

IT-Sicherheit und mehr

Im australischen Brisbane diskutierten Experten IT-Security-Themen



Kai-Oliver Detken

Konferenzen der IFIP finden weltweit statt und adressieren IT-Security-Themen im Umfeld von Multimedia- und Kommunikationstechnologien. In diesem Jahr war die 21. IFIP-Konferenz in Australien auf dem World Computer Congress zu