Special Innovation

Raum für Neues schaffen

Forschung, Humankapital und neue Technologien sind die zentralen Wachstumstreiber für Industrieländer.

Manfred Lechner

Erstmals fanden heuer im Vorfeld des Anfang März vergebenen Staatspreises „Innovation“ die Innovationstalks statt. „Es gelang uns, namhafte Vertreter aus der heimischen innovativen Wirtschaftsszene zu versammeln und unter dem Motto ‚Leidenschaf(f)t Innovation‘ über den aktuellen Stand des Innovationsbarometers zu diskutieren“, erklärt Sonja Hammerschmid, Leiterin des Bereichs Technologie und Innovation bei dem veranstaltenden austria wirtschaftsservice (aws). Klar ist, dass das Thema Innovation einen relevanten Faktor in allen Fragen der Standortsicherung und -qualität darstellt. Weiters waren sich alle Teilnehmer einig, dass Nachholbedarf in unterschiedlichen Bereichen gegeben ist, damit Österreich jenes innovationsfreundliche Klima bieten kann, das nachhaltiges Wachstum möglich macht.

Peter und Ursula Lisec (1. Reihe v.l.n.r.) wurden mit dem Staatspreis „Innovation“ von Helmut Leopold, Technikchef von Telekom Austria, Minister Martin Bartenstein, Wirtschaftskammerpräsident Christoph Leitl und Peter Takacs vom austria wirtschaftsservice ausgezeichnet. Foto: aws

Technologiewechsel

„Der Technologiewechsel findet derzeit mit einer extremen Geschwindigkeit statt“, stellt Helmut Leopold, Technologiechef von Telekom Austria (TA) und Sprecher der Staatspreis-Innovation-Jury, fest, „die zur Folge hat, dass sich nicht nur im Informations- und Kommunikationstechnologie-Bereich Geschäftsmodelle, Marktakzeptanz und Benutzung verändern.“ Um diesen Wandel erfolgreich bewältigen zu können, bedarf es aber einer Optimierung im Zusammenspiel aller innovativen Marktteilnehmer. Großunternehmen übernehmen für Leopold in diesem Prozess für Klein- und mittlere Unternehmen die Rolle des „Ermöglichers“. Als Beispiel verweist Leopold auf zwei von TA mit Partnern realisierte Projekte. „Gemeinsam mit Häfele, einem Spezialisten für Zutrittssysteme und Beschläge, entwickelten wir die ‚Intelligente Tür‘, ein Produkt, das unseren Kunden im Vergleich zum ausschließlichen Netzgebrauch einen eindeutigen Mehrwert bietet. Die Synergie besteht darin, dass wir kein Zutrittssystem entwickeln mussten und Häfele jetzt in weit mehr informations- und kommunikationstechnologiekonzentrierten Geschäftsfeldern tätig ist als zuvor.“ Vergleichbar gestaltete sich die Partnerschaft von TA mit dem Wiener St. Anna Kinderspital. Ziel ist es, medizinische Betreuungsprozesse mittels IT-gestützter Systeme zum Vorteil der behandelten Kinder, Eltern und auch des medizinischen Personals zu verändern. „Wichtig ist, Innovation nicht ausschließlich als technische Spitzenleistung, die im gesellschaftlich luftleeren Raum entsteht, zu verstehen“, erklärt Monika Kircher-Kohl, Finanzvorstand von Infineon, „denn ohne Berücksichtigung sozialer Fragen wird es nicht gelingen, ein innovationsfreundliches Klima zu erzeugen.“ Darunter versteht sie auch die Entwicklung neuer Arbeitszeitmodelle oder die bessere Integration von derzeit auf dem Arbeitsmarkt benachteiligten Gruppen, wie Frauen oder ältere Arbeitnehmer. „Auf Unternehmensebene hingegen sind harte regulative Prozesse erforderlich“, so Kircher-Kohl, „deren Qualität so beschaffen sein soll, dass Transparenz, Kreativität und Fehlertoleranz möglich sind.“ Als Beispiel erwähnt sie die beiden von Infineon geschaffenen gleichwertigen Aufstiegsoptionen. Kircher-Kohl: „Gewählt werden kann zwischen dem traditionellen Karriereweg im Management oder als Techniker, der sich ohne Personalverantwortung ausschließlich mit Forschung beschäftigt.“

Aus der Sicht eines erfolgreichen Start-ups meint Barbara Gimeno, Vorstand der GAT Microencapsulation AG, „dass technisches Know-how und exzellente innovative Produkteigenschaften noch keine Garantie für Erfolg bedeuten.“ Das von ihr und ihrem Mann 1997 gegründete Unternehmen spezialisierte sich auf die Mikroverkapselung von Nahrungsmittelzusätzen wie Omega-3-Fettsäuren und hat mittlerweile 45 Mitarbeiter. Der Exportanteil beträgt nahezu 100 Prozent. „Wichtig ist es, Entscheidungen zu treffen, selbst wenn sie falsch sein sollten, damit der Prozess des Unternehmensaufbaus vorangetrieben werden kann.“ Als weitere Erfolgsfaktoren nennt sie ein kommunikationsfähiges Team und Geschäftspartner, deren Prozesse auf der gleichen Wellenlänge ablaufen.

High-Tech für Flughafensicherheit

Österreichischer Löschfahrzeughersteller Rosenbauer setzt neue Maßstäbe hinsichtlich Einsatzgeschwindigkeit.

Das österreichische Unternehmen Rosenbauer wurde für die völlig überarbeitete Version seines seit den 90er Jahren hergestellten Flughafenlöschfahrzeugs „Panther“ für den Staatspreis Innovation nominiert.

Der Zeithorizont für den Einsatz von Flughafenfeuerwehren ist klein: Binnen zwei Minuten muss ein Flugzeugbrand gelöscht werden. Rosenbauer entwickelte mit dem „Panther“ ein Fahrzeug, das sowohl größten Komfort für die Bedienmannschaften als auch schnellstmögliche Einsatzbereitschaft gewährleistet. Das Unternehmen setzt, was die Sprint-Eigenschaften und Spitzengeschwindigkeiten betrifft, neue Maßstäbe: Das 40 Tonnen schwere Fahrzeug ist mit 135 Stundenkilometern unterwegs. Was die Umweltverträglichkeit betrifft, entspricht das Fahrzeug den strengen Euro-3-Abgasvorschriften. Der „Panther“ ist mit maximal 14.500 Litern Löschmittel zu beladen und auch bereits für Einsätze im Hinblick auf den neuen Airbus A380 ausgelegt. Um schnelle Verfügbarkeit des Fahrzeugs zu gewährleisten, wurde der „Panther“ mit einer Vorwärmanlage für Motor und Getriebe ausgestattet. Im Notfall starten die Feuerwehrmänner das Fahrzeug mittels eines Alarm-Start-Knopfes von außen. Springen die letzten Männer ins Fahrzeug, fährt der Fahrer los, und die Schwingtüren schließen sich automatisch ab einer Fahrgeschwindigkeit von fünf Stundenkilometern. Das ergonomische Armaturenbrett erlaubt eine „Ein-Mann-Bedienung“ der gesamten Lösch- und Fahrzeugtechnik. Das bedeutet, dass der Feuerwehrmann im Einsatz das Fahrzeug lenken und auch mittels Joystick die Löschtechnik bedienen kann. Die Basis dafür bildet das in Eigenregie entwickelte elektronische Steuerungskonzept Logic Control System. Weiters wurde die Fahrzeugkabine neu gestaltet. Die Design-Aufgabe, die Sicht zu optimieren, konnte mittels einer Panorama-Windschutzscheibe und transparenter Türen gelöst werden.

