EUROPEAN EXPERT GROUP FOR IT-SECURITY

eicar

DIE STRAFRECHTLICHE RELEVANZ VON IT-SICHERHEITSAUDITS

WEGE ZUR RECHTSSICHERHEIT BEI IT-SICHERHEITSÜBERPRÜFUNGEN VOR DEM HINTERGRUND DES NEUEN COMPUTERSTRAFRECHTS

von Christian Hawellek*
entstanden aus einer Projektarbeit gemeinsam mit Dennis Jlussi*
*candi. iur. an der Gottfried Wilhelm Leibniz Universität Hannover

Inhalt

Abstract

IT-Sicherheitsüberprüfungen sind unabdingbar zur Gewährleistung des Informationsschutzes und der Daten- und Netwerksicherheit. Die rechtlichen Rahmenbedingungen hingegen sind, gerade mit Blick auf das deutsche Computerstrafrecht – seit Sommer 2007 erheblich ausgeweitet –, keineswegs trivial. Während einzig rein passive Scans nach Sicherheitslücken keinen Straftatbestand verwirklichen, fällt üblicherweise jede Art der Ausnutzung dieser in den Anwendungsbereich des § 202a StGB (Ausspähen von Daten). Simulierte DOS-Attacken stellen eine Computersabotage im Sinne des § 303b StGB dar, Handlungen in Zusammenhang mit Überprüfungen der Leistungsfähigkeit von Antivirus- und Antispy-Programmen können in den Anwendungsbereich des § 303a StGB (Datenveränderung) fallen. Der Einsatz sog. „Sniffer" – unabdingbar zur Sicherstellung der Netzwerkfunktionalität – ist schließlich ein klassischer Fall des Abfangens von Daten (§ 202b StGB). Während letzteres Vorgehen aufgrund § 88 III 1 TKG gerechtfertigt ist, ist hinsichtlich jeder der vorgenannten Handlungen – abgesehen von den seltenen Fällen des Eingreifens eines Rechtfertigungsgrundes wie etwa Notstand – die Gestattung durch den jeweiligen Rechtsgutsträger zwingende Voraussetzung für die strafrechtliche Zulässigkeit. Im Falle von Unternehmen geschieht dies durch deren rechtliche Vertreter, wie etwa den Vorstand bei Aktiengesellschaften, wobei dieses Recht auch im Rahmen der Unternehmensorganisation an bestimmte einzelne Abteilungen delegiert werden kann. In den wenigen Konstellationen, da private Daten auf Unternehmenssytemen gespeichert sind und kein Rechtfertigungsgrund eingreift, ist die Zustimmung des jeweiligen betroffenen Arbeitnehmers obligatorisch, soweit nicht entsprechende Betriebsvereinbarungen existieren. Die Einverständniserklärung sollte die jeweiligen Überprüfungen und ihre Zielsetzung umfassen sowie die zu untersuchenden Systeme und jedwedes ggf. bestehende Risiko benennen.

IT security audits are essential to grant information protection as well as data and network security. However, the legal framework, especially regarding german computerrelated criminal law – considerably extended since summer 2007 –, is anything else than trivial. While mere passive scanning for vulnerabilities alone constitutes no offence, any kind of exploitation generally meets the scope of § 202a StGB (data espionage). Simulated DOS attacks represent a system interference in terms of § 303b StGB, actions related to antivirus and antispy software efficiency testing may fall within the scope of § 303a StGB (data interference). Finally the usage of any socalled „sniffer software" – indispensable in context of securing network functionality – would constitute a classical case of data interception (§ 202b StGB). While the latter is justified due to § 88 III 1 TKG, any of the former actions – apart from those rare cases when it would be justified as an act of necessity (such as §§ 228 BGB, 34 StGB) – will demand approval of the respective authorised person to remain legal. Authorised persons to legitimate security audits in case of companies are their legal representatives, such as the management board of a corporation, whereas this right can be delegated in terms of company organisation to single departments, too. In those few constellations, where private data on company systems is affected and the respective action is not justified, the approval of the particular employee is mandatory, if there is no corresponding employer/works council agreement. The declaration of approval should name the particular tests and their purpose, the systems to be audited and any existing risk in that context.

Einleitung

Die Sicherstellung der Integrität und Funktionalität der eigenen IT-Systeme ist für Unternehmen von grundlegender Bedeutung. Nicht nur birgt ein potentieller Ausfall informationeller Infrastrukturen erhebliche wirtschaftliche Risiken, auch ist ein Risikomanagementsystem zumindest für Aktiengesellschaften aufgrund des durch das KonTraG eingeführten § 91 II AktG rechtlich geboten. Gleich ob Dienstleistungen externer Anbieter in Anspruch genommen werden oder eigene CERTs und IT-Sicherheitsabteilungen bestehen: die Gewährleistung von Informationsschutz, Datensicherheit, Netzwerkfunktionalität und Applikationssicherheit hat hohe Priorität.

Gerade hinsichtlich gezielter Angriffe auf die entsprechenden Infrastrukturen können effektive Sicherheitsüberprüfungen aber oftmals nicht ohne entsprechende Simulationen durchgeführt werden. Dabei ist diesbezüglich allerdings die Rechtslage gerade im Hinblick auf das Computerstrafrecht alles andere als trivial. Zuletzt zeigte sich dies bei der Einführung des § 202c StGB durch das 41. Strafrechtsänderungsgesetz im Sommer 2007 in der Diskussion um die Frage, ob die Beschaffung sog. Hacker-Tools – für die IT-Sicherheitsbranche zur Durchführung realitätsnaher Audits unumgänglich – möglicherweise zur Kriminalisierung der beteiligten Fachkreise führe[1].

