NDS-BWK 1

Frau Svea Anlauf

Kurzfassung: Der strafrechtliche Schutz des E-Mail Verkehrs im Internet

Obwohl der (unverschlüsselte) E-Mail-Verkehr in Bezug auf die Vertraulichkeit der Daten mit einer Postkarte vergleichen werden kann und diverse Möglichkeiten bestehen, Daten im Internet „abzuhören“, gewinnt die Kommunikation per E-Mail immer mehr an Bedeutung. Strafrechtlichen Schutz geniessen per E-Mail übersandten Informationen jedoch nur dann, wenn die Daten i.S.d. Art. 143 StGB „gegen unberechtigten Zugriff besonders geschützt“ sind, d.h. wenn der über die Daten Verfügungsberechtigte entsprechende Sicherungs-massnahmen zur Schutz seiner Daten eingesetzt hat. Derzeit stellt sich die Datensicherheit im Internet als problematisch dar, wobei der gesamte Übertragungsweg vom Absender zum Empfänger potentielle Angriffspunkte bietet. Will sich der „Datendieb“ E-Mail-Daten im Internet „beschaffen“, kann er einerseits Kabel, Funkstrecken und sonstige Fernübertragungseinrichtungen „physisch“ anzapfen und zum anderen den Datenverkehr durch Hacking/Cracking-Angriffe, mittels spezieller Software (Packet-Sniffing, Routing- und Man-In-The-Middle-Attacken) auf den Servern und Routern der Internet Provider „abhören“. In der Rechtsliteratur zu Art. 143 StGB werden als Zugriffsicherungen bei der Datenfernübertragung die Verwendung von Betonhüllen und sonstigen Abschirmmassnahmen zur Verhinderung des Auffangens des Datenstroms sowie die Datenverschlüsselung diskutiert; darüber hinaus soll nach einem Teil der schweizerischen Lehre aufgrund des im Fernmeldegesetz normierten Fernmeldegeheimnisses bereits die Nutzung von Telefonleitungen und drahtlosen Übermittlungskanälen eine Datensicherung i.S.d. Art. 143 StGB darstellen.
Die dargestellten Varianten erfüllen jedoch nur zum Teil die Anforderungen an Zugriffsicherungen i.S.d. Art. 143 StGB. Zwar unterfallen sämtliche, mit dem E-Mail-Verkehr und damit auch mit möglichen „Lausch“Angriffen zusammenhängende Einrichtungen wie Leitungen und Funkstrecken, Verbindungseinrichtungen, die von den Internet Service Providern (ISP) betriebenen Server und Router sowie die digitalen Schnittstellen dem Fernmeldegesetz, doch können weder das in Art. 43 FMG normierte Fernmeldegeheimnis, noch das in Art. 50 FMG normierte Verbot, mittels Fernmeldeanlagen nichtöffentliche Informationen zu empfangen und zu verwenden, die nicht für ihn bestimmt sind, geeignete Zugriffsicherungen i.S.d. Art. 143 StGB darstellen. So unterfällt dem in Art. 43 FMG normierten Fernmeldegeheimnis selbst zwar der gesamte, mit der Übermittlung von E-Mails betraute Personenkreis, d.h. u.a. die Betreiber von Telefon-, oder Datenübertragungsnetzen und die ISPs, die E-Mail-Dienste via eigener Anschlusstechnologie oder via öffentlich zugänglichen Fernmeldenetzen erbringen, nicht aber der hier interessierende „externe Datendieb“, der sich die per E-Mail übermittelten Daten durch die dargestellten „Abhör“Methoden beschafft. Darüber hinaus entsprechen die Regelungen des Fernmeldegesetzes nicht den von der Literatur aufgestellten Anforderungen an die Zugriffsicherung i.S.d. Art. 143 StGB.
Auch wenn sich der Rechner des Absenders einer E-Mail ebenso wie derjenige des Empfängers in der Schweiz befindet, und sich beide eines inländischen Providers bedienen, wird die Verbindung zwischen diesen beiden Rechnern relativ häufig über ein Drittland (z.B. die USA) hergestellt. Aufgrund der Architektur des Internets ist es für den Absender einer E-Mail weder vorhersehbar, welchen genauen Weg die Datenpakete auf dem Weg durch das

