Ulrich Emmert in: Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Eds.): Security, E-Learning, E-Services, 17. DFN-Arbeitstagung über Kommunikationsnetze, Düsseldorf, 2003. LNI 44 GI 2004, ISBN 3-88579-373-3

Reichen die deutschen Gesetze zur Bekämpfung der Cyberkriminalität?

Angesichts der Unterzeichnung des Cybercrime-Abkommens im November 2001 ist die Diskussion über die Erweiterung der Strafrechtstatbestände im Bereich der Internet-Kriminalität neu entflammt. Gerade im Bereich des Ausspähens von Daten und der Datenveränderung entstehen bisher Strafbarkeitslücken, die mit der fortschreitenden Entwicklung des Internets zu immer größeren wirtschaftlichen Schwierigkeiten führen können.

Für die rechtliche Erörterung der Grenzbereiche der bisherigen strafrechtlichen Regelung haben wir uns mehrere Bereiche und Konstellationen herausgesucht:

1) Strafbarkeit des Auslesens von freigegebenen Windows-Shares
2) Strafbarkeit des Auslesens von Domino-Logdateien
3) Strafbarkeit des WLAN-Hackings mit/ohne Publikum
4) Strafbarkeit der Überwindung von Sicherungen, die nicht zur Steigerung der Sicherheit eingebaut wurden (Switches)
5) Strafbarkeit von Angriffen aufWebshops
6) Strafbarkeit von indirekten Attacken und Notwehr bei Angriffen
7) Strafbarkeit des Besitzes von Hackertools

Die rechtlichen Aspekte der Gesetzgebung im Bereich Cyberkriminalität sollen nach Möglichkeit nicht isoliert, sondern im Zusammenhang mit einer praktischen Vorführung der Hackertechniken dargestellt werden, um die Probleme besonders anschaulich zu machen. Die rechtliche Erörterung soll zeigen, dass das deutsche Strafrecht im Bereich Cyberkriminalität auf der einen Seite noch Lücken aufweist, während auf der anderen Seite die Strafbarkeit über den Bereich hinausgeht, der eine Strafverfolgung rechtfertigt. Zum anderen soll der Vortrag zeigen, dass fehlende technische Sicherheitsvorkehrungen sogar dazu führen können, dass eine Rechtsverfolgung nicht einmal möglich ist und dadurch für jeden Nutzer die Einhaltung von technischen Mindeststandards zur Gewährleistung einer späteren Rechtsverfolgung dringend geboten ist.

