

communicate!

2/2011



Sind Sie schon im Netz gefangen?

Von Netzwerken, Würmern und Sicherheiten.



- 2 **Editorial von Peter Kulmbrein**
Es hat sich ausgegurt.
- 3 **Surreale Welt der IT-Sicherheit**
Wokurka und der begabte Nachwuchs
- 5 **Jörg Hofmann im Interview:**
„Mobilität ist für Unternehmen ein strategischer Imperativ.“
- 9 **Auf zum Angriff, fertig, los!**
Glossar einiger perfider Begriffe
Sicheres Passwort? %xlr*\$PASS+W
BYOD – what?
- 10 **Mobile Devices – ein Sicherheitsleck in Unternehmen?**
- 11 **Alles Denkbare ist auch machbar.**
Televis setzt Netzwerkkonzept um.
- 15 **Haben wollen!**
Blühender Schwarzmarkt für Kreditkarten und Bankdaten
- 16 **Was ist denn bloß ... SPAM?**
- 17 **Service? Bitte sehr!**
Gestatten, wir sind Standort Salzburg!
- 18 **Gewinnen!**
Frage beantworten und in die Steiermark fahren.



Das nächste „**communicate!**“ erscheint am 06.10.2011 und beschäftigt sich mit der Frage, was zum perfekten Kundenservice gehört, wie Callcenter kundenfreundlich aufgebaut sein müssen und ob Kundenbetreuung auch über Social Media möglich ist.

Wenn Sie auch weiterhin kein „communicate!“ versäumen möchten, können Sie jetzt kostenlos ein Abonnement per E-Mail an marketing@televis.at bestellen. Über Feedback zu unseren Artikeln freuen wir uns immer. Schreiben Sie uns, was Sie von unserem Kundenmagazin halten – oder in Zukunft noch alles erwarten: marketing@televis.at

Impressum:

communicate!
DAS KUNDENMAGAZIN VON TELEVIS

Herausgeber, Medieninhaber und Verleger: Televis Telekommunikation und Service GmbH, 1120 Wien, Altmannsdorfer Straße 76, Tel.: 05/08787 0, Fax: 05/08787 8500, E-Mail: office@televis.at, Homepage: www.televis.at, FN 330634b ATU65104335

Konzept, Redaktion: atello verlag gmbh, 1010 Wien, Fischhof 3/6, E-Mail: verlag@atello.at, Homepage: www.atello.at.

Druck: Friedrich VDV, Vereinigte Druckereien- und Verlags-GmbH & CO KG, Zamenhofstraße 43-45, 4020 Linz, E-Mail: office@friedrichvdv.com, Homepage: www.friedrichvdv.com

Nachdruck von Texten, Bildern, Zitaten und Anzeigen, auch nur auszugsweise, nur mit ausdrücklicher schriftlicher Genehmigung des Medieninhabers. Für Satz- und Druckfehler wird keine Haftung übernommen. Coverfoto: shupian

Es hat sich ausgegurkt.



Foto: David Sailer

Die Gurke ist seit letztem Monat wohl das prominenteste Sicherheitsrisiko. Kurzfristig im Ranking von den Sojasprossen überholt, die aber nachhaltig nicht bestehen konnten. Unappetitliche Geschichte. Der Mai war in vielerlei Hinsicht ein riskanter Monat, aber die Gurke rückte einiges in den Hintergrund. Sony musste zugeben, dass sich Angreifer unbemerkt Zugriff auf Daten von hundert Millionen Mitgliedern des Playstation-Netzwerkes verschaffen konnten, darunter auch eine Datenbank mit Kreditkartendaten. Ungute Geschichte. Einige Tage darauf folgte eine Cyber-Attacke gegen den amerikanischen Rüstungskonzern Lockheed Martin – den größten Auftragnehmer des US-Militärs. Beteuert wurde hoch und heilig, dass man sich wehren konnte, bevor Daten geklaut wurden. Beunruhigende Geschichte. Der IT-Sicherheitskonzern RSA muss Millionen Passwort-Anhänger tauschen, nachdem schwere Sicherheitsprobleme eingestanden wurden. Die so genannten „SecurID“-Tokens werden von rund 40 Millionen Nutzern verwendet, darunter befinden sich auch Rüstungskonzern und Regierungsbehörden. RSA wurde im März selbst Ziel von Cyberkriminellen, die offenbar wesentliche Informationen stehlen konnten. Ein Zusammenhang zwischen dem RSA-Zwischenfall und dem Angriff auf Lockheed Martin wird in den Raum gestellt. Fast schon ein wenig verspielt mussten Hacker gewesen sein, die Anfang Juni den Spielkonsolenhersteller Nintendo in die Mangel genommen haben. Geklaut wurden angeblich Million Datensätze inklusive Passwörter. Super Mario in Gefahr? Nein, wir sollten über diese Geschichte nicht lachen, obwohl die vermeintlichen Angreifer – eine Gruppe unter dem Pseudonym LulzSec (ausgeschrieben „laughing at your security“) – das wahrscheinlich tun. Es geht weiter: Millionen von Neckermann-Daten gestohlen, Cyber-Gangster hackten Morgan Stanleys Netzwerk; Rechner der EU-Kommission unter Beschuss; Googles Passwort-System gestohlen; Hacker klauen australische Regierungsmails; Elite-Hacker führen Cyberwar für China und USA wollen Hackerangriffe zum Kriegsgrund erklären.

Alle Meldungen führen nicht unbedingt zu einem besseren Sicherheitsgefühl. Und dennoch glauben wir nicht daran, dass sich irgendeiner dieser in höchsten Kreisen tätigen Hacker für unser Unternehmen interessieren könnte. Viel zu klein, viel zu unwichtig, keine Pläne für den Bau von Kampfjets gespeichert. Denkste! Laut Schätzungen von IBM werden täglich 13 Milliarden digitale Attacken auf private Rechner und Unternehmensnetzwerke verübt. Welcher Schaden dabei angerichtet wird, lässt sich nicht genau errechnen, manche Analysten sprechen von 70 Milliarden Euro, andere sogar vom Zehnfachen. Microsoft veröffentlichte jüngst im „Security Intelligence Report“, dass neun von 1.000 Rechnern im zweiten Halbjahr 2010 infiziert waren. Ob aufgrund von Lücken im System, Viren, Würmern und Trojanern oder aufgrund des Leichtsinns der Mitarbeiter – Sie sollten die Attraktivität Ihres Unternehmens für Cyberkriminelle nicht unterschätzen und Ihr Netzwerk absichern.

In unserem Kundenmagazin werden Sie erfahren, welche Anforderungen moderne Netzwerke erfüllen müssen, wieso mobile Devices die Datensicherheit von Unternehmen bedrohen und wie der Hightech-Produzent EV Group ein redundantes Netzwerkkonzept umsetzen konnte.

In diesem Sinne: Meiden Sie potenzielle Gefahrenquellen, vertrauen sie keiner Gurke und haben Sie einen schönen Sommer. Wir freuen uns jetzt schon, wenn Sie im Herbst wieder im communicate! lesen.

A handwritten signature in black ink, appearing to read 'Peter Kulmbrein'. The signature is stylized and fluid.

Mag. Peter Kulmbrein
Geschäftsführer

Surreale Welt der IT-Sicherheit

Trojaner und Würmer sind kein Streichelzoo und der Love-Virus keine Liebeserklärung.

Gleich vorweg: Es gibt keinen Königsweg und kein Wundermittel für eine hundertprozentige und ewige Sicherheit. Sicherheit ist auch kein einmaliger Prozess, sondern eine permanente Herausforderung. Dazu noch komplex und nicht umsonst.

Der Love-Virus demonstrierte vor vielen Jahren allorts, wie verwundbar die digitale Welt ist. Blitzartig hat er sich vermehrt und einen Schaden in Milliardenhöhe hinterlassen. Klick, Doppelklick und schon war das Desaster perfekt. Und das trotz des liebevoll klingenden Namens. Dabei soll der Virus nicht einmal besonders heimtückisch gewesen sein, zumindest war ein wirksames Gegenmittel rasch gefunden.