Tatsächlich bestehen aber weit über den Anwendungsbereich des § 202c StGB hinaus erhebliche, in der Praxis mitunter kaum wahrgenommene Strafbarkeitsrisiken. So werden bei umfänglichen IT-Sicherheitsüberprüfungen üblicherweise beinahe alle einschlägigen Straftatbestände des Computerstrafrechts berührt. Rechtliche Zulässigkeit setzt hier daher zwingend eine hinsichtlich Umfang und Legitimationskette einwandfreie vorherige Befugnis voraus, deren Anforderungen sich keineswegs allein aus dem Gesetz erschließen. Vielmehr bedarf es vertiefter strafrechtlicher Kenntnisse, um die rechtlichen Rahmenbedingungen für zulässige IT-Sicherheitsüberprüfungen präzise abzustecken. Insbesondere bei erlaubter Privatnutzung der IT-Systeme durch Arbeitnehmer gestaltet sich die Rechtslage dabei relativ komplex.

Dies sei zum Anlass genommen, die für IT-Sicherheitsüberprüfungen relevanten Straftatbestände kurz darzustellen und die gängigen Testhandlungen hinsichtlich ihrer strafrechtlichen Relevanz zu untersuchen. Abschließend soll aufgezeigt werden, wie in der Praxis Rechtssicherheit durch eine rechtlich einwandfreie Befugnis zu erlangen und wie diese zu gestalten ist.

[1] Vgl. für eine ausführliche Darstellung Jlussi, „IT-Sicherheit und § 202c StGB", EICAR Positionspapier, http://www.eicar.org/press/infomaterial/JLUSSI_LEITFADEN_web.pdf; Jlussi/Hawellek, „IT-Sicherheit im Lichte des Strafrechts".

B. Die einzelnen Straftatbestände

Das Computerstrafrecht wurde in Deutschland 1986 mit dem 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität[2] in das Strafgesetzbuch eingeführt und durch das 41. Strafrechtsänderungsgesetz[3] im Sommer 2007 modifiziert und ergänzt. Die im Rahmen von IT-Sicherheitsüberprüfungen relevanten Strafnormen finden sich dabei in zwei unterschiedlichen Abschnitten des StGB. In den 15. Abschnitt „Verletzung des persönlichen Lebens- und Geheimbereiches" wurden jene Straftatbestände eingefügt, die den unberechtigten Zugang zu Informationen unter Strafe stellen – § 202a StGB (Ausspähen von Daten), § 202b StGB (Abfangen von Daten) und § 202c StGB (Vorbereitung des Ausspähens und Abfangens von Daten). Die Strafbarkeit der Manipulation von Daten und EDV-Systemen wiederum ist im 27. Abschnitt „Sachbeschädigung" durch Einfügung der Straftatbestände der Datenveränderung (§ 303a StGB) und der Computersabotage (§ 303b StGB) geregelt worden.

I. § 202a StGB – Ausspähen von Daten

§ 202a StGB – Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

Strafbar nach § 202a StGB ist die Erlangung des Zugangs zu fremden Daten, wenn diese hiergegen besonders gesichert sind und diese Sicherung umgangen wird. Der Straftatbestand wurde 1986 geschaffen, um die seinerzeit bestehende Strafbarkeitslücke hinsichtlich des „Hackens" von Informationssystemen zu schließen. Die Tat ist Erfolgsdelikt, der reine Versuch bleibt straflos. Da Informationsschutz zu den wesentlichen Zielen von IT-Sicherheitsüberprüfungen zählt, wird diese Strafnorm hierbei mit Abstand am häufigsten tangiert. Neu ist seit Sommer 2007, dass die Daten nicht mehr tatsächlich abgerufen werden müssen, sondern dass die bloße Möglichkeit hierzu ausreicht, was den Bereich der Strafbarkeit erheblich ausgedehnt hat.

„Daten" sind im hier untersuchten Kontext alle elektronisch codierten Informationen in Informationssystemen,[4] ganz gleich wie marginal der Informationsgehalt auch sei – erfasst sind mithin beispielsweise auch Verzeichnisinhalte.[5] „Zugang" bedeutet dabei, dass zumindest die Möglichkeit des Abrufs besteht. Unerheblich ist, ob die Daten gespeichert sind oder sich gerade in der Übertragung befinden, so dass auch das Abfangen und Entschlüsseln von Nachrichten erfasst ist.[6]

Charakteristisches Merkmal des Straftatbestands ist die Überwindung einer Zugangssicherung, welche gerade den Berechtigten vor dem unberechtigten Abruf der Daten schützen soll und sein Geheimhaltungsinteresse dokumentiert.[7] Ohnehin allgemein zugängliche Daten – wie etwa Webseiteninhalte mit lediglich „geheimer" URL – können somit nicht tatbestandsverwirklichend ausgespäht werden. Zugangssicherungen sind dabei alle Arten von Zugriffssperren, beispielsweise Passwortsperren oder RFID-Zugangskarten, ebenso die

[2] 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität, BGBl. 1986 I S. 72.
[3] 41. Strafrechtsänderungsgesetz, BGBl. 2007 I S.1786.
[4] 2. WiKG-E, BT-Drucks. 10/5058, S. 29; MünchKomm-Graf, § 202a Rn. 7f.; Sch/Sch-Lenckner, § 202a Rn. 3.
[5] MüchKomm-Graf, § 202a Rn. 8ff.
[6] 2. WiKG-E, BT-Drucks. 10/5058, S. 29; MünchKomm-Graf, § 202a Rn. 10.
[7] 2. WiKG-E, BT-Drucks. 10/5058, S. 29; MünchKomm-Graf, § 202a Rn. 28; Sch/Sch-Lenckner, § 202a Rn. 7.

B. Die einzelnen Straftatbestände

Verschlüsselung ansonsten frei abrufbarer Daten. Wird also eine nicht gegen Download geschützte, jedoch verschlüsselte Datei von einem Server geladen und sodann die Verschlüsselung umgegangen oder sonst aufgehoben, ist auch dies tatbestandlich erfasst.[8]

Für die Zulässigkeit von IT-Sicherheitsüberprüfungen von besonderer Bedeutung ist die Frage der Bestimmung der Daten. Erfolgt der Zugriff mit Einverständnis des Verfügungsberechtigten, so sind die Daten nicht mehr „nicht für den Täter bestimmt"[9], so dass der Tatbestand und damit die Strafbarkeit entfällt. Daher ist eine IT-Sicherheitsüberprüfung im Auftrag des Verfügungsberechtigten, trotz Anwendung der ansonsten strafbaren Methoden, zulässig.

