”Hacking” – forbrydelse eller digitalt selvforsvar?

Temanummer: Cybersikkerhed

Vi kender først og fremmest "hacking" som en forbrydelse. De større, opsigtsvækkende "hacking"-angreb hører vi om i nyhederne. Dog bliver "hacking"-metoden nu også italesat som en it-sikkerheds-kompetence. Således udbydes flere steder kurser i "hacking", og Forsvarets Efterretningstjeneste har oprettet et "Hackerakademi" for at rekruttere talenter til statens tjeneste. Begrebet "hacking" kan skabe forvirring, for alt er ikke tilladt for at optimere eller teste sikkerheden ved it-systemer. Denne artikel klarlægger, hvornår der straffes for "hacking" efter straffeloven. Desuden undersøges, om en it-sikkerhedsaktør må bruge "hacking" som et forsvar, når it-systemer bliver angrebet af en fjendtlig "hacker". I artiklen illustreres, at det kan være vanskeligt at forudsige, hvor grænserne for strafansvar går for den, der vil optimere sikkerheden ved sine systemer.

LENE WACHER LENTZ
adjunkt, ph.d.,
Juridisk Institut,
Aalborg Universitet,
lwle@law.aau.dk

JENS MYRUP PEDERSEN
lektor, ph.d.,
Institut for Elektroniske Systemer,
Aalborg Universitet,
jens@es.aau.dk

Gode og onde hackere

Vi tænker først og fremmest på ”hacking” af it-systemer som en forbrydelse, der håndteres af politi og retsvæsen, hvor angrebet klarlægges, og de skyldige strafforfølges. Imidlertid ses en stigende tendens til at italesætte ”hacking” som en it-sikkerhedskompetence, hvor forskellige ”hacking”-metoder anvendes for at teste sikkerheden ved it-systemer. Således udbydes flere steder kurser i ”hacking”. Desuden har Forsvarets Efterretningstjeneste oprettet et ”Hackerakademi”, under henvisning til, at en væsentlig del af opgaven med at beskytte Danmark og danske interesser ”… udføres af hackere, som er specialiseret i at indhente oplysninger ved at skabe adgang til lukkede netværk, it-systemer og computere” (Forsvarets Efterretningstjeneste, 2016).

Metoden ”hacking” af it-systemer indgår således i flere sammenhænge, og forståelsen af ”hacking” varierer betydeligt: I sociologiske kredse ses eksempler på en bredere forståelse af ”hacking”, der uafhængigt af tekniske og juridiske definitioner anskues som ”hacktivisme”, hvor en borger, der værner om sin digitale frihed, udfordrer forskellige online-overvågningsinstrumenter (Kaufmann, 2020; Hampson, 2012).

I den øgede fokus på it-sikkerhed, og generelt når vi agerer på online platforme og it-systemer, er det vigtigt at have en forståelse for, hvor grænserne går for det strafferetlige ”hacking”-ansvar. Alt må ikke gøres i den gode sags tjeneste – i optimering og test af it-sikkerhed – eller i egen oplevelse af berettigelse.

Vi vil med denne artikel klarlægge, hvad der forstås ved forbrydelsen ”hacking” af et it-system ud fra både et it-sikkerhedsperspektiv og et juridisk perspektiv.

I it-sikkerhedskredse navigeres ofte ud fra sondringen, "black-hat-hackere", som betegnelsen for de ondsindede "hackere", "white-hat-hackere", som de gode "hackere", og endelig "grey-hat-hackerne" som en gråzone derimellem. Straffelovens bestemmelse om "hacking" skal ideelt set balancere to grundlæggende hensyn over for hinanden: På den ene side står den systemejer, der investerer ressourcer i et it-system, og derfor må være den, der tillader og regulerer adgangen hertil. Heroverfor står hensynet til, at vi som brugere på internettet kan agere frit og anonymt for søge information på hjemmesider og platforme, og at det er muligt for os at påvise fejl og uhensigtsmæssigheder ved it-systemerne samt stille kritiske spørgsmål om det, man finder, uden at risikere strafansvar. Vi vil imidlertid se, at den danske straffelov er ganske klar: Man skal have lov af systemejeren for at få adgang til et it-system. Hvis man på eget initiativ og ud fra egne idealistiske eller godgørende formål tester sikkerheden ved andres systemer, risikerer man en straffesag.

» **den danske straffelov er ganske klar: Man skal have lov af systemejeren for at få adgang til et it-system. Hvis man på eget initiativ og ud fra egne idealistiske eller godgørende formål tester sikkerheden ved andres systemer, risikerer man en straffesag.**

Vi vil dernæst se på, om man må begå "hacking" som digitalt selvforsvar, hvis man selv bliver angrebet. Det følger af straffelovens bestemmelser om nødværge og nødret, at hvis man begår et strafbart forhold for at afværge et angreb eller for at redde ting i nødsituationer, kan man i visse tilfælde blive fri for straf. Der er tale om strafferetlige begreber, der er udviklet over mange år og i vidt omfang ud fra fysiske scenarier. Der ses ikke i den strafferetlige teori at være taget stilling til, hvordan man digitalt må forsvare sig selv ved angreb. Her møder de traditionelle strafferetlige begreber altså en ny teknologisk kontekst.

Vi vil illustrere "hacking"-metoden og det digitale selvforsvar ved en case om en "honeypot". En honeypot er et it-system, der er etableret med det formål at tiltrække angreb, eventuelt som afledning fra det egentlige it-system, hvor man har sine dyrebare data. Vi har valgt honeypotten som eksempel, fordi det efterhånden er et udbredt it-sikkerheds-setup, og fordi it-sikkerhedsaktøren både kan forberede honeypotten på angreb og ved monitorering af honeypotten tidsmæssigt ofte vil have mulighed for at reagere og forsvare sig, inden den fjendtlige "hacker" når til de rigtige data og systemer. Vi undersøger de retlige rammer for den situation, hvor en honeypot bliver udsat for et "hacking"-angreb, og it-sikkerhedsaktøren overvejer som selvforsvar at pacificere eller ødelægge den indtrængende software eller at iværksætte et "hacking"-angreb på den fjendtlige "hacker".

