

# IT und Recht

Über Aktuelles aus Informationstechnik und Recht referierten Experten beim 6. Österreichischen IT-Sicherheitstag am 4. November 2009 an der Alpen-Adria Universität in Klagenfurt.

**S**ocial Engineering, die Methode, Menschen Informationen zu entlocken, ist nach wie vor ein Thema: Gerald Kortschak, Mitglied der *IT-Security Experts Group WKÖ* ([www.its-securityexperts.at](http://www.its-securityexperts.at)), fasste die Methoden zusammen: *Dumpster Diving* – das Durchstöbern von Müll. *Tailgating* – einer autorisierten Person in ein Gebäude nachfolgen. *Shoulder Surfing* – über die Schulter eines anderen dessen Bildschirminhalt mitlesen.

*Google Hacking* – über *Google* Informationen über ein Zielobjekt erlangen bzw. Schadcode über *Google* ausführen. *Vehicle Surveillance* – Ausspähen von Informationen, die sich an und in Fahrzeugen befinden (Ausweise, Parkberechtigungen). *Badge Surveillance* – Ausweiskarten ausspionieren, manipulieren oder stehlen.

„Im Grunde genommen läuft Social Engineering im persönlichen Kontakt auf das hinaus, was ein guter Verkäufer an Einfühlungsvermögen haben muss“, betonte Kortschak, der das Ergebnis einer Ende 2008 durchgeführten Umfrage unter österreichischen KMUs präsentierte, ob diese Unternehmen bereits einmal Opfer eines IT-Sicherheitsproblems wie Computer-Virus, Mitarbeiter, Hacker usw. wurden. 36 Prozent waren betroffen, davon ein Fünftel mit einem 5.000 Euro übersteigenden Schaden.

Auffällig war, dass die Schadensfälle weitgehend unabhängig davon waren, ob Sicherheitsregeln bestanden haben oder nicht. Das lässt den Schluss zu, dass die getroffenen Abwehr-



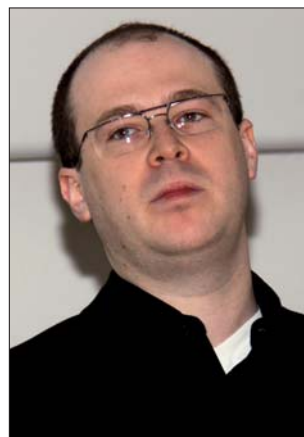
Alpen-Adria Universität Klagenfurt: Tagungsort des 6. Österreichischen IT-Sicherheitstags.



Andreas Kersche: „Internet hat für Kriminelle neue Möglichkeiten geschaffen.“

maßnahmen an der Realität vorbeigehen und nicht gelebt werden.

Der Umsatz der Schattenwirtschaft im Internet wird auf 150 Milliarden Dollar geschätzt, und ist ein gut organisierter Schwarzmarkt, berichteten Siegfried Schauer und Georg Kremser von *Ikarus Security Software GmbH* ([www.ikarus.at](http://www.ikarus.at)). Die Online-Kriminalität bewegt ähnlich viel Geld wie der weltweite Drogenhandel. Das *Russian Business Network* stellt Know-how, Experten, Kontakte und juristischen Beistand zur Verfügung. Bisher un-



Gerald Kortschak: „Menschen Informationen zu entlocken, bleibt ein Thema.“

bekannte Sicherheitslücken in Betriebssystemen oder Applikationen werden auf Plattformen ab 50.000 US-Dollar verkauft; *Zero-Day-Exploits* können ersteigert werden.

„Das Internet hat die Art und Weise der Delikte nicht geändert, sondern lediglich neue Möglichkeiten geschaffen“, führte Andreas Kersche aus. Bereicherung durch Betrug, Rufschädigung, Betriebsspionage und Vandalismus (Stören von Diensten) sind bevorzugte Ziele, wie auch die Verbreitung von Ideologien. Durch den Umstand, dass die Täter

von jedem beliebigen Ort aus meist anonym vorgehen können, fällt es leichter, die Hemmschwelle zu einem Delikt zu überwinden.