Zielvorgabe für die Überarbeitung im Design war, eine Synthese zwischen Funktionalität und Ästhetik zu finden. Foto: Rosenbauer

Weltweit vertreten

Rosenbauer ist der zweitgrößte Hersteller von Feuerwehrfahrzeugen weltweit. Der Konzern unterhält in mehr als 100 Ländern ständige Vertretungen. Mit der breiten Palette an Löschfahrzeugen nach europäischen sowie US-Normen gilt Rosenbauer als der „Vollsortimenter“ der Branche. *malech*

Special Innovation

Lernen in Mini-Portionen

Microlearning baut auf den kleinsten Bausteinen der Google-Galaxis auf und nutzt diese für seine Zwecke.

Manfred Lechner

Erfolgreiche Unternehmen tätigen hohe Investitionen in die Schulung ihrer Mitarbeiter. „Was die Kapitalrendite solcher Maßnahmen betrifft, herrscht Unzufriedenheit bei den Personalentwicklern“, erklärt Martin Lindner vom Studio E-Learning Environments. In der Regel sind Mitarbeitern bereits drei Wochen nach einer Schulung rund 80 Prozent des erworbenen Wissens wieder entfallen.

Rasches Vergessen

Das im Rahmen der Research Studios Austria (RSA) betriebene Forschungslabor ist eine der weltweit bedeutendsten Einrichtungen, die sich mit völlig neuen Formen der Vermittlung von Lerninhalten beschäftigt. „Unter dem Begriff Microlearning verstehen wir Lernen im Zeitalter des Google-Universums, das sich aus völlig anderen Bausteinen zusammensetzt als die Gutenberg-Welt“, erklärt Lindner. Um neue, effizientere Lernmethoden zu entwickeln, war es notwendig, die kleinsten Bausteine dieses Universums zu identifizieren. „Dabei handelt es sich um Mikro-Content“, so Lindner, der in diesem Zusammenhang darauf verweist, dass beispielsweise jede Google-Abfrage eine Vielzahl von Mikro-Contents ergibt. Da User mit dieser Art der Informationsaufnahme völlig vertraut sind, macht sich Microlearning diese Eigenschaft zunutze und serviert kleine Lernhappen. Die bekannteste Anwendung derzeit ist ein Englisch-Kurs, bei dem das Handy die Funktion einer Lernkarte übernimmt. Prototypen von webbasierten Schulungsapplikationen sind aber auch bereits bei der Firma Quality Austria, die Unternehmen, Personen und Produkte zertifiziert, im Einsatz.

Der Klick zum Lernfortschritt: Microlearning baut auf bereits erworbenen Techniken von Usern auf, um Lerninhalte abwechslungsreich zu vermitteln. Foto: Bilderbox.com

Die von E-Learning Environments entwickelten Lösungen unterscheiden sich grundlegend von anderen E-Learning-Angeboten. Herkömmliches E-Learning besteht in zwei Ausprägungen, einerseits als elektronisches Klassenzimmer und andererseits aus anzuklickenden Informationen, die nach etlichen Klicks darüber Auskunft geben, ob man die Lerneinheit erfolgreich absolviert hat. „Alles in allem ein wenig anwenderfreundliches Verfahren“, diagnostiziert Lindner, der davon ausgeht, dass Microlearning binnen kürzester Zeit auch im deutschsprachigen Raum jenen Stellenwert bekommen wird, über den es in Nordamerika bereits verfügt.

Internationale Konferenz

Als einer der Big Player in diesem Bereich veranstaltet das Studio E-Learning Environments am 21. und 22. Juni in Innsbruck zum dritten Mal eine international ausgerichtete Konferenz. „Bemerkenswert ist, dass sich diese Veranstaltung als eine gemeinsame Plattform für Forscher der universitären Welt und frei arbeitende Interface-Designer etablieren konnte“, so Lindner, „denn Vertreter der unversitären Welt publizieren in Fachzeitschrften, während Designer ihre auch für die Theoriebildung wichtigen Reflexionen ausschließlich in Blogs veröffentlichen.“

Eric-Jan Kaak: „Die durch die Neuen Medien gegebenen Möglichkeiten versetzen uns in die Lage, bisher ungenutzte, überraschende Situationen für das Lernen zu adaptieren“, erklärt der operative Leiter des Studios E-Learning Environments, einem Bereich der Research Studios Austria.

Kaffeemaschine mit Zusatznutzen

economy: ***Wie kann man sich zukünftige Microlearning-Anwendungen vorstellen?***

Eric-Jan Kaak: Für uns ist wichtig, dass Menschen, ohne in ihren täglichen Abläufen gestört zu werden, Lernfortschritte erzielen und ihre Lernaufgaben in vielfältigen Alltagssituationen zwischendurch erledigen können. Vorstellbar ist Folgendes: Ein Mitarbeiter wartet vor dem Kaffeeautomaten auf sein Getränk und löst währenddessen eine Lerneinheit. Voraussetzung dafür ist, dass der Mitarbeiter mit einer Firmenkarte bezahlt und der Automat netzwerkfähig ist.

Welche Voraussetzungen müssen erfüllt sein, wenn Unternehmen das neue Lernen einsetzen möchten?

Es erfordert ein Umdenken in der Organisation, denn Microlearning-Lösungen müssen in die laufenden Organisationsentwicklungsprozessse integriert werden. Wichtig ist weiters, dass es Mitarbeitern nicht als neues „Allheilmittel“ übergestülpt wird. Würden diese den Eindruck gewinnen, die Lernunterstützung diene ihrer Überwachung, käme es zu einer massiven Ablehnung dieser Ressource. Gelingt es Unternehmen aber, die Mitarbeiter von Microlearning dahingehend zu überzeugen, dass sie tatsächlich davon profitieren können, steht einer erfolgreichen Anwendung nichts im Wege.

Liegen bereits weitere Praxiserfahrungen vor?

Als sehr beliebt erwies sich folgende Anwendung: Verließen Mitarbeiter das Intranet und loggten sich beispielsweise in Orf.at ein, konnten sie die Seite erst dann abrufen, wenn sie zuvor ein paar Lernaufgaben bewältigt hatten. Dies ist ein besonders gutes Beispiel dafür, wie Microlearning bereits jetzt in der Praxis funktioniert. Entscheidender Vorteil ist, dass alle Applikationen serverbasiert, daher beliebig verteilbar sind.

Serverbasierte Lösungen erlauben es, Lernapplikationen auf Handys oder Computern laufen zu lassen. Foto: Bilderbox.com

Denken Sie an den Vertrieb von Lernapplikationen über Netzbetreiber?

Solche Vorstellungen existieren. Unsere Zielrichtung ist aber, Microlearning in einem ersten Schritt auf Unternehmensebene zu verankern. Wie aus den genannten Beispielen hervorgeht, sind, was neue Anwendungen betrifft, der Fantasie nahezu keine Grenzen gesetzt. Tatsache ist aber, dass die Einführung einer neuen Technologie ein strategisches Vorgehen erforderlich macht, damit wir unsere beschränkten Ressourcen optimal nutzen können.

