web.sicher

So nützlich und nicht mehr wegzudenken das Internet ist – Verhaltensweisen sollten überprüft und juristische Spielregeln beachtet werden.

Etwa 80 Teilnehmerinnen und Teilnehmer hatten sich am 6. Oktober 2011 zum 8. österreichischen IT-Sicherheitstag eingefunden, der erstmalig in der Messe Klagenfurt abgehalten wurde. Veranstaltet wurde die Tagung wie bisher von der Forschungsgruppe *Systemsicherheit (syssec; www.syssec.at)* der Universität Klagenfurt, geleitet und moderiert von Ass.-Prof. Dr. Peter Schartner.

„Bring your own device" – mit diesem Schlagwort wird umschrieben, dass Mitarbeiter am Arbeitsplatz ihre eigenen Geräte benützen sollten. Mit ihnen können sie umgehen, auf ihnen befinden sich benutzerfreundlichere Programme, als sie vom Unternehmen zur Verfügung gestellt werden. Zudem wird ein mobiler Zugriff von Endgeräten wie Smart-Phones fast schon vorausgesetzt. Das wirft weitere Sicherheitsprobleme auf. Ing. Franz Stögerer von der *Kapsch BusinessCom AG* informierte über Lösungsmöglichkeiten.

Es geht bei diesen darum, eine lückenlose Kontrolle über alle Endgeräte und die darauf verwendeten Programme zu erhalten, ohne deren Anwendung zu verhindern, sondern sie als Business-Enabler einzusetzen.

Social Media. „Um die Nutzung sozialer Netzwerke als Kommunikationsplattform kommen Unternehmen heutzutage nicht mehr herum", sagte Dr. Frank Innerhofer-Oberperfler (Universität Innsbruck, Institut für Informatik). „Über derartige Netze können bestehende Kontakte gepflegt, zukünftige Mitarbeiter geworben und

Messe Klagenfurt: Veranstaltungsort des 8. österreichischen IT-Sicherheitstags.

unzählige potenzielle Endverbraucher erreicht werden." Nach Angaben der *Wirtschaftskammer Österreich* nutzen 48 Prozent der Unternehmen in Österreich diese Netze. *Facebook* beispielsweise hat nach dieser Studie über 2,2 Millionen Mitglieder in Österreich, *Twitter* an die 40.000.

Man sollte jedoch das Geschäftsmodell bei sozialen Medien nicht außer Acht lassen. Es besteht aus Datamining und dem Verkauf von Werbeflächen. Die Daten und Kontakte der Nutzer und Aufzeichnung ihres Verhaltens sind das Kapital der sozialen Netzwerke. „Gefällt-mir"-Buttons geben diesbezüglich Hinweise.

Durch die Möglichkeit, sein Adressbuch hochzuladen, werden Daten über Personen geliefert, die bisher noch nie ein Konto angelegt haben. Zudem werden die Netzwerke untereinander immer mehr verknüpft – die Trennung zwischen privaten und beruflichen Netzwerken beginnt zu verschwimmen. Letztlich werden durch die Nutzung mobiler Endgeräte die sozialen Netzwerke auch in die Lage versetzt zu verfolgen, wo sich der einzelne User aufhält.

„Eine Strategie zur Nutzung sozialer Netzwerke muss in die Risikomanagement-Prozesse eingebaut werden", forderte Innerhofer-Oberperfler. „Mitarbeiter müssen über aktuelle Risiken der Nutzung solcher Netze aufgeklärt und laufend darin geschult werden."

Cloud-Computing. Beim Computing „in the Cloud" wird auf Programme und Speicherplatz zurückgegriffen, die sich auf virtualisierten, physikalisch nicht voneinander getrennten Servern im Internet befinden. Dadurch können Ressourcen dynamisch auf Gastsysteme zugewiesen werden. Die Anschaffung komplexer und teurer Programme sowie der Aufwand, diese immer auf dem neuesten Stand zu halten, werden eingespart; die erforderliche Hardware kann reduziert werden.