Schadprogramme – wie Viren (=Programme, die ihren Programmcode in fremde Programme einfügen, Schaden anrichten und sich durch Selbstreplikation oder Kopiervorgänge verbreiten), Würmer (=Viren, die sich selbst auf andere PCs verschicken und befallene Rechner arbeitsunfähig machen), Trojaner (= Programme, die sich als nützliche Anwendung ausgeben, aber unbemerkt eine andere schädigende Funktion erfüllen) oder Spyware (=Programme, die heimlich Daten eines Nutzers sammeln und an Hersteller der Software oder Dritte weitergeben) – erscheinen in immer kürzeren Entwicklungszyklen und in „optimierten“ Varianten. Nicht nur Würmer sind wieder im Kommen, schreibt der österreichische CERT-Internet-Sicherheitsbericht 2010. Gefälschte Antivirus-Software ist ebenso auf dem Vormarsch und auch Phishing (=ein Angriff, bei dem der Nutzer per E-Mail über vertrauliche Daten ausge-

fragt wird) ist nicht totzukriegen. Die zunehmende Komplexität der Netzwerke und der Trend zur verteilten Arbeitsumgebung machen das Beschützen der Daten zu einem regelrechten Kraftakt.

Es gibt kaum präzise Zahlen über die weltweite Gesamtverseuchung des Internets. Laut dem „Security Intelligence Report“ von Microsoft, der zweimal jährlich publiziert wird, sind in Österreich drei von insgesamt 1.000 Rechnern infiziert. Weltweit sind es neun Rechner, weshalb Österreich in Bezug auf Botnetze und Malware generell als eher sauber einzustufen ist. Im Fall von Cornficker (=auch als Downup, Kido und Worm.Win32/Conficker bezeichnet, ein Computerwurm, der mit dem Betriebssystem Microsoft Windows ausgerüstete Computer infiziert) sind laut Schätzungen rund 12.000 Rechner mit der Version A. oder B. und rund 300 mit der Version C. infiziert. Ein besonders aggressiver Wurm, der erstmals 2008 aufgetaucht ist und hierzulande bekannt wurde, als er im Januar des darauffolgenden Jahres 3.000 PCs der Kärntner Landesregierung lahmlegte.

Irgendwo draußen sitzen also Menschen, die Malware programmieren und die digitale Welt lahmlegen, Informationen stehlen oder Zugangsdaten ausspionieren. In Malware stecken böartige Softwarecodes, sie ist ein Überbegriff für all die Viren, Trojaner, Würmer, Exploits und sonstige Schadprogramme. Doch politisch motivierte Hackeraktionen oder kreative „Robin Hoods der Wissensgesellschaft“, die eine gewisse Hacker-Ethik (Wissen ist Macht, aber Machtausübung ist Machtmissbrauch) befolgen, sind vereinzelt anzutreffen, vielmehr geht es heute um organisiertes Verbrechen, das zu einem sehr lukrativen Massengeschäft geworden ist. Dabei ist der digitale Untergrund immer



auf der Suche nach besonders leichter Beute. Die Gefahr droht vielerorts. Sie kommt aus sozialen Netzwerken, wo die sorglose Klickmentalität zu schneller Verbreitung von Viren sorgt. Trügerische Weblinks werden beispielsweise über Konten von Facebook-Freunden versendet, wer dem Link folgt, liefert seine Daten ab oder fängt sich einen Trojaner. Gefährdet ist man aber nicht nur auf dem eigenen Rechner, sondern überall dort, wo persönliche Daten hinterlassen werden. Die Mehrzahl der erfolgreichen Angriffe kommt aus dem Inneren der Unternehmen. Die größte Sicherheitslücke sitzt also vor dem Computer.

Social Hacking lautet der Fachbegriff, wenn die Sicherheitslücke Mensch ausgenutzt wird. Die Angreifer schaffen ein Vertrauens- oder Respektverhältnis zum potenziellen Opfer, das dann nicht einmal merkt, dass es gerade Informationen preisgegeben hat. Ein Massenphänomen ist Phishing. Eine E-Mail, in der vermeintlich eine Bank oder ein anderer Diensteanbieter Benutzerdaten oder Kontonummern abfragt. Andere Methoden laufen per Telefon ab, wo gezielt Informationen gesammelt werden, um Schwachstellen von Unternehmen aufzudecken. Der Zweck ist unterschiedlich: Industriespionage, Erpressung oder Business. Oder vielleicht auch persönlich motivierte Rache?

Wenn von der Sicherheitslücke Mensch die Rede ist, geht es um Anwenderfehler und den sorglosen Umgang mit Daten. Sei es eben das Herunterladen von Apps oder das Öffnen von unbekanntem Anhängen, das Speichern von Unternehmensinformationen auf externen Festplatten, unzureichend gesicherte Verbindungen, verlorene oder gestohlene Geräte. Die Mitarbeiter werden immer mobiler und Unternehmensdaten dadurch zu virtuellen Nomaden. Das Zugangspasswort muss heute nicht einmal am Bildschirm kleben.

Die Gefahrenliste ist schier unendlich. Deshalb brauchen Unternehmen nicht nur Sicherheitssoftware, sondern ein wirksames Sicherheitskonzept, das die

Mitarbeiter einbezieht und deren Bewusstsein schärft. Und die beste Hard- und Software gewährleistet nicht automatisch Sicherheit, wenn sie nicht laufend gewartet, aktualisiert und konfiguriert wird.

Fazit: Wir leben gefährlich. Dennoch: Kein Grund, paranoid zu werden.

Wokurka und der begabte Nachwuchs:

Der abgeschlossene Kurzroman.



Foto: Dennis Cox

„Was Hänchen nicht lernt, lernt Hans nimmermehr,“ dozierte Kommerzialrat Roderich Wokurka und ließ den Blick über die gerahmten Ehrenurkunden an seiner Bürowand schweifen. „Was ein Häkchen werden will, krümmt sich beizeiten. Und ... – hörst du mir überhaupt zu, Bub?“

Nein. Er hörte nicht zu. Im Besuchersessel lümmelte ein in Tiefschwarz gehülltes, knapp 1,90 langes, pickeliges Elend und tippte unablässig in ein fabrikneues iPhone. Kevin Wokurka war alles andere als der Enkel, den sich der rührige Speditionsgründer erträumt hatte.

„KEVIN! Jetzt legst du diesen Apparat weg und hörst mir zu!“

„Gleich, Opa!“

„JETZT! DALLI! Du bist noch keine 17 und eben von der dritten Schule geflogen, Bub! Wie soll das enden?“

„Gib mir deine Banane, du wilder alter Silberrücken.“

„Dir fehlt jedes Talent für ... – WAS hast du gerade gesagt?“

„Gib mir deine Banane, schreibt dir da so eine urpeinliche Tussi: nadine@total.org.ru. Wer ist das, Opa?“

Wie bezeichnen wir den Farbton, den Roderich Wokurkas Gesicht spontan annahm? Schlaganfall-Lila? „Wo hast du diese E-Mail her?“

„Aus deiner Mailbox. Ich schau mich grad bisserl in deiner Firma um.“

„WIE BITTE?“

„Jetzt bin ich im Ordner Sonderzahlungen. Sag, du schickst 100.000 Euro an den Minister, äh ...“

„Bub! Wie kannst du meine geheimsten ...“

„Is ureinfach, Opa. Das Passwort fürs Firmennetzwerk ist der Name von der Oma, das Passwort für deine Kiste ist der Name von der Mama und brauchen tät ich's gar nicht, weil eure Firewall ist ein Sieb. Da ist die von unserer Schule besser und trotzdem schau ich immer die Aufgaben von der nächsten Mathearbeit nach.“ Wäre Wokurkas für seine 62 Lenze erstaunlich komplette Haarpracht nicht längst schlohweiß gewesen – sie wäre es jetzt geworden. Eine Schweißperle turnte von seiner Augenbraue und lief dann langsam sein Brillenglas hinab.

„Unsere IT hat ein Vermögen gekostet und du kannst einfach mir nichts, dir nichts ...?“

„Naja – installiert habt ihr sie, wart mal, am 16. Juni 2006 und das letzte Update war, Moment... – Uuuuuuh! Spare in der Zeit, dann hast du in der Not, gell, Opa?“

„Kevin?“

„Ja, Opa?“

„Könntest du dir vorstellen, mit der Schule aufzuhören und mein Sicherheitsbeauftragter zu werden?“

„Klingt gut. Aber andere Frage ...?“

„Was denn?“

„Was ist das eigentlich – ein Silberrücken?“

„Mobilität ist für Unternehmen

Jörg Hofmann, Country Manager von Extreme Networks, im Interview: Über den Fünf-Jahres-Plan des Netzausrüsters, die Mobilität als Zukunftstrend und das Sicherheitsrisiko von innen eines Unternehmens.

Extreme Networks

Der Netzausrüster mit Headquarter in Santa Clara, Kalifornien, wurde 1996 gegründet, ist weltweit in 50 Ländern vertreten und beschäftigt inzwischen über 1.000 Mitarbeiter. Extreme Networks entwickelt und vertreibt konvergente Ethernet-Netze, die Unternehmen und Service-Providern die Übertragung von Daten, Sprache und Video ermöglichen. Das Produktportfolio des Herstellers umfasst drahtgebundene und drahtlose Infrastrukturkomponenten. Hierzu zählen sichere LAN-Ausstattung, Rechenzentrumsinfrastruktur und Ethernet-Transport-Lösungen für Service-Provider, ergänzt durch einen globalen, 7x24 verfügbaren Support.

