SK-Nr. 2007/187

Die 2. Strafkammer des Obergerichts des Kantons Bern,
unter Mitwirkung von Obergerichtssuppleant Bähler (Präsident i.V.), Oberrichter Righetti und Oberrichter Cavin sowie Kammerschreiberin Alemayehu

vom 13. November 2007

in der Strafsache gegen

G.

vertreten durch Fürsprecher A.

wegen unbefugter Datenbeschaffung

Regeste

Das Erfordernis des besonderen Schutzes als objektives Tatbestandselement der unbefugten Datenbeschaffung (Art. 143 StGB) ist bei Computern erfüllt, wenn diese über einen Schutz mittels eines gängigen, marktüblichen Produkts mit genereller Eignung zum Schutz der Daten verfügen. Es ist nicht erfordlich, dass spezifisch gegen die eingetretene Bedrohung (vorliegend ging es um sogenannte "Trojaner"-Computerviren) Sicherungsmassnahmen getroffen wurden.

Redaktionelle Vorbemerkungen

Auf Appellation des Angeschuldigten waren in oberer Instanz u.a. die erstinstanzlich ergangenen Schuldsprüche wegen unbefugter Datenbeschaffung zu überprüfen. Nachfolgend werden die dazu gemachten Erörterungen der Kammer wiedergegeben.

Auszug aus den Erwägungen:
(...)

III. SACHVERHALT UND BEWEISWÜRDIGUNG

1. (...) Der Angeschuldigte räumte ein, er habe im Internet nach einer Spyware gesucht und eine solche (...) gefunden. Den erworbenen so genannten „Trojaner" verschickte er unter fiktiven Namen (...) und mittels fingierten Emailadressen (...) als zip-Datei an die Geschädigten, welche vorgetäuschten Offertanfragen, Fragebogen und ähnlichem als Emailanhang beigefügt war. Das Trojaner-Programm installierte sich selbständig und für den Anwender unbemerkt auf dem Computer des Emailempfängers, sobald dieser den Anhang anklickte. War das Programm einmal installiert, konnte der Angeschuldigte sämtliche Tastaturbewegungen auf dem Computer über eine ihm zugängliche Webseite durch so genannte Keylogdateien nachvollziehen. Insgesamt hat sich der Angeschuldigte rund 27'000 solche Keylogdateien über die ihm zugängliche Webseite auf seinen Rechner übermittelt und bekam auf diese Weise unter anderem Einsicht in Dateieingaben, eingegebene Benutzernamen, Passworte, das Surfverhalten im World Wide Web und ähnlichem. Dies ermöglichte es ihm sodann, sich beispielsweise in ein Emailkonto einzuloggen, den gesamten Mailverkehr einzusehen und das Konto nach Belieben zu bearbeiten (z.B. Löschen oder Weiterleiten von Emails), so dass der rechtmässige Empfänger die Email nur in veränderter Form oder gar nicht mehr einsehen konnte. (...)

2. (...). Aus dem Einvernahmeprotokoll des vorerwähnten Fahnders R. geht hervor, dass es im Nachhinein nicht mehr möglich gewesen sei, die Computer der Geschädigten auf allfällige Schutzprogramme hin zu prüfen, da die meisten Geräte bereits neu installiert oder ersetzt worden seien, weshalb man sich darauf beschränkt habe, die Geschädigten nach den verwendeten Schutzprogrammen zu befragen. Eine Überprüfung, ob bei den Geschädigten eine Firewall installiert war, wurde nicht vorgenommen (p. 950). Gemäss den Aussagen der verschiedenen Geschädigten, an deren Glaubwürdigkeit für die Kammer keine Zweifel bestehen, ergibt sich Folgendes betreffend den installierten Schutzprogrammen auf den jeweiligen Computern gegen Zugriffe zur Zeit der vorgeworfenen Taten:

Name	Schutz
G.	McAffee bis Februar 2004, seither AVG (p. 226)
L.	Virenschutzprogramm Kaspersky (p. 954)
B.	erst Norton Antivirus, dann Antivirussystem G-Data (p. 242)
D.	AniVir, Spyboot (p. 261)
S.	Symantec Firewall, später auch Norton Antivirus (p. 265 ff.)
L.	Anti-Spy-Software, Virenscanner (p. 353)

