapasindianerene.

Gruppens idé var å skape en prosess der en stor gruppe mennesker kunne samles til en «sitdownstreik». Målet var at gruppen skulle skape en symbolsk handling for å vise sine meninger. For å kunne gjennomføre en slik sitdownstreik på nettet kontaktet Dominguez hackeren Carmen Karasic. Hun er skaperen bak *FloodNet*, programvaren som er blitt gruppens fremste våpen. FloodNet er et program som automatiserer oppdateringsprosessen på et nettsted. Folk som hadde installert Floodnet på sin maskin kunne få FloodNet til å hente ned bestemte nettsider om igjen og om igjen. Gjorde tilstrekkelig mange dette samtidig, kollapset nettsiden.

Karasic sier i filmen; «*Alle politiske budskap man sender ut i cyberspace bør være kollektive. Det skal ikke bare være min mening, men tusenvis av menneskers meninger.*» Dette er et interessant punkt hvis man sammenligner med andre distribuerte tjenestenektingsangrep, som dette faktisk er. I motsetning til vanlige tjenestenektingsangrep hvor gjerne én person har kontroll over tusenvis av maskiner, må deltakerne ved et angrep utført av gruppen til Dominguez rekrutteres og aktivt være med på selve angrepet. Etikken i et slikt angrep er at det er mange som deler samme politiske syn og dermed har de rett til å bli hørt. Dette er en form for sivil ulydighet, som jeg vil diskutere mer i kapittel 3.2.8 hvor jeg oppsummerer forskjellige typer hackere og crackere.

Floodnet fungerer kun gjennom *massiv* mobilisering av mennesker og det er en forutsetning at tusenvis av mennesker deltar i en koordinert aksjon hvis det skal ha noen effekt. Hver enkelt aktivist må laste ned og installere FloodNet og sitte og vente til angrepet skal starte. Det at så mange samarbeider om et angrep gir en viss maktfølelse og gjør det lettere å bli sett og hørt. Det er nettopp denne sammenblandingen av teknologi (hacking) og mobilisering av menneskelig deltakelse (aktivisme) som utgjør «hacktivisme».

3.2.3 Black hat hacker

En *black hat hacker* er, i motsetning til en white hat hacker, en som bryter seg inn i datasystemer eller nettverk med onde hensikter. Denne typen crackere benytter mulighetene med å ha brutt seg inn i systemet ved for eksempel å ødelegge filer eller stjele informasjon til egen vinning (Wikipedia 2006a). De «svarte» hackerne opptrer uetisk ved at de utfører datakriminalitet.

Begrepet *grey hat hacker* kan man også noen ganger høre. Den «grå» hackeren er en blanding av den «hvite» og «svarte». En grey hat hacker kan noen ganger opptre lovlig, mens andre ganger ikke. De hacker ikke for personlig vinning og har ingen onde hensikter, men de begår lovbrudd (Wikipedia 2006b). Jeg har valgt å bare nevne begrepet, men velger å ikke bruke det videre i oppgaven. Dette fordi jeg vil forenkle og definere en person som enten en hacker eller en cracker. Hvis er person utfører lovbrudd er han etter mine definisjoner en cracker, en uetisk person.

3.2.4 Cyberpunk

Wikipedia definerer ordet *cyberpunk* som en sub-genre av science fiction som fokuserer på datamaskiner og informasjonsteknologi (Wikipedia 2005c). En typisk handling i cyberpunk-litteraturen omhandler ofte konflikten mellom hacker, kunstig intelligens og *megacorps* (store mektige virksomheter). Gardner Dozois er den personen som gjorde *cyberpunk* populær som en litteraturgenre etter publiseringen av artikkelen *Sf in the Eighties* in Washington Post in 1984 (Dozois 1984). Senere ble begrepet brukt om science fiction forfattere som inntok sjangeren på 80-tallet. En av disse forfatterne var Bruce Sterling, som i boken *The hacker crackdown* beskriver to trekk ved cyberpunkerne;

> «Forfatterne hadde en uimotståelig interesse for informasjonsteknologi, en interesse nær beslektet til science fictions tidlige fascinasjon med reiser i rommet. I tillegg var disse forfatterne 'punks', med alt det førte med seg; bohemisk oppførsel, viltre ungdommer, opprør, rare klær og hår, merkelig politikk, kjærlighet for støyende rock and roll; med andre ord, trøbbel.»
>
> (Sterling 1992, s. 140)

Påvirket av cyberpunk litteraturen på midten av 80-tallet, begynte diverse grupper å referere seg selv som cyberpunks. Datanerder, crackere, hackere, politisk radikal ungdom og musikere trykket raskt begrepet til sitt bryst. Cyberpunkerne hentet inspirasjon fra litteraturen og filmene til både klessdrakt, språk, musikk og fritidssysler. Cyberpunk gir assosiasjoner til personer som er opprørsk og udannet og som befinner seg på utsiden av eller i opposisjon til det rådende systemet. Det er disse «ulydige» cyberpunkerne i en datakontekst jeg ønsker å se i en sammenheng med de andre termene jeg

beskriver i dette kapittelet. Den «negative» ladningen av ordet og det faktum at cyberpunkerne balanserer på kanten av loven har gjort at jeg har karakterisert dem som en type crackere.

3.2.5 Phreaker

Phreaking er et «slang»-uttrykk for å beskrive aktiviteten til en subkultur av personer som eksperimenterer med, eller utnytter telefoner, telefonselskaper og systemer som er tilkoblet eller som er en del av Public Switched Telephone Network (PSTN) (Wikipedia 2005j). En phreaker er aktøren bak disse aktivitetene. «Phreak» er en sammensetning av ordene «phone» og «freak», men begrepet kan også referere til forskjellige lydfrekvenser (FREQuencies) som brukes til å manipulere telefonsystemer.

Et tidlig phreaking-verktøy, «The blue box», er en elektronisk innrettning som simulerer en telefonoperatørs telefonkonsoll (Wikipedia 2005b). Den fungerer slik at den reproduserer tonene som brukes for å svitsje langdistanse samtaler og bruke disse til å rute din egen oppringning. Det mest typiske formålet med dette verktøyet var å ringe gratis.

I begynnelsen av 1970 årene lagde og solgte en del personer slike *blue boxes*. En av dem var phreakeren John Draper, også kjent som Captain Crunch. Levy (Levy 1994, s. 248) forklarer hvordan Draper fikk dette tilnavnet da han ved å blåse i fløytene som fulgte med frokostblandingen *Captain Crunch*, nøyaktig

kunne reprodusere toner med samme frekvens som ble brukt til å rute telefonsamtaler.

En phreaker er etter min oppfatning også en type cracker. Både phreakere og crackere bryter lovverket ved å manipulere systemer. Fremgangsmåten deres består i å utnytte svakheter i systemene.

3.2.6 Scriptkiddie

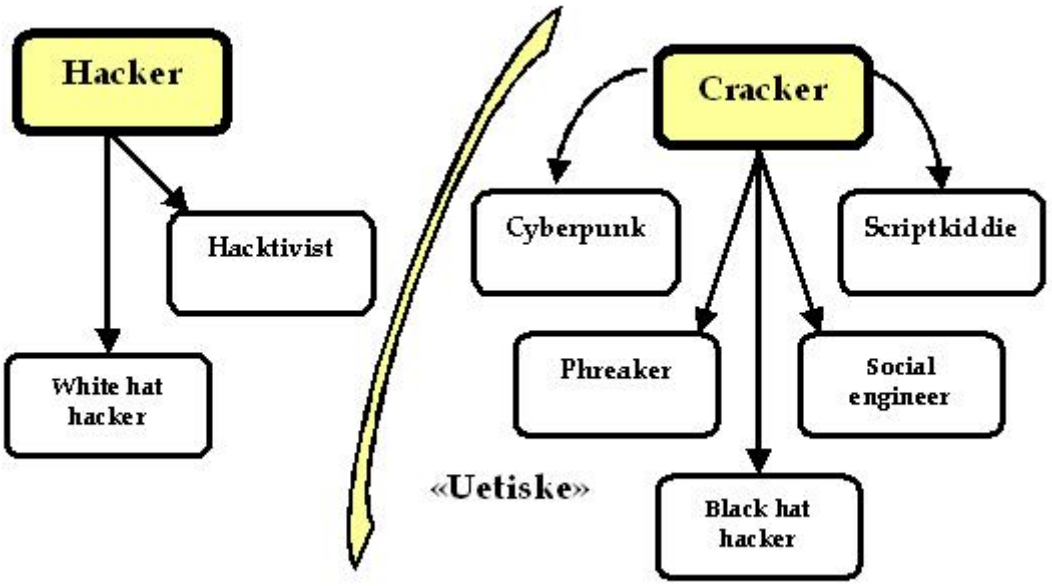
Observasjoner utført av VDI og Økokrim, viser at man ut i fra trafikken på Internett kan se at mesteparten av alle angrep som skjer, utføreres av *scriptkiddies*. Begrepet er en nedsettende term for en uerfaren cracker som bruker skript og programmer utviklet av andre for å kompromittere datamaskiner og for å sette i gang angrep mot datasystemer (Wikipedia 2005e). Begrepet handler mer om en strategi enn om personer, en strategi som går ut på å ta det svakeste byttet. Dette innebærer at en angriper ikke er på jakt etter spesifikk informasjon, men søker å tilegne seg rettigheter i forskjellige datasystemer så enkelt som mulig. Angriperen fokuserer på et lite antall sikkerhetshull og skanner et definert IP-område på Internett etter disse hullene. Sannsynligheten for at han finner systemer med svakheter er stor. Når så et sikkerhetshull er oppdaget kjører de et ferdiglagd program, Exploit (jf. kapittel 3.3.1), for å utnytte akkurat denne svakheten. Dette er gjerne en maskin som ikke har oppdatert programvare eller som ikke har endret standardinnstillingene i systemet.

3.2.7 Social engineer

En *social engineer* er en person som lurer folk til å oppgi sensitiv informasjon eller å få dem til å gjøre noe som er i mot virksomhetens sikkerhetsbestemmelser (Wikipedia 2005l). Dette er kyniske personer som bruker ikke-tekniske metoder får å få tilgang til informasjon han ellers ikke skulle hatt.

3.2.8 Sammenhengen mellom variantene

I figuren på neste side har jeg prøvd å sette de forskjellige hacker- og crackertermene i en visuell sammenheng. Figuren er «delt» i to hvor jeg viser de «etiske» hackerne på en side og de «uetiske» crackerne på andre siden. Hacker og cracker befinner seg på høyeste nivå i figuren og resterende begreper utspringer igjen fra disse og beskriver en type hacker eller cracker.



Figur 1: Hacker- og crackerbegrepene sett i en visuell sammenheng.

Som man ser ut i fra figuren har jeg gjort et skille på etiske og uetiske grupperinger. Etikk, som er læren om rett og galt, står sentralt når jeg skal prøve å finne motivasjonene som ligger bak hackernes og crackernes (u)gjerninger. Men når kan man egentlig kalle personer etiske eller uetiske? Dette er et vanskelig tema og man berører nå en del av filosofien som undersøker hva som er rett og galt, og som setter normer og prinsipper for riktig handlig. Dersom man sier noe er «uetisk» eller «umoralsk», mener man at det er i strid med visse normalnormer. Dersom man for eksempel mener det er umoralsk å utøve vold, betyr dette at man slutter opp om den normalnormen som sier at man ikke bør utøve vold.

Det er liten tvil om at man kan kalle personene plassert til høyre i figuren for uetiske. Personene på denne siden strider mot normalnormer som folk ellers i samfunnet overholder. Flesteparten av oss er enige i at «å ta seg inn på annen

manns eiendom» er galt og noe man ikke gjør. Crackere har ikke samme oppfattelse som gjør at man kan kategorisere dem som uetiske.

Hackere derimot følger samfunnets normalnormer og mener at cracking er feil, noe som gjør at hackere kan karakteriseres som etiske. Det som imidlertid er interessant i figur 1 er at jeg har plassert hacktivistene på venstresiden, den etiske siden. Hvordan kan jeg gjøre dette når hacktivister er villige til å bryte loven for å oppnå sine mål? Svaret er «sivil ulydighet» som er et politisk virkemiddel som brukes for å markere motstand mot en spesiell politisk sak ved å bryte loven (Wikipedia 2005k). Sivil ulydighet er et vanskelig tema, men er en nødvendighet i de fleste samfunn. Det finnes mange måter å utøve sivil ulydighet på. Ofte innebærer det hindring av ferdsel ved fastlenking av aksjonister, enten i ferdselstraseen eller på selve kjøretøyene, eller å ta seg inn på stengt eiendom. Men sivil ulydighet kan også utøves i kyberrommet, slik hacktivistene i *Electronic Disturbance Theater* er et eksempel på.

Indiske Mahatma Gandhi er kanskje en av de mest kjente internasjonale tilhengerne av sivil ulydighet. Gandhi er kjent for sin ikke-voldelige linje og sivile motstand for å bedre indiske folks rettigheter under det britiske kolonistyret i landet.

> "Sivil ulydighet er en borgers naturlige rettighet. Han kan ikke gi avkall på den uten å gi avkall på sitt menneskeverd".
>
> (Mahatma Gandhi)

Hacktivistenes holdninger kan sammenlignes med Gandhis da hacktivistene bruker teknologi for å utøve sivil motstand mot politiske standpunkter de er uenige med. Både Gandhi og hacktivister viser at i forholdet mellom rett og galt, er det ikke alltid de rettslige reglene som gir det beste grunnlaget for å handle riktig. I visse tilfeller kan moralen stå over rettsystemet, og det finnes situasjoner hvor man kan forsvare bruk av sivil ulydighet. Av den grunn kan man karakterisere hacktivister for etiske mennesker.

3.3 Metoder for hacker- og crackerangrep

I forrige subkapittel presenterte jeg en rekke hacker- og crackervarianter. Altså *hvem* som står bak ulike angrep. Jeg vil fortesette dette kapittelet med *hvordan* silke personer kan utøre forskjellige typer angrep og hvordan de kan holde kontrollen på kompromitterte maskiner.

3.3.1 Exploits

En *exploit* er en mye brukt term når det er snakk om datasikkerhet. Begrepet referer til programkode som utnytter feil og svakheter i datasystemer (Wikipedia 2005f). Exploiter er vanlig å bruke når personer skal penetrere datasystemer og derfor er dette relevant å ta med i dette kapittelet.

Internett flommer over av ferdiglagde exploits som fritt kan lastes ned og kjøres. Det går stadig kortere tid fra et sikkerhetshull blir oppdaget til det blir utnyttet av ondsinnet programvare. Det snakkes da om «zero-day exploits»,

dvs. at ondsinnet programvare utnytter et sikkerhetshull *før* en oppdatering av svakheten er tilgjengelig.

På Internett finnes det i dag utallige nettsider som offentliggjør Exploits. Sidene inneholder oppskrifter, tilpassede verktøy og skripter som fritt kan lastes ned. Mange sider har også tilgjengelig egne «hacker-kit» som inneholder alt man trenger for å finne og bryte seg inn i systemer med sikkerhetshull. På nettsiden til den franske sikkerhetsorganisasjonen Frsirt[7] legges det ut beskrivelser på nye sikkerhetshull og ferdige exploits på mange av disse hullene. Det samme gjøres også på Packet Storms[8] nettsider hvor man til en hver tid finner de ferskeste sårbarhetene.

Det finnes mange måter å klassifisere exploits på, men den mest vanlige er hvordan exploiten kontakter systemsvakheten. En «remote exploit» benytter nettverket og utnytter svakheten uten noen form for rettigheter på systemet det angriper. En «local exploit» krever rettigheter til det sårbare systemet som så utnytter systemet for å øke brukerrettighetene til den som kjører exploiten. SANS Institute (Sans Institute 2002) gir en kort beskrivelse av hvordan man kan kategorisere exploits og hvilke typer exploits som finnes. Noen generelle exploits kan være IP forfalsking, sesjonskapring, DNS angrep og buffer oversvømming.

[7] http://www.frsirt.com

[8] http://www.packetstormsecurity.org

3.3.2 IRC og botnet

IRC (Internet Relay Chat) er en protokoll for å snakke sammen på Internett i sanntid (Wikipedia 2005h). IRC er et sentralt punkt når temaet er hacking og cracking. IRC er en møteplass hvor hackere og crackere møtes for å utveksle informasjon og erfaringer. Men IRC brukes også til å holde kontrollen på store nettverk at kompromitterte maskiner som kan brukes i uærlig henseende. Dette gjør at jeg ser på IRC og botnet som et sentralt tema som er viktig å belyse i denne masteroppgaven.

Protokollen er utviklet av finnen J. Oikarinen i 1988 og er beskrevet i dokumentet RFC1459 (Oikarinen og Reed 1993). IRC er en tjeneste som lar brukere verden over kommunisere med hverandre via et interaktivt nettverk i sanntid. IRC benytter chatterom/kanaler hvor to eller flere brukere kan kommunisere med hverandre samtidig. Det finnes en rekke IRC-klienter, men kanskje den mest kjente er mIRC[9]. Klienten kobler til en tjener som igjen kommuniserer med andre tjerner via en hub.

En bot eller en robot som forkortelsen tilsier, er et program som er laget for å automatisere og utføre oppgaver som omhandler vedlikehold av IRC-kanaler. En slik IRC-bot står som oftest på en eller annen ekstern datamaskin med høy oppetid, slik at boten skal kunne være pålogget hele tiden.

[9] http://www.mirc.com

En bot blir ofte brukt som en «dørvakt» for IRC-kanaler. Her passer boten på hva som skjer i kanalen, og skulle det oppstå konflikter så er den programmert til å utføre en handling av gitte situasjoner. En IRC-bot passer på at riktige brukere av kanalen får kontroll over kanalen, slik at ingen har mulighet til å ta over kanalen.

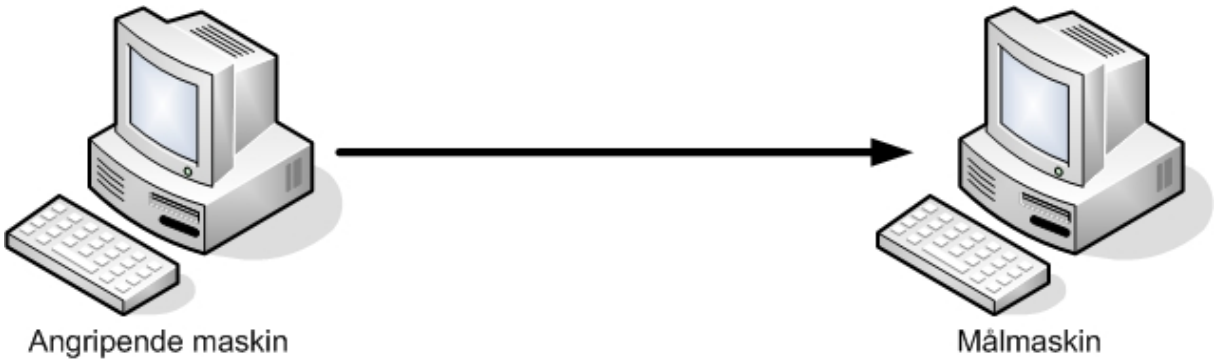
En bouncer (bnc) er en ekstern klient du kobler deg opp mot via din egen klient. Fordelen med dette er at du alltid vil være pålogget. En bouncer brukers blant annet til å passe på kallenavn på IRC-nettverket der man ikke kan reservere sitt eget kallenavn.

Personer kan bygge egne botnet som består av maskiner de har kontroll på. Disse nettene kan blant annet brukes til å utføre DoS-angrep som beskrives i neste avsnitt.

3.3.3 DoS/DDoS

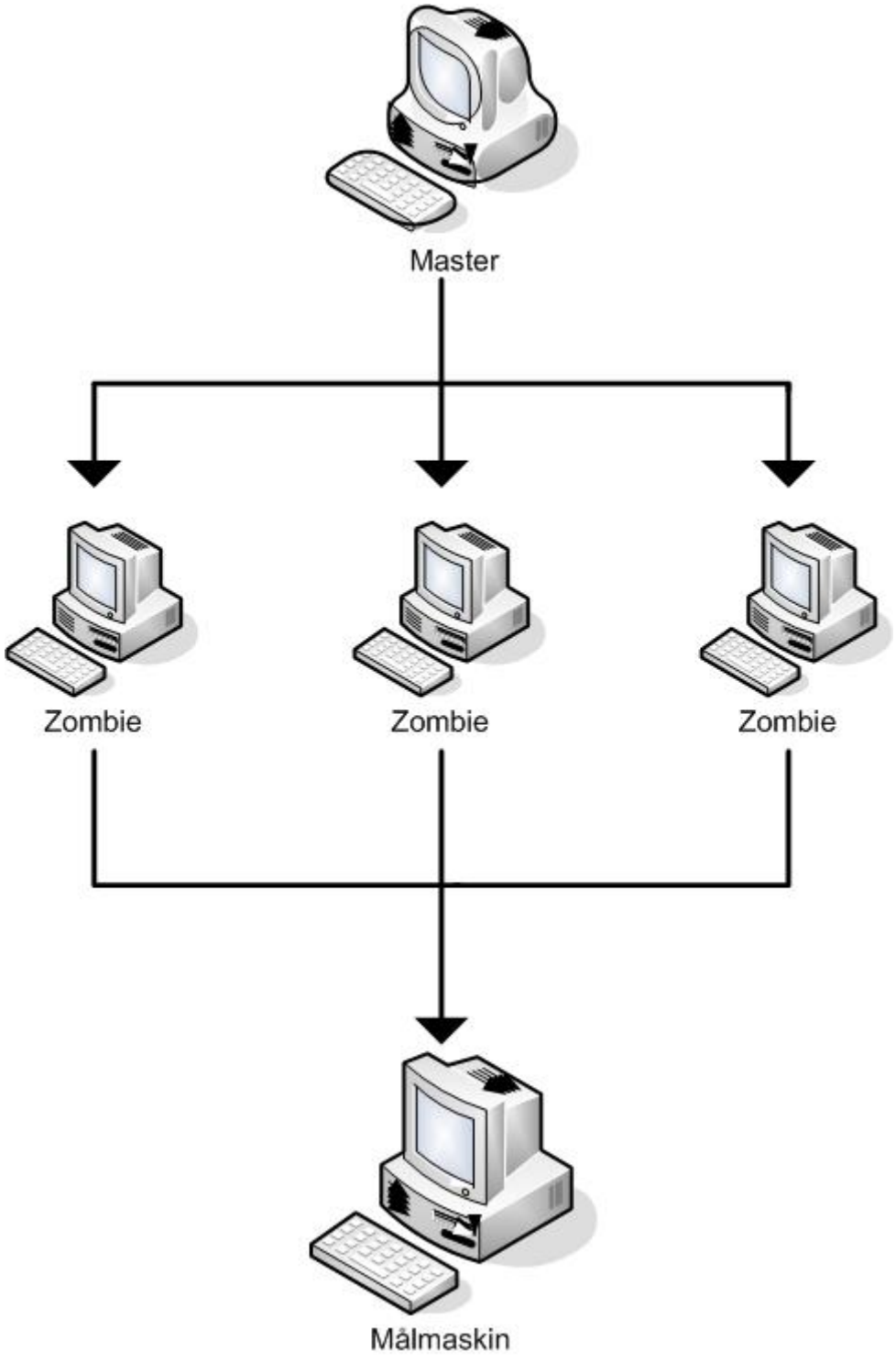
Et tjenestenektingsangrep (Denial of Service (DoS) attack) er et angrep på en datamaskin eller nettverk som fører til tap av tjenester til brukere. Typisk er dette tap av nettverksforbindelse og tjenester som opptar båndbredden til offerets nettverk eller overbelasting av ressurser på offerets maskin (Wikipedia 2005e).

Ved et tjenestenektingsangrep forsøker en angriper å hindre at legitime brukere får tilgang til tjenester og/eller informasjon. Den vanligste formen for tjenestenektingsangrep er å oversvømme nettet med trafikk. For eksempel gjøre nettsteder utilgjengelige ved å sende en stor menge forespørsler til webtjeneren. Hensikten er som oftest ikke å få tilgang til informasjon selv, men rett og slett bare være destruktiv. Figur 2 viser det tradisjonelle DoS-angrepet hvor én enkelt maskin angriper en annen. Hackeren sitter som oftest ikke selv på den angripende maskinen, men bruker en maskin som han har tatt kontrollen over, uten at eieren vet om det.



Figur 2: Det tradisjonelle tjenestenektangrepet. DoS.