Extrême Networks liefert hochperformante und hochverfügbare Netzwerklösungen. Weltweit tätig, rasant gewachsen und laut firmeneigenen Angaben seit der Gründung 1996 über 25 Mio. Ethernet-Ports an Kunden ausgeliefert. Wenn wir Ihre Referenzliste auf Österreich einschränken, wen werden wir vorfinden?

Der größte Kunde ist sicherlich das Bundesministerium für Inneres. Es folgen Land Tirol, einige Stadtwerke, Wasserwerke oder auch die Graz AG. Generell sind unsere Kunden in allen vertikalen Marktsegmenten zu finden, obwohl wir in Österreich derzeit sicher eine Stärke im Verwaltungsbereich vorweisen können.

In welchen Märkten gibt es global gesehen die größten Wachstumsbereiche?

Geografisch gesehen ist die EMEA-Region der stärkste Markt für Extreme Networks, was für einen amerikanischen Konzern eher ungewöhnlich ist. Wir sind beispielsweise in der Schweiz und in Österreich innerhalb der letzten zwei Jahre um fast 100 Prozent gewachsen. Lösungsspezifisch gesehen ist die gesamte Bandbreite von Cloud Computing das dominante Thema und in diesem Bereich erwarten wir auch die größten Wachstumsraten.

Zu Ihren Mitbewerbern zählen globale Player, wie Cisco oder HP. Im Vergleich zu denen ist Extreme Networks ein kleines Unternehmen. Wie können Sie sich differenzieren?

Wir sind im Vergleich klein, aber stark auf unsere Kernkompetenz fokussiert. Durch unsere Größe und unser Vertriebssystem sind wir extrem flexibel und haben gleichzeitig die Möglichkeit, Unternehmensnetzwerke wesentlich kostengünstiger zu betreiben. Insgesamt ist der Markt von einer hohen Konsolidierung geprägt, was uns in eine ziemlich spannende Position bringt, weil wir heute der einzige reine Netzerkäufer sind. In diesem Punkt verfolgen wir einen komplett anderen Ansatz als Cisco oder HP, die ihre Lösungen vom Server über Netzwerk bis hin zum Telefon in einem Paket anbieten und vorgeben, dass nur dann alles perfekt funktioniert, wenn es von einem Anbieter kommt. Das stimmt nicht und wurde schon mehrfach widerlegt. Für Unternehmen ist es wesentlich effizienter, wenn sie sich aussuchen können, was für sie das Beste ist.

Welche Vision verfolgt Extreme Networks?

„Make your network mobile“ – das ist unsere Vision. Die Mobilität ist der ultimative Zukunftstrend und für Unternehmen ein strategischer Imperativ, seit sie wollen, dass ihre Mitarbeiter mobil sind. Im nächsten Jahr werden zum ersten Mal mehr Tablets und Smartphones verkauft als Desktops und Notebooks. Aber auch die Applikationen und Anwendungen werden mobil. In den Unternehmen verändern sich die Arbeitsweisen und für Netzwerkadministratoren ist das natürlich ein Albtraum, wenn alles in Bewegung ist. Auf

ein strategischer Imperativ.“





Links: www.extremenetworks.com

Jörg Hofmann (44)

Seit 2009 ist er Country Manager des amerikanischen Netzwerkausrüsters Extreme Networks und für den Ausbau der Vertriebsaktivitäten sowie die Betreuung der Partner, Distributoren und Endkunden im österreichischen und Schweizer Markt verantwortlich. Jörg Hofmann verfügt über langjährige Branchenerfahrung im IT- und Telekommunikationsmarkt, war unter anderem bei Netbeat, Getronics und 3Com als Sales Manager tätig, 2004 wechselte er in die Funktion des Managing Directors zu Avaya Switzerland und von 2006 bis 2009 verantwortete er als Country Manager die Entwicklung der Dimension Data AG. Der zweifache Vater studierte an der Fachhochschule in Bern und wohnt in Münsingen, Schweiz.

diese Entwicklungen und Anforderungen müssen wir reagieren. Die Vision, die wir verfolgen, ist, dass mein Unternehmensnetzwerk mich in dem Moment erkennt, wenn ich mein Notebook einschalte. Dann soll ich als Jörg Hofmann erkannt werden, das Netzwerk soll automatisch die Verbindung herstellen und den Zugriff auf die Applikation ermöglichen, die ich laut Berechtigung auch verwenden darf.

Wann wird die Vision zur Realität?

Wir haben eine Fünf-Phasen-Strategie. Im Moment befinden wir uns in der Phase zwei bis drei und es wird in etwa fünf Jahre dauern, bis die Umsetzung abgeschlossen ist. Wir benötigen komplett neue Standards im Bereich der Mobilkommunikation, denn der mobile Datenverkehr wird sich verzehnfachen.

Was ist die größte Herausforderung bei der Verwirklichung dieser Strategie? Das Thema der Sicherheit oder das Herunterbrechen der Komplexität?

Sicher die Komplexität und das Zusammenspiel der verschiedenen Technologien. Ich glaube, technologisch ist die Verwirklichung nicht das Problem, die Herausforderung liegt in der Definition der Standards, die dann von den Herstellern eingeführt werden müssen.

In Zukunft haben Mitarbeiter nur ein mobiles Device, das die gesamte Kommunikation bündelt.

Und vor allem wird der Mitarbeiter ein Gerät haben, das ihm am besten entspricht. Jahrzehntlang haben Unternehmen standardisiert und einheitliche Notebooks oder Mobiltelefone an die Mitarbeiter ausgehändigt, ohne berücksichtigt zu haben, ob der einzelne Benutzer unbedingt auch jenes Gerät bekommt, mit dem er am effektivsten arbeitet. Heute geht der Trend in die umgekehrte Richtung. Die Unternehmen kaufen das Equipment nicht mehr standardmäßig, sondern der Mitarbeiter soll das bekommen, was er möchte. Für die IT-Infrastruktur wird es zwar komplexer, für die Benutzer umso einfacher.

Wie vertragen sich Mobilität und Datensicherheit?

Sicherheit hat einen sehr hohen Stellenwert. Mit unserer „Make your network mobile“-Strategie interpretieren wir das Netzwerk-Betriebssystem anders und erkennen in dem Moment, in dem Sie sich im Netzwerk anmelden, wer Sie sind und welche Rolle Sie innerhalb des Unternehmens haben. Entsprechend Ihrer Rolle wird das Netzwerk dynamisch mit entsprechenden Priorisierungen für Sie konfiguriert. Wir gehen sicherheitsmäßig einen großen Schritt weiter, als es andere Mitbewerber tun.

Fakt ist, es gibt keine absolute Sicherheit.

Nein.

Mit Sony hatten wir einen aktuellen Fall von fehlender Sicherheit bei sensiblen Unternehmensdaten. Wie können solche Fehler einem so großen Unternehmen passieren?

Das ist eine gute Frage. Dass gerade einem technologieaffinen Konzern, wie Sony, so etwas passiert, ist für mich eigentlich nicht nachvollziehbar. Auch wenn der Aufwand groß ist – es ist absolut machbar, für entsprechende Sicherheit zu sorgen. Normalerweise ist es aber nicht die Technologie, die versagt, sondern der Mensch. Das größte Sicherheitsrisiko in einem Unternehmen kommt von innen. Noch immer ist der einfachste Weg, an Unternehmensdaten zu gelangen, auf einem Firmensparkplatz USB-Sticks zu verteilen, die infiziert sind. Sobald der Mitarbeiter den USB-Stick an seinem Computer angesteckt hat, kann man sich die gewünschten Daten aus dem Netzwerk holen. Unbemerkt, schnell und einfach.

Sind sich Unternehmen der Gefahr bewusst, die ihnen von innen droht?

Das Bewusstsein ist bei vielen noch nicht vorhanden. Meist werden Unternehmen erst dann für dieses Thema sensibilisiert, wenn schon etwas passiert ist. Kaum jemand investiert auch gerne Geld in seine Versicherung, trotzdem macht man es, weil man weiß, dass man sie braucht, wenn das Haus abrennt. Entsprechende Sicherheitstechnologien kosten eben einiges.

Welche Anforderungen haben Unternehmen an ihre Netzwerke?