Dr. Thomas Rössler von der *Datentechnik Innovation GmbH (www.datentechnik-innovation.com)* informierte über ein auf das E-Government zugeschnittene Betriebsmodell des Cloud-Computings, die „EGovernment Cloud". Dieses Modell wurde für kleine und mittlere Gemeinden und Städte entwickelt, an die zwar hohe Ansprüche an Service-Qualität gestellt werden, denen aber die entsprechenden Ressourcen nicht zur Verfügung stehen. „Etwa 2.300 der über 2.500 Gemeinden Österreichs haben weniger als 10.000 Einwohner", sagte Rössler. Statt dass alle für sich Einzellösungen vorsehen, können Leistungen so vernetzt und gebündelt werden, dass alle daran kostengünstig teilhaben können.

Software-Lösungen im Premium-Bereich (elektronischer Akt, Finanzbuchhaltung, Bürgerportal, Zustellsysteme, ERP/Management, Amtssignatur) werden unter Beibehaltung der Eigenständigkeit für kleinere Gemeinden erschwinglich. Eine Absicherung der Systeme gegen Angriffe kann effizienter durchgeführt werden, als dies bei kleineren Einheiten möglich ist. Ein Pilotprojekt wurde in der Steiermark gestartet. Das für E-Government entwickelte Betriebsmodell der „Shared Services" kann in die Privatwirtschaft übertragen werden.

Mit dem Betriebsmodell eng in Zusammenhang stehen die elektronische Amtssignatur sowie die elektronische Identität. Bei der Amtssignatur wird das auszustellende Dokument am Server signiert. Zusatzgeräte wie Kartenleser sind nicht erforderlich. Anstelle eines Stempels wird die Signatur mit

FOTO: KÄRNTER MESSE

Frank Innerhofer-Oberperfler: „Strategie zur Nutzung sozialer Netzwerke in Risikomanagement einbauen."

der Maus in das Dokument gezogen, das elektronisch versendet wird. Die Identität des Absenders ergibt sich aus der auf dem ausgedruckten Dokument ersichtlichen Prüfinformation, die eine Nachprüfung bei einer vertrauenswürdigen Stelle gestattet.

Spionageabwehr. „Gleichgültig, ob aus einem Unternehmen Informationen abfließen durch fremde Nachrichtendienste (Wirtschaftsspionage) oder zum Nutzen von Wettbewerbern (Industriespionage) – der Effekt ist für das Unternehmen derselbe", sagte Klaus Schäfers von *Orgaconsult (www.orgaconsult.at)*.

Schäfers wies auf Beispiele hin, wie den Schmuggel der Seidenraupe von China nach Indien um 500 n. Chr., das Verbringen des Geheimnisses der Papierherstellung aus dem arabischen Raum nach Europa im Jahr 1389, des Geheimnisses der Porzellan-Herstellung oder den Diebstahl von Kautschukbaumsamen durch Henry Wickham in Brasilien und deren Anpflanzung in den britischen Kronkolonien Indien, Ceylon, Borneo und Malakka. Wickham wurde dafür von Königin Viktoria in den Adelsstand erhoben.

Thomas Rössler: „Mit E-Government Cloud können Gemeinden kostengünstig an E-Government teilhaben."

Alle Informationen können von Interesse sein – über Produkte und Produktionsweisen, Kunden und Lieferanten, über Mitarbeiter, Preise und Kalkulationen und Zahlungen. Angriffspunkte sind zum einen Menschen, die unzufrieden und frustriert sind, in finanziellen Schwierigkeiten stecken oder denen es an Sicherheitsbewusstsein mangelt. Sie sind durch Social Engineering angreifbar, mit dem Ziel, durch erlangte Informationen in gesicherte Systeme einzudringen.

