

Studie

Rechtssicherheit in der Informations- und Kommunikationstechnologie

Spammer, Hacker, Phisher usw sind nicht nur zur Plage geworden, sondern limitieren mit Milliarden Schäden auch das wirtschaftliche Potential der Informations- und Kommunikationstechnologie. Die kürzlich beobachteten Phishing-Attacken gegen die BAWAG machen die Aktualität der Thematik deutlich. Die Studie des e-center zeigt rechtliche Schutzmechanismen auf. Sie beschäftigt sich mit der Rechtslage bei Spamming, Hacking, Cracking, WarDriving, Viren/Würmern, Phishing und Dialern. Da Computerkriminelle oft nicht zu fassen sind, wird auch die Verantwortlichkeit der Provider behandelt.

Spamming verursacht allein in Deutschland jährlichen Schaden von 300 Millionen Euro. Liegt nach österreichischem Recht vor allem bei Versand von Werbemails und Massenmails (mehr als 50 Empfänger) vor (auch SMS und MMS). Ist gemäß § 107 Telekommunikationsgesetz ohne vorherige Zustimmung B2C grundsätzlich unzulässig (opt in), B2B grundsätzlich zulässig, wenn bestimmte Vorkehrungen eingehalten werden, insb Absender nicht verschleiert und Abbestellung ermöglicht wird (opt out). Problem der Abgrenzung: jede mail an Unternehmensmitarbeiter erfasst oder nur an Unternehmensadresse (zB info@xyz.com) bzw nur in Bezug auf Produkte oder Dienstleistungen, die unternehmensgegenständlich? Im Zweifel sollte im Hinblick auf diese und weitere Rechtsunsicherheiten vom Versand von Werbemails abgesehen (Sanktionen: bis Eur 37.500 Strafe, Schadenersatz- und Unterlassungsklage) bzw die Rechtslage vorher spezifisch untersucht werden.

Hacking (Eindringen in fremde Netzwerk- bzw Computersysteme) kann je nach Art und Intensität des Angriffs vor allem folgende Konsequenzen nach sich ziehen:

- Schadenersatz
- Strafbarkeit gemäß
 - § 51 Datenschutzgesetz (Datenverwendung)
 - § 118 StGB (Widerrechtlicher Zugriff auf ein Computersystem)
 - § 119 StGB (Verletzung des Telekommunikationsgeheimnisses)
 - § 119a StGB (Missbräuchliches Abfangen von Daten)
 - § 123 StGB (Auskundschaften von Geschäfts- und Betriebsgeheimnissen)
 - § 126 StGB (Datenbeschädigung)

Cracking liegt vor, wenn Schutzmechanismen von Software „geknackt“ werden, um das Anfertigen illegaler Kopien zu ermöglichen. Weltweiter Schaden wird auf 29 Milliarden USD geschätzt, davon 109 Millionen in Österreich. Rechtlichen Schutz bietet vor allem das Urheberrecht, und zwar einerseits in Form zivilrechtlicher Ansprüche (Unterlassung, Beseitigung, Schadenersatz), andererseits in Form von Straftatbeständen bei gewerblicher Begehung. Das vom Urheberrecht ausdrücklich eingeräumte Recht auf Privatkopie (für den eigenen, nicht-kommerziellen Gebrauch, nicht für Software) wird durch das ebenfalls vom Urheberrecht gewährte Recht auf Kopierschutz relativiert.

Im Bereich des Digital Rights Management bedeutet dies, dass der Kopierschutz dem Recht auf Privatkopie vorgeht, der Schutzmechanismus also nicht unter Berufung auf das Recht auf Privatkopie überwunden werden darf. Ob das Recht auf Privatkopie auch dann besteht, wenn die Kopiervorlage rechtswidrig ist (vor allem bei Musikaustauschbörsen), ist in Österreich nicht klar geregelt und daher noch immer umstritten. In anderen Ländern (zB Deutschland) ist die Rechtslage eindeutig: keine Privatkopie, wenn Vorlage erkennbar rechtswidrig. Bei Software besteht auch in Österreich kein Recht auf Privatkopie.

WarDriving setzt sich aus der Abkürzung für Wireless Access Revolution und Driving zusammen und bezeichnet das Abfahren bestimmter Gegenden zum Zwecke des Aufspürens von WLANs. Gebräuchlich sind auch Begriffe wie WarWalking oder WarChalking (Anzeigen von gefundenen WLANs auf Hauswänden mittels Kreidezeichen). Dies Phänomen gewinnt im Hinblick auf die Zunahme von WLANs bzw Hotspots vor allem deshalb an Bedeutung, weil nach aktuellen Untersuchungen die meisten WLANs ungesichert sind. Wer in solche Netzwerke eindringt, hat je nach Art und Intensität des Angriffs bzw auch nach (wirtschaftlicher) Beschaffenheit des Netzwerks (zB Flat Rates, dann kein unmittelbarer Schaden für den WLAN-Nutzer) mit folgenden Konsequenzen zu rechnen:

