Software-Aussteller auf der Systems 2008: „Die Informationstechnologie soll grüner werden."

Sebastian Schreiber demonstrierte, wie Hacker in die Netzwerke von Unternehmen eindringen.

Grün, sicher, konvergent

IT-Security, Green IT und Unified Communications waren die Trendthemen der Systems 2008 vom 21. bis 24. Oktober 2008 in München.

Deutschland braucht MINT" war Thema einer jener Diskussionsrunden in der „Systems 2008". *MINT* steht für Mathematik, Informatik, Naturwissenschaften und Technik und kennzeichnet den Mangel an qualifizierten Fachkräften in der Hightech-Branche Deutschlands. In der Education Area wurden Lösungsansätze hiefür im Bildungsbereich geboten, die Job Town war der zentrale Anlaufpunkt für Firmen, die Arbeitskräfte suchen, und für jene, die sich über Stellenangebote möglichst direkt informieren wollten.

„Grüner" soll die Informationstechnologie werden. Da sie nach den Feststellungen des Freiburger Öko-Instituts *(www.oeko.de)* mittlerweile bereits so viel CO2-Ausstoß verursacht wie der gesamte Flugverkehr, soll sie durch effizientere Energie-Ausnützung zum Umweltschutz beitragen. Sie soll beispielsweise Elektroschrott vermeiden durch Ressourcen schonendes Druck-Management, oder Tele- und Online-Konferenzen abhalten anstelle von Geschäftsreisen. Die *Experton Group* erwartet für den Green-IT-Markt bis 2010 ein jährliches Wachstum von über zwei Drittel.

„Konvergenz" bezeichnet die Integration der verschiedenen Kommunikationssysteme, der „alten" Technologie, wie Festnetztelefonie und Fax mit den neuen, IP-basierten Telekommunikationsnetzen und der mobilen Kommunikation („Unified Communications").

„Sicherer" soll die IT ebenfalls werden und diesem Thema hat sich die IT-Security Area in besonderem Maße gewidmet. Mit rund 300 Ausstellern auf 11.000 m^2 Hallenfläche war IT-Sicherheit wiederum ein Schwerpunkt der Systems. Im Viertelstundentakt gab es Vorträge, und zwar im *Forum Blau* mit technischer Ausrichtung und im *Forum Rot* auf Management-Ebene. Dort wurden auch um jeweils 12 Uhr („High Noon") Diskussionsrunden zu Themen wie Persönlichkeitsschutz, Data Leakage oder die Risken des Web 2.0, des „Mitmach-Internets", abgehalten. Die Handouts und Videos der Vorträge sind unter *www.it-sa.de/programm* abrufbar.

Jeder Messetag wurde im Forum Blau mit den „Morning Star Hackings" eröffnet, bei dem Sebastian Schreiber und sein Team von der *Syss GmbH (www.SySS.de)* vorführten, wie Hacker in die Netzwerke von Unternehmen eindringen. Sogar zehn Jahre alte Tricks – solange ist die IT-Security Area Bestandteil der Systems – funktionieren heute noch.

Wie jedes Jahr war auch *Bundesamt für Sicherheit in der Informationstechnik (BSI)* als Aussteller in der Security-Area vertreten. Experten des *BSI* hielten Vorträge zu den Themen IT-Grundschutz, IT-Sicherheitszertifizierung und über die Schriftenreihe des BSI.

Neuheiten. *Ironkey (www.ironkey.com)* hat einen Speicherstick (Flash-Drive) mit USB-Anschluss vorgestellt, der mechanisch äußerst widerstandsfähig ist (beispielsweise auch wasserdicht nach militärischen Standards) und den gesamten Inhalt seines Speichers mit 128 Bit nach dem AES-CBC-Verfahren verschlüsselt. Die Speicherkapazität des Sticks von momentan maximal 8 GB reicht zusammen mit einer hohen Verarbeitungsgeschwindigkeit (30MB/s read, 20MB/s write) aus, auch lauffähige Programme darauf abzulegen, sodass, abgesehen vom Bildschirm, der Stick im Grunde ein Notebook ersetzt – mit dem Vorteil, dass bei einem Verlust ohne Kenntnis des Passworts niemand zu den Daten Zugang hat. Das Passwort wird beim erstmaligen Anstecken des Sticks vergeben, ohne dass weitere Software installiert werden müsste. Wird das Passwort in der Folge zehnmal hintereinander falsch eingegeben, werden die abgespeicherten Daten vernichtet; der Stick ist nicht weiter verwendbar. Gleiches ist der Fall, wenn versucht wird, den Stick mechanisch zu öffnen.

Passwortschutz. Damit das Passwort bei der Eingabe nicht ausspioniert und während der Eingabe auch keine Schadprogramme wie Trojaner installiert werden

Fotos: Kurt Hickisch, Messe München

können, hat *Cyprotect (www.cyprotect.com)* eine Softwarelösung entwickelt. Das Passwort wird eingegeben, indem aus vom Programm vorgegebenen Zeilen von Buchstaben und Ziffern, die rhythmisch blinken, über Mausklick die richtigen ausgewählt werden. Ausgelesen werden kann von außen her nur die Stellung des Mauszeigers, mit der ein Außenstehender ohne Kenntnis der dahinter stehenden Maske nichts anfangen kann. Zudem wird während dieser Passworteingabe der Rechner mit Aufgaben wie etwa einer Primzahlenberechnung so ausgelastet, dass er keine anderen Eingaben mehr verarbeiten kann. Während der Dunkelzeiten wird einem Lauscher nur ein dunkler Bildschirm geboten.