**Passwörter** sollten Buchstaben in Groß- und Kleinschreibung, Sonderzeichen und Zahlen enthalten und mindestens acht Zeichen umfassen. Nur – wer merkt sich schon solche Zeichenfolgen. Sie werden manchmal auf einem Zettel unter die Tastatur geklebt. Zwei Methoden, ein komplexes Passwort, das man sich trotzdem merken kann, zu generieren, hat Martin Krumböck von *Hackattack* („We hack to protect you“) vorgestellt. Nach der Satzmethode nimmt man die Anfangsbuchstaben der Wörter in deren Groß- und Kleinschreibung von einem Satz, den man leicht im Gedächtnis behält. Bei der Substitutionsmethode werden bestimmte Zeichen durch andere ersetzt. Aus Passwort wird dann beispielsweise *P4\$\$w0rt*. Angriffe auf Passwörter werden entweder mit Wörterbüchern durchgeführt (*Dictionary Attack*), mit Durchprobieren von Zeichenkombinationen (*Bruteforce Attack*) oder unter Ausnutzung von Schwachstellen der kryptografischen Verschlüsselung, unter denen sie abgelegt sind.

**Jüngste Judikate** des OGH zum IT-Recht hat Ass.-Prof. Dr. Sonja Janisch, LL.M von der Universität Salzburg erläutert.

In der Entscheidung vom 29.11.2007, Zl. 2 Ob 108/07g, hat der OGH zur Frage der Beweisbarkeit des



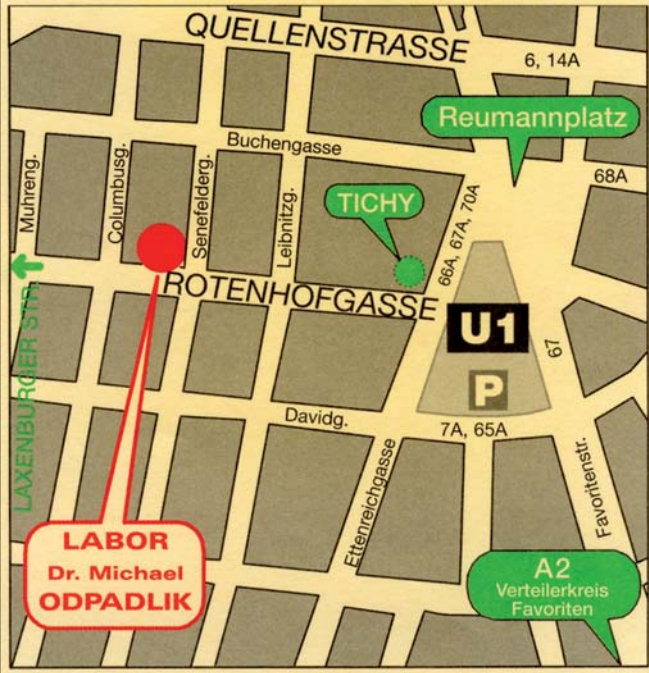
Medizinische Laboratorien Wonnert & Partner

## Labor Dr. Michael Opadlik

Facharzt für med. und chem. Labordiagnostik

A-1100 Wien, Rotenhofgasse 14

Montag bis Donnerstag 7.00 – 18.00, Freitag 7.00 – 16.00 Uhr  
Tel: +43-1-604-91-19 · Fax +43-1-604-91-19 – 31  
ALLE KASSEN · Email: labor@labor-odpadlik.at  
Zu erreichen mit: U1, 6, 67, 7A, 14A, 65A, 66A, 67A, 68A, 70A



## DR. HANS HOUSKA

Rechtsanwalt

1010 Wien  
Bartensteingasse 16  
Tel. 01 / 405 83 03  
Fax 01 / 405 83 03-72

## IT-SICHERHEIT

Zugangs einer E-Mail Stellung genommen und ausgeführt, dass aus dem Umstand, dass eine E-Mail – anhand des Sendeprotokolls beweisbar – abgesendet wurde, noch nicht mit der sonst für einen Anscheinsbeweis erforderlichen typischen Verknüpfung geschlossen werden könne, dass die Mail dem Empfänger auch zugegangen ist.

Beispielsweise könnte die Mail etwa wegen Übermittlungsfehlern nicht in die Mailbox des Empfängers gelangt sein; genauso, wie ein abgesendeter Brief nicht zwangsläufig in den Briefkasten des Empfängers gelangen muss. Will der Absender daher sicher sein, dass die Nachricht den Empfänger erreicht hat, empfiehlt es sich, eine Bestätigung des Zugangs zu verlangen.