- Besitzstörungs- und Schadenersatzansprüche
- Strafbarkeit nach § 148a StGB (Betrügerischer Datenverarbeitungsmissbrauch), § 149 Abs 2 StGB (Missbrauch von Leistungsautomaten), § 119 StGB (Eingriff in das Telekommunikationsgeheimnis), § 126c StGB (Missbrauch von Computerprogrammen oder Zugangsdaten)
- Haftung, Strafbarkeit und Verwaltungsstrafe nach dem Zugangskontrollgesetz

Viren und Würmer sind Programme, die sich zwar technisch unterscheiden (zB braucht das Virus einen „Programmwirt“, während sich der Wurm allein verbreiten kann). Gemeinsam ist aber beiden Programmen, das sie Schäden anrichten können, um deren Ersatz bzw Strafbarkeit es auch jeweils geht, so dass juristisch kein Unterschied besteht. Jedenfalls (straf- und zivilrechtlich) verantwortlich ist derjenige, der den Virus/Wurm vorsätzlich in Umlauf bringt. Da dieser Täter allerdings oft nicht gefasst werden kann, ist auch an eine Verantwortlichkeit derjenigen zu denken, die – zB über e-mails erhaltene – Viren/Würmer unabsichtlich weiterleiten oder als Dienstnehmer durch Öffnen entsprechender mails für Schädigungen des Dienstnehmers sorgen. Je nach Lage des Falles ist eine solche Verantwortlichkeit denkbar, bei Dienstnehmern jedoch durch dienstrechtliche Sonderbestimmungen eingeschränkt.

Phishing bedeutet das „Ausspionieren“ und den Missbrauch der Zugangs- bzw Transaktionsdaten von Online-Banking Kunden (abgeleitet aus Password und Fishing), idR durch mails, die den Eindruck erwecken, von der Bank zu stammen und die entsprechenden Daten abzufragen, oft auch durch Umleitung auf eine gefälschte Seite, die jener der Bank entspricht. Schaden in den USA im Jahr 2003: 1,2 Milliarden USD.

Zuletzt wurden auch in Österreich zahlreiche Phishing-Attacken registriert. Der Phisher selbst macht sich strafbar, ist jedoch häufig nicht zu fassen. Je nach Lage des Falles trägt der Kunde das Risiko, wenn er von der Bank darüber informiert wurde und die Phishing-Attacke daher als solche hätte erkennen können. Die Bank haftet vor allem dann, wenn das Online-Banking System nicht dem Stand der Technik entspricht oder sie es unterlässt, Kunden vor möglichen Phishing Attacken zu warnen. Insb hat sie darauf hinzuweisen, dass sie ihren Kunden keine Zugangs- bzw Transaktionsdaten per e-mail abverlangt.

Dialer stellen (automatisch) Internet- oder Telefonverbindungen her und sind rechtlich dann problematisch, wenn die „Einwahl“ vom Nutzer unbemerkt erfolgt. 40% der von der Schlichtungsstelle der Regulierungsbehörde (RTR-GmbH) im Jahr 2004 behandelten Fälle betreffen Dialer. Der Missbrauch von Dialern ist strafbar. Das unbemerkte (nicht erkennbare) Einwählen hat der Kunde grundsätzlich nicht zu bezahlen, wobei im Einzelfall allerdings die Beweislage oft schwierig ist. Die (deutsche) Judikatur tendiert diesbezüglich (Beweislast) zugunsten des Kunden. Auch eine österreichische Verordnung (KEM-V) enthält verschiedene Schutzvorschriften zugunsten des Kunden:

- Zahlungspflicht nur dann, wenn der Dialer bei der RTR registriert ist
- Transparente Information über Kosten usw
- Automatische Trennung der Verbindung nach 30/60 Minuten (je nach Verbindungsentgelt)

Provider stehen deshalb im Blickpunkt rechtlicher Security Fragen, weil der unmittelbare Täter einer Rechtsverletzung oft nicht gefasst werden kann. Die Verantwortlichkeit der Provider ist allerdings – da sie an Rechtsverletzungen in der Regel nur infrastrukturell beteiligt sind – stark eingeschränkt:

- *Access-Provider* (vermitteln Netzzugang) sind grundsätzlich von
- jedweder Verantwortlichkeit befreit
- *Host-Provider* (speichern fremde Information, indem sie zB Speicherplatz für Websites zur Verfügung stellen) sind dann nicht verantwortlich, wenn sie keine Kenntnis von der Rechtsverletzung haben bzw die rechtswidrige Information unverzüglich sperren. Zur Sperre sind sie nach der Judikatur verpflichtet, wenn die Rechtsverletzung offenkundig ist
- *Kein Provider* ist dazu verpflichtet, von sich aus nach rechtswidrigen Information zu suchen (daher zB keine Verpflichtung zur Verwendung von Screening-Programmen), unter bestimmten Voraussetzungen bestehen aber Informationspflichten gegenüber Behörden und Privatpersonen oder Unternehmen, die durch Rechtsverletzungen beeinträchtigt werden (§ 18 E-Commerce-Gesetz).