Internet nehmen, noch, ob die Daten durch Kabel, mittels terrestrischem Richtfunk oder per Telekommunikationssatteliten übertragen werden. Da die Daten somit auch beim E-Mail-Verkehr innerhalb der Schweiz i.d.R. über das Ausland fliessen, d.h. den räumlichen Geltungsbereich des Fernmeldegesetzes verlassen, können sie bereits objektiv nicht als Zugriffsicherung eingesetzt werden. Darüber hinaus stellen die Ge- und Verbote des Fernmeldegesetzes weder physische oder EDV-mässige Sicherungs"Vorkehrung" dar, noch wählt der Absender einer E-Mail die dem Fernmeldegesetz unterstehenden Übertragungseinrichtungen mit der Zielrichtung, zumindest gleichrangig neben anderen Zielen auch den Schutz der zu übermittelnden Daten vor unberechtigtem Zugriff zu gewährleisten. Demgegenüber stellt die Datenverschlüsselung, auch wenn sie nicht den (physischen) Zugang zu den chiffrierten Daten verhindert, sondern lediglich davor schützt, dass der Täter den Bedeutungsgehalt der Daten zur Kenntnis nehmen kann, aufgrund der systematischer Stellung des Art. 143 StGB bei den Vermögensdelikten eine geeignete und ausreichende Zugriffssicherung i.S.d. Art. 143 StGB dar. Hierbei ist von Bedeutung, dass der technische Datenbegriff nicht mit demjenigen des Art. 143 StGB übereinstimmt, d.h. dass „Daten" i.S.d. Art. 143 StGB in erster Linie nicht als eine „Kombination" von Bits zu definieren sind, sondern vielmehr als die von einer Datenverarbeitungsanlage verarbeiteten, gespeicherten oder weitergegebenen Informationen über einen Sachverhalt. Da diese Informationen aber trotz ihrer Verschlüsselung erhalten bleiben und übermittelt werden, sind sie auch Objekt der Tathandlung, d.h. des „Abhören" während der Datenfernübertragung. Vergleicht man des Weiteren die Aneignung des in einer Sache verkörperten (Sach)Wertes mit der Aneignung des in den Daten verkörperten (Informations)Wertes, so ist der Datenberechtigte (vergleichbar dem Eigentümer einer Sache) dann in seinem Verfügungsrecht verletzt, wenn sich der Täter den durch die Daten „verkörperten" (Informations)Wert beschafft. Insofern umfasst Art. 143 StGB aber nicht nur das Recht des Verfügungsberechtigten, darüber bestimmen können, wer seine Daten besitzt, sondern auch, wer seine Daten, d.h. die „hinter" den Daten stehenden Informationen zur Kenntnis nimmt. Weiterhin stellt die Datenverschlüsselung auch eine geeignete Zugriffssicherung dar. In Anlehnung an § 243 Abs. 1 Nr. 2 StGB (D), wonach ein besonders schwerer Fall des Diebstahls vorliegt, wenn der Täter eine Sache entwendet, die durch eine Schutzvorrichtung gegen Wegnahme besonders gesichert ist, muss der Datenberechtigte (entsprechend dem Eigentümer einer Sache) seine Daten gegen die jeweilige „Wegnahme"- d.h. Zueignungshandlung und somit die Erlangung der Verfügungsbefugnis über den Informationswert der Daten schützen. Insofern aber ist ein Zugriffsschutz ausreichend und erforderlich, der - wie die Verschlüsselung - den Täter eben gerade von der Erlangung dieser Informationen abhält. Schliesslich stellen die heute gängigen Verschlüsselungsstandards, d.h. eine mindestens 40-Bit-Verschlüsselung, die Personen in der Rolle des konkreten Täters üblicherweise verunmöglicht, ohne besonderen Aufwand an die geschützten Daten heranzukommen, auch eine ausreichende Zugriffssicherung i.S.d. Art. 143 StGB dar. Ob die Schutzmassnahmen bezogen auf die Sensibilität der Daten dem im konkreten Fall üblichen technischen, d.h. angemessenen und zumutbaren Standard der Sicherung entsprechen müssen, d.h. ob per E-Mail übermittelte sensible Daten mit einer Mindest-Schlüsselstärke zu sichern sind, ist fraglich und insbesondere abhängig davon, ob und inwieweit des Prinzip der Opfermitverantwortung auf Art. 143 StGB anzuwenden ist. Im Sinne eines Ausblicks wäre grundsätzlich zu überlegen, ob zur Auslegung des Art. 143 StGB nicht die in Sicherheitspolitiken und Sicherheitshandbüchern strukturierten und für alle Mitarbeiter einer Unternehmung verbindlich festgehaltenen allgemein anerkannten Informatiksicherheitsanforderungen, die sog. „Baselines Controls" wie der britischen Code of Practice for Information Security Management oder das deutsche IT-Grundschutzhandbuch herangezogen werden müssten.