Distribuert tjenestenektingsangrep (Distributed Denial of Service (DDos) attack) derimot innebærer at mange maskiner på forskjellige steder «samarbeider» om et angrep på ett mål. Ved at mange maskiner samarbeider blir angrepet straks mer kraftig. Figur 3 viser hvordan et distribuert tjenestenektingsangrep utføres. Mastermaskinen kontrollerer en rekke maskiner som bare venter på angrepsordren.



Figur 3: Distribuert tjenestenektingsangrep. DDoS.

En «bot» (forkortelse for «robot») er en maskin som er kompromittert og kan kontrolleres eksternt. Disse maskinene kalles også «zombier» da de kan vekkes

av crackeren som kontroller dem. Virus og annen ondsinnet programvare installerer programvare på maskiner som lytter på bestemte porter og/eller laster ned botprogrammer fra dertil egnede nettsteder. Et «botnet» er en samling av boter som blir kontrollert av én person eller maskin. Til en hver tid er det et stort antall maskiner i verden som inngår i slike botnet uten at eieren av maskinen vet om det. Botnet eller bot-programvare blir rutinemessig leid ut eller solgt til for eksempel spammere og utpressere. Kriminelle driver utpressing av virksomheter ved å true med DDoS-angrep, da man vet at det vil være svært kritisk for mange bedrifter å ha nedetid på systemene sine.

En artikkel i *USA Today* (Acohido og Swartz 2004) rapporterte i september 2004 at prisen for et botnet med 20 000 maskiner var 2000–3000 USD. Andre kilder oppgir prisen til opptil 40 USD per bot for kraftige maskiner med rask nettilknytning. Prisen på disse store nettene av kompromitterte maskiner er doblet siden sommeren 2003 da *The Register* (Leyden 2004) rapporterte at et botnet med 10 000 zombier var verd 500 USD.

3.3.4 Social engineering

Social engineering, som gjerne kalles «sosial ingeniørkunst» på norsk, er en metode for å skaffe seg konfidensiell informasjon ved å manipulere legitime brukere (Wikipedia 2005l). En person som driver social engineering bruker ofte telefonen for å lure personer til å gi fra seg sensitiv informasjon (for eksempel passord), eller få dem til å gjøre noe som er imot virksomhetens sikkerhetsrutiner. Ved å benytte seg av denne metoden, kan svindlere utnytte andre personers godtrohet, istedenfor å utnytte sårbarheter i datasystemer.

Man er generelt enige om at «brukere er det svake ledd» innen datasikkerhet og det er dette som gjør social engineering mulig.

Phishing er et uredelig forsøk på å skaffe seg sensitiv informasjon, og er en spesialisert form for social engineering. Den klassiske metoden med å svindle personer over telefon er byttet ut med svindelforsøk over elektroniske medier som e-post eller instant messaging (IM)[10]. Formålet er det samme; å forsøke å skaffe seg passord- eller kredittkortopplysninger ved å utgi seg for å være en pålitelig person eller virksomhet som har bruk for denne typen informasjon. (Wikipedia 2005i).

Den mest klassiske phishing-metoden er å forsøke å svindle bankkunder til å gi fra seg personlige opplysninger ved hjelp av falske e-postmeldinger. Dette kan være opplysninger om navn, adresse, bankkortnummer eller pinkoder. E-postmeldningene ser ut til å komme fra en ekte bank og oppgir en tilsynelatende korrekt URL[11] som mottageren skal klikke seg inn på. Disse linkene fører ikke til banken, men til en side som ligner hvor brukeren blir bedt om å skrive inn sine personlige data. Siden er ofte svært godt laget hvor designelementer er importert fra bankens egen nettside.

På lik linje med social engineering og utsendelse av spam er phishing metoder for å utnytte mennesker til egen vinning. Bak disse uærlige handlingene finnes

[10] Instant messaging et verktøy for å sende meldinger i sanntid.

[11] Uniform Resource Locator.

kyniske personer med lav moral som ikke skyr noen midler for å oppnå sine mål.

3.3.5 Virus

I dag er «datavirus» en del av dagligtalen til folk som bruker datamaskiner. Et virus er en type dataprogram som kan reprodusere seg selv ved å lage kopier av seg selv (Wikipedia 2005q). Hovedkriteriet for å klassifisere en bit av eksekverbar kode som et virus, er at det sprer seg vha. en vert. Et virus kan bare spre seg fra en datamaskin til en annen når verten føres til andre datamaskiner over nettet eller på et lagringsmedium som for eksempel en CD-plate eller en USB-nøkkel. Virus sprer seg også til andre maskiner ved å infisere filer på et nettverk eller filsystem som aksesseres av andre maskiner. Ut i fra definisjonene mine er det som oftest black hat hackere eller scriptkiddies som står bak spredningen av virus.

I media brukes ofte datavirus for å betegne nært sagt alle former for angrep på et datasystem. Men det kan imidlertid være nyttig å skille på forskjellige typer angrep. For eksempel blir virus ofte forvekslet med ormer og trojanske hester.

Ormer

En «orm» (ibid) kan spre seg til andre maskiner uten å være avhengig av en vert. Mange datamaskiner er nå knyttet mot Internett og til lokalnett, noe som gjøre spredning lettere. Mange av dagens virus benytter seg også av

nettverkstjenester som World Wide Web, e-post og fildeling som måter å spre seg på, noe som gjøre det vanskelig å skille mellom ormer og virus.

Trojanske hester

En «trojansk hest» er et ondsinnet program som er forkledd som et legitimt program (Wikipedia 2005o). Termen stammer fra den klassiske myten om den trojanske hesten. Under beleiringen av byen Troy, lagde grekerne en stor trehest utenfor byen. Trojanerne var overbevist om at det var en gave og flyttet hesten til innsiden av bymurene. Det viste seg senere at hesten var hul og inneholdt greske soldater som i løpet av natten åpnet dørene til bymuren slik at den greske hær kunne invadere byen. Et trojansk hest på en datamaskin fungerer på samme måten; de ser nyttige og interessante ut, men er i virkeligheten skadelige når de blir eksekvert.

3.3.6 Spyware / Adware

«Spyware» er programvare som samler og rapporterer informasjon om en datamaskinbruker uten brukerens viten og samtykke (Wikipedia 2005n). Det kan da dreie seg om informasjon som skal brukes til å markedsføre på bakgrunn av dine nettvaner. Noe av spywaren kan også inneholde tastaturloggere som sender alle dine tastetrykk tilbake til personene som har laget spywareprogrammet. Spyware som en kategori av ondsinnet kode, overlapper med «adware»[12]. Adware er programvare som viser reklame når programmet kjører (Wikipedia 2005a). Men det finnes adware som er godkjent

[12] Advertising-supported software.

og ønsket av brukeren og adware som ikke er ønsker av brukeren. Og det er den uønskede delen av adware som overlapper med spyware.

3.3.7 Spam

Spamming defineres som bruk av hvilket som helst elektronisk kommunikasjonsmedium for vilkårlig å sende spontane meldinger i stort omfang (Wikipedia 2005m). For folk flest er den mest kjente formen for spam den som blir sendt på e-post som en måte å reklamere for et eller annet produkt.

«Spam» er opprinnelig en betegnelse på et temmelig uappetittlig hermetisert kjøttprodukt som produseres i USA. Årsaken til at søppelpost nå har fått dette tilnavnet skyldes den britiske komikergruppen Monty Pyton som i en sketsj oppsøker en restaurant der det eneste på menyen er spam som serveres gjentatte ganger i ulike varianter.

Spam er dessverre en lønnsom geskjeft for de som sender ut store mengder e-post som ingen vil ha. En håndfull selskaper i verden står bak 90 prosent av all spam, og sender ut millioner av e-poster hver dag. Metodene de bruker er å bruke kompromitterte maskiner til uvitende personer for utsendelsene. Crackere har altså tatt kontroll over store antall maskiner som de lar spammerne bruke mot et passelig beløp. En cracker som har bygget seg opp et stort nettverk av maskiner kan med andre ord tjene gode penger på å la spammere få (mis)bruke disse maskinene.

3.4 Dagens situasjon

I dette kapittelet hvor jeg går i gjennom relevant teori vil jeg prøve å gi et innblikk i hvilke trusler og trender som finnes på nettet i dag. Jeg skal forsøke å framlegge noen fakta som viser hvilken aktivitet, og i hvilket omfang disse aktivitetene utspiller på Internett.

2004 årsrapporten til SIS (Senter for Informasjonssikring) beskriver dagens trusler og trender. Rapporten forteller at det er en klar utvikling i retning av at sikkerhetsproblemer blir mer og mer utnyttet for økonomisk vinning. Produksjon av ondsinnet kode er ikke lenger en «gutteroms-aktivitet»; de som står bak er organiserte kriminelle og store pengebeløp er involvert. Ved hjelp av virus som spres via e-post blir flere og flere pc-er kompromittert og gjort til «zombier» eller «bots» og utnyttet til for eksempel utpressing. Ved hjelp av e-postmeldinger som tilsynelatende kommer fra nettbanker eller kredittkortselskaper («phishing»), blir brukere lurt til å gi fra seg navn og kredittkortnummer. Samtidig er «spyware», som avlytter passord og annen sensitiv informasjon, i all stillhet blitt installert på flere titusen pc-er (Norsis 2005).

3.4.1 Mørketallsundersøkelsen

Mørketallsundersøkelsen 2003 ble presentert 16. juni 2004 og omhandler både datakriminalitet og andre uønskede IT-hendelser. Rapporten er utarbeidet av Næringslivets sikkerhetsråd (NSR) i samarbeid med Senter for Informasjonssikring (SIS) og Økokrim. Resultatene fra undersøkelsen er dokumentert i en kortversjon hvor de viktigste resultatene er omtalt, eller i en

fyldigere versjon[13] hvor en kan lese mer om de enkelte funn samt sammenligninger med forrige undersøkelse i 2001 (Næringslivets sikkerhetsråd 2004).

Rapporten er utarbeidet på grunnlag av et spørreskjema som ble sendt ut til et representativt utvalg av 1 300 norske virksomheter, både offentlige og private. Totalt ble det samlet inn 722 svar. Spørsmålene i undersøkelsen gikk kort fortalt ut på hvilke tiltak de har satt i verk for å beskytte seg mot datakriminalitet, hvilke typer uønskede IT-hendelser de var blitt utsatt for og hvilke følger disse hendelsene har fått for bedriften.

I rapporten defineres *datakriminalitet* som straffbare handlinger der data eller en datamaskin er objekt for den straffbare handlingen. *Sikkerhetsbrudd* blir definert som hendelser som er forårsaket av at personell har brutt gjeldene sikkerhetsregelverk i virksomheten. *Uønskede hendelser* defineres som alle uønskede hendelser i en virksomhet, både uhell, ulykker, og tilsiktede handlinger.

Jeg mener en metodisk svakhet med denne rapporten er at den ikke klart definerer hva som menes med *datainnbrudd* og *forsøk på datainnbrudd.* For å få et klart svar på hva som menes med disse termene har jeg hatt e-post kontakt med Lillian Røstad fra Sintef, som var med å utarbeide rapporten. I en e-post forklarer hun at det er spesielt vanskelig å skille på gjennomført og forsøk på

[13] Kan bestilles på http://www.nsr-org.no

datainnbrudd. Men at med datainnbrudd menes at uautoriserte brukere får tilgang til et IT-system («system» brukes her i bred betydning – nett, applikasjon osv…). Et forsøk er et «ikke vellykket» innbrudd – dvs. at uautoriserte forsøkte å få tilgang men klarte det ikke.

Den såkalte Norman-dommen, som er en høyesterettsavgjørelse fra desember 1998 slår fast at en sjekk av hvilke tjenester en maskin på Internett tilbyr, ikke kan betraktes som et forsøk på datainnbrudd (Den Norske advokatforening 1998). Det betyr at det ikke er ulovlig å kjøre portscan-programmer, som normalt vil vise hvilke tjenester som går på spesielle porter på en datamaskin. Dette kan sammenlignes med å kjenne på dør for å se om den er åpen.

Mørketallsundersøkelsen fra 2003 viser blant annet at norske virksomheter ble utsatt for omtrent:

- 5200 datainnbrudd.
- 2,7 millioner forsøk på datainnbrudd.
- 150 000 virusinfeksjoner.
- 50 millioner forsøk på virusinfeksjon.

60 prosent av respondentene i undersøkelsen ble rammet av datakriminalitet eller andre uønskede IT-hendelser i 2003. Av 722 respondenter var det altså 433 virksomheter som var utsatt for én eller flere slike hendelser. Tall fra politiet viser at bare 187 tilfeller ble anmeldt. Bare 50 av datainnbruddene

(mindre enn 1 prosent) ble anmeldt. Så selv om virksomhetene kjenner til innbruddene velger de av ulike årsaker å ikke anmelde dem.

Siden mørketallsundersøkelsen ikke gir forklaringer på hvorfor så få virksomheter anmelder datainnbrudd, har jeg tatt kontakt med Universitetets senter for informasjonsteknologi (USIT) for å høre om deres erfaringer. Der snakket jeg med Knut Borge[14] og Are Garnåsjordet[15], som kunne fortelle at Universitetet sjelden anmeldte datainnbrudd. Noe av grunnen for at terskelen for å anmelde datainnbrudd er så høy, er i følge dem at det er nesten umulig å følge opp. Det kreves mye arbeid bare for å anmelde en hendelse og i tillegg har politiet lite ressurser til å følge opp en slik sak. For politiet kreves det mye arbeid med å kartlegge hva som har skjedd under et innbrudd og i de fleste tilfeller blir saken henlagt.

Spesielt angrep som kommer fra utlandet er svært vanskelig å oppklare da det må et internasjonalt samarbeid til for å etterforske saken. Kommer angrepet fra Norge og vi har en del opplysninger, er terskelen mindre for å anmelde, sier Borge og Garnåsjordet.

Mørketallsundersøkelsen viser at to av tre virksomheter vil få vesentlige problemer allerede etter én dag dersom de viktigste IT-systemene er ute av drift. Åtte av ti virksomheter har lagret verdifull informasjon elektronisk og ni av ti vil få problemer hvis informasjonen er upålitelig eller gal.

---

[14] Seksjonssjef for SAPP (System- og applikasjonsdrift) ved USIT.

Undersøkelsen viser altså at norske virksomheter er svært sårbare hvis bedriftens IT-systemer er satt ut av spill. Etter et datainnbrudd er oppdaget er det vanskelig å vite hva som faktisk har skjedd i virksomhetens systemer, og man vet ikke om man kan stole på den informasjonen som finnes i systemet. Det som gjerne er et stort problem er at virksomheten ikke vet hvilke handlinger inntrengeren har gjort, han kan for eksempel lagt inn en bakdør i systemet slik at han lett kan komme tilbake senere. Men det som er verre er at virksomheten ikke lenger kan stole på informasjonen som de har lagret. Ofte etter et innbrudd må de sette opp systemene sine på nytt og validere den informasjonen som de har i sine systemer. Det er dette som koster svært mye tid og penger.

Men det står derfor i skarp kontrast at bare hver fjerde virksomhet som ble rammet av datainnbrudd, kunne anslå hvor mye de hadde tapt. Undersøkelsen sier at det kun er 12 prosent som har rutiner for å beregne slike tap. Undersøkelsen anslår at det samlete tapet for norske virksomheter kan anslås til 5 milliarder kroner. 70 prosent av virksomhetene får ekstra arbeid på grunn av slike hendelser.

I undersøkelsen ser man at bare hver femte virksomhet som har vært utsatt for datakriminalitet, har greid å identifisere en gjerningsmann. For å få det til, må man vite hva som foregår i systemene. Selv om mange virksomheter logger aktivt, går mindre enn halvparten systematisk gjennom loggene. De fleste

[15] Gruppeleder for OS – Windows operativsystem ved USIT.

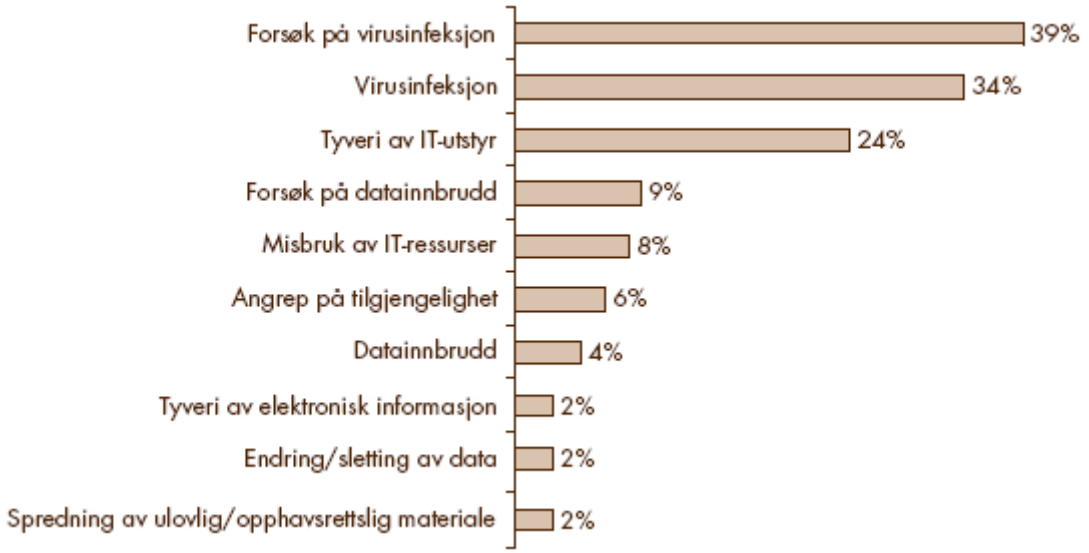
mangler rutiner for rapportering dersom de skulle avdekke en uønsket hendelse.

Undersøkelsen viser også at hver tredje virksomhet er trege med å oppdatere sin antivirusprogramvare, og like mange slurver med sikkerhetsoppdatering av annen programvare. Dette til tross for datasikkerhetseksperter og -firmaer stadig vekk forteller oss hvor viktig det er med jevnlig oppdatering av antivirusprogramvare og all annen programvare for å holde systemene sikre.

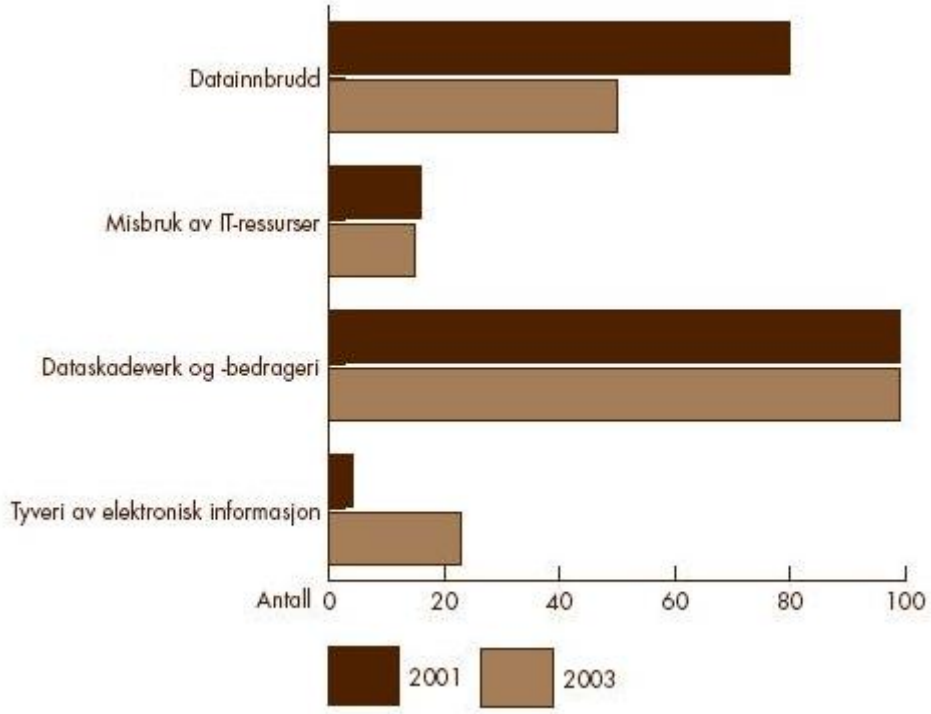
En annen oppsiktsvekkende statistikk fra undersøkelsen er at bare halvparten av virksomheter i helse- og sosialsektoren, som lagrer store mengder personopplysninger, ikke vet om de har vært utsatt for datainnbrudd eller datatyveri. Det kommer fram i undersøkelsen at sektoren bruker sikringsmekanismer som kryptering i langt mindre grad (13 prosent) enn andre sektorer. Til sammenligning bruker 40 prosent av virksomhetene innen bank- og finansnæringen kryptering.

Trådløse nett brukes av stadig flere, og i undersøkelsen kommer det fram at mer enn 30 prosent unnlater å sikre disse dataene med kryptering. Dette er også en trend som vi kan se igjen hos privatpersoner. I en artikkel i Aftenposten i april 2005 (Haugnes 2005) sier Eystein Kallhovde fra Oslo Prosjektservice at drøyt 20 prosent av alle hjemmene i Oslo har installert trådløse nett. Bare halvparten av disse er sikret. Disse tallene blir også bekreftet av markedssjefen i D-Link i samme artikkel. Dette er riktig nok bare tall fra Oslo, men jeg vil påstå at det er lite som tyder på at folk i andre deler av landet er flinkere til å sikre sine private hjemmenett.

Under har jeg lagt ved noen figurer fra mørketallsundersøkelsen 2003 for å vise en grafisk oversikt over noen av de viktigste resultatene fra undersøkelsen.



Figur 4: Andelen virksomheter utsatt for datakriminalitet og IT-sikkerhetshendelser. (Mørketallsundersøkelsen 2003)



Figur 5: Antall anmeldelser av datakriminalitet i 2001 og 2003. (Mørketallsundersøkelsen 2003)

Mørketallsundersøkelsen kommer ut annen hvert år og neste undersøkelse vil bli presentert i løpet av 2006.

Grunnen til at jeg har tatt med dette kapittelet om mørketallundersøkelsen er for å prøve å vise hvilket omfang datakriminalitet har samfunnet vårt i dag. Jeg ønsker å gi et bilde på hvilke problemer og kostnader crackere kan skape for virksomheter som blir offer for crackerangrep. Kanskje noen av mine funn fra datainnsamlingen kan være med på å forklare hvorfor crackere begår datakriminalitet og koster samfunnet så mye tid og ressurser.

3.4.2 Åndsverksloven

De siste årene har det vært mye snakk om den nye Åndsverkloven (ÅVL). Forslag til ny lov ble lagt fram den 11. februar 2005 av Kultur- og kirkedepartementet som har jobbet med en endring i åndsverkloven siden 2003 etter direktiv fra EU. Vårt medlemskap i EØS forplikter Norge til å gjennomføre endringer i denne loven. Ot.prp.nr. 46 (Kultur- og kirkedepartmentet 2005) ga et forslag om endringer i åndsverkloven, hvor det blant annet ble foreslått å fjerne retten til privat kopiering. Meningen var at det skulle bli straffbart å kopiere til privat bruk dersom verket var utstyrt med et «teknisk beskyttelsessystem» (DRM), ofte omtalt som «kopisperre». Ved å gi kopisperrer lovbeskyttelse ville departementet ta fra oss retten til å kopiere til privat bruk, og retten til selv velge hvilken plattform eller mediespiller forbrukerne kan spille av mediefilen sin på. Åndsverkloven omhandler mye mer enn kopisperrer, men jeg beskriver bare de delene av loven som jeg mener er relevant for min oppgave.

Loven er kontroversiell og har vært mye diskutert mellom platebransjen og opposisjonen som kjemper for vanlige folks rettigheter. Stridens kjerne er forbudet mot å kopiere musikk fra egne CD-plater med kopisperre til digitalt avspillingsutstyr. Samt at DRM-systemer avskjærer bestemte kundesegmenter (for eksempel Linux-brukere) fra å kunne kjøpe og nyttegjøre seg lovlige åndsverk som kan lastes ned fra Internett. Opponentene er uenige om hva som skal være lovlig og ulovlig.

Det finnes i dag flere DRM-systemer i bruk, men de mest kjente (og brukte) er knyttet til Microsofts (WM-DRM) og Apples (FairPlay). Begge disse systemene

forutsetter at man benytter programvare fra den som eier DRM-systemet for å kunne spille av DRM-beskyttet innhold. Microsoft og Apple ønsker henholdsvis å benytte mediaspillerene *Windows Media Player* og *iTunes* for å spille av DRM-beskyttet materiale.

