

führt hingegen zu Typengemischen überwiegend leihvertraglicher Prägung (§§ 598 ff. BGB). Probleme ergeben sich hinsichtlich Letzterer insbesondere im Hinblick auf die GPL, welche auch in ihrer Version 3 der Netzwerknutzung von Software nicht hinreichend Rechnung trägt. Stützt man sich auf den genauen Wortlaut der GPLv3, wird es einem SaaS-Anbieter sogar möglich, ausschliesslich GPL-lizenzierte Software unter Zurückhaltung des Quellcodes via SaaS bereitzustellen. Jene Lücke schließt auch Ziff. 13 der GPLv3 nicht, der lediglich Kombinatio-

nen aus GPLv3 und Affero GPL berücksichtigt. Im internationalen Kontext stellt sich ferner die Frage nach dem anwendbaren Urheberrecht. Datenschutzrechtlich sind im Rahmen von SaaS-Leistungen vor allem die Vorschriften zur Auftragsdatenverarbeitung zur berücksichtigen (§ 11 BDSG). Finden Datenverarbeitungsprozesse im außereuropäischen Ausland statt, ist auf ein angemessenes Datenschutzniveau zu achten. Den übrigen Compliance-Anforderungen im Bereich des Geheimnisschutzes und im fiskalischen Bereich ist ebenfalls Rechnung zu tragen.

K&R-Newsletter Schweiz

RAin Dr. Ursula Widmer, Bern*

I. Überwachung des Internetverkehrs

Im Juni 2009 hatten die Behörden bei den Telekom-Anbietern eine vertrauliche Vernehmung bezüglich des Ausbaus der Überwachung (lawful interception) des Internetverkehrs im Rahmen von Strafuntersuchungen durchgeführt. Nachträglich wurde dies dann doch publik (vgl. Neue Zürcher Zeitung, 17. 7. 2009, S. 14).

Nach der bisher gültigen Rechtslage ist die Überwachung des Internetverkehrs nur eingeschränkt möglich. Das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) bietet die Grundlage für die Überwachung der gesamten Telekommunikation (Festnetz-/Mobiltelefonie, Internet). In der dazugehörigen Verordnung (VÜPF) wird jedoch in Bezug auf den Internetverkehr nur eine beschränkte Anzahl von Überwachungstypen festgelegt. Ausschliesslich für den E-Mail-Verkehr ist sowohl die Echtzeitüberwachung von Inhaltsdaten sowie der zugehörigen Randdaten als auch die rückwirkende Überwachung für Randdaten vorgesehen. Sonst ist lediglich die rückwirkende Überwachung der Randdaten bezüglich der Einwahl (Dial-up) über öffentliche Kommunikationsnetze sowie der Zuteilung von dynamischen IP-Adressen durch die Provider geregelt.

Mit den neuen organisatorischen, administrativen und technischen Richtlinien der für die Abwicklung der Überwachungsmaßnahmen zuständigen Bundesstelle, des Dienstes Überwachung Post- und Fernmeldeverkehr, soll die Echtzeitüberwachung der Inhaltsdaten für den gesamten Internetverkehr eingeführt werden. Auch soll die Überwachung der Internet-Telefonie in der gleichen Weise durchgeführt werden können wie für die übrige Telefonie, wenn Nummern des Nummernplans E.164 verwendet werden. Die neuen Richtlinien wurden gemäß der publik gewordenen Planung per 1. August in Kraft gesetzt, mit einer Übergangsfrist zur Implementierung durch die Anbieter bis Ende Juni 2010.

Das seitens der Behörden gewählte Vorgehen erstaunt. Die VÜPF sieht zwar den Erlass von Richtlinien durch den Dienst Überwachung Post- und Fernmeldeverkehr vor, jedoch nur bezogen auf die in der Verordnung geregelten Überwachungstypen. Dass der Dienst in seinen Richtlinien neue Überwachungstypen einführen kann, die in der Verordnung nicht geregelt sind, lässt sich hingegen dem Wort-

laut der VÜPF nicht entnehmen und entspricht auch nicht der Systematik und hierarchischen Ordnung im Verhältnis zwischen BÜPF, VÜPF und Richtlinien des Dienstes.

Man darf gespannt sein, wie die Gerichte dieses Vorgehen beurteilen werden, sollte sich entweder ein von einer solchen Überwachungsmaßnahme Betroffener dagegen zur Wehr setzen oder ein Provider sich weigern, die für die neuen Überwachungstypen erforderlichen technischen Investitionen auf seine Kosten vorzunehmen, weil er die rechtliche Basis als ungenügend erachtet.

