

Sicherheit, Datenschutz und Recht

Die Förderung der IT-Sicherheit bei kleinen und mittleren Unternehmen (KMU) war einer der Schwerpunkte beim 2. Österreichischen IT-Sicherheitstag am 9. November 2005 in Graz.

Rund 250 Unternehmen unterzogen sich von April bis Juli 2005 in 21 Städten einem kostenlosen IT-Sicherheitscheck im Rahmen der Roadshow „Telefit 05“ der Wirtschaftskammer Österreichs. Demnach ist schon bei der physischen Sicherheit einiges nachzuholen, etwa bei der Unterbringung der Rechner und der Datenarchive. Bei 7 Prozent der Firmen waren Türen der Datenräume ungesichert, die Fenster zu 24, Fluchtwege zu 33 und Luken zu 50 Prozent. „Eine Kassa würde man ja auch nicht ungesichert herumstehen lassen“, sagte Ing. Martin Prager, Sprecher der „Experts Group IT-Security“, beim 2. Österreichischen IT-Sicherheitstag in der Wirtschaftskammer Steiermark in Graz. „Wenn die Computer weggetragen werden können, hilft der beste programmtechnische Schutz nichts.“

Zur physischen Sicherheit gehöre die Entsorgung von Papier und Datenträgern, erläuterte Prager. „Jeder Rechtsanwalt hat einen Schredder, aber wie sieht es etwa bei Ärzten aus?“

Liegen ausreichende Anweisungen für die Mitarbeiter über den Umgang personenbezogenen oder sensiblen Daten vor? Ist geregelt, wer die Software installiert, sie updatet und wer Daten sichert und archiviert? Wurden Regelungen über die Nutzung des Internets getroffen, wurden die Mitarbeiter auf die aus der Nutzung möglichen Gefahren hingewiesen?

Antworten auf diese Fragen gab die Wirtschaftskammer im Oktober 2005 mit der Aktion it-safe.at (<http://it-safe.at>), unterstützt vom Wirtschaftsministerium und A-SIT, dem Zentrum für Sichere Informationstechnologie Austria. Im Rahmen der Aktion wurde das IT-Sicherheits-



Sonja Janisch warnt vor leichtfertigem Umgang mit dem Urheberrecht im WWW.

handbuch herausgegeben. KR Hans-Jürgen Pollirer, Obmann der Bundessparte *Information und Consulting (BSIC)*, stellte dieses Handbuch beim Sicherheitstag vor. Das Werk baut auf dem Grundschutzhandbuch auf und soll Entscheidungsträgern grundlegende Kenntnisse und Verständnis vermitteln, so dass sie in die Lage versetzt werden, Probleme zu erkennen und deren Lösung mit Hilfe von Fachleuten in Angriff zu nehmen.

It-safe.at bietet eine weitergehende Online-Version des Handbuchs an, die dem Sicherheitsbedarf eines Klein- oder Mittelunternehmens individuell angepasst werden kann. Anhand eines Online-Fragebogens wird festgestellt, welcher Sicherheitsbedarf erforderlich ist,



Univ.-Prof. Patrick Horster organisierte den IT-Sicherheitstag in Österreich.

wobei dann nur mehr die Teile des Handbuchs angezeigt werden, die für diesen Sicherheitsbedarf in Frage kommen. Nicht Erforderliches wird ausgeblendet, der Zeitaufwand beim Durcharbeiten verkürzt sich. Zudem kann zwischen einer Entscheider- und einer Administrator-Version gewählt werden, wobei diese mehr auf technische Belange zugeschnitten ist. Ein Unternehmen, das sich beraten lässt, erhält sechs Beratungsstunden zur Verfügung gestellt. 75 Prozent der Kosten werden von der Kammerorganisation getragen, die restlichen, vom Unternehmen zu zahlenden Kosten bewegen sich um 100 Euro. Allein die dem Unternehmen im Zuge der Beratung zur Verfügung gestellte Software hat einen Wert von etwa 300 Euro.