For overskuelighedens skyld bruger vi i det følgende betegnelsen "hackeren" om den fjendtlige angriber, der "hacker" et it-system, mens betegnelsen

"it-sikkerhedsaktøren" angår den aktør (en virksomhed, en ansat eller en privat borger), der måtte overveje at anvende "hacking" som digitalt selvforsvar.

Af pladsmæssige hensyn inddrages i det følgende alene straffelovens bestemmelse om "hacking", ikke det eventuelle strafansvar for uberettiget behandling af personoplysninger (GDPR).

"Hacking" som forbrydelse – de farvede hatte

Fra et it-sikkerhedsperspektiv indebærer selve metoden "hacking" blot, at man udfordrer sikkerheden ved et it-system. Det nærmere formål med "hackingen", og hvorvidt "hackingen" er lovlig, har i internationale it-sikkerhedskredse ført til den udbredte brug af sondringen "black-hat-hackere", "white-hat-hackere", og "grey-hat-hackere" (Malwarefox, 2019; Norton, 2020; Kaufmann, 2020; Kirsch, 2014). Ifølge den amerikanske softwarevirksomhed, Norton, er disse betegnelser inspireret af gamle westernfilm, hvor skurken bar sort cowboyhat og helten en hvid cowboyhat (Norton, 2020).

Den fjendtlige "hacker" kender vi: "Black-hat-hackeren", der angriber et it-system for at forvolde skade, hvorved man begår en forbrydelse og bliver strafansvarlig. Heroverfor står "white hat-hackeren", også kaldet "den etiske hacker", som betegner en person, der med et legitimt formål anvender offensive metoder til at teste sikkerheden i systemer, organisationer og virksomheder. Det centrale i forståelsen af "white-hat" er først og fremmest, at man tester systemet ud fra et klart defineret mandat fra systemejeren, som også har fastlagt, hvordan der nærmere skal afrapporteres om eventuelle sårbarheder i sikkerheden (Norton, 2020).

Imellem de to kategorier, "black-hat" og "white-hat", ses en større gråzone, hvor "grey-hat-hackeren" udfordrer sikkerheden ved it-systemer uden forudgående aftale med systemejeren. "Grey-hat-hackeren" kan agere ud fra meget forskellige motiver, eksempelvis nysgerrighed eller et ønske om at opnå anerkendelse. Der kan også være tale om et idealistisk sigte, f.eks. at man gerne vil medvirke til at opretholde en høj grad af beskyttelse ved it-systemer og personoplysninger. Der kan være stor forskel på, dels hvor langt man går for at påvise en sårbarhed, dels hvordan man kommunikerer om de sårbarheder, man finder: Om man foretager en loyal, detaljeret afrapportering til virksomheden, eller om man offentliggør sine fund gennem medierne med fuld eksponering af virksomheden (ENISA, 2016; Kirsch, 2014).

Disse farvede hatte bruges som et fingerpeg om det lovlige ved at bruge "hacking"-metoden til at udfordre sikkerheden ved et it-system. Der kan dog opstå en vis begrebsforvirring, eksempelvis hvis man – ud fra et i egen overbevisning berettiget formål – opfatter sig selv som en "white-hat-hacker", selv om man ikke har fået lov til at få adgang til systemet. Til illustration ses en omtale fra efteråret 2019 om, at en "white-hat-hacker" havde sikret 26 mio stjålne kreditkortoplysninger fra dark web ("www.pymnts.com"). Denne person, som næppe var tilladt adgang af systemejeren, må rettelig betegnes som

en "grey-hat-hacker". Uanset det anerkendelsesværdige formål det kan være at sikre stjålne kreditkortoplysninger, er en "grey-hat-hackers" adfærd problematisk. Som det vil fremgå af det følgende, vil en "grey-hat-hacker" kunne ifalde strafansvar for "hacking" efter den danske straffelov.

"Hacking" som forbrydelse efter straffeloven

Det følger af straffelovens § 263, stk. 1, at strafansvaret omfatter den, der "uberettiget skaffer sig adgang til en andens datasystem eller data, som er bestemt til at bruges i et datasystem". Ordet "datasystem" skal her forstås synonymt med it-system. Man kan straffes med fængsel indtil et år og seks måneder. Ved forskellige skærpende omstændigheder kan straffen stige til fængsel indtil seks år.

Populærbetegnelsen "hacking" antyder, at man skal forcere en sikkerhedsforanstaltning, men det er ikke et krav efter dansk ret (Lentz, 2018: 141 ff.). Adgangen skal blot være "uberettiget", hvilket helt enkelt kan bero på, at man ikke har fået lov til at få adgang af systemejeren. En "white-hat-hacker", der har samtykke og et klart mandat fra systemejeren til for eksempel en "penetration-test", hvor man simulerer et angreb med henblik på at kortlægge angrebsflader og sårbarheder, vil have en berettiget adgang og dermed ikke ifalde strafansvar for "hacking".

Man kan straffes for "hacking", hvis man har en berettiget adgang til en del af systemet, men går ud over denne adgang og tilgår andre dele, som man ikke er berettiget til at tilgå. Forbrydelsen er fuldbyrdet, når man har opnået adgang til systemet, det kræves ikke, at man har opnået kendskab til noget, ødelagt noget eller på anden vis rådet over data. Dette kan eventuelt straffes særskilt som hærværk mv.

For at straffe kræves, at den pågældende har "forsæt" til at skaffe sig uberettiget adgang, hvori ligger en vis grad af viden om eller hensigt til at begå forbrydelsen. I de tilfælde, hvor man ikke opnår adgang, vil der kunne straffes for forsøg. Dette skete i en sag, hvor den tiltalte havde forsøgt at opnå adgang til den forurettedes skattemappe ved at indtaste personens CPR-nummer, som tiltalte havde aflæst på forurettedes Facebook-profil (UfR, 2015: 345). Selv om tiltalte kunne argumentere med alene at have brugt oplysninger, der var fuldt tilgængelige for ham, og formålet alene var at se, om det kunne lade sig gøre at tilgå skattemappen og måske drille forurettede, stod det alligevel klart for ham, at han ikke var berettiget til at tilgå forurettedes skattemappe. Blot "at se om man kan" kan dermed let få én i strafferetlige problemer.