Die Netzwerkindustrie ist vielleicht 25 Jahre alt und am Anfang waren Netzwerke sehr instabil. Sie waren nur Mittel zum Zweck, heute sind sie aber unternehmenskritisch, denn ein Netzwerkausfall kann für ein großes Unternehmen bis zu 200 Mio. Dollar pro Stunde kosten. Netzwerke haben somit einen ganz anderen Stellenwert als früher. Gleichzeitig sind die Selbstverständlichkeit der Verfügbarkeit und die Anforderungen an die Sicherheit extrem gestiegen. Netzwerke müssen schnell, sicher verfügbar und für den Benutzer möglichst transparent sein.

Was müssen Unternehmen bei der Anschaffung ihres Netzwerkes beachten?

Wesentlich ist sicher die Skalierbarkeit. Unternehmen sollten auf alles vorbereitet sein, was in Zukunft auf ihren Netzwerken passieren kann. Zudem ist die Unterstützung offener Standards anstelle von proprietären Ansätzen wichtig, da dies den Unternehmen erlaubt, aus einer Vielzahl von Applikationen diejenige auszuwählen, welche die Anforderungen am besten abdeckt.

Die Technologie schreitet rasant voran. Kann man da noch erahnen, was mittelfristig alles auf ein Unternehmen zukommt?

Wir wissen, in welche Richtung die Technologie in etwa geht. Beispielsweise haben wir heute in den Netzwerken die 10.000-fache Geschwindigkeit gemessen an jener von vor zehn Jahren, wobei sich die Investitionskosten im gleichen Zeitraum halbiert haben. Mit Cloud Computing wird sich alles noch einmal verändern, weil der Bedarf an zusätzlicher Geschwindigkeit zunimmt. Wir sprechen heute von 100-GBit-Technologien, die neuesten Switches, die wir produzieren, haben eine Leis-

tung von über 20 Tbit/s. Unternehmen streben auch danach, zukünftig nur noch ein Netzwerk zu haben und nicht mehr mehrere parallel. Über dieses Netzwerk wird Fernsehübertragung, Sprache, Videokommunikation, Datentransfer, Gebäudesicherheit und vieles mehr laufen. Das geht aber nur dann, wenn ein Netzwerk offen gestaltet ist und die Standards auch unterstützt.

Sind Unternehmen bereit, in die Zukunft zu investieren?

Der Stellenwert der Unternehmensnetzwerke ist von Branche zu Branche unterschiedlich ausgeprägt. Der Finanzbereich ist beispielsweise eher netzwerkaffin als die verarbeitende Industrie. Es ist eben eine Frage der Anschaffungs- und Betriebskosten. Für viele Unternehmen sind die Erstinvestitionskosten das Entscheidungskriterium für einen Netzwerkanbieter und sie vergessen allzu oft auf die laufenden Kosten. Wenn Sie sich langfristig ein bis zwei Mitarbeiter ersparen können, weil viele Prozesse automatisiert ablaufen und dadurch weniger Betriebsaufwand entsteht, dann zahlen sich höhere Anschaffungskosten relativ schnell aus.

Cloud-Studie: Gewitterwolken am Horizont

Für die Sicherheit in einer Cloud ist der Cloud-Nutzer selbst verantwortlich. Davon gehen zumindest 69 Prozent der Cloud-Anbieter aus, die im Rahmen einer Sicherheitsstudie von CA Technologies und dem Ponemon Institute befragt wurden. Derselben Ansicht sind hingegen nur 35 Prozent der Cloud-Nutzer. Für 32 Prozent fällt dies klar in den Aufgabenbereich der Anbieter. Wer für die verbleibenden 43 Prozent der Cloud-Nutzer für die Sicherheit nun verantwortlich ist, bleibt rätselhaft. Insgesamt legen die Cloud-Anbieter einen deutlich stärkeren Fokus auf schnelle Einführung und Kostenreduzierung als auf Sicherheit. Die Mehrheit (79 Prozent) stellt nur zehn oder weniger Prozent an IT-Ressourcen für Sicherheit oder Kontrollmechanismen zur Verfügung. Wenn allerdings Kosteneinsparungen und Agilität nicht mehr reichen, um das Sicherheitsrisiko zu kompensieren, könnte es zu einer Verlangsamung der Cloud-Einführung oder gar zu einem Stillstand kommen, wird von CA Technologies befürchtet.

Gigabytes, vermehrt euch!

Der weltweite Datenverkehr über das Internet wird sich bis 2015 auf fast ein Zettabyte vervierfachen. Das geht aus der soeben veröffentlichten Cisco-Studie hervor. Ein Zettabyte ist eine Eins mit 21 Nullen. Verteilt auf alle Nutzer würden dann pro Kopf 11 GB übertragen. Noch rasanter entwickelt sich der mobile Datenverkehr. Weltweit werden 2015 mehr als 5,6 Milliarden Tablet-PCs und Smartphones verwendet. Vergleicht man allein das Jahr 2010 mit dem Vorjahr, dann hat sich der weltweite mobile Datenverkehr um 159 Prozent erhöht und wuchs damit 4,2-mal schneller als der drahtgebundene Breitband-Verkehr. Pro Monat wurden 237 Petabyte (Eins mit 15 Nullen) – umgerechnet 60 Millionen DVDs – mobil übertragen. 2015 wird der mobile Datenverkehr 75 Exabyte (Eins mit 18 Nullen) betragen und dem 75-fachen des gesamten IP-Verkehrs im Jahr 2000 entsprechen.

Auf zum Angriff, fertig, los!

Der CIP-Report 2010 (Critical Infrastructure Protection) des Sicherheitsanbieters Symantec zeigt, dass sich Schlüsselindustrien nur unzureichend auf Cyberangriffe vorbereitet fühlen. Rund 1.600 Unternehmen aus 15 Ländern, deren Infrastruktur für die Wirtschaft und Gesellschaft als bedeutsam eingestuft wird, sollten im Rahmen des Berichtes ihre aktuelle Sicherheitslage einschätzen. Insgesamt wurde auf sechs Industriezweige fokussiert: das Energie-, Banken- und Finanzwesen sowie Kommunikation, IT und Gesundheit. Das Fazit der Studie: Die Bedrohung durch Cyberangriffe für die Infrastruktur von Schlüsselindustrien nimmt deutlich zu und verursacht immense Kosten. Insgesamt 53 Prozent der Unternehmen waren bereits Cyberangriffen ausgesetzt. Über den Zeitraum der vergangenen fünf Jahre hatten die betroffenen Unternehmen einen durchschnittlichen Schaden von insgesamt rund 600.000 Euro erlitten. Erschreckend ist, dass sich nur rund ein Drittel der Betreiber kritischer Infrastruktur auf Cyberangriffe bestmöglich vorbereitet fühlt.

BYOD – what?

Eine neue Abkürzung für einen neuen Trend. „Bring your own device“ bedeutet nichts anderes, als dass Mitarbeiter ihre privaten Devices auch dienstlich nutzen können. Eigentlich nichts Schlechtes dran, denn der Mitarbeiter fühlt sich geborgen, wenn er mit jenem Gerät arbeiten darf, das ihm am besten gefällt (siehe Motivation) und das Unternehmen erspart sich zumeist die Investitionskosten für irgendeine Standard-Hardware. Vielleicht freut sich der IT-Administrator nicht so sehr über die Modellvielfalt der in Zukunft zu verwaltenden Geräte.

Glossar einiger perfider Begriffe

Botnets: Netzwerke gekidnappter Rechner. Mit Trojanern, die sich durch manipulierte Webseiten oder fingierte E-Mails auf einen Rechner einschleusen, wird auf den fremden PC Zugriff erlangt und er über Web gesteuert.

Drive-by: Beeinflussung eines Rechners oder die Infizierung durch den bloßen Besuch einer verseuchten Webseite. So können Viren verbreitet, Spyware installiert und Browseranfragen zu Webseiten umgelenkt werden, deren Betreiber dafür bezahlen.

Fakeware: Meist nutzlose, aber nervige Programme, die gefälscht sind und vor Gefahren warnen, die nicht vorhanden sind, um zu einem Kauf zu bewegen.

Ransomware: Der Rechner wird gekidnappt und zur Geisel gemacht. Das normale Arbeiten wird verhindert, Viren aus dem Netz geladen und eine Art Lösegeld verlangt.

Sicheres Passwort? %xlr*\$PASS+W

Wirklich kreativ sind folgende Passwörter nicht: „123456“, „geheim“, „iloveyou“ oder auch nur „passwort“. Sicher sind sie schon gar nicht. Auch der Name der Frau, das Geburtsdatum der Kinder und ähnliches sind relativ leicht auszukundschaften. Genau diese Passwörter werden von Benutzern aber am häufigsten verwendet. Empfehlenswerter wäre es, sich ein kompliziertes Passwort für jeden einzelnen Dienst auszudenken.