1) Netbios-Scanning

Jeder Internet-User, der sich in das Internet einwählt und gleichzeitig Ressourcen wie Laufwerke, Verzeichnisse oder Drucker im lokalen Netz freigegeben hat, läuft Gefahr, dass diese Informationen auch im weltweiten Internet sichtbar sind. Ohne weitere Sicherungsmaßnahmen können durch die Verwendung von Portscannern und Freewaretools wie z.B. das Programm .Languard" aus dem Internet viele Informationen abgefragt und die freigegebenen Festplatteninhalte direkt ausgelesen werden. Aus rechtlicher Sicht ist dies nichts anderes als eine andere Form des Webbrowsers, der jedoch nicht auf freigegebene Webressourcen auf Port Nr. 80 lauscht, sondern die unter Port 139 freigegebenen Informationen von Windows-Rechnern zur Anzeige bringt. Es liegt auf Seiten des Anbieters keine besondere technische Sicherung vor, die zu einer Strafbarkeit nach § 202a StGB notwendig wäre, sofern kein Windows-Passwort bzgl. der Freigabe gesetzt wurde. Der Nutzer des Tools im Internet kann also fast beliebig fremde Rechner durchstöbern, ohne selbst rechtlich belangt werden zu können. Es fehlt bisher die Bestimmung, dass das Auslesen der Daten rechtswidrig wird, wenn der Nutzer erkennt, dass die Daten nicht für seine Nutzung bestimmt sind, wie dies sinngemäß bei der Datenveränderung geregelt ist. Grenzen ergeben sich nur aus den Vorschriften des § 17 Abs. 2 UWG beim Ausspähen von fremden Geschäftsgeheimnissen oder der §§ 43f. Bundesdatenschutzgesetz bei der Weiterverbreitung von personenbezogenen Daten. Fraglich ist bei der Grenzziehung durch diese Gesetze jedoch, inwieweit durch das freiwillige, ohne jede technische Hürde weltweit im Internet verbreitete Angebot der Daten noch eine Gesetzesverletzung durch weitere Verbreitung überhaupt möglich ist oder die Offenkundigkeit der Daten nicht jegliche Strafbarkeit in diesen Fällen ausschließt.
Anders sieht es natürlich rechtlich aus, wenn technische Hürden überwunden werden, also z.B. Windows-Passwörter geknackt werden. Einen tatsächlichen Schutz bieten z.B. Windows 95/98-Passwörter dennoch nicht, da diese innerhalb einer Sekunde geknackt werden können und Netbios-Angriffe in der Regel gar nicht bemerkt werden. Dann beginnt bereits die Strafbarkeit mit dem Herausfinden des Passwortes. Wenn jedoch keine fremden Informationen zum Knacken des Zielsystems notwendig sind (wie z.B. die Antwort des Systems auf Passwortrateattacken), dann bleibt selbst das Hacken von fremden Systemen in Deutschland straflos, wenn anschließend keine Daten ausgespäht werden. Der rechtliche Grund liegt darin, dass der "elektronische Hausfriedensbruch" nicht unter Strafe gestellt wurde, d.h. der reine Knackversuch ohne anschließende Mitnahme von Daten entsprechend dem Einbruchsdiebstahl im realen Leben.
Wenn man sich unter Verwendung von Languard unbedingt strafbar machen möchte, ist es natürlich auch möglich, beliebige Daten auf dem Zielsystem zu ändern oder auszudrucken und damit gegen § 303a StGB zu verstoßen. Übrigens ist es dabei umstritten, ob lediglich die Veränderung von bestehenden Daten unter Strafe

steht oder auch das Überschreiben von leeren Festplattenbereichen. So etwas wäre im wirklichen Leben als Gebrauchsdiebstahl in der Regel straflos.

Für das Opfer des Netbios-Scannings ergeben sich überraschenderweise noch viel häufiger und mehr Möglichkeiten als für den Täter, sich strafbar zu machen. Das beginnt bei Datenschutzverletzungen wegen des unbefugten Bereitstellens von personenbezogener Daten Dritter und geht über die Verbreitung von urheberrechtsgeschützter Software, Musik, Filmen oder sonstiger urheberrechtsgeschützter Daten wie auch z.B. werthaltige Datenbanken bis zur Verbreitung von jugendgefährdendem Material ohne Alterskontrolle im Internet.

2) Strafbarkeit des Auslesens von Domino-Logdateien

Eine Schwäche des Lotus-Domino-Webservers besteht darin, dass die Logdateien names.nsf, log.nsf, domlog.nsf und catalog.nsf standardmäßig nicht durch eine Passwortabfrage geschützt sind. Daher können in vielen Fällen durch einfachen Aufruf der entsprechenden URL im Webbrowser interne Datenbanken angezapft werden und Ereignisse wie das Verschicken von Mails etc. auf dem eigenen Rechner angezeigt werden. Die Eingabe der nicht verlinkten Namen der Logseiten des Dominoservers stellt aber zweifelsfrei keinen besonderen technischen Schutz dar, da die Daten mehr oder weniger frei auf der Datenautobahn herumliegen. Sonst könnte mit der gleichen Begründung das Probieren beliebiger Domains im Browserfenster ebenfalls schon unter Strafe gestellt werden. Auf die Absicht des Benutzers kommt es im Rahmen der Prüfung, ob hier objektiv ein technischer Schutz vorliegt, gerade nicht an. Damit bleibt diese Attacke nach § 202a StGB straflos. Daneben sind eben noch wie oben besprochen die Bestimmungen des Datenschutzrechts und des § 17 Abs. 2 UWG zu prüfen.