Nach § 5 Abs. 1 Z 3 ECG hat ein Diensteanbieter im Internet den Nutzern Angaben zur Verfügung zu stellen, auf Grund derer diese mit ihm rasch und unmittelbar in Verbindung treten können, einschließlich seiner elektronischen Postadresse. Die Frage, ob auch die Telefonnummer im Webauftreten zwingend anzugeben ist, hat der Europäische Gerichtshof auf Grund eines Vorabentscheidungsersuchens des deutschen BGH verneint und es als ebenso rechtskonform bezeichnet, wenn eine Webanfrage etwa über eine Anfragemaske ermöglicht wird, die innerhalb kurzer Zeit beantwortet wird. Auf Anfrage muss nach elektronischer Kontaktaufnahme auch ein nicht elektronischer Kommunikationsweg eröffnet werden. Die Postadresse allein anzugeben, ist nicht ausreichend (EuGH C-298/07).

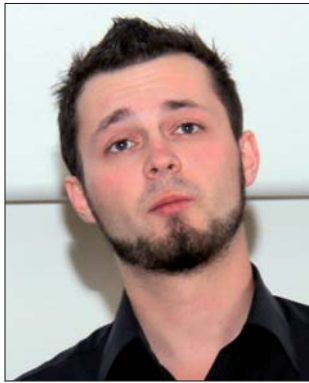
In einem vom Sachverhalt her umgekehrten Fall hat ein Werbeschreiben für einen Abo-Vertrag nur eine

Telefonnummer und eine Internet-Adresse enthalten. Die Antwortsendung war an eine Postfachadresse gerichtet. Die Postadresse konnte über die Internet-Adresse ermittelt werden.

Nach § 5c Abs. 1 Z 1 KSchG muss der Verbraucher rechtzeitig vor Abgabe seiner Vertragserklärung über Informationen über Name (Firma) und ladungsfähige Anschrift des Unternehmers verfügen. Wie der OGH im Urteil vom 8.7.2008, Zl. 4 Ob 57/08y, festgestellt hat, muss eine ladungsfähige Adresse bereits in der Papierwerbung enthalten sein. Ein Hinweis auf eine solche Adresse auf der Website ist unzulässig. Die Information muss auf dem gleichen Medium enthalten sein, sonst würde ein „Medienbruch“ vorliegen.

Wenn auf einer Website eine Leistung groß als gratis beworben wird, sich hingegen aus dem Kleingedruckten Entgeltlichkeit ergeben hat (die gratis erstellte Lebenserwartungsprognose war nur dann kostenlos, wenn innerhalb von 14 Tagen gekündigt wurde), ist die Gestaltung des Angebots wettbewerbswidrig und verstößt gegen die Preisangabepflicht des § 5c Abs. 1 Z 3 KSchG. Ein Verbraucher, der durch die Betonung der Unentgeltlichkeit in Irrtum geführt wird, muss nicht mehr nach Hinweisen auf allfällige Kosten suchen (OGH 20.5.2008, 4 Ob 18/08p).

Nach § 5d Abs. 2 KSchG sind dem Verbraucher rechtzeitig schriftlich oder auf einem für ihn verfügbaren dauerhaften Datenträger Informationen über die Bedingungen und Einzelheiten der Ausübung des Rücktrittsrechtes zu übermitteln. Ein Kunde hat nach der Anmeldung zu einem Dienst lediglich eine E-Mail mit einem Link auf die AGB er-



**Martin Krumböck: „Passwörter sollten Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen enthalten.“**

halten, die Informationen über das Rücktrittsrecht enthalten haben. Eine E-Mail ist zwar als dauerhafter Datenträger anzusehen, ist aber bei einem Link auf die AGB – wenn überhaupt – nur dann ausreichend, wenn die E-Mail einen konkreten Hinweis auf die Informationen enthält, die unter dem Link abrufbar sind, insbesondere das Rücktrittsrecht. Das Problem, dass bei einem Abruf der Bedingungen über die Ausübung des Rücktrittsrechtes über E-Mail der Verbraucher selbst den dauerhaften Datenträger zur Verfügung stellen müsste, wurde im vorliegenden Fall (OGH 4 Ob 18/08p) nicht mehr erörtert.