II. „Safe Harbor“ für Daten aus der Schweiz in den USA

Mit einem Briefwechsel zwischen der Schweiz und den USA wurden die Grundlagen für das „U.S.-Swiss Safe Harbor Framework“ geschaffen, das seit Anfang 2009 in Kraft ist (vgl. die Website des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, EDÖB, unter <http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=de>, Stand: 24. 8. 2009). Vorbild war das vergleichbare Framework, das zwischen den USA und der EU bereits seit 2000 besteht.

Mit dem Framework ist es für schweizerische Unternehmen einfacher, Personendaten an US-Unternehmen weiterzugeben. Da in den USA kein angemessener gesetzlicher Datenschutz besteht, war es vorher für Schweizer Unternehmen – abgesehen von einigen eng umschriebenen Ausnahmen – nur dann rechtlich zulässig, Personendaten in die USA weiterzugeben, wenn sie den Datenempfänger in einem Vertrag zur Beachtung des Datenschutzes verpflichtet hatten. Dieser Vertrag musste beim EDÖB zur Prüfung eingereicht werden und erst nach dessen Freigabe durften die Daten übermittelt werden.

Gemäß dem Safe Harbor Framework können sich US-Unternehmen nun beim US-Handelsministerium zur Einhaltung der im Framework definierten Datenschutzregeln verpflichten und entsprechend zertifizieren lassen. Damit ist ein nach schweizerischen Standards angemessener Datenschutz gewährleistet und Schweizer Unternehmen dürfen auch ohne vorgängigen Abschluss eines vom EDÖB

* Mehr über die Autorin erfahren Sie auf S. VIII.

zu prüfenden Vertrages Daten an die betreffenden US-Unternehmen weitergeben.

Vor allem für solche US-Unternehmen, die bereits unter dem U.S.-EU Safe Harbor Framework zertifiziert sind oder die in regelmäßigem Datenaustausch mit mehreren Unternehmen in der Schweiz stehen, oder für Konzerne mit Gruppengesellschaften in der Schweiz und den USA kann das Framework von Vorteil sein. Da die Zertifizierung beim Handelsministerium für die US-Unternehmen mit einem gewissen Aufwand verbunden ist, bietet das Framework jedoch nicht in allen Fällen eine sinnvolle Lösung. Der Abschluss eines Vertrages mit dem Datenempfänger in den USA kann sich gegebenenfalls nach wie vor als der einfachere Weg herausstellen. Dies ist jeweils im Einzelfall zu prüfen.

III. Kein Anspruch auf ungehinderten E-Mail-Verkehr

Der Absender und der vorgesehene Empfänger einer E-Mail, die im Spam-Filter des Providers des Empfängers hängen geblieben war, hatten den Erlass einer beschwerdefähigen Verfügung verlangt, wonach festzustellen sei, dass durch die Blockierung der E-Mail ihr Recht auf freie Kommunikation gemäß Art. 10 EMRK verletzt worden sei. Das Bundesamt für Kommunikation (BAKOM) hatte es abgelehnt, in dieser Sache zu verfügen, unter Hinweis darauf, dass das Verhältnis zwischen Absender und Empfänger und ihren jeweiligen Providern privatrechtlicher Natur sei und daher Ansprüche gegenüber den Providern vor den Zivilgerichten durchzusetzen seien.

In zweiter Instanz gab das BVerwG (Urteil A-6437/2008 vom 12. 2. 2009) den Beschwerdeführern insofern Recht, als das BAKOM seinen Entscheid, die verlangte Feststellung nicht zu treffen, in einer formellen Nichteintretensverfügung hätte erlassen sollen. In der Sache bestätigte das Gericht die Auffassung des BAKOM, wonach Ansprüche von Kunden gegenüber ihren Providern gemäß dem schweizerischen Fernmelderecht nicht in einem Verwaltungsverfahren, sondern auf dem Rechtsweg vor den Zivilgerichten geltend zu machen sind. Auch aufgrund der EMRK ergebe sich nichts anderes.

Das Gericht beurteilte dabei das Anliegen der Beschwerdeführer nicht unter dem Aspekt von Art. 10 EMRK, wie von diesen verlangt, da diese Bestimmung der EMRK die öffentliche Massenkommunikation zum Gegenstand habe, während es sich beim E-Mail-Verkehr um Privatkommunikation handle, welche durch Art. 8 EMRK geschützt sei. Diese letztere Vorschrift diene in erster Linie der Abwehr von staatlichen Eingriffen in die Privatsphäre. Staatliche Schutzmaßnahmen könnten dagegen nur unter besonderen Voraussetzungen verlangt werden.