"Hacking" er underlagt "betinget offentligt påtale", hvilket betyder, at der kun bliver en straffesag, hvis forurettede anmelder forholdet til politiet eller i øvrigt tilkendegiver, at man ønsker forholdet strafforfulgt, jf. straffelovens § 275, stk. 2.

Som det ses, er "hacking"-bestemmelsen meget bred med formuleringen "uberettiget adgang", når der samtidig ikke er noget krav om, at en sikkerhedsforanstaltning skal være overvundet. Det kan være en fordel, fordi straffebestemmelsen hele tiden kan fortolkes i forhold til den teknologiske udvikling. Lovgiver skal ikke konstant omformulere teksten, efterhånden som nye "hacking"-metoder ser dagens lys. Omvendt betyder en sådan uklarhed, at det kan være svært for borgeren præcist at forudsige, hvad der er strafbart.

"Grey-hat-hackerens" test af it-systemer

"Hacking"-bestemmelsen handler om "uberettiget adgang", men hvornår kan man teknisk set siges at have opnået adgang? Ved systemer beskyttet af password vil dette være let at svare på: Når man har omgået password-beskyttelsen, eksempelvis ved at gætte password eller bruge andres password uden at have fået lov, eller man har måske fundet en bagdør til at få adgang til systemet udenom password-beskyttelsen. Ved andre it-systemer kan det være sværere at fastlægge, hvornår der er opnået "adgang". Problematikken er særlig relevant for de it-kyndige: Hvor meget må man undersøge sikkerheden på andres systemer, før man kan siges at have fået "uberettiget adgang" til datasystemet?

Spørgsmålet var relevant i en ankedom afsagt af Østre Landsret den 7. marts 2017, hvor en far havde opdaget en sikkerhedsbrist i et it-system, som blev brugt som kommunikationsplatform mellem forældre og børnehave. Sårbarheden bestod i, at det var muligt at skrive programkode i et beskedfelt, der ellers normalt er rensede for programkode. Ved at udnytte denne sårbarhed, lavede faren et popup-vindue, som fremkom hos brugerne med teksten: "Ring til [systemudbyderen] og sig, at jeres nye intranet-løsning er blevet hacket". Byretten dømte for "hacking" under henvisning til, at adgangen var uberettiget, idet adgangen gik ud over den adgang, som forældre, der benytter tjenesten, normalt har, hvilket tiltalte havde indset. Retten lagde navnlig vægt på, at tiltalte skrev beskeden i et beskedfelt på en måde, så den blev vist som et popup-vindue, dog fandt retten det ikke bevist, at tiltalte havde haft til hensigt, at popup-vinduet skulle vises hvert tiende sekund. Den omstændighed, at tiltaltes gerning kun var mulig på grund af en sikkerhedsbrist, kunne ikke føre til et andet resultat. Straffen blev fastsat til 10 dagbøder a 500 kr. under henvisning til den begrænsede skade, og til at tiltalte ikke derved fik adgang til personfølsomme oplysninger, samt at formålet med handlingen var at påpege et sikkerhedsproblem (Lentz, 2018: 149).

Landsrettens flertal frifandt for "hacking" og lagde vægt på, at et vidne fra Rigspolitiet havde udtalt, at den tiltalte ikke havde fået adgang til serveren "i den forstand, at han havde adgang til oplysninger eller ændrede noget på denne". På den baggrund blev det konkluderet, at tiltalte ikke havde "skaffet sig adgang til oplysninger fra [systemudbyderens] informationssystem eller adgang til programmer, han ikke var berettiget til at tilgå", eller at tiltalte i øvrigt havde "foretaget ændringer i de oplysninger og/eller programmer, han

var berettiget til at tilgå." Landsrettens mindretal på én voterende ville dømme for "hacking" (Lentz, 2018: 149).

Uanset at tiltalte ikke havde fået adgang til oplysninger om andre brugere, er det dog ganske klart, at han var gået ud over sin berettigede brugeradgang som forælder og var tilgået området for administrators tekniske opsætning af siden, når han tilmed var i stand til at "låse" brugerfladen af med et popup-vindue og hindre andre i at bruge systemet (Lentz, 2018: 149).

Dommen er desværre ikke trykt i de juridiske tidsskrifter, men sagen opnåede en del medieopmærksomhed (Version2, 2016). Umiddelbart kan frifindelsen måske opfattes som et carte blanche til, at man godt må undersøge og udfordre sikkerheden ved it-systemer ved at lave popup-vinduer. Nogen vil måske også kunne få tanken, at det er tilladt at udfordre sikkerheden, hvis man selv eller ens nærmeste pårørende har personfølsomme oplysninger liggende i systemet. Dette vil være en forkert udlægning af dommen. Som nævnt afhænger det strafferetlige ansvar af, om man har fået samtykke af systemejeren og dernæst af, om man er gået ud over samtykket til at tilgå en del af datasystemet, som man ikke har haft berettiget adgang til. Popup-vinduer må således vurderes helt konkret. Derudover har det ingen betydning, om ens egne data er lagret i it-systemet.

IT-Branchen udgav i 2018 på baggrund af denne og andre lignende sager en vejledning om, hvordan man skal forholde sig, hvis man opdager en sikkerhedsbrist med samtidig opfordring til virksomheder om ikke at anmelde dem, der indrapporter fejl og sårbarheder (IT-Branchen, 2018; Version2, 2018). En række virksomheder har tilsluttet sig dette samarbejde, "Kodeks for Indrapportering af Sikkerhedsbrister". Initiativet skal ses som en håndsrækning til de "grey-hat-hackere", der ikke har intention om at gøre skade, og som en erkendelse af, at hvis sikkerheden ved it og data generelt skal forbedres, så må man komme sådanne personer i møde.

