

Sicherheit im Web

Das weltweite Datennetz ermöglicht neue Begehungsformen für Straftaten und erleichtert Delikte. Im Zusammenhang mit der Internetkriminalität treten neue Rechtsfragen auf.

Die sieben goldenen Ws der Kriminalistik gelten auch für Straftaten, die über das Internet begangen werden. Aber es gibt doch markante Unterschiede zu Ermittlungen in der realen Welt“, erläuterte Bezirksinspektor Christian Baumgartner vom Stadtpolizeikommando Klagenfurt beim 7. Österreichischen IT-Sicherheitstag am 3. November 2010 in Graz.

Täter, Opfer, Zeugen („Wer?“) können sich hinter Nicknamen, IP- und E-Mail-Adressen verbergen. Die rechtliche Beurteilung dessen, was begangen wurde, kann von Land zu Land verschieden sein, was für die Möglichkeiten zur Strafverfolgung von Bedeutung ist. Welche Tatzeit („Wann?“) kommt in Frage (Ortszeit, GMT, Serverzeit)? Wo die Tathandlung gesetzt wurde, kann bei der weltweiten Vernetzung ebenfalls zweifelhaft sein, genauso das „Wie?“ des Tathergangs, wenn Logfiles nicht mehr vorhanden sein sollten oder Daten gelöscht wurden. Das Tatbehebungsmittel, womit etwas passiert ist, kann Schadsoftware sein, aber auch durch Social Engineering können Informationen abgefließen sein. Am ehesten lässt sich noch vermuten, warum etwas passiert ist – es ergibt sich aus der Art des Delikts.

Wenn man aus der Vielfalt der möglichen Delikte den Internetbetrug herausgreift, stößt man auf verschiedenste Begehungsarten. Betrügereien kommen vor beim Online-Shopping, bei Internet-Auktionen, beim Fahrzeugkauf im Internet, oder bei der Partnersuche: Für den in Aussicht gestellten Besuch ist Geld für Flugkarten zu überweisen, des Weiteren für plötzlich erkrankte Angehörige, die zu versorgen sind – dem Einfallsreichtum sind keine Grenzen gesetzt. Mit widerrechtlich erlangten Daten von Kreditkarten werden Einkäufe getätigt oder es tritt der Täter im Internet überhaupt mit gestohlener Identität auf. Oder man erfährt, völlig unerwartet angeblich eine reiche Erbschaft gemacht zu haben – zu deren Abwicklung allerdings Spesen verschiedenster Art anfallen.

Das Internet macht die Begehung mancher Delikte wesentlich einfacher.



Wolfgang Feiel: „EU-Telekompaket regelt die Sperre des Internet-Anschlusses.“



Peter Mader: „Vor Domain-Anmeldung abklären, ob Rechte Dritter verletzt werden.“



Sonja Janisch: „Kunde hat bei Einkauf im Web ein befristetes Rücktrittsrecht.“



Christian Baumgartner: „Im Netz keine persönlichen Daten bekannt geben.“

Es muss kein Tatort ausgekundschaftet, kein Fluchtfahrzeug besorgt, kein Alarm und keine unmittelbare physische Verfolgung befürchtet werden. Alles, was ein Täter im Internet braucht, ist eine Online-Verbindung zum Opfer und die Möglichkeit, zu den erschlichenen Vermögenswerten zu gelangen.

„Geben Sie nach Möglichkeit im Internet keine persönlichen Daten bekannt“, rät Baumgartner. Einkaufen sollte man nur auf Internetseiten, die als seriös einzustufen sind. Wenn eine Anfrage über „whois“ ergibt, dass die Seite erst seit Kurzem besteht, ist Vorsicht geboten. Beim Fahrzeugkauf nicht bloß auf Bilder vertrauen, sondern das Fahrzeug in Augenschein nehmen. Geld nicht im Vorhinein überweisen. Bei Online-Auktionen sollte auf den Anbieter geachtet werden, wie er bewertet wird und welche Zahlungsvarianten er anbietet. Auf Spam nicht antworten und keine Anhänge öffnen – sie

könnten Viren oder Trojaner enthalten. „Sie haben mit hoher Wahrscheinlichkeit keine Erbschaft in Nigeria gemacht!“, sagte Baumgartner.

