

IT-SICHERHEIT UND RECHT

E-Mails, Viren und E-Commerce

Rechtsprobleme im Zusammenhang mit E-Mails und E-Commerce waren Schwerpunktthemen beim österreichischen IT-Sicherheitstag 2004 in Klagenfurt.

Wie ist die Rechtslage, wenn etwa ein Autor einem Verlag ein elektronisches Dokument übermittelt, das einen Virus enthält, der bei seiner Aktivierung erheblichen Schaden am Computersystem des Verlages anrichtet, und der Verlag den Schaden ersetzt haben will?

"Wenn der Versender eines elektronischen Dokuments oder einer E-Mail wusste, dass er ein Programm mittransportiert, das Daten beschädigt, ist die Rechtslage klar", berichtete Univ.-Prof. Dr. Peter Mader (Universität Salzburg). "Der Versender hat strafrechtlich das Delikt der Datenbeschädigung (§ 126 a StGB) zu verantworten und ist zivilrechtlich für den entstandenen Schaden haftbar."

In der Praxis ist der Täter allerdings nur schwer auszuforschen, weshalb wohl in den meisten Fällen auf Anzeigen verzichtet wird. Die Kriminalstatistik weist für 2003 österreichweit lediglich 31 angezeigte Straftaten nach § 126a StGB auf. Demgegenüber sind Fälle von Geldbeschaffungsaktionen bekannt geworden, indem Mahnbriefe wegen angeblich versendeter Viren ausgesendet wurden.

Wenn jemand unwissentlich Viren versendet und dadurch Schaden verursacht, ist Voraussetzung für eine zivilrechtliche Haftung, dass zumindest Fahrlässigkeit vorliegt. Die allgemeine Auffassung geht dahin, dass bei einer Teilnahme am Internet-Verkehr eine Verkehrssicherungspflicht besteht, ähnlich der, dass beispielsweise ein Gehsteig im Winter zu räumen ist. Es gilt, Schaden durch geeignete Virenvorsorge zu verhindern, unabhängig davon, ob eine geschäftliche oder vertragliche Beziehung zu einem Kommunikationspartner besteht. Eine von Mader als zu weit gehend abgelehnte Rechtsauffassung geht sogar dahin, dass bereits mit der Aufnahme eines Kommunikationspartners in das elektronische Adressbuch die Verpflichtung zur Vorsorge gegen Viren besteht.

Die Verpflichtung zur Verwendung geeigneter Schutzprogramme besteht jedenfalls für Unternehmer, die sich der elektronischen Kommunikation bedienen. Bei Privatpersonen werden die Anforderungen geringer sein, doch sind die Details in der juristischen Diskussion noch umstritten. Die Sorgfaltspflicht umfasst auch, die Virenschutzprogramme entsprechend zu warten und auf dem neuesten Stand zu halten (regelmäßige Durchführung von Updates). Die Haftung wird dann entfallen, wenn ein konkreter Virus zum Zeitpunkt der Versendung von einem gängigen Virenschutzprogramm noch nicht erfasst war ("rechtmäßiges Alternativverhalten").

Die Verpflichtung, aktuelle Virenschutzprogramme zu verwenden, trifft auch den Empfänger einer elektronischen Sendung, was zur Schadensteilung führen kann. Allerdings liegt, soweit überschaubar, zur gesamten Problematik weder in Deutschland noch in Österreich eine Gerichtsentscheidung vor. Die eigene Nachricht mit einer Erklärung zu versehen, dass man für allenfalls eintretende Schäden nicht haftet (Disclaimer), bringt rechtlich nicht viel: Eine einseitige Freizeichnung ist nicht möglich. Schäden, die Außenstehende verursachen, werden durch eine Betriebshaftpflichtversicherung gedeckt. Eine Versicherung des eigenen

Unternehmens gegen Virenschäden bieten die wenigsten Versicherer an; das Risiko ist zu hoch.

Zur Spam-Problematik erläuterte Prof. Mader das nach § 107 TKG 2003 geltende System: Demnach ist die Versendung von E-Mails (und SMS) an Verbraucher im Sinne des Konsumentenschutzgesetzes (KSchG) ohne deren vorherige Einwilligung unzulässig ("Opt-in-System") und mit Verwaltungsstrafe bis zu 37.000 Euro bedroht, wenn sie zur Direktwerbung erfolgt oder an mehr als 50 Empfänger gerichtet ist (auch eine gut gemeinte Virenwarnung unterliegt dem Verbot der Massensendung).

