Datainnbrudd

Juridisk oppgave

BACHELOROPPGAVE (BOPPG30)

Politihøgskolen

2017

Kand.nr: 342

Antall ord: 6220

Innholdsfortegnelse

1. Innledning **3**

2. Problemstilling og avgrensning **4**

3. Oppbygning og metode **5**

3.1 Lovtekst 5

3.2 Rettspraksis 5

3.3 Forarbeid til straffeloven 5

3.4 Gammel straffelov 5

3.4 Europarådets konvensjon av 8. november 2001 7

3.5 Juridisk litteratur 7

4. Hva bestemmelsen verner **7**

5. Bryte en beskyttelse **8**

5.1 Sårbarhetsinnbrudd 9

5.2 Passordinnbrudd 10

5.2.1 Phishing som illustrasjon på passordinnbrudd 11

5.3 Tilgangen må være uberettiget 12

6. Annen uberettiget fremgangsmåte **13**

7. Å skaffe seg tilgang **14**

7.1 Eksempler på etterfølgende bruk 16

8. Hva er et datasystem? **17**

8.1 Illustrasjon av hva som omfattes som et datasystem 19

9. Oppsummering **20**

Litteraturliste **22**

Bøker 22

Lovverk 22

Forarbeider 22

Rettsavgjørelser 22

Nettkilder 23

1. Innledning

I bacheloroppgaven min vil jeg ta for meg temaet datainnbrudd, populært omtalt som hacking. Jeg har valg dette temaet på grunn av at jeg har en stor interesse for den digitale verden. Helt fra jeg en liten har jeg holdt på med data og annet teknologisk utstyr, og bygde opp en stor interesse for dette. Etter at jeg begynte på Politihøgskolen fikk jeg også interesse for hvordan digitalt utstyr brukes kriminelt og hvordan man kan etterforske datakriminalitet.

En annen grunn til at jeg valgte dette temaet er at datakriminalitet fører til enorme kostnader over hele verden. Det ble i 2014 anslått at datakriminalitet årlig koster verdenssamfunnet over 400 milliarder amerikanske dollar[1]. Det er også snakk om store kostnader i det norske samfunnet som følge av datakriminalitet. For Norge er det beregnet at datakriminalitet årlig koster 20 milliarder kroner i året.[2]

Informasjonsteknologi har hatt en enorm økning de siste tiårene. Slik teknologi har i dag en stor innvirkning på samfunnet, mange av dem positive. For eksempel har mobilteknologien gjort at vi kan være tilgjengelige til alle døgnets tider, noe som er til stor hjelp om man skulle være i en nødsituasjon og trenger hjelp.

Dessverre har denne utviklingen sine negative sider. Et eksempel på dette er hvor mye sensitiv informasjon om enkeltpersoner som ligger på internett, eller på servere til forskjellige firmaer. Dette kan være sensitive bilder, kontoutskrifter fra banken eller andre personlige opplysninger. Dersom uvedkommende personer får tak i denne informasjonen, kan dette eksempelvis brukes til utpressing av den personen som informasjonen er stjålet fra.

En annen grunn til at jeg skriver om dette temaet, er at jeg synes det virker som kunnskapsnivået innenfor dette området, er noe som bli bedre i politietaten. I praksisåret merket jeg at mange var usikre på hvordan man skal elektroniske spor som blir funnet ute på åstedsundersøkelser. Det sier seg selv at dersom man ikke har nok kunnskap om informasjonsteknologi, vil det ikke være lett å etterforske datakriminalitet.

[1] Center for Strategic and International Studies (2014).
[2] Nasjonal Sikkerhetsmyndighet (2011).

2. Problemstilling og avgrensning

Datainnbrudd kan sees på som en underkategori av datakriminalitet. Datakriminalitet kan defineres som «en straffbar ytring eller handling som er formidlet eller utført ved bruk av datateknologi».[3] Temaet datakriminalitet er et alt for stort tema til å kunne omfattes i en så kort oppgave som dette. I denne oppgaven vil jeg derfor undersøke hva som objektivt sett må til for å straffes for innbrudd i et datasystem, jf. straffeloven § 204. Jeg kommer også til å se på konkrete eksempler på datainnbrudd, for å vise hva som omfattes av straffebudet. Andre temaer innenfor datakriminalitet vil ikke bli behandlet.

For å kunne straffes må alle straffbarhetsvilkårene i straffebudet være oppfylt. I denne oppgaven vil jeg ha særlig fokus på den objektive gjerningsbeskrivelsen i straffebudet. Skyldkravet for overtredelse av straffeloven § 204 er forsett, jf. straffeloven § 21. Utover dette kommer jeg ikke til å behandle de subjektive vilkårene, vurdering av tilregnelighet eller straffefrihetsgrunner.

Straffenivået for brudd på straffeloven § 204 er bot eller fengsel inntil 2 år. Det vil være flere forhold som vil ha innvirkning på hvor høyt straffenivået blir satt i den enkelte saken, men det er noe jeg ikke kommer ikke til beskrive i denne oppgaven. Jeg går heller ikke inn på hvor høyt rettspraksis setter straffen i hver enkelt sak.

Siden strafferammen for datainnbrudd er inntil 2 år fengsel, og det ikke er uttrykkelig er bestemt noe annet i lovbestemmelsen, er forsøk på å gjennomføre et datainnbrudd er også straffbart, jf. straffeloven § 16, 1. ledd. Et forsøk på datainnbrudd kan være en som prøver å bryte seg gjennom en beskyttelse til et datasystem, men ikke får det til. Dette kan være på grunn av at han ikke har nok kunnskap om hvordan datasystemet er bygget opp, ikke har gode nok ferdigheter eller ikke har dette rette utstyret for å bryte seg inn. På grunn av oppgavens lengde, kommer jeg ikke til å gå mer inn på forsøk.