Systemejeren har rådigheden over, om der bliver en straffesag mod "greyhat-hackeren". Straffelovens "hacking"-bestemmelse aktualiseres kun, hvis forurettede anmelder forholdet til politiet eller i øvrigt tilkendegiver, at man ønsker forholdet strafforfulgt. I en anerkendelse af "greyhat-hackerens" gode intentioner, kan systemejeren blot lade være med at indgive en anmeldelse om "hacking".

Hvis systemejeren anmelder forholdet, er straffeloven restriktiv: Det gælder helt grundlæggende inden for strafferetten, at det ikke fritager for straf, hvis man med en strafbar handling ønsker at sætte fokus på en problemstilling og skabe samfundsdebat. Således vil det heller ikke være en undskyldning for straf, hvis man skaffer sig uberettiget adgang til et it-system, fordi man er bekymret over it-sikkerheden og opbevaringen af ens egne eller nære pårørendes data. Dog kan et sådant formål i sammenhæng med en begrænset skade være en omstændighed, der konkret kan begrunde, at man idømmes en mildere straf (Lentz, 2018: 150).

» enten har man samtykke og dermed lovlig adgang til et system, eller også har man ikke, og adgangen vil være uberettiget og strafbar. Kun 'white-hat-hackeren' med det klare mandat fra systemejeren vil gå fri, 'grey-hat-hackeren', der på egen hånd 'hacker' systemer vil være strafansvarlig

Konklusionen er derfor, at hvis man opdager sårbarheder ved et it-system, må dette blot konstateres. Man skal tage kontakt til systemudbyderen for at informere om sårbarhederne og få det nødvendige samtykke, hvis man vil tilbyde at teste yderligere. I fortsættelse af diskussionen om "white-hat-hacking"-begrebet gælder der derfor ikke i strafferetlig henseende nogen farvet hat: enten har man samtykke og dermed lovlig adgang til et system, eller også har man ikke, og adgangen vil være uberettiget og strafbar. Kun "white-hat-hackeren" med det klare mandat fra systemejeren vil gå fri, "grey-hat-hackeren", der på egen hånd "hacker" systemer vil være strafansvarlig. Sådan må det nødvendigvis være. Alternativet er meget vanskeligt: Hvem skulle bestemme, hvad der er anerkendelsesværdigt formål, der berettiger til, at man uden tilladelse bryder sikkerheden ved andres it-systemer? Man kan tilmed spørge, hvorfor skulle borgeren have adgang til på egen hånd at "hacke" – og måske ødelægge – andres systemer for at "sætte fokus på sårbarheder", når der er offentlige myndigheder som Datatilsynet og politiet til at håndhæve sikkerheden ved it-systemer. Sat på spidsen ville alle "hackere" kunne undskylde sig i retten med, at de blot testede sikkerheden ved andres systemer.

Selv om en "grey-hat-hacker" måske tør gøre det, som politiet ikke har kompetencer eller ressourcer til, som f.eks. den person, der sikrede 26 mio. stjålne kreditkortoplysninger fra dark web, er der tale om en glidebane af selvtægt. Hvem er de gode? Den person, der tror, han gør noget godt ved at "hacke" en "hacker", har måske misforstået noget, så han "hacker" nogle helt andre. At der ikke ville blive noget strafferetligt efterspil mod den "grey-hat-hacker", der sikrede stjålne kortoplysninger fra dark web, beror i en dansk kontekst på, at et sådant forhold naturligvis ikke ville blive anmeldt til politiet af den systemejer på dark web, som opbevarede de stjålne kortoplysninger. Han har jo selv et forklaringsproblem og risikerer et strafansvar. Pragmatisk set bliver der således ikke danske straffesager mod de "grey-hat-hackere", der rammer plet mod kriminelle. Disse sager bliver ikke anmeldt. Men det er på eget ansvar og egen risiko at ramme plet.

"Hacking" som digitalt selvforsvar

I det følgende vil vi undersøge, om man for at beskytte sine systemer mod et "hacking"-angreb, selv må "hacke" tilbage for at forsvare sig. Ved vurderingen af denne form for digitalt selvforsvar må vi se på, hvad straffeloven egentlig forstår ved selvforsvar.

Hvis man begår et strafbart forhold for at forsvare sig, kan man blive straffri, hvis man opfylder betingelserne for "nødværge" i straffelovens § 13. Betingelserne er restriktive: Handlingen skal være nødvendig for at modstå eller afværge et påbegyndt eller overhængende uretmæssigt angreb. Desuden må handlingen ikke åbenbart gå ud over, hvad der under hensyn til angrebets farlighed, angriberens person og det angrebne godes betydning er forsvarligt.

Som det ses, skal angrebet være aktuelt, og man skal forsvare sig direkte over for angrebet. Hverken i tiden før et angreb bliver aktuelt, eller efterfølgende når angrebet er slut, er det tilladt at gøre noget strafbart for at forsvare sig. Man må gøre det "nødvendige" og "forsvarlige" for at forsvare sig, men hvad ligger der nærmere i det?

Nødværge er ofte relevant i forbindelse med fysiske angreb på personer, hvor det nødvendige og forsvarlige vil være at afværge et voldeligt angreb med samme form for vold, hvorimod det almindeligvis ikke vil være forsvarligt at afværge et knytnæveslag med et knivsstik. Nødværgebestemmelsen angår dog også afværgelse af angreb på ting mv. Skulle det ske, at selvforsvaret går ud over det tilladelige, er der alligevel en vis mulighed for at gå fri efter straffelovens § 13, hvis selvforsvaret "ikke åbenbart går ud over" det forsvarlige, hvor der altså gives et lille spillerum. I øvrigt er der mulighed for straffrihed, hvis selvforsvaret var "rimeligt begrundet i den skræk eller ophidselse", man har oplevet ved at blive angrebet, jf. § 13, stk. 2.

Nødværgebestemmelsen suppleres af straffelovens § 14, der angår "nødret": En handling straffes ikke, hvis den var nødvendig til at afværge truende skade på person eller gods, og lovovertrædelsen må anses for at være af forholdsvis underordnet betydning. Her er det altså tilladt at ofre et mindre gode for at redde personer eller ting fra skade, eksempelvis hvis man bruger andres ting til at slukke en ildebrand med.