Keine Zustimmung des Verbrauchers ist erforderlich, wenn bestehende Kundenkontakte fortgesetzt werden, doch der Kunde muss klar und deutlich die Möglichkeit erhalten haben, künftige Werbung dieser Art kostenfrei und problemlos abzulehnen (§ 107 Abs 3 TKG 2003).

An Nichtverbraucher darf elektronische Werbung auch ohne deren vorherige Einwilligung gesendet werden, es muss ihnen aber die Möglichkeit eingeräumt werden, den Empfang weiterer elektronischer Post abzulehnen ("Opt-Out-System"). Jedenfalls verboten und ebenfalls mit Verwaltungsstrafe bedroht ist es, Nachrichten zum Zweck der Direktwerbung ohne Angabe des Absenders zu versenden. Zusätzlich verlangt § 7 E-Commerce-Gesetz (ECG, BGBl I 2001/152), kommerzielle Kommunikation als solche erkennbar zu machen.

Probleme ergeben sich im E-Mail-Verkehr schließlich daraus, dass die Absender-Adresse leicht verfälscht werden kann (und damit die Behauptung "das habe ich nie geschrieben" kaum zu widerlegen ist). Andererseits ist der Eingang beim Empfänger nicht sicher nachweisbar (Lesebestätigungen können verweigert werden – "das habe ich nie erhalten").

Letztlich kann der Inhalt der Nachricht verändert worden sein ("das habe ich nicht geschrieben"). Abhilfe bietet die elektronische Signatur; allerdings kann auch sie keinen Zugangsbeweis liefern. Allenfalls kann dieser durch automatische Übermittlungsbestätigungen des Mailservers des Empfängers erbracht werden, doch ist fraglich, ob die Gerichte das anerkennen werden.

Informationspflichten

Dr. Sonja Janisch (Universität Salzburg) referierte über Webauftritte von Unternehmen. "Diensteanbieter" (§ 3 Z 2 ECG) haben Informationspflichten zu beachten, selbst wenn sie nur eine Website betreiben, nämlich darüber, wer sie sind und wie sie erreicht werden können (Impressumpflicht, § 5 Abs 1 ECG). Preise sind leicht lesbar auszuzeichnen (§ 5 Abs 2 ECG). Verstöße gegen die allgemeinen Informationspflichten sind mit Verwaltungsstrafe bis 3.000 Euro bedroht (§ 26 Abs 1 Z 1 ECG), außerdem drohen – wegen des hohen Streitwerts, in der Regel 36.000 Euro – teure Unterlassungsklagen nach § 1 UWG. Webshop-Betreiber haben darüber hinaus nicht nur anzugeben, wie eine Bestellung bei ihnen abläuft (§ 9 ECG), sie treffen auch sich aus dem KSchG ergebende zusätzliche Informationspflichten vor und nach dem Vertragsabschluss (§§ 5 c und 5 d KSchG).

Dem Verbraucherschutz dient, dass bei Fernabsatzgeschäften eine Rücktrittsfrist von 7 Werktagen (Samstage zählen nicht) gilt (§ 5 e KSchG); bei Waren gerechnet vom Eingang beim Verbraucher, bei Dienstleistungen mit dem Tag des Vertragsabschlusses.

Der Rücktritt braucht nicht begründet zu werden, ein schlichter Meinungswechsel genügt. Verbraucher und Unternehmer haben dann Zug um Zug zurückzuerstatten, was sie vom jeweils anderen erhalten haben (§ 5g Abs 1 KSchG), wobei dem Verbraucher nur die

unmittelbaren Kosten der Rücksendung auferlegt werden dürfen, und dies auch nur dann, wenn vertraglich eine solche Vereinbarung getroffen wurde (§ 5g Abs 2 KSchG).

Kurt Hickisch

Österreichischer IT-Sicherheitstag

Der Österreichische IT-Sicherheitstag 2004 am 22. September an der Universität Klagenfurt wurde von Univ.-Prof. Dr. Patrick Horster (Universität Klagenfurt) veranstaltet und moderiert. Vorausgegangen war eine zweitägige Konferenz zum Thema "Elektronische Geschäftsprozesse". Eine ähnliche Veranstaltung, bei der Prof. Horster im Programmkomitee den Vorsitz führt, wird für den 15. und 16. März 2005 unter dem, die Teilnehmerländer bezeichnenden Titel D.A.CH Security 2005 an der TU Darmstadt vorbereitet.

Universität Klagenfurt, Institut für Informatik – Systemsicherheit, Universitätsstraße 65-67, A-9020 Klagenfurt.

<http://syssec.uni-klu.ac.at/>