[3] Sunde (2016) s. 17

3. Oppbygning og metode

3.1 Lovtekst

Hoveddelen av oppgaven vil gå til å drøfte lovteksten i straffeloven § 204, noe jeg vil gjøre ved bruk av juridisk metode. Juridisk metode er en prosess vi går gjennom for å finne svar på forskjellige rettsspørsmål. I denne delen av oppgaven vil jeg drøfte hvert enkelt vilkår som er nevnt i lovbestemmelsen. Straffeloven § 204 lyder slik:

«Med bot eller fengsel inntil 2 år straffes den som ved å bryte en beskyttelse eller ved annen uberettiget2 fremgangsmåte skaffer seg tilgang til datasystem eller del av det.»

3.2 Rettspraksis

Det er ikke lenge siden Norge fikk en ny straffelov, og det gjør at det enda ikke er mange rettsavgjørelser angående straffeloven § 204. Det ble i forarbeidene til den nye straffeloven uttrykkelig sagt at praksis rundt den gamle bestemmelsen fortsatt vil være relevant.[4] Derfor vil jeg, når det er hensiktsmessig, bruke rettsavgjørelser som omhandler straffeloven 1902, § 145, 2. ledd. Jeg vil da også drøfte om disse rettsavgjørelsene fortsatt er relevante, etter at Norge gikk over til den nye straffelov.

3.3 Forarbeid til straffeloven

Ot.prp.nr.22 (2008-2009), som er forarbeidet til straffeloven av 2005, er noe som kommer til å stå sentralt i drøftelsesdelen av denne oppgaven. Dette fordi det er forarbeidet som danner grunnlaget for lovteksten, noe som gjør den til en viktig del av oppgaven, siden det sier hva lovgiver ønsker med innholdet i straffebudet.

3.4 Gammel straffelov

Jeg kommer til å se på forskjellen mellom straffeloven fra 1902 og straffeloven fra 2005, for å se om det har skjedd en realitetsendring. Enkelte forskjeller mellom den nye og gamle straffeloven vil behandles fortløpende i oppgaven når de blir aktuelle. Det er likevel noen momenter som er viktig å merke seg, og som ikke naturlig hører til noen av kapitlene i denne

[4] Ot.prp.22 (2008-2009) s. 403.

oppgaven. Disse momentene vil derfor bli behandlet her. Straffeloven 1902 § 145, 2. ledd, lød slik:

«Det samme gjelder den som uberettiget skaffer seg adgang til data eller programutrustning som er lagret eller overføres ved elektroniske eller andre hjelpemidler».

Den gamle straffebudet vernet altså både data som var lagret og data som ble overført. Med data menes elektroniske signaler, som ved hjelp av et datasystem eller elektronisk kommunikasjonsnett, lagres, behandles eller overføres.[5] Dette kan for eksempel være bilder, videoer, musikkfiler mm.

I den nye straffeloven er dette splittet opp i to forskjellige bestemmelser. Straffeloven § 204 verner data som er lagret, mens straffeloven § 205, bokstav b verner data som overføres. Denne oppdelingen av det gamle straffebudet ble i forarbeidene vurdert som hensiktsmessig, fordi det å skaffe seg tilgang til data under overføring er av en annen karakter, sammenlignet med det å skaffe seg tilgang til data som er lagret.[6] Dette betyr at det nye straffebudet ikke kan anvendes på samme måte som det gamle, da det nye straffebudet kun verner data som er lagret. Selv om det gamle straffebudet har blitt splittet opp, er ikke dette en endring som medfører store realitetsendringer, da begge forholdene fortsatt er vernet av straffeloven.

Et annet punkt som er verdt å merke seg er hvordan strafferammen var splittet opp i det gamle straffebudet. I utgangspunktet var strafferammen fengsel, bøter inntil 6 måneder eller begge deler, jf. ordlyden i straffeloven 1902 § 14, 2. ledd «Det samme gjelder …». Det siktes her til strafferammen som er satt i 1. ledd. Det som er verdt å merke seg er at det i 3. ledd i det gamle straffebudet fantes straffeskjerpende momenter, som gjorde at fengselsstraff inntil 2 år kunne anvendes.

Dette er heller ikke noe som er videreført i straffeloven 2005 § 204, hvor strafferammen for alle brudd på straffebudet er bøter eller fengsel inntil 2 år. Det er ikke straffeskjerpende momenter i det nye straffebudet. Det ble i forarbeidet til den nye straffeloven likevel poengtert at den øverste delen av strafferammen var tiltenkt de grove overtredelsene.[7]

[5] NOU 2007:2 s. 61.
[6] Ot.prp.nr. 22 (2008-2009) s. 51
[7] Ot.prp.nr.22 (2008-2009) s. 403

3.4 Europarådets konvensjon av 8. november 2001

Jeg kommer enkelte steder i oppgaven til å se på Norges ratifikasjon av Europarådets konvensjon av 8. november 2001, artikkel 2, for å se om det norske regelverket oppfyller kravene i konvensjonen. På grunn av betydningen ratifikasjonen hadde for utviklingen av lovverket, er dette noe som ikke burde oversees. For enkelthets skyld vil jeg når jeg referer til denne konvensjonen, kun kalle den for «konvensjonen».

3.5 Juridisk litteratur

Det er ikke mye juridisk litteratur som er skrevet om dette temaet, og er derfor ikke noe som vil bli benyttet i stor grad i denne oppgaven. Jeg kommer likevel til å benytte to bøker av Inger Marie Sunde, som begge omhandler datakriminalitet.[8]

4. Hva bestemmelsen verner

Ett datainnbrudd er kjennetegnet ved at man bryter seg inn i et datasystem for å få tilgang til data som er beskyttet.[9] Gjennom et datainnbrudd får en gjerningsperson mulighet til å kjøre programmer som finnes på systemet, i tillegg til at han får tilgang til data som er lagret på datasystemet.