Das Passwort sollte eine nicht im Wörterbuch zu findende Zeichenfolge sein, die mit Sonderzeichen und Ziffern versehen ist, sich mindestens über zehn Zeichen erstreckt und in keinem Zusammenhang mit dem Nutzer steht. Zudem hilft das beste Passwort nichts, wenn man es mitlesen kann.



Gegen „Keylogger“ auf dem eigenen Computer, die jede Eingabe protokollieren, kann man sich freilich nur mit regelmäßigen Softwareupdates und einem Virenschanner absichern. Vorsicht ist auch bei der Benutzung fremder WLANs geboten. In diesen Fällen sollte die Verbindung mit dem Server zumindest verschlüsselt ablaufen. Zudem sollten Passwörter hin und wieder geändert werden. Hier muss jeder Benutzer abwägen, wie viel Sicherheit er haben will und wie leicht er sich die neu erfundenen Passwörter merken kann.

Foto: James Thew

Mobile Devices – ein Sicherheitsleck in Unternehmen?

Televis hat bei Markus Robin, Geschäftsführer von SEC Consult, nachgefragt.

Wo lauern die Gefahren bei mobilen Endgeräten?

Das größte Sicherheitsrisiko ist nicht, wie weitläufig angenommen, der Benutzer, sondern die von sehr vielen Softwareherstellern eingebauten Sicherheitsschwachstellen, die sich im Betriebssystem, der Kommunikationssoftware, einer Business-Anwendung oder in Onlinegames befinden können. Diese qualitativ mangelhafte, unsichere oder auch als „toxisch“ bezeichnete Software ist höchst gefährlich und ermöglicht einem Angreifer beispielsweise, Daten auszuspähen oder eine komplette Fernsteuerung des mobilen Endgeräts vorzunehmen.

Welche häufigsten Fehler begehen Unternehmen bei mobilen Endgeräten?

Sie schätzen das Risiko falsch ein. Für kaum ein Unternehmen wäre es akzeptabel, wenn ihr Datenserver mit vertraulichen Daten in der U-Bahn vergessen und gestohlen würde. Wird aber zum Beispiel das Mobiltelefon eines Abteilungsleiters mit direktem Zugang auf das Firmennetz (und den Datenserver) entwendet, ist das scheinbar nur ein kleiner ärgerlicher Vorfall. Falsch. Es ist auch falsch, das eigene Unternehmen als unwichtiges Ziel für Angreifer einzustufen.

Was können Unternehmen ihren Mitarbeitern erlauben, was müssen sie verbieten?

Wichtigste Regel bei Geboten und Verboten in der IT-Sicherheit: Was für die Mitarbeiter gelten soll, muss für die Abteilungs- und Bereichsleiter sowie für die erste Führungsebene auch gelten. Die festzulegenden Vorschriften reichen von Passwort-Längen über die Nutzungseinschränkungen für private Aktivitäten, von der Verpflichtung zur Verwahrung bis hin zu Meldepflicht von Sicherheitsvorfällen, vom Verbot der Installation neuer Software bis hin zu Hinweisen bei der Nutzung ungesicherter WLAN-Access-Points. Dabei hat Verständlichkeit für die Benutzer Vorrang vor exakter technischer Terminologie.

Wie können sich Unternehmen vor den Risiken schützen bzw. die Risiken reduzieren?

Lassen Sie einen Security-Check Ihrer bestehenden mobilen Endgeräte vornehmen und warten Sie nicht, bis Sie ein Zwischenfall zum Umdenken zwingt. Wie bei einem echten Angriff wird dabei versucht, an Ihre wichtigsten Firmendaten zu gelangen. Auf Basis dieser Ergebnisse organisieren Sie den Prozess Sicherheit mit den Verantwortlichen und erst danach sollten Sie Geld für den gezielten Einkauf von Sicher-



Markus Robin ist Experte auf dem Gebiet der Informationssicherheit und seit 2005 Geschäftsführer des Beratungsunternehmens SEC.

Foto: SEC

heitsprodukten ausgeben. Und beachten Sie, dass der Prozess Sicherheit eine laufende Aktivität und keine einmalige Initiative ist.

Wo liegen die größten Herausforderungen im Bereich Sicherheit für die Unternehmen in der Zukunft?

Das aktuelle Risiko, unsichere und „toxische“ Software bei Endgeräten zu minimieren, bleibt auch in Zukunft die größte Herausforderung. Zusätzlich steigen die Komplexität der IT-Systeme, die Anzahl der verwendeten Technologien und die Vernetzung. Das Internet, die Maschine-zu-Maschine-Kommunikation, die Car-to-Car-Kommunikation und die Öffnung von geschlossenen Prozessrechnersystemen zum Internet vergrößern die Angriffsfläche enorm. Unternehmen, die bereits heute beim Einkauf von Software und Systemen explizit und nachdrücklich den Stand der Technik bei Anwendungssicherheit einfordern, gehen sorgsamer und zukunftsorientierter mit dem investierten Geld um.

Alles Denkbare ist auch machbar

Televis implementiert am Hauptsitz der EV Group ein redundantes Netzwerkkonzept.

Die EV Group wurde 1980 mit einer klaren Vision gegründet: Erich und Aya Maria Thallner wollten die Anlagentechnologie zur Waferbearbeitung für die Halbleiterindustrie, die Mikrosystemtechnik und die Nanotechnologie revolutionieren und der Industrie neue Horizonte öffnen. 30 Jahre später nimmt das Unternehmen mit seinen Produkten und Dienstleistungen in den Kernmärkten weltweit eine Spitzenposition ein. Doch Innovationen kommen bei EV Group nicht von ungefähr. Die fortwährende Forschung und Entwicklung sowie die Verbesserung und Stärkung bestehender Technologien und Prozesse sind die Basis der Zukunft. Und die Umsetzung der komplexen Forschungsaufgaben bis hin zur industriellen Großserienproduktion von Micro- und Nanobauteilen, ohne dabei Qualität, Produktivität und Zuverlässigkeit aus den Augen zu verlieren, die technologische Stärke der EV Group.

Obwohl die jährlichen Ausgaben für Forschung und Entwicklung nicht kommuniziert werden, handelt es sich um einen „substanziellen Umsatzanteil“, wie Josef Alexander Buttinger, Corporate IT Manager der EV Group, versichert. Nur so könne ein Hightech-Unternehmen vorne sein. Generell gehört es nicht zur Philosophie des eigentümergeführten Produzenten, mit großen Umsatzzahlen zu prahlen. Relevant seien vielmehr das stetige Wachstum und das Ergebnis, das am Ende des Tages übrigbleibt. In den Vordergrund rückt stattdessen die rasante Entwicklungsgeschichte. 1994 wurde die erste Niederlassung in Phoenix, USA eröffnet, drei Jahre später folgte Yokohama, Japan, 2000 ein zweiter Standort an der Ostküste der USA und 2003 EVG-Jointech in Chung-Li, Taiwan. Die jüngste Expansion erfolgte 2008 nach Seoul, Südkorea.