Ist auch an einen Einsatz in Schulen gedacht?

Lehrer lassen sich dadurch nicht ersetzen. Meine Mitarbeiter und ich adaptierten den Handy-Englischkurs zu Testzwecken für unsere Kinder so, dass sie nur dann telefonieren oder SMS abschicken können, wenn sie eine gewisse Anzahl von Fragen beantwortet haben. Weiß man, wie viele SMS Jugendliche schicken, kann man sich ausrechnen, wie schnell Lernfortschritte gemacht werden können. Der große Unterschied zu Lernkärtchen ist der verwendete Algorithmus. Bei Nichterreichen des Lernziels kann die Wiederholung didaktisch so aufgebaut werden, dass die Inhalte völlig neu gemischt präsentiert werden. Erst diese Flexibilität garantiert ein erfolgreiches, da abwechslungsreiches Lernen. *malech*

Steckbrief

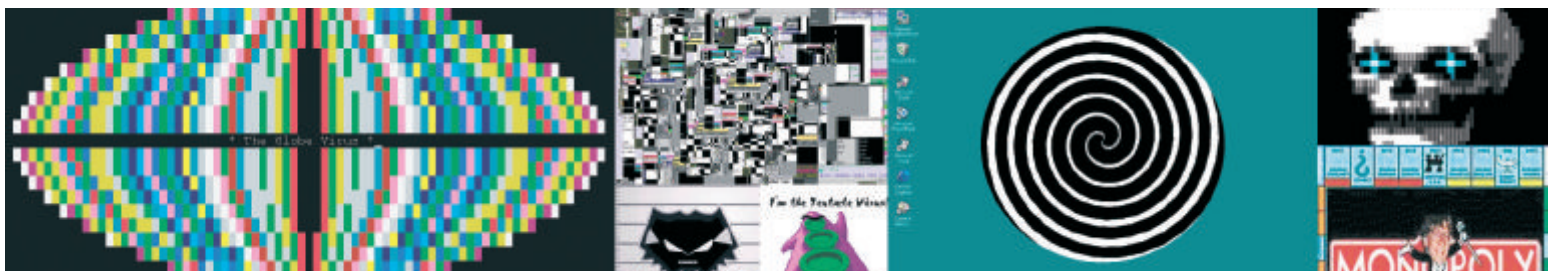
Eric-Jan Kaak ist operativer Leiter des Studios E-Learning Environments in Innsbruck. Foto: RSA

Special Innovation

Im Namen der Sicherheit

Das Thema Security wird immer wichtiger, wie die weltgrößte Computermesse Cebit in Hannover zeigt.

Ernst Brandstetter



Screenshots mit Grusel-Effekt: So zeigen sich einige der bekanntesten Schadprogramme auf dem Bildschirm. Die Bedrohungen der Sicherheit nehmen zu, die IT-Security-Branche hat Hochkonjunktur. Foto: Sophos

Sie heißen Globe, Phantom, Tentacle, Tequila, Vbsmonopoly, Coconuta oder Mydoom. Wer eines der nebenstehenden Sujets schon einmal auf seinem Bildschirm hatte, erinnert sich mit Schrecken zurück. Sie sind nämlich allesamt höchst ansteckend – Computerviren und andere Schadprogramme. Der aktuelle Internet Security Threat Report von Symantec nennt derzeit einen Anstieg neuer Schwachstellen der IT-Sicherheit um 18 Prozent auf 2249, wobei fast zwei Drittel davon auf Web-Anwendungen entfallen.

Der Security-Anbieter Sophos fand im vergangenen Jahr 41.536 neue Schadprogramme und stellte eine zunehmende Globalisierung der Computerbedrohungen fest, denn fast ein Drittel der Programme stammt aus China, wo sowieso alles billiger produziert wird. Laut Sophos werden täglich rund 5000 Websites entdeckt, die schädliche Programmcodes enthalten. Da muss auch die Gegenseite aufrüsten.

Das zeigt sich massiv bei der weltgrößten IT-Messe Cebit, die bis 18. März in Hannover stattfindet. „Die Nachfrage nach Ausstellungsfläche im Security-Bereich der Cebit setzt sich kontinuierlich fort“, freuen sich die Veranstalter. Genügte für den Security-Themenkreis 2005 noch eine einzige Halle, so erstreckt sich die Cebit Security World 2007 bereits über zwei Hallen, und 2008 sollen es noch mehr werden. Mehr als 250 Aussteller aus der IT-Sicherheitsbranche präsentieren auf einer Fläche von 8500 Quadratmetern ihre Produkte und Lösungen bezüglich IT-Sicherheit.

Frauen surfen sicherer

Frauen sind beim Internet-Surfen übrigens deutlich vorsichtiger als Männer, ermittelte Symantec. Sie surfen zwar nicht viel weniger als Männer, doch nutzen sie das Web nicht so intensiv als Informationsquelle vor geplanten Einkäufen. Laut Symantec sucht knapp ein Fünftel der Männer im Internet nach Software, ohne dabei darauf zu achten, wie seriös die Quelle ist. Das ist dagegen nur bei sieben Prozent der Frauen der Fall. Sie laden zudem seltener Filme, Musik oder Software herunter, fast die Hälfte aller befragten Frauen sieht komplett von Downloads jeglicher Art ab. Sogar beim Shoppen ist das weibliche Geschlecht vorsichtiger. Nur ein Drittel gibt Kreditkartendaten in Online-Shops preis – mehr als die Hälfte der Männer hat damit keine Probleme. Dagegen aktualisieren nur rund 30 Prozent der Frauen regelmäßig die Programme auf ihrem Computer. Bei den Männern sind es doppelt so viele. 90 Prozent aller Anwender haben aber wenigstens ein Antivirenprogramm. Nur rund 48 Prozent besitzen Software gegen Spionageprogramme. Etwa 25 Prozent verfügen über keine Firewall.

Special Innovation

Keine Chance den Viren

Egal ob Kleinunternehmer oder Global Player: Wer von unliebsamen, zumeist kostspieligen Überraschungen verschont werden will, muss sein Computernetz vor externen und internen Bedrohungen schützen.