Datakrimutvalget nevner tre forhold som straffebudet må verne om: konfidensialitet, integritet og tilgjengelighet. Ved et datainnbrudd får uvedkommende kjennskap til data som er lagret på datasystemet (konfidensialitet). Videre kan dataene som er lagret urettmessig bli endret (integritet). I tillegg vil et datainnbrudd føre til at datasystemet blir belastet, som gjør at brukbarheten for den rettmessige innehaveren blir svekket (tilgjengelighet).[10]

Straffeloven § 204 dekker kun selve innbruddet i datasystemet. Det dekker ikke handlinger som skjer etter at datainnbruddet er fullbyrdet, for eksempel uautorisert bruk av datasystemet eller endring av data som er på datasystemet, som henholdsvis blir dekket av straffeloven § 343 og § 351.[11] Dette er også i samsvar med forarbeidet til straffebudet, hvor det står at

[8] Inger Marie Sunde, *Lov og rett i cyberspace: internettkriminalitet og etterforskningsmetoder* Bergen, 2006 og Inger Marie Sunde, *Datakriminalitet: En fremstilling av strafferettslige regler om datakriminalitet,* Bergen 2016.
[9] Politiet.no, 2015.
[10] NOU 2007:2 s. 22.
[11] Sunde (2016) s. 71

bestemmelsen kun indirekte verner informasjon ved å hindre tilgang til informasjonen. Det som straffes er kun det uautoriserte innbruddet i datasystemet.[12]

Man må derfor bruke flere straffebud i konkurrens for å fullt ut verne om forholdene som Datakrimutvalget listet opp. Dette temaet vil bli videre behandlet i kapittel 7.1. Det er verdt å merke seg, at dersom straffebud brukes i konkurrens vil dette ha betydning for straffeutmålingen, jf. straffeloven § 79, 1. ledd, bokstav a.

5. Bryte en beskyttelse

Det første objektive vilkåret som fremkommer i lovteksten, er at gjerningspersonen må «… bryte en beskyttelse …». Når man hører dette, vil nok mange tenke på en hacker som bryter seg gjennom en brannmur, noe man ofte ser på film. Brannmur er en programvare som beskytter et datasystem, eller et større nettverk. Det er likevel flere handlinger som vil gå under vilkåret om å bryte en beskyttelse, noe jeg behandler senere i kapittelet.

Historisk sett har vilkåret om å måtte bryte en beskyttelse vært noe omstridt. I Datakrimutvalgets utredning om datakriminalitet fra 1985, konkluderte de med at det var innehaveren av anlegget som hadde ansvar for beskyttelse mot innsyn fra uberettigede.[13] Vilkåret om å bryte en beskyttelse, ble fjernet fra den tidligere straffeloven ved lovendring 8. april 2005 nr. 16. Grunnlaget for endringen kom i en uttalelse fra Økokrim, om at det strafferettslige vern om data burde være på linje med det man har for andre gjenstander. Det stilles ikke noe krav om at en gjenstand skal være beskyttet for at den som stjeler den blir tiltalt for tyveri.[14] Vilkåret har nå blitt gjeninnført i den nye straffeloven, da dette regnes for å være den mest praktiske måten å gjennomføre datainnbrudd på.[15]

Datakrimutvalget anbefalte at dette ikke skulle være i et vilkår i den nye straffeloven, noe de begrunnet med tre argumenter:

- Selv om et datasystem er passordbeskyttet, vil det fortsatt være sårbart ved inntrengning ved sårbarhetsinnbrudd.

[12] Ot.prp.nr.22 (2008-2009) s. 403
[13] NOU 1985:31 s. 31.
[14] Innst.O.nr.53 (2004-2005) s. 5.
[15] Ot.prp.nr.22 (2008-2009) s. 51

- Det kan fortone seg et kunstig skille mellom beskyttede og ubeskyttede systemer i absolutt forstand, da man aldri vil kunne sikre seg helt mot datainnbrudd.
- Anvendelse av tilgangskontroll har ingen betydning for datainnbrudd som skjer ved sårbarhetsinnbrudd. Siden tilgangskontroll ikke har noen funksjon ved denne metoden, vil det være meningsløst med et vilkår om at datasystemet skal være beskyttet.[16]

Likevel ble det dette vilkåret ansett som det mest praktiske alternativet, og det ble derfor særskilt nevnt i loven.[17] Det som er viktig å huske på her, er at det å bryte en beskyttelse ikke er et kumulativt vilkår, jf. ordlyden «… eller ved annen uberettiget fremgangsmåte …» i lovbestemmelsen. Man kan med andre ord straffes for datainnbrudd, selv om man ikke har brutt en beskyttelse. Et eksempel på å bryte seg inn i et datasystem uten å bryte en beskyttelse, er å først skaffe seg brukerinformasjonen til en som har berettiget adgang til systemet, og bruke dette for å få tilgang til datasystemet. Dette er noe jeg vil beskrive nærmere i kapittel 6.

Når man snakker om å bryte en beskyttelse, er det primært to metoder som benyttes for å gjennomføre et datainnbrudd, enten ved passordinnbrudd eller sårbarhetsinnbrudd.[18] I det følgende vil jeg gå inn på hva disse to metodene innebærer.

5.1 Sårbarhetsinnbrudd

Alle dataprogrammer inneholder feil, det er ikke mulig å lage et feilfritt program. Innenfor teknologiverdenen kalles disse feilene for bugs, og kan utnyttes på forskjellige måter. Dersom bugen er av en slik karakter at den fører til utilsiktet virkning i programmet, blir den omtalt som en sårbarhet. Brukes denne sårbarheten til å skaffe seg tilgang til et datasystem, snakker vi om et sårbarhetsinnbrudd. Å benytte slike sårbarheter til å fremkalle utilsiktede virkninger, kalles for exploits, eller utnyttelse oversatt til norsk.[19]

Et praktisk eksempel på sårbarhetsinnbrudd finner vi en dom fra Agder lagmannsrett, hvor en mann ble dømt til 60 timers samfunnsstraff for datainnbrudd.[20] På tiden dommen ble var ikke den nye straffeloven trådt i kraft. Mannen ble derfor domfelt for overtredelse av straffeloven 1902 § 145, 2. ledd. Dommen er likevel relevant for å illustrere det å bryte en beskyttelse, og

[16] NOU 2007:2 s. 78.
[17] Ot.prp.nr.22 (2008-2009) s. 403.
[18] Sunde (2016) s.76.
[19] NOU 2007:2 s. 23.
[20] LA-2003-83

vil derfor være anvendbar ovenfor straffeloven 2005 § 204. Dette fordi de objektive vilkårene som den gangen ble vurdert under hovedforhandlingen, tilsvarer de vilkårene som vi finner i den nye straffeloven.