(...) Aufgrund der dürftigen Abklärungen im Rahmen der Voruntersuchung und der Hauptverhandlung sowie der Tatsache, dass durch die monatelange Ermittlungsdauer gewisse technische Abklärungen nicht mehr möglich waren, ist es heute nicht möglich den direkten Beweis zu erbringen, dass die Computer der Geschädigten M., W., G. und B. gegen Zugriffe geschützt waren. Es entsprach jedoch bereits in den Jahren 2003 und 2004 dem technischen Standard, dass Computer bereits auf der Festplatte über vorinstallierte Programme verfügten oder Programme mit dem Computer mitgeliefert wurden, die den Anwender vor Zugriffen durch Viren, Würmer und ähnlichem schützen sollten. Zudem war zur Zeit der vorgeworfenen Tatbegehungen die Hacker- und Virenproblematik bekannt, genauso wie gängige Schutzmöglichkeiten. Heimanwender waren in der Regel damals schon nicht mehr völlig ungeschützt gegen Viren, Würmer und ähnliches, sondern verfügten über ein gängiges Schutzprogramm. Umso mehr kann dies bei Geschäftsleuten angenommen werden, die in einer Branche tätig waren, welche sich mit technischen Abläufen, Möglichkeiten und Neuerungen befasst, wie dies vorliegend bei den Geschädigten M., W., G. und B. der Fall ist. Es darf allerdings nicht angenommen werden, dass diese Schutzprogramme regelmässig aufdatiert wurden. Völlige Schutzlosigkeit geschäftlich genutzter Computer widerspricht jedoch der Lebenserfahrung.

Die Kammer gelangt demnach zur Überzeugung, dass keiner der Computer der Geschädigten völlig ungeschützt gegen Zugriffe war und geht davon aus, dass alle Computer über einen gängigen Zugriffsschutz, sei es durch eine entsprechende Software, sei es durch eine Firewall, verfügten.

In allen Fällen als gegeben erachtet die Kammer zudem den Passwortschutz der verschiedenen Emailaccounts, da dieser bei den verschiedenen Anbietern standardmässig vorgegeben ist. Um sich Zugang zu einem Emailkonto verschaffen zu können, wird und wurde schon zur Zeit der Tatbegehungen stets die Eingabe von Benutzername und Passwort vorausgesetzt.

IV. RECHTLICHES

1. Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, sich oder einem andern elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind, macht sich der unbefugten Datenbeschaffung im Sinne von Art. 143 StGB strafbar. Die Norm ergänzt die weitgehend auf den Schutz von Eigentumsrechten an Sachen beschränkten Straftatbestände wie unrechtmässige Aneignung oder Diebstahl (BBl 1991, Bd. II, S. 1009).

2. Folgende Elemente bilden den objektiven Tatbestand der Norm:
   - die Beschaffung fremder, elektronisch oder in vergleichbarer Weise gespeicherter Daten für sich oder einen Dritten;
   - die Daten dürfen nicht für den Täter bestimmt sein;
   - die Daten müssen gegen unbefugten Zugriff besonders geschützt sein.

   a. Der Angeschuldigte beschaffte sich die Daten der Geschädigten wie vorerwähnt durch die Installation eines trojanischen Pferdes, einer Art der Spyware, welches er den Geschädigten im Emailanhang getarnt als Fragekatalog oder ähnlichem zugestellt hatte und das sich selbständig und für den Geschädigten selber unbemerkt installierte. Damit hat er es sich ermöglicht, Daten der Geschädigten einsehen zu können. In allen überwiesenen Fällen betrifft dies Tastaturbefehle der Geschädigten, in den Fällen von M., W., B. und G. verschaffte er sich durch Auswerten der Keylogdaten ausserdem Zugang zu den Emailaccounts der Geschädigten und konnte so den Emailverkehr direkt einsehen. Dieses Vorgehen fällt unter das so genannte social engineering, welches ein „Überlisten" der berechtigten Person beinhaltet (http:// www.melani.admin.ch/themen/00103/00202/ index.html?lang=de). Dass die erlangten Daten somit nicht für den Angeschuldigten bestimmt waren und ein Beschaffen fremder Daten vorliegt, zeigt sich durch die Vorgehensweise deutlich. Der Angeschuldigte hat sich durch sein Vorgehen Verfügungsgewalt über Daten verschafft, die auf den Computern der Geschädigten gespeichert waren, womit auch das Tatbestandselement der Fremdheit offensichtlich erfüllt ist.