Men det er ikke bare begrensingen til å velge plattform og leverandør som var problematisk med det nye lovforslaget. Digitale åndsverk kommer i dag enten på skrøpelige medier med begrenset levetid, eller som datafiler med en eller annen form for «beskyttelse». Lovforslaget ville altså verne om mekanismer som regulerer muligheten til å privatkopiere CD-/DVD-plater for brukere som ønsker å ha en kopi i tilfelle mediet blir ødelagt (noe som er fort gjort med optiske medier). De fleste produsentene legger sterke begrensinger på sikkerhetskopiering, noe som gjør det svært vanskelig for forbrukerne å ta sikkerhetskopier av CD-/DVD-plater eller datafiler som man har kjøpt som man har kjøpt på nettet. Skulle du så være så uheldig at harddisken din krasjet, ville filene dine være tapt og eneste mulighet for å få filene tilbake er å kjøpe dem på nytt.

Gisle Hannemyr mener at lovforslaget ikke primært var en *anti-pirat*lov, men en lov som skal hjelpe film- og musikkindustrien med å låse kunder til faste formater, segmenter markeder, og stenge ute uavhengige konkurrenter. I tillegg til at forbrukerne må kjøpe produktene sine flere ganger på grunn av inkompatible formater og lav levetid (Hannemyr 2005b). Hannemyr mener at forbrukerne blir taperne ved innføring av en slik lov og at det er de store markedskreftene som blir vinnerne.

Direktøren i foreningen for norsk platebransje, IFPI[16], Sæmund Fiskvik, er ikke like enig og ønsker den nye loven velkommen. Fiskvik mener at Norge trenger denne loven for å stoppe piratene som driver ulovlig musikkopiering. Han sammenligner det å bryte kopisperrer med å stjele. Fiskvik mener loven er en lov for fremtiden, når Internett blir verdens største markedsplass for musikk, film og spill. Han mener at loven ikke handler om MP3 og CD-plater, men om hvordan omsettingen av musikk på Internett skal reguleres. Det vil bli en maktkamp mellom artist/opphavmann, stat og forbruker mener Fiskvik.

Den 30. mai 2005 la kulturkomiteen på Stortinget fram sin innstilling til ny åndsverkslov (Familie- kultur- og administrasjonskomiteen 2005). I innstillingen går komiteen inn for at vanlige forbrukere fortsatt skal ha lov til å kopiere over musikk fra CD til digitale musikkavspillere – også fra CD-er med kopisperre. Men innstillingen slår også fast at det blir ulovlig å åpne effektive digitale sperrer som er lagt på digitalt innhold. Dette vil blant annet gjøre det umulig for Linux-brukere å spille av DRM-beskyttet materiale som brukes mye i lyd- og bildefiler fra giganter som Microsoft og Apple. Det vil være ulovlig å utvikle mediespillere som kan spille av et slikt materiale, noe som kan bety kroken på døren for de mindre aktørene i markedet.

Etter en lang om omstendelig prosess ble endringene vedtatt i en ekstraordinær sesjon i Stortinget lørdag 4. juni 2005. I følge Gisle Hannemyr (Hannemyr 2005a) er det forbrukerne og kunstnerne som er taperne av den nye loven. Vinnerne er de store selskapene som kontrollerer såkalte «tekniske

[16] International Federation of the Phonographic Industry.

beskyttelsessystemer», som regulerer bruken av åndsverk.

Hannemyr sier at DRM-systemene nå har fått et sterkere vern, som gjør at de store aktørene som Microsoft og Apple ikke trenger frykte konkurranse fra tredjeparter. For det eneste som dagens DRM-systemer i praksis gjør, er å forhindre at lovlig kjøpte verk blir avspilt på annet avspillingsutstyr enn det som produsentene ønsker. DRM-systemene avskjærer bestemte kundesegmenter fra å kunne kjøpe og nyttegjøre seg av åndsverk som lastes ned fra nettet mot betaling. Linux-brukere vil få det vanskelig å benytte seg av musikk- og filmbutikkene på nettet, da verket ikke lar seg avspille på denne plattformen.

Fiskvik synes det er greitt at den nye åndsverksloven tillater kopiering av egne kjøpte CD-er. Det som var viktig for platebransjen i den nye loven er at regjeringen tar fullt vern for DRM og filer som leveres på Internett. Han mener det må være lov å lage beskyttelsessystemer slik at ikke alle kan stjele musikken.

Et tankekors om bestemmelsen er at vernet av DRM-systemer fjerner brukernes mulighet til å velge programvare for en rekke daglige oppgaver. Jeg mener at dette kan synes å kollidere med moderniseringsdepartementets politikk for åpne standarder og muligheter for programvareselskaper som bruker åpen kildekode. Ved å beskyttet DRM-systemer har man tatt et steg tilbake i planen om å få det offentlige til å bruke åpne standarder.

Det er i dag mange forbrukere og forbrukerorganisasjoner, som for eksempel Elektronisk Forpost Norge, som er motstandere mot DRM-systemer og de dominerende aktørene bak disse systemene. Jon Johansen er en person som bruker mye tid å krefter på å kjempe mot de store selskapene som ønsker å binde forbrukerne til sine produkter. Johansen var med på å utvikle PyMusique, som omgår kopisperren på Apples musikknedlastningstjeneste iTunes. PyMusique knekker ikke DRM-systemet i iTunes, den bare leder musikken utenom programmet. iTunes sender filene uten DRM over nettet, og det er først når filen er lastet ned på brukerens pc at kopibeskyttelsen legges på. Det PyMusique gjør er at det overtar musikkfilene på pc-en før de plukkes opp av iTunes og dermed har Johansen og hans kompanjonger faktisk ikke brutt noen kopibegrensing, som åndsverksloven forbyr. Dermed er beskyttelsessystemet omgått og musikken er gjort tilgjengelig for brukere som har andre mp3-spillere enn iPod og andre operativsystemer enn Microsoft Windows og Apples Mac OS.

Noe av grunnen til at jeg tok med et avsnitt om den nye åndsverkloven, og da spesielt den delen som omhandler kopisperrer, er at loven var svært omdiskutert og fordi hackere som Johansen er opptatt av at en slik lov ikke skal begrense brukernes rettigheter. Den legendariske hackeren Richard Stallmann, som jeg har beskrevet tidligere i oppgaven, er også en aktiv motstander av proprietære standarder og åndsverkloven er et godt eksempel på hvilke verdier hackerne prøver å motarbeide. Faktisk har Stallmann og Free Software Foundation utarbeidet en ny versjon av GPL-lisensen som blant annet innholder motstand mot DRM-systemer. Et utkast av versjon 3.0 ble fremlagt i begynnelsen av januar 2006. Stallmann mener DRM er ondsinnet og at beskyttelsessystemet står i direkte opposisjon til hans egen organisasjon. Den nye GPL-lisensen skal forhindre at programvare skal kunne distribueres

med DRM under GPL. Hele utkastet til GPL 3.0 kan leses på hjemmesidene til Free Software Foundation[17].

3.4.3 Trender

I tillegg til de trendene og tallene som ble påpekt i mørketallsundersøkelsen, finnes det en del andre utviklinger de siste årene som er verdt å merke seg. På e-Crime Congress i London i begynnelsen av april 2005, sa Bors Miroshnikov fra K-avdelingen i det russiske politiet, at det pleide å være guttepøbler som drev med cracking. Nå har de imidlertid blitt voksne og skjønt at dersom man er flink til noe bør det brukes til å tjene penger. De cracker for å gjøre seg rike, og de organiserer seg i nettverk (Ilett 2005).

Dette er en trend som jeg tror vi kommer til å se mer og mer av i fremtiden. Det strømmer stadig mer penger over Internett og det blir stadig viktigere for virksomheter å være på nett. Bare noen få timers nedetid på nettsider eller andre virksomhetskritiske systemer, kan få store økonomiske konsekvenser. Dette vet ondsinnede crackere å benytte seg av.

Miroshnikov oppfordret til at man ble enige om internasjonale lover mot internettkriminalitet, slik at det blir enklere for politiet å sikte folk rundt om i verden. Først når regjeringene får internettoperatører, politi, offentlig sektor og

[17] http://gplv3.fsf.org/draft

privat sektor til å samarbeide, vil man kunne ha suksess med å stoppe denne typen kriminalitet, hevder Miroshnikov.

BBC (BBC News 2005) skriver i en artikkel på sine nettsider at en undersøkelse utført av Zone-H[18] viser at webserver angrep og nettside defacing[19] vokste raskt i 2004. Dette året vokste cracking av webservere med 36 prosent og nærmere 400 000 hendelser ble registrert. Dette kommer fram i en rapport som baserer seg på at et verdensomspennende nettverk av frivillige har sanket inn statistikk om ulovlige serverinnbrudd og websabotasje. Jeg mener at disse tallene viser at angrep på servere er et økende problem, noe som betyr at sikkerhetsbransjen har en utfordring i fremtiden.

3.4.4 Cracking teknikker

Det finnes mange metoder for å cracke systemer. Hvilken teknikk man bruker avhenger blant annet av hva som er motivet med angrepet. Metodene har forskjellig alvorlighetsgrad og noen av teknikkene krever mer kunnskap enn andre. Mange av teknikkene bruker ferdiglagde verktøy som raskt kan lastes ned fra Internett og brukes uten store datakunnskaper. Under har jeg prøvd å lage en oversikt over noen teknikker som finnes og hva de gjør.

[18] http//www.zone-h.org

1. Tilegne seg uautorisert aksess

Det finnes mange måter å uautorisert ta seg inn i datasystemer. Det kan være å knekke passord enten ved at man gjetter dem eller at man på tekniske måter greier å tilegne seg passord. En annen måte kan være å snike inn en trojan i offerets system som åpner opp systemet for folk som i utgangspunktet ikke skal ha tilgang. Dette kan gjøres ved å sende ondsinnet kode som vedlegg i en e-post. Offeret må imidlertid selv aktivere trojaneren som utgir seg for å være noe annet enn det den er. På denne måten lurer crackeren offeret til å gi ham tilgang til informasjon han ikke har rett til å se. En slik «bløff» er en måte å drive social engineering på som jeg omtalte i kapittel 3.3.4.

I noen tilfeller er det mulig å utnytte svakheter i *daemons* (tjenesteserver som kjører). Det finnes nok av systemer som ikke er «patchet» og som inneholder svakheter som bare venter på å bli utnyttet. Men kanskje den mest utspekulerte og enkleste metoden for å skaffe seg uautorisert tilgang til et system er å angripe hvor det er svakest. Ofte er det brukerne som regnes for å være det svakeste punktet ved et datasystem. Social engineering utnytter brukere av systemet til å gi fra seg sensitiv informasjon som for eksempel brukernavn og passord.

Tjenestenekting (DoS/DDoS)

Tjenestenekting er teknikk som kan forårsake stor skade, og det finnes flere forskjellige måter å gjennomføre et slik angrep. En måte er å overbelaste offerets nettverk ved å utnytte svakheter i nettverksprotokollene. Angriperen

[19] Defacement er i følge wikipedia at en hacker (cracker) erstatter innholdet på en original nettside med noe annet (Wikipedia 2005d).

oppretter da store mengder tilkoblinger til offeret slik at ingen andre kan koble til. Overbelastning av resurser er en annen metode som fungerer slik at man sender et stort antall pakker til offeret eller setter to tjenester opp mot hverandre for å bruke opp all minne og/eller prosessorkraft. En tredje måte er å overbelaste båndbredden til offeret. Ved å sende store mengder data til eller fra offeret gjør at det blir vanskelig å kommunisere med offeret.

3. Knekke serial-/lisensbeskyttelser

Nettet florerer av crackede spill og programmer. Dette er produkter som er tenkt solgt men som crackere (og andre) ønsker å benytte gratis. Mange produkter har en lisensnøkkel som følger med produktet. Dyktige crackere greier å skaffe slike koder enten på uærlig vis eller de modifiserer programmet ved å for eksempel hoppe over sjekken av lisenskode. Samme er det med trail-programmer[20] hvor man kan endre datoer i programmene slik at de virker utover en fastsatt periode.

4. Nettsider

Det finnes mange måter å ulovlig aksessere nettsteder på. *Bruteforce* er en automatisk metode hvor script sammenligner virkelig passord med en liste av ord. Metoden kan brukes til å knekke innloggingspassord men er tidkrevende og det er lett å bli oppdaget.

[20] Produkter som kan benyttes gratis i en bestemt periode.

Variable scope er en annen metode hvor variabler kan brukes andre steder enn de er tenkt til. Tidligere var dette en svakhet i skripspråket PHP, hvor bruk av globale variabler var aktivert som standard. Dette er lite hendig da alle variabler, uansett hvor de kommer fra, kan kalles fra hvor som helst. For at crackere skal kunne bruke denne metoden, må de få en slik variabel inn i systemet. Dette kan gjøres på flere måter. En måte er å sende variabler som input fra tekstfelter i skjemaer. Har utvikleren av systemet gjort en dårlig jobb, kan crackeren sende variabler inn i systemet som gjør at man systemet kan utnyttes. Denne metoden ligner på SQL-injection som jeg omtaler i slutten av dette kapittelet. En annen metode er å utnytte HTTP-protokollen for sending av skjemainformasjon. Sending av skjemainformasjon kan gjøres med to metoder, POST og GET. Hvis skjemaet er satt opp til å bruke GET-metoden, vil all informasjonen som sendes fra skjemaet vises i URL`en. Ved å editere informasjonen i URL`en kan crackere manipulere data som sendes inn i systemet.

Cookie- og sesjonskapring er metoder hvor man kaprer informasjonskapsler eller sesjoner. Dette er metoder hvor crackeren greier å utgi seg for å være en annen en den han er. Innholdet i cookies kan dekrypteres slik at uærlige personer kan få tilgang til informasjon de i utgangspunktet ikke skulle hatt. Crackere kan bruke snifferprogrammer på nettverk for å kapre sesjoner, men det er tidkrevende og lett for å bli oppdaget.

Sql-injection er en metode som utnytter svakheter i hvordan skript utfører spørringer mot en sql-database. På dårlig designede nettsider kan bestemte kommandoer sendes direkte inn i databasen som kan føre til at en uærlig person kan autentiseres mot serveren.

4. Forskningsmetode

Dette kapittelet beskriver forskningsmetoden brukt i dette studiet. Først introduseres metode generelt, deretter forklarer jeg litt om mine metodevalg. Videre skal jeg beskrive hvordan jeg har utført datainnsamlingen og analysen. Til slutt i dette kapittelet vil jeg kommentere noen av de hjelpemidlene jeg har benyttet under datainnsamlingen og analysen. Refleksjoner av arbeidet med metodene vil komme i slutten av oppgaven i kapittelet *Erfaringer* (kapittel syv).

4.1 Introduksjon

Det finnes mange ulike metoder man kan benytte seg av for å gjennomføre forskning og undersøkelser. Generelt sett kan man si at måten man velger å legge opp forskningen på avhenger av flere faktorer, blant annet hva vi vil undersøke, hvor lang tid vi har til rådighet, hvilke spørsmål vi stiller, hvordan vi stiller spørsmålene osv. De forskningsmetoder som velges vil være med på å bestemme hva man vil se eller oppdage. Vidt definert er «metode» en fremgangsmåte for å frembringe kunnskap eller etterprøve kunnskapskrav, dvs. påstander som framsettes med krav om å være sanne, gyldige eller holdbare (Tranøy 1986, s. 127). Metoder finnes på flere nivåer og jeg skal begynne med å presentere forskjellene på kvantitative og kvalitative metoder.

4.2 Kvantitativ vs. kvalitativ metode

Når man samler inn informasjon i en masteroppgave, har man behov for å systematisere, komprimere og bearbeide materialet slik at man kan besvare forskningsspørsmålene som er stilt. Metodene man har for å bearbeide informasjon, kan være alt fra statistiske metoder for å analysere informasjon i numerisk form (kvantitative metoder) til metoder for å tolke tekstmateriale (kvalitative metoder). Jeg vil ikke gå inn på en lang og detaljert utredning om forskjellen på kvantitative og kvalitative metoder, men nøye meg med en kort og enkel forklaring.

Cornford og Smithson mener *kvantitativ* forskning har som mål å fremstille tall og statistikker som kan benyttes til å beskrive det fenomen som studeres (Cornford og Smithson 1996). Slike data kan i etterkant analyseres ved hjelp av teknikker som statistiske analyser. De påstår at naturvitenskapen har hatt en kraftig innflytelse på den utbredte bruken av slike metoder innenfor sosialvitenskap generelt, og spesielt innenfor informatikken.

Kvalitative metoder definerer Cornford og Smithson som de metodene som prøver å unngå statistiske resultater og heller forsøker å fange og analysere (forstå) data (ibid). De mener kvalitative metoder gir forskeren mulighet for å beskrive fenomener på mer differensierte måter og at disse metodene benytter andre teknikker for å samle inn og analysere data. Kvalitativ forskning er mer basert på ord enn på tall. Historier og hendelser gir ofte et mer meningsfylt og konkret budskap til leseren enn masse sider med tall og statistikk kan gjøre. Ved kvalitative studier må forskeren bruke mye tid i felten for å samle inn store mengder med ustrukturerte data, for senere å prøve å analysere dem.

Problemstillingen min forteller at jeg ønsker å finne karakteristikker, motivasjoner og metoder, og til dette passer en kvalitativ metode bedre enn en kvantitativ. Derfor har jeg valgt å bruke en kvalitativ tilnærming. Ved å bruke kvalitative metoder skal jeg prøve å danne et bilde av helheten i temaet, i tillegg til å få med viktige detaljer. Jeg ønsker å gå i dybden i forhold til det temaet jeg ønsker å utforske, ved å innhente opplysninger fra et begrenset antall respondenter og fra sekundærlitteraturen. Det handler altså ikke om en måling, men om forståelse og tolkning. Målet er at denne metoden skal kunne hjelpe meg med å finne svar på den problemstillingen som er definert.

Utvalget av informanter jeg har intervjuet er valgt for å kunne presentere en faglig bredde innen temaet. Kvalitativ metode egner seg godt dersom man ikke på forhånd har helt klart for seg hva man ønsker spørre informanten om. Derfor har jeg brukt en intervjuguide (se Vedlegg C) som tar for seg de mest sentrale temaene. I tillegg til å snakke om temaene fra intervjuguiden stilte jeg også andre relevante spørsmål. All samtale fra disse intervjuene ble tatt opp for senere analyse. Denne måten å jobbe på er svært fleksibel og hvert intervju blir unikt. Ved å endre intervjuguiden etter hvert som kunnskapen og forståelsen øker mellom hvert intervju er det lettere å få den informasjonen man er på jakt etter.

4.3 Metoder for datainnsamling og analyse

I forrige kapittel tok jeg en beslutning om å benytte kvalitative studier for å oppnå en forståelse av hva som karakteriserer hackere og crackere. Det finnes imidlertid mange kvalitative metoder man kan benytte. Hvilke kvalitative

metoder jeg har valgt, hvorfor jeg har valgt de, samt hvordan jeg har benyttet de, vil jeg beskrive i dette kapittelet.

Innsamling av primærdata har foregått ved hjelp av halvstrukturerte dybdeintervjuer, samt uformelle samtaler, e-post utvekslinger, nettsamtaler, diskusjonsgrupper og telefonsamtaler. Hovedvekten har vært på de halvstrukturerte dybdeintervjuene hvor jeg har intervjuet personer med særlig kjennskap til mitt tema. De andre metodene for å samle inn primærdata har stort sett vært benyttet for å supplere dybdeintervjuene eller brukt der hvor dybdeintervjuer ikke har vært mulig.

Sekundærdata har jeg skaffet meg gjennom publisert materiale som bøker, artikler og informasjon fra Internett. Disse dataene var ment for å gi meg en bedre forståelse, men har også direkte vært benyttet under analysearbeidet.

Jeg har valgt å benytte *grounded theory* som en overordnet metode for å samle inn og analysere mine empiriske data. Jeg vil nå gi en kort innføring i hva grounded theory er, hvordan den er ment å brukes, samt hvordan jeg praktisk har benyttet den. Deretter vil jeg gå nærmere inn på de forskjellige metodene for å samle inn primær- og sekundærdata.

4.3.1 Grounded theory

Grounded theory er en metodologi for å oppdage teori ut fra empirien, teori som forklarer handlinger i den sosiale kontekst som studeres. Metoden er en induktiv form for emperibasert teoriutvikling som har utviklet seg innenfor sosiologien (Glaser og Strauss 1967).

Noe av det som kjennetegner grounded theory er at datainnsamling og analyse foregår parallelt ut i fra det syn at fortløpende sammenlikning av data genererer teoridannelse. I følge Glaser & Strauss er noen av de vanligste metodene for datainnsamling i grounded theory sosial interaksjon, feltstudier, deltakende observasjon og halvstrukturerte intervjuer. Samtidig som man samler inn data foregår det en konstant sammenligning av data som leder til koding og kategorisering av dataene, analysen. (Vil beskrive mer om hvordan dette foregår i neste subkapittel).

Grounded theory ble skapt av Glaser & Strauss på slutten av 60-tallet og i følge dem passer metoden bra å bruke på områder hvor det er gjort lite forsking fra før og der en muligens kan få fram nye aspekter ved et fenomen. Forfatterne ble senere noe uenige om teoriens utforming og begge har i ettertid kommet med egne utgivelser. Jeg har imidlertid basert meg på Glaser sin oppfattelse av metoden (Glaser 1998).

Jeg har valgt grounded theory som metodisk tilnærming, under noe tvil da jeg er en uerfaren forsker og det sies at grounded theory er noe vanskelig. Men jeg har valgt å prøve meg og tror denne metoden passer bra til det arbeidet jeg har

utført. Locke mener metoden passer bra til kvalitative studier, og hun nevner blant annet at metoden er egnet til å få fatt på kompleksiteten der handlingene finner sted (Locke 2001). Hun mener også at metoden er velegnet til å bygge bro mellom teori og praksis.

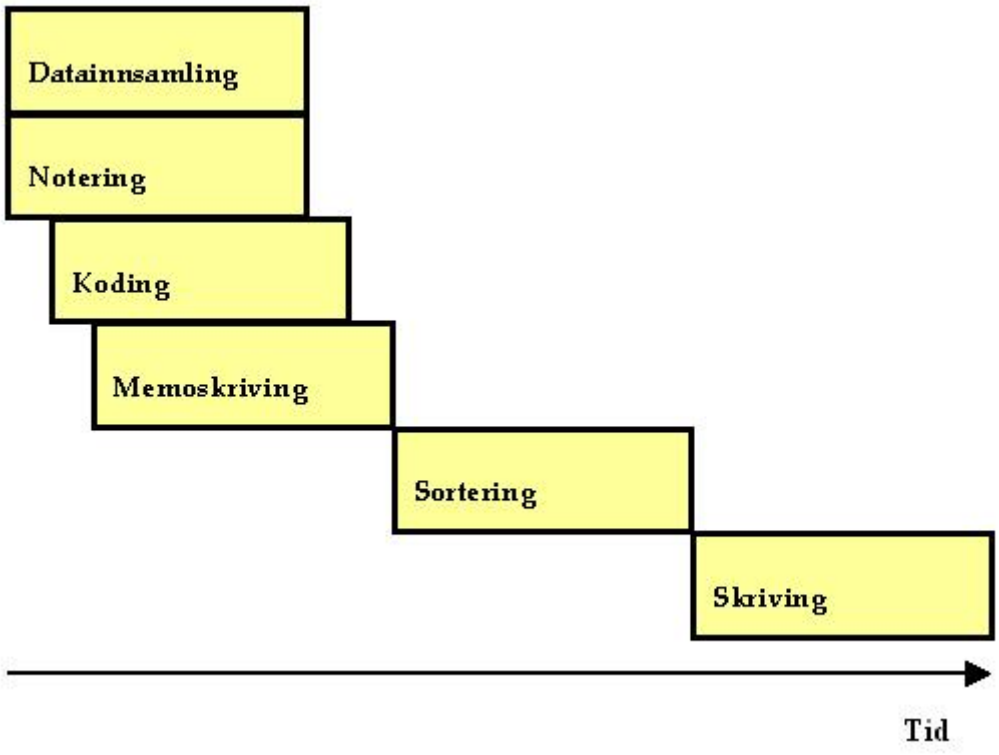
Noen av metodens sterke sider er at teorien er empirisk forankret («grounded»). Utrykket «grounded» vil si at teorien er basert på det empiriske materialet man samler inn. Etter hvert som forskeren samler inn data vil han oppdage ledetråder og ideer. Dette er et sentralt punkt i grounded theory. Samtidig som teorien vokser fram av data, så blir datainnsamlingen styrt av de data som fremkommer gjennom undersøkelsen, og derfor må datainnsamlingen og kodingen skje parallelt. Intervju og intervjuguide vil ofte måtte revideres underveis, noe jeg også har gjort.