Domfelte var ansatt i et firma som tilbudte flere tjenester, blant annet en tjeneste en SMS-tjeneste hvor man får varsel om politiets trafikkontroller. Domfelte brøt seg inn i en database til en konkurrerende nettside som tilbudte samme tjenesten. Serveren som domfelte brøt seg inn i var passordbeskyttet. Dette gjorde han ved hjelp av programmer han hadde lastet ned fra internett.

Det første han gjorde var å skanne et større antall servere som var koblet til internettet. Da han skannet serveren til det konkurrerende firmaet, fant han en programvarefeil. Domfelte utnyttet denne feilen til å trenge inn i serveren til konkurrenten. Her har han med andre ord gjennomført et sårbarhetsinnbrudd, ved å bruke svakheter i programvaren til å gjennomføre datainnbruddet.

Denne saken ble også brakt inn for høyesterett, men dette var på grunn av andre forhold i samme sak. Høyesterett sa seg enig med lagmannsretten, men ila i tillegg domfelte et bot på 10.000 kroner, noe de grunnla med allmennpreventive hensyn.[21]

5.2 Passordinnbrudd

Passordinnbrudd er en utbredt form for datainnbrudd, hvor gjerningspersonen skaffer seg brukerinformasjonen (brukernavn og passord) til en som har rett til å bruke systemet. Dette er gjerne skaffet gjennom urettmessige metoder, for eksempel dataavlytting. Ved bruk av denne metoden får gjerningspersonen de samme bruker rettighetene som den rettmessige brukeren har.[22]

Et eksempel på passordinnbrudd finner vi i en dom, populært kalt Photobucket-dommen, som er omhandlet i Rt. 2012 s. 1669. Domfelte hadde her i første omgang brutt seg inn i databasen til nettsiden photobucket.com. Dette er å anse som et sårbarhetsinnbrudd, men i domfeltes etterfølgende bruk av databasen ble det gjennomført flere datainnbrudd hvor passordinnbruddsmetoden ble benyttet.

[21] Rt. 2004 s. 94
[22] NOU 2007:2 s. 22.

Databasen til Photobucket inneholdt blant annet e-postadresser, brukernavn og passord til alle brukerne av nettsiden, som på den tiden var omtrent 66 millioner. Domfelte kopierte disse og lagret disse på egen maskin. Han fant så ut at mange av brukerne brukte samme brukernavn og passord på andre nettsteder, og brukte dette til for eksempel å logge seg inn på andres e-postkontoer.[23] Domfelte brøt seg inn i 187 forskjellige e-postkontoer ved bruk av denne metoden, som er å anse passordinnbrudd.

Under hovedforhandlingen i tingretten[24], ble alle disse datainnbruddene samlet under en tiltalepost. Isolert sett vil likevel hvert enkelt innbrudd være å anse som et straffbart forhold, da hvert enkelt datainnbrudd er en selvstendig handling. Hvert datainnbrudd var en manuell handling fra tiltale, det var ikke noe som skjedde automatisk. Det vil da være relevant å anvende realkonkurrens, som vil ha innvirkning på straffenivået, jf. straffeloven § 79, 1. ledd bokstav a.

5.2.1 Phishing som illustrasjon på passordinnbrudd

Det finnes flere måte en gjerningsperson kan skaffe seg brukerinformasjon. En svært utbredt metode er det som kalles for phishing. Den vanligste måten å gjennomføre dette på er at gjerningsmannen sender en e-post til personen som er målet for angrepet. I e-posten utgir gjerningsmannen seg for å være noen andre som offeret stoler på, for eksempel en bank.[25] Det kommer så frem i e-posten at offeret må oppdatere bruker informasjonen sin til banken, og legger ved en lenke som tilsynelatende linker til nettstedet til banken. I virkeligheten går den linken til en nettside som for brukeren ser identisk ut til den virksomheten gjerningsmannen utgir seg for å være.[26]

Når offeret deretter skriver inn sin nye brukerinformasjon, blir dette sendt direkte til gjerningsmannen. Siden mange bruker samme brukerinformasjon på forskjellige nettsteder, vil gjerningspersonen nå kunne få tilgang til brukerkontoene hvor offeret benytter seg av samme brukerinformasjon. Det trengs heller ikke store ressurser for å gjennomføre dette, da slike e-poster kan sendes ut til mange mottakere.

[23] Rt. 2012 s. 1669
[24] TOSLO-2010-62157
[25] Sunde (2016) s. 137
[26] Bøe H. O., Hornnes E. M., Mykland H. O., Nätt T. Heine (2012) s. 114

En lignende metode ble nylig brukt i et russisk hackerangrep mot organisasjoner i Norge.[27] I denne saken ble det benyttet såkalt spear-phishing, som er en målrettet form for phishing. Ofre blir nøye utvalgt, gjerne på bakgrunn av deres posisjon i en organisasjon, i dette tilfellet var personer innenfor blant annet PST og Forsvaret.

5.3 Tilgangen må være uberettiget

Av ordlyden i straffebudet «… ved å bryte en beskyttelse eller ved annen uberettiget fremgangsmåte …» fremgår det at tilgangen må være uberettiget, ikke bare når det er snakk om annen fremgangsmåte, men også når vilkåret om å bryte en beskyttelse anvendes. Vilkåret om at tilgangen må være uberettiget ved annen fremgangsmåte, vil bli behandlet i neste kapittel.

Dersom noen har brutt en beskyttelse for å komme seg inn i et datasystem, vil nok mange se på det som en selvfølge at tilgangen er uberettiget. Det er likevel noen situasjoner hvor en slik tilgang ikke kan regnes som uberettiget, og jeg vil i det følgende behandle et slikt eksempel.