II. § 202a StGB – Abfangen von Daten

§ 202b – Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

Mit der Schaffung des § 202b StGB im Rahmen des 41. Strafrechtsänderungsgesetzes ist im Sommer 2007 die Strafbarkeitslücke hinsichtlich des Abfangens unverschlüsselter Daten, das nicht von § 202a StGB erfasst ist, geschlossen worden. Der Schutzbereich unterscheidet sich von demjenigen des § 202a StGB mithin dahingehend, dass es hier gerade nicht auf das Vorhandensein einer besonderen Zugangssicherung ankommt, also das Recht auf „Nicht-Öffentlichkeit der Kommunikation"[10] im Allgemeinen geschützt wird. Im Bereich der IT-Sicherheit spielt die Norm primär beim Einsatz sog. „Sniffer"-Software eine Rolle, wie sie zur Wartung und Fehlersuche in IP-Netzen eingesetzt wird.

III. § 303a StGB – Datenveränderung

§ 303a – Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

[8] Sch/Sch-Lenckner, § 202a Rn. 8.
[9] 41. StrÄndG-E, BT-Drucks. 16/3656, S. 9.
[10] 41. StrÄndG-E, BT-Drucks. 16/3656, S. 11.

B. Die einzelnen Straftatbestände

Der Straftatbestand der „Datenveränderung" (§ 303a StGB) schützt das Recht auf unversehrte Verwendbarkeit der in den Daten gespeicherten Information gegen jedwede Form der Veränderung, einschließlich des Entzuges der Daten oder der Vernichtung des Informationsgehaltes.[11] Anders als bei § 202a StGB kommt es hier ebenfalls nicht auf einen besonderen Schutz gegen unberechtigte Veränderung an. Hinsichtlich von IT-Sicherheitsüberprüfungen spielt die Norm meist dann eine Rolle, wenn Viren oder Trojaner zum Test der Leistungsfähigkeit entsprechender Abwehrsoftware eingesetzt werden und dadurch Daten wie etwa Registry-Einträge verändert werden. Bedeutung hat sie weiterhin dann, wenn unsichere Passwörter geändert und dadurch Daten gesperrt werden. Auch hinsichtlich § 303a StGB führt die Zustimmung des an den Daten Verfügungsberechtigten zur Straffreiheit, da mit der rechtfertigenden Einwilligung die Rechtswidrigkeit entfällt.

IV. § 303b StGB – Computersabotage

§ 303b – Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht,

2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder

[...]

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

[...]

Schutzgut des § 303b StGB ist das Interesse des Inhabers am störungsfreien Ablauf der Datenverarbeitung auf seinen Informationssystemen,[12] die entsprechende Störung muss eine Erheblichkeit aufweisen, die eine mit geringem (finanziellen, zeitlichen etc.) Aufwand behebbare Beeinträchtigung übersteigt – eine reine Gefährdung reicht hierfür nicht aus.[13] Der Straftatbestand der Computersabotage hat durch das 41. Strafrechtsänderungsgesetz insofern eine Ergänzung erfahren, als dass nunmehr – unter Nr. 2 etwas kryptisch formuliert – auch DOS-Attacken explizit unter Strafe gestellt werden.[14]

Im Rahmen von IT-Sicherheitsüberprüfungen spielt die Norm eher eine untergeordnete Rolle, da im Allgemeinen derart aggressive Tests nicht durchgeführt werden. Sofern dies dennoch der Fall sein sollte, sind üblicherweise die ersten beiden gesetzlich normierten Fälle einschlägig. Dies ist zum einen eine Datenveränderung nach § 303a StGB, wenn sie entsprechend schwerwiegende Konsequenzen aufweist (etwa das Überscheiben eines Bootsektors durch einen Testvirus), zum anderen stellen DOS-Attacken, sofern sie eine erhebliche Störung verursachen, eine nach § 303b StGB strafbare Handlung dar. In beiden Fällen schließt auch hier die Einwilligung desjenigen, in dessen Vermögen das Informationssystem

[11] Sch/Sch-Stree, § 303a Rn. 1.
[12] Sch/Sch-Stree, § 303b Rn. 1.
[13] Beschlussempfehlung des Rechtsausschusses zum 2. WiKG-E, BT-Drucks. 10/5058, S. 35.
[14] Dies ergibt sich aus der Begründung, 41. StrafÄndG-E, BT-Drucks 16/3656, S. 13.

B. Die einzelnen Straftatbestände

steht, die Strafbarkeit auf Rechtfertigungsebene aus, wobei die Befugnis hierzu allerdings aufgrund des hohen Risikos nach ausreichender vorheriger Aufklärung über mögliche Konsequenzen erteilt werden muss. Soweit lediglich extra zu diesem Zweck eingerichtete separate Testsysteme entsprechenden Überprüfungen unterzogen werden, ist allerdings in der Regel bereits der Tatbestand des § 303b StGB mangels „wesentlicher Bedeutung" der dort laufenden Datenverarbeitung nicht erfüllt, so dass bereits deshalb die Strafbarkeit entfällt.

C. IT-Sicherheitsüberprüfungen in der Praxis und ihre strafrechtliche Relevanz

I. Informationsbeschaffung über „Hacker-Foren" und ähnliche Quellen

Die Informationsbeschaffung über Schwachstellen in Software und deren Ausnutzung steht im Vorfeld von IT-Sicherheitsüberprüfungen und gehört zu den täglichen Aufgaben eines CERT, um mit kürzest möglichen Reaktionszeiten neuen Gefahrenpotentialen begegnen zu können. Die Suche nach derartigen Informationen erfüllt dabei, gleich welche Quelle herangezogen wird, keinen Straftatbestand. Strafbarkeit setzt stets erst mit der (unbefugten) tatsächlichen Ausnutzung von Schwachstellen ein.