3) Strafbarkeit von Webshop-Hacking

Darf man das überhaupt? Macht sich jemand nicht schon strafbar, wenn er so etwas ohne Kenntnis der Webshopbetreiber ausprobiert oder gar auf dem BSI-Kongreß vorführt? Es wäre vermutlich ziemlich schlecht für einen Referenten, wenn er nach dem Kongreß hinter schwedischen Gardinen säße. Vergleichen wir die Vorgehensweise einmal mit dem Tante-Emma-Laden nebenan!
Der Onlineshop sieht zunächst so aus wie ein virtueller Supermarkt mit einem virtuellen Warenkorb, der vom Webshop aufgefüllt wird, wenn der Nutzer etwas per Mauseliek aus dem virtuellen Regal nimmt. Nun kommt der Hacker mit seiner virtuellen Etikettiermaschine und verändert den Preis auf dem Etikett, um nur einen geringeren Preis zahlen zu müssen. In einem richtigen Supermarkt wäre die Umetikettierung Urkundenfälschung, weil über den Urheber der Etikettierung getäuscht wird. An der Kasse würde dann versucht, die Kassiererin damit auch noch zu täuschen, womit auch noch ein Betrug auf das Konto des Ganoven geht. Ladendiebstahl wäre das dagegen nicht, da nichts an der Kasse vorbeigemogelt wird, sondern nur an der Kasse gemogelt wird.
Wie sieht das nun im Internet aus?
Doch zunächst der Reihe nach: Der Hacker fängt die auf seinem Rechner erstellte Anfrage an den Webserver ab und ändert diese vor der Übermittlung an den Webserver. Da die Daten freiwillig an ihn geschickt wurden und diese zudem nicht einmal technisch geschützt waren, liegt kein Ausspähen von Daten vor. Er hat auch keine unerlaubte Datenveränderung begangen, da er berechtigt ist, die Daten auf seinem Rechner zu ändern, der Webshopbetreiber erwartet ja gerade, dass der Kunde nach seinen Wünschen einkauft, er hat nur etwas unerwartet am Datensatz herumgeschraubt. Die oben festgestellte Urkundenfälschung hat aber auch ihre Entsprechung im Internet: Es liegt bereits eine Fälschung beweiserheblicher Daten vor, wenn jemand zur Täuschung im Rechtsverkehr Daten manipuliert, die als Beweis verwendet werden können. Auf die Berechtigung zum Datenändern kommt es hier gar nicht an. Hier liegt die Datenmanipulation der beweiserheblichen Daten bereits vor, wenn der Warenkorb mit dem Hacker-i.Sonderangebot" bestückt wird, weil der Preis der Ware im virtuellen Warenkorb als Beweis fiir die Höhe der Forderung gegenüber dem Onlinekunden geeignet ist.
Die Frage ist, ob der Hacker den Webshopbetreiber überhaupt täuschen will oder ob er ihm einfach nur ein Gegenangebot macht und handelt wie auf dem türkischen Bazar, um die Ware billiger zu bekommen. Man könnte sich ja vorstellen, der reduzierte Preis im Warenkorb sei ein preisreduziertes Angebot des Hackers, das der Webshopbetreiber mit seiner Auftragsbestätigung annimmt. Das kann natürlich nicht richtig sein, da der Webshopbetreiber den neuen Preis gar nicht zur Kenntnis genommen hat, sondern nur jemand sein Computerprogramm clever überlistet hat. Der Computer des Webshopbetreibers ist aber für beide Seiten erkennbar gar nicht befugt, über Preisänderungen zu entscheiden. (Selbst bei ebay darf der Computer nicht selbständig Preisverhandlungen führen, sondern nur Zuschläge nach Zeitablauf erteilen.) Daher ist fiir den Hacker klar, dass der Webshopcomputer hier getäuscht werden soll.
Der "Täter" hätte also schon an diesem Punkt ein massives Problem, wenn er wirklich billig einkaufen wollte. Da es ihm aber nur um das technische Problem geht und er keine Täuschungsabsicht hat (und die Ware auch gar