Elektronische Unterschrift. Beim Abschluss von Mobilfunk- oder Versicherungsverträgen, bei Bezahlvorgängen, kommt es immer häufiger vor, dass die Unterschrift unter den lediglich am Bildschirm einsehbaren Vertragstext elektronisch auf einem Signatortablet zu leisten ist, das mit dem PC oder Laptop verbunden ist. Die Unterschrift erscheint im Dokument am Bildschirm und man erhält in der Folge entweder einen Ausdruck des Dokuments oder es wird per E-Mail zugesendet.

Der Umstand, dass die Unterschrift elektronisch gespeichert ist, wirft die Frage auf, ob sie nicht auch missbräuchlich auf andere Dokumente kopiert werden kann.

„Nein, so ist das nicht“, sagt Gerald Cäsar, Geschäftsführer der Firma „xyzmo“ (www.xyzmo.com). „Die elektronische Unterschrift ist mehr als nur ein Foto der Unterschrift“.

Erfasst werden nämlich bei dem vorgestellten System nicht nur der Schriftzug, sondern auch der beim Schreiben auf die Unterlage ausgeübte Druck, der Winkel, unter dem der Schreibstift gehalten wird, die Beschleunigung. Durch die Erfassung der Geschwindigkeit beim Schreibvorgang scheidet ein bloß bedächtiges Nachzeichnen des Schriftbildes als Fälschungsmethode von vornherein aus. Ferner werden nicht nur ein fotografisches Abbild der Unterschrift verwendet, sondern zusätzlich die erwähnten Daten. Überdies werden alle diese Daten mit einem vom Anwender gewählten Schlüssel verschlüsselt. Die Unterschrift liegt zu keinem Zeitpunkt in ihrem Rohformat vor.

Dazu kommt, dass das Unterschriftsbild samt den Unterschriftsdaten mit dem gesamten Inhalt des Dokuments und seinen Anhängen gleichsam in ein Paket (PDF-File) verpackt wird. Über alles wird – wie eine „Verschnürung“ – eine eindeutige, aus dem

gesamten Inhalt abgeleitete Prüfsumme („Hashwert“) gelegt. Bei einer Signaturprüfung wird eine Veränderung erkannt, gleichgültig, ob sie im Dokument, in den Anhängen oder in den eingebetteten Daten erfolgt. Wie bei nachträglichen Veränderungen in einem Papierdokument ist das zwar kein Schutz vor einer Veränderung. Anders als bei einem Papierdokument, an dem Überschreibungen, Radierungen, Löschungen mitunter erst durch kriminaltechnische Untersuchungen erkannt werden können, zeigt ein anderer Hashwert eine Veränderung an, sodass in einem solchen Fall nicht von einem Original ausgegangen werden kann.

Bei einer hinterlegten Unterschriftprobe ist zu bedenken, dass sich eine Unterschrift – als biometrisches Merkmal – im Laufe der Zeit verändern kann. Körper- und Handhaltung, die Art des Tablets sind von Einfluss; dazu kommen Faktoren wie Zeitdruck oder Nervosität. Eine zum Vergleich vorgelegte, gleiche Unterschrift wäre ein Fälschungsmerkmal. Es wird daher im Server eine Serie von typischerweise sechs Musterunterschriften abgelegt. Mit diesen gespeicherten Vergleichswerten wird eine später elektronisch abgegebene Unterschrift an Hand eingestellter Toleranzfaktoren auf Echtheit überprüft.

Judikatur. Ass.-Prof. Dr. Sonja Janisch (Universität Salzburg) erläuterte in letzter Zeit ergangene Gerichtsentscheidungen zum IT-Recht, darunter das schon mehrmals (u. a. ÖSI 1-2/11, S. 87) erörterte Urteil des OGH vom 14.7.2009, 4 Ob 41/09x, nach welchem bei Urheberrechtsverletzungen keine Auskunftspflicht eines Access-Providers über den hinter einer (dynamischen) IP-Adresse stehenden Anschlussinhaber besteht. § 87b Abs. 3 UrhG ist daher nach derzeitiger Rechtslage ohne praktische Wirksamkeit. Allerdings könnte sich die Rechtslage mit Inkrafttreten der TKG-Novelle zur Vorratsdatenspeicherung ändern.