Rücktritt vom Vertrag und Kündigung eines Vertrages haben unterschiedliche Rechtswirkungen: Ein Rücktritt führt zu einer Rückabwicklung des Vertrags; erbrachte Leistungen müssen rückerstattet werden. Bei der Kündigung brauchen demgegenüber nur künftige Leistungen nicht erbracht werden. Wenn daher bei einem Abo-Vertrag dem Verbraucher zwar ein weitgehendes Kündigungsrecht eingeräumt wurde, hingegen eine Belehrung über das Rücktrittsrecht fehlte, liegt ein Verstoß gegen die Informationspflicht nach § 5c KSchG vor (OGH 4 Ob 57/08y).

In einem Fall wurden an Kindern vor Volksschulen Werbeprospekte verteilt, mit denen für den Beitritt zu einem Pony-Club geworben und monatliche Abenteuer versprochen wurden. Der OGH hat (OGH 4 Ob 57/08y) an Kinder gerichtete Werbung zwar nicht als absolut unzulässig bezeichnet, doch aus wettbewerbsrechtlichen Gründen (§ 1a iVm Z 28 des Anhangs zum UWG) ist es verboten, Kinder direkt zum Kauf oder zur Überredung der Eltern zum Kauf aufzufordern. Unzulässig ist Werbung, wenn Preise nur unvollständig angegeben werden, und wenn ein Gewinnspiel ohne den Hinweis angeboten wird, dass ein Vertrag nicht abgeschlossen zu werden braucht. Werbung per E-Mail oder SMS, die ohne vorherige Einwilligung des Empfängers versendet wird, kann teuer kommen. Die Strafen haben laut Janisch im Einzelfall schon Beträge von 20.000 Euro erreicht, bei einer gesetzlichen Obergrenze von 37.000 Euro (§ 107 Abs. 2 iVm § 109 Abs. 3 Z 20 TKG).

Weitere Vorträge des vom Institut für Angewandte Informatik – *Systemsic* (*syssec*; [www.syssec.at](http://www.syssec.at)) der Universität Klagenfurt nunmehr bereits zum sechsten Mal veranstalteten IT-Sicherheitstages betrafen den aktuellen Informationsbedarf österreichischer Unternehmen zur IT-Sicherheit; System-Management im Umfeld der IT-Security; bevorstehende Änderungen des europäischen Rechtsrahmens für elektronische Kommunikation; Zertifikatsprüfungen; Laufwerksverschlüsselungen; Back-up-Strategien und den sicheren Umgang mit Dokumenten. Der nächste IT-Sicherheitstag wird im November 2010 stattfinden.

*Kurt Hickisch*

**Sicherheit(s)-Technik**

Sicherheitstüren bieten zuverlässigen Schutz vor:  
Einbruch, Lärmbelästigung, Geruchsbelästigung und Zugluft

Geprüft nach ÖNORM B 5338 ■  
schnelle, saubere Montage ■  
Topqualität aus Österreich ■

**Gratis Hotline: 0800/50 10 75**

**BÖHM-MITSCH security systems** Intelligent sichern ■  
1070 Wien, Lindengasse 58 / Ecke Zieglergasse

**Produkte für den Sicherheitsbereich**

Alarmanlagen    Videoüberwachung

Beratung • Planung • Verkauf • Montage • Service

Ing. **Witke** Ges.m.b.H

**01 / 769 83 50**

1110 Wien • Simmeringer Hauptstraße 257  
[office@witke.com](mailto:office@witke.com) • [www.witke.com](http://www.witke.com)

**WISAG** Sicherheitsdienste

Ein Dienstleistungsunternehmen mit langjähriger nationaler und internationaler Erfahrung.

Dienstleistungen im Bereich:

- Sicherheitsanalyse- und Beratung
- Objekt- und Werkschutz
- Empfangs- und Portierdienst
- Revier- und Streifendienst
- Veranstaltungssicherheit

**WISAG Sicherheitsdienste GmbH & Co KG**  
A-1030 Wien, Landstraßer Hauptstraße 99/3A  
Tel.: +43 (1) 713 69 20-35  
[www.wisag.at](http://www.wisag.at)