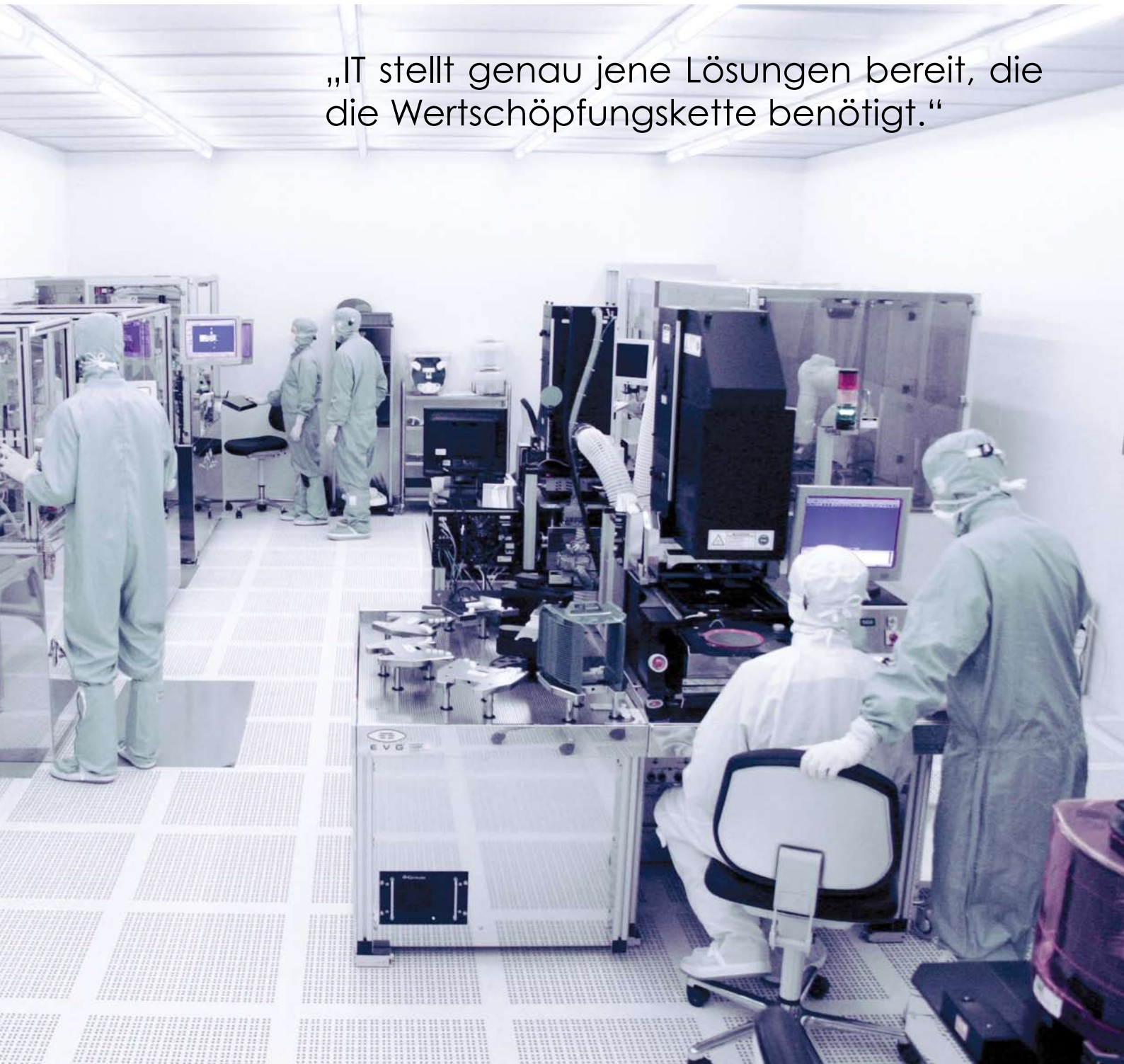
Weltweit werden 450 Mitarbeiter beschäftigt, 360 davon am Hauptsitz in St. Florian am Inn. Dass ein Technologieunternehmen seinen Standort in Österreich hält, ist ein bewusster Schritt der Eigentümer und „ein wesentlicher Teil unserer Ideale“, wie es Buttinger ausdrückt. Die gute Ausbildung der Humanressourcen und die Qualität der vorherrschenden Produktionsstandards sind natürlich mitentscheidend. Es sei schlicht nicht notwendig, in große Städte oder gar ins Ausland abzuwandern, wenn innovative Mitarbeiter, mitunter auch internationalen Ursprungs, in Österreich zu finden sind, oder bereit sind für ein attraktives Unternehmen hierher zu kommen. „Wir sind auch überzeugt, dass wir hier die bessere Qualität produzieren können.“ Die Entscheidung ist richtig. EV Group ist in fünf Märkten tätig und in vielen Technologien weltmarktführend. Zu den Referenzkunden zählen Konzerne wie Robert Bosch, Samsung, Toshiba oder Infineon. Nicht alle wollen genannt werden, es seien aber die mitunter größten Technologieunternehmen der Welt, die Anlagen und Prozess-Know-How der EV Group kaufen.

Nicht zuletzt ist auch die Informationstechnologie an dieser Leistung beteiligt, „weil sie genau jene Lösungen bereitstellt, die die Wertschöpfungskette benötigt“, so Buttinger stolz. Er ist seit 1997 im Unternehmen und war an der Implementierung der firmenweiten Informationssysteme beteiligt. Sein 19-köpfiges Team erledigt



Foto: EV Group

„IT stellt genau jene Lösungen bereit, die die Wertschöpfungskette benötigt.“



„Die Linie zwischen Sicherheit und Produktivität wird immer dünner.“

aus Effizienz- und Geschwindigkeitsgründen das meiste vor Ort, auf Outsourcing wird bewusst verzichtet. „Das ist unser strategischer Vorteil, nur so können wir rasch auf neue Geschäftssituationen reagieren.“ Performance und Ausfallsicherheit – generell zwei Aspekte, die im Vordergrund stehen. Um für zukünftige Anforderungen noch besser gerüstet zu sein, war Buttingers Team in den letzten sechs Monaten mit der Erneuerung des Computer- und Telekommunikationsnetzwerks am Hauptsitz beschäftigt. Gemeinsam mit Televis wurde ein redundantes Netzwerkkonzept ausgearbeitet und nun umgesetzt. Fällt eine Komponente aus, übernimmt eine andere innerhalb von Sekundenbruchteilen. Vereinfacht ausgedrückt. „Das gibt Sicherheit“, so der IT-Manager, bedeutet aber eine größere Komplexität der Aufgabe. Buttinger weiß, was er will und was er von seinem Anbieter erwarten kann. Televis kann seinen Ansprüchen vollends genügen. Dass er sich die Suche nach einem „kompetenten Partner“ alles andere als einfach gemacht hat, wird klar, wenn man erfährt, dass es europaweit insgesamt 8 Unternehmen auf seine Kandidatenliste geschafft haben. „Die IT ist ein träges Schiff und wer an quick-wins glaubt, liegt für meine Begriffe falsch“, sagt er. Es geht um die Abbildung hochkomplexer Vorgänge und kein Unternehmen möchte seine Netzwerke nach kurzer Zeit wieder neu aufbauen. Wer eine Entscheidung sorgfältig fällen möchte, müsse sich den Markt eben ganz genau ansehen und die Konzepte strategisch ausrichten. Buttinger denkt nachhaltig.

Was die technologische Zukunft anbelangt, sieht er eine der großen Herausforderungen in der Bewältigung der Mobilität. „Online forever“, bezeichnet Buttinger den Trend, gepaart mit dem Anspruch, immer online zu sein und von überall auf die aktuellsten Informationen zugreifen zu können. Er warnt aber auch vor Unterschätzung der Gefahr, die von der „derzeitigen Cyberkriminalität“ droht. „Ich glaube, dass es bei vielen Software-as-a-Service Systemen eine abrupte Sensibilisierung geben wird“, sagt er und hört gerade aufgrund der aktuellen Ereignisse rund um das Sony Playstation Netzwerk die Alarmglocken läuten. Die totale Sicherheit ist selbstverständlich nie zu erreichen. Letztlich hätten dann sämtliche Mobility-Lösungen und Connectivity-Tools keine Berechtigungen mehr und den Mitarbeitern müsste alles verboten werden. Der springende Punkt wäre, die Balance zwischen Sicherheit und Produktivität zu finden. Auch wenn „die Linie zwischen diesen zwei Zielen immer dünner wird“. Dass diese Balance innerhalb des Unternehmens zielgerichtet ausgelotet wurde, davon ist er überzeugt. Schwieriger sei es, wenn die Kompatibilität zu den Lieferanten- und Kundennetzwerken gefunden werden muss, um gut interagieren und kollaborieren zu können. „Sicherheitsansprüche, die wir als EV Group an uns stellen, können wir nicht immer von unserer Lieferkette erwarten“, so Buttinger. Teilweise müssten durchaus auch Abstriche in Kauf genommen werden. Und genau das wird eine seiner Aufgaben für die Zukunft sein, den „Regenschirm so aufzuspannen, dass er auch die gesamte Lieferanten- und Kundenstruktur umfasst und nicht nur unser Unternehmen.“



Interview:

Josef Alexander Buttinger
Corporate IT Manager der EV Group

Welche Herausforderungen bringt es mit sich, wenn ein Unternehmen global agiert und mehrere Niederlassungen IT-mäßig in das Gesamtkonstrukt integrieren muss?

Es ist ein Balanceakt zwischen autarken und zentralisierten IT-Systemen, der unternehmenskritisch ist. Bestimmte Lösungen müssen auch dann in der Niederlassung funktionieren, wenn aus Telekommunikationsgründen die Mutterfirma nicht erreichbar ist. Bei uns laufen wichtige Kommunikationssysteme, wie beispielsweise E-Mail oder Collaborate Messaging autark, während die Informationssysteme wie ERP oder CRM zentralisiert sind.

EV Group ist ein hochtechnologisches Unternehmen und einem permanenten Anpassungsbedarf der IT an äußere und innere Entwicklungen ausgesetzt. Wie schwer ist es, den Mitarbeitern neue Projekte zu kommunizieren und im Unternehmen zu implementieren?