For det digitale selvforsvar er det navnlig nødværge-bestemmelsen, der er relevant: Må man begå et strafbart forhold mod angriberen for at stoppe et digitalt angreb? Kernen i nødværge-bestemmelsen er, at man må afværge et aktuelt angreb med det nødvendige, forsvarlige middel. Det oplagte for it-sikkerhedsaktøren ville først være at overveje, om det er muligt midlertidigt at lukke ned for de systemer eller servere, der er angrebet. Ellers vil det måske være muligt at stoppe et igangværende "hacking"-angreb ved at pacificere de fjendtlige systemer. Er der tale om egentlig ødelæggelse af software eller hardware, vil dette som udgangspunkt være hærværk efter straffeloven. Dette kan dog være berettiget som nødværge for at afværge et "hacking"-angreb, uanset om det giver visse dønninger eller ulemper tilbage i det system, der bruges til at styre angrebet.

Til spørgsmålet om it-sikkerhedsaktøren må begå decideret "hacking" ved at skaffe sig adgang til et andet it-system for at forsvare sig mod et påbegyndt eller overhængende "hacking"-angreb, vil svaret formentlig være et nej.

Dette vil næppe være det nødvendige og forsvarlige at gøre for at afværge det "hacking"-angreb, man selv er udsat for.

Man kunne forestille sig, at it-sikkerhedsaktøren overvejer at forsvare sig med metoden, man kender fra DDoS-angreb, hvor man overbelaster angriberens server med forespørgsler, hvilket måske kan stoppe det fjendtlige "hacking"-angreb. Her får it-sikkerhedsaktøren ikke "adgang" til et andet it-system, men afbryder så at sige udefra aktiviteten fra det angribende system. Forsætligt at overbelaste andres servere og dermed hindre ejerens rådighed er som udgangspunkt strafbart efter straffelovens § 293, stk. 2, men det er ikke utænkeligt, at en sådan handling kan være straffri som nødværge for at afværge et "hacking"-angreb. Uanset berettigelsen som nødværge er der dog den usikkerhed ved metoden, at man ikke kan være sikker på at ramme den fjendtlige angriber, idet angrebet kan komme fra systemer og servere, der uforvarende er blevet involveret (se nedenfor om proxy-servere).

Grænsen for nødværge går ved det afsluttede angreb. Man kan dog diskutere, hvornår et angreb er helt afsluttet. Således er det den traditionelle antagelse ved tyveri, at det vil være lovlig nødværge at løbe efter tyven for at fratage ham den genstand, han netop har stjålet fra én (Toftegaard, 2019: 130; Langsted og Waaben, 2015: 140). Er der ikke tale om en sådan umiddelbar reaktion på tyveriet, er der ikke tale om nødværge. I stedet betragtes handlingen som selvtægt, der alene har et genoprettende sigte og således som udgangspunkt ikke fritager for strafansvar for den strafbare handling, man måtte udføre f.eks. for at skaffe sine ting tilbage. Begår man indbrud i tyvens hjem for at få sine ting tilbage, begår man en strafbar handling i form af husfredskrænkelse, der som udgangspunkt vil blive straffet, dog vil der måske i forhold til strafudmålingen være tale om formildende omstændigheder (Langsted og Waaben, 2015: 139).

Indenfor strafferetten har Waaben argumenteret for, at der kan være et område – om end begrænset – for lovlig selvtægt. Dette illustreres med, at hvis man har fået stjålet sin cykel, må man straffrit kunne tage cyklen tilbage, hvis man ser den parkeret på offentlig vej, idet man ikke ved denne handling vil krænke andres interesser (Langsted og Waaben, 2015: 140, se endvidere Langsted, 2020: 19). Ligeledes argumenteres for, at det vil være lovlig selvtægt at gå ind i tyvens forhave, hvor man kan se ens stjålne cykel stå, og formentlig vil man også kunne opnå straffrihed for at ødelægge en lås, som gerningsmanden efterfølgende har forsynet cyklen med (Langsted og Waaben, 2015: 140).

Disse cykel-eksempler fra den strafferetlige teori angår en genstand, som tyven har borttaget fra ejeren, og som nu er i tyvens besiddelse, og som ejeren nu med sikkerhed identificerer som sin egen. Eksemplerne er vanskelige at omsætte til en digital kontekst, hvor man udsættes for et "hacking"-angreb. Først og fremmest kan det diskuteres, hvor længe et "hacking"-angreb er i gang, og hvornår det egentlig kan siges at være afsluttet. Man kan godt forestille sig, at "hacking"-angrebet bliver en tilstand, hvor malware forbliver i systemet, og angrebet ikke endeligt er stoppet, og angriberen ikke endeligt er

lukket ude. Så længe der er et igangværende angreb, må der være adgang til forsvarlig og nødvendig nødværge. Når angrebet er afsluttet, kan man ikke begå en strafbar handling og opnå straffrihed som nødværge. Her er det også vanskeligt at omsætte cykel-eksemplet ovenfor til en digital kontekst, da det næppe giver mening at "løbe efter 'hackeren' for at få sine data tilbage". Her må man henvises til at indgive anmeldelse til politiet om dét, man har været udsat for og overlade håndhævelsen til myndighederne.

At begå præventiv nødværge

Det ligger i nødværgereguleringen, at man skal reagere på et "påbegyndt eller overhængende angreb" og i relation til den nødretlige straffrihed, at man skal afværge "truende skade på person eller gods" ved at ofre ting af mindre værdi for at redde et større gode. I begge situationer reagerer man på en pludseligt opstået situation. Det forudsættes her, at har man mere tid, eller kan angrebet eller faresituationen forudses, så er der ikke adgang til nødværge eller nødret, som fritager én for straf for det strafbare forhold, man har begået. Så må man i stedet for planlægge efter det, tage sine forholdsregler eller kontakte politiet, hvis man føler sig truet og frygter at blive angrebet, eller tilkalde beredskabsmyndighederne ved fare, brand etc.