      Eingehend zu prüfen ist allerdings das objektive Tatbestandsmerkmal der besonderen Sicherung der Daten gegen unbefugten Zugriff.

   b. Der Gesetzgeber wollte den Anwendungsbereich des Art. 143 StGB beschränken, da ein Straftatbestand, der unterschiedslos alle fremden Daten unter Schutz stellte, den Strafrechtsschutz überdehnte. Wenn man bedenke, so die Botschaft des Bundesrates, dass beispielsweise in Schulen oft eine Grosszahl von Computeranschlüssen vorhanden sowie ohne Weiteres zugänglich seien und dadurch eine grosse Menge von Daten und Programmen verfügbar und benutzbar seien, werde deutlich, dass nicht jede an sich unkorrekte Datenbeschaffung a priori strafwürdig sei. Es könne nicht richtig sein, dass die beispielsweise in einem Büro ohne Weiteres von einer Datenverarbeitungsanlage abrufbaren Daten oder Programme, für die vielleicht gar kein Schutzbedürfnis bestehe, zur Anwendung von

Art. 143 StGB und zur Verhängung einer Sanktion wie bei Diebstahl führten. Vor allem wäre es stossend, gewisse Informationen nur deshalb strafrechtlich zu schützen, weil sie elektronisch oder in vergleichbarer Weise gespeichert seien, während die in Schriftstücken erfolgte Niederlegung gemäss Art. 179 Abs. 1 StGB nicht geschützt wäre, da die Verletzung des Schriftgeheimnisses für die Strafbarkeit voraussetze, dass der Täter die verschlossene Sendung öffne und Hausfriedensbruch verlange, dass in abgeschlossene Räume eingedrungen werde. Es sei also notwendig, dass der Zugang zu den betreffenden Daten durch Verschliessen des Computerraumes, Einschliessen der Datenträger, Verwendung von Passwörtern, Chiffrierung von übermittelten Daten oder ähnlichen Massnahmen gesperrt werde und der Täter diese für ihn erkennbare Schranke übersteigen müsse (BBl 1991, Bd. II, S. 1010 f.). Seit 1991 hat sich im technischen Bereich vieles verändert. Wann eine Sicherung heute besonders ist, darüber schweigt sich das Gesetz aus. In allgemeiner Form wird man verlangen müssen, dass die Sicherungsmassnahmen unter den Umständen des jeweiligen konkreten Falls üblicherweise ausreichen, um Unbefugte von den Daten fernzuhalten, was ihre generelle Abwehrtauglichkeit voraussetzt. Ob die Daten mit dem üblichen Sicherungsstandard bereits besonders geschützt sind, oder ob der im fraglichen Bereich übliche Sicherungsstandard übertroffen sein muss, ist ungeklärt, gemäss WEISSENBERGER jedoch abzulehnen. Von den Datenberechtigten dürften nur zumutbare, üblicherweise hinreichende Selbstschutzmassnahmen verlangt werden, nicht aber ein Spitzenaufwand. Die Anforderungen an die Zugriffssicherung seien den jeweiligen konkreten Umständen anzupassen. So seien beispielsweise Daten im Geschäftsleben aufwändiger zu sichern als diejenigen auf privaten Laptops. Das Sicherungserfordernis beziehe sich ausserdem auf die Datenverarbeitungseinrichtung selbst und nicht auf die einzelnen Daten (WEISSENBERGER, PHILIPPE, in: Niggli/Wiprächtiger, Basler Kommentar, Strafgesetzbuch II, Art. 111 - 401 StGB, Basel/Genf/München 2003, N 12 zu Art. 143 StGB, m.w.H.). SCHWARZENEGGER vertritt die Auffassung, dass die Anforderung an die besondere Sicherung gemäss Art. 143 StGB gleich auszulegen sei, wie in Deutschland das Erfordernis der besonderen Sicherung gegen unberechtigten Zugang gemäss §202a StGB (SCHWARZENEGGER, CHRISTIAN, Computercrimes in Cyberspace, in: Jusletter vom 14.10.2002, www.jusletter.ch, N 72). Eine besondere Sicherung im Sinne von §202a StGB ist dann gegeben, wenn Vorkehrungen getroffen sind, die objektiv geeignet und subjektiv nach dem Willen des Berechtigten dazu bestimmt sind, den Zugriff auf Daten auszuschliessen oder wenigstens nicht unerheblich zu erschweren. Dies braucht zwar nicht ihr einziger