Zwei Urteile des OGH (2 Ob 107/08m vom 19.2.2009 und, inhaltlich ähnlich, 9 Ob 3/08v vom 24.2.2009) sind zu Phishing-Fällen ergangen. In beiden Fällen wurde ein Bankkunde Opfer einer Phishing-Attacke. Das Geld wurde im Fall 2 Ob 107/08m auf das Konto einer zuvor per E-Mail angeworbenen Bankkundin („Distanzmitarbeiterin“ eines englischen Unterneh-



Tatort Internet: Für einen Internetbetrug genügt dem Täter eine Online-Verbindung zum Opfer und ein geringer Aufwand.

mens) überwiesen, die es vereinbarungsgemäß von ihrem Bankkonto unter Einbehaltung einer Provision in Form einer Barüberweisung an eine Bank in Lettland weiterleitete. Die Kernaussagen der beiden Urteile sind, dass die Zahlung dem scheinbar Überweisenden, also dem Opfer, nicht angelastet werden kann und dass die Gutschrift mangels eines wirksamen Überweisungsauftrags selbst einem gutgläubigen Empfänger gegenüber unwirksam ist. Die Bank hat gegen den Empfänger der Leistung (der angeworbenen Bankkundin) ein Stornierungsrecht und – wenn wie im vorliegenden Fall über den überwiesenen Betrag bereits verfügt wurde – einen Bereicherungsanspruch. Nicht auseinanderzusetzen brauchte sich in beiden Fällen der OGH mit der Frage eines Verschuldens des Opfers, was allenfalls zu einer anderen Beurteilung führen hätte können.

Nach § 5e Konsumentenschutzgesetz (KSchG) hat ein Verbraucher bei Vertragsabschlüssen im Internet (Fernabsatz) ein innerhalb von sieben Werktagen auszuübendes Rücktrittsrecht. Folge eines solchen Rücktritts ist die Auflösung des Vertrags. Nach § 5g Abs. 1 Z 2 KSchG hat der Verbraucher die empfangenen Leistungen zurückzustellen und dem Unternehmer ein angemessenes Benützungsentgelt und eine Entschädigung für Wertminderung zu leisten.

Eine bloße Begutachtung der Sache und ein bloßes Ausprobieren rechtfertigen noch keinen Anspruch. Eine AGB-Klausel, die eine pauschale Bearbei-

tungsgebühr für den Fall eines Rücktritts vorsieht, ist unzulässig (OGH vom 18.6.2009, 8 Ob 25/09y). Der Anspruch besteht nur bei extensiver Benutzung (OGH vom 27.9.2005, 1 Ob 110/05s. Ein Monitor war 43 Stunden betrieben worden).

Rücksendungskosten muss der Verbraucher nur dann bezahlen, wenn dies vereinbart wurde (§ 5g Abs. 2 KSchG). Die Frage, wer die Hinsendekosten der Ware zum Verbraucher trägt, wurde vom EuGH mit Urteil vom 15.4.2010, C-511/08 (Heine/VZ Nordrhein-Westfalen e.V.) dahingehend entschieden, dass eine Überwälzung der Hinsendekosten auf den Verbraucher unzulässig ist, auch die Festsetzung eines pauschalierten Versandkostenanteils, den der Konsument in jedem Fall zu tragen hätte. Das Urteil ist zwar nur für die Parteien des betreffenden Verfahrens verbindlich, hat aber Auswirkungen auf österreichische Fälle, da die Gerichte im Sinne einer richtlinienkonformen Auslegung grundsätzlich zum gleichen Ergebnis kommen sollten.