Det er i dag svært vanlig at innehaveren av et datasystem prøver å bryte seg inn i sitt eget datasystem. Dette gjøres for å teste sikkerheten til systemet, og for å avdekke sårbarheter. Det er også vanlig at folk med spesiell kompetanse blir ansatt for å drive med slik sikkerhetstesting. Dersom man bryter seg inn i et datasystem på denne måten, vil ikke dette kunne anses som en uberettiget tilgang, da den som bryter seg inn allerede har berettiget tilgang.

Det er likevel ikke slik at sikkerhetstesting automatisk gjør at tilgangen blir berettiget, noe som vises i en dom fra Borgarting lagmannsrett.[28] Domfelte mente at flere teleselskaper ikke oppbevarte personopplysninger på en sikker måte. For å vise dette konstruerte han selv en programvare som hentet ut personopplysninger fra teleselskapet Combitel. Domfelte fikk personopplysninger om totalt 72.269 personer. Selv om intensjonen til domfelte var god, ble han dømt for overtredelse av straffeloven 1902 § 145, 2. ledd, jf. 1. og 3. ledd. Dette var ikke en handling som ble gjennomført på oppdrag av Combitel, og tilgangen til personopplysningene som domfelte tilegnet seg, måtte vurderes til uberettiget.

[27] NRK.no (2017)
[28] RG. 2011 s. 328

Ut fra denne dommen kan vi si at det å ha gode intensjoner ikke, er nok til å gjøre en slik sikkerhetstest berettiget. Man må ha uttrykkelig samtykke fra innehaveren av systemet om at slik sikkerhetstesting kan gjennomføres, før tilgang blir berettiget.

6. Annen uberettiget fremgangsmåte

Straffebudet dekker også datainnbrudd som er gjennomført ved «… annen uberettiget fremgangsmåte …». Det vil si i tilfeller hvor gjerningspersonen har trengt seg inn i et datasystem, uten å bryte en beskyttelse. Straffebudet gir ingen eksempler som veiledning for vurderingen av om tilgangen er uberettiget. Hva som er å anse som uberettiget fremgangsmåte er derfor en skjønnspreget rettsstridsvurdering. Rettspraksis av straffeloven § 1902 § 145, 2. ledd vil være relevant for vurderingen om en tilgang er berettiget eller uberettiget, noe som fremkommer av forarbeidene til den nye straffeloven.[29]

Det er verdt å merke seg at straffeloven 1902 ikke hadde dette vilkåret. Det som var gjeldende da, var «… den som uberettiget skaffer seg adgang …». Dette er viktig å huske på, fordi rettspraksisen da aldri kunne konkludere med at det var brukt annen uberettiget fremgangsmåte. Man må derfor selv skille mellom datainnbrudd som er gjennomført ved beskyttelsesbrudd eller ved annen uberettiget fremgangsmåte når man leser gjennom rettspraksis knyttet til den gamle straffeloven.

Datakrimutvalget mente som sagt at det ikke burde være et vilkår om at et datainnbrudd skjer ved å bryte en beskyttelse. De mente at rettstridvilkåret, altså at tilgangen er uberettiget, alene ville være tilstrekkelig.[30] I sin vurdering la Datakrimutvalget til grunn at lovovertrederen ikke skal ha rettslig grunnlag for tilgangen, og at han må være klar over at han ikke har det for at han skal kunne straffes. Selv om utvalgets anbefaling om å ikke ha et vilkår om brudd på beskyttelse i straffebudet, vil den øvrige vurderingen være relevant for hvordan loven skal tolkes. Dette fordi det har sammenheng med vilkåret annen uberettiget fremgangsmåte.

Mannen som ble dømt i Photobucket-saken, var i samme sak tiltalt for å ved uberettiget fremgangsmåte sett på og kopiert innhold fra en datamaskin som tilhørte en bekjent av ham.

[29] Ot.prp.nr. 22 (2008-2009) s. 403
[30] NOU 2007:2 s. 78

Eieren av datamaskinen hadde fått et virus på datamaskinen, og spurt domfelte om han kunne fikse den. I sammenheng med dette, fikk domfelte overlevert passordet til datamaskinen av den bekjente. Domfelte hadde med andre ord lovlig tilgang til datamaskinen. Problemstillingen oppstod imidlertid da domfelte gikk se og kopierte privat innhold på datamaskinen som ikke var omfattet av avtalen mellom domfelte og den bekjente.

Høyesterett kom her fremt til at domfelte ikke kunne dømmes for datainnbrudd, da adgangen han hadde til datamaskinen ikke var uberettiget, dette på grunn av at domfelte på berettiget måte hadde fått passordet til datamaskinen. [31]

Et annet eksempel er der man får tilgang til en datamaskin som er utstyrt med tilgangskontroll, men denne ikke er aktivert. Med tilgangskontroll menes det kreves for eksempel passord og brukernavn for å få tilgang til innholdet på en datamaskinen. At tilgangskontrollen ikke er aktivert kan skje når at du går bort fra datamaskinen din, uten å aktivere skjermlåsen. Innholdet på datamaskinen står altså åpen for alle som er i nærheten, uavhengig om de har brukerrettighet på den eller ikke.

Problemstillingen her er om det å benytte denne tilgangen uten samtykke, er tilstrekkelig for å vurdere hendelsen som annen uberettiget fremgangsmåte. Det må i så fall kreves at handlingen er i strid med hva som regnes som akseptabel atferd på det aktuelle livsområdet. Handlingen må i tillegg være kvalifisert klandreverdig.[32] Det å bruke denne tilgangen uten samtykke kan derfor ses på som uberettiget tilgang. Det er likevel ikke noe rettspraksis som løser denne problemstillingen.

7. Å skaffe seg tilgang

Dette vilkåret må sees i sammenheng med de forannevnte vilkårene «bryte en beskyttelse» og «annen uberettiget fremgangsmåte». Bruddet på beskyttelsen eller andre uberettigede fremgangsmåter skal føre til at gjerningspersonen skaffer seg tilgang.

