



Workshop zu mechanischer Einbruchssicherheit beim 7. Security Forum in Hagenberg.

Schutz, Recht, Sicherheit

„Let's talk security“ war das Motto beim 7. Security Forum des Hagenberger Kreises am 22. und 23. April 2009 in der Fachhochschule Hagenberg.

Sind die Leute denn schon süchtig nach Unsicherheit?“, fragte Prof. Edward Humphreys, Direktor der britischen IT-Sicherheitsberatungsfirma *XiSEC* (www.xisec.com) und verwies auf Raucher, oder Alkoholranke, die zwar auch ihr Risiko kennen, aber in vielen Fällen ihre Gewohnheiten nicht ändern. „Wollen Unternehmen mit IT-Sicherheitsproblemen in den Medien aufscheinen? Sind sie selbstgefällig? Kümmern sie sich einfach nicht darum? Geht es um den Kick, das Spiel mit dem Feuer? Wie sonst ist es zu erklären, dass bei Unternehmen Daten gestohlen oder vernichtet werden, die IT-Systeme durch Schadprogramme infiziert werden, keine Notfallpläne

bestehen oder Attacken über Social Engineering immer noch erfolgreich sind?“

IT-Grundschutz, Standardsicherheit im IT-Bereich bietet der IT-Grundschutz, wie ihn das deutsche *Bundesamt für Sicherheit in der Informationstechnik (BSI)* entwickelt hat. Das erste IT-Grundschutzhandbuch ist 1994, drei Jahre nach Gründung des BSI, erschienen, damals nur für Behörden, seit 1995 für die Öffentlichkeit, und ist seither laufend weiterentwickelt worden. Die Idee ist, mit standardisierten Schutzmaßnahmen ein Sicherheitsniveau zu erreichen, das angemessen und ausreichend ist und die Basis für hochschutzbedürftige IT-Anwendungen bilden kann, berich-

tete Dipl.-Inf. (FH) Michael Ruck vom BSI. Mit verhältnismäßig wenig Aufwand kann viel an Sicherheit erreicht werden – als IT-Grundschutz. Jedes Mehr erfordert einen bereits überproportional ansteigenden Aufwand. In etwa 80 Prozent der Fälle wird der IT-Grundschutz ausreichend sein. Er beruht darauf, dass in Form einer Risikoanalyse jene Gefahren aufgelistet werden, die der Informationssicherheit drohen (Gefährdungskatalog), wie etwa höhere Gewalt, organisatorische Mängel, menschliches Fehlverhalten und vorsätzliche Handlungen, technisches Versagen. Dazu werden Bausteine entwickelt, die zu einem Katalog von Maßnahmen führen, die organisatorisch, personell, in-

frastrukturell und technisch umzusetzen sind, um den Schutzbedarf zu erreichen. Ein einmal hergestelltes Sicherheitsniveau darf nicht auf sich beruhen, sondern muss ständig überprüft und weiterentwickelt werden. Die Methodik hinter dem IT-Grundschutz ist in den BSI-Standards 100-1 bis 1004-4 beschrieben.

Das IT-Grundschutzhandbuch, das kostenlos von der Homepage des BSI (www.bsi.bund.de) heruntergeladen werden kann, liegt auch als kurzgefasster „Leitfaden IT-Sicherheit“ vor. Auf Details wird in dieser Darstellung verzichtet; der Schwerpunkt liegt bei organisatorischen Maßnahmen und technischen Hinweisen. Mit dieser Kurzfassung soll auch ein Anreiz geschaffen

werden, sich vertieft mit Informationssicherheit zu beschäftigen.

Das BSI bietet einen Webkurs „IT-Grundschutz“ an. (www.bsi.bund.de/grundschutz/webkurs). Zielgruppen sind IT-Sicherheitsbeauftragte und IT-Mitarbeiter, denen mit Anleitungen, Beispielen, Übungen und Tests ein schneller Einstieg ermöglicht werden soll, verbunden mit einer Demonstration, wie bei einem fiktiven Unternehmen an die Etablierung des IT-Grundschutzes herangegangen werden soll.

Das „GSTOOL“ ist ein Hilfsmittel zur Dokumentation, um die Ergebnisse der Strukturanalyse, der Feststellung des Schutzbedarfes, der Risikoanalyse und des Basis-Sicherheitschecks zu erfassen und einen Bericht zu erstellen. In die IT-Grundschutz-Kataloge wurden neue Bausteine wie

Patch- und Änderungsmanagement, allgemeiner Verzeichnisdienst und *Active Directory* aufgenommen; Bausteine wie Sicherheitsmanagement und häuslicher Arbeitsplatz wurden überarbeitet. Im Februar 2009 ist der BSI-Standard 100-4 „Notfallsmanagement“ erschienen, der erste deutschsprachige Standard zu Business Continuity.