Må man begå et strafbart forhold som præventiv nødværge, hvis et angreb fremstår sandsynligt for én, men angrebet ikke er påbegyndt eller overhængende? Som udgangspunkt vil svaret være nej, fordi det ikke opfylder betingelserne for nødværge efter straffelovens § 13. Denne problematik har navnlig været aktuel i sager om familiedrab, til eksempel, UfR 1993.193 V, hvor den tiltalte havde dræbt sin storebror med to skud, da han lå og sov på sofaen. Den dræbte havde terroriseret hjemmet og mishandlet familiemedlemmerne i årevis. I sådanne situationer får man ikke straffrihed som følge af nødværge, fordi der ikke er et påbegyndt eller overhængende angreb, som man forsvarer sig imod. Dog kan sådanne forhold indgå som formildende omstændigheder, når straffen skal fastsættes.

Hvordan forholder det sig med andre former for forberedelse af nødværge? Det er klart, at man må have en kniv liggende på sit natbord for at være forberedt på at forsvare sig, hvis der kommer en indbrudstyv, eller man bliver udsat for et overfald. Ved blot at lægge kniven frem har man ikke begået et strafbart forhold, og nødværge-bestemmelsen bliver ikke aktuel. Skulle der opstå en situation, hvor man faktisk bruger kniven til at forsvare sig med, skal det selvfølgelig vurderes, om denne handling er straffri som nødværge.

I den strafferetlige teori tales desuden om at etablere generelle afværgeforanstaltninger, f.eks. at anbringe en glubsk hund for at forhindre, at tyve trænger ind på en byggeplads om natten. Her er der ikke tale om, at man forsvarer sig mod et påbegyndt eller overhængende angreb, og situationen falder derfor uden for nødværge-bestemmelsen (Toftegaard, 2019: 130). I en sag fra 1973 havde ejeren forbundet sin bil, der var parkeret på gaden, med lysnettet for at forhindre tyveri af bilen. Installationen blev opdaget ved, at en forbipasseren-

des hund fik stød, da den lod sit vand op ad bilen. Retten vurderede, at installationen ikke var straffri som nødværge, og tiltalte blev dømt for overtrædelse af stærkstrømsreglementet (sagen er omtalt i Kommenteret straffelov, s. 188, med henvisning til TFDP 1973.401, hvor sagen er refereret).

Hvorvidt sådanne "faretilstande", man måtte etablere for at forsvare sig mod et eventuelle angreb, kan tillades, afhænger af en helt konkret vurdering, hvori indgår, om en lovregulering er overtrådt, og hvad der findes af advarsler til beskyttelse både af tilfældigt forbipasserende og af de ulovligt indtrængende, dette eksempelvis i relation til "glubske pladshunde" (Kommenteret straffelov, s. 188). Desuden må lovligheden bero på en almindelig forsvarlighedsvurdering (Baumbach, 2014: 435).

Som ovenfor nævnt vil det næppe være straffrit som nødværge, hvis it-sikkerhedsaktøren begår "hacking" af et andet it-system for at forsvare sig mod et aktuelt angreb. Skulle man vælge at sætte sine systemer op til et automatisk "hack-back", kommer nødværge slet ikke på tale, fordi der ikke er et aktuelt angreb, man forsvarer sig imod. En sådan automatisk opsætning skal vurderes som en generel afværgeforanstaltning, hvis tilladelighed skal vurderes helt konkret, se videre nedenfor i honeypot-eksemplet.

Skulle it-sikkerhedsaktøren alligevel vælge at lave et "hack-back" eller at sætte systemet op til at foretage en sådan handling, er det langt fra sikkert, der bliver et strafferetligt efterspil mod den pågældende. Hvis man har ramt plet mod den fjendtlige "hacker", vil denne næppe anmelde it-sikkerhedsaktøren til politiet. Men it-sikkerhedsaktøren bør være klar over, at denne fremgangsmåde er problematisk i forhold til straffeloven, og som nævnt ovenfor vil det også her være på eget ansvar og egen risiko at ramme plet.

Honeypot som digitalt selvforsvar

Vi vil illustrere "hacking" som digitalt selvforsvar ved en case om en "honeypot". En "honeypot" er betegnelsen for et it-system, der er etableret med det formål at blive angrebet. Typisk vil det være en selvstændig form for digital kopi eller "dobbeltgænger" af et kørende system eller service, som ligner det rigtige system udefra, hvorved it-sikkerhedsaktøren får mulighed for at se, hvilke angreb der foretages mod systemet. Man kan forestille sig en producent, der etablerer en honeypot af et af sine produkter for at kunne følge med i, hvordan produktet angribes, hvis det eksponeres direkte mod internettet. En anden variant er at bruge en honeypot som afledning. Man kan forestille sig, at en "hacker", der forsøger at angribe et universitet, i sin indledende søgen kommer til at betræde den etablerede honeypot, hvorved der genereres en alarm, fordi man ved, at der under normale omstændigheder ikke skal være aktivitet omkring honeypotten.

» En "honeypot" er betegnelsen for et it-system, der er etableret med det formål at blive angrebet

Strafferetligt er der intet til hinder for, at man etablerer en honeypot for på denne måde at optimere sin sikkerhedsindsats ved at sætte et falsk offer frem, som kan blive udsat for ondsindede angreb. Honeypotten skal her ses som en sikkerhedsforanstaltning, hvor man så at sige befinder sig på sin egen banehalvdel. Det aktualiserer ikke noget strafansvar for ejeren af honeypotten. Tværtimod vil man være berettiget til at anmelde de angreb, som honeypotten udsættes for, som "hacking" eller forsøg på "hacking". Hvis man konstaterer aktivitet på sin honeypot, som tolkes som et angreb, hvor "hackeren" forsøger at få uberettiget adgang til det it-system, hvor ens data er beskyttet, må it-sikkerhedsaktøren afværge angrebet. Det nødvendige og forsvarlige kan være at ødelægge den indtrængende software, selvom det kan give visse dønninger tilbage i hackerens system. Dog vil det umiddelbart ikke være tilladt som nødværge at lave et "hacking"-angreb på et andet it-system.