Ut fra denne ordlyden er det verdt å merke seg at straffebudet har et avgrenset anvendelsesområde. Straffebudet dekker kun selve handlingen om å skaffe seg adgangen til

[31] Rt. 2012 s. 1669
[32] Sunde (2016) s. 82

datasystemet. Gjerningspersonen trenger altså ikke å ha gjort seg kjent med innholdet på datasystemet for at han skal kunne straffes. Det dekker ikke hva en gjerningsperson gjør med datasystemet gjør i etterkant av at han har skaffet seg denne tilgangen.[33]

Det er sjeldent at en gjerningsperson bryter seg inn i et datasystem, uten å gjøre noe mer med datasystemet han får tilgang til. Svært ofte vil han ha et mål med datainnbruddet, og derfor foreta seg andre handlinger etter at han har brutt seg inn. Hva disse handlingene består av vil variere, men kan for eksempel være endring eller sletting av data eller installering av skadelig programvare på fornærmedes datasystem.

Noe som må regnes som en positiv konsekvens av at straffebudet kan bli anvendt så fort gjerningspersonen har brutt seg inn i datasystemet ditt, er at det vil føre til et sterkere vern av det teknologiske utstyret ditt. Terskelen for når straffebudet er overtrådt er liten. Man kan også sammenligne dette med et helt vanlig innbrudd i et hus. Det holder at en gjerningsperson uberettiget har skaffet seg adgang til huset ditt for at han skal kunne straffes etter straffeloven § 268. Hva han gjør inne i huset er ikke av betydning for anvendelse av det straffebudet.

Etter konvensjonens artikkel 2 var det valgfritt for partene om straffebudet måtte kreve at innbruddet ble foretatt med hensikt om å skaffe seg data, eller at overtrederen hadde annen uærlig hensikt, jf. ordlyden «… that the offence be comitted … with the intent of obtaining computer data or other dishonest intent …».[34] Dette var likevel ikke et krav, og lovgiver i Norge valgte å ikke implementere dette, og straffebudet er derfor oppfylt allerede dersom tilgangen til datasystemet er oppnådd.

Det er her en språklig forskjell sammenlignet med straffeloven 1902 § 145, 2. ledd, hvor ordlyden var «… skaffer seg adgang …». Adgang er i den nye straffeloven endret til «tilgang». Den nye ordlyden ble i forarbeidene vurdert til å være mer dekkende språklig sett. Det var likevel ikke ment at dette skulle føre til en realitetsendring.[35]

[33] Ot.prp.nr.22 (2008-2009) s. 403
[34] Ot.prp.nr. 40 (2004-2005) s. 12
[35] Ot.prp.nr. 22 (2008-2009) s. 403

7.1 Eksempler på etterfølgende bruk

Siden datainnbrudd oftest skjer i sammenheng med andre straffbare handlinger, må man som nevnt i kapittel 5 anvende straffebudet i konkurrens med andre straffebud som dekker handlingene som blir foretatt etter innbruddet. Som nevnt tidligere dette ha innvirkning på straffenivået, jf. straffeloven § 79, 1. ledd, bokstav a.

Jeg vil i det følgende kort gå inn på andre straffebud som kan være relevante i sammenheng med bestemmelsen om datainnbrudd. Dette er ikke ment å være en uttømmende liste over hva som er å regne som etterfølgende bruk, det er kun ment som eksempel på hva den etterfølgende bruken kan bestå av.

Dersom gjerningspersonen bruker tilgangen han har skaffet seg til å søke gjennom og kartlegge informasjonen som ligger på datasystemet, vil dette rammes av straffeloven § 343, som gjør ulovlig bruk av løsøre straffbart.

Har gjerningspersonen uberettiget endret data som finnes på datasystemet, er dette å anse som skadeverk, jf. straffeloven § 351.[36] Endring av data omfatter endring av innholdet som er på datasystemet, samt sletting eller opprettelse av filer.

Dersom man installerer programvare som loggfører all data som blir sendt og mottatt på en datamaskin, vil dette dømmes etter straffeloven § 205, bokstav b.

En dom fra Høyesterett[37] gir et fint eksempel på hvordan man skal vurdere datainnbrudd og etterfølgende bruk i praksis. Her hadde domfelte brukt en trojaner til politiet bryte seg inn i DnB NORs nettbankløsning. Etter at han hadde skaffet seg tilgang, brukte han den til å overføre penger fra bankens kunder til andre kontoinnehavere. Domfelte fikk tilgang til 25 bankkontoer, og overførte totalt 809.883,- fra disse kundene til andre personer.

Mannen ble domfelt for straffeloven 1902 § 145, 2. ledd, for å ha brukt trojaneren til å skaffe seg tilgang til nettbanken. En trojaner er en programvare som fremstår som legitim og ufarlig, og gjerne utgir seg for å være en nyttig applikasjon for datamaskinen din. Det som skjer når du laster ned trojaneren, er at den lager en bakdør til systemet ditt. Denne bakdøren gir

[36] Sunde (2016)
[37] Rt. 2012 s. 1968

gjerningspersonen full tilgang datasystemet ditt. I mange tilfeller vil trojaneren være godt skjult, og kan ligge uoppdaget over lang tid.

Den videre bruken, hvor domfelte overførte penger fra en konto til en annen, må sees på som en egen straffbar handling. Domfelte ble for dette for grovt bedrageri etter straffeloven 1902 § 271, jf. § 270, 1. ledd, nr. 2.

8. Hva er et datasystem?

Det siste vilkåret i straffebudet er at datainnbruddet må være rettet mot et «… datasystem eller del av det …». Når man hører datasystem, er det nok mange som ser for seg at dette vilkåret kun dekker datamaskiner, nettbrett og mobiltelefoner. Altså enheter som enten er eller har samme virkeområde som en tradisjonell datamaskin.