Det som skiller grounded theory fra andre kvalitative metoder er at det ikke foreligger en teori eller en hypotese som skal bekreftes eller avkreftes. På grunn av dette kan ikke problemidentifikasjon skje på forhånd og forskningsspørsmålene kan heller ikke formuleres presist før undersøkelsen starter. Før jeg startet mine undersøkelser hadde jeg definert en problemstilling, som ga en viss ramme for hvilke forskningsspørsmål jeg kunne utforme.

4.3.2 Prosessen i grounded theory

Jeg vil i dette kapitelet gjøre rede for prosessen i grounded theory slik Glaser (Glaser 1998) og Dick (Dick 2005) beskriver den. Jeg vil så forsøke å relatere denne prosessen til hvordan jeg har benyttet meg av grounded theory.

Målet med grounded theory er å skape teori ut i fra empiriske data. Forskeren forsøker å forstå hva som skjer i situasjonen som undersøkes og hvordan aktørene utspiller sine roller. Figur 6 viser de forskjellige stegene i grounded theory;



Figur 6: Stegene i Grounded Theory, slik Dick fremstiller dem.

Første steg, *data innsamling*, kan være intervjuer, observasjoner og dokumenter som brukes i situasjonen. Men i følge Glaser kan nesten hva som helst være data til bruk i en grounded teoretisk metode. Etter hvert som man henter inn data, noterer man ned hovedpoengene, i *noteringsfasen.* Glaser anbefaler å ikke ta opp intervjuene eller ta notater under intervjuene. Han mener det tar for lang tid å bearbeide opptakene og at man opparbeider seg en bedre forståelse ved heller å gjøre flere intervjuer, hvor man i etterkant av intervjuene skriver ned hovedpoengene. Måten jeg har gjort det på er at jeg har tatt opp intervjuene for deretter umiddelbart skrevet ned stikkord fra intervjuene. I etterkant har jeg transkribert lydopptaket hvor jeg har tatt med de viktigste dataene. Grunnen til at jeg har tatt opp intervjuene, er at jeg da fullt kan konsentrere meg om å stille spørsmål og holde «flyten» i intervjuet istedenfor å måtte konsentrere meg om å ta notater.

Konstant sammenligning er det sentrale i hele prosessen. Til å begynne med sammenligner man dataene (for eksempel intervju med intervju). Av dette utvikles det raskt teori. Når teori har begynt å skapes, sammenligner man data med teori. Resultatene av denne sammenligningen skrives i margen på notatene som *koder*. Forskerens oppgave er her å identifisere kategorier (omtrent tilsvarende temaer og variabler) og deres egenskaper (som blir deres subkategorier). Etter hvert som jeg har sammenlignet intervjuer har jeg funnet ut hvilke temaer og variabler som er relevante og viktige å ta med i neste intervju. Mellom intervjuene har jeg gjort små endringer på intervjuguiden basert på erfaringene og sammenligninger av foregående intervju. Jeg skrev små notater fra sammenligningen av de innsamlede dataene som jeg la til grunn for neste intervju.

Etter hvert som man koder, vil man kunne se teoretiske temaer. Disse kan dreie som om forbindelser mellom kategorier eller om en kjernekategori; en kategori som virker sentral i prosjektet. Mens kategoriene og egenskapene oppstår, vil de og forbindelsene mellom dem produsere teori. Forskeren prøver da å skrive dette ned; *memoskriving*. Ettersom datainnsamlingen og kodingen pågår, vil kodene og memoene akkumuleres. Det er disse notatene som da danner grunnlaget for analysen av de empiriske dataene som jeg har samlet inn.

Glaser forteller videre at forskeren deretter vil plusse på det innsamlede materialet med såkalt *theoretical sampling,* teoretisk utvalg, som er et vanlig prinsipp hvor datainnsamlingen styres av den pågående analysen (Glaser 1998, s. 157). Meningen med dette er å øke bredden av det innsamlede ved å søke etter forskjellige egenskaper. Når kjernekategorien og dens forbindelser med andre kategorier når et slags metningspunkt, hvor lite nytt skjer (ingen nye kategorier og/eller egenskaper forekommer), så er det et tegn på at man går over i en *sorteringsfase*. Forskeren vil her gruppere memoene sine, like sammen med like, og så putte dem i en rekkefølge som forskeren mener best klargjør teorien. Sorteringsfasen gir et skjelett for skriving av analysekapittelet. Etter sorteringen går forskeren så inn i *skrivefasen*.

Grounded theory snakker om sosial interaksjon (*social interaction*), som er en prosess som skjer når mennesker handler i relasjon til hverandre (Glaser og Strauss 1967). Denne prosessen oppstår når mennesker møter andre mennesker i sosiale situasjoner. Sosial interaksjon blir beskrevet i grounded theory som en metode, på lik linje med halvstrukturerte intervjuer. Nettprat,

diskusjonsgrupper og e-post er kanaler som muliggjør sosial interaksjon og jeg har benyttet meg av alle disse kanalene.

Den sosiale interaksjonen på nettet er noe forskjellig fra dybdeintervjuene som jeg har hatt med informantene. Premissene er noe annerledes. Kommunikasjonen over nettet blir mer asynkron og upersonlig i tillegg til at den fremmer refleksjonen i ytringene, fordi refleksjon ofte krever tid og modning. I tillegg er et interessant aspekt ved denne snakkeformen at man ikke kan avbryte hverandre eller snakke i munnen på hverandre. Man kan også i etter kant se hva en selv eller andre har skrevet, ved at det logges eller lagres.

Dette er noen av de positive konsekvensene av nettbasert interaksjon, men det finnes også ulemper med å kommunisere på denne måten. Opplevelsen av nærhet svekkes selvsagt ved at kommunikasjonen/interaksjonen *bare* foregår skriftlig. Dermed forsvinner alle ikke-verbale elementer i normal sosial interaksjon. Dette kan lett føre til at man misforstår hverandre eller at viktige detaljer ikke oppfattes.

4.3.3 Dybdeintervjuer

Det kvalitative forskningsintervju er et åpent intervju hvor målet ikke er å styre informantens svar, men heller la intervjupersonene få svare så fritt som mulig. Når man skal samle informasjon gjennom et intervju er det viktig å tenke på to aspekter. Hvilken grad av standardisering og strukturering man

ønsker å ha på intervjuet. Grad av s*tandardisering* sier oss hvor mye ansvar som legges på intervjueren når det gjelder utforming av spørsmålene og den innbyrdes rekkefølgen (Patel og Davidson 1995). Dels må man tenke på i hvilken utstrekning intervjupersonen kan tolke spørsmålene fritt avhengig av sin innstilling eller sine tidligere erfaringer. Dette kalles grad av *strukturering* (ibid).

De kvalitative intervjuene jeg har gjennomført har vært halvstrukturerte og med en lav grad av standardisering. Det å ha en lav grad av standardisering gjør at jeg kan formulere spørsmålene ved intervjuene og stille spørsmålene i den rekkefølgen som passer en bestemt intervjuperson. Under intervjuene fulgte jeg intervjuguiden med temaer og spørsmål som jeg har supplert med oppfølgingsspørsmål. Det blir av den grunn ikke den «laveste» grad av standardisering.

Når det gjelder graden av strukturering, dreier det seg om hvilke muligheter til svarvariasjoner intervjupersonen får. Et kvalitativt intervju deles ofte opp i to typer; det halvstrukturerte intervju og det ustrukturerte intervju. Siden den ustrukturerte intervjuformen ligner mer en alminnelig samtale, valgte jeg den halvstrukturerte intervjutypen. Denne formen for intervju er delvis strukturert ved at man i forveien har formulert formålet med undersøkelsen. Det vil si at:

- Intervjuet fokuserer på bestemte temaer og det er gjort en begrepsmessig og teoretisk forståelse av temaet som skal undersøkes.

- Forskeren har også formulert spørsmålsstillinger, en intervjuguide, men man er ikke bundet til kun å holde seg til disse spørsmålene, da man kan utdype dem og stille uforberedte spørsmål.

I følge Kvale vil det være mest relevant å bruke halvstrukturert intervju når fokuset er et bestemt tema (Kvale 1997). Dette for å få de mest relevante, valide og gyldige svarene på problemstillingen.

4.3.4 Nettsamtaler (chat)

Etter dybdeintervjuer er nettsamtaler den metoden jeg har benyttet meg mest av for å samle inn primærdata. Det finnes mange måter og steder på veven hvor man kan chatte. I mitt tilfelle chattet jeg en del over IRC-nettverket. (IRC ble beskrevet i kapittel tre). Dette er et nettverk hvor alt fra nybegynnere til erfarne databrukere kommer sammen for å utveksle informasjon. På dette nettverket holder mange hackere og crackere til for å dele erfaringer og holde kontakten med miljøet. Det var viktig for meg å komme i direkte kontakt med hackere og crackere, men også være en passiv bruker som observerer hva som skjer på et utvalg av kanaler på IRC.

Til å begynne med var jeg opptatt å bli en del av miljøet på IRC. Jeg hadde en forestilling om at jeg ved å få nær kjennskap til miljøet kunne få et mer interessant datasett. Siden jeg var en relativt uerfaren IRC-bruker, var det viktig for meg å lære sjargongen og hvordan man oppfører seg på de ulike kanalene. Jeg ønsket å være ærlig og ville gi mine motivasjoner til kjenne. Når jeg innledet samtaler med personer (eller de med meg), informerte jeg dem om

at jeg var en mastergradsstudent som var på jakt etter informasjon til min oppgave. Dette opplevde jeg ikke som noe problem i forhold til de jeg snakket med. De menneskene jeg var i kontakt med på IRC var hjelpsomme og svarte som oftest villig på mine spørsmål.

Selv om denne måten å kommunisere på ligner mer på den muntlige samtalen enn for eksempel e-posten, er det flere ting som skiller den fra ansikt-til-ansikt-kommunikasjon. Den viktigste forskjellen er at kroppsspråket ikke kan brukes til å utdype meningen i det vi prøver å kommunisere. Det som i hovedsak kjennetegner chatternes måte å kommunisere på er bruk av korte (ofte ortografisk ufullstendige) setninger, akronymer og såkalte emoticons (eller smileys). Denne sjargongen har også flere likhetstrekk med tekstmeldinger på mobiltelefoner. Flere av kanalene på IRC kan ha en egen sjargong som kan være vanskelig å forstå for personer som kommer utenfra dette miljøet.

En fordel med å snakke med personer over nettet er at de kan opptre anonyme og at de av den grunn har lettere for å åpne seg og fortelle ting som de kanskje ikke ville fortalt om man hadde fysisk hadde truffet personen. Dette er noe jeg har fått erfare i praksis under mitt arbeid med oppgaven. Flere av de jeg har vært i kontakt med var villige til å diskutere temaer over nettet, men ønsket ikke å møtes fysisk.

4.3.5 E-post samtaler

E-postkommunikasjon er en type asynkron kommunikasjon, men langt mindre asynkron enn for eksempel formidling av tekst gjennom bøker. E-post gir mulighet for å rette opp og utdype argumenter på rimelig kort tid. Dette er en primærmetode som for meg blant annet har fungert som en forlengelse av intervjuene mine når det har forekommet uklarheter eller jeg har ønsket å stille noen oppfølgingsspørsmål i etterkant av et intervju. Men jeg har også benyttet denne metoden i forbindelse med sekundærdataene. Et eksempel på dette er da jeg gikk igjennom mørketallsundersøkelsen 2003. Her det dukket opp noen spørsmål som jeg ikke fant svar på, men som jeg fikk oppklart ved å sende e-poster til personene bak denne rapporten.

I tillegg til å fungere som en bra metode for å stille oppfølgingsspørsmål har e-post også vært et godt hjelpemiddel for å avtale intervjumøter.

4.3.6 Diskusjonsgrupper

Diskusjonsgrupper bygger på det samme prinsippet som e-post. Meldingene blir distribuert via e-posttjenere og sendt til den enkelte brukes innboks. I noen tilfeller blir meldingene også lagret på veven, som gjør at de som ikke tilhører gruppen/listen også kan lese meldingene. Forskjellen fra e-post er at en med slike grupper kan sende meldinger til mange mottakere på en gang, ved å sende til *en* gruppeadresse. Bruk av diskusjonsgrupper kan være bra hvis man ønsker å diskutere et tema i plenum eller ønsker å stille et spørsmål som er vanskelig å finne svar på.

Innsamling av data fra diskusjonsgrupper har vært brukt både som en primærmetode og sekundærmetode. Primærdata fra diskusjonsgrupper har jeg tilegnet meg hvor jeg selv har vært aktiv bruker av diskusjonsgruppen. Med aktiv bruker mener jeg at jeg selv har lagt inn innlegg og svart på andre sine innlegg i forumer. Sekundærdata fra diskusjonsgrupper har jeg innhentet ved å være en inaktiv bruker, og kun lest hva andre har ytret gjennom sine innlegg.

4.3.7 Litteraturstudie

Etter jeg hadde bestemt meg for tema for masteroppgaven, begynte jeg å samle inn sekundærdata om temaet. Jeg leste en rekke bøker for å øke min forståelse av temaet jeg hadde valgt, og for å finne ut hva som har vært skrevet om temaet før. Dette er noe jeg har fortsatt med under hele prosjektet, hvor jeg har lest bøker og annet publisert materiale som omtaler hacking og cracking.

En viktig del av det å kunne greie ut om en problemstilling er å studere tidligere forsking gjort om emnet. Ved å lese og analysere tidligere arbeid gjort på samme tema, øker man forståelsen for feltet problemstillingen befinner seg under. I mitt tilfelle fant jeg mange gode kilder som omhandlet noe av det samme som jeg har studert nærmere. Jeg opplevde at det var mange gode kilder som var relevant for min forskning, men at det var forholdsvis lite forskning/litteratur knyttet direkte mot min problemstilling.

Grounded theory handler om å oppdage ny teori og eksisterende litteratur behandles ikke spesielt av denne metoden. Men Glaser sier ikke at man skal unngå litteraturen, men at annen forskning og relevante felt kan innarbeides i analysen etter hvert (Glaser 1992). Poenget er å vente med å trekke fram litteraturen til en vet hvilken litteratur det viser seg å være relevant å benytte. «*The literature (...) will always be there. It does not go away!*» (ibid, s. 32).

Selv om jeg har lest litteratur gjennom hele arbeidet med masteroppgaven ventet jeg med å trekke inn relevant litteratur til jeg var i gang med analysearbeidet. Jeg har gjerne benyttet mer litteratur enn det grounded theory mener man skal, men jeg har fulgt Glasers anbefaling med å vente med å trekke den inn før det viser seg relevant.

4.4 Hjelpemidler

Opptak av lyd og/eller bilde kan være til stor hjelp for en forsker. Selv har jeg valgt å benytte meg av en digital lydopptaker hvor det har vært hensiktsmessig og godkjent av informanten.

Det er ofte en stor fordel å kunne ta opp et intervju som man senere hører på og transkriberer. Som intervjuer er det nesten umulig å få med seg alt som blir sagt eller gjort under et intervju. I tillegg er det lett å glemme deler av hva man har sett eller hørt. Ved senere gjennomgang av opptaket vil man lettere huske situasjonene og også lettere huske hva som ble insinuert, selv om ikke alt er med på opptaket. Det er for eksempel ingen lett oppgave å ta notater samtidig

som en/flere personer snakker samtidig. Det er ikke vanlig å ta hensyn til den som noterer, og dette er heller ikke meningen da det vil virke forstyrrende og fører til at intervjuet blir oppstykket og usammenhengende. Lydopptakene gjør at forskeren i ettertid kan sette seg ned i fred og ro for å gå igjennom intervjuet og dermed få med seg alt.

Hensikten med å transkribere et intervju som man har tatt opp er å ha en skriftlig oversikt over de viktigste resultatene fra intervjuene, slik at man skal slippe å måtte høre igjennom opptakene om igjen og om igjen.

4.4.1 Intervjuguide

Første utgave av intervjuguiden utformet jeg ganske tidlig i prosjektet. Selv om fokuset i oppgaven har forandret seg noe under arbeidet har intervjuguiden stort sett hatt det samme innholdet under hele prosjektet. For eksempel var jeg i begynnelsen av prosjektet usikker på hvordan jeg skulle definere en hacker og om jeg bare skulle ta med den negative siden av begrepet. Men som jeg skriver i kapittel tre skiller jeg på hackere og crackere og tar da med begge «sider» av dette fenomenet. Så noen justeringer på intervjuguiden har det vært underveis, samt at jeg har utformet tilleggspørsmål til hver informant.

Guiden består ikke av et fast antall spørsmål, men heller en rekke tema og spørsmål som jeg brukte som en veiledning under intervjuene. Mange av spørsmålene hadde jeg i hodet noe som gjorde det lettere å få intervjuet til å ligne en samtale. Siden jeg ikke var avhengig av å se på intervjuguiden og

følge den slavisk hele tiden, ble ikke intervjuet oppstykket og det var lettere for meg å stille oppfølgingsspørsmål. Intervjuguiden er lagt ved som «Vedlegg C».

4.4.2 Intervjuavtale

I forkant av intervjuene delte jeg ut en intervjuavtale som informantene måtte skrive under på. En kopi skulle beholdes av forskeren og en kopi til informanten. (Intervjuavtalen ligger vedlagt.) I avtalen opplyses det blant annet om at intervjuet vil bli tatt opp på lydbånd for deretter bli transkribert. Avtalen opplyser informanten om at transkripsjoner og lydbånd bare vil være tilgjengelig for studenten, veilederen og ekstern sensor. Etter prosjektslutt vil intervjumateriale bli destruert.

Intervjuavtalen fantes i to versjoner. Som jeg forklarte i kapittel to, er informantene delt opp i to utvalg, A og B (se «Vedlegg A» og «Vedlegg B»). En versjon av avtalen til hvert utvalg. Utvalg A av bestod av offentlige personer som enten var hackere eller personer med kjennskap til hacking og/eller cracking. Med deres tillatelse bruker jeg deres navn hvor det er naturlig.

Personer i utvalg B var personer som drev datakriminalitet eller som balanserte på grensen til datakriminalitet og er av den grunn anonymisert. Alle informanter og organisasjoner som har ytret ønske om det er behandlet anonymt i denne oppgaven. De fleste i utvalg B har jeg vært i kontakt med gjennom IRC. Alle personene jeg har snakket med her er anonymisert, det

samme er kanalene de oppholdt seg på. Dette fordi det ikke skal være mulig å spore informanten eller kanalen. Man skulle gjerne tro at brukerne på IRC er anonyme siden de opererer bak et kallenavn. Men mange av brukerne på IRC har gjerne hatt det samme kallenavnet i mange år og mange vet hvem som skjuler seg bak dette navnet. I tillegg er gjerne kallenavnet brukt i andre sammenhenger enn IRC og det er derfor ofte ikke noe stort problem å finne ut hvem som bruker dette kallenavnet. I tillegg består ofte kanalene av en fast «kjerne» av personer som kjenner hverandre. Ofte ønsker de å holde en lav profil slik at et lite miljø med samme interesser kan kommunisere sammen.

Begge utvalgene hadde en restriksjon som gikk ut på at informanten kunne reservere seg retten til å editere eller trekke tilbake intervjuet. I tillegg hadde utvalg B en restriksjon hvor informanten kan be om anonymitet, slik at ikke noe informasjon som kan identifisere personen eller hans/hennes tilknytning, brukes i masteroppgaven.

Min datainnsamling ha blant annet bestått av å intervjue personer som driver datakriminalitet og personer som ønsker å stoppe datakriminalitet. Dette for å få et innsyn fra begge sider og på den måten få undersøkt saken fra begge sider. Men jeg har ikke fått gjennomført dybdeintervju (med intervjuavtale) med personer som driver datakriminalitet. (Konsekvensene av dette vil jeg drøfte videre i kapittel fem).

5. Analyse og diskusjon

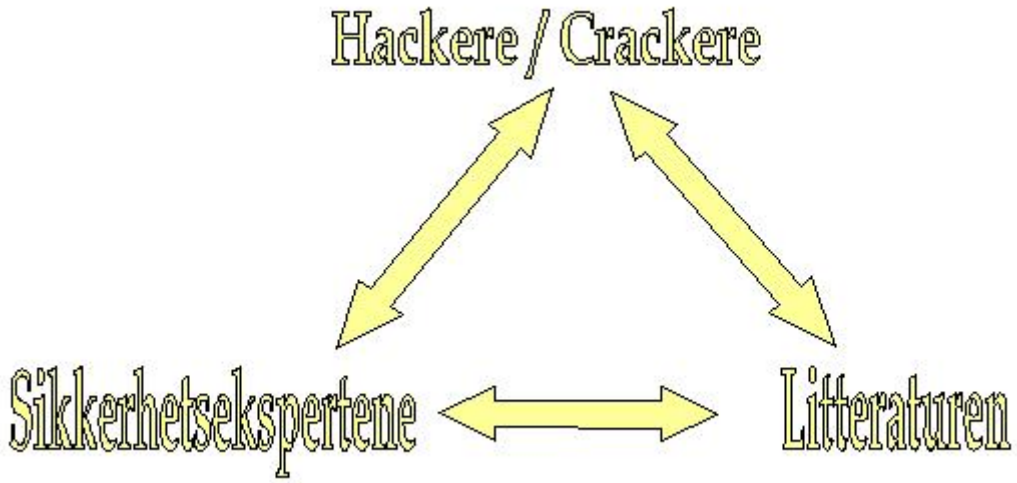
I dette kapittelet vil jeg presentere mine funn fra de empiriske dataene. På bakgrunn av teorien som tidligere er presentert vil jeg gjøre en beskrivelse av relevante data. Jeg vil gjøre en analyse av funnene, samt gjøre en tolkning hvor jeg drøfter mine data. Problemstillingen som jeg beskrev i kapittel en ønsker jeg å belyse og drøfte med bakgrunn i dataene jeg har samlet inn. Siden jeg ikke fikk intervjuet så mange informanter som jeg ønsket, kommer jeg i dette analysekapittelet til å trekke inn data fra sekundære kilder, i tillegg til primærdataene.

5.1 Introduksjon

Det finnes flere måter å presentere et analysekapittel på. Det er ofte vanlig med en tredeling av kapittelet; beskrivelse av data, analyse av data og tilslutt tolkning av data der analyseresultatene drøftes i lys av den teorien som benyttes. Jeg har med alle tre delene i mitt analysekapittel, men har valgt å ikke ha en slik klar tredeling. Istedenfor har jeg delt opp kapittelet i temaer basert på problemstillingen og presentert, analysert og tolket dataene fortløpende. Jeg synes det er en fornuftig oppdeling når jeg kan tolke funnene mine samtidig som jeg presenterer dem. Dette har jeg gjort for å få et mer sammenhengende analysekapittel.

Tolkningen min skjer ved at jeg sammenlikner likheter og forskjeller, samt kritiserer og diskuterer de ulike temaene. Dette gjør jeg ved å sette funnene fra

crackerne/hackerne, sikkerhetsekspertene og sekundærlitteraturen opp mot hverandre og se hva som er likt og hva som skiller seg ut. Dette har jeg illustrert i følgende figur:

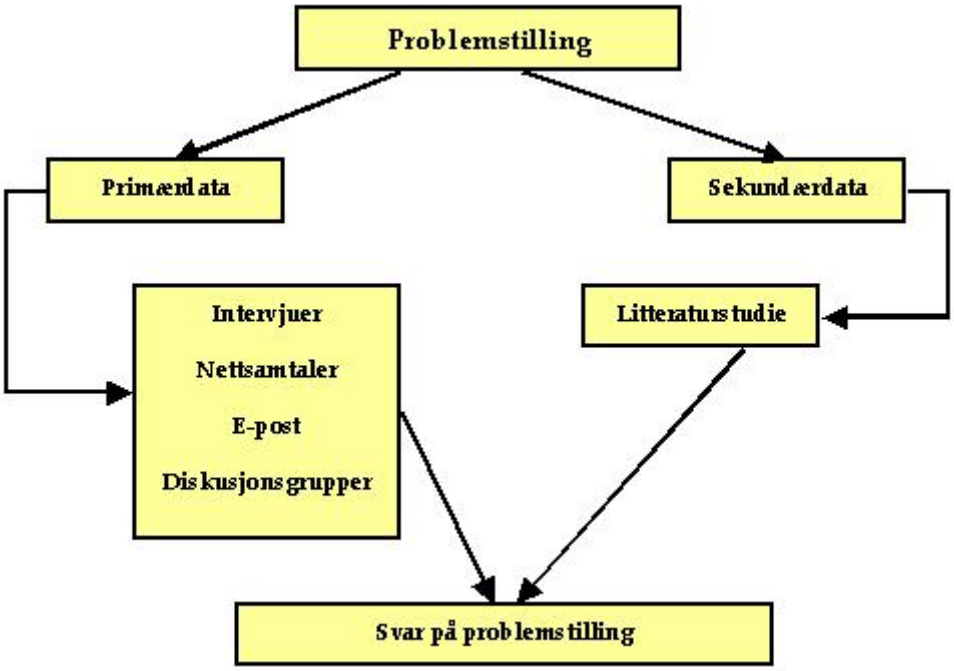


Figur 7: Kilder tolkningen baseres på.