nicht haben will), macht er sich dennoch hier nicht strafbar, obwohl er die Tathandlung bezüglich der Datenfälschung bereits abgeschlossen hat.
Anschließend ginge ein Hacker mit dem gefälschten Warenkorb zur Kasse und legt die eigenmächtig preisreduzierte Ware auf den virtuellen Kassentisch.

Der Webshopbetreiber hat wie oben bereits festgestellt nicht bewusst dem neuen reduzierten Preis zugestimmt und ist schlicht und einfach übers Ohr gehauen worden. Der erste Gauner, dem es Anfang der achtziger Jahre gelungen ist, einen Computer erstmals per Vortäuschung falscher Daten zur Herausgabe eines geldwerten Vorteils zu bringen, ist noch straffrei ausgegangen, da damals nur das Betrügen von Menschen unter Strafe gestellt war. Damals hat jedoch der Gesetzgeber schnell reagiert und Computerbetrug neben einigen anderen Computerstraftaten ebenfalls mit Strafe bedroht.
Wenn der "Täter" nur die technische Möglichkeit zeigen und die Bestellung nicht abschicken möchte, macht er sich hier weder des Computerbetrugs noch des Computerbetrugsversuchs schuldig.

5) Strafbarkeit von WLAN-Hacking

Nach Strafgesetzbuch ist bei unverschlüsselten Daten Sniffen in Ordnung, wenn man eben verschiedene andere Vorschriften aus Datenschutz, UWG und TKG nicht verletzt. Nach der Meldung des Heise-Newstickers vom 14.5.2002 hält das Bundesjustizministerium WLAN-Hacking auch nur dann für strafbar, wenn die Daten verschlüsselt sind.
(http://www.heise.de/newsticker/data/ju-13.05.02-000D·

Nach einer Auslegung des § 86 TKG könnten aber öffentliche Vorfiihrungen oder absichtliche Eindringversuche unter Umständen Probleme bereiten:

Man darf bei unbeabsichtigtem Eindringen in fremde Netze dies nicht anderen mitteilen. Das unbeabsichtigte Abhören ist auch nach § 86 TKG kein Problem, nur wenn man absichtlich bestimmte WLANs ausspioniert, ist das verboten. Wenn man jetzt aber zufällig WLANs entdeckt und jemand dabei zuschaut, ist das meines Erachtens noch nicht strafbar, weil man ja zu dem Zeitpunkt noch nicht weiss, dass es sich hier um Daten handelt, die nicht für einen bestimmt sind. Es können ja auch freie WLAN-Hotspots auf Messen oder Flughäfen sein, deren Nutzung sonst verboten wäre. Nur eine anschließende Mitteilung der Inhalte oder wie man die Inhalte empfängt, würde meines Erachtens Probleme bereiten. Daher wäre die Nennung von Access Points für andere Hacker im Internet, per Zeitungsbericht oder per Kreide (sogenanntes War-Chalking) und eine entsprechende Anleitung auch ein Problem des § 86 TKG.

Weiter ist hier zu überlegen, ob Funkübertragung nach § 86 TKG vorliegt, die nicht für einen bestimmt ist oder ob bei der automatischen Zuteilung einer IP-Adresse durch den Access Point nicht ein Einverständnis des WLAN-Betreibers angenonunen werden muss. So lange nur ein Hexeode in einem Snifferprogramrn erkennbar ist, in dem kein Klartext zu sehen ist, ist auch die Frage, ob das schon Inhalte von Nachrichten sind, aber die Bekanntgabe der Tatsache des Empfangs entsprechend § 86 TKG kann auch in diesem Fall schon problematisch sein.

