»Uns entgeht nichts«

»Neun von zehn Unternehmen setzen mobile Geräte bereits im Geschäftsalltag ein. Nur wenige verfügen über Richtlinien für den sicheren Umgang mit Smartphones und Tablet-Devices«, warnt Michael Gruber, schoeller network control.

»Under control – Uns entgeht nichts.« Unter diesem Motto stand das Jahresevent von schoeller network control in seinem 15. Jahr.

Von Karin Legat

Die Liftfahrt ließ schon eine hochwertige Veranstaltung erahnen: Mit rasanten 6,2 Metern pro Sekunde ging es in den 35. Stock des Twin Towers – andere Aufzüge fahren in der Regel mit etwa 2,5 Metern pro Sekunde. Sicher angekommen, ging es mit Sicherheit weiter. Nach einer Studie von Forrester widmen Unternehmen der Sicherheit ihrer Datenbanken zu wenig Aufmerksamkeit. »75 % der Datenbanken in heimischen Unternehmen sind nicht geschützt«, leitete Geschäftsführer Michael Gruber das network control forum 2013 ein.

IT im **Wandel**

»Mobility und Cloud ändern die IT«, bringt es ein Vertreter des kanadischen IPAM-Anbieters Blue Cat Networks (IP Address Management) auf den Punkt. Fast täglich berichten Medien über den fahrlässigen Umgang mit vertraulichen Daten oder den Diebstahl ganzer Datenbestände. 95 % der Arbeiternehmerinnen und Arbeitnehmer greifen bei beruflichen Aufgaben zumindest auf ein privates Gerät zurück. 2014 werden 130 Millionen Anwender in Unternehmen mobile Apps nutzen. »Outsourcing und Cloud Computing verlangen im höchsten Maß nach Flexibilität, Dynamik, Leistungsfähigkeit und Sicherheit auf allen Gebieten der IT-Infrastruktur«, betont Gruber. Damit war die Bühne frei für die Vorstellung zahlreicher innovativer IT-Security-Bausteine und -Services.

Security **2013 ff**

»Vor 15 Jahren haben wir mit unserem Programm Cybercop auf Sicherheitslücken im Netzwerk, unsichere Passwörter, Datenverschlüsselung und sichere Authentifizierung mit Secure ID reagiert«, erinnert sich Gruber. Heute braucht es mehr, wie beim Forum deutlich wurde. Mit Mobilgeräten, Malware im Unternehmen, mit Hightech und Social Engineering hat sich die Risikolandschaft geändert. Neue Sicherheitsprioritäten für ein schnell veränderliches, externalisiertes Geschäftsumfeld sind gefragt.

Alle Innovationen des schoeller Forums vorzustellen würde den Rahmen sprengen, deshalb nur einige der zentralen Ansätze der schoeller-Partner. SafeNet ermöglicht mit ProtectPack die sichere, verschlüsselte Übertragung und Speicherung vertraulicher Datendateien auf ungeschützten tragbaren wie auch vernetzten Medien. eSafe ist eine umfassende Content-Security-Lösung für die intelligente Echtzeitprüfung des gesamten eingehenden und ausgehenden Web- und Mail-Datenverkehrs. Der Vulnerability Manager for Databases von McAfee dagegen reduziert durch die Übersicht von Datenbankschwachstellen und Expertenempfehlungen für Behebungsmaßnahmen die Wahrscheinlichkeit schädigender Sicherheitsverstöße. »Database Activity Monitoring schützt mit einem Satz vorkonfigurierter Verteidigungsmittel und unterstützt beim Aufbau individuell zugeschnittener Sicherheitsrichtlinien«, informiert Channel Account Manager Stefan Dobrisek. Advanced Malware Detection bietet einen umfassenden Schutz gegen Malware-Infiltrierungen. Herkömmliche Firewalls beurteilt F5 aufgrund immer komplexer werdender Bedrohungen aus dem Internet als gescheitert und hat darauf mit der Application-Delivery-Firewall-Lösung reagiert, die Netzwerk, Anwendungen, Daten und Nutzer unter einer einzigen Sicherheitsstrategie zusammenführt. Bei Good Secure Mobility Solution von Good Technology liegt der unternehmensweite Mailverkehr in einem verschlüsselten Good-Container am mobilen Device. Das Konzept erlaubt die optimale Umsetzung von Bring Your Own Device, funktional festgelegten Geräten, mobil zugänglichen Mainframe-Anwendungen und individuellen Applikationsentwicklungen für iOS, Android und Windows 8. ❐

UNTERSTÜTZUNG FÜR SECURITY

Zum Thema Security unterstützt schoeller network control praxisnah mit Trainings. Ein Beispiel: »Vulnerability Assessment und Penetration Testing« befasst sich mit der Auffindung, Analyse und Ausnutzung von Sicherheitslücken im Rahmen einer gemeinsam mit den Teilnehmern simulierten Serie von Angriffen auf ein fiktives Unternehmen. Ziel ist die Vermittlung eines Überblicks über mögliche Angriffsvektoren aus der Sicht eines potenziellen Angreifers sowie eines ganzheitlichen Securityansatzes.