Jeder IT-Leiter ist ständig mit dieser Frage konfrontiert. Ich glaube, ein Erfolgsrezept ist, wenn die IT nicht als ein eigener, kleiner Betrieb im Betrieb gesehen wird, sondern ein so genanntes „IT to Business Alignment“ geschaffen wird, indem die IT ihre Services ständig an die Unternehmensziele anpasst. Sicherlich schaffen wir das deshalb, weil wir bei neuen strategischen Änderungen sehr früh von der Geschäftsleitung in den Prozess eingebunden werden. Und letztlich sind wir als EV Group durch die IT erfolgreicher, weil sie genau jene Lösungen bereitstellt, die die Wertschöpfungskette benötigt.

Oft scheitert die Umsetzung neuer IT-Projekte an der Finanzabteilung.

Sie müssen bei jeder neuen Technologie Überzeugungsarbeit leisten und in jedem IT-Leiter muss ein gewisses Maß an kaufmännischem Geschick stecken. Letztlich ist es aber ein gesunder Dialog zwischen dem Finanz- und Technologiebereich, den man zu suchen und auch zu führen hat.

Josef Alexander Buttinger (37)

Nach der Informatikausbildung an der Universität Linz und einem Industrietraining für IT-Fachkräfte bei Infineon Melaka in Malaysia begann Josef Alexander Buttinger 1997 bei der EV Group als Software-Entwickler für EVG-Prozessanlagen. Seit 2000 ist er für die IT des internationalen Technologieführers zuständig. Neben seiner Funktion als Corporate IT Manager übernahm er 2007 auch die Funktion des Corporate Security Managers.

Haben wollen!

Abhör gesichert funken

Als besonders sicher bewirbt Microsoft sein neues Tastatur-Maus-Set Wireless Desktop 2000. Eine 128-Bit-AES-Verschlüsselung schützt die 2,4-GHz-Funkstrecke zwischen Tastatur/Maus und Empfänger und soll das „Mithören“ von Tastatureingaben verhindern. Das Abhören von



Funktastaturen ist kein neues Problem, bereits vor zwei Jahren wurden die Verschlüsselung geknackt und Abhörprogramme veröffentlicht. Nun soll alles anders werden, wenn auch die AES-Verschlüsselung nicht gegen Keylogger – versteckte Schadsoftware zum Abfangen von Tastenanschlägen – ankommt, weil die Eingaben erst nach der Funkstrecke mitgelesen werden. Und da liegen sie bereits wieder unverschlüsselt vor.

Doppelt gemoppelt

Wer sich nicht zwischen Netbook und Tablet entscheiden kann, dem empfiehlt Dell das Inspirion Duo. Ein 10-Zoll-Display, Windows 7 Betriebssystem und eine relativ breite Tastatur. Aber das wirkliche Highlight ist der Bildschirm, der sich um seine Achse drehen und auf die Tastatur legen lässt. Und so wird im Handumdrehen aus dem Netbook ein Tablet-PC. Das Inspirion Duo kann vieles ein bisschen, ob es letztlich etwas so richtig gut kann, muss jeder selbst entscheiden.



Beeriges Playbook

Einmal Blackberry, immer Blackberry – sagen zumindest die Anhänger. Das erste Tablet soll nun noch mehr Blackberry bieten und mit Multimedia und Geschwindigkeit überzeugen. Es ist klein und megaschnell. Was fehlt, ist ein mobiler Internetzugang: E-Mails verschicken geht leider nur per WLAN. Aber mit Updates soll bald alles besser werden. Businessstauglich? Hauptsache schön..

Blühender Schwarzmarkt für Kreditkarten und Bankdaten

Wer ein Online-Banking-Konto mit einem garantierten Deckungsrahmen von 82.000 Dollar haben möchte, kann es in der heutigen Zeit über einen Online-Store um 700 Dollar erwerben. Für weniger belastbare Konten muss man dafür nur 80 Dollar ausgeben. Diese und andere suspekten Preise gehen aus einem Bericht des Antivirus-Software-Herstellers Panda hervor, der sich eigenen Angaben zufolge über Monate in kriminelle Netzwerke eingeschlichen hat, in denen mit gestohlenen Daten gehandelt wird. Rund 50 solcher Online-Stores wurden

auskundschaftet und aus den erzielten Erkenntnissen eine interessante Preisliste ermittelt.

So belaufen sich die Kosten für eine geknackte Kreditkarte auf zwei bis 90 Dollar – je nach Kreditrahmen, versteht sich. Kreditkartenattrappen mit aufkopierten, gestohlenen Benutzerdaten können ab 30 bis 300 Dollar in den Warenkorb. Wer sich nicht traut, mit fremden Daten einkaufen zu gehen, kann auch einen Strohhalm engagieren, für 30 bis 300 Dollar ja nach Einkaufsvolu-

men. Weiter im Angebot sind Aufsätze für Bankomaten, um Benutzerdaten in Eigenregie zu kopieren (3.000 Dollar) oder ein nachgemachter Bankomat, den man dann an einer belebten Einkaufsstraße positionieren kann. Der schlägt allerdings bereits mit 35.000 Dollar zu Buche.

Die illegalen Webshops sind angeblich auch kundenfreundlich gestaltet und bieten zahlreiche Sonderangebote, Mengenrabatte oder Try&Buy-Dienste an. Der einzige Unterschied besteht in der Bezahlung: Kreditkarten werden nicht angenommen, erwünscht sind lediglich Zahlungen über ausgewählte Dienste.

Was ist denn bloß ... SPAM?

Eigentlich der Name eines amerikanischen Formschinkens. Gut, inzwischen mehr das Synonym für unerwünschte, massenweise versendete E-Mail-Nachrichten. Richtig, es geht um den E-Mail-Müll, der täglich in den Posteingängen abgelagert wird und die Empfänger vor viele Fragen stellt. Wer um Himmels Willen braucht schon Nachrichten, in denen Penisverlängerungen, Viagra-Pillen zu Schnäppchenpreisen oder sichere Millionengewinne versprochen werden? Anscheinend gibt es irgendeine Art der Nachfrage.

Wie die Spammer an die jeweilige Adresse kommen, ist hingegen leichter erklärt. Ausgeforscht werden öffentlich zugängliche Mailinglisten – Webseiten, auf denen Kontaktdaten stehen – oder die Daten stammen aus befallenen Adressbüchern irgendwelcher Geschäftspartner. Fraglich ist, ob sich der Aufwand für die Spammer lohnt, Millionen Nachrichten zu versenden. Ja, er lohnt sich – Spam ist ein lukratives Geschäft,

weil irgendwelche Menschen doch mitmachen.

Aber ist Spam nicht eigentlich verboten? (...) *Die Zusendung einer elektronischen Post als Massensendung oder zu Werbezwecken bedarf der vorherigen – jederzeit widerruflichen – Zustimmung des Empfängers.* So steht es zumindest im § 107 des österreichischen Telekommunikationsgesetzes. Verboten ist Spam also eigentlich schon, leider ist es nicht so einfach, den Spammern das Handwerk zu legen.

Fakt ist: Spam ist lästig und unbrauchbar. Freude können daran wohl nur die Anbieter von Anti-Spam-Programmen haben. Eine wirksame Sicherheitsmaßnahme gegen Spam – neben einer gut funktionierenden und ständig auf dem aktuellen Stand gehaltenen Antivirus-Software – besteht darin, mit seiner E-Mail-Adresse möglichst behutsam umzugehen und seine Kontaktdaten nicht online für jedermann preiszuge-

ben. Und wenn mal eine Spam-Mail ihren Weg in den Posteingang gefunden hat, dann gilt: Bloß nicht irgendeiner Aufforderung nachkommen, keine Links anklicken, keine persönlichen Daten offenbaren und schon gar nicht darauf antworten. Denn dann, ja dann ist es zu spät und viele unerfreuliche Dinge können die Folge sein. Beispielsweise lädt man sich einen Virus oder sonstige böse Software auf seinen Computer, mit der Passwörter oder Adressen gestohlen werden. Oder der Computer wird selbst zum Versenden von weiterem Spam missbraucht, ohne dass man etwas davon merkt.