Det som har vært viktig for meg er å alltid ha data for å kunne underbygge mine påstander, samt det å kunne skape sammenhengen mellom teori og empiri ved å referere til de teoretiske diskusjonene mine. Dette mener jeg selv jeg har fått til i teksten som følger i dette kapittelet.

Målet med dette kapittelet er å prøve å komme frem til et svar på det som er problemstillingen. I modellen på neste side har jeg prøvd å illustrere hvordan jeg har kommet fra problemstilling til konklusjonen på den. Utgangspunktet var å hente alle data fra primære kilder, men da dette ikke gikk som planlagt hentet jeg også inn data fra sekundære kilder. Med data hentet inn av meg og

data hentet inn av andre, har jeg fått nok informasjon til kunne presentere funn og gjøre meg opp noen konklusjoner.



Figur 8: Modell over mine datainnhentingsmetoder.

Analysefasen i dette prosjektet er den viktigste delen av oppgaven hvor det er meningen å ende opp med konklusjoner fra datainnsamlingen og gi et svar på problemstillingen. Etter å ha samlet inn mye data, satt jeg igjen med stort materiale som var vanskelig å få oversikt over. Jeg måtte derfor prøve å komprimere og systematisere for å gjøre dataene mine mer oversiktlig. Mye var allerede gjort ved at jeg hadde transkribert dybdeintervjuene og utelatt irrelevante detaljer derfra. Når jeg startet analysen fant jeg ut at det ville være lurt å klassifisere sentrale kategorier og nøkkelbegreper. Her var intervjuguiden til stor hjelp, siden den allerede inneholdt forskningsspørsmålene.

Jeg har brukt forskningsspørsmålene i intervjuguiden som et utgangspunkt, og de vil fremstå som et rammeverk for analysen. Intervjuguiden består av en rekke variabler som jeg valgt å benytte som analysekategorier. I analysen vil jeg ta for meg én kategori om gangen, slik at jeg får med meg alle de viktige delene fra intervjuguiden. Analysen er delt opp ved at jeg har brukt variablene fra intervjuguiden som overskrifter for kategoriene. I hver slik del skal jeg presentere, analysere og tolke dataene som jeg har hentet inn. Jeg ønsker å presisere at det er disse spørsmålene som skal resultere i et svar på problemstillingen.

Forskningsspørsmål som jeg ikke fikk belyst tilstrekkelig med data fra primærmetodene fjernet jeg eller supplerte med data fra sekundærlitteraturen. Om jeg fjernet dem eller hentet inn data fra sekundære kilder, var avhengig av om jeg så på spørsmålene som relevante eller lite relevante. På samme måte når jeg fant interessante funn i datamaterialet som belyste relevante spørsmål som ikke var stilt i problemstillingen, formulerte og inkorporerte jeg disse. På denne måten prøver jeg å skape samsvar mellom spørsmålene i problemstillingen og de funn og poenger jeg presenterer og diskuterer i analysen.

5.2 Sentrale kategorier

Dette subkapittelet tar for seg kategoriene fra intervjuguiden med funn, analyse og tolkning.

5.2.1 Hvordan forklares hacker- og crackerterminologiene?

I kapittel tre gikk jeg igjennom en rekke definisjoner på begreper som jeg finner relevante for denne oppgaven. I den delen av oppgaven presenterte jeg mitt syn på hvordan jeg har valgt å bruke disse begrepene. Jeg brukte mye tid på å forklare hvordan jeg tolker hva som er en hacker og hva som er en cracker. Det var ikke helt trivielt siden det fra slutten av 80-tallet har vært uenigheter og diskusjoner om hvordan man skal bruke disse uttrykkene. Det interessante under mine dybdeintervjuer har vært å høre hvordan informantene selv definerer og bruker begrepene.

Alle informantene som jeg har snakket med (jf. kapittel to) er klar over at det finnes forskjellige måter å definere termene på og at det er delte meninger om hvordan de brukes. Noen av informantene har en klar oppfattning om hva som er forskjellen på termene, mens andre mener det viktigste er å bruke en definisjon man kan forholde seg til og bruke denne konsekvent. For Christer Berg Johannesen er det viktig å gjøre et skille på hackere og crackere. Han definerer seg selv som en hacker; *«en datakyndig person som skrur og mekker og som ikke har noen skumle hensikter»*. Johannesen mener det er viktig å forstå hva som er forskjellen på en hacker og en cracker fordi hackere ikke fortjener å bli forbundet med noe kriminelt. Han oppfatter hackerne som personer som ønsker å gjøre verden til et bedre sted ved å forbedre datasikkerheten. Crackere oppfatter han som «bad guys», som ved hjelp av datamaskiner, utfører handlinger som er i strid med loven.

Den samme oppfattelsen har også Stein Møllerhaug. Sitat: «*Jeg ser på termene dit hen at forskjellen på en hacker og en cracker oppstår i det øyeblikket du bryter*

loven». En person som ved hjelp av datamaskiner bryter loven, defineres altså som en cracker i følge Møllerhaug. Jeg tolker synet på disse termene på samme måte som både Johannesen og Møllerhaug, slik jeg beskriver i kapittel tre. Jeg sa der at en cracker var en som oppnår, eller prøver å oppnå uautorisert tilgang til datasystemer, altså noen som utfører eller prøver å utføre kriminelle handlinger.

Stein Willassen har et litt mer avslappet forhold til hvordan man skal omtale hackere/crackere. Han er ikke så opptatt av hvordan man definerer dette, og ønsker å holde seg unna diskusjonen om det heter hacker eller cracker. Hos Økokrim kaller de det ikke hacker eller cracker, men gjerningsperson eller gjerningsmann. Willassen sier hacker og cracker er karakteriserende begreper, som egentlig er uviktig, det som er interessant er hvem som står bak et konkret forhold som er anmeldt.

Willassen konstaterer imidlertid at mange i datamiljøet bruker ordet cracker om personer som driver datakriminalitet, mens alle andre bruker hacker om det samme. Han forteller at når politiet er ute i media og snakker om cracking, så brukes ordet hacker fordi det er det vanlige folk forstår.

Etter å ha hørt hvordan Møllerhaug og Johannsen beskriver hackere og crackere var det et spørsmål som dukket opp; hva kaller man så en person som bryter seg inn i et datasystem, men med GODE hensikter? Har motivasjonen noe å si for hvordan man skal karakterisere en person? Johannesen påpeker jo at en hacker ikke har noen skumle hensikter, men defineres man fremdeles som en hacker så lenge personen ikke gjør noe skade under et datainnbrudd?

Hvordan skal man omtale en person som ønsker å kartlegge/forbedre sikkerheten i datasystemer ved først å bryte seg inn og deretter påpeke svakheter i systemet? Jeg stilte Møllerhaug dette spørsmålet, og han mener at man fremdeles er en cracker når man først tar deg inn på andres IT-systemer. Han forklarte at en rekke land ser utrolig strengt på dette og at de ikke skiller på gode og skumle hensikter. I forbindelse med dette spørsmålet fortalte han en historie fra USA som illustrerer dette godt;

> «En sikkerhetskonsulent hadde fått i oppdrag å teste sikkerheten på et system, et subnett. Han hadde fått godkjenning av testingen og skriftlig bestilling fra oppdragsgiver. Eneste problemet var at oppdragsgiveren hadde gitt han feil ipadresse, med de følgene at han testet et helt annet nettverk enn det han hadde avtale med å teste. Konsulenten fant flere sikkerhetshull og ble plutselig klar over at dette ikke kunne være riktig nettverk. Han kontakter da dette firmaet han har cracket og forteller dem at det har skjedd en feil, og at han har fått feil bestilling fra sin arbeidsgiver. Konsulenten forklarer problemet og fremlegger informasjonen han har funnet. Firmaet på sin side ser ingen andre muligheter enn å politianmelde saken. Finanslovgivningen i USA stiller krav om at en slik sak blir anmeldt. Konsulenten blir dermed dømt og får fire og et halvt år for cracking».

Historien som Møllerhaug forteller viser hvor alvorlig handling dette er om det kommer inn under USAs lovgivning. Den viser også hvordan en lovlydig hacker uheldigvis kan bli en cracker.

Jeg mener imidlertid at selv om crackeren har gode hensikter med sitt innbrudd, er han fremdeles uetisk og utfører en kriminell handling. Så lenge personen har brutt seg inn i systemet, mener jeg han bør stilles til ansvar for

sine handlinger. Det at han ikke hadde onde hensikter bør ikke legitimere crackerens handling.

Cracker#2 har en litt annen oppfatning på hva en hacker og cracker er i forhold til sikkerhetsekspertene. Han mener en hacker er en som er god å programmere, mens en cracker er en person som bryter seg inn på datasystemer. Cracker#2 påpeker imidlertid at man fint kan være både hacker og cracker. Slik jeg tolker Cracker#2 mener han at en hacker er en person som kan lage egne exploits og finne hull i programvare, mens en cracker ikke er like dyktig og bruker ferdiglagde verktøy. Han tar altså utgangspunkt i at både hackere og crackere driver med ulovligheter, og at det er ferdighetsnivået som skiller om man er en hacker eller cracker.

Cracker#3 deler samme syn som Cracker#2. Cracker#3 mener at en hacker har gode kunnskaper programmering for å kunne lage sine egne programmer og kompilere exploits. En god hacker bruker ifølge Cracker#3 ikke andre sine verktøy men lager det meste selv. Cracker#3 omtaler hackere som personer som driver datakriminalitet.

Dette viker fra hvordan sikkerhetsekspertene ser på termene. Det vil være umulig å sammenligne disse oppfattelsene opp mot litteraturen da den innholder mangfoldige versjoner om hvordan man skal bruke disse termene. Som jeg tidligere har skrevet brukes termene forskjellige fra miljø til miljø og er derfor vanskelig å sette opp mot hva informantene sier om bruken av termene.

5.2.2 Hvordan forklares hackernes/crackernes motivasjoner?

Motivasjonen til hackere og crackere er et kjernepunktet i denne oppgaven. Det er dette spørsmålet jeg har brukt mest tid og innsats på å finne ut av. Jeg har valgt å gjøre en grov oppdeling av de motivene som jeg har funnet under min datainnsamling for å kunne påpeke særegenheter ved de forskjellige motivene. En oppsummering av motivene som jeg presenterer under, kan ses i figur 9 på side 113.

Status

Willassen forklarer at Økokrim sin erfaring med datainnbrudd er at motivet er sosial omgang med andre på nettet, status i et miljø. Det er først og fremst i IRC-miljøene, hvor det å ha kontroll på en eller flere kanaler gir status. For å holde kontrollen på en kanal må du ha boter, og for å ha boter trenger du en maskin som står tilkoblet Internett hele tiden som du kjører botene på. Willassen forteller at det er vanlig å prøve å overta hverandres boter ved å kjøre DoS angrep mot hverandre. Dette vil da ramme de bedriftene som eier de maskinene som er kompromittert. I følge Willassen er inntrykket til Økokrim at de fleste datainnbrudd skyldes status i et miljø.

Hvorfor Økokrim har denne oppfatningen av crackere tror jeg er fordi det finnes veldig mange scriptkiddies som ønsker å vise seg frem. De er aktive i IRC-miljøer hvor status er en del av drivkraften bak handlingene. Mange av dem er unge gutter med begrenset datakunnskap, noe som gjør at de er lettere å oppdage og anmelde. Status i et miljø får man ved at flest mulig vet om hva du har gjort eller hva du er i stand til, og da følgelig lettere å anmelde.

Willassen nevner også at i warez[21]-miljøene kan motivasjonen for å gjøre datainnbrudd være ulovlig spredning av opphavbeskyttet programvare. Årsaken til at de bryter seg inn i andre datamaskiner er at det ikke er særlig lurt å dele denne typen programvare fra egen maskin da faren for å bli tatt øker betraktelig. Derfor kompromitterer de maskiner for å kunne spre ulovlig programvare fra disse. Status får de ved å vise andre at de har «kontroll» på en eller flere maskiner. Men det er ikke bare datainnbruddet i seg selv om gir crackerne status. Cracking av opphavbeskyttet programvare gir også status i miljøene. Willassen mener det er «konkurranse» i miljøene om å komme raskest ut med nye «cracks» (fjerning av kopibeskyttelsen).

Christopher Birkeland støtter oppunder oppfattelsen til Willassen. Han mener det finnes veldig mange scriptkiddies og at det er blitt en trend at disse cracker for å vise sine kunnskaper ovenfor sine kamerater. Kartleggingen som VDI foretar seg forteller at flesteparten av angrepene mot norske virksomheter følger kjente mønstre. Dette tyder på at det er noen som kjører ferdiglagde verktøy mot offentlig kjente svakheter i datasystemer.

Ut ifra hva informantene har fortalt under intervjuene og hva jeg har lest i sekundærlitteraturen, står statusmotivet som et sentralt motiv når det gjelder cracking. Dette motivet oppfatter jeg som litt «barnslig» da eneste grunnen for å bryte seg inn i systemer er å vise andre hva du er i stand til å gjøre. Statusmotivet kan man se tydelig på IRC hvor det oppholder seg store mengder scriptkiddies. Som flere av informantene nevner vokser mange av personene fra seg denne trangen til å «vise seg fram» og enten slutter helt med

21 Warez er et utrykk som betyr piratkopiert materiale.

å bryte seg inn i datamaskiner eller finner andre motivasjoner som er vanskeligere å oppdage. For mange er det en periode i livet som de går igjennom, mens for andre blir det en livsstil.

Når jeg spurte de informantene som cracket om hvilke motivasjoner de hadde, var det ingen av dem som nevnte motivet status. Dette tror jeg ikke er tilfeldig. Det er ingen som ønsker å innrømme at bakgrunnen for handlingene deres er å imponere andre. Det gjelder for kunnskaper i dataverden som ellers i livet; svært få av oss ønsker å innrømme at det er status vi vil oppnå ved å vise andre hva vi kan.

Økonomi

Møllerhaug nevner at profitt motivet står sterkt når det gjelder cracking. Han nevner blant annet utsending av spam som kan gi store inntekter til bakmennene. Møllerhaug gir et enkelt regnestykke på hva man kan tjene på å sende ut spam med en svarprosent på 0,2 prosent, og en produktkostnad på $20. Ved å sende ut 10 millioner e-poster, blir det fort penger av det. Normalt forbinder man kanskje ikke spam med cracking, men jeg mener man kan se på spam som informasjon man ikke ønsker og blir påtvunget av andre. Dessuten bruker spammerne kompromitterte pc-er for å sende ut spam. Eksempelet til Møllerhaug illustrerer uansett at det kan være penger å tjene på å utnytte personer og datasystemer.

Økonomimotivasjonen blir også bekreftet av Cracker#2 som sier at crackergruppen han er med i, har klare økonomiske motiver for aktivitetene

de bedriver. Under en samtale over IRC sier han at gruppen hans er ute etter å tjene penger på sine aktiviteter ved å endre databaser de har kompromittert. Cracker#2 sier at motivasjonen først var å ha det gøy og å lære seg mest mulig om hvordan man sikrer seg selv mot angrep. I ettertid har de funnet ut at man kan tjene penger på sine aktiviteter ved å kompromittere og endre databaseservere hos banker og gamblingfirmaer på nettet.

Tron Øgrim mener også at det finnes økonomiske motiver bak cracking. Han mener man bare har sett begynnelsen. Stadig mer penger knyttes til Internett og da knyttes også flere kriminelle Internett, mener Øgrim. De kriminelle flytter seg etter hvor pengene er, og i tiden fremover vil vi oftere se crackere som er ute etter penger, forklarer Øgrim. Med de økende pengebeløpene på Internett og gode sikkerhetsmekanismer vil du få forskjellige former for cracking. Et faremoment er når sikkerhetsmekanismene blir for gode. Da vil forbryterne gå på deg som person framfor å angripe systemene. Et eksempel på dette er utpressing.

Birkeland nevner nettopp utpressing som økonomiske motiver for enkelte crackere. Han gir eksempler på hvor crackere krever penger fra en virksomhet og får de ikke det, krasjer de virksomhetens systemer. Her ser vi utviklingen fra gutteromsaktiviteter til organiserte kriminelle på jakt etter penger, sier Birkeland. Dette ble også påpekt som en trend på e-Crime Congressen som jeg omtalte i kapittel 3.4.3.

Dette er en utvikling som viruseksperten Eugene Kaspersky forklarer med at organiserte kriminelle har tatt over virusindustrien, og at disse personene er

innrettet mot å tjene penger (Rossen 2005). Kaspersky forteller at det ikke er innbringende å infisere millioner av pc-er og provosere virusverner, politi og etterretning til å bruke store ressurser på oppsporing. Derimot er det svært innbringende å raskt kunne opprette zombie-hærer på opptil 10 000 pc-er for å leie dem ut til spammere eller bruke dem til distribuerte tjenestenektangrep.

En annen side av organisert datakriminalitet er industrispionasje som er en alvorlig forbrytelse og som kan gi uærlige personer fordeler og fremtrinn. Ved å bryte seg inn i datasystemer kan crackere få tilgang til informasjon som de kan utnytte, enten som et konkurransefortrinn eller ved å selge sensitiv informasjon videre. Johannesen mener det hører med til sjeldenhetene at noen har slike skumle hensikter, men at det må tas alvorlig. Det er et fåtall personer som bruker store ressurser på å gjennomføre slike innbrudd.

I følge en rapport utarbeidet av Verisign er penger motiv for stadig flere dataangrep (Verisign 2004). I rapporten fremgår det at angrepene blir stadig mer sofistikerte og at det er dårlig sikrede hjemme-pc-er som blir angrepet. Målet for angrepene er i følge rapporten å tjene penger enten gjennom utpressing, kredittkortsvindel eller inntekter fra spam.

Det er altså helt klart at enkelte crackere har økonomiske motiver bak sine handlinger. Det som er interessant å se er hvor målrettet og bevisst den økonomiske motivasjonen er. Som Cracker#2 sier det, så kom det økonomiske motivet først etter hvert. Interessen for datasikkerhet gjorde at det var lett å «gå et steg videre». Når crackergruppen hans først han kompromittert en maskin hvor man lett kan skaffe seg ekstra penger, er ikke steget langt å ta.

Møllerhaug, Øgrim og Birkeland beskriver mer ekstreme og målrettede crackingmetoder for å skaffe seg økonomiske goder. I deres eksempler fortelles det om forbrytere som ikke skyr noen midler for å oppnå sine mål (spammere, utpressere). Det blir straks mye verre da motivet utelukkende blir å tjene penger på datainnbrudd.

Slik jeg tolker tilbakemeldingene fra alle informantene gir de et unisont uttrykk for at det i dag finnes mange personer rundt om i verden som ønsker å tjene penger på sine skumle datakunnskaper. Informantene er enige om at dette bare kommer til å bli verre i tiden som kommer. Denne tendensen har vi også sett media rapportere mye om den siste tiden. Stadig oftere hører vi eksempler på svindel hvor phishing er en metode som benyttes flittig.

Jeg tror at det nå er viktig for programvareprodusentene å ta datasikkerheten på alvor slik at ikke vanlige forbrukere ikke mister all tiltro til Internett og de systemene som benyttes her.

Politikk og ideologi

Møllerhaug nevner idealisme som en viktig motivasjon for mange crackerne. Han mener at organisasjoner som pådrar seg forskjellige aktivisters vrede, får en ganske markert økning i anslagene mot seg. Et eksempel han nevner er abortmotstandere som angriper systemene til abortklinikkene for å få vise sin motstand mot abort. Et annet eksempel på politiske motiver tok jeg opp i kapittel tre hvor jeg fortalte om hacktivistene som ved hjelp av DDOSing blant annet protesterte mot Mexicos regjering for undertrykkingen av

Chiapasindianerene. Her bruker hacktivistene sin politiske overbevisning som motivasjon for å kjempe mot saker de er uenige i eller som de oppfatter som urettferdige.

Politiske motiver finner vi også bak handlingene til Jon Lech Johansen. I et intervju med Slyck.com utrykker han helt klart idealistiske meninger om ting som opptar han (Mennecke 2005). Blant annet svarer han på hva som var motivasjonen bak programmet DeCSS, som han forklarer med et ønske om å kunne spille av DVD-er på den måten han ønsker. Han uttaler at han ikke ønsker å bli tvunget til å bruke bestemte operativsystemer eller avspillere, men heller selv bestemme hvordan han skal spille av DVD-plater. Johansen liker heller ikke å bli tvunget til å se reklame på DVD-plater han selv eier. Gjennom slike uttalelser utrykker Johansen klare politiske motiver bak sine handlinger. Han ønsker selv å bestemme hvordan han benytter sine egne eiendeler, og ønsker å være lovlydig. Johansen har tidligere uttalt; «*Jeg ville ikke gjøre noe ulovlig. Jeg ville bare se film på PC-en min [...] Det er galt å kopiere. I hvert fall for salg. Men kunnskapen om hvordan du gjør det, kan ingen forby*» (Neset 2000). Dette sitatet fra Dagbladet utrykker kort og godt Johansens motiver og hva han selv mener han er berettiget til å gjøre.

Jeg vil kalle Johansens arbeid for hacktivisme. Johansen har klare politiske motiver bak sitt engasjement mot de store markedsaktørene som ønsker å binde forbrukere til bestemte formater. Han er en tilhenger av fri konkurranse og at man selv skal kunne velge mellom de ulike tilbud som finnes. Proprietære standarder er han motstander av fordi de låser forbrukerne til en spesifikk plattform eller produkt.

Kanskje de mest farligste idealistiske motivasjonene som noen besitter og som vi kommer til å se mer av i tiden fremover, er terroristene. De har sterke politiske motivasjoner som de er villige til å gå langt for å gjennomføre. Terroristene bruker da Internett som et verktøy for å gjennomføre ekstreme handlinger. Når stadig flere livsviktige og kritiske systemer i samfunnet kobles til nettet, må man være klar over at dette kan være potensielle terroristmål. Jeg tenker da for eksempel på systemer som forvalter strøm og vann og systemer for samferdsel og helse. Eksempler hvor terrorister har angrepet slike systemer har man ikke sett mye til heldigvis, men jeg tror det er en trussel som bør taes alvorlig.

Richard Stallmann er en mann som ikke legger skjul på at utvikling av programvare handler om ideologi. Det er nærmest «religiøse» takter over det Stallmann står for når det gjelder utforming og spredning av programvare. Stallmann har en sterk overbevisning om at all programvare som skal benyttes bør være fri. Han beskriver kampen mot proprietære systemer som en tøff kamp mot sterke rivaler, men påpeker at han selv og de som er enige med han er villige til å ta opp kampen. Drivkraften til Stallmann gjenspeiler seg i de politiske standpunktene han står for.

Interesse for datasikkerhet

Møllerhaug mener det er mange som hacker/cracker for den tekniske interessen. Interessen for datasystemer og fokuset på datasikkerhet er drivkraften som ligger bak mange hackere og crackere. Om man da hacker eller cracker bestemmes da av om man hacker egne systemer eller systemer hvor tillatelse er gitt eller om man tar seg inn i andres datasystemer.

Cracker#1 gir den samme begrunnelsen. Han brøt seg inn i en virksomhets billettsystem fordi han oppdaget en svakhet ved systemet ved en tilfeldighet. Han ønsket å teste dette mer og sjekke hvor dårlig sikret systemet egentlig var. Han kunne fortelle meg at dette kun var fordi han var svært opptatt av datasikkerhet og at han studerte datasikkerhet. Det han gjorde var å gjøre en enkel SQL-injection[22] mot en Oracle database. Han mener det er allmennkunnskap for alle som har programmert mot Oracle databaser, og utviklerne av systemet viser et klassisk eksempel på programmeringsfeil av verste sort.