Cold Boot. Die auf Penetrationstests spezialisierte *SySS GmbH (www.syss.de)* hat auf eine neue Gefahrenquelle für die Sicherheit der auf Laptops abgelegten Daten hingewiesen: Durch Kühlung kann erreicht werden, dass Transistoren ihren Schaltzustand auch nach dem Abschalten der Stromquelle noch durch einige Minuten beibehalten. Das

Systems 2008: 300 Aussteller präsentierten Produkte und Dienstleistungen.

RAM eines Laptops, der Arbeitsspeicher, auf dem die Daten wie auch das Passwort, beispielsweise das einer Festplattenverschlüsselung, bei bestehender Stromversorgung unverschlüsselt abgelegt sind, kann als einziger großer Transistor aufgefasst werden. Bei einem im Standby-Betrieb gehaltenen Laptop, zu dessen Start die Eingabe eines Passworts erforderlich wäre, können bei einem Unterkühlen der Speicher auch nach dem Abschalten des Geräts die Daten noch im Klartext ausgelesen werden und es kann, nunmehr in Kenntnis des Passworts das Gerät wieder hochgefahren werden.

„Die Nutzanwendung dieser Cold-Boot-Attack besteht darin, dass Laptops bei Nichtbetrieb schon aus Sicherheitsgründen tatsächlich abgeschaltet und nicht nur im Stand-by-Modus betrieben werden sollten“, sagte Dipl.-Inf. Karsten Kinder der *SySS GmbH*.

Virtuelle Honeypot Appliance. Mit virtuellen „Honigtöpfen“ können Angriffe im internen Netzwerk und Schadprogramme, die oft automatisiert von Botnetzen ausgesendet werden, angelockt, in sicherer Umgebung erkannt und den Endgeräten zugeordnet werden. *SecXtreme (www.sec-xtreme.com)* stellt mit der neuentwickelten Honeypot Appliance bis zu tausend solcher Honeypots zur Verfügung, wodurch firmeninterne Netzwerke flächendeckend überwacht und geschützt werden können. Erkannte Angriffsversuche werden zentral protokolliert und lösen Alarm aus. „Honeypots dürfen es Angreifern weder zu schwer noch zu leicht machen, in sie als vermeintliche Schwachstelle eines Systems einzudringen“, erläuterte der Geschäftsführer des Unternehmens, Diplom-Informatiker Christian M. Scheucher.

RZ-Container. Die Idee, Container für den Einbau von Rechenzentren zur Verfügung zu stellen, ist nicht neu. Neu ist der systemgeprüfte Container, den die auf die physische Sicherheit von Datenträgern etwa durch Datentresore spezialisierte Firma *Lampertz* als Weltneuheit vorgestellt hat. Der Container samt seinen aufeinander abgestimmten, für den Betrieb von Rechenzentren notwendigen Komponenten (Lüftung, Kühlung, Brandschutz, EMV-Schutz, Zutrittskontrolle) bildet mit der einbruchshemmenden Gestaltung ein zusammenpassendes System, das nach dem Baukastenprinzip erweitert werden kann. *Kurt Hickisch*

SYSTEMS

Neues Konzept

Die Systems 2008 hat mit insgesamt 1.061 Ausstellern und rund 39.000 Besuchern etwa die Zahlen des Vorjahres erreicht. Ausgebucht waren die Veranstaltungstermine im Internationalen *Congress Centrum München (ICM);* es konnten rund 4.000 Besucher verzeichnet werden. Dennoch war die 27. Systems die letzte in ihrer knapp 40-jährigen Geschichte. Sie wird, was die IT-Security betrifft, abgelöst durch die darauf spezialisierte IT-Sicherheits-Messe IT-SA *(www.it-sa.de),* die, organisiert vom *SecuMedia-Verlag,* nach dem Stand von Anfang Dezember 2008, vom 13. bis 15. Oktober 2009 in Nürnberg stattfinden wird. In die IT-Security werden die physische Sicherheit sowie Storage und Brandschutz integriert werden. „Fenster und Türen eines Raums, in dem sich Rechner befinden, sind genauso zu sichern wie die Computer selbst“, erläuterte Veronika Laufersweiler, Geschäftsführerin des *SecuMedia-Verlages,* bei der Vorstellung des Konzepts am 22. Oktober 2008.

Als Nachfolgeveranstaltung der Systems hat die *Messe München International (MMI) (www.messe-muenchen.de)* unter dem Namen „discuss & discover“ eine neue internationale Veranstaltung im Event-Format für Entscheider rund um alle Aspekte der Informationstechnologie angekündigt, die erstmals vom 20. bis 22. Oktober 2009 auf dem Gelände der *Neuen Messe München* stattfinden wird. Unter dem Motto „beyond bits and bytes“ will das Projekt Technologie- und Geschäftsentscheidern, Entwicklern aus Unternehmen, Forschung und Wissenschaft sowie Experten aus Politik und Gesellschaft ein Forum bieten, in dem sie sich frühzeitig strategisch auf künftige IT-Trends einstellen können, um sie aktiv mitzugestalten.

Foto: Kurt Hickisch