Der Begriff der Direktwerbung als unerbetene elektronische Post (§ 107 Abs. 2 Z 1 TKG) ist weit gefasst zu verstehen. Im Urteil des OGH vom 30.9.2009, 7 Ob 168/09w, wurde der Unterlassungsklage eines Rechtsanwalts stattgegeben: Ein Sachverständiger hatte ihn und andere Rechtsanwälte per E-Mail über seine Eintragung in die Liste gerichtlich beeideter Sachverständiger in Kenntnis gesetzt. Dem Urteil lässt sich entnehmen, dass eine Gestaltung einer E-Mail als Newsletter oder

RECHTSANWALT
DR. WOLF-GEORG SCHÄRF

1010 WIEN, TIEFER GRABEN 21/3
TELEFON: +43 (0) 1/533 39 51
FAX: +43 (0) 1/533 39 51-50
E-MAIL: office@lawschaerf.at



Strandgasthaus Birner
21., An der oberen Alten Donau 47
Tel. 01/271 53 36

Eines der besten Gasthäuser mit schattigem Garten an der Alten Donau mit Blick auf das Angelbad. Altwiener Küche, div. Familien- und Firmenfeste, Weihnachtsfeiern und Kabarets

office@gasthausbirner.at
www.gasthausbirner.at

Sommer: kein Ruhetag (9–23 Uhr warme Küche)
Winter: kein Ruhetag (9–22 Uhr warme Küche)

SANTRANS KRANKENBEFÖRDERUNG
die patientenzentrierte Krankenbeförderung
TRANSPORTANMELDUNG unter
01/ 958 11 11

SITZEND - und LIEGENDTRANSPORTE
für Patienten der BVA, KFA, SVA, VAE, WVB, SVB, PVAng, AUVA
BEFÖRDERUNG zu KUR - und REHABILITATIONSZENTREN

teicht jöch1
RECHTSANWÄLTE

Dr. Gerhard Jöch1
Rechtsanwalt
Rathausstraße 19/DG/53
1010 Wien
Tel: + 43 1 405 92 20
Fax: + 43 1 408 51 94
E-Mail: tj@ra-joechl.at

PRINTSHOP
Sabrina Neumann

iPrinter.at
Ihr Partner für Druck und Design

1210 Wien, Ignaz-Köck-Straße 1/25, Tel.: 01/278 81 75, Mail: scn@printshop.at
Shopping Center Nord

Info-Mail die Qualifikation als Direktwerbung nicht hindert und dass eine Zustimmung zum Empfang nicht aus der Angabe einer Mailadresse beispielsweise auf einer Website abgeleitet werden kann.

Domainrecht. Univ.-Prof. Dr. Peter Mader (Universität Salzburg) behandelte Rechtsprobleme, die sich im Domainrecht ergeben. Domains – Adressen, an denen jemand im Internet erreicht werden kann – müssen weltweit einzigartig sein und können nur einmal vergeben und benützt werden. In der Regel wird, als Second-Level-Domain, die links neben Endungen wie .at, .com, .org (Top-Level-Domain) steht, eine Bezeichnung, ein Name oder ein Unternehmenskennzeichen verwendet. Die Vergabe erfolgt durch private Institutionen (für Österreich nic.at in Salzburg), die aber ohne rechtliche Prüfung die Zuweisungen nach dem Prinzip des „first come, first served“ durchführen.

Rechtsstreitigkeiten können sich daraus ergeben, dass Domains reserviert werden, um einen geschäftlichen Konkurrenten daran zu hindern, seinen eigenen Namen im Internet zu verwenden (Domain-Grabbing) und/oder ihn dazu zu bringen, die bereits reservierte Domain abzukaufen. Auch außerhalb dieser Fälle kann durch eine Domainverwendung in bestehende Namens-, Kennzeichen- oder Urheberrechte eingegriffen werden, auch in Wettbewerbsrecht, Markenrecht und Firmenrecht (§§ 37 UGB schützt den im Firmenbuch eingetragenen Unternehmensnamen die Firma vor unbefugtem Gebrauch durch andere Personen). Weiters kann eine missbräuchliche Verwendung darin bestehen, einen Namensträger zu kritisieren oder zu beleidigen.

„Domainprozesse können sehr teuer werden“, sagte Mader, weshalb beispielsweise die für die Zulassung von Registrierungsstellen und Adressen (.org, .eu usw.) zuständige ICANN (www.icann.org) ein außergerichtliches Streitbeilegungsverfahren zur Verfügung stellt. Die für Rechtsverletzungen im Zusammenhang mit Domains in Betracht kommenden Gesetze sehen Unterlassungsansprüche vor. Bei Verschulden besteht Anspruch auf Schadenersatz. Es empfiehlt sich daher, vor Anmeldung einer Domain abzuklären, ob durch diese Rechte Dritter verletzt werden können.