Zweck zu sein, jedenfalls aber muss der Berechtigte durch die Sicherung gerade auch sein spezielles Interesse an der Geheimhaltung der Daten dokumentieren. Folglich muss eine Sicherung, um als solche gelten zu können, erstens eine objektive Hürde im Sinne einer erhöhten Anstrengung des die Sicherung Überwindenden darstellen, zweitens muss der Sichernde das Wissen und den Willen um das Erschweren des Zugangs zu den Daten aufweisen, d.h. einen Zweck zur Sicherung verfolgt haben (SCHMID, PIRMIN, Computerhacken und materielles Strafrecht - unter besonderer Berücksichtigung von §202a StGB, Diss. Konstanz, 2001, S.73). Der erforderliche Sicherungsgrad und damit die Eignung zur Dokumentation des Geheimhaltungswillens ist nach P. SCHMID dann erfüllt, wenn es für den Computerlaien nicht ohne weiteres möglich ist, die Sicherung zu überwinden (SCHMID, P., a.a.O., S.99).

Wie beim körperlichen Eindringen in ein Haus, bei dem die Tür offen, zu aber nicht verschlossen, verschlossen jedoch nur mit einem Standardschloss oder verschlossen mit einem Sicherheitsschloss sein kann, sind auch bei der Sicherung von Daten verschiedenste Schutzmassnahmen möglich. Das Tatbestandmerkmal der besonderen Sicherung vor Zugriff darf generell weder auf eine Weise ausgelegt werden, dass es immer erfüllt ist, noch derart, dass es kaum erfüllt sein kann. Allgemein sind keine allzu hohen Anforderungen an den Berechtigten zu stellen. Die Vorinstanz kam zum Schluss, dass der Ausschluss eines körperlichen Zugriffs auf den Rechner und der Umstand, dass für den Datenverkehr gegen aussen nur eine Telefonleitung zur Verfügung stand, als besonderer Schutz im Sinn des Gesetzes genügen müsse (p. 1030). Dem folgt die Kammer allerdings aus folgendem Grund nicht: Art. 143bis StGB setzt als Tathandlung gerade voraus, dass der Täter auf dem Wege von Datenübertragungseinrichtungen in eine fremde Datenverarbeitungsanlage eindringt. Dies ist dann der Fall, wenn der Täter über drahtverbundene Wege wie beispielsweise das Telefonnetz, elektrische Leitungen oder drahtlose Kanäle der Datenfernübermittlung, wie zum Beispiel UMTS, Zugangsschranken zur Datenverarbeitung wie Passwörter oder Verschlüsselungen aktiv ausschaltet bzw. überwindet (WEISSENBERGER, a.a.O., N 9 zu Art. 143bis StGB). Der Ausschluss eines körperlichen Zugriffs auf den Rechner und der Umstand, dass für den Datenverkehr gegen aussen nur eine Telefonleitung zur Verfügung stand, wäre somit keine besondere Sicherung im Sinne von Art. 143bis StGB. Diese Norm tritt jedoch als Auffangtatbestand zurück, wenn der Täter mit seinem Eindringen in fremde Datenverarbeitungssysteme ein über das blosse Eindringen hinausgehendes Ziel verfolgt und dadurch unter einen der übrigen Computer-Straftatbestände wie Art. 143 StGB fällt (SCHMID, NIKLAUS, Computer- sowie Check- und Kreditkarten-Kriminalität, Ein Kommentar zu