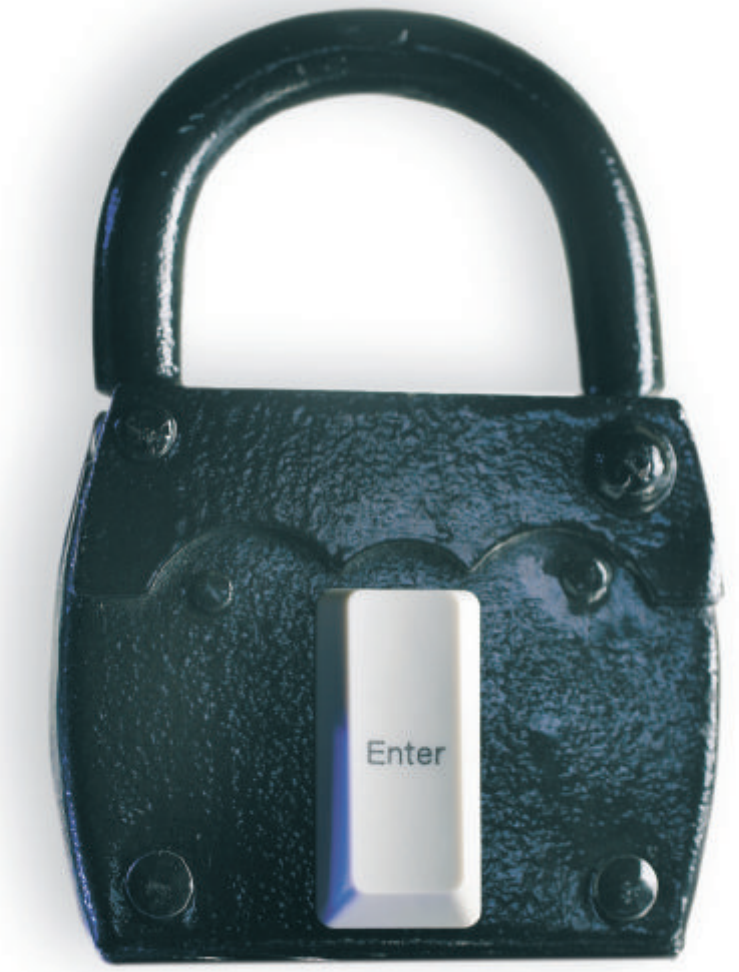
Sonja Gerstl

Unternehmensnetzwerke sind sensible Gebilde. Böswillige Attacken, Hacker-Aktivitäten oder auch fahrlässiges Handeln können Betriebssysteme empfindlich beeinträchtigen und immense Folgekosten verursachen. Geeignete Software kann alle Aktivitäten eines Netzwerkes überwachen sowie Auskunft über eventuell vorhandene Sicherheitslücken erteilen und entsprechende Gegenmaßnahmen setzen.

Die Basics hierfür sind jedem PC-User bekannt. Punkt 1: die Firewall. Jeder, der Zugriff auf das Internet hat oder mittels E-Mail mit anderen kommuniziert, braucht eine intelligente Firewall-Lösung. Das gilt selbstredend auch für die Absicherung von Netzwerken. Ein Firewall-System soll effektiv und leicht administrierbar sein. Punkt 2: Antivirus-Lösungen. Der lokale Virenschutz am Arbeitsplatz hat ausgedient, seitdem Mail Server und Server die bevorzugten Betätigungsfelder von Viren, Würmern und sogenannten Trojanischen Pferden sind. Die Software-Industrie offeriert jährlich neue Produkte, die einen umfassenden Schutz versprechen. Mitunter ist ein enormer infrastruktureller Aufwand notwendig, um in vernetzten Unternehmen Daten vor unerlaubten Zugriffen zu schützen. Viele IT-Security-Anbieter sind deshalb dazu übergegangen, Packages anzubieten, die neben konventionellen Sicherheitsfunktionen auch noch zahlreiche Goodies wie zum Beispiel Net Flow Analyzer, die eine permanente Kontrolle von Netzwerken garantieren, offerieren.

High-End-Lösungen

Die Angebotspalette reicht hierbei von Einsteigerapplikationen bis hin zu High-End-Lösungen mit Monitoring und automatischer Alarmierung. Darüber hinaus bietet der Markt auch All-in-one-Security-Lösungen, die effizienten Schutz vor externen und internen Bedrohungen gewährleisten. Vor allem interne Bedrohungen machen Betriebssystemen diversen Statistiken zufolge schwer zu schaffen. Demnach ereignen sich rund 80 Prozent der Vergehen gegen die IT-Security innerhalb des eigenen Datennetzwerkes. Nicht immer steckt Absicht dahinter. Oftmals ist es Unwissenheit oder Neugier, die Mitarbeiter die Grenzen des Systems austesten lassen. Damit derlei Experimentierfreudigkeit nicht massive Schäden anrichten kann, verfügen viele Firmen mittlerweile über ein Intrusion-Detection-System. Vergleichbar mit einer Alarmanlage, reagiert dieses unverzüglich bei Auffälligkeiten – also wenn etwa ein Mitarbeiter versucht, an Unternehmensdaten zu gelangen, für die er keine Zugriffsberechtigung hat. Automatisierte Reaktionen, die bis zur Blockierung der Anbindung des betreffenden Users an das Netzwerk reichen, sind die Folge.



Zugriffsberechtigungen für sensible Unternehmensdaten sollten sorgsam ausgestellt werden. Foto: Bilderbox.com

Viren & Würmer

Gezielt, effizient und zerstörerisch.

Viren, Würmer und Trojanische Pferde gehören zu den Schattenseiten des Computerzeitalters. Sie beschädigen Hardware, Software und Daten, belegen Arbeitsspeicher und deaktivieren Firewalls und Antivirenprogramme. Auch wenn Bedrohungen à la Sasser-Wurm vorerst gebannt sind – Entwarnung ist nicht angesagt. Um sich vor katastrophalen Folgen zu schützen, empfehlen Experten einen sorgsamen Umgang mit E-Mails unbekannter Absender. Darüber hinaus wird zu einem permanenten Update der Antivirus-Software geraten. Finger weg auch von Software-Programmen, die kostenlos zum Download angeboten werden – diese gelten als anfällig für Trojanische Pferde, also Computerprogramme, die wie nützliche Software aussehen, in Wahrheit aber Viren ins Netzwerk schleppen. Virenkarten (wie auf *www.de.trendmicro-europa.com*) informieren laufend über weltweit akute Bedrohungen. *sog*

Erhöhte Wachsamkeit ist angezeigt. Foto: Kapsch BusinessCom

Interne Verlustträger

Mitarbeiter stellen höchstes Sicherheitsrisiko für Firmen dar.

Als hätten sie nicht schon alle Hände voll damit zu tun, potenzielle externe Gefahren wie Hacker-Attacken abzuwehren, droht Unternehmen nun auch eine sukzessive Zersetzung von innen. Schuld daran haben der durchschnittliche europäische Mitarbeiter und sein allzu leichtfertiger Umgang mit vertraulichen Geschäftsdaten. Zu dem Ergebnis kam jedenfalls eine im Auftrag des IT-Sicherheitsunternehmens McAfee erstellte Umfrage. Demnach verlassen pro Woche und Mitarbeiter neun Dokumente gemeinsam mit ihren jeweiligen Sachbearbeitern das Büro. Meistens handelt es sich um Unterlagen zum laufenden Geschäftsverkehr, die auf elektronischem Wege oder auf Speichermedien wie USB-Sticks aus Unternehmen gelangen. Aber auch Kundendaten und Kundenakte werden gerne nach Hause mitgenommen. Dalibor Galic, Sales-Spezialist der Alcatel-Lucent AG: „Das höchste Sicherheitsrisiko ist der Mitarbeiter – ob absichtlich oder unabsichtlich sei dahingestellt." Vor allem die zunehmende und häufig unternehmensintern forcierte Mobilität ihrer Belegschaft mache Firmen immer mehr zu schaffen. „Oftmals werden Laptops, Handys und andere Datenträger gar nicht als Unternehmens-, sondern vielmehr als Privateigentum betrachtet", erläutert Thomas Blaschka, Head of Product Management bei Kapsch Business Com, die Problematik. Künftig, so ist man sich einig, müsse das Sicherheitsmanagement von Unternehmen verstärkt nach innen gerichtet sein. *sog*

Ein sorgloser Umgang mit Unternehmensdaten kann fatale Folgen haben. Foto: Kapsch BusinessCom

Beruf: Hacker

Experten decken Sicherheitslücken auf.