Die Wirtschaftskammer Steiermark hat zudem, aufbauend auf dem Modell des E-Business Managers, das Berufsbild des „IT-Security Consultants“ geschaffen. Wer als IT-Dienstleister einen hohen Standard voraussetzenden Test besteht, erhält ein Zertifikat, darf ein entsprechendes Logo verwenden und wird in den Pool der IT-Sicherheitsberater aufgenommen, aus dem Firmen Berater aussuchen können (<http://stmk.itsecurity.co.at>).

Bürgerkarte. Bei der Bürgerkarte handelt sich nicht, wie der Name vermuten lässt, um eine physische Karte. „Sie ist eine seit etwa drei Jahren bestehende Funktionalität“, erklärte DI Thomas Gert Rössler von der A-SIT. Sie kann auf verschiedenen Medien und mit verschiedenen Technologien realisiert werden, etwa auf Bankomatkarten, Studentenausweisen, Signaturkarten oder mit dem Handy. Eine weite Verbreitung wird im Zuge der flächendeckenden Versendung der E-Card erwartet, auf die die Funktionalität der Bürgerkarte ebenfalls aufgebracht werden kann.

Die Bürgerkarte ist für den Einzelnen der Schlüssel zum E-Government, eingeführt durch das mit 1. März 2004 in Kraft getretene E-Government-Gesetz (E-GovG), BGBl I 10/2004. Sie dient dem Nachweis der Identität eines Einschreiters und der Authentizität eines elektronisch gestellten Anbringens (§ 4 E-GovG).

Die eindeutige Identifikation dessen, der sich der Funktion der Bürgerkarte bedient, erfolgt über die Stammzahl. Diese wird, bei Personen, die im Melderegister eingetragen sind, durch ein kryptografisches Verfahren aus der ZMR-Zahl gebil-

IT-SICHERHEIT

IT-Sicherheitstag

Organisator des ersten österreichischen IT-Sicherheitstags 2004 in Klagenfurt und der zweiten Veranstaltung 2005 in Graz waren Univ.-Prof. Dr. Patrick

Horster von der Universität Klagenfurt, Informatik – Systemsicherheit (www.syssec.at) und Dr. Peter Schartner.

Der dritte IT-Sicherheitstag findet im Herbst 2006 in Wien statt.

det, bei juristischen Personen, je nach ihrer Rechtsgrundlage, aus der Firmenbuchnummer oder der Zahl des *Zentralen Vereinsregisters (ZVR)*. Betroffene, die in keinem dieser Register eingetragen sind, etwa jene, die im Ausland leben, können sich über Antrag in ein Ergänzungsregister eintragen lassen.

Stammzahlenregisterbehörde ist die Datenschutzkommission, die diese Aufgabe im Wege des DVRs wahrnimmt (§ 7 Abs 1 E-GovG). Die Stammzahl natürlicher Personen darf weder von einer Behörde noch von anderen gespeichert werden, sie bleibt unter der alleinigen Kontrolle des Bürgers. Sie wird auch nicht direkt zur Identifikation in E-Government-Prozessen verwendet, sondern nur zu der mit kryptografischen Methoden erfolgenden Bildung des bereichsspezifischen Personenkennzeichens (bPK; § 9 E-GovG) bzw., bei Verwendung der Bürgerkartenfunktion im privaten Bereich, zur Bildung des wirtschaftsbereichsspezifischen Personenkennzeichens (wbPK; § 14 E-GovG).

In der E-Government-Bereichsabgrenzungsverordnung (E-Gov-BerAbgrV, BGBl II 289/2004) sind insgesamt 35 Tätigkeitsbereiche der staatlichen Verwaltung festgelegt. Nur innerhalb eines solchen Bereiches kann das gleiche bPK verwendet werden, nicht aber in den anderen, sodass also etwa aus dem Bereich „Sicherheit und Ordnung (SO)“ keine Verbindung beispielsweise zum Bereich „Steuern und Abgaben (SA)“ hergestellt werden kann – was einen umfassenden Einblick in alle Lebensbereiche ausschließt und der Gefahr des „gläsernen Menschen“ entgegenwirkt.