II. „Honeypots" als Angriffsziele

Größere Unternehmen verfügen oft über eigene IT-Sicherheitsabteilungen, die für den Schutz der IT-Infrastruktur zuständig sind. Da hier die IT-Sicherheit in einem bekannten und weitestgehend statischen technischen Umfeld sichergestellt werden soll, bietet es sich an, sog. „Honeypots" aufzustellen, also Informationssysteme, die einzig dem Zweck dienen, Angriffziel zu sein. Mit dieser Methode lassen sich reale Angriffe „einfangen" und hinsichtlich Vorgehensweise und Person des Angreifers analysieren. Das Aufstellen solcher Systeme erfüllt keinen Straftatbestand und stellt im Übrigen auch keine Anstiftung zu einer Straftat dar.

C. IT-Sicherheitsüberprüfungen in der Praxis und ihre strafrechtliche Relevanz

III. Einsatz von Scannersoftware zur Schwachstellenanalyse

Zu Beginn der meisten IT-Sicherheitsüberprüfungen steht der Einsatz von Scannersoftware zur Schwachstellenanalyse wie etwa AppScan, GFI Languard oder Nessus. Hierbei werden Daten an das gescannte System gesendet, um derart offene Ports und sonstige Schwachstellen zu erkennen und aus der Reaktion des Systems (der „Signatur") Rückschlüsse auf dort im Einsatz befindliche Software zu ziehen. Die Durchführung dieser passiven Scans führt zwar zu einer Übermittlung von Daten aus dem gescannten System, hierbei handelt es sich aber ausschließlich um Informationen, die logisch vor einer ggf. vorhandenen Zugangssicherung liegen und daher selbst nicht gegen Zugang gesichert sind. § 202a StGB ist demnach auf rein passive Scans nicht anwendbar. In den seltenen Fällen, in denen der Scan wider Erwarten zu einem Systemabsturz des gescannten Systems führen sollte, wurde ein solcher jedenfalls nicht vorsätzlich herbeigeführt, so dass auch eine eventuelle Strafbarkeit nach § 303b I Nr. 2 ausscheidet. Passive Scans sind somit strafrechtlich zulässig.

IV. Die Ausnutzung von Schwachstellen

Teils bietet Scannersoftware – so etwa AppScan – die Möglichkeit, gefundene Schwachstellen im Anschluss an den Scanvorgang auszunutzen, um so die Verwundbarkeit des überprüften Systems weiter zu erforschen. Dies kann gleichermaßen unter Verwendung eigener oder fremder Exploits geschehen. Grundsätzlich wird hierbei der Anwendungsbereich des § 202a StGB berührt, allerdings sind die Fälle des Ausnutzens von Sicherheitslücken oder der vom Software-Ersteller bewusst eingebauten Trap-Doors rechtlich umstritten. Ein solches Vorgehen könnte man als Zugang ohne Überwindung einer Zugangssicherung betrachten, weil eine solche hinsichtlich der Lücke ja gerade nicht vorliegt. Da allerdings auf das Informationssystem als Ganzes abzustellen ist, stellt sich die Ausnutzung versteckter Lücken gerade als Überwindung der für den regulären Zugang vorhandenen Sicherungen dar.[15] 202a StGB bleibt also anwendbar.

Soweit lediglich Testsysteme angegriffen werden, entfällt die Strafbarkeit regelmäßig, da Angreifer und Rechtsgutsträger identisch sind bzw. sich aus der Bereitstellung des Testsystems zu diesem Zweck bereits das Einverständnis des Berechtigten ergibt. Werden Produktivsysteme wie etwa Webserver angegriffen, so entfällt die Strafbarkeit nur, wenn das Vorgehen vom Einverständnis des Rechtsgutsträgers gedeckt ist. Gleiches gilt, wenn der Zugang zu einem geschützten Netzwerk oder Endgerät durch IP-Spoofing oder die Übernahme einer Session[16] oder aber – wenn auch nur beschränkt – durch SQL-Injections oder Cross-Site-Scripting erlangt wird.

VI. Passwortcracks und Einsatz von Trojanersoftware

Die erfolgreiche Überwindung von Passwortsperren fällt klassisch in den Anwendungsbereich des § 202a

[15] MünchKomm-Graf, § 202a Rn. 66.
[16] MünchKomm-Graf, § 202a Rn. 72.

C. IT-Sicherheitsüberprüfungen in der Praxis und ihre strafrechtliche Relevanz

StGB, wenn dadurch ein Zugriff auf geschützte Daten und Systeme ermöglicht wird. Dabei ist es unerheblich, ob das Passwort durch manuelles Ausprobieren, eine Brut-Force- oder eine Wörterbuch-Attacke erlangt wird. Erfordert das Cracken des Passwortes zudem Daten aus dem System, beispielsweise Hash-Werte, die zunächst verschafft werden müssen, um sodann mittels Rainbow-Tables auf den Plaintext zurück gerechnet zu werden, so ist bereits das Auslesen des Hashwertes strafbar, sofern schon dieser ebenfalls gegen Zugang gesichert ist. Ist dies nicht der Fall, setzt die Strafbarkeit wie bei allen weiteren Passwortcracks erst mit der erfolgreichen Überwindung der Passwortsperre ein. Werden die Daten einer RFID-Zugangskarte entschlüsselt, erfüllt bereits dies den Tatbestand, ohne dass im Anschluss hieran eine mit diesen Daten gefälschte RFID-Karte auch tatsächlich zur Anwendung kommen müsste.

Das Ausspähen von Passwörtern oder sonstigen Daten mittels Trojaner-Software ist, wenn zur deren Installation Zugang zu einem geschützten System bestehen muss, bereits mit Erlangung dieses Zugriffs strafbar. Wird der Trojaner auf einem anderen Weg in das System eingeschleust, beispielsweise, indem durch Täuschung des Benutzers dieser selbst zur Installation veranlasst wird, so beginnt die Strafbarkeit in dem Augenblick, in dem die Möglichkeit zur Übermittlung geschützter Daten besteht. Ändert die Trojaner-Software zudem Daten wie Registry-Einträge im infizierten System, ist weiterhin auch der Tatbestand des § 303a StGB erfüllt.