Johannesen faller også under interessemotivet. Han ønsker å gjøre verden til «et bedre sted» ved å forbedre sikkerheten i datasystemer. Interessemotivet er den viktigste motivasjonen crackere har mener Spafford i artikkelen *Are computer hacker break-ins ethical?* (Spafford 1992). I følge Spafford er den vanligste motivasjonen for datainnbrudd at personene bak innbruddet ønsker å illustrere sikkerhetsproblemer for et miljø som ellers ikke vil bryr seg om problemet. Men som Spafford sier i artikkelen; «*folk som ønsker å rapportere et sikkerhetsproblem, trenger ikke utnytte svakheten i systemet for å rapportere det*». En analogi til dette er at man setter ikke fyr på det lokale kjøpesenteret for å påpeke brannfaren i en av butikkene, for deretter å påstå at brannmennene ellers ikke ville ta brannsikkerheten på alvor.

Når jeg snakket med Willassen i politiets datakrimsenter, fortalte han at mange av gjerningspersonene bak datakriminalitet oppga utforskning som motiv for

[22] Teknikk som brukes for å utnytte svakheter i Web-applikasjoner som benytter databaser.

sine handlinger. Men dette sa han ikke var deres erfaring. Han sa at deres erfaring var at motivet for datakriminalitet var sosial omgang med andre på Internett. Willassen mente at crackerne oppga utforskning og interesse som motivasjon, men at det egentlig var status som lå bak. Dette gjaldt først og fremst i IRC-miljøene der det å ha kontroll på en eller flere boter gir status.

Cracker#3 er en person som tidligere hadde egen kanal på IRC med crackede boter. Men motivasjonen som Cracker#3 oppgir til meg samsvarer ikke med hva Willassen sier. Cracker#3 oppgir motivasjoner som ønske om å utvikle sine ferdigheter, lære noe nytt og mestre utfordringer. Willassen oppgir at Økokrim har erfaring med at det er status som driver crackere. Cracker#3 taler Willassen imot ved at han forklarer at det er interessen for å lære som driver han.

I følge Spafford (Spafford 1992) er det enkelte inntrengere som hevder at de ikke gjør noe skade, det eneste de gjør er å lære mest mulig om hvordan datamaskiner fungerer. Crackerne argumenterer med at datamaskiner er dyre og at de utvider sin kunnskap på en kostnadseffektiv måte. Da kan man bruke analogien om at det ville vært det samme som at jeg tjuvlåner bilen din, fordi jeg selv ikke har råd til en, for å lære meg å kjøre.

Hevn

Et annet motiv som Møllerhaug nevnte under intervjuet var ansatte som hevner seg på arbeidsgiver, enten fordi de har fått sparken eller fordi de er misfornøyd med sin egen situasjon i bedriften. Møllerhaug nevner eksempler

på IT-sjefer som får sparken og deretter bruker sin kunnskap om bedriften til å sabotere systemene. Dette er jo et tankekors hvis IT-sjefene cracker egen bedrift. IT-sjefene sitter gjerne med rettigheter til det meste og er gjerne de som overvåker systemloggene, slik at det nesten er umulig å oppdage.

Willassen tar også opp denne problemstillingen med at ansatte i en bedrift ønsker å få tak i informasjon de ikke har tilgang til. Bakgrunnen kan være at det har vært en konflikt på arbeidsplassen og den ansatte enten er sagt opp eller har sluttet. Motivet kan da være ren hevn eller økonomisk. Den ansatte starter konkurrerende bedrift og bruker kunnskapen han besitter mot sin gamle arbeidsgiver eller passord han kjenner til å bryte seg inn i bedriftens systemer.

En amerikansk undersøkelse utført av US Secret Service og US CERT viser at personlig hevn er den vanligste motivasjonsfaktoren for cracking av firmaer (Keeney et al. 2005). Ut ifra informantene som jeg har intervjuet har ikke jeg den samme oppfattelsen av at dette er den største motivasjonen for cracking. Av informantene som jeg snakket med var det kun Møllerhaug og Willassen som tok opp denne motivasjonen og i litteraturen har jeg sett lite eksempler på dette. Noe av forklaringen til at mine data avviker fra den amerikanske undersøkelsen kan være at slike angrep er vanskeligere å oppdage da angriperen ofte har god kjennskap til systemet og rettigheter på systemet. Det kan av den grunn være vanskeligere å oppdage. Men det er også sannsynlig at denne hevnmotivasjonen ikke kom like godt fram fra mitt arbeid fordi jeg hadde et lavt antall informanter.

Andre motiver

Jeg har allerede snakket om interessemotivet som Spafford tar opp i artikkelen «Are Computer Hacker Break-ins Ethical?» (Spafford 1992), men han nevner også flere motiver. Dette er motiver som jeg selv ikke har erfart fra min egen datainnhenting, men som jeg tar med for å vise at det finnes flere motiver for hacking og cracking enn det jeg har samlet inn fra informantene. Årsaken til at jeg ikke har erfart disse motivene fra min egen datainnsamling kan være at jeg kun har et fåtall av informanter.

- **Utnyttelse av ledige maskinressurser**

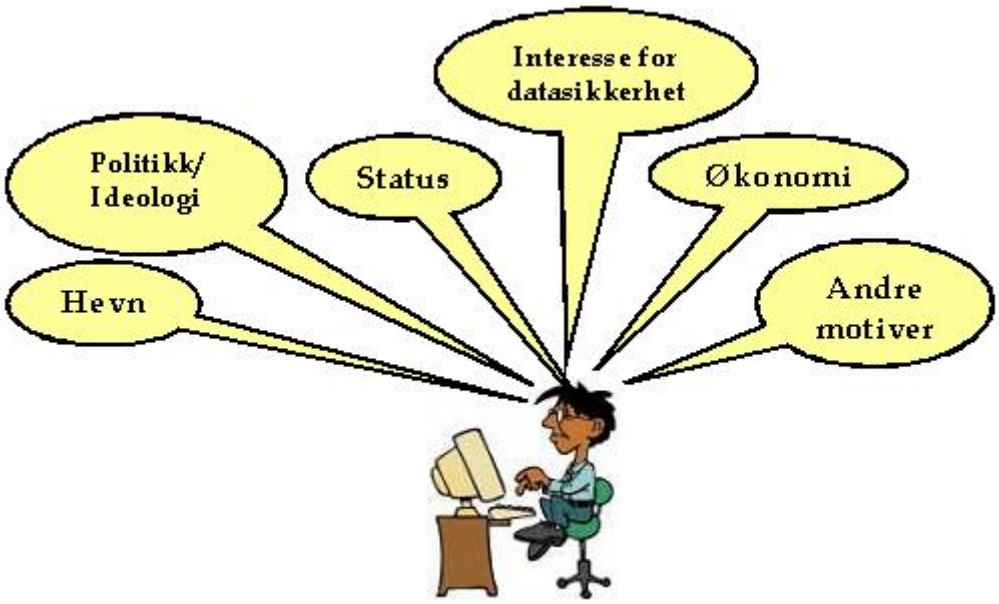
En motivasjon som ligger bak datainnbrudd er i følge Spafford at crackere ganske enkelt bare utnytter ledig maskinressurser. Crackerne mener at siden systemene på langt nær brukes i nærheten av hva de har kapasitet til, er crackerne berettiget til å bruke dem. Det kan være flere grunner til at crackerne ønsker å bruke maskinressurser på andre maskiner. Lagringskapasitet kan være en av grunnene. Crackerne kan for eksempel bruke kompromitterte maskiner som lagringsplass for data de ønsker å dele med andre. En annen forklaring kan være at crackerne ønsker å skaffe seg ekstra maskinressurser for å holde kontrollen på pratekanaler på IRC. Mange virksomheter har servere med høy oppetid og kraftige linjer, noe som kan virke fristende for crackere. Jeg er enig med Spafford at dette er et tåpelig argument. Det er det samme som om noen skulle lånt bilen din når du selv ikke bruker den.

- **Sosial beskytter**

En annen motivasjon som Spafford nevner er at crackere bryter seg inn i systemer for å hindre misbruk av data. I den forbindelse blir crackeren en

sosial beskytter fremfor en kriminell. Selv om datainnbrudd ikke kan forsvares viser i alle fall dette motivet at ikke alle crackere er ute etter å lage kvalme, men at det finnes personer som ønsker å gjøre noe positivt, tross datainnbrudd.

Motivene som jeg fant under datainnsamlingen og som jeg nå har presentert har jeg prøvd å illustrere og oppsummere i figuren under. Figuren oppsummerer bare motivene og sier ingenting om noen motivasjoner i større grad enn andre. Etter å ha presentert motiver i dette kapittelet, kan jeg si at flere av dem henger tett sammen og at hackerne og crackerne gjerne har flere motvier.



Figur 9: Motivasjoner fra mine funn og sekundærlitteraturen.

5.2.3 Hvordan ser hackerne/crackerne på sin egen aktivitet? Moraler/normer?

Møllerhaug sier at hackeretikken ikke er like gjennomført i dag slik den var tidligere. Han mener mye av dette har med å gjøre at crackingen er mindre personlig nå enn tidligere. Dette illustrerer han med følgende metafor; «*hvis du skal skyte en person, og stikker pistolen mellom øynene hans og trekker av, så er det en veldig stor psykisk belastning. Hvis du derimot sitter i et bombefly ti tusen meter over bakken og slipper bomber, er ikke det den samme belastningen*». Møllerhaug mener at mye av det som gjorde at crackerne beholdt sin etikk var at en slags nærhet og et behov for å rettferdiggjøre det de gjorde. Nå har de fått en veldig stor fjernhet i forhold til de IT-systemene de bruker og tar seg inn på. Han mener dermed at deler av denne etikken er i ferd med å vannes ut.

Dette er også en utvikling som Willassen har merket seg. Crackere, og da særlig scriptkiddies, vet at det de gjør ikke er lovlig, men det som kanskje er farligere med denne gruppen er at de ikke skjønner konsekvensene av aktivitetene de bedriver. Willassen mener de får et abstrakt forhold til det de holder på med. Det er liksom ikke det samme som å gå rundt i byen med brekkjern og bryte seg inn i hus. For mange kan det bli som et dataspill, og de forstår ikke konsekvensene for de som blir rammet.

Ut i fra Økokrims synspunkt, vet personene som cracker at de gjør noe ulovlig. Erfaringer som Willassen har gjort seg tyder på at personene som driver datakriminalitet vet at de gjør noe galt, men at de så nekter for forholdene i avhør.

Det samme synet deler Øgrim. Han ser på hackere og crackere som nyttige. Øgrim mener at den typen cracking som har til hensikt å se om systemene fungerer og som ikke motiveres av vinnings hensikt, bør være legal. Han mener de forbedrer systemer og at de setter fokus på svakheter i datasystemer. Rent prinsipielt forsvarer han crackere som er destruktive og umoralske nettopp fordi han mener de er nyttige for den teknologiske utviklingen.

Det som er interessant i forhold til moraler og normer er hvordan hackerne og crackerne selv ser på sin aktivitet. Når det gjelder Jon Johansen har han en oppfatning om at det han holder på med er moralsk forsvarlig. Johansen har blant annet i et «Tett på nett»-møte på vg.no i forbindelse med DVD-saken uttalt; «*Dersom en kode er utviklet for kun å skade forbrukerne, slik som i denne saken, så ser jeg ikke hvordan det kan være ulovlig eller moralsk forkastelig å gå rundt denne».* (Johansen 2000) Han forklarer dette med at koden på DVD ikke beskytter mot piratkopiering, men en kode for å beskytte mot avspilling, slik at filmindustrien får et monopol på DVD-spillere. Johansens ytringer viser at han ikke ser på sin egen aktivitet som umoralsk eller forkastelig.

Cracker#2 mener det er greit å bryte seg inn i datasystemer så lenge det finnes en «grunn» for å gjøre det. Cracker#2 og hans crackergruppe ønsker ikke å bryte seg inn i systemer for å ødelegge. Holdningene virker på meg veldig lik det Møllerhaug snakker om, at Craker#2 får en slags fjernhet til hva han holder på med.

Når det gjelder Cracker#1 har heller ikke han noen betenkeligheter med å bryte seg inn i datasystemer så lenge det er for å gjøre virksomheter oppmerksomme på datasikkerheten.

Siden de opprinnelige hackerne ikke oppførte seg umoralsk hadde de heller ingen problemer med å se på sin egen aktivitet som etisk. Formålet deres var å stadig utvikle bedre datamaskiner og datasystemer og da uten å stride mot vanlige normer i samfunnet. Dette er noe Johannesen støtter opp om, og siden han ikke driver med noe ulovlig er det heller ikke noe av det han gjør umoralsk. Det var, og er fremdeles, viktig for hackerne som Johannesen å følge hackeretikken som sier at all informasjon om hvordan verden fungerer skal være tilgjengelig for alle. Selv om det ikke er alle virksomheter som føler det på samme måte og utvikler proprietær programvare, er hackerne fremdeles moralske ved at de unnlater å bryte seg inn i andres systemer for å lære mer.

Skal jeg tolke Willassen, så mener han at crackerne er fullstendig klar over hva de gjør, og at det er straffbart. Spørsmålet er da hvorfor de gjør det likevel. Som jeg har vært inne på tidligere i oppgaven, kan noe av årsaken til dette være at crackerne får en slags fjern nærhet til offeret. Jeg mener at crackere som bryter seg inn i datasystemer vet hva de gjør, men ikke alle vet konsekvensene av hva de gjør. Mange scriptkiddies laster ned programvare som de har hørt skal kunne brukes til å kompromittere maskiner, kjører disse uten helt å vite hva de gjør. Jeg har et inntrykk av at disse «pek-og-klikk»-crackerne ofte er snille gutter i det daglige som ikke ville nasket en sjokolade på butikken en gang. Men når de sitter foran datamaskinen blir alt litt «fjernt» for dem. Jeg mener derfor at det ikke nødvendigvis ikke er noe galt med

moralen til disse personene, men at de heller har et problem med å skjønne konsekvensene av sine handlinger.

5.2.4 Hvilke metoder og fremgangsmåter har hackerne/crackerne?

I kapittel tre omtalte jeg en rekke teknikker for hvordan cracking kan gjennomføres. Jeg gikk igjennom fire måter for hvordan man kan cracke systemer; tilegne seg uautorisert aksess, tjenestenekting, knekke serial-/lisensbeskyttelser og cracke nettsider. Når jeg intervjuet informantene og når sekundærlitteraturen omtaler cracking, er det nesten utelukkende tilegning av uautorisert aksess det snakkes om. Så i dette avsnittet snakkes det om metoder og fremgangsmåter hackere og crackere benytter for å skaffe seg aksess på systemer.

Møllerhaug forklarer at mesteparten av angrepene som skjer på datasystemer følger standardiserte oppskrifter. Han sier at man kan se rekkefølgen i angrepene, og se hvilke pakker som kommer. Da vet du hvilke verktøy som henger i andre enden. Men en gang i mellom ser man ting som avviker fra de vanlige, som betyr at du har fingre mot tastaturet i andre enden. Dette stemmer overens med erfaringene til VDI hvor store deler av angrepene, eller forsøk på angrep, består av ferdiglagde script som forsøker å angripe et stort antall maskiner. Birkeland mener at det er de angrepene som ikke er robotisert som er farlige. Ved slike angrep sitter det en intelligens bak angrepet og det blir da straks mer alvorlig.

Møllerhaug skiller på to typer dataangrep; opportunistiske og rettede angrep. De opportunistiske angrepene fungerer slik at de sveiper over store ipområder og ser hva de kommer inn på med enkle teknikker. På denne måten tar crackere over maskiner og bygger nettverk av disse. Måten slike angrep skjer på kan for eksempel være at crackeren kjører en portscanner for å kartlegge svakheter, for deretter angripe det «letteste» offeret. I oktober i år kunne Computerworld.no melde om tidenes største bot-nettverk (Schreurs 2005). Tre personer var i Nederland arrestert for å ha benyttet over 100 000 såkalte zombie-pc-er. Dette viser at slike opportunistiske angrep skjer i stor skala og at det finnes mange zombie-pc-er i verden. Møllerhaug anslår at de opportunistiske angrepene står for 98 prosent av alle angrep på Internett.

De resterende prosentene står de rettede angrepene for. Møllerhaug forteller at dette er angrep hvor angriperen vet hvem han skal angripe. Crackeren sveiper da ikke over IP-områder for å finne et offer, men er målrettet og velger offeret ut i fra bestemte kriterier eller motiver. Dette kan for eksempel være at angriperen ønsker å utøve hevn mot offeret eller at crackeren ønsker å stjele informasjon som han vet offeret besitter. Metoden angriperen bruker er da å gå direkte på brannmuren for å prøve å bryte igjennom den eller komme rundt den på en eller annen måte. Angrep som er målrettet er svært alvorlig og er de angrepene som er vanskeligst å beskytte seg mot. Rettede angrep skiller seg fra de opportunistiske på flere områder. En forskjell er at det ofte ikke finnes sikkerhetsmekanismer mot rettede angrep da de som oftest gjennomfører angrepene ved å omgå eksisterende sikkerhetssystemer. En annen viktig forskjell er at når personen(e) bak et målrettet angrep først har funnet et offer, holder de seg til dette, i motsetning til de opportunistiske som bare sveiper rundt etter det letteste byttet.

Johannesen mener hackere og crackere ofte har forskjellige fremgangsmåter på hvordan de jobber. Generelt sett mener han at crackerne går rett på sak, og at det er lettere å vite hva motivasjonen deres er. Han mener at crackerne er dårligere til å researche enn hackerne og at de ofte setter i gang et angrep uten helt å vite hva som skjer. Disse karakteristikkene kan man lett kjenne igjen hos scriptkiddiene. Som jeg har skrevet tidligere i oppgaven benytter scriptkiddiene ofte ferdiglagde programmer som de ikke alltid skjønner konsekvensene av. Scriptkiddiene er typiske den typen crackere som står bak det store antallet opportunistiske angrep.

Johannesen mener hackere bruker andre metoder for hvordan de jobber. Han mener de ofte følger et mønster, og at de benytter egenutviklet programvare og standardverktøy. Noen av eksemplene på programmer som brukes er portscannere som Nmap og strobe. Hackerne bruker disse programmene til å kartlegge svakheter i systemene. Han mener hackere vet hva de forskjellige programmene gjør og at de har oversikten over sårbarheter og exploits som ligger tilgjengelig på nettsider og e-postlister.

Willassen forteller at politiets erfaringer med crackernes metoder er at det er vanlig å bruke ferdiglagde programmer som utnytter svakheter i operativsystemer og annen programvare. Exploitene og fremgangsmåtene for å bruke de finner de på Internett. Willassen forteller at den vanligste fremgangsmåten for crackere er å bruke exploits som utnytter svakheter, for å komme seg inn på maskiner man ikke har tilgang til.

Andre fremgangsmåter som Willassen har erfaringer med er urettmessig bruk av brukernavn og passord. Han forteller at hvis en person får fatt på brukernavn og passord og bruker dette til å logge seg inn, er dette også datainnbrudd. Metoder for å skaffe seg dette kan for eksempel være ved å sniffe opp nettverkstrafikk, sosial ingeniørkunst, lete etter passord som er skrevet ned eller prøve å gjette. Alt dette er forskjellige metoder på hvordan man kan lykkes i å gjøre datainnbrudd.

Willassen forteller at det finnes en hel «industri» på nettet som finner sårbarheter i operativsystemer og som utvikler exploits for å kunne utnytte sårbarhetene og dermed skaffe seg rettigheter på systemet. Med industri mener Willassen at det finnes en organisert aktivitet på nettet som utvikler og distribuerer exploits. Men det er her vanskelig å skille på dem som utvikler og distribuerer exploits med skumle hensikter og dem som gjøre det samme for å lære mer om svakheter i datasystemer. I kapittel 3.3.1 viste jeg noen eksempler på noen nettsteder som offentliggjør sårbarheter og exploits. Bakgrunnen for at disse nettstedene offentliggjør sikkerhetshull er ikke for å oppfordre til datakriminalitet, men fordi de ønsker å sette fokus på trusler og svakheter i programvare.

Crackerne bruker programvare for å finne bestemte svakheter og bruker så bestemte exploits for å utnytte disse svakhetene. Dette er en kjent metodikk i IRC- og warezmiljøene forteller Willassen. Ofte brukes ferdiglagde scannere og exploits, men politiet har også sett at crackere selv lager slike programmer. Ofte samarbeider de om utviklingen av spesielle programmer som skal gjøre helt spesifikke oppgaver. Og det gir selvfølgelig status i miljøene å være med på utviklingen av slike programmer.

Willassen sier at det foregår en gradvis utvikling av folks kompetanse, med at de starter med å bruke ferdiglagde programmer, men at de over tid begynner å utvikle egne programmer. Fremgangsmåtene de bruker avhenger da altså av kompetansen de besitter. Black hat hackers har ofte metoder som avviker fra «standardmetodene», noe som gjør at innbruddene er «farligere» og vanskeligere å oppdage.

Når jeg spurte Cracker#2 om hvilke metoder han og gruppen han var medlem i brukte, var han svært sparsommelig med opplysningene. Men han kunne fortelle at gruppen hadde hatt en stadig utvikling og at de nå utviklet mye av programvaren selv. Etter samtalene med Cracker#2 vil jeg omtale han og hans gruppe som black har hackere som utfører målrettede angrep. De utvikler egne exploits og passer på å holde verktøyene internt i gruppen. Cracker#2 var litt sparsommelig med informasjonen om hvilke metoder hans gruppe brukte, men i følge han selv, var dette metoder som ikke var kjent, noe som gjorde at de hadde den «suksessen» de hadde.

Cracker#1 var ikke like «hemmelighetsfull» om metodene sine som Cracker#2 og fortalte villig vekk om metodene han brukte. Han mente at metodene han brukte for å hente ut informasjon fra et datasystem, ikke var noen hemmelighet. Systemet som han angrep var dårlig programmert og alle med litt programmeringserfaring kunne greidd å hente ut informasjon fra det systemet.

5.2.5 Hvordan er hackere/crackerne organisert?

De tidlige hackermiljøene var kjent for sitt sterke samhold og ønske om samarbeid. Jeg har prøvd å finne ut om måten hackere og crackere jobber på er forandret siden de første hackerne og frem til i dag. Willassen sier at når motivasjonen for cracking er status i et miljø, sier det seg selv at crackerne opptrer i et stort miljø hvor det er viktig å vise seg frem. Han påpeker at mange jobber på egenhånd. Willassen sier at det finnes eksempler på faste grupperinger som henger sammen, og at det er noen som styrer og bestemmer hva man skal gjøre. Han sier at de fleste grupperingene er løse, og at det er mer et nettverk enn en gruppe som samarbeider for å oppnå status. Willassen snakker her spesielt om IRC miljøene som gir et klassisk bilde på hvordan hackere og crackere samhandler.

Johannesen er et eksempel på hva Willassen snakker om. Johannesen som jo beskriver seg selv som en hacker, er flittig bruker på IRC kanaler og holder kontakten med personer med samme interesser gjennom disse nettverkene. Johannesen bekrefter at hackerne inngår i et fellesskap hvor deling av innformasjon og erfaringer er viktig for å finne ut av ting. Det er en holdning blant hackerne om å hjelpe hverandre hvor det er mulig. Dette var også den samme holdningen som de første hackerne hadde.

Møllerhaug forklarer at det finnes de som jobber alene, men hva er vitsen med å være briljant hvis ingen vet om det? Han sier at gruppetilhørigheten er for å fremme seg selv, sitt ego, slik at faktisk noen vet hva du har utrettet. Dette viser igjen at status i miljøene er viktig for mange av hackerne og crackerne. Møllerhaug sier videre at det varierer hvor tett gruppene er bundet. Noen av

dem er veldig bundet sammen og noen er løst bundet sammen. Noen har aldri møtt hverandre, mens andre møtes regelmessing. Møllerhaug mener organisasjonsformen varierer veldig og det er forskjell på hvordan de forskjellige gruppene averterer. For eksempel har mange av hackergruppene fengende navn som er den del av identiteten deres. Men hvis man snakker om kriminelle grupper holder de en lavere profil og annonsere ikke noe slående gruppenavn.

Øgrim har samme oppfatning som de andre informantene om at hacker- og crackerunderverdenen er åpen og naiv hvor folk utveksler informasjon i stor målestokk. Han mener nettverkene er relativt åpne og at det er lett å komme inn i miljøene.

Under mitt arbeid med masteroppgaven oppsøkte jeg IRC kanaler hvor jeg visste hackere og crackere befant seg. Jeg kan bekrefte hva informantene forteller om hvordan hackerne og crackerne forholder seg i forhold til hverandre. Når jeg snakket privat (samtale med én person) med personer på ICR, var det ofte at navn på andre personer på kanalen ble nevnt. Personene jeg snakket med kjente tydeligvis godt til mange av de andre personene på kanalen, og jeg ble ofte henvist til andre når jeg stilte konkrete spørsmål om hacker- crackertemaet.