4) Sniffen am Switch

Streiten kann man sich trefflich darüber, ob eine besondere Sicherung nach § 202a StGB auch absichtlich zum Schutz der Daten installiert worden sein muß oder nur aus anderen Gründen eingeführt worden sein kann, wie z.B. im Falle eines Switches zur Verbesserung der Bandbreite gegenüber einem Hub. Meines Erachtens kommt es aber im objektiven Bereich der Strafbestimmung nur auf die tatsächliche Sicherung an, nicht auf den ursprünglichen Zweck, auch wenn das Wort "besonders" vielleicht eine Absicht zur Sicherung nahe legen könnte.

5) Ausspähen von Homebanking-Daten durch eine Man-in-the-middle-Attack

Das Ausspähen von per SSL verschlüsselten Homebanking-Daten gelingt natürlich nur, wenn die verschlüsselte Verbindung durch Täuschung des Computers des Nutzers über den Hacker umgeleitet wird. Zunächst wird dabei ggf. ein Switch wie oben beschrieben manipuliert, um die Anfragedaten auch an den Hacker weiterzuleiten (§ 202a StGB). Dann sendet er falsche DNS-Daten an den PC des Users und täuscht ihn damit über die richtige IP-Adresse (Computerbetrug 263a StGB). Der Hacker begeht daraufhin eine Fälschung der Zertifikatsdaten (§ 269 StGB), um den Computer bei der Eingabe von PIN und TAN beim Homebanking über die sichere Verbindung

zur Bank zu täuschen. Getäuscht wird hier nicht der PC, sondern der User selbst, weshalb hier kein Computerbetrug, sondern ein klassischer Betrug vorliegt. Anschließend begeht der Hacker dann noch einmal Computerbetrug, wenn er mit der erspähten PIN und T AN Geld vom Konto seines Opfers auf sein eigenes überweist. Ein so komplexer Angriff wie die Man-in-the-middle-Attack besteht also aus einer ganzen Reihe von Straftaten, die aber in der Praxis so lange schwer abzuwehren ist, so lange selbst Behörden wie das deutsche Patentamt standardmäßig gleiche Fehlermeldungen beim Aufruf von SSL-Verbindungen zeigen wie beim Angriff über diese Technik. Rechtlich haftet der Anbieter von Homebanking-Verfahren nach deutschem Auftragsrecht, so lange er den Nutzer nicht genauestens über die Schwächen des vom Anbieter ausgewählten Verfahrens und deren Erkennung und Verhinderung durch den Nutzer aufgeklärt wurde.

6) Haftung und Notwehr bei indirekten Hackerangriffen (z.B. DOS)

Haftung bei Hackerangriffen wird immer dann schwierig, wenn es sich um indirekte Angriffe handelt. Diese werden aber (zumindest bei destruktiven Denial-of-Service-Angriffen / § 303b StGB) den Regelfall darstellen, da Hacker (außer im Fall von UDP-Paketen) ihre IP-Adresse bei TCP-Paketen wegen des Routings der Rücksendung nicht beliebig verfälschen können. Daher werden Hacker (A) in den meisten Fällen indirekte Angriffe wählen, um die eigene Identität geheim zu halten. Dabei kann es für das erste Opfer (B) und gleichzeitigen Ausgangspunkt für den eigentlichen Angriff (auf C) zu sehr unangenehmen juristischen Folgen kommen.
Erstens haftet derjenige, der anderen Hackerangriffe von seinen Systemen aus ermöglicht, spätestens dann nach § 9 Teledienstegesetz, wenn er trotz Hinweises auf einen laufenden Angriff keine Gegenmaßnahmen ergreift. Noch komplizierter wird es, wenn sich der von dem gehackten Rechner Angegriffene im Rahmen seiner Notwehrrechte revanchiert und seinerseits den Rechner von B angreift, um den laufenden Angriff zu stoppen. Dabei werden meist Tools zum Abschießen des Rechners benutzt, was unter normalen Umständen regelmäßig nach § 303b als Datensabotage strafbar ist. Damit wird der schon gehackte Rechner von B nach § 228 BGB ggf. rechtmäßig ein zweites Mal angegriffen (oder sogar zerstört, wenn kein anderes Mittel verfügbar ist). Der dann Angegriffene B, der von dem ersten Angriff nichts mitbekommen hat, hält nun seinerseits ggf. eine Notwehraktion gegen C fiir gerechtfertigt und wehrt sich daher im festen Glauben rechtmäßigen Handeins gegen die Notwehraktion des C mit Fortsetzung siehe oben. Es kann also schnell zu einer Spirale der Gewalt fuhren, in der der zuerst angegriffene B oder auch C je nach den Umständen fiir den gesamten Schaden zur Verantwortung gezogen werden können, je nachdem, wer rechtmäßige Notwehr-lNotstandshandlungen durchgeführt hat.