Sämtliche der genannten Vorgehensweisen sind daher nur zulässig, soweit sie im Einvernehmen mit dem jeweiligen Rechtsgutsträger erfolgen.

VII. Das Ändern unsicherer Passwörter

Werden bei der Überprüfung der Passwortsicherheit unsichere Passwörter entdeckt – beispielsweise solche, die in Hardware werksseitig voreingestellt sind –, so müssen diese in aller Regel aus Sicherheitsgründen geändert werden. Dies fällt als Sperrung von Daten in den Anwendungsbereich des § 303a StGB, ist also mit den zuständigen Stellen im Unternehmen abzustimmen. Dürfen Arbeitnehmer zulässigerweise auch private Daten auf Unternehmensrechnern speichern – was in der Praxis eher selten der Fall ist –, ist zu bedenken, dass diese hinsichtlich ihrer Privatdaten selbst Rechtsgutsträger sind. Das Ändern von unsicheren Passwörtern wird zwar, wenn der entsprechende Arbeitnehmer nicht rechtzeitig ermittelt werden kann und ein entsprechendes Gefahrenpotential für die Rechtsgüter des Unternehmens vorliegt, in aller Regel als Notstandshandlung gerechtfertigt sein, dennoch sollte der Betroffene bald möglichst in Kenntnis gesetzt werden.

VIII. Einsatz von Virensoftware

Zur Überprüfung der Funktionalität und Leistungsfähigkeit von Abwehrprogrammen kann es notwendig sein, existierende oder selbst geschriebene Viren einzusetzen. Der Einsatz solcher Software fällt üblicherweise in den Anwendungsbereich des § 303a StGB. Zulässig ist ein solches Vorgehen auf Testsystemen,

C. IT-Sicherheitsüberprüfungen in der Praxis und ihre strafrechtliche Relevanz

die zu diesem Zweck bereit- bzw. selbst aufgestellt werden. Während der Überprüfung im Einsatz befindliche Produktivsysteme könnten nach ausreichender Aufklärung über gegebene Risiken und anschließender expliziter Gestattung ebenfalls derartigen Tests unterzogen werden, dies erscheint aber angesichts des Risikos selten notwendig. Das Programmieren von Viren, etwa mit Virusconstruction-Kits, ist nicht nach § 202c i. V. m. § 303a III StGB strafbar, wenn deren Einsatz einzig zu Testzwecken unter den oben genannten Bedingungen erfolgen soll (und dies optimalerweise auch dokumentiert ist) und die Virensoftware nicht an Dritte weitergegeben wird.[17]

IX. Einsatz von „Sniffern" zur Gewährleistung der Netzwerksicherheit

Zur Sicherstellung der Netzwerkfunktionalität wie auch zur Analyse von Angriffen kann es notwendig sein, den Netzwerktraffic mit sog. „Sniffern" zu überwachen und Einsicht in die einzelnen IP-Pakete zu nehmen. Allerdings ist der Einsatz von Sniffer-Software klassischer Anwendungsfall des § 202b StGB. Problematisch ist in diesem Zusammenhang, dass der Verfügungsberechtigte an den erlangten Daten nicht im Vorfeld zu ermitteln ist, da nicht abzusehen ist, wessen Daten hierbei abgefangen werden. Zulässigkeit aufgrund vorheriger Gestattung kommt hier also nicht in Betracht, eine nachträgliche Genehmigung im Sinne des Zivilrechts kennt das Strafrecht nicht.
Es stellt sich allerdings die Frage, wie es sich mit dem Einsatz von Sniffer-Software verhält, wenn diese ausschließlich der Sicherung der Funktionalität der Telekommunikationsnetze dient und hierfür unerlässlich ist. Dann wäre zumindest das Fernmeldegeheimnis aufgrund der Konkretisierung in § 88 III 1 TKG nicht berührt. Das Verhältnis von § 202b StGB zu § 88 TKG ist bisher rechtswissenschaftlich nicht untersucht. Es ist jedoch kein Grund ersichtlich, der für eine Schutzwürdigkeit der Nicht-Öffentlichkeit der Kommunikation noch über das Fernmeldegeheimnis hinaus spräche. Insbesondere wäre es zweckwidrig, die zur Netzwerksicherheit erforderlichen Maßnahmen zunächst durch § 88 III 1 TKG zu gestatten, um sie sodann über § 202b StGB wieder unter Strafe zu stellen. Insofern ist der Einsatz von Sniffer-Software, soweit er unerlässlich zum sicheren Betrieb des Telekommunikationsnetzes ist, nach § 88 III 1 TKG gerechtfertigt und damit nicht strafbar.

[17] Jlussi, „IT-Sicherheit und § 202c StGB", EICAR Positionspapier, S. 12, http://www.eicar.org/press/infomaterial/JLUSSI_LEITFADEN_web.pdf; Jlussi/Hawellek, „IT-Sicherheit im Lichte des Strafrechts", S. 69.
[18] Telekommunikationsgesetz, BGBl. I S. 1190, zuletzt geändert durch Artikel 2 des Gesetzes vom 21. Dezember 2007, BGBl. I S. 3198.

D. Rechtliche Anforderungen an die Einverständniserklärung

I. Bestimmung der Rechtsgutsträger

Entsprechend der soeben erfolgten Darstellung ist die überwiegende Zahl der IT-Sicherheitsüberprüfungen jeweils nur dann zulässig, wenn zuvor durch den Rechtsgutsträger die entsprechenden Tätigkeiten im vorgenommenen Umfang gestattet wurden. Die Bestimmung des Rechtsgutsträgers variiert dabei abhängig von der Schutzrichtung der jeweils einschlägigen Strafnorm. Daneben ist in bestimmten Fällen nach Daten, die das Unternehmen betreffen und die Arbeitnehmer im Rahmen ihrer beruflichen Tätigkeit auf Unternehmensrechnern anlegen (Unternehmensdaten) und solchen Daten, die Arbeitnehmer dort privat speichern (private Daten), zu differenzieren.