I forarbeidene blir et datasystem definert som «enhver innretning bestående av maskinvare og data, som foretar behandling av data ved hjelp av dataprogrammer».[38] Dette betyr at for at noe skal bli ansett som et datasystem, må det kunne foreta automatisk databehandling.[39] Denne definisjonen omfatter mange elektroniske innretninger som vi bruker hver dag. I tillegg til datamaskiner og mobiltelefoner, omfatter den juridiske definisjonen av et datasystem mer enn mange ser for seg, blant annet TV'er, moderne biler og til og med oppvaskmaskiner.

Det er også elektroniske innretninger som selvstendig ikke kan ansees som et datasystem, for eksempel eksterne harddisker eller andre lagringsmedier. Disse anses ikke som datasystem, fordi de ikke alene kan utføre automatiske databehandlinger. Men når den eksterne harddisken kobles til en datamaskin, kan innholdet på harddisken leses og endres, og vil da ansees som en del av datasystemet når den er tilkoblet.[40]

I forarbeidene nevnes det spesifikt at dersom man med utgangspunkt i sin egen brukerkonto, uberettiget trenger seg inn på andres brukerkontoer eller den administrative delen av et datasystem, vil dette omfattes av straffebudet, med henvisning til ordlyden «… del av det».[41] Denne beskrivelsen tilsvarer hendelsesforløpet i Photobucket-saken, som er omhandlet

[38] Ot.prp.nr 22 (2008-2009) s. 400
[39] Sunde (2016) s. 42
[40] Sunde (2016) s. 74
[41] Ot.prp.nr 22 (2008-2009) s. 403

tidligere i oppgaven. Domfelte installerte et dataprogram på brukerkontoen sin hos Photobucket, noe som gjorde at han fikk tilgang til serveren til selskapet. Det var slik domfelte fikk adgang til brukerinformasjonen, som han senere brukte til å bryte seg inn på flere e-postkontoer.[42]

Hvorfor forarbeidene spesifikt nevner denne fremgangsmåten, kommer ikke frem. Det ble trolig gjort fordi dette er en vanlig måte å gjennomføre datainnbrudd på. Det gjør også at påtalemyndigheten og domstolene ikke er i tvil om at en slik fremgangsmåte ikke er lovlig.

Domfelte i den saken var som nevnt også tiltalt for datainnbrudd på en bekjents datamaskin, men domfelte ble frifunnet for dette. Domfelte skulle hjelpe den bekjente med å fjerne virus på datamaskinen. Da domfelte gjorde dette, kopierte han samtidig personlig informasjon om den bekjente, blant annet personnummer og kontonummer. Domfelte ble frifunnet på dette tiltalepunktet, fordi den bekjente frivillig hadde gitt domfelte tilgang til hele datamaskinen.

Her har det imidlertid oppstått et skille mellom straffeloven av 1902 og 2005, som antageligvis ville hatt innvirkning på utfallet av denne saken hadde den blitt tatt opp i retten i dag. I straffeloven av 1902 var ordlyden «… den som uberettiget skaffer seg adgang til data eller programutrustning …». I straffeloven av 2005 er dette gjort om, slik at straffebudet rammer den som «… skaffer seg tilgang til datasystem eller del av det». I forarbeidene til den nye straffeloven, ble det sagt at ordlydsendringen ikke var ment å innebære noen realitetsendringer.[43] Det er likevel en viktig forskjell mellom ny og gammel straffelov. I tillegg til å verne et datasystem, verner den nye straffeloven også selvstendige deler av et datasystem. Det gjorde ikke den gamle straffeloven.

Avtalen som var mellom domfelte og hans bekjente, var at domfelte skulle fikse datamaskinen. Det var ikke gitt samtykke til å gå inn på privat innhold på datamaskinen. Da domfelte gikk inn på det private innholdet, som ikke var omfattet av avtalen dem imellom, kan det ses på som at han uberettiget gikk inn på en del av datasystemet. Det kan derfor være at han kunne blitt dømt etter det nye straffebudet, men det foreligger foreløpig ikke rettspraksis som har avklart lignende tilfeller.

[42] Rt. 2012 s. 1669
[43] Ot.prp.nr 22 (2008-2009) s. 51

8.1 Illustrasjon av hva som omfattes som et datasystem

En type kriminalitet som er verdt å merke når man drøfter hva som er et datasystem, er skimming. Skimming gjennomføres som regel ved at gjerningspersonen fester en falsk kortleser på en minibank. Disse kortleserne kan se helt like ut til de som opprinnelig er på minibanken, og kan være svært vanskelig å oppdage. Når bankkundene skal ta ut penger av minibanken, leser den falske kortleser av magnetstripen på bankkortet som blir satt inn. Kortleseren lagrer så informasjonen om kortet. I tillegg har gjerningspersonen montert et kamera over minibanken, slik at han ser hvilken pinkode som blir tastet inn.

Gjerningspersonen kan så i etterkant lage falske bankkort med den informasjonen som er lagret på kortleseren og kameraet. Når gjerningspersonen benytter det falske bankkortet, vil det være eier av det originale bankkortet som får kontoen sin belastet.

Det som er interessant her, er at når bankkortet blir satt inn i kortleseren, kobler kortet seg til banksystemet, og er derfor å anse som en del av et datasystem. Skimming vil derfor være å anse som et datainnbrudd, og tiltales etter straffeloven § 204. Ved skimming skaffer gjerningspersonen seg tilgang til del av et datasystem, ved annen uberettiget fremgangsmåte. De objektive vilkårene i straffebudet er altså oppfylt ved gjennomførelse av skimming.

En slik sak er godt beskrevet i en dom fra Agder lagmannsrett, hvor gjerningspersonen ble domfelt for flere brudd på straffeloven § 1902, § 145, 2. ledd.[44] Med metoden som er beskrevet ovenfor, gjennomførte han skimming i tre forskjellige minibanker. I dommen ble det lagt til grunn at han hadde lagret informasjon om totalt 64 forskjellige bankkort.