7) Haftung für den Besitz von Tools zur Umgehung von Zugangskontrolldiensten zu gewerbsmäßigen Zwecken

Das Zugangskontrolldiensteschutzgesetz stellt bereits den Besitz von manchen Hacker- Tools, die zur Dekodierung von verschlüsselten Diensten geeignet sind, unter Strafe. Dabei ist die Formulierung des Gesetzes so unglücklich gewählt, dass nach dem Wortlaut des Gesetzes auch der Sicherheitsberater, der im Auftrag eines Kunden Sicherheitstests durchfuhrt, in die Gefahr der Strafbarkeit geraten kann. Die Vorverlagerung der Strafbarkeit bei Computerbetrug oder Leistungserschleichung durch unberechtigte Nutzung von bezahlten Diensten in Rundfunk oder Onlinemedien ist dringend geboten, da die eigentliche Nutzung meist zu Hause erfolgt und damit unter Beachtung von Art 13 GG (Unverletzlichkeit der Wohnung) nur sehr schwer verfolgbar ist. Daher muss bereits im Vorfeld eingegriffen werden und bereits die Verteilung entsprechender Werkzeuge beschränkt werden. Der negative Effekt besteht jedoch darin, dass einmal Security Consultants der eigene Besitz verboten wird, da sie dies zu gewerblichen Zwecken benötigen. Zum anderen besteht ein Problem darin, dass auch der Erwerb erschwert wird, da die meisten Tools der Berater direkt aus dem Internet heruntergeladen werden. Dieses Problem des doppelten Verwendungszwecks ist wie bei Waffen oder Drogen nur mit einer generellen Einschränkung des Verbots für bestimmte Gruppen oder mit einer Ausnahmegenehmigung im Einzelfall zu lösen. Im Endeffekt kann sonst das Gesetz das Gegenteil bewirken, nämlich dass die Waffengleichheit zwischen Hackern und Security Consultants zum Nachteil der letzteren gestört wird, weil sich die Hacker nicht an das Gesetz halten werden und dadurch deutlich im Vorteil sind.

Fazit:

Die derzeitige Gesetzeslage im Bereich der Cyberkriminalität hat verschiedene Problempunkte, die zum einen für einen zu geringen und zum anderen für einen zu großen Anwendungsbereich sorgen. Bei § 202a StGB ist eine Ausweitung der Strafbarkeit jedoch zwingend mit einer Stärkung der subjektiven Voraussetzungen verbunden, was in ermittlungstechnischer Hinsicht zu einer Erschwernis fuhrt und die Möglichkeiten für Ausreden und nicht beweisbaren Absichten vermehrt.
Beim Zugangskontrolldiensteschutzgesetz ist die Stärkung der subjektiven Elemente unvermeidbar, um einer unnötigen Kriminalisierung von Security Consultants vorzubeugen.

Dagegen ist beim Problem von unklaren Rechtfertigungslagen bei Hackerangriffen eine Lösung schwierig. Sie kann meines Erachtens nur darin liegen, die Verteidigung gegen Hackerangriffe zu verbessern und auf Gegenschläge ganz zu verzichten.