1. Personeller Schutzbereich des § 202a StGB

Schutzgut des § 202a StGB ist die sog. formelle Verfügungsbefugnis[19] über die Daten, also das Recht am Zugang zum gedanklichen Inhalt der gespeicherten Informationen. Unberücksichtigt bleiben dabei sowohl die Eigentumsverhältnisse hinsichtlich des verwendeten Datenträgers[20] als auch – obwohl dies die systematische Stellung der Norm nahe legen würde – der persönliche Geheimbereich.[21] So genießt den Schutz der Norm nicht etwa derjenige, auf den sich die Daten beziehen[22] – wie es im Datenschutzrecht der Fall ist –, sondern diejenige Person, die das Recht inne hat, über den Zugang zu den Daten zu entscheiden.[23] Sind also beispielsweise personenbezogene Daten der Mitarbeiter in geleasten Informationssystemen des Arbeitgebers gespeichert, so ist hinsichtlich eines Hackings dieser Systeme nur der Arbeitgeber selbst geschützt, nicht aber etwa der Leasinggeber als Eigentümer der Systeme oder der Arbeitnehmer, dessen Daten ausgelesen wurden. Letzterer wiederum erfährt ausreichenden strafrechtlichen Schutz durch die spezialgesetzlichen Regelungen der §§ 43, 44 BDSG, die datenschutzrechtliche Verstöße sanktionieren.[24] Rechtsgutsträger im Sinne des § 202a StGB ist also, wer berechtigt ist, den Zugang zu den Daten zu gestatten und sein Geheimhaltungsinteresse durch eine Zugangssicherung dokumentiert.

a) Unternehmensdaten

Hinsichtlich von Unternehmensdaten wird durch Zugangssicherungen im Rahmen des Informationsschutzes das formelle Geheimhaltungsinteresse des Unternehmens an seinen Daten gegen Zugang durch Unbefugte innerhalb und außerhalb des Unternehmens geschützt. Dabei kommt es nicht darauf an, wer diesen Zugriffschutz tatsächlich installiert oder wer die geschützten Daten speichert. Relevant ist vielmehr, in wessen Auftrag dies geschieht und wer hinsichtlich des Zugangs zu den Informationen entscheidungsbefugt ist.[25] Daher ist es hinsichtlich der Verfügungsbefugnis an Unternehmensdaten unerheblich, dass der Arbeitnehmer ein persönliches, nur ihm bekanntes Passwort verwendet und die geschützten Daten durch ihn eingeben wurden. Denn dadurch wird kein eigenes formelles Geheimhaltungsinteresse des Arbeitnehmers gegenüber dem Unternehmen an dessen Daten begründet, vielmehr erfüllt der Arbeitnehmer lediglich seine Pflicht, den durch die unternehmensseitig eingerichteten Zugangssicherungen gewährleisteten Schutz zu vervollständigen. Rechtsgutsträger hinsichtlich von Unternehmensdaten ist damit allein das Unternehmen.

[19] SK-Hoyer, § 202a Rn. 1, Sch/Sch-Lenckner, § 202a Rn. 1, Lackner/Kühl, § 202a Rn. 1, LK-Schünemann, § 202a Rn. 2.
[20] MünchKomm-Graf, § 202a Rn. 17; Weißgerber, NZA 2003, 1005-1009 [1007].
[21] 2. WiKG-E, BT-Drucks. 10/5058, S. 28.
[22] Sch/Sch-Lenckner, § 202a Rn. 1.
[23] SK-Hoyer, § 202a Rn. 1; LK-Schünemann, § 202a Rn. 2, Sch/Sch-Lenckner, § 202a Rn. 1.
[24] Sch/Sch-Lenckner, § 202a Rn. 1.
[25] BayObLG v. 24.06.1993 – 5 St RR 5/93; MünchKomm-Graf, § 202a StGB Rn. 17.

D. Rechtliche Anforderungen an die Einverständniserklärung

b) Private Daten

Ist allerdings die Privatnutzung der vom Unternehmen bereitgestellten Hardware in einem bestimmten Umfang zulässig, so stellt sich die Frage, wer hinsichtlich der dadurch entstehenden privaten Daten verfügungsberechtigt ist. Dies erlangt bereits dann Relevanz, wenn zwar keine privaten Daten auf den Datenspeichern abgelegt werden dürfen, diese aber bei erlaubter privater Internetnutzung beispielweise als Browser-History oder Cookies automatisch anfallen. Diese Fallkonstellation ist juristisch umstritten und bisher nicht abschließend geklärt.

Auch hier kommt es allerdings entscheidend auf die Frage an, wer durch die Einrichtung einer Zugangssicherung sein Geheimhaltungsinteresse an diesen Daten zum Ausdruck bringt. Da der Arbeitnehmer keine zusätzlichen Zugangssicherungen auf dem von ihm genutzten Informationssystem installieren darf, kann er damit auch nicht in rechtlich zulässiger Weise ein Geheimhaltungsinteresse gegenüber dem Unternehmen dokumentieren. Vielmehr genießt der Arbeitnehmer den Schutz, den die vom Unternehmen eingerichteten Zugangssicherungen ohnehin bieten. Dies macht diese Zugangssicherungen aber noch nicht zu solchen des Arbeitnehmers, da er auf ihren Bestand, ihre Eigenschaften und die Frage, wer sonst auf das System Zugriff hat, keinen Einfluss nehmen kann. Insbesondere ist dem Arbeitnehmer bekannt, dass er selbst zwar Daten auf seinem Rechner niemandem sonst zugänglich machen darf, das Unternehmen hingegen sehr wohl weiteren Arbeitnehmern – beispielsweise Administratoren – den Zugang über deren Passwörter gestatten kann. Letztlich ist es alleinige Entscheidung des Unternehmens, welcher Arbeitnehmer zu welchem Betriebsmittel Zugang haben soll oder nicht.