Arbeitsrecht. Über Rechtsfragen im Zusammenhang mit der privaten Nutzung von Internet und E-Mail am Arbeitsplatz referierte Rechtsanwältin Mag. Gregor Royer, Wels. Unbestritten ist, dass dem Arbeitgeber Überwachungsrechte zustehen, schon allein, um den Abfluss unternehmensinterner Informationen zu verhindern. Sogar Überwachungspflichten bestehen, indem etwa sexuelle Belästigung durch über E-Mail

versandte pornografische Darstellungen bei sonstiger Schadenersatzpflicht verhindert werden muss. Eine Haftung des Arbeitgebers als Betreiber des Firmen-Netzwerks kann auch durch den Download von Musikdateien entstehen, bei dem in der Regel Urheberrechte verletzt werden.

Eine Überwachung steht allerdings in einem Spannungsverhältnis zu Grundrechten des Einzelnen, etwa nach Art 8 EMRK, der dem Schutz des Privatlebens und des Briefverkehrs dient; dem Grundrecht auf Datenschutz nach § 1 DSG sowie arbeits- und arbeitsverfassungsrechtlichen Bestimmungen. Ein rechtswidriger Eingriff in die Privatsphäre eines Menschen verpflichtet nach § 1328a ABGB zu Schadenersatz.

Eine Kontrolle des Verhaltens des Arbeitnehmers verstößt noch nicht gegen

seine Persönlichkeitsrechte, sondern gehört zum Wesen des Arbeitsverhältnisses (OGH 13.6.2002, 8 ObA 288/01p). Auf die Art der Kontrolle kommt es allerdings an. Durch eine zu hohe Kontrolldichte kann die Menschenwürde verletzt werden. Ist das der Fall, bedarf die Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer nach § 96 Abs. 1 Z 3 ArbVG zu ihrer Rechtswirksamkeit der Zustimmung des Betriebsrats. Fehlt sie, müssen die Weisungen von den Arbeitnehmern nicht befolgt werden; die Nichtbefolgung bildet keinen Entlassungsgrund (OGH 20.4.1995, 8 ObA 340/94). Ist kein Betriebsrat eingerichtet, ist eine Regelung durch Betriebsvereinbarung erforderlich oder die Zustimmung des Arbeitnehmers.



EVVA
access to security

Mechanische Schließsysteme

Elektronische Schließsysteme, Zutrittskontrolle

Hochwertige Alarmsysteme

Lückenlose Videoüberwachung

▶▶▶

Umfassende Sicherheit.
Zuhause und im Unternehmen.

Schützen Sie sich mit EVVA vor dem Zutritt unberechtigter Personen! Wir sind ein führender Hersteller in Europa und Ihr innovativer Partner in allen Sicherheitsfragen: vom mechanischen oder elektronischen Schließsystem bis zur individuell abgestimmten Alarm- und Videoanlage. Für ein rundum beruhigendes Gefühl!

▶▶▶
www.evva.com

Dem Arbeitgeber steht es frei, bei den Betriebsmitteln die private Nutzung von Internet und E-Mail zu verbieten. Die Einhaltung des Verbots kann auch ohne Zustimmung des Arbeitnehmers überwacht werden, allerdings nur im unbedingt erforderlichen Ausmaß. In Ausnahmefällen wird die private Nutzung dieser Dienste bei Vorliegen wichtiger Gründe entschuldbar sein, zum Beispiel dann, wenn dadurch eine sonst erforderliche Abwesenheit vom Dienst vermieden werden kann (Anfragen bei Behörden, Terminvereinbarungen beim Arzt).

Gestattet der Arbeitgeber die private Nutzung, empfiehlt es sich, deren Umfang konkret festzulegen und beispielsweise zeitlich zu beschränken sowie Maßnahmen zu treffen, die die Sicherheit des Systems und der gespeicherten Daten gewährleisten.

Wurde keine Regelung getroffen, bedeutet das nicht, dass die private Nutzung von Internet und E-Mail schrankenlos zulässig ist. Dienstpflichten dürfen nicht vernachlässigt und Arbeitsabläufe nicht beeinträchtigt werden.

Es kommt auf die Umstände des Einzelfalls, den Ortsgebrauch sowie die Übung des redlichen Verkehrs an. Durch die private Nutzung dürfen keine Sicherheitsrisiken entstehen, Gesetze verletzt oder die Ressourcen des EDV-Systems beeinträchtigt werden.