Spørgsmålet er, om en honeypot må programmeres til som en generel afværgeforanstaltning at pacificere eller ødelægge den indtrængende software. Også her er det vanskeligt at omsætte de strafferetlige eksempler til en digital kontekst. I det øjeblik installationen laves, overtræder man umiddelbart ikke nogen regulering, i modsætning til bilejeren, der havde overtrådt stærkstrømsreguleringen ved at sætte strøm til sin bil for at forhindre tyveri. Det er dog ligeså klart, at hvis man programmerer honeypotten til at ødelægge eventuel, senere indtrængende software, har man forberedt en automatisk hærværkshandling. Da der på tidspunktet for programmeringen ikke er et aktuelt angreb, er vi uden for nødværge-bestemmelsen. Hvorvidt en sådan automatisk hærværks-installation er tilladelig, vil afhænge af en konkret vurdering af, hvordan det er sikret, at den ikke rammer nogen, der uforvarende har bevæget sig ind på honeypotten, og hvorvidt installationen i det hele vurderes at være forsvarlig. Selvsagt er det, vi kender fra den fysiske verden, hvor man advares om en bidsk hund på den afspærrede byggeplads i aftentimerne, vanskeligt at overføre til den digitale kontekst. Det er domstolene, der i sidste ende vil vurdere tilladeligheden af sådanne generelle afværgeforanstaltninger, og spørgsmålet bliver først aktuelt, hvis nogen eller noget er blevet påvirket negativt af foranstaltningerne, og et eventuelt strafansvar skal afgøres.

Uanset hvordan it-sikkerhedsaktøren vælger at afværge et angreb, er det tilladt at indsamle oplysninger om den fjendtlige "hacker". Man kan måske forestille sig, at det med forskellige tracking-teknologier vil være muligt at skaffe sig oplysninger om "hackerens" IP-adresse (der identificerer en computers eller anden enheds globale adresse på internettet, og som tildeles af internetudbyderen), land, browserversion mv. Her får man ikke uberettiget adgang til noget it-system, men man sikrer sig vigtige identifikationsoplysninger, som vil kunne videreformidles til politiet i forbindelse med anmeldelse af det angreb, man har været udsat for.

Dog knytter der sig en stor usikkerhed til en sådan identifikation af den formodede angriber. Dette skyldes, at den globale IP-adresse, der identificeres, kan være delt mellem flere computere og brugere. Desuden kan angriberen

meget vel være gået gennem en eller flere proxy-maskiner i sit angreb og dermed have camoufleret sin egen IP-adresse. Sådanne proxy-maskiner kan være intetanende borgeres computere eller netværk med dårlig sikkerhed, som bliver brugt af kriminelle til "gennemgang" for at skjule, hvem der egentlig står bag forbrydelsen. Skulle en it-sikkerhedsaktør i en sådan situation ty til et "hack-back", vil den computer eller server, man umiddelbart kan se, at angrebet kommer fra, ikke være forbryderens computer. Derimod er ejeren i denne sammenhæng en intetanende borger eller virksomhed, der nu oplever et "hacking"-angreb med mulig ødelæggelse af udstyr, software og kompromittering af data til følge. Situationen illustrerer fint, hvorfor "hack-back" og anden digital selvtægt i egen oplevelse af berettigelse generelt ikke er nogen farbar vej.

Teknologi og strafferet

Vi har i denne artikel klarlagt, hvad der forstås ved "hacking" som forbrydelse efter straffeloven, hvor det afgørende er, om der er samtykke fra systemejeren til, at man får adgang. I forhold til den internationalt anvendte terminologi om de farvede hatte, vil ikke bare den ondsindede "black-hat-hacker" blive straffet efter straffeloven. "Grey-hat-hackeren", der i egen opfattelse af berettigelse tilgår it-systemer uden systemejerens samtykke, vil også få problemer med den danske straffelov.

Stadig har vi brug for som samfund at få alle gode kræfter i spil, når det gælder konstant fokus og optimering af it-sikkerhed til gavn for os alle. Det er et tiltrængt initiativ, at IT-Branchen har udarbejdet et kodeks for fair behandling af de "grey-hat-hackere", der loyalt indrapporterer sikkerhedsbrister ved it-systemer. Det er ikke hensigtsmæssigt, hvis strafferetten skal løse situationer med dårlig dialog mellem sådanne whistleblowere med gode intentioner og den systemejer, der nu får chancen for at rette op på sikkerheden ved sine systemer. I nogle tilfælde vil systemejeren derved undgå at få en bøde fra Datatilsynet for dårlig sikkerhed ved opbevaring af personoplysninger.

» Den traditionelle strafferetlige tankegang om nødværge, hvor man forsvarer sig mod angreb, er vanskelig at anvende i en digital sammenhæng. Eksemplet om at løbe efter tyven, der har stjålet ens cykel for at få cyklen tilbage, er meget vanskeligt at omsætte til en digital virkelighed

Den traditionelle strafferetlige tankegang om nødværge, hvor man forsvarer sig mod angreb, er vanskelig at anvende i en digital sammenhæng. Eksemplet om at løbe efter tyven, der har stjålet ens cykel for at få cyklen tilbage, er meget vanskeligt at omsætte til en digital virkelighed, hvor man gerne vil forsvare sine systemer mod angreb, måske undersøge et igangværende "hacking"-angreb og forsøge at opspore "hackeren" og klarlægge, hvad der er sket med ens data og forhindre fortsat uberettiget brug af data. Det man må gøre, hvis man

er udsat for et "hacking"-angreb, er som udgangspunkt kun det nødvendige og forsvarlige for at afværge dét angreb, men giver ikke adgang til hævn eller "hack-back" af gerningsmandens systemer. Når man i sit digitale selvforsvar selv bliver "hacker", kan man blive strafansvarlig.