10 Tipps gegen Spam

1. Vermeiden Sie E-Mail-Adressen, deren Alias nur aus drei oder vier Buchstaben besteht.
2. Benutzen Sie zwei E-Mail-Adressen: eine öffentliche und eine private, denn je freigiebiger Sie mit Ihrer E-Mail-Adresse umgehen, desto größer ist Ihr Spam-Risiko.
3. Verwenden Sie Ihre Hauptadresse nur, wenn Sie tatsächlich mit jemandem kommunizieren wollen und geben Sie diese nicht heraus, wenn Sie Newsletter abonieren, an Gewinnspielen teilnehmen oder in öffentlichen Foren unterwegs sind.
4. Reagieren Sie niemals auf eine Spam-Mail.
5. Klicken Sie niemals auf einen Link in einer Spam-Mail.
6. Schicken Sie Kettenbriefe oder Virenwarnungen nicht weiter.
7. Verwenden Sie Verteilerlisten oder das BCC-Feld, wenn Sie eine E-Mail an mehrere Empfänger versenden.
8. Meiden Sie öffentliche Adressverzeichnisse.
9. Geben Sie keine E-Mail-Adressen auf Ihrer Homepage an, besser sind Kontaktformulare.
10. Verwenden Sie einen Spam-Blocker.

Service? Bitte sehr!

Das mit dem Service ist so eine Sache. Irgendwie unklar, was er sein soll und wem er was bringen kann und wie so sich Unternehmen eigentlich durch den Service differenzieren müssten. Aus dem Englischen stammend bedeutet Service auf deutsch sowas wie dienen. Das klingt schön. Wir sind nun ständig mit Service oder seinen Pendanten, dem „Nicht-Service“ und dem „Möchtegern-Service“, in Kontakt. In gedruckten Prospekten, in formschönen Angeboten, in mangelnden Abläufen, in der Warteschleife eines Callcenters. Sie merken, zumeist bleibt uns die negative Service-Erfahrung in Erinnerung. Bei österreichischen Menschen deshalb, weil es sich um eine chronische Nörglernatur handelt, bei anderen Völkern, weil sie entweder mit dem Service-Gen auf die Welt gekommen sind und Service als das höchste Gesetz deuten oder weil sie Service jeglicher Ausprägung schon für eine grandiose Leistung halten (hat viel mit geschichtlicher Entwicklung und einem West-Ost-Gefälle zu tun). Halten wir also fest: Service konfrontiert uns permanent mit positiven oder negativen Ereignissen, ist uns aber bei der Orientierung in der Konsumwelt enorm behilflich. Fachlich korrekt ausgedrückt, könnte man sagen, dass ein Service ein Bündel von Nutzeffekten ist, den ein Dienstleister auf Abruf indivi-

duell für einen Servicekonsumenten erbringt. Ein Service ist die Lieferung einer online bestellten Pizza genauso wie die Reparatur eines Computers oder der Transport von A nach B. Kaum ein Unternehmen würde in seiner Imagebroschüre darauf verzichten, seinen tollen Service hervorzuheben. Jeder möchte im Dienste seiner Kunden stehen. Doch nicht alle Unternehmen erfüllen auch das, was sie versprechen. Nur wer langfristig eine Bindung zu seinen Kunden aufbaut, kann auch auf langfristige Kundenbeziehungen blicken. Und die erreicht man mit zufriedenstellendem Service. Wer gut bedient wird, hat keinen Grund, seinen Lieferanten zu wechseln. Außer der Service steht in keinem Preis-Leistungsverhältnis zum erzielten Mehrnutzen. Aber das ist eine andere Geschichte. Die Herausforderung ist vielmehr, dass „der Kunde immer gerne mehr hätte, als was wirtschaftlich machbar und technologisch sinnvoll ist“, sagt Peter Kulmbrein, CEO der Televis. Und, dass Service nicht immer positiv im Kopf des Servicekonsumenten besetzt ist. Kein Problem, wenn man als Unternehmen das Motto verfolgt: „Kundenerwartungen sind nicht nur zu erfüllen, sondern zu übertreffen.“ Absatzwechsel und zum nächsten Thema: ein neuer Servicestützpunkt in Salzburg. Wenn das kein Streben nach perfekten Servicebedingungen ist ...

Gestatten, wir sind Standort Salzburg!

Um noch schneller bei unseren Kunden zu sein, haben wir mit 1. Mai 2011 einen weiteren Televis-Standort eröffnet. Der neue Punkt auf unserer Servicelandkarte befindet sich in Salzburg. Ausgewählt wurde ein Industriegebäude in Eugendorf, das verkehrsgünstig direkt an der Abfahrt von der A1 sowie an der B1 gelegen ist. Wir haben hier nicht nur einen passenden Arbeitsort für unsere Mitarbeiter gefunden, sondern sind überzeugt, dass sich in den modern eingerichteten Büroräumlichkeiten auch unsere Kunden wohlfühlen werden. Mit Salzburg ist nun der nächste Schritt für die flächendeckende Österreich-Vorortbetreuung getan.

Roman Schneider (39)

Er ist für den Vertrieb im Raum Salzburg zuständig und der erste Ansprechpartner für unsere Kunden vor Ort. Er war nach einer elektrotechnischen Ausbildung zunächst in der Entwicklung tätig und wechselte dann in den Vertrieb von Kommunikationssystemen. Mit mehr als 20-jähriger Branchenerfahrung verfügt Roman Schneider über die nötige Expertise, um für unsere Kunden die jeweils optimale Kommunikationslösung zu finden.



Roman Forsthuber (25)

Er verfügt über umfassendes Wissen in den Bereichen LAN/WAN, VPN, Routing und Security und sorgt für die technische Realisierung unserer Lösungen. Roman Forsthuber absolvierte bei der Bausparkasse Wüstenrot eine Lehre zum Betriebselektriker, machte danach eine Ausbildung zum Systembetreuer und parallel neben seiner Tätigkeit als EDV-Techniker bei GMS zum Werkmeister für Informationstechnologie.





Gewinnen!

Frage: Wann wurde das Hightech-Unternehmen EV Group gegründet?

Frage beantworten, Antwort mit Ihren Kontaktdaten bis 31. August 2011 per E-Mail an gewinnspiel@televis.at senden und einen Wochenendaufenthalt in einem der PURESLeben Ferienhäuser gewinnen.



Man nehme die malerische Landschaft der Südsteiermark, edle Tropfen des Weinbauers Silly und die „g’standene Steirerin“, die in kulinarischer Höchstleistung mit Originalrezepten ihre Protagonisten bekocht, vermische alles mit feinsinniger Architektur und reichere es mit viel Stille an – dann entstehen PURESLeben Ferienhäuser. Jedes anders, jedes für sich einzigartig, alle außergewöhnlich. Je nach Größe, Lage und Ausstattung entsprechen sie entweder einem „Weinstöckl“, einem „Winzer“- oder einem „Lagenhaus“. Wer es puristisch bevorzugt und dennoch auf massives Eichenholz schwört, zudem von Holunderbäumen umzingelt sein möchte, wird in den Häusern am Tunauberg und in Kitzeck seine Zeit verbringen wollen. Dem Liebhaber des Landhausstils sei das kleine Weinstöckl am Graßnitzberg mit einer alten Weinpresse ans Herz gelegt, obwohl sich der

Urlaub auch im benachbarten Winzerhaus mit Ofenbett frei von Überflüssigem, mit Blick auf das Wesentliche, gestalten lässt. Die Lagenhäuser hingegen locken mit frei schwebenden Glasvorsprüngen und unendlichen Glasfronten. An die umliegenden Weinhänge als ständige Zuschauer gewöhnt man sich rasch, und dass die pure Natur, Massivholzmöbel und WLAN, Flachbildfernseher oder ein Weinklimaschrank einander nicht ausschließen, gefällt sicher ebenfalls. Das kennzeichnende Element aller sieben PURESLeben Häuser ist der Luxus der Einfachheit, in dem man auf nichts verzichten muss. Verwirklicht wurde das Konzept von Dietmar Silly, der seinen Gästen eine Auszeit vom Alltäglichen mit der Einkehr ins „private Heim“ bescheren möchte und ihnen dabei die Schönheit und Unbeschwertheit der Region näherbringt.

Unter allen richtigen Einsendungen wird ein Gutschein für zwei Personen über zwei Übernachtungen in einem der PURESLeben Ferienhäuser inklusive Frühstückskorb verlost.

Der Gutschein kann von Oktober 2011 bis 12. Dezember 2011 und ab 7. Januar 2012 bis einschließlich März 2012 nach Terminvereinbarung eingelöst werden. Eine Barablöse ist nicht möglich. Der Rechtsweg ist ausgeschlossen. Mitarbeiter der Televis und deren Angehörige sind vom Gewinnspiel ausgeschlossen. Die Gewinner werden schriftlich verständigt. Einsendeschluss: 31. August 2011.



It's time
to redefine
mobility.



Sicherheit.

Schnelligkeit.

Zuverlässigkeit.



Make Your Network Mobile

Wir orientieren uns einzig an dem, was Sie für Ihr Geschäft benötigen.

Extreme Networks GmbH | Jörg Hofmann | Tel.: +41.31.721.01.58 | jhofmann@extremenetworks.com

www.extremenetworks.com