Zulässigerweise auf den Informationssystemen gespeicherten privaten Daten mangelt es damit an einer besonderen Zugangssicherung, die das formelle Geheimhaltungsinteresse des Arbeitnehmers gerade gegenüber dem Unternehmen manifestieren würde.[26] Auf eine gesonderte Einverständniserklärung des betroffenen Arbeitnehmers kommt es daher nach hier vertretener Ansicht auch bei IT-Sicherheitsüberprüfungen, die den Zugang zu privat gespeicherten Daten ermöglichen, nicht an.

Dieses Ergebnis stellt den Arbeitnehmer keineswegs schutzlos, da § 202a StGB nur die formelle Verfügungsbefugnis schützen soll, nicht aber den persönlichen Geheimbereich desjenigen, den die Daten betreffen. Letzterer wiederum genießt ausreichenden Schutz durch §§ 43, 44 BDSG. Der Arbeitgeber oder ein von ihm beauftragter Dritter darf sich also zu den privaten Daten des Arbeitnehmers, sofern diese Personenbezug im Sinne des § 3 I BDSG aufweisen, nur unter Geltendmachung überwiegender berechtigter Interessen gemäß § 28 I Nr. 2 BDSG Zugang verschaffen und diese nur soweit hierzu erforderlich einsehen. Liegen derartige berechtigte Interessen, zu denen auch die Sicherheit und Funktionalität der Informationssysteme zählt, vor, so ist ein Eingriff in den persönlichen Geheimbereich des Arbeitnehmers datenschutzrechtlich zulässig. Erst recht erscheint es dann aber vor diesem Hintergrund wenig überzeugend, einen Eingriff in das formelle Geheimhaltungsinteresse des Arbeitnehmers zu konstruieren, um damit eine IT-Sicherheitsüberprüfung über den Umweg des § 202a StGB zu sanktionieren.

Nichtsdestotrotz ist diese Auffassung in der Rechts-

[26] Barton, CR 2003, 842.
[27] Für einen strafrechtlichen Schutz privater Arbeitnehmerdaten bspw. Weißgerber, NZA 2003, 1007.

D. Rechtliche Anforderungen an die Einverständniserklärung

wissenschaft nicht unumstritten.[27] Rechtssicherheit auch nach der gegenteiligen Ansicht kann nur dann erlangt werden, wenn im Falle erlaubter Privatnutzung auch das Einverständnis betroffener Arbeitnehmer zu den jeweiligen IT-Sicherheitsüberprüfungen vorliegt. Sofern unternehmensinterne IT-Sicherheitsabteilungen tätig sind, könnte dazu auf eine entsprechende Betriebsvereinbarung hingewirkt werden, beispielsweise als Teil derjenigen Betriebsvereinbarung, die die Privatnutzung der Betriebsmittel wie PC und Internetzugang regelt.

2. Personeller Schutzbereich der §§ 202b, 303a, 303b StGB

Personell geschützt durch § 202b StGB ist der an den abgefangenen Daten Verfügungsberechtigte. Dessen Bestimmung ist allerdings bei den praxisrelevanten Fällen des Einsatzes von Sniffersoftware im Vorfeld unmöglich, da nicht vorherzusehen ist, wessen Daten hierbei zufällig abgefangen werden. Das Abfangen von Daten ist jedoch entsprechend obiger Darstellung, soweit es zur Gewährleistung der Netzwerkfunktionalität und -sicherheit erforderlich ist, aufgrund der Rechtfertigung aus § 88 III 1 TKG zulässig, so dass es in diesen Fällen auf ein Einverständnis des an den abgefangenen Daten Berechtigten nicht ankommt, sofern der Ausführende tatsächlich rechtswirksam mit der Sicherstellung der Netzwerkfunktionalität betraut ist.

Rechtsgutsträger hinsichtlich Unternehmensdaten im Sinne des § 303a StGB ist ebenfalls das Unternehmen. Auch hier ist der Arbeitnehmer, auch wenn er die Daten angelegt hat, selbst nicht Rechtsgutsträger, da letztlich einzig dem Unternehmen das Recht zusteht zu bestimmen, ob Daten verändert, gelöscht oder gesperrt werden sollen. Sofern allerdings private Daten auf den Informationssystemen des Unternehmens gespeichert sind, ist eine Änderung dieser regelmäßig nur mit Einwilligung des Arbeitnehmers erlaubt. Ausnahmen hiervon bestehen nur in Fällen, in denen die Änderung – beispielsweise aus Notstand – gerechtfertigt ist, wie etwa in den beschriebenen Fällen der Änderung unsicherer Passwörter.

§ 303b StGB schützt in personeller Hinsicht den Inhaber der Informationssysteme, im hiesigen Kontext mithin ebenfalls das Unternehmen. Da Testsysteme mangels wesentlicher Bedeutung der dortigen Datenverarbeitung tatbestandlich bereits gar nicht erfasst sind, ist in der Praxis eine Gestattung nur bei Angriffen gegen Produktivsysteme notwendig, namentlich DOS-Attacken gegen Server. Zu beachten ist hierbei, dass eine wirksame Einwilligung ein entsprechendes Wissen über die Konsequenzen voraussetzt, so dass es maßgeblich auf eine vollständige und korrekte Aufklärung ankommt.

II. Weitere Anforderung an die Einverständniserklärung

1. Person des Gestattenden

Soweit das Unternehmen alleiniger Rechtsgutsträger ist, werden IT-Sicherheitsüberprüfungen durch dessen rechtliche Vertreter, etwa den Geschäftsführer der GmbH (§ 35 I GmbHG) oder den Vorstand der Aktiengesellschaft (§ 78 I AktG) gestattet. Das Recht hierzu kann allerdings im Rahmen der Unternehmensorga-

[27] Für einen strafrechtlichen Schutz privater Arbeitnehmerdaten bspw. Weißgerber, NZA 2003, 1007.