Noe annet som er verdt å merke seg fra denne dommen, er at det ble uttrykkelig sagt at lovbruddet anses som fullbyrdet når all den skjulte informasjonen om bankkortet er avdekket. Altså når man har lest av både kortinformasjonen og pinkoden. Det vil si at med en gang informasjonen om bankkortet er registrert på den falske kortleseren, og pinkoden er blitt fanget opp av videokameraet, kan gjerningspersonen straffes etter straffeloven § 204. Dette betyr at gjerningspersonen ikke trenger å gjøre seg kjent med informasjonen om bankkortet, eller bruke denne informasjonen for å lage falske bankkort for å kunne straffes.

[44] LA-2011-49530

9. Oppsummering

Datakriminalitet er noe som medfører store økonomiske kostnader. I tillegg til dette er dette en form for kriminalitet som i mange tilfeller krenkende på andre måter, kanskje aller mest mot privatlivet. I denne oppgaven har jeg derfor sett på de objektive vilkårene for datainnbrudd, som er omhandlet i straffeloven § 204, og forsøkt å finne frem til hva som objektivt sett skal til for å straffes etter dette straffebudet. Straffebudet verner spesielt tre forskjellige hensyn: konfidensialitet, integritet og tilgjengelighet.

Forarbeidene til den nye straffeloven at det nye straffebudet viderefører det gamle. I denne oppgaven har jeg likevel vist noen forskjeller, som også har medført noen realitetsendringer, og hvordan straffebudet kan anvendes. Likevel er det nye straffebudet samlet sett svært likt det gamle, og rettspraksis tilknyttet det gamle straffebudet vil i mange tilfeller være veiledende for hvordan det nye straffebudet skal anvendes.

Måten datainnbruddet gjennomføres på, er stort sett uten betydning. Det sentrale for vurderingen om straffebudet er overtrådt, er ikke om datainnbruddet skjedde ved å bryte en beskyttelse, eller ved annen fremgangsmåte. Det mest sentrale i vurderingen, er om tilgangen til datasystemet er uberettiget. Dersom en person tar seg inn i datasystem han ikke har berettiget tilgang til, snakker vi med stor sannsynlighet om et datainnbrudd.

Hvis en gjerningsperson gjennomfører et datainnbrudd, må sannsynligvis flere straffebud anvendes i konkurrens. Straffeloven § 204 rammer kun handlingen hvor gjerningspersonen bryter seg inn i et datasystem. Handlinger som gjerningspersonen foretar seg etter at han har brutt seg inn i et datasystem, omfattes av andre straffebud. Det at datainnbrudd i seg selv er straffbart, gjør at det er en lav terskel for å kunne straffes. Så fort gjerningspersonen uberettiget har skaffet seg tilgang til et datasystem, har han overtrådt straffebudet. Det kreves ikke at han gjør seg kjent med innholdet på datasystemet. Dette er med på å styrke vernet de elektroniske innretningene som vi daglig bruker.

Straffebudet er svært omfattende, og oppgavens størrelse ga meg ikke mulighet til å gå inn på alle problemstillingene som er knyttet til dette temaet. Det er flere forhold som ikke er tatt med i denne oppgaven, som kan ha betydning i rettslig sammenheng. Likevel har jeg her gått gjennom det grunnleggende. I tillegg til dette, har jeg også gått inn på konkrete eksempler på

hva som kan straffes etter straffeloven § 204, som phishing og skimming. Det at det samme straffebudet dekker begge disse handlingene, som er svært forskjellige, viser at straffebudet har et bredt anvendelsesområde.

Litteraturliste

Bøker

Bøe H. O., Hornnes E. M., Mykland H. O., Nätt T. Heine (2012). *IT 1, Basisbok for informasjonsteknologi 1* (2. utg.). Halden: Gyldendal Akademisk og Halden Dataservice.

Sunde I. M. (2006). *Lov og rett i cyberspace: internettkriminalitet og etterforskningsmetoder.* Bergen: Vigmonstad & Bjørke AS.

Sunde I. M. (2016). *Datakriminalitet: En fremstilling av strafferettslige regler om datakriminalitet.* Bergen: Vigmonstad & Bjørke AS.

Lovverk

Straffeloven (1902). *Almindelig borgerlig straffelov av 22. mai 1902 nr. 10.*

Straffeloven (2005). *Lov om straff av 20. juni 2005 nr. 28.*

Forarbeider

Innst. O. nr. 53 (2004-2005). (2005). *Lovtiltak mot datakriminalitet.*

NOU 2007: 2 (2007). *Lovtiltak mot datakriminalitet.*

NOU 1985:31 (1985). *Datakriminalitet.*

Ot.prp.nr.22 (2008-2009). *Om lov om endringer i straffeloven 20. mai 2005 nr. 28 (siste delproposisjon - sluttføring av spesiell del og tilpasning av annen lovgivning).*

Rettsavgjørelser

Norges Høyesterett, Rt. 2012 s. 1669 (HR-2012-2056-A)

Norges Høyesterett, Rt. 2012 s. 1968 (HR-2012-2397-A)

Norges Høyesterett, Rt. 2004 s. 94 (HR-2004-127-A)

Agder lagmannsrett, LA-2011-49530.

Agder lagmannsrett, LA-2003-83.

Borgarting lagmannsrett, RG. 2011 s. 328 (LB-2010-181392)

Oslo tingrett, TOSLO-2010-62157.

Nettkilder

Center for Strategic and International Studies (2014). *Net losses: Estimating the Global Cost of Cybercrime. Economic impact of cybercrime II*. Hentet 16. juni 2016 fra http://www.cyberriskinsuranceforum.com/sites/default/files/pictures/rp-economic-impact-cybercrime2.pdf

Nasjonal Sikkerhetsmyndighet (2011). *Kvartalsrapport for 4. kvartal 2011*. Hentet 16. juni 2016 fra https://www.nsm.stat.no/globalassets/rapporter/norcert_q4_2011.pdf

Norsk rikskringkasting (NRK). *Norge utsatt for et omfattende hackerangrep*. Hentet 12. februar 2017 fra https://www.nrk.no/norge/norge-utsatt-for-et-omfattende-hackerangrep-1.13358988

Politiet (2015, 9. februar). *Kripos: Datakriminalitet.* Hentet 26. juni 2016 fra https://www.politi.no/kripos/datakriminalitet/