Aktive Datensicherheit ist allen Unternehmen wichtig. Nicht immer ist allerdings auf den ersten Blick ersichtlich, wie die bestehende Infrastruktur abgesichert werden kann, welche Daten und Applikationen geschützt werden müssen und wie das firmeninterne Netzwerk vor Missbrauch bewahrt werden kann. Abhilfe versprechen Security-Spezialisten, die Unternehmen bei der Erstellung, Umsetzung und dem Betrieb eines maßgeschneiderten Konzeptes unter die Arme greifen.

Risikoanalyse

Kapsch Business Com bietet als spezielles Security Service einen sogenannten Hack Check, der Sicherheitslücken in Netzwerken sichtbar machen soll. Dabei werden Komponenten wie Firewall, Mail Server oder Web Server überprüft. Kapsch dringt dabei von außen in das Netz des Kunden ein – agiert also wie ein „normaler" Hacker. Selbstverständlich erfolgt dieser „Angriff" in Abstimmung mit dem zu „hackenden" Unternehmen. Neben der technischen Überprüfung wird noch eine andere Form der Risikoanalyse angeboten. Hierbei wird zwecks Mängelaufdeckung physisch in das Unternehmen des Auftraggebers eingedrungen. Thomas Blaschka, Head of Product Management bei Kapsch Business Com: „Wir versuchen Dokumente, die eigentlich geshreddert werden müssten, aus Papierkübeln rauszufischen. Oder wir stehlen uns in Besprechungsräume, benutzen die Telefonanlage, aktivieren Computer und testen, wie weit wir an unternehmensinterne Daten herankommen können." Nur: So genau wollen es Österreichs Unternehmen anscheinend nicht wissen – die Nachfrage nach diesem Full-Service ist derzeit noch enden wollend. *sog*

Special Innovation

Thomas Blaschka: „Firmen sollten darauf achten, welche Informationen ihr Haus verlassen. Derzeit ist es so, dass Mitarbeiter via E-Mail alles wegschicken können. Das stellt ein großes Sicherheitsrisiko dar“, erklärt der Head of Product Management der Kapsch Business Com AG.

Das Pickerl für den Computer

Sonja Gerstl

economy: ***Wie sieht das Bedrohungspotenzial für Unternehmensnetzwerke grundsätzlich aus?***

Thomas Blaschka: Das jeweilige Bedrohungspotenzial ist stark vom Unternehmen und von dessen Umfeld abhängig. Insofern kann man keine verbindlichen Aussagen tätigen. Eindeutig feststellbar ist jedoch, dass die Angriffsszenarien nicht mehr willkürlich sind. Früher hat man gesagt: Da sitzt irgendwo ein junger enthusiastischer Mensch, der mit irgendwelchen Tools irgendwo einzudringen und dort Unruhe zu verbreiten versucht. Mittlerweile agieren Hacker und Co wesentlich zielgerichteter. Vor allem regional abgegrenzte Attacken werden immer häufiger.

Worauf haben Unternehmen in puncto Netzwerksicherheit zu achten? Gibt es spezielle Bereiche, die ganz besonders anfällig sind, wie etwa E-Mail?

E-Mail ist sicher ein großes Thema. Hier stellt sich die Frage, ob es nicht sinnvoll wäre, die private Nutzung von E-Mail – aber auch von Internet – einzuschränken. Eine weitere Frage wäre, inwieweit das Unternehmen darauf achtet, welche internen Informationen das Haus verlassen dürfen. Derzeit ist es so, dass Mitarbeiter via E-Mail alles wegschicken können. Das stellt natürlich ein gewaltiges Sicherheitsrisiko dar.

Zum Beispiel?

Der Mitarbeiter X kann beispielsweise Konstruktionspläne, Vertragsentwürfe und so fort an seine private Mail-Adresse schicken. Der Heim-PC steht aber auch allen anderen Familienmitgliedern zur Verfügung und ist darüber hinaus nicht entsprechend gesichert. Ich denke, es muss einfach gewährleistet sein, dass interne Dokumente da bleiben, wo sie hingehören. Selbiges gilt für Wechselmedien wie USB-Sticks oder externe Festplatten – aber auch iPods. Kaum einer achtet darauf, dass auch in diesem Fall die Daten verschlüsselt sein müssen. So ein USB-Stick geht leicht verloren oder wird irgendwo liegen gelassen. Nachdem diese Medien im Normalfall keinen Schutz haben, kann jeder die Daten, die sich darauf befinden, ganz leicht einlesen.

Welche administrativen Aufgaben und welchen zeitlichen Aufwand erfordert eigentlich eine angemessene IT-Security?

Es ist ein Irrglaube zu meinen: Ich kaufe mir jetzt so ein Teil, lasse es mir implementieren und damit hat sich die Sache erledigt. Natürlich gibt es Möglichkeiten, mit denen man die Administration bis zu einem gewissen Grad automatisieren kann. Regelmäßige Überprüfung ist aber dennoch unumgänglich. Ein Grundmonitoring sollte täglich gemacht werden, eine Re-Auditierung des Netzes sollte zumindest – je nach Größe des Unternehmens – pro Quartal beziehungsweise halbjährlich erfolgen. Mit seinem Auto fährt man ja schließlich auch einmal im Jahr zur Pickerl-Überprüfung.

www.kapsch.net

Das Informationszeitalter birgt eine Menge von Risiken. Sicherheit wird so zu einem wesentlichen Bestandteil von Firmennetzwerken. Foto: Kapsch BusinessCom

Steckbrief

Thomas Blaschka ist Head of Product Management der Kapsch Business Com AG.
Foto: Kapsch BusinessCom

Special Innovation

Christoph Riesenfelder: „Das Internet ist schlicht und ergreifend ein Spiegel der Gesellschaft. Betrug findet dort genauso statt wie auch im normalen Leben. Und zwar auf eine äußerst gefinkelte Art und Weise“, erklärt der Security-Spezialist von IBM Österreich.

Internet ist Vertrauenssache

Sonja Gerstl

economy: ***Welche Entwicklungen stellt IBM in seinem Global-Business-Security-Index-Report in Sachen Internet-Kriminalität für 2007 in Aussicht? Mit welchen akuten Gefahren sehen sich Unternehmen konfrontiert?***

Christoph Riesenfelder: Zwei Themenbereiche stehen hier ganz deutlich im Vordergrund oder weisen ein erhöhtes Risikopotenzial auf. Der eine ist der Bankensektor – und hier ganz speziell die Sparte Online-Banking. Der andere Themenbereich betrifft Ebay und andere Online-Auktionshäuser. Sowohl Banken als auch Online-Auktionshäuser haben zunehmend damit zu kämpfen, dass ihre Kunden mitunter massiven Sicherheitsbedrohungen und perfiden Attacken organisierter Internet-Kriminalität ausgesetzt sind. Daraus resultieren enorme Image-Probleme.

Wer trägt die Verantwortung für diese Angriffe?