den neuen Straftatbeständen des schweizerischen Strafgesetzbuches, Zürich 1994, §5, N 34 f.). Die beiden Normen unterscheiden sich nebst dem subjektiven Aspekt der Bereicherungsabsicht lediglich darin, dass Art. 143^{bi}s StGB nicht erst wie Art. 143 StGB das Beschaffen von Daten, sondern analog zum Hausfriedensbruch als Vorbereitungshandlung dazu bereits das Eindringen erfasst. Eine besondere Sicherung wird jedoch bei beiden Straftatbeständen vorausgesetzt, weshalb die Kammer zum Schluss kommt, dass bei den Anforderungen an diese besondere Sicherung gleiche Massstäbe anzulegen sind und somit der Ausschluss eines körperlichen Zugriffs auf den Rechner und der Umstand, dass für den Datenverkehr gegen aussen nur eine Telefonleitung zur Verfügung stand weder im Sinne von Art. 143^{b1}s StGB noch demjenigen von Art. 143 StGB eine besondere Sicherung darzustellen vermag.

Im vorliegenden Fall geht die Kammer beweiswürdigend davon aus, dass die jeweiligen Computer aller Geschädigten über einen gängigen Schutz, sei es durch eine entsprechende Software, sei es durch eine Firewall, verfügten (vgl. Ziff.III.2). Zwar hat nur der Geschädigte L. ein spezielles Schutzprogramm zur Erkennung und Abwehr des Trojaners installiert gehabt - womit der Tatbestand der besonderen Sicherung bei ihm klarerweise bejaht wird - ein besonderer Schutz der Daten im Sinne von Art. 143 StGB kann bei den übrigen Geschädigten jedoch nicht per se verneint werden. Es ist nicht errorderlich, dass spezifisch gegen die eingetretene Bedrohung Sicherheitsmassnahmen getroffen wurden. Eine derartige Auslegung würde bei der Vielfalt und Raschheit der Veränderung von Bedrohungen im Computerbereich kaum einmal erfüllt werden, da die Verteidigungsmöglichkeiten immer hinter den Angriffsmöglichkeiten herhinken (vgl. Interview mit Natalya Kaspersky, SonntagsZeitung vom 11.11.2007, http://www.sonntagszeitung.ch/dyn/news/multimedia/ 811763.html). Der Zweck der Norm würde ausgehöhlt, wenn die besondere Sicherung nur in Fällen bejaht würde, in denen ein besonderes Schutzprogramm gegen den konkret erfolgten Angriff installiert wäre. Denn dieses Schutzprogramm würde aufgrund seiner Programmierung den Angriff erkennen und somit auch verhindern können, womit in Fällen, in denen die besondere Sicherung bejaht würde, stets nur ein Versuch vorläge, ausser das Schutzprogramm selbst würde durch den Angriff sogleich mitmanipuliert. Die Kammer kommt daher zum Schluss, dass ein gängiges, marktübliches Produkt mit genereller Eignung zum Schutz der Daten vor Zugriffen zur Erfüllung des objektiven Tatbestandselements des besonderen Schutzes genügt. Über die Installation eines eben solchen Produkts verfügten gemäss Beweisergebnis (Ziff. 111.2) alle Computer der Geschädigten. Die Tatsache, dass diese Programme gemäss Aussagen des

Fahnders R. den Trojaner nicht erkennen konnten (p. 948), ist der vorerwähnten Schnelllebigkeit der Angriffsprogramme zuzuordnen, nicht der generellen Schutzeignung vor Zugriffen und ist somit irrelevant.

Im Falle des Vorwurfs der unbefugten Datenbeschaffung betreffend die Emails, ist beweismässig erwiesen, dass alle Emailaccounts passwortgeschützt waren und somit den Anforderungen an den besonderen Schutz in diesen Fällen gemäss herrschender vorzitierter Lehre genüge getan wurde (vgl. Ziff. 11.2; WEISSENBERGER, SCHWARZENEGGER, SCHMID P., SCHMID N.).