Cracker#2 er et konkret eksempel på at crackere samler seg i grupper og hans gruppe har holdt tett sammen i nesten ti år. Avhengig av hvilke formål gruppen har avgjør hvor tett og lukket gruppen er. Gruppen til Cracker#2 ønsker å holde en lav profil og de holder informasjonen sin kun internt i

gruppen. Dette for å sikre seg mot at de skal bli oppdaget eller at andre skal avsløre metodene de bruker.

Hvis jeg skal sammenligne hvordan de opprinnelige hackerne var organisert med hvordan dagens hackere og crackere er organisert vil jeg si det har skjedd en utvikling. Jeg mener at hackerne og crackerne nå har et mer anonymt forhold til hverandre. Det er få som vet hvem som egentlig skjuler seg bak de forskjellige kallenavnene. Innenfor miljøene kjenner folk hverandre igjen på kallenavnene uten å vite hvem som opererer bak det. En annen forskjell som jeg mener er forskjellig fra de første hackerne er at det nå finnes flere motiver for å samhandle i grupper. I begynnelsen var formålet å dele informasjon for å best mulig kunne utvikle programvare. Gruppene var åpne og deling av erfaringer og informasjon var en selvfølge. Denne motivasjonen finnes fremdeles hos hackerne, men crackerne har dratt med seg andre motivasjoner som gjør at noen crackergrupper holder en lav profil. En gruppe som samhandler om datakriminalitet ønsker ikke å dele all informasjon med alle og av den grunn og det oppstår ofte en sammensveiset «kjerne».

5.2.6 Hvordan er informasjonsflyten til hackerne/crackerne?

I følge Møllerhaug foregår det meste på Internett. Men det er også noen som møtes fysisk. Det er klart at de gruppene som møtes fysisk er mindre utsatt for infiltrasjon enn de gruppene hvor deltakerne aldri har sett hverandre. Ved at man møtes fysisk er det lettere å holde en lav profil og det er lettere å stole på folk.

Willassen mener at det er Internett som er den viktigste informasjonskanalen til hackerne og crackerne. Men han sier det varierer fra miljø til miljø på hvordan hackere og crackere deler informasjon på Internett. Han mener IRC er en gjenganger, men også at e-post brukes en del. I lukkede grupper brukes ofte krypterte IRC-meldinger og e-post. Han sier at politiet sjelden ser at de treffes i det virkelige liv, og at det nok ikke skjer ofte.

At Internett brukes mye av hackere for å dele informasjon og erfaringer kan bekreftes av Johannesen. Spesielt IRC er en viktig kanal for å holde kontakten med likesinnede i miljøet. I etterkant av intervjuet med Johannesen har jeg snakket med han på IRC hvor han har henvist meg til andre personer som han kjente når han mente de kunne svare på spørsmål i forbindelse med mitt arbeid. Både Cracker#2 og Cracker#3 kom jeg i kontakt med på IRC, så det er helt klar at dette er et medium som er i stor grad benyttet av hackere og crackere.

Hvis jeg skal se på hvordan de opprinnelige hackerne delte informasjon seg imellom, så var jo dette på en tid før Internett og før maskinene kunne kommunisere seg imellom. Det tidlige hackermiljøene var relativt små, og var stort sett lokalisert på universitetene. Så i begynnelsen foregikk kommunikasjonen som oftest med de som befant seg på samme universitet.

Etter hvert som maskiner ble koblet samme i nettverk, var det lettere å dele informasjon uavhengig av geografi. Etter en stund ble BBS`ene et viktig hjelpemiddel for å dele erfaringer og kunnskap med hverandre.

Det som er et tegn fra hackernes/crackernes opprinnelse er at informasjon er viktig. Informasjonen skal kunne deles raskest mulig og ikke være avhengig av hvor man befinner seg i verden. Til dette er Internett et supert verktøy. Deling av informasjon er fremdeles viktig for hackere og crackere. Spesielt er dette viktig for hackerne hvor det nærmest er en moralsk plikt å dele informasjon, løse problemer og gi løsningene videre slik at andre hackere kan løse nye problemer fremfor å finne opp hjulet på nytt.

Jeg mener det er en forskjell på informasjonsflyten til hackere kontra crackere. Hackerne kan dele sin informasjon med alle andre som ønsker det, mens crackerne deler ofte bare med de som inngår i den gruppen de selv er med i. Dette virker logisk og som Cracker#2 sier det er dette for å holde sine egne «cracks» hemmelig for andre samtidig som det er lurt å holde en lav profil med tanke på at de tross alt driver datakriminalitet.

6. Konklusjon

Arbeidet med denne masteroppgaven har gått ut på å gå hackere og crackere nærmere etter i sømmene. Tidlig i oppgaven presenterte jeg følgende problemstilling;

Hva karakteriserer hackere og crackere og hva er deres motivasjon og metoder?

Dette er en vid problemstilling som ikke åpner for konkrete konklusjoner. Det har vært et ambisiøst område å utforske og jeg vil ikke påstå at jeg har funnet ALLE svarene. Resultatet av et slik studie er ikke et svar med to streker under, men ved hjelp av forskningsspørsmålene har det vært mulig å komme frem til noen konklusjoner på hva som karakteriserer hackerne og crackerne, samt deres motivasjoner og metoder.

Etter å ha gått grundig igjennom forskningsspørsmålene i kapittel fem, vil jeg med noen få avsnitt nå oppsummere de viktigste funnene mine og dermed kort besvare problemstillingen min;

Hacker- og crakertermene defineres på utallige måter avhengig av hvem som definerer dem. Ikke nok med at disse termene ofte forveksles, finnes det andre ord og uttrykk som ikke sjelden sammenblandes med disse beskrivelsene. Jeg tenker da spesielt på flere av de definisjonene som jeg gikk igjennom i kapittel tre. Termene brukes ulikt i forskjellige kontekster, for eksempel er det

hacker folk flest forbinder med datakriminalitet, mens i it-miljøer kan man bruke cracker om det samme. En ting som har vært interessant å observere er at de som kaller seg hackere, ikke vil bli assosiert med crackerordet. De mener at crackere er uetiske og destruktiv, noe de selv ikke ønsker å være. Uansett hvordan man velger å bruke termene, er det viktig å ta et valg og være konsekvent på bruken av ordene.

Uavhengig om personene er «etisk» eller «uetisk», kan man si at hackere og crackere ikke kan sees på som en homogen gruppe. Jeg mener dermed at man kan avlive myten om at hackere og crackere er unge, kvisete nerdegutter med briller som sitter foran pc-en sin innelåst på rommet sitt. Mine erfaringer med arbeidet med denne oppgaven er at begge grupperingene for det meste består av menn i alderen 15 – 30 år. Flesteparten er menn, men det finnes også kvinner representert. Hackere og crackere finnes i alle samfunnslag og er uavhengig av politisk bakgrunn og geografisk tilhørighet.

Hackere og crackere har forskjellige motiver og fremgangsmåter og det er ikke mulig å finne en felles drivkraft for alle sammen. Hvis jeg, ut i fra de få informantene jeg hadde, skal si noe om hva som er det viktigste motivet for en hacker, mener jeg det er ønsket om å lære mest mulig om datamaskiner og –systemer. Dette er et motiv som har vært konstant fra de første hackerne frem til i dag. Ellers mener jeg at politiske motiver er viktig for mange hackere.

Når det gjelder crackere er motivene ikke like enkle. For mange crackere er nok status en viktig motivasjon, da spesielt scriptkiddiene som er en stor gruppering. Et annet motiv som jeg tror blir mer og mer fremtredene er det

økonomiske motivet. Stadig mer penger flyttes over Internett, samtidig som virksomhetskritiske systemer knyttes til nettet. Her har systemutviklere og sikkerhetsfirmaer en utfordring i fremtiden. På samme måte som hackere har også mange crackere et ønske om å lære mer om datasystemer. Dette er også et motiv som står sterkt for mange crackere.

Hva som kan sies å være den «vanligste» motivasjonen for hacking og cracking er nok ikke så lett å si. Willassen mener det er status som er den vanligste forklaringen på hvorfor personer bryter seg inn i datasystemer. Spafford mener noe annet, og at det er interessen for å lage bedre programvare som driver dem. Når US Secret Service og US CERT konkluderer med at det er hevn som er den vanligste motivasjonen, viser dette at det ikke er helt enkelt å fastslå hva som får personer til å hacke/cracke.

Noe av forklaringen på at forskjellige kilder oppfatter ulikt hva som er den vanligste motivasjonen, kan være fordi at noen av motivene er lettere å oppdage enn andre. En som cracker fordi han er ute etter status, kan være mye lettere å oppdage enn en cracker med andre motiver. Siden personen da ønsker at andre personer skal vite om hva han har gjort, kan dette virke som en vanlig motivasjon. I motsatt fall kan det være vanskeligere å oppdage en cracker som benytter hevn som motiv. Personen prøve å skjule så godt han kan sine handlinger og hvis personen da i tillegg utøver hevn mot en arbeidsgiver, kan det være ekstra vanskeligere å oppdage da personen som oftest kjenner til systemet.

Hvordan hackerne og crackerne ser på sin egen aktivitet, har jeg også fått noen inntrykk på fra datainnsamlingen min. Jeg mener at folk generelt sett vet hva som er rett og galt her i verden, også hackerne og crackerne. Spørsmålet er da hvorfor så mange crackere bedriver datakriminalitet. Noe av grunnen til dette tror jeg kan være at mange får et veldig distansert forhold til det de driver med. Det å sitte å gjøre noen små endringer på en pc, på andre siden av jordkloden, kan virke ganske ufarlig, men kan utgjøre store forskjeller for dem som blir rammet. Jeg mener det ofte blir vanskelig å se konsekvensene av det man holder på med. Moralen kan av disse grunnene virke litt «utvannet» for crackerne og mange av dem har ikke betenkeligheter ovenfor handlingene sine.

Hackerne derimot har ikke samme «dårlige» moral. Men jeg vil påstå at hackeretikken ikke er like sterk som den var i hackerens barndom. Dette har nok igjen sammenheng med at hackingen er blitt mindre personlig enn tidligere. Alt skjer i mye større skala i dag enn da de opprinnelige hackere drev på. Miljøene er mye større, systemene flere og gruppetilhørigheten ikke like sterk.

Det som er interessant er å legge merke til, er hvordan hacktivistene ser på sine aktiviteter. De driver jo datakriminalitet, men mener likevel at de er etiske og det de står for ikke er galt. De mener de har rett til å drive sivil ulydighet, så lenge det er nok folk som støtter opp om deres politiske verdier.

Det finnes utallige fremgangsmåter for hvordan man kan omgå sikkerhetssperrer i datasystemer. Hackere og cracker bruker ofte samme

metoder, men forskjellen er på hvilke moralske plan de bruker dem. Mange crackere, da spesielt scriptkiddiene, bruker ofte ferdiglagde verktøy som de ikke alltid skjønner konsekvensene av. I motsetning til dette er hackerne mer opptatt av å skjønne hva som skjer og utvikler verktøyene selv. Den metoden som jeg vil påstå er den mest brukte for å bryte seg inn i datasystemer, er opportunistiske angrep. Disse angrepene skjer ofte, men sjelden farlige hvis man har tatt sine forhåndsregler med tanke på sikkerhet. Metoden er enkel, som nok er grunnen til at den er mye brukt, og går ut på å bruke programmer eller skript for å lete etter svakheter i datasystemer. Når man så finner svakhetene man leter etter, bruker man videre verktøy for å utnytte svakhetene.

Hackere og crackere er «flokkdyr» som opptrer i store åpne miljøer. Det å inngå i et felleskap skaper trygghet og samhørighet. Det er lett å bli en del av de store nettverkene og informasjon deles i stor målestokk. I tillegg til de store miljøene finnes det også små lukkede grupperinger som ikke er like lett å bli en del av. Min oppfatning er at det varierer hvor tett grupperingene er bundet sammen og at det ofte er gruppens formål som avgjør hvor tett og lukket gruppen er. Det som er vanlig er at hackerne og crackerne er anonyme for hverandre og det er sjelden de vet hvem de andre i gruppen er.

Det er liten tvil om at mesteparten av informasjonen deles over nettet. IRC er en gjenganger hvor hackere og crackere møtes for å dele informasjon, men også e-post brukes mye. I de lukkende gruppene brukes ofte krypterte meldinger og e-post for å unngå at informasjon kommer på avveie. Internett er et supert verktøy til å dele erfaringer og kunnskap raskt og enkelt og ikke minst spiller det ingen rolle hvor man befinner seg i verden.

Informasjonsflyten kan variere litt mellom hackere og crackere. Det spiller liten rolle for hackerne om alle andre ser informasjonen de deler, mens for crackerne kan spredning av informasjon få skjebnesvangre konsekvenser, spesielt hvis lovens håndhevere får tak i den.

7. Erfaringer

Dette kapittelet vil ta opp både frustrasjoner og gleder ved det å skrive en masteroppgave. Jeg vil forsøke å oppsummere hvilke erfaringer jeg sitter igjen med etter endt masteroppgave.

7.1 Arbeidsform

Hvis det var en ting jeg ville gjort annerledes når det gjelder arbeidet med oppgaven, så ville jeg skrevet oppgaven sammen med en annen student. Det har til tider vært svært tunge stunder på lesesalen, og alt har virket håpløs. I slike stunder hadde det virkelig vært nyttig å ha en å dele frustrasjoner med. Mine erfaringer fra gruppe- og pararbeid ved kurs og oppgaver på Universitetet, viser at det er mye lettere å løse problemer og å komme seg videre når man kan bakke hverandre opp og jobbe seg ut av frustrasjoner. Ved å jobbe sammen presser man hverandre til å yte det beste og oftere er man mer besluttsom slik at man får den jevne progresjonen i arbeidet.

På slutten av oppgaven opplevde jeg utfordringer som å være lei av oppgaven og at jeg følte at jeg stagnerte og ikke kom videre. Det hadde da vært en stor fordel å ha en person ved siden av seg som kunne motivert og oppmuntret en til å fortsette arbeidet.

Men samarbeid om en masteroppgave kan også være en risiko å ta. Hvis man har forskjellig ambisjonsnivå for oppgaven kan det føre til splid i gruppen som igjen kan føre til dårlig oppgave. Det å jobbe så tett over så lang tid kan lett føre til uenighet og i verste fall splittelse. Så forutsetningen for at jeg ville startet en masteroppgave med en annen, ville vært at vi hadde kjent hverandre, jobbet sammen før og at vi hadde hatt ett felles ambisjonsnivå.

En bakdel med å være to, kan være at man blir uenig og at sliter med å bli enige om hvordan ting skal gjøres eller skrives. Selv om jeg har kommet meg igjennom denne oppgaven på egenhånd, er jeg rimelig sikker på at jeg ville valgt å ha en partner hvis jeg skulle starte på en masteroppgave i dag. Alt i alt er jeg fornøyd, og er faktisk ganske stolt av at jeg helt alene har klart å ferdigstille denne masteroppgaven.

7.2 Veiledning

Gjennom arbeidet mitt med masteroppgaven har behovet mitt for veiledning variert noe. Til å begynne med hadde jeg veiledning annenhver uke og det var greit å få en gode innspill i starten. Etter hvert følte jeg at jeg ikke trengte like mye veiledning og at jeg heller ville jobbe frem til jeg hadde noe håndfast som jeg ønsket tilbakemelding på. I store deler av arbeidet var det veiledning «etter behov», men mot slutten av oppgaven ble veiledningsmøtene hyppigere, naturlig nok.

Likevel har det vært til stor nytte å ha en ressursperson å henvende seg til når jeg stod fast og ønsket tilbakemeldinger. Heldigvis har samarbeidet med veileder fungert bra og han har vært behjelpelig og fleksibel, samt gitt gode råd og vink. Siden skriving av masteroppgave var helt nytt for meg var det svært viktig for meg å ha en veileder som hadde stor erfaring og kompetanse på området.

7.3 Holde fokus!

Gjennom arbeidet med oppgaven har det ikke alltid vært like enkelt å holde fokus på det man skal holde fokus på. Det er svært lett å begi seg ut på arbeid som er lite relevant for det som skal være fokuset i oppgaven. Dette er særdeles vanskelig i slike lange oppgaver som dette, hvor man ikke alltid husker hvilke veivalg man tidligere har valgt.

Et godt råd ved skriving av masteroppgave er å skrive logg slik at man ut i arbeidet kan gå tilbake å se på hvilke beslutninger og tanker man tidligere hadde. En slik logg er til stor nytte ved slutten av arbeidet da alle tråder skal samles og man skal gjøre en oppsummering og se om man har fått med alt man har tenkt gjennom hele perioden. Selv om loggen jeg førte ikke innholdt detaljerte opplysninger om hva jeg hadde gjort, var den likevel til stor hjelp mot slutten av oppgaven, da jeg enkelt kunne bla meg bakover i «prosjektet».

Til tider var det svært lite motiverende å skrive masteroppgave. Etter å ha holdt på å skrive på et avsnitt i flere dager, måtte jeg flere ganger bare legge

fra meg den delen av oppgaven og bare skrive på noe annet i andre kapitler. Det hjalp ofte, men noen ganger var det fullstendig skrivestopp. I slike stunder var det svært lett å miste fokus, og de minste ting i omgivelsene fikk min oppmerksomhet. Eneste løsning da var å legge fra seg oppgaven og finne helt andre ting å gjøre på. Når jeg da gikk tilbake til oppgaven var det en helt ny giv og arbeidet gikk mye lettere.

7.4 Slit

Mot slutten av oppgaven fikk jeg meg fast jobb og jeg måtte kombinere avslutningen av studiet med arbeidslivet. Dette var en svært slitsom periode. Ved arbeidsdagens slutt måtte jeg finne frem skolearbeidet og jobbe hardt for å komme i mål. Det ble flere sene dager i uken og mange timer i helgene måtte brukes for at jeg skulle kunne gjøre meg ferdig med oppgaven. De siste tre månedene gjorde jeg stort sett ikke annet enn å jobbe og skrive oppgave. I denne perioden var det utrolig stor støtte i mine nærmeste som oppmuntret meg til å stå på og gjøre en siste innsats for å nå en mastergradstittel. Dette inspirerte meg og fikk meg til å skjønne at dette skulle jeg greie selv om jeg måtte ofre mye at min fritid den perioden. Heldigvis nådde jeg mitt mål.

7.5 Tid

Det å skrive en masteroppgave består av mer enn bare å skrive en stor rapport. Det ligger mye arbeid bak selve det å skrive oppgaven. I starten brukte jeg mye tid på å lese sekundærlitteratur som var skrevet om feltet før. Jeg leste blant annet bøker av kjente forfattere som var relevante for mitt arbeid. Flere

av disse har jeg referert til i oppgaven. Men ikke bare har jeg brukt mye tid på å lese, jeg har også brukt mye tid på å skaffe informanter til intervjuene og avtale møter med dem. Dette er arbeid og tid som man ikke kan se direkte i oppgaven men som likevel er en del av det å gjennomføre en masteroppgave. Slike tidskrevende aktiviteter har tatt mer tid enn jeg trodde på forhånd. Dette er tid man ikke regner med å bruke og det er lett for at tiden flyr av gårde.

Det å formatere en masteroppgave og få den til å se anstendig ut er også et tidssluk uten like. Selv om man er bevisst på å bruke riktige formateringer på de forskjellige elementene i oppgaven fra begynnelsen av gjenstår det alltid en formidabel jobb med layouten til slutt.

Min erfaring med tidsbruk på ting som ikke direkte kommer med i oppgaven er at man aldri kan planlegge nok. En nøye gjennomtenkt plan kan spare deg for mye tid i en allerede stressende avslutting. Tid til å skaffe og planlegge møter med informanter må man bare sette av mye tid til.

I begynnelsen av oppgaven lagde jeg en milepælsplan for progresjonen min. Denne reviderte jeg flere ganger i løpet av arbeidet mitt. Milepælene var vanskelig å holde, og jeg måtte utsette oppgaven en stund da jeg slet med å få tak i informanter. Men selv om jeg ikke alltid greide å holde meg til milepælsplanen har jeg forstått viktighetene med en slik oversikt. Det er et meget godt verktøy for ikke å rote bort for mye tid og som jeg har hatt stor nytte av.

7.6 Metodeerfaringer

Utvalget av informanter ble litt mindre enn hva jeg hadde planlagt. Mitt mål var å ha fire – fem informanter fra begge leire. Jeg ønsket å gjøre dybdeintervjuer med fire – fem hackere og fire – fem dybdeintervjuer med eksperter på dette området. Som sagt gikk ikke dette helt etter planen, men jeg mener selv at jeg har fått et fyldig datasett likevel. Eksperter med kunnskap om hacking og cracking var lett å få tak i, men crackerne var litt verre. Jeg kompenserte da med intervjuer over nettet (nettsamtale, e-post), samt noen telefonsamtaler i tillegg til at jeg trakk inn sekundærlitteratur for å få tilstrekkelig datamateriale.

Min plan for å samle inn data var å dybdeintervjue alle informantene «face-2-face», men i alle tilfeller var ikke dette mulig. I noen tilfeller måtte jeg innhente informasjonen uten å snakke med informantene direkte. Noen ganger snakket jeg med personer på telefon, men mange samtaler forgikk på nettet.

Grunnene til at jeg ikke fikk snakket med alle «face-2-face» hadde flere årsaker. Flere av de jeg har vært i kontakt med har uført straffbare handlinger og de er av den grunn litt forsiktige med å dele informasjon. Selv om de visste hvilke motiver jeg hadde og at de var sikret full anonymitet, var ikke det alltid nok til at jeg kunne få møte dem.

Men det trenger nødvendigvis ikke være en ulempe for denne masteroppgaven å måtte intervjue noen over nettet. En stor fordel med å intervjue personer på denne måten, og da spesielt personer som har vært på

«kant» med loven, er at det er lettere for dem å fortelle om det da. Nettet skaper en følelse av anonymitet og det er lettere for en informant å åpne seg og fortelle om sine aktiviteter enn hvis jeg hadde sittet rett ovenfor han.

I et tilfelle utvekslet jeg noen e-poster og hadde et par telefonsamtaler med en person som hadde brutt seg inn i en norsk bedrifts systemer. Dette er den personen som jeg omtaler som Cracker#1 i kapittel to. Han sa et han var opptatt av datasikkerhet og at det bare var en tilfeldighet at han hadde kommet over denne systemsvakheten. Dette var også eneste gang han hadde brutt seg inn i et system. Jeg fant ut at et fysisk møte med Cracker#1 ikke ville skaffet meg noe særlig mer relevant informasjon enn det som allerede var blitt sagt over telefon og på e-post.

I noen tilfeller har jeg brukt eksisterende informasjon som en del av grunnlaget for min analyse, blant annet intervjuer gjennomført av andre. Dette har blant annet vært publiserte intervjuer med personer som har ytret seg om temaer som jeg belyser i denne oppgaven.

Det var altså et stort problem for meg å få intervjuet crackere i forbindelse med denne masteroppgaven. Dette var jeg også oppmerksom på før jeg startet med oppgaven, men jeg var villig til å gjøre et forsøk på å få tak i tilstrekkelig med informanter. Etter en stund kom jeg til et punkt i prosjektet at jeg måtte gi opp med å få tak i de personene jeg ville og heller kommer meg videre i prosjektet. Følgende av dette er at jeg har måttet bruke mer data fra sekundærlitteraturen for å kunne skape en fornuftig analyse.

Selv om min plan med dybdeintervjuer ikke gikk helt som planlagt mener jeg selv at jeg har et stort nok datamaterialet til å kunne trekke noen konklusjoner fra funnene mine. Jeg har hele tiden vært oppmerksom på at jeg har måttet endre litt på hva som ble datamaterialet mitt og dette har jeg tatt hensyn til i beskrivelsen og analysen av funnene mine.

7.7 Videre arbeid

I dette avsnittet vil jeg prøve å identifisere noen retninger jeg føler kunne vært aktuelle hvis jeg selv (eller andre) ville forsket videre på emnet om hackere og crackere.

Hvis jeg skulle ha fortsatt på oppgaven eller skrevet den på nytt, ville jeg hatt mer fokus på det tekniske. Jeg ville sett på hvordan hackere og crackere bryter seg inn på datamaskiner og hvilke hjelpemidler de bruker for å få dette til. Dette er noe jeg kunne ha skrevet mer om i min oppgave, men det ville nok vært en oppgave i seg selv.