Um beim Online-Banking zu bleiben: Hier stehen wir zunehmend vor der Problematik, dass die Sicherheitsverfahren, die beim Online-Banking in Österreich eingesetzt werden, mitunter nicht mehr dem Stand der Technik entsprechen. Es gibt natürlich Banken, die diesbezüglich sehr weit sind – andere wiederum weniger. Grundsätzlich muss man jedoch sagen, dass in der Regel die zumeist ungenügend geschützten Endgeräte der Kunden, und nicht etwa der Bankenrechner, zunehmend Ziel von organisierter Internet-Kriminalität werden.

Natürlich sind auch Banken gefordert, damit derartige Attacken möglichst vermieden werden können. Aber Phishing *(der betrügerische Versuch, per E-Mail den Empfänger zur Herausgabe von Zugangsdaten und Passwörtern zu bewegen, Anm.)* findet primär auf dem Privat-PC statt. Es gab eine Zeit, da haben Banken Schadenersatzforderungen von Kunden, die Internet-Betrügern aufgesessen sind, aus Kulanz heraus – und natürlich auch aus Angst vor Imageverlusten – Folge geleistet. Mittlerweile ist das nicht mehr der Fall.

Wie ist das nun bei Online-Auktionshäusern wie Ebay? Da sitzen ja quasi Anbieter und Kunden daheim vor dem Privat-PC.

Ebay ist ein interessanter Fall: Es operiert mit einem Geschäftsmodell, das darauf basiert, dass Kunden über diese Online-Plattform sicher und zuverlässig Auktionen tätigen können. Nun ist es aber so, dass das Vertrauen der Kunden in diese Plattform zunehmend abnimmt. Eben weil in letzter Zeit verstärkt schwere Mängel in Sachen Datensicherheit aufgetreten sind – etwa Attacken auf Kundenkonten. Kundenkonten wurden auch schon mehrfach erfolgreich geknackt. Auch die missbräuchliche Verwendung von Daten ist eine Gefahr, mit der sich Online-Auktionshäuser zunehmend konfrontiert sehen. Für Unternehmen, die ihr Business zu 100 Prozent via Internet tätigen, stellt das naturgemäß ein massives Problem dar. Diese Firmen riskieren, dass ihnen die Kundenbasis sukzessive abhanden kommt, wenn nicht massiv in die IT-Security investiert wird.

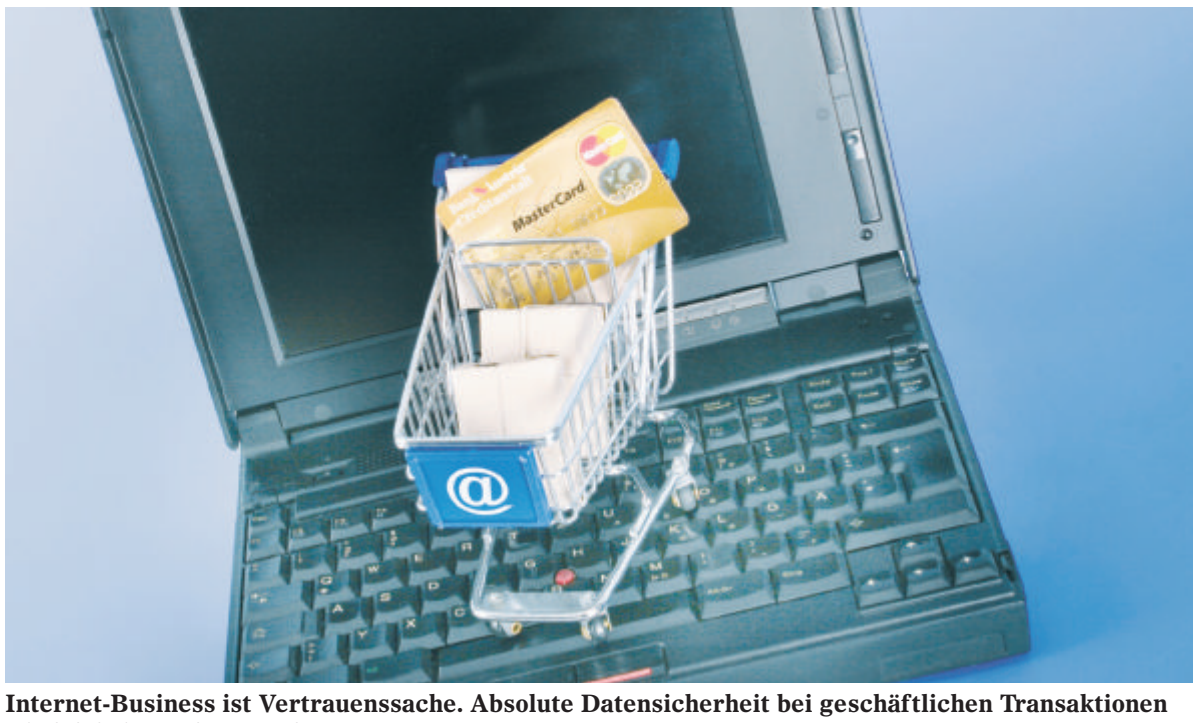
Naiv gefragt: Wie konnte es so weit kommen? Sind hier mittlerweile betrügerische Vollprofis am Werk, oder sind die Unternehmen in puncto Datensicherheit „schlampig“ geworden?

Eigentlich sind es keine Sicherheitslücken in der IT, die für diese Entwicklung verantwortlich zeichnen. Das Internet ist ein Spiegel der Gesellschaft. Betrug findet dort genauso statt wie im normalen Leben auch. Und zwar auf eine äußerst gefinkelte Art und Weise. Grundsätzlich unterliegen Transaktionen, die über das Internet stattfinden, einer eigenen Dynamik. Man sitzt allein vor dem Computer – hört nichts, spürt nichts, riecht nichts, empfindet nichts. Man sieht nur ein Bild, und diesem Bild muss man vertrauen. Darauf basieren Internet-Handel und Internet-Dienstleistungen. Ist dieses Vertrauen nicht da, dann macht man das auch nicht.

www.ibm.at

Steckbrief

Christoph Riesenfelder ist Security-Spezialist bei IBM Österreich. Foto: IBM



Internet-Business ist Vertrauenssache. Absolute Datensicherheit bei geschäftlichen Transaktionen wird dabei von den Kunden vorausgesetzt. Foto: Bilderbox.com

In vier Schritten zur sicheren Firma

Maßgeschneiderte IT-Security-Lösungen schützen Unternehmensdaten und Firmennetzwerke vor Zugriffen.

Kommunikation über das Internet birgt Gefahren, die vielfach unterschätzt werden. Vor allem bei Unternehmen, die via Internet mit ihren Kunden in Kontakt treten beziehungsweise Geschäfte abwickeln, muss eine umfassende Daten- und Netzwerksicherheit gewährleistet sein. Beim Einstieg in das Thema Internet-Sicherheit tut sich jedoch sehr schnell eine verwirrende Vielfalt von Konzepten und Lösungsstrategien auf. Wer den Überblick behalten will, muss strukturiert vorgehen. Für die Auswahl der richtigen Security-Politik bedarf es einer nüchternen Bestandsanalyse, exakter Planung und einer kompetenten Durchführung des Konzepts.