3. In subjektiver Hinsicht verlangt Art. 143 StGB
   - Vorsatz und
   - Bereicherungsabsicht des Täters,

   ansonsten die Norm keine Anwendung findet. Das subjektive Tatbestandselement des Vorsatzes ergibt sich implizit, da gemäss Art. 12 Abs. 1 StGB nur strafbar ist, wer ein Verbrechen oder Vergehen vorsätzlich begeht, ausser das Gesetz bestimme es ausdrücklich anders, was bei Art. 143 StGB nicht der Fall ist.

   a. (...), womit erstellt ist, dass der Angeschuldigte diesbezüglich vorsätzlich vorging (p. 390 ff. u. p. 923).

   b. (...)

      Die Vorinstanz kam zum Schluss, dass der Einsatz des Trojaners nicht anders zu verstehen sein könne, als dass der Angeschuldigte habe in Erfahrung bringen wollen, was die Geschädigten auf ihren Rechnern machten. Diese Erfahrung wiederum könne nur im Zusammenhang mit der geschäftlichen Tätigkeit der Betroffenen stehen. Gerade bei der Einsichtnahme in den Emailverkehr der Konkurrenz habe der Angeschuldigte sich vertrauliche Informationen aneignen können, die im Geschäftsbereich von wesentlicher Bedeutung sein könnten. Informationen über Kundenbeziehungen und Vertragsverhandlungen seien von wesentlicher Bedeutung. Die vom Angeschuldigten verfolgte Absicht war nach Auffassung der Vorinstanz die Möglichkeit, die Daten nutzbringend im wirtschaftlichen Bereich, vor allem im Wettbewerb einzusetzen (vgl. SCHMID, N., a.a.O., §4, N 70). Es bedürfe keiner weiteren Begründung, dass das Wissen um das Marktverhalten von Konkurrenten und von bisherigen oder allenfalls neuen Kunden im Wirtschaftsleben einen eklatanten geldwerten Vorteil bringe. Dieses Wissen habe der Angeschuldigte sich aneignen wollen (p. 1032). Die Kammer kommt zum selben Schluss. Sämtliche Betroffenen waren aktuelle oder potenzielle Konkurrenten oder ehemalige, aktuelle oder potenzielle Kunden der D. AG und der Konkurrenz. Die

mittels der Spyware erschlossenen Informationen, insbesondere über Offerten und Vertragsverhandlungen, waren geeignet, der D. AG Wettbewerbsvorteile zu bringen, die sie auf legalem Weg nicht erhalten konnte und die sich in aller Regel in Geld ummünzen lassen. Selbst wenn es dem Angeschuldigten entsprechend seinen Aussagen primär darum gegangen wäre, ungerechtfertigte Nachteile der D. AG im Konkurrenzkampf zu beseitigen (wobei offen gelassen werden kann, wie er dies hätte bewerkstelligen wollen), verschaffte er sich Zugriffsmöglichkeiten auf alles, was auf den ausspionierten Computern geschrieben wurde sowie auf die Emailkonti der Betroffenen. Er konnte dadurch der D. AG letztlich finanzielle Vorteile verschaffen. Der Angeschuldigte selbst hätte zudem direkt von diesen finanziellen Vorteilen profitiert, schliesslich war er nicht irgendein Angestellter der D. AG, sondern einer von zwei Geschäftsleitern mit einer Aktienbeteiligung von 40%. Die Kammer geht daher von direkter Bereicherungsabsicht des Angeschuldigten aus, insbesondere da die Aussagen desselben betreffend unlauteres Verhalten der Betroffenen (allenfalls mit Ausnahme im Falle des Geschädigten W.) nicht verifiziert werden konnte.

4. Der Angeschuldigte hat sich somit - mit Ausnahme vom Fall L. - vorsätzlich und mit der Absicht sich unrechtmässig zu bereichern elektronisch gespeicherte Daten beschafft, die offensichtlich nicht für ihn bestimmt waren und die gegen seinen unbefugten Zugriff im Sinne des Gesetzes besonders gesichert waren. Sein Verhalten erfüllt damit sämtliche objektive wie auch subjektive Tatbestandsmerkmale der unbefugten Datenbeschaffung gemäss Art. 143 StGB.