Selv om jeg føler at jeg har svart dekkende på min problemstilling mener jeg det finnes muligheter for å jobbe videre med deler av den. Et eksempel, som har vært sentralt for meg, er hackernes og crackernes motivasjoner. Dette temaet føler jeg kunne være interessant å jobbet videre med. Jeg mener at motivene bak datainnbrudd kunne vært spennende å fordype seg enda mer i, spesielt med tanke på at fremtidens systemer trenger strenge krav til sikkerhet.

Referanser

Acohido, Byron og Swartz, Jon (2004) Going price for network of zombie PCs: $2,000-$3,000, *USA Today*.

BBC News (2005) *Web server attacks "growing fast"*, lokalisert: [11.06.2005] <http://news.bbc.co.uk/1/hi/technology/4480689.stm>

Cornford, Tony og Smithson, Steve (1996) *Project research in information systems : a student's guide,* Macmillan, Houndsmills.

Den Norske advokatforening (1998) *Norsk retstidende 1998-1971,* Den norske advokatforening, Oslo.

Dick, Bob (2005) *Grounded theory: a thumbnail sketch.*, lokalisert: [09.06.2005] <http://www.scu.edu.au/schools/gcm/ar/arp/grounded.html>

Dozois, Gardner (1984) Sf in the Eighties.

Familie- kultur- og administrasjonskomiteen (2005) Innstilling fra familie-, kultur- og administrasjonskomiteen om lov om endringer i åndsverkloven m.m., *Innst.O.nr.103 (2004-2005)*, nr. 19.06.2005, s. 54.

Finkel, Raphael (1975) *The Original Hacker's Dictionary*, lokalisert: [13.06.2005] <http://www.dourish.com/goodies/jargon.html>

Glaser, Barney G. (1992) *Basics of grounded theory analysis,* Sociology Press, Mill Valley, Cal.

Glaser, Barney G. (1998) *Doing grounded theory : issues and discussions,* Sociology Press, Mill Valley, Ca.

Glaser, Barney G. og Strauss, Anselm L. (1967) *The discovery of grounded theory : strategies for qualitative research,* Aldine, Chicago.

Hannemyr, Gisle (1998) The Art and Craft of Hacking, *Scandinavian Journal of Information Systems,* vol. 10:1-2, nr. 1-2.

Hannemyr, Gisle (1999) Technology and Pleasure: Considering Hacking Constructive, *First Monday,* vol. 4:2.

Hannemyr, Gisle (2003) Hester, ormer, snoker og virus, *Computerworld,* vol. 43.

Hannemyr, Gisle (2005a) *ENDRINGER I ÅNDSVERKLOVEN - Til lykke med dagen, Bill Gates og Steve Jobs!*, lokalisert: [24.06.2005] <http://folk.uio.no/gisle/essay/ipr09.html>

Hannemyr, Gisle (2005b) *FORSLAG TIL ENDRINGER I ÅNDSVERKLOVEN - Et brudd med norsk opphavsrettstradisjon*, lokalisert: [05.07.2005] <http://folk.uio.no/gisle/essay/copyr04.html>

Haugnes, Gunhild M. (2005) *Lever farlig i trådløst nett*, lokalisert: [25.06.2005] <http://www.aftenposten.no/nyheter/nett/article1008438.ece>

Henriksen, Petter og Eriksen, Trond Berg (2005) *Aschehoug og Gyldendals store norske leksikon,* Kunnskapsforl., Oslo.

Ilett, Dan (2005) *Russian police: "Our hackers are the best"*, lokalisert: [10.05.2005] <http://news.com.com/Russian+police+Our+hackers+are+the+best/2100-7348_3-5661547.html?tag=nefd.top>

Internet Systems Consoritum (2005) *ISC Internet Domain Survey*, lokalisert: [22.11.2005] <http://www.isc.org/index.pl?/ops/ds/>

Johansen, Jon Lech (2000) *Tett på Nett: Jon Johansen*, lokalisert: [02.03.2005] <http://interaktiv.vg.no/CGI/intervju/intervju/jonjoh>

Keeney, Michelle , et al. (2005) *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, lokalisert: [11.09.2005] <http://www.cert.org/archive/pdf/insidercross051105.pdf>

Kultur- og kirkedepartmentet (2005) *Om lov om endringer i åndsverkloven m.m.*, lokalisert: [14.04.2005] <http://odin.dep.no/repub/04-05/otprp/46>

Kvale, Steinar (1997) *Det kvalitative forskningsintervju,* Ad notam Gyldendal, Oslo.

Levy, Steven (1994) *Hackers : heroes of the computer revolution,* Penguin, London.

Leyden, John (2004) *Phatbot arrest throws open trade in zombie PCs*, lokalisert: [01.06.2005] <http://www.theregister.co.uk/2004/05/12/phatbot_zombie_trade/>

Locke, Karen D. (2001) *Grounded theory in management research,* Sage, London.

Mennecke, Thomas (2005) *Slyck.com Interviews Jon Lech Johansen*, lokalisert: [17.08.2005] <http://slyck.com/news.php?story=733>

Neset, Tore (2000) *Jon (16) er Hollywoods skrekk*, lokalisert: [26.08.2005] <http://www.dagbladet.no/nyheter/2000/01/19/189498.html>

Norsis (2005) *Årsrapport 2004*, lokalisert: [20.08.2005] <http://www.norsis.no/data/vedlegg/78_20041215_SIS_aarsrapport_2004.pdf>

Nærings- og handelsdepartementet (2000) *Samfunnets sårbarhet som følge av avhengighet til IT*, lokalisert: [08.08.2005] <http://odin.dep.no/nhd/norsk/dok/andre_dok/rapporter/024101-220004/dok-bn.html>

Næringslivets sikkerhetsråd (2004) *Mørketallsundersøkelsen*, lokalisert: [17.03.2005] <http://www.nsr-org.no/docs/79281401M.pdf>

Oikarinen, J. og Reed, D. (1993) *RFC 1459 - Internet Relay Chat Protocol*, lokalisert: [02.06.2005] <http://en.wikipedia.org/wiki/Script_kiddie >

Patel, Runa og Davidson, Bo (1995) *Forskningsmetodikkens grunnlag : å planlegge, gjennomføre og rapportere en undersøkelse,* Universitetsforl., Oslo.

Raymond, Eric S. (1993) *The New hacker's dictionary,* MIT Press, Cambridge, Mass.

Raymond, Eric S. (2005a) *How To Become A Hacker*, lokalisert: <http://www.catb.org/~esr/faqs/hacker-howto.html>

Raymond, Eric S. (2005b) *The Jargon File*, lokalisert: [07.04.2005] <http://www.catb.org/~esr/jargon/html/go01.html>

Rossen, Eirik (2005) *Derfor er det slutt på virusflodbølgene*, lokalisert: [21.08.2005] <http://www.digi.no/php/art.php?id=215239>

Sans Institute (2002) *Hacker Techniques, Exploits, and Incident Handling* lokalisert: [12.06.2005] <http://www.sans.org/WashingtonDC/track4.php>

Schreurs, Nard (2005) *Stort zombie-nettverk avslørt*, lokalisert: [11.10.2005] <http://www.computerworld.no/index.cfm/fuseaction/artikkel/id/54219>

Skagmo, Øyvind og Wikström, Solveig (2004) *Caplex leksikon : norges- og verdensatlas, stort tabellverk,* Cappelen, Oslo.

Spafford, Eugene H. (1992) Are Computer Hacker Break-ins Ethical?, *Journal of Systems and Software,* vol. 17 (1), ss. 41-48.

Stallmann, Richard (2005a) *The Free Software Definition*, lokalisert: [07.12.2005] <http://www.fsf.org/licensing/essays/free-sw.html>

Stallmann, Richard (2005b) *Free Software Foundation*, lokalisert: [11.11.2005] <http://www.fsf.org/>

Stallmann, Richard (2005c) *GNU*, lokalisert: [11.11.2005] <http://www.gnu.org/>

Stallmann, Richard (2005d) *The GNU Manifesto*, lokalisert: [04.05.2005] <http://www.gnu.org/gnu/manifesto.html>

Steele jr., Guy L.; , et al. (1983) *The Hacker's dictionary : a guide to the world of computer wizards,* Harper & Row, New York.

Sterling, Bruce (1992) *The hacker crackdown : law and disorder on the electronic frontier,* Bantam Books, New York.

Taylor, Paul A. (1999) *Hackers : crime in the digital sublime,* Routledge, London.

The Hacktivist (2005) *Hacktivist*, lokalisert: [14.05.2005] <http://thehacktivist.com/hacktivism.php>

Tranøy, Knut Erik (1986) *Vitenskapen - samfunnsmakt og livsform,* Universitetsforl., Oslo.

Verisign (2004) *Internet Security Intelligence Briefing*, lokalisert: [23.06.2005], Verisign<http://www.verisign.com/static/017574.pdf>

Wangensteen, Boye;, Norsk språkråd og Universitetet i Oslo . Seksjon for leksikografi og målføregransking (2004) *Bokmålsordboka : definisjons- og rettskrivningsordbok,* Kunnskapsforlaget, Oslo.

Wikipedia (2005a) *Adware*, lokalisert: [13.07.2005]
<http://en.wikipedia.org/wiki/Adware>

Wikipedia (2005b) *Blue Box*, lokalisert: [01.06.2005]
<http://en.wikipedia.org/wiki/Blue_box>

Wikipedia (2005c) *Cyberpunk*, lokalisert: [06.06.2005]
<http://en.wikipedia.org/wiki/Cyberpunk>

Wikipedia (2005d) *Defacement*, lokalisert: [13.10.2005]
<http://en.wikipedia.org/wiki/Defacement_%28vandalism%29>

Wikipedia (2005e) *Denial of Service Attack*, lokalisert: [08.07.2005]
<http://en.wikipedia.org/wiki/Denial-of-service_attack>

Wikipedia (2005f) *Exploit*, lokalisert: [02.06.2005]
<http://en.wikipedia.org/wiki/Exploit_%28computer_security%29>

Wikipedia (2005g) *Hacker*, lokalisert: [20.06.2005]
<http://en.wikipedia.org/wiki/Hacker>

Wikipedia (2005h) *IRC*, lokalisert: [04.06.2005]
<http://no.wikipedia.org/wiki/Irc>

Wikipedia (2005i) *Phishing*, lokalisert: [06.06.2005]
<http://en.wikipedia.org/wiki/Phishing>

Wikipedia (2005j) *Phreaker*, lokalisert: [01.06.2005]
<http://en.wikipedia.org/wiki/Phreak >

Wikipedia (2005k) *Sivil ulydighet*, lokalisert: [18.01.2006]
<http://no.wikipedia.org/wiki/Sivil_ulydighet>

Wikipedia (2005l) *Social engineering*, lokalisert: [13.04.2005]
<http://en.wikipedia.org/wiki/Social_engineering_%28computer_security%29>

Wikipedia (2005m) *Spam*, lokalisert: [13.07.2005]
<http://en.wikipedia.org/wiki/Spam_%28electronic%29>

Wikipedia (2005n) *Spyware*, lokalisert: [13.07.2005]
<http://en.wikipedia.org/wiki/Spyware>

Wikipedia (2005o) *Trojansk hest*, lokalisert: [13.07.2005]
<http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29>

Wikipedia (2005p) *Uncap*, lokalisert: [02.06.2005]
<http://en.wikipedia.org/wiki/Uncap>

Wikipedia (2005q) *Virus*, lokalisert: [13.07.2005]
<http://en.wikipedia.org/wiki/Computer_virus#Definition>

Wikipedia (2006a) *Black hat hacker*, lokalisert: [20.01.2006]
<http://en.wikipedia.org/wiki/Black_hat>

Wikipedia (2006b) *Grey hat hacker*, lokalisert: [21.01.2006]
<http://en.wikipedia.org/wiki/Grey_hat>

Wikipedia (2006c) *White hat hacker*, lokalisert: [20.01.2006]
<http://en.wikipedia.org/wiki/White_hat>

Vedlegg A: Intervjuavtale – Utvalg A

For å tilfredsstille kravene til en mastergrad ved Universitetet i Oslo, vil Ørjan Nordvik gjennomføre en rekke intervjuer som vil danne grunnlaget for forskningen som vil bli presentert i hans masteroppgave.

Formålet med denne masteroppgaven er å gjøre undersøkelser av hva som karakteriserer hackere og crackere. Jeg vil forsøke å finne deres motivasjoner, framgangsmåter og metoder, samt hvordan de er organisert og hvordan de jobber.

Intervjuet vil bli tatt opp på lydbånd for deretter å bli transkribert.

Tilgang til originale transkripsjoner og lydopptak vil kun være tilgjengelig for forskeren, veilederen for oppgaven og ekstern sensor. Ikke under noen omstendigheter vil transkripsjoner, lydopptak eller annet materiale fra disse intervjuene som kan identifisere informanten, være tilgjengelig for andre enn nevnte personer.

Transkripsjonene og eventuelle lydopptak, vil bli oppbevart inntil masteroppgaven er ferdig og karakter er fastsatt. Deretter vil intervjumateriale bli destruert. Prosjektslutt er beregnet til 1. februar 2006.

Ved behandling av sensitive opplysninger, garanteres det for anonymitet. Alle direkte sitat og alt omskrevet materiale må være anonymisert i masteroppgaven, også i offentlige og/eller skolemessige presentasjoner utledet fra det materialet anskaffet gjennom dette intervjuet. Ikke noe informasjon som kan identifisere personen eller hans/hennes tilknytning vil bli brukt i masteroppgaven. Alle navn på personer og bedrifter vil bli erstattet med fiktive navn, som ikke har noe likhet med virkelige navn. Bare kjønn og alder kan bli gjengitt.

Informanten kan reservere seg retten til å editere eller trekke tilbake intervjuet (se Restriksjon #1 nedenfor). Hvis informanten ønsker å benytte seg av denne restriksjonen, vil han/henne motta en transkripsjon av hele intervjuet (eller den delen som er relevant), så fort transkripsjonen foreligger. Hvis dette blir tilfelle, vil kun de delene av intervjuet som er transkribert og godkjent, bli brukt i senere faser i masteroppgaven. Ved mottakelse av transkripsjon fra intervjuet, skal informanten informere intervjueren om han/henne godkjenner transkriberingen eller ber om endringer. Hvis informanten ikke godkjenner transkriberingen, eller det ikke foreligger en enighet om hvordan transkriberingen skal endres, vil intervjuet være ugyldig og skal ikke benyttes i noe forbindelse.

Før et intervju er påbegynt, skal to signerte kopier av denne avtalen foreligge. En kopi beholdes av forskeren og en kopi til informanten.

Ved å signere nedenfor, bekrefter forskeren at han har forklart betingelsene for dette intervjuet, som er beskrevet i denne avtalen. I tillegg skal formålet og hensikten med masteroppgaven være forklart.

Ved å signere nedenfor, bekrefter informanten at han/henne har lest overforstående, og at han/henne har samtykket til intervjuet, med følgende restriksjoner. *(Merk med symbolet «v» hvis restriksjonen ønskes benyttet og merk med symbolet «o» hvis restriksjonen ikke ønskes benyttet):*

___(Restriksjon #1: Tilbakekalling) Transkripsjoner av intervjuet skal presenteres for informanten. Informanten reserverer seg retten til å kreve endringer på transkripsjonen, eller til å tilbakekalle intervjuet hvis det ikke er oppnådd enighet om hvordan transkripsjonen skal endres.

Prosjektet er meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelig datatjeneste.

Intervjudato: _____ Sted: _____

Navn på forsker: _____

Signatur: _____

Navn på informant: _____

Signatur: _____

Skal det vise seg at noen av de personene som har signert ovenfor, har spørsmål om rettigheter i forbindelse med dette intervjuet, kan de kontakte veilederen til intervjueren.

Kontaktinformasjon:

Veileder:

Gisle Hannemyr

Institutt for informatikk
Forskningsparken II
Gaustadalléen 21
0371 Oslo

22 85 24 32

gisle@hannemyr.no

Intervjuer:

Ørjan Nordvik

Institutt for informatikk
Informatikkbygget
Gaustadalléen 23
0371 Oslo

93 00 31 60

onordvik@yahoo.no

Vedlegg B: Intervjuavtale – Utvalg B

For å tilfredsstille kravene til en mastergrad ved Universitetet i Oslo, vil Ørjan Nordvik gjennomføre en rekke intervjuer som vil danne grunnlaget for forskningen som vil bli presentert i hans masteroppgave.

Formålet med denne masteroppgaven er å gjøre undersøkelser av hva som karakteriserer hackere og crackere. Jeg vil forsøke å finne deres motivasjoner, framgangsmåter og metoder, samt hvordan de er organisert og hvordan de jobber.

Intervjuet vil bli tatt opp på lydbånd for deretter å bli transkribert.

Tilgang til originale transkripsjoner og lydopptak vil kun være tilgjengelig for forskeren, veilederen for oppgaven og ekstern sensor. Ikke under noen omstendigheter vil transkripsjoner, lydopptak eller annet materiale fra disse intervjuene som kan identifisere informanten, være tilgjengelig for andre enn nevnte personer.

Transkripsjonene og eventuelle lydopptak, vil bli oppbevart inntil masteroppgaven er ferdig og karakter er fastsatt. Deretter vil intervjumateriale bli destruert. Prosjektslutt er beregnet til 1. februar 2006.

Forskeren kan sitere eller omskrive materiale som er skaffet gjennom intervjuene i sin masteroppgave. Hvis informanten har bedt om anonymitet (se Restriksjon #1 nedenfor), vil ikke noe informasjon som kan identifisere personen eller hans/hennes tilknytning, bli brukt i masteroppgaven. Alle navn på personer og bedrifter vil bli erstattet med fiktive navn, som ikke har noe likhet med virkelige navn. Bare kjønn og alder kan bli gjengitt.

Informanten kan reservere seg retten til å editere eller trekke tilbake intervjuet (se Restriksjon #2 nedenfor). Hvis informanten ønsker å benytte seg av denne restriksjonen, vil han/henne motta en transkripsjon av hele intervjuet (eller den delen som er relevant), så fort transkripsjonen foreligger. Hvis dette blir tilfelle, vil kun de delene av intervjuet som er transkribert og godkjent, bli brukt i senere faser i masteroppgaven. Ved mottakelse av transkripsjon fra intervjuet, skal informanten informere intervjueren om han/henne godkjenner transkriberingen eller ber om endringer. Hvis informanten ikke godkjenner transkriberingen, eller det ikke foreligger en enighet om hvordan transkriberingen skal endres, vil intervjuet være ugyldig og skal ikke benyttes i noe forbindelse.

Før et intervju er påbegynt, skal to signerte kopier av denne avtalen foreligge. En kopi beholdes av forskeren og en kopi til informanten.

Ved å signere nedenfor, bekrefter forskeren at han har forklart betingelsene for dette intervjuet, som er beskrevet i denne avtalen. I tillegg skal formålet og hensikten med masteroppgaven være forklart.

Ved å signere nedenfor, bekrefter informanten at han/henne har lest overforstående, og at han/henne har samtykket til intervjuet, med følgende restriksjoner. *(Merk med symbolet «v»hvis restriksjonen ønskes benyttet og merk med symbolet «o» hvis restriksjonen ikke ønskes benyttet):*

___(Restriksjon #1: Anonymitet) Alle direkte sitat og alt omskrevet materiale må være anonymisert i masteroppgaven, også i offentlige og/eller skolemessige presentasjoner utledet fra det materialet anskaffet gjennom dette intervjuet.

___(Restriksjon #2: Tilbakekalling) Transkripsjoner av intervjuet skal presenteres for informanten. Informanten reserverer seg retten til å kreve endringer på transkripsjonen, eller til å tilbakekalle intervjuet hvis det ikke er oppnådd enighet om hvordan transkripsjonen skal endres.

Prosjektet er meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelig datatjeneste.

Intervjudato: _____ Sted: _____

Navn på forsker: _____

Signatur: _____

Navn på informant: _____

Signatur: _____

Skal det vise seg at noen av de personene som har signert ovenfor, har spørsmål om rettigheter i forbindelse med dette intervjuet, kan de kontakte veilederen til intervjueren.

Kontaktinformasjon:

Veileder:

Gisle Hannemyr

Institutt for informatikk
Forskningsparken II
Gaustadalléen 21
0371 Oslo

22 85 24 32

gisle@hannemyr.no

Intervjuer:

Ørjan Nordvik

Institutt for informatikk
Informatikkbygget
Gaustadalléen 23
0371 Oslo

93 00 31 60

onordvik@yahoo.no

Vedlegg C: Intervjuguide

Tidspunkt:

Sted:

Tilstede:

Briefing

- Fortelle litt om meg selv.
    - Min bakgrunn.
    - Litt om masteroppgaven.
    - Hva jeg er ute etter.
- Få godkjent bruk av båndopptaker.
- Få presentert intervjuavtalen og godkjent denne.
- Hvordan jeg har tenkt å gjennomføre intervjuet:
    - Frie, åpne spørsmål. Samtale hvor informanten prater fritt uten at intervjueren stiller ledende spørsmål.
    - Ingen begrensninger. Snakk fritt!
    - Kanskje noen spørsmål kan virke irrelevante, men kan gi et helhetlig bilde.

Om informanten

- Kan du fortelle litt om deg selv og hva du driver med?
- Hvordan vil du karakterisere deg selv? (Hva vil du karakterisere deg selv som?)

- Hvilken bakgrunn har du?
- Formell kompetanse?
- Er du selvlært eller har du en utdanning?
- Hvilken tilknytning har du til databransjen?
- Hvilken stilling har du i dagliglivet?
- Hva er dine daglige arbeidsoppgaver?
- Hvor lenge har du jobbet med det du gjør?

Terminologi

- Hvordan vil du forklarer ordene; hacker, hacktivist, cracker, datasnok, cyberpunk, phreaker og scriptkiddie?
- Hvordan definerer du datainnbrudd? (Hvor mener DU grensen for det lovlige/ulovlige går?)
- Kan datainnbrudd forsvares? Hvis noen tilfeller, hvilke?

Motivasjon

- Hvorfor ønsker personer å bryte seg inn i andres datasystemer?
- Hva er deres motivasjon? ***(Egne stikkord:)***
    - Personlig vinning?
    - Lære mest mulig om datasystemer?
    - Avdekke svakheter i systemer for å kunne forbedre dem?
    - Interessant?
    - Spenning?
    - Hærverk?
    - Oppmerksomhet?
    - Fokus på manglende sikkerhet?
    - Politisk motiv? Ønsker fri programvare, åpne systemer.

- Ønske om å være destruktiv eller ønske om å gjøre samfunnet en «tjeneste» ved å avdekke sikkerhetshull?

Syn på egen aktivitet

- Hvordan er deres syn på egen aktivitet? ***(Egne stikkord:)*** Legitim? Eventuelt hvorfor?
- Er det saker de brenner for? ***(Egne stikkord:)*** Politisk?

Moral/normer

- Hvordan er moralen deres?
- Har de noen grenser/normer som de selv ikke er villig til å bryte? Hvilke?
- Normer som regulerer deres aktivitet?

Metoder/fremgangsmåter

- Metoder, fremgangsmåter? ***(Egne stikkord:)*** Prøve seg fram? Oppskrifter? Alene? Sammen med andre?
- Metoder for å unngå sporing? Elektroniske spor. (Tekniske spørsmål)
- Hvilke kriterier legger de til grunn for hvem du skal angripe? ***(Egne stikkord:)*** Politisk? Status? Tilfeldig? Tiltrekke oppmerksomhet? Størst mulig utfordring (Microsoft, Pentagon)?
- Hvordan lærer de seg om ulike typer datasystemer?

Organisering

- Hvordan er de organisert? ***(Egne stikkord:)*** Gruppe? Alene?
- Hvordan foregår læring i miljøet?

Informasjonsflyt

- Hvordan kommuniserer de med personer i samme miljø?
- Hvordan frembringer de selv sin informasjon til andre? ***(Egne stikkord:)*** Boards, Internett, Diskusjonsgrupper osv…
- Hvordan får de tak i informasjon? ***(Egne stikkord:)*** Social engineering, Bøker, Internett, Diskusjonsgrupper osv...
- Hvordan ser de på viktighet for å dele informasjon?
- Betrakter de informasjon som en byttevare?

Spesielle spørsmål

Spørsmål som passer den enkelte informant. Saker informanten har et spesielt engasjement til eller saker informanten har vært involvert i.

Debrifing

Nå har jeg ikke flere spørsmål. Har du flere ting du vil ta opp, eller spørre om, før vi avslutter intervjuet?

Takk for intervjuet!