Zum anderen bieten unzureichend gewartete und hard- sowie softwaremäßig (fehlende Updates) nicht auf den letzten Stand gebrachte Rechner Angriffsmöglichkeiten.

Die Technik allein mache es aber immer schwieriger, den Abfluss von Informationen zu verhindern; beim Mitarbeiter sei anzusetzen. „Drohen, verbieten, sanktionieren ist nicht der richtige Weg", betonte Schäfers. „Es gilt, neben technischen Maßnahmen, die Mitarbeiter einzubeziehen und sie für Sicherheitsgedanken zu gewinnen."

Zahlungsdienste. Im juristischen Teil der Veranstaltung referierte Ass.-Prof. Dr.

Peter Mader: „Domains zu erwerben, um sie später zu verkaufen, ist sittenwidriger Behinderungswettbewerb."

Sonja Janisch der Universität Salzburg über Internet-Zahlungssysteme im Lichte des am 1. November 2009 in Kraft getretenen Zahlungsdienstegesetzes (ZaDiG), das eine umfassende Regelung des Zahlungsverkehrs in Österreich mit sich gebracht hat.

Für Zahlungen, die mittels Kreditkarte über das Internet erfolgen, ist die Frage von Bedeutung, wer das Risiko einer missbräuchlichen Verwendung des Zahlungsmittels trägt. In Betracht kommen der Karteninhaber, der Kartenaussteller und der Vertragshändler. § 44 Abs. 1 ZaDiG bestimmt, dass der Zahlungsdienstleister (Kartenaussteller) im Fall eines nicht autorisierten Zahlungsvorgangs den Betrag dem Zahler (Karteninhaber) unverzüglich zu erstatten und das belastete Konto wieder auf den Stand zu bringen hat, auf dem es sich ohne den nicht autorisierten Zahlungsvorgang befunden hätte.

Allerdings können Schadenersatzansprüche gegen den Karteninhaber geltend gemacht werden. Bei Betrug oder vorsätzlicher oder grob fahrlässiger Pflichtenverletzung haftet der Karteninhaber unbeschränkt, bei nur leicht fahrlässiger Pflichtenverletzung bis zu höchstens 150 Euro (§ 44 Abs. 2). Trifft ihn kein Verschulden, haftet er nicht, auch nicht nachdem er den Verlust, den Diebstahl oder die missbräuchliche Verwendung dem Kartenaussteller angezeigt hat (§ 36 Abs. 2; sofern keine betrügerische Absicht dahintersteckt).

Nachdem die von den Kreditkarten-Firmen mit den Vertragshändlern abgeschlossenen Verträge in der Regel ein Rückbelastungsrecht des Kartenausstellers vorsehen, wenn der Karteninhaber die Bestellung bestreitet, trifft das Risiko eines Drittmissbrauchs in der Praxis den Vertragshändler. Die Haftungssituation für den Kunden wurde durch das ZaDiG günstiger. Entscheidend ist die Abgrenzung zwischen grober und leichter Fahrlässigkeit. In den Verträgen der Kartenaussteller mit den Karteninhabern ist durchgehend vorgesehen, dass neben den allgemeinen Sorgfaltspflichten wie die sichere Verwahrung der Karte unverzügliche Mitteilung eines Diebstahls, die Kreditkarte im Internet nur in verschlüsselten Systemen verwendet werden darf.

Wenn die Eingabe eines Passworts oder einer PIN erforderlich ist, wird in der Regel, in Form eines Anscheinsbeweises, zunächst davon ausgegangen, dass der Karteninhaber der Besteller der Ware ist und demgemäß den vom Kartenaussteller zu seinen Lasten geleisteten Betrag nicht rückfordern kann.

Die Beweislast kehrt sich in diesem Fall um: Nunmehr müsste der Karteninhaber beweisen, die Bestellung nicht getätigt und seine PIN nicht weitergegeben zu haben. Bei PIN-gesicherten Systemen hat der Händler in der Regel eine Zahlungsgarantie.