Branchen-Profis wie IBM empfehlen folgende Vorgehensweise. Phase 1: Entwickeln der Sicherheitspolitik. Entscheidend für das Gelingen ist eine klare Zuteilung der Zuständigkeiten. Im Idealfall ist es ein Sicherheitsmanagement-Team, das in weiterer Folge gemeinsam Ziele formuliert und die individuelle Sicherheitspolitik und -strategie festlegt.

Step by Step

Phase 2: Erstellen eines Sicherheitskonzepts. Sind die Ziele klar vorgegeben, geht es nunmehr darum, zu identifizieren, welche Unternehmensbereiche geschützt werden sollen. Christoph Riesenfelder, IT-Spezialist bei IBM Österreich: „Vielen Unternehmen ist im Endeffekt nicht wirklich klar, was sie eigentlich schützen wollen.“

Ein Sicherheitsmanagement-Team sorgt für die Umsetzung der unternehmensinternen IT-Security. Foto: Bilderbox.com

Nach Festlegung der relevanten Bereiche, die künftig via IT-Security vor Zugriffen geschützt werden sollen, der Wahl der hierfür geeigneten Software und einer umfassenden Kosten-Nutzen-Analyse, kann Phase 3 – Umsetzen des Sicherheitskonzepts – eingeläutet werden. Diese erschöpft sich jedoch nicht nur in der Implementierung des Programms oder der Programme. Ein ganz wesentlicher Aspekt hierbei ist auch die umfassende Schulung und Sensibilisierung der Mitarbeiter mit der neuen IT-Security. Ohne IT-Sicherheitsbewusstsein bei den Mitarbeitern, ist man sich in Fachkreisen einig, sind die Wirkungen technischer Maßnahmen unzureichend. Phase 4: Aufrechterhaltung des Sicherheitsniveaus. Daten- und Netzwerksicherheit kommt nicht ohne permanente Kontrolle und konsequente Updates der implementierten Programme aus. Schließlich verursacht Nachlässigkeit in diesen Belangen mitunter irreparable Schäden fürs Business. *sog*

Special Innovation

Sicherheit durch Identifikation

Chipkartenbasierte Zugangssysteme ermöglichen klare Rollenvergabe und sparen Zeit.

Ernst Brandstetter

Schutz für sensible Daten durch Chipkarten-Identifikation. Damit wird vermieden, dass es zu unterschiedlichen Rechteverteilungen in verschiedenen Systemen kommt. Zudem bleibt der Überblick über die Berechtigungen stets voll erhalten. Foto: Thiel Logistik

In großen Unternehmen geht es oft lustig zu, was die Computersicherheit betrifft: Passwörter werden einfach oder mehrfach verwendet, vergessen, notiert, verlegt, und oft weiß niemand mehr, wer Zugang haben darf oder nicht. Denn auch bei Benutzer-Accounts herrscht gerne Chaos, es gibt Dubletten, Sperren werden vergessen oder verschlampt, und die Benutzerstammdaten in unterschiedlichen Systemen sind nicht standardisiert. Eine Dokumentation über Änderungen ist meist nicht vorhanden oder hoffnungslos veraltet.

Der größte Schaden nach einem Sicherheitsvorfall in IT-Systemen liegt für Unternehmen im Verlust geschäftskritischer Daten, erklärten 82 Prozent der Befragten einer unter 100 IT-Experten erhobenen Untersuchung der deutschen Nationalen Initiative für Internet-Sicherheit (Nifis e.V.). Danach folgen der Ausfall produktiver Systeme (72 Prozent) und finanzielle Schäden, wobei 66 Prozent hier „teilweise“ und nur 14 Prozent mit einem klaren „Ja“ zustimmen. 63 Prozent der Unternehmen hatten im vergangenen Jahr Probleme mit der Informationssicherheit zu bewältigen.

Hinter dem Verlust geschäftskritischer Daten folgt an zweiter Stelle mit 72 Prozent der Stimmen die lange Ausfallzeit produktiver Systeme. Ein Ausfall der Produktivsysteme hat für die meisten Unternehmen weitreichende Konsequenzen, wenn dadurch Produktion oder Absatz nicht möglich sind. Mehr als die Hälfte der Fachleute (52 Prozent) sieht darüber hinaus im Imageverlust ein besonderes Problem. Wenn ein Sicherheitsvorfall in der Öffentlichkeit bekannt wird, kann der Folgeschaden infolge von Kündigungen seitens bestehender Kunden und fehlender neuer Geschäftsabschlüsse sogar liquiditätsbedrohend sein, so das Ergebnis der Umfrage.

Die Lösung sei ein professionelles Secure Identity Management (SIM), erklärt der Geschäftsführer der Raiffeisen Informatik Wilfried Pruschak. Eine Karte und ein Passwort ermöglichen dann den gesicherten, berechtigten Zugang zu allen firmeninternen Anwendungen. Das wird besonders bei sicherheitsrelevanten Bereichen oder bei Gefahr von unberechtigten Datenzugriffen immer wichtiger.

„Der Zugriff zu unternehmenskritischen Daten muss koordiniert, kontrolliert sowie gesichert ablaufen“, erklärt Pruschak, der aus Erfahrung weiß, dass „viele Unternehmen die Zutritts- und Zugriffsberechtigungen noch sehr undurchgängig managen.“ Das aber birgt hohe Sicherheitsrisiken, vor allem im Hinblick auf Informationssicherheit. Secure Identity Management von Raiffeisen Informatik steuert die Berechtigungen über eine einzige Karte mit Chip und in Verbindung mit einem Code. Damit können sich User auf allen Systemen, für die sie berechtigt sind, einloggen. Man muss sich dann auch nicht mehr für jede Applikation erneut anmelden. Verlässt man den Arbeitsplatz, wird die Karte aus dem Lesegerät entfernt, und alle Systeme sind automatisch vor fremdem Zugriff geschützt. Pruschak: „Das bringt zusätzliche Zeitersparnis in der Administration sowie Sicherheit im Unternehmen und bietet dadurch mehr Effizienz.“

Einfache Handhabung

Die einheitliche Administration derartiger Karten über standardisierte Workflows erleichtert zudem die User-Administration erheblich. Die Berechtigungsvergabe erfolgt funktionsbezogen über User-Rollen. Darüber hinaus profitiert das Unternehmen von der Protokollierung, Auswertung sowie Archivierung der Vergabe von User-Rechten und ist von diversen Routinetätigkeiten wie etwa dem Passwortrücksetzen entlastet. Für alle Typen von Mitarbeitern können bestimmte Rollen festgelegt werden, die zentral verwaltet werden.

Info

- **Secure Identity Management (SIM).** Die Kernfunktionalitäten von SIM bestehen aus Identity Management, einer Single-Sign-on-Lösung und Publik Key Infrastructure. Die SIM-Lösung vereinfacht Benutzerverwaltungsprozesse erheblich und dient als zentrales System für benutzerrelevante Daten. So werden einerseits Kosteneinsparungen in der Administration erzielt, andererseits der Sicherheitsstandard auf aktuellem Stand gehalten.

- **Identity Management (IM).** IM ermöglicht den richtigen Personen zur rechten Zeit den gesicherten Zugang zu Applikationen, Ressourcen und Daten.