Der Arbeitnehmer haftet für Schäden, die durch sein weisungswidriges Verhalten entstehen. Da Schäden, die durch die private Nutzung von Internet und E-Mail entstehen, in der Regel mit der Erbringung der Dienstleistung für den Arbeitgeber nicht in Zusammenhang stehen, kommt das Dienstnehmerhaftpflichtgesetz, das



Michael Ruck: „Sicherheitsniveau mit standardisierten Schutzmaßnahmen erreichen.“

Begünstigungen vorsieht, nicht zur Anwendung. Gewisse grundlegende Vorsorgen, wie etwa die Installation von Virenschutzprogrammen, wird allerdings auch der Arbeitgeber zu treffen haben; deren Fehlen kann als Mitverschulden angerechnet werden.

Die weisungswidrige Privatnutzung kann bei Angestellten bis zur Entlassung führen, nämlich bei Vertrauenswürdigkeit, beharrlicher Dienstverweigerung oder Dienstunfähigkeit (§ 27 AngG). Schädigungsabsicht oder Eintritt eines Schadens sind nicht Voraussetzung für eine Entlassung.

Als Vertrauenswürdigkeit begründend wurden von der Judikatur angesehen die versuchte Verschleierung der Privatnutzung des Firmenrechners; die Installation privater Software; die Löschung privater Dateien entgegen einer auf Erhaltung dieses Beweismittels gerichteten Weisung sowie der Einbau von Sperrcodes oder Löschroutinen in Computerprogrammen.

Eine beharrliche Verletzung von Dienstpflichten liegt vor, wenn eine Ermahnung erfolgt ist, am besten schriftlich, mit der Androhung der Entlassung.

Dienstunfähigkeit kann sich an einem Arbeitsplatz mit Internet-Anschluss bei



Gregor Royer: „Arbeitgeber stehen Überwachungsrechte zu, um Abfluss von Daten zu verhindern.“

Internet-, Spiel- oder Sexsucht ergeben.

Gesundheitsdaten. Unter anderem wird von *Google* angeboten, Gesundheitsdaten zu speichern, damit sie dem Berechtigten jederzeit weltweit zur Verfügung stehen und im Bedarfsfall abgerufen werden können (*Personal Health Record*).

Der Gedanke hat etwas Bestechendes, nur – wie sicher sind diese doch überaus sensiblen Daten vor dem Zugriff anderer? Muss man da nicht blind auf ein Sicherungssystem vertrauen, das man nicht kennt? Und, selbst wenn die Daten nur autorisierten Benutzern zugänglich und verschlüsselt abgelegt sind, können nicht schon aus der Anzahl der Anmeldungen im System und dem Umfang der transferierten Informationen Schlüsse auf den Gesundheitszustand eines Menschen gezogen werden und, aus den Kommunikationswegen, von welchen Ärzten und welchen Krankenanstalten Daten übermittelt oder angefragt werden, an welchen Krankheiten ein Mensch leidet?

Dr. Christian Stingl und Daniel Slamanić, MSc von der Fachhochschule in Klagenfurt stellen Lösungsmöglichkeiten vor. Kommunikationsanonymität kann

durch das Versenden über einen oder auch mehrere Anonymisierungsproxys (die ihrerseits wieder vertrauenswürdig sein müssen) erreicht werden oder durch ein „Untertauchen“ in einer Menge anderer (Crowds), über die die Daten nach Zufallsgesichtspunkten versendet (geroutet) werden. Der Nachteil ist, dass die Datenpakete bei diesen Verfahren immer länger werden und dadurch die Performance leidet.

Authentifikationsanonymität bei der Datenabfrage kann ebenfalls über eine Gruppe erfolgen, von der alle Benutzer den gleichen geheimen Schlüssel haben. Innerhalb der Gruppe hat jedes Mitglied eine eigene Box, die es mit einem geheimen Schlüssel öffnen kann. Das Verfahren wird allerdings bei großen Gruppen ineffizient.

Datenschutz. Dr. Hans G. Zeger, Obmann der *Arge Daten*, wies darauf hin, dass seiner Auffassung nach Daten zu schnell gesammelt würden: „Das Erste, wenn ein Problem auftaucht, ist ein neues Register.“ Das führe aber nur zu einer Vergrößerung des Heuhaufens. Es gebe kein Patentzept; aber Konflikte zu erkennen und zu lösen sei besser, als Angst zu erzeugen.

Weitere Themen der Vorträge beim Security-Forum in Hagenberg waren Secure Coding; die zentrale Loganalyse als Basis für eine sichere IT-Infrastruktur; Schutzmechanismen für Webapplikationen und Database Forensics.

Einer der Workshops befasste sich mit mechanischer Einbruchssicherheit, aus der Überlegung heraus, dass Rechenzentren nicht nur in ihren logischen Systemen, sondern auch physisch geschützt werden müssen.

Kurt Hickisch