Das Bestehen einer staatlichen Schutzpflicht sei unter Abwägung anderer legitimer Interessen zu beurteilen. Solchen anderen Interessen, nämlich der Bekämpfung von Spam, gab das Gericht den Vorrang. Es berücksichtigte insbesondere, dass die Telekom-Anbieter gemäß Art. 45 a des schweizerischen Fernmeldegesetzes verpflichtet sind, Spam zu bekämpfen, und hierzu gemäß Art. 83 der Verordnung über Fernmeldedienste ihre Kunden gegen den Erhalt von Spam schützen müssen, soweit dies der Stand der Technik zulässt. Mit anderen Worten, die Provider müssen Spam-Filter einsetzen. Dabei ist es nach Auffassung des Gerichts hinzunehmen, dass Spam-Filter nicht absolut fehlerfrei sind und auch vereinzelt E-Mails darin hängen bleiben, die keinen Spam darstellen.

Rechtsprechung

Keine Grundrechtsverletzung durch „Hacker“-Paragraf

BVerfG, Beschluss vom 18. 5. 2009 – 2 BvR 2233/07, 2 BvR 1151/08, 2 BvR 1524/08

§ 202 c StGB

1. Der objektive Tatbestand des § 202 c Abs. 1 Nr. 2 StGB erfasst keine dual-use-Programme.

2. Der Einsatz von Schadsoftware zu Penetrationstests mit Einverständnis des Verfügungsberechtigten des betreffenden Computersystems erfolgt nicht „unbefugt“ i. S. d. §§ 202 a, 202 b StGB und erfüllt somit nicht das nach § 202 c Abs. 1 StGB erforderliche subjektive Merkmal der Vorbereitung einer Computerstraftat. (Leitsätze der Kommentatoren)

Sachverhalt

Die Verfahren betreffen die Frage, ob die Strafbarkeit des Vorbereitens des Ausspähens und Abfangens von Daten nach § 202 c Abs. 1 StGB, insbesondere dessen Nr. 2, mit dem Grundgesetz vereinbar ist.

Der Beschwerdeführer F. war Geschäftsführer der Firma V. Deutschland GmbH (im Folgenden: V.). Das Unternehmen bietet Dienstleistungen im Bereich der Sicherheit von Informations- und Kommunikationstechnologien an. Im Rahmen ihres Geschäftsbetriebes führt die Firma V. unter anderem so genannte Penetrationstests durch. Dabei handelt es sich um Sicherheitsüberprüfungen von EDV-Anlagen durch Simulation nicht autorisierter Zugriffsversuche: Die Mitarbeiter der V. versetzen sich in die Situation eines Angreifers und versuchen, Sicherheitslücken zu finden, um auf diese Weise in das zu überprüfende EDV-System – typischerweise ein Netzwerk eines Unternehmens – einzudringen. Gegenstand der unternehmerischen Tätigkeit der V. ist damit unter anderem die Feststellung, wie verletzlich das Zielsystem für „Hacker-Angriffe“ ist. Nach Abschluss der Überprüfung wird ein Bericht erstellt, der es dem Inhaber der geprüften EDV-Anlage ermöglicht, im Falle aufgedeckter Sicherheitslücken Gegenmaßnahmen zu ergreifen und so die Systemsicherheit zu verbessern. Die V. wird dabei ausschließlich im Auftrag und mit Einverständnis des Betreibers der EDV-Anlage tätig. Zur Realisierung der Penetrationstests setzt die Firma V. eine Vielzahl von EDV-Programmen ein, deren mögliche Einsatzbereiche nicht immer eindeutig definiert sind. Teilweise handelt es sich um Analysewerkzeuge, die sowohl vom berechtigten Nutzer/Administrator eines Computersystems zu dessen bestimmungsgemäßer Wartung und Pflege als auch ohne oder gegen den Willen des Berechtigten zum Zwecke des Ausspähens von Schwachstellen verwendet werden können (dual use tools). Teilweise entstammen die Programme auch anonymen „Hacker-Foren“ im Internet, die vermuten lassen, dass die Programme von ihren Urhebern zum Zwecke des illegalen Eindringens in EDV-Systeme konzipiert wurden (so genannte malware oder Schadsoftware). Mit der fristgerecht (§ 93 Abs. 3 BVerfGG) eingegangenen Verfassungsbeschwerde rügt der Beschwerdeführer F., § 202 c StGB verstoße gegen Art. 12 Abs. 1 GG.