D. Rechtliche Anforderungen an die Einverständniserklärung

nisation an der Unternehmensleitung nachgeordnete Stellen übertragen werden,[28] in diesen Fällen können die zuständigen Mitarbeiter der entsprechenden Abteilungen ebenfalls rechtswirksam IT-Sicherheitsüberprüfungen gestatten. In den seltenen Fällen, in denen auch Rechtsgüter der Arbeitnehmer betroffen sein und kein Rechtfertigungsgrund wie etwa Notstand eingreifen sollte, ist deren Zustimmung einzuholen, sofern nicht diesbezüglich Betriebsvereinbarungen bestehen.

2. Individuelle Vereinbarung oder generelle Regelung

Die Gestattung von IT-Sicherheitsüberprüfungen kann individuell-konkret im Einzelfall oder generell-abstrakt durch unternehmensinterne Regelungen erfolgen. Ersteres bietet sich jeweils dann an, wenn externe Dienstleister in Anspruch genommen werden oder konzerneigene IT-Sicherheitsabteilungen in rechtlich selbständigen Tochtergesellschaften Sicherheitsaudits durchführen. In beiden Fällen werden üblicherweise Tests nur für einen bestimmten Zeitraum in überschaubarer Anzahl durchgeführt. Hier kann im Vorfeld jeweils individuell geregelt werden, welche Überprüfungen unter Anwendung welcher Methoden durchgeführt werden sollen.

Sollen hingegen regelmäßig IT-Sicherheitsüberprüfungen etwa durch das unternehmenseigene CERT erfolgen, können diese auch generell innerhalb des unternehmensinternen Regelwerks gestattet werden. Dies gestaltet sich praktischerweise als zweistufiger Vorgang. Zunächst wird die Unternehmensleitung, die grundsätzlich einzig befugt ist, derartige Überprüfungen zu gestatten, dieses Recht an eine nachgeordnete Stelle delegieren, um nicht selbst hiermit belastet zu sein. Es ist also unternehmensintern zu regeln, dass eine bestimmte Abteilung Zulässigkeit und Rahmen von IT-Sicherheitsüberprüfungen festlegen darf und von der Unternehmensleitung ausdrücklich befugt ist, hierzu Eingriffe in die entsprechenden strafrechtlich geschützten Rechtsgüter im als erforderlich erachteten Umfang zu gestatten. Auf der zweiten Stufe werden sodann von dieser Abteilung Regelungen für die Durchführung von IT-Sicherheitsüberprüfungen erstellt, die Vorgehensweisen und Umfang im Detail beschreiben. Diese können je nach Bedarf und technischer Entwicklung unproblematisch angepasst werden, dabei können auch ganze Klassen von Überprüfungen (etwa Tests aller Webserver auf Applikationssicherheit) insgesamt gestattet werden, soweit dies hinreichend präzise und abgrenzbar formuliert wird. Ebenfalls möglich sind zusätzliche einmalige Gestattungen ansonsten nach dem Regelwerk nicht zulässiger Tests, falls beispielsweise einmal ausnahmsweise ein laufender Webserver auf DOS-Sicherheit überprüft werden soll.

3. Zeitpunkt und Form der Befugnis

Strafrechtlich wird hinsichtlich der Gestattung von Eingriffen in geschützte Rechtsgüter rechtsdogmatisch zwischen dem tatbestandsausschließenden Einverständnis (z. B. bei § 202a StGB) und der rechtfertigenden Einwilligung (z. B. bei §§ 303a, 303b StGB) des Rechtsgutsträgers differenziert. Während ersteres lediglich tatsächlich vorzuliegen braucht, muss letztere stets explizit vor Ausführung der tatbestandlichen Handlung erklärt werden. Mit Blick auf die Rechtssicherheit des Überprüfenden bietet es sich allerdings in beiden Fällen an, bereits vor Testbeginn sicher zu stellen, dass eine entsprechende Befugnis schriftlich fixiert ist. Derart können Beweisschwierigkeiten wie

[28] MünchKomm-Graf, § 202a Rn. 18.

D. Rechtliche Anforderungen an die Einverständniserklärung

im Übrigen auch zivilrechtliche Haftungsrisiken vermieden werden.

4. Inhalt der Einverständniserklärung

Die Einverständniserklärung sollte zunächst die durchzuführenden Tests und deren Zielsetzung enthalten, weil dies wesentliche Merkmale des Umfangs des jeweils gestatteten Eingriffs sind. In Zweifelsfällen sollten daher auch angedachte Vorgehensweise angegeben werden, wenn sich dies nicht bereits aus den ersten beiden Punkten zwingend ergibt. Des Weiteren sind die zu überprüfenden Systeme klar abzugrenzen, so dass sichergestellt ist, dass keine Tests durchgeführt werden, die von der Gestattung nicht erfasst sind. Soweit Risiken bestehen, dass überprüfte Systeme – auch und insbesondere wenn dies mit dem Test nicht beabsichtigt wird – ausfallen oder sonst gestört werden, ist über deren Art und Gefahrenpotential aufzuklären, falls nicht ausschließlich separate Testsysteme betroffen sind. Derartige Risiken sollten zumindest stichpunktartig in der Einverständniserklärung erwähnt werden, um Beweisschwierigkeiten hinsichtlich des Umfangs der Aufklärung zu vermeiden. Soweit dies möglich ist, sollte schließlich sichergestellt werden, dass die gestattende Person hierzu auch tatsächlich befugt ist, falls sich dies nicht bereits aus ihrer Funktion im zu auditierenden Unternehmen ergibt. Generell gilt: je größer das Risiko und je intensiver der Eingriff in das geschützte Rechtsgut, desto höher sind die Anforderungen an die vorherige Aufklärung und an die Detailliertheit der entsprechenden Einverständniserklärung. Soweit dies berücksichtigt wird, können IT-Sicherheitsüberprüfungen ohne Strafbarkeitsrisiken durchgeführt werden.