Har man mulighed for at tilvejebringe identifikationsoplysninger om "hackeren", vil dette uden tvivl være værdifuld viden, som skal angives i anmeldelsen til politiet, eksempelvis om den IP-adresse, angrebet er sket fra, hidrører fra dansk territorium. Der er ingen tvivl om, at den første indledningsvise screening for politiets efterforskning vil være at klarlægge, om der er danske efterforskningsmuligheder, og om angrebet ser ud til at være begået af en gerningsmand i Danmark. Dansk politi har kun kompetence til at efterforske i Danmark, og efterforskning i udlandet, f.eks. ved at opspore, hvem der har anvendt en bestemt udenlandsk IP-adresse, kræver det andet lands retshjælp. Resultatet vil være en mere kompliceret og langvarig efterforskning på tværs af landegrænser, og dette vil formentlig kun iværksættes i sager af en vis grovhed, eksempelvis hvor der er sket en større økonomisk skade.

I den fortsatte optimering af it-sikkerhed ved danske it-systemer og udvikling af nye teknologiske værktøjer til digitalt selvforsvar, er det vigtigt konstant at være opmærksom på strafferettens grænser for, hvad man må foretage sig. Den strafferetlige lovgivning, man skal orientere sig i, bygger i vidt omfang på brede formuleringer, hvor tanken har været, at også nye teknologiske muligheder skulle rummes heri. Vi så det ved "hacking"-bestemmelsen, hvor den meget brede formulering "uberettiget adgang" til datasystemer dog kan give anledning til tvivl om, hvor meget man må undersøge andres systemer, og hvornår der teknisk set kan siges at være opnået adgang. Hvad angår det digitale selvforsvar, og hvad man må gøre, når man udsættes for et "hacking"-angreb, er det straffelovens nødværge-begreb, der er det centrale omdrejningspunkt. Igen er der tale om en meget bred bestemmelse. Her må man ty til fysiske eksempler om drab i familieforhold, cykeltyveri, biler tilsat strøm samt bidske hunde på byggepladser for at skitsere, hvordan nødværge-begrebet skal forstås i en ny digital kontekst. For lovgiver kan sådanne brede formuleringer være en fordel, for så kan man lade området udvikle sig i retspraksis, når domstolene tager stilling til konkrete sager med nye teknologiske metoder. Ulempen er for den enkelte borger, at det er svært at forudsige præcist, hvad man må foretage sig, og hvornår man kan rammes af et strafansvar. Der er ingen tvivl om, at it-sikkerhedsaktøren sættes på en vanskelig opgave.

Litteratur

Baumbach, Trine (2014), "Strafferet og menneskeret", København: Karnovgroup.

ENISA, European Union Agency for Cybersecurity (2016), "Good Practice Guide on Vulnerability Disclosure. From challenges to recommedations", www.enisa.europa.eu/publications/vulnerability-disclosure

Forsvarets Efterretningstjeneste (2016), "FE opretter hackerakademi", pressemeddelelse, 16. marts, https://fe-ddis.dk/Nyheder/nyhedsarkiv/2016/Pages/Hackerakademi.aspx

Hampson, Noah C. (2012), "Hacktivism: A New Breed of Protest in a Networked World", *Boston College International and Comparative Law Review*, 35(2): 511-42.

IT-Branchen (2018), "Kodeks for Indrapportering af Sikkerhedsbrister", https://itb.dk/raadgivning/kodeks-for-indrapportering-af-sikkerhedsbrister/laes-kodekset/

Kaufmann, M. (2020), "Hacking surveillance", *First Monday*, 25(5), https://doi.org/10.5210/fm.v25i5.10006

Kirsch, Cassandra (2014), "The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law", *Northern Kentucky Law Review*, 41(3): 383-403.

Langsted, Lars Bo (2020), "Ulovlig selvtægt. En analyse af straffelovens § 294", *Juristen*, 1, pp. 16-21.

Langsted, Lars Bo og Knud Waaben (2015), *Strafferettens almindelige del*, København: Karnovgroup.

Lentz, Lene Wacher (2018), "'Hacking' og det digitale privatliv", *Juristen*, 4, pp. 141-53.

Madsen, Lasse Lund, Thomas Elholm og Morten Niels Jakobsen (2019), *Kommenteret straffelov, almindelig del*, København: Jurist- og Økonomforbundets Forlag.

Malwarefox (2019), "10 Types of Hackers You Should Know", https://www.malwarefox.com/types-of-hackers/

Norton (2020), "What is the Difference Between Black, White and Grey Hat Hackers?", https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html

Symantec (2019), "Internet Security Threat Report", volume 24, www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

Tidsskrift for Dansk Politi (1973), s. 401, København: Dansk Politiforbund.

Toftegaard Nielsen, Gorm (2019), *Strafferet 1. Ansvaret*, på grundlag af Lasse Lund Madsen, København: Djøf Forlag.

Version 2 (2018), "Sikkerhedsbrister: Længe ventet vejledning til whistleblowing udgivet", 15. juni, www.version2.dk/artikel/sikkerhedsbrister-laenge-ventet-vejledning-whisteblowing-udgivet-1085420

Version2 (2016), "Dom faldet i kontroversiel hackersag", 15. april, www.version2.dk/artikel/dom-faldet-i-kontroversiel-boernehave-hackersag-709985

www.pymnts.com (2019), "White-Hat Hacker Swipes 26M Stolen Credit Cards From Dark Web", 15. oktober, www.pymnts.com/news/security-and-risk/2019/white-hat-hacker-swipes-stolen-credit-cards-from-dark-web/

Domme

UfR (Ugeskrift for Retsvæsen), 2017 p. 247 V.

UfR 2015, p. 345 Ø.

UfR 1998, p. 1769/2 Ø.

TfK (Tidsskrift for Kriminalret), 2008, p. 745/2 V.

Østre Landsrets utrykte ankedom af 7. marts 2017 (S-2696-16)

Love

Straffeloven (lovbekendtgørelse nr. 976 af 17. september 2019)

Stærkstrømsreguleringen, den nugældende elsikkerhedslov, lovbekendtgørelse nr. 26 af 10. januar 2019 med tilhørende bekendtgørelser.