Die Bürgerkarte ermöglicht es auch, elektronische Dokumente rechtsverbindlich zu signieren, so dass der Empfänger des Dokuments sicher sein kann, dass das elektronisch übermittelte

Schriftstück von dem stammt, der es ausgestellt hat, und dass es nicht verändert wurde (Authentizität und Integrität). Technisch gesehen, wird dem Signator ein durch kryptografische Verfahren erstelltes Zertifikat zugeordnet, das, als Signaturstellungsdatum im Sinn des Signaturgesetzes auf dem Datenträger generiert wird („privater Schlüssel“). Dazu gibt es den „öffentlichen Schlüssel“ (Signaturprüfdatum), der mit dem Namen des Signators in Form eines digitalen Zertifikats veröffentlicht wird. Um ein elektronisches Dokument zu signieren, wird von diesem ein eindeutiger „Fingerabdruck“ (Hash-Wert) gebildet, der vom Signierenden mit dem nur ihm bekannten privaten Schlüssel verschlüsselt wird.

Beim Empfang des Dokuments wird wiederum dessen Hashwert berechnet und der vom Signator verschlüsselte und mitgeschickte „Fingerabdruck“ mit seinem öffentlichen Schlüssel entschlüsselt. Stimmen die beiden Werte überein, wurde das Dokument nicht verändert und stammt auch tatsächlich vom Signator.

Websites. „Bei der Gestaltung von Websites kann man leicht mit dem Urheberrecht in Konflikt kommen“, führte Dr. Sonja Janisch (Universität Salzburg) in ihrem Referat aus. Das Urheberrecht schützt Werke bis zu 70 Jahre nach dem Tod des Urhebers, und nicht nur Werke, die eine gewisse Werkhöhe erreichen, sondern auch einfache Fotos, Gebrauchsgrafiken oder Soundfiles („Verwandte Schutzrechte“, II. Hauptstück des UrhG). Ohne Zustimmung des Berechtigten dürfen fremde Websites oder Teile davon nicht übernommen werden. Nicht einmal das eigene Passfoto darf auf Websites verwendet werden, wenn es von einem Fotografen hergestellt wurde und dieser als Urheber nicht die Zustimmung zu dieser Verwendung gegeben hat.

Das Recht am eigenen Bild (§ 78 UrhG) kann verletzt werden, wenn fremde Personen fotografiert und ihre Bilder ins Netz gestellt werden. Links zu anderen Websites dürfen zwar gesetzt werden, doch darf nicht der Eindruck entstehen, dass deren Inhalt zur eigenen Website gehört. Für den Link, auf den verwiesen wird, wird nach dem E-Commerce-Gesetz ab dem Zeitpunkt gehaftet, von dem man von der Rechtswidrigkeit des Inhalts erfahren hat und den Link dann nicht unverzüglich entfernt. Die Frage, ob der Inhaber einer Website auch für Eintragungen in seinem Gästebuch haftet, wird vom OGH geprüft.

Verstöße nach dem Gesetz gegen den unlauteren Wettbewerb (UWG) liegen vor, wenn durch Maßnahmen bei der Gestaltung des Webauftritts Suchmaschinen manipuliert werden, dass die eigene Seite bei Anfragen in den Vordergrund gedrängt wird.

Die gerichtliche Geltendmachung von Unterlassungs-



Martin Prager: „Niemand würde eine Kassa ungesichert herumstehen lassen.“

ansprüchen nach dem UrhG ist vom Verschulden unabhängig. Zur Geltendmachung ist keine vorherige Aufforderung zur Unterlassung erforderlich und auch eine sofortige Entfernung schützt nicht. Neben dem Unterlassungsanspruch bestehen noch Ansprüche auf Beseitigung, auf kostenpflichtige Veröffentlichung des Urteils, auf Zahlung angemessenen Entgelts,



Hans-Jürgen Pollirer präsentiert das IT-Sicherheitshandbuch.

Schadenersatz und Herausgabe des Gewinns, Rechnungslegung und Auskunft (§§ 81 – 87b UrhG). „Bei einem üblicherweise mit 35.000 Euro angesetzten Streitwert, von dem die Gerichtsgebühren und Anwaltskosten berechnet werden, sind solche Verfahren meist teuer“, meint Janisch und rät: „Vermeiden ist besser als zahlen.“ Dazu kommen die strafrechtlichen

Konsequenzen (Freiheitsstrafe bis zu 6 Monaten oder Geldstrafe bis zu 360 Tagessätzen – § 91 UrhG).