EU-Recht. Dr. Wolfgang Feiel (Rundfunk und Telekom Regulierungs-GmbH) referierte über das am 25. November 2009 beschlossene neue EU-Telekompaket, bestehend aus der Richtlinie „Bessere Rechtsetzung“ 2009/140EG mit Änderungen der Rahmen-, Zugangs- und Genehmigungs-RL, der Richtlinie „Rechte der Bürger“ 2009/136/EG sowie der Verordnung 1211/2009 zur Einrichtung des Gremiums Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) und des Büros. Verbraucherrechte werden verbessert (Beschleunigung der Rufnummernportierung auf einen Tag; Verkürzung der Mindestlaufzeit von Verträgen; aber auch Zulässigkeit der Sperre des Internetzugangs mit richterlicher Genehmigung). Die nationale Umsetzung der Richtlinien muss bis 25. Mai 2011 durchgeführt sein; das wird in Österreich wahrscheinlich durch eine Novellierung des TKG erfolgen.

Weitere Vorträge betrafen Fragen der Sicherheit von Websites; Security Management; die Tätigkeit einer „schnellen Eingreiftruppe“ (Virus Emergency Response Team – VERT) bei durch Malware bedingten Systemausfällen; den Umgang mit solchen Vorfällen sowie die digitale Beweissicherung im Unternehmenskontext.

Kurt Hickisch

SYSSEC

IT-Sicherheitstag

Der 7. Österreichische IT-Sicherheitstag wurde unter der Leitung von Ass.-Prof. Dr. Peter Schartner (Forschungsgruppe Systemsicherheit, Universität Klagenfurt) am 3. November 2010 im Europasaal der Wirtschaftskammer Steiermark in Graz abgehalten. Veranstalter waren das Institut für Angewandte Informatik – Forschungsgruppe Systemsicherheit der Universität Klagenfurt und die Fachgruppe UBIT der Wirtschaftskammer Steiermark.

Der 8. Österreichische IT-Sicherheitstag wird von Prof. Dr. Patrick Horster und Dr. Peter Schartner organisiert und findet am 6. Oktober 2011 im Rahmen des Veranstaltungsprogramms der *IT Carinthia* in Klagenfurt statt.

<http://www.syssec.at/sitag2011>

PORSCHE WR. NEUSTADT
Alles unter einem Dach...
 Neu, Gebraucht, Service, Reparatur, Karosseriezentrum



...mit Sicherheit in besten Händen

2700 Wr. Neustadt, Neunkirchner Straße 90
Tel.: 02622 / 23 5 91-0, Fax: 02622 / 23 5 91-40

DI. RICHARD ANZBÖCK

STAATLICH BEFUGTER UND BEEIDETER ZIVILINGENIEUR FÜR SCHIFFSTECHNIK
 ALLGEMEIN BEEIDETER UND GERICHTLICH ZERTIFIZIERTER SACHVERSTÄNDIGER
 FÜR WASSERFAHRZEUGE UND SCHIFFBAU

1190 WIEN, GUGITZGASSE 8/29

TEL.: 01/320 88 93

MESSBRIEFE

TECHNISCHE BERATUNG

KINO
 TULLN
 Langenlebarner Strasse 9
 Ticket-line **02272/64591**
www.kino-tulln.at

**Wir machen Kino
 zum Erlebnis für
 Gross und Klein.**

**Apotheke
 „Zur Spinnerin
 am Kreuz“**
 Mag. pharm.
 Mag. iur. Albert Ullmer KG
 1100 Wien
 Wienerbergstraße 6
 Tel.: 01/604 33 45
www.apotheke-spinnerin.at

**Wir beraten Sie gerne in allen
 Fragen der Gesundheit!**

Wir stehen Ihnen zur Verfügung:
 Mo. bis Fr.: 8 -18 Uhr, Sa.: 8 -12 Uhr
 Bereitschaftsdienst nach Dienstkalender



BERTMANN Ges.m.b.H.
 Feinmechanische Erzeugnisse - Medizintechnik - Implantate



A-1230, Sulzengasse 3
 Telefon +43 1 / 688 46 11 - 13
 Fax +43 1 / 688 46 13 20
office@bertmann.at