§ 44 ZaDiG ist auch auf andere Internet-Zahlungsformen anwendbar, etwa auch

Fotos: Kurt Hickisch

Zahlung mit Kreditkarte im Internet: Im Fall eines nicht autorisierten Zahlungsvorgangs hat der Kartenaussteller den Betrag dem Karteninhaber unverzüglich zurückzuerstatten.

Foto: Egon Weissheimer

auf das Online-Banking. Damit trifft die Unterscheidung zwischen grober und leichter Fahrlässigkeit auch beispielsweise auf das Phishing zu, dass also jemandem seine PINs und TANs herausgelockt werden und damit nicht autorisierte Behebungen von seinem Konto erfolgen.

Die Feststellung, ob überhaupt ein und welches Maß an Verschulden den Kontoinhaber trifft, wird nur im Einzelfall möglich sein. Es wird darauf ankommen, ob etwa Warnungen durch die Bank erfolgt sind, die URL überprüft wurde (und inwieweit dies zugemutet werden kann), ob die Website der Bank nur durch Direkteingabe aufgerufen werden kann, entsprechende Pflichten in den AGBs statuiert wurden, ob etwaige Mitteilungspflichten an die Bank verletzt wurden und wer bei offensichtlich gefälschten Phishing-Mails haftet. Im Hinblick auf die Widerrufbarkeit von Zahlungsaufträgen ist durch das ZaDiG allerdings eine Verschlechterung der Situation des Kunden eingetreten. Nach der bis zum Inkrafttreten dieses Gesetzes geltenden Rechtslage konnten Zahlungsaufträge bis zum Zeitpunkt der Gutschriftserteilung auf dem Empfängerkonto widerrufen werden.

Nunmehr statuiert § 40 Abs. 1 Z 1 ZaDiG, dass der Zahlungsdienstnutzer einen Zahlungsauftrag nicht mehr widerrufen kann, wenn der Zahlungsauftrag beim Zahlungsdienstleister eingegangen ist.

So wurde die Klage des Käufers einer Spiegelreflexkamera in einem Web-Shop von den Gerichten im Instanzenzug abgewiesen, dem nach der Geldüberweisung Bedenken hinsichtlich der Seriosität des Unternehmens gekommen waren und der etwa 4,5 Stunden nach Erteilung des Überweisungsauftrags eine Rückbuchung des überwiesenen Betrages von der Bank verlangt und dies letztlich eingeklagt hatte (LG Salzburg 22 R 127/11x).

Internet-Wortadressen

(Domains) haben den Zweck, die für jeden Rechner im Internet bestehende, aus vier durch Punkten voneinander getrennten Zahlengruppen bestehende eindeutige Internetadresse (URL) nach einem System in für den Menschen leichter handhabbare Buchstabenkombinationen zu übersetzen. Diese Domain-Namen werden durch nationale *(nic.at)* und internationale private Einrichtungen *(ICANN)* nach der zeitlichen Reihenfolge der Anmeldung ohne rechtliche Prüfung durch Registrierung vergeben. Wie bei jeder Namensverwendung können Konflikte mit Trägern gleichen oder ähnlichen Namens auftreten, die sich aus namensrechtlichen (§ 43 ABGB) Gesichtspunkten ergeben können, aber auch aus solchen wettbewerbs-, marken-, firmen- und urheberrechtlicher Art.

Durch eine Domain-Blockade wird ein anderer daran gehindert, eine Domain zu verwenden, durch Domain-Vermarktung wird eine Domain in der Absicht erworben, sie später zu verkaufen. Beides, bekannt unter „Domain-Grabbing“ oder „Cybersquatting“, ist im geschäftlichen Bereich ein sittenwidriger Behinderungswettbewerb. „Domainprozesse können teuer werden“, warnte Univ.-Prof. Dr. Peter Mader von der Universität Salzburg davor, Domains leichtfertig oder sogar missbräuchlich zu verwenden.

Kurt Hickisch