Seit der Mediengesetz-Novelle BGBl I 49/2005, die am 1. Juli 2005 in Kraft getreten ist, gilt die Offenlegungspflicht nach § 25 MedienG auch für Websites. Selbst wenn sie keine über die Darstellung des persönlichen Lebensbereichs oder die Präsentation des Medieninhabers hinausgehende Informationen enthalten, müssen Name oder Firma, gegebenenfalls der Unternehmensgegenstand, sowie der Wohnort oder der Sitz des Medieninhabers ständig leicht und unmittelbar auffindbar angegeben werden (§ 25 Abs 1 und 5 MedienG). Für andere Websites und Newsletter gelten die weiter gehenden Bestimmungen des § 25 MedienG. Zusätzliche Informationspflichten, die mit denen des Mediengesetzes verbunden werden können, können sich aus dem E-Commerce-Gesetz ergeben. *K. H.*

DATENSCHUTZ

Sensible Daten

Die Verwendung personenbezogener Daten ist an das DVR zu melden.

Laut Univ.-Prof. Dr. Dietmar Jahnelt (Universität Salzburg) ist die Verwendung personenbezogener Daten an das DVR (Datenverarbeitungsregister) zu melden. Eine private Homepage, bei der keine solchen Daten verwendet werden, ist nicht meldepflichtig. Eine Website mit Bestellmöglichkeit fällt unter die Standardanwendungen „Rechnungswesen und Logistik“ oder „Kundenbetreuung und Marketing“ und ist als Standardanwendung auch nicht meldepflichtig. Sonst besteht Meldepflicht; die Verwendung personenbezogener Daten muss gerechtfertigt sein, etwa durch die Zustimmung des Betroffenen. Bei

der Verwendung nichtsensibler Daten kann eine Abwägung der jeweiligen Interessen erfolgen. Sensible Daten (Daten über rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder Sexualeben; § 4 Z 2 DSGVO) dürfen nur im Rahmen der taxativ aufgezählten Rechtfertigungsgründe des § 9 DSGVO verwendet werden.

Logfiles, aus denen sich die IP-Adresse ergibt, sind personenbezogene Daten. Auf sie findet das Telekommunikationsgesetz Anwendung. Als Verkehrsdaten dürfen Logfiles nur zur Verrechnung gespeichert wer-

den; datenschutzrechtlich gelten sie als „potenziell“ sensible Daten – man kann nicht von vornherein sagen, dass sie keine sensiblen Daten betreffen. Daher müssen auf Logfiles die strengeren Regeln angewendet werden, dass bei Fehlen einer ausdrücklichen Zustimmung ihre Verwendung beispielsweise erforderlich sein muss, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen, und dass die Verwendung nach besonderen Rechtsvorschriften zulässig ist (§ 9 Z 11 DSGVO).

Hat der Arbeitgeber die private Nutzung des Internets erlaubt, dürfen Logfiles ohne ausdrückliche Zustimmung (etwa Betriebsvereinbarung) nicht gespeichert werden. In einem solchen Fall besteht keine Notwendigkeit zu einer Protokollie-

rung – außer für technische Zwecke. Bei eingeschränkter oder verbotener Privatnutzung ist die Protokollierung erlaubt, soweit sie für die Überwachung nötig ist, und Stichproben dürfen ohne Herstellung eines Personenbezugs gemacht werden. Erst bei Missbrauchsverdacht darf es zu einer Auswertung kommen. In allen Fällen ist der Zugriff auf Logfiles zu protokollieren.

Die in Deutschland vertretene Rechtsmeinung, ein Arbeitgeber, der die private Nutzung seiner Kommunikationsdienste zulasse, werde zum Betreiber eines Kommunikationsdienstes, mit allen sich daraus ergebenden Verpflichtungen, trifft für Österreich nicht zu, weil der Arbeitgeber den Kommunikationsdienst nicht „öffentlich“ zur Verfügung stellt (Urteil des OGH vom 13. Juni 2002, 8 Ob A 288/01p).