- **Public Key Infrastructure (PKI).** Als Kern der Sicherheitsinfrastruktur kommt PKI zum Einsatz. Sie ermöglicht mittels User-Zertifikaten eine Authentifizierung über die Karte und zusätzlich über ein Passwort. Weiters bietet dieses System die Basis für die Bereitstellung von Zertifikaten, welche für Sicherheitsfunktionen wie Vertraulichkeit, Integrität und Nicht-Abstreitbarkeit von diversen Applikationen genutzt wird.

- **Single-Sign-on.** Mit einem Log-in können alle Systeme genützt werden, zu denen man zugangsberechtigt ist. Das verbessert die Bedienungsfreundlichkeit der IT-Systeme für Anwender, weil sich Mitarbeiter für alle angebundenen Systeme nur einmal authentifizieren/anmelden müssen.

Steckbrief

Wilfried Pruschak ist Geschäftsführer der Raiffeisen Informatik GmbH.
Foto: Raiffeisen

Special Innovation

Sicheres Zahlen entscheidet

Neue Systeme für das rasch wachsende digitale Business legen die Basis für weiteres Wachstum.

Ernst Brandstetter

Johann Nestroy würde dazu wahrscheinlich „Die Welt steht auf kein' Fall mehr lang" sagen, denn der Fortschritt der digitalen Systeme ist offensichtlich unaufhaltbar. Seit 1. Februar zahlt sogar das Bundesheer seinen Präsenzdienern auf Wunsch den Sold bargeldlos aufs Konto und liefert die Chipkarte dazu. Die 176,84 Euro können mit einer eigenen Karte und maximal vier kostenlosen Bargeldbehebungen am Bankomaten, vier Bezahlungen an Bankomat-Kassen und vier Guthabensabfragen per Telefon oder Internet gratis umgesetzt werden.

Mit 440 Mio. Transaktionen über Produkte von Europay Austria haben die Österreicher 2006 insgesamt Zahlungen von 16,1 Mrd. Euro abgewickelt. Das Gesamttransaktionsvolumen betrug sogar 35,1 Mrd. Euro. Rekordtag war der 22. Dezember mit mehr als zwei Mio. Transaktionen, einem Viertel mehr als dem Spitzenwert des Vorjahres.

Sicherheit spielt bei dieser Entwicklung eine enorm wichtige Rolle, erklärt Europay-Prokurist Walter Bödenauer, als Bereichsleiter zuständig für Sicherheit, Inkasso und Reklamationen. „Wenn ein Verfahren nicht sicher ist, hat man auch keine Kunden", beschreibt er das Umfeld. Bargeldloses Zahlen mit Karte und Code und der dazugehörenden technischen Infrastruktur mit intelligenten Terminals ist seiner Ansicht nach völlig sicher, „wenn der Kunde sich an die Geheimhaltung der Daten hält."

Gut abgesichert ist auch der Datenverkehr mit den Terminals und zu den Geldinstituten. Bödenauer: „Die Datenübertragung ist verschlüsselt, und wir kennen auch nicht die Daten der Kunden, sondern nur die Code-Daten der Karten. Nur die jeweilige Bank kann dann Kartendaten und Kundendaten zusammenführen." Was heute in den Systemen angewandt wird, so Bödenauer, ist „State of the Art".

Neue Dimensionen

Als Vorstoß in neue Dimensionen bezeichnet Bödenauer die Erhöhung der Sicherheit beim Bezahlen im Internet. Ist doch das E-Commerce-Geschäft 2006 laut Europay im vergangenen Jahr um 20 Prozent gestiegen und auch heuer eine Steigerung in ähnlichem Ausmaß zu erwarten. Wenn Unternehmen hier keine Sicherheitsprüfung anbieten können, drohen damit steigende Schäden durch Betrug. Mit Secure Code biete Europay jedem Unternehmen die Möglichkeit, jeden Kunden auf der ganzen Welt zu erreichen und dennoch die gleiche Sicherheit beim Bezahlen zu haben wie von Angesicht zu Angesicht. Firmen, die Secure Code nützen, können registrierte Kartenin-

Doppelt sicher: Das Bundesheer schützt die Grenzen und sorgt sich um sichere Zahlungsformen für die Grundwehrdiener. Foto: Bilderbox.com

haber problemlos akzeptieren. Bödenauer: „Damit ist eine zentrale Prüfung möglich, und die Zahlung auf digitalem Weg hat den gleichen Wert wie eine Unterschrift." Über einen eigenen Secure Code kann zudem sichergestellt werden, dass der Kunde nicht nur registriert ist, sondern sich auch selbst im Besitz der Karte befindet. Größter Vertragspartner von Europay bei diesem System sind derzeit die Österreichischen Lotterien.

Umfassende Alarmsysteme

International kommunizierendes Monitoring-System löst Warnsignal aus, wenn Duplikatskarten verwendet werden.

Die seit 1995 mit einem Chip ausgestattete Maestro-Bankomatkarte entspricht dem höchsten technischen Sicherheitsniveau, das derzeit international für den kartenbasierten Zahlungsverkehr zur Verfügung steht. In Österreich werden sämtliche Maestro-Transaktionen bereits seit Mitte der 90er Jahre am Bankomaten sowie an der Bankomatkasse mit Code über den Chip der Karte abgewickelt. Der Chip gilt als absolut sicher und nicht kopierbar, weil Kartenduplikate nur auf Magnetstreifendaten basieren und an österreichischen Bankomaten und Bankomatkassen nicht einsetzbar sind. Bei ausländischen Transaktionen erkennt ein international kommunizierendes Monitoring-System umgehend, wenn eine Duplikatskarte verwendet wird, und schlägt Alarm.

Bei ausländischen Transaktionen erkennt ein Monitoring-System, wenn eine Duplikatskarte verwendet wird, und schlägt Alarm. Foto: Bilderbox.com

Standardisierte Technologie

Seit 2003 setzt Europay Austria in der Chiptechnologie auf den internationalen Standard EMV (Europay, Master Card, Visa), der gemeinsam von den internationalen Zahlungsverkehrsgesellschaften Master Card, Europay International und Visa entwickelt wurde. Auf Basis dieses Standards wird künftig weltweit jede EMV-Zahlungskarte mit jedem EMV-kompatiblen Terminal Informationen austauschen können. Verwendung finden dabei Mikroprozessoren der allerneuesten Generation, die zusätzlich mit einem kryptografischen Ko-Prozessor ausgestattet und somit in der Lage sind, sowohl RSA als auch andere Algorithmen wie Elliptic Curves zu rechnen. Konsumenten empfiehlt Europay dennoch zusätzliche Vorkehrungen.

Dazu gehören die Geheimhaltung des Codes und die regelmäßige Kontrolle der Kontoauszüge. Die eigene Bankomatkarte samt Code sollte man niemand anderem zur Verfügung stellen. Anfragen, bei denen der Code mitgeteilt werden soll, werden von den Banken niemals gestellt und sollten daher nicht beantwortet werden. Die Codes sollen auch an keinen anderen Geräten als an den Bankomaten und offiziellen Terminals eingegeben werden. *bra*

Das Special Innovation entsteht mit finanzieller Unterstützung von ECAustria. Die inhaltliche Verantwortung liegt bei *economy.*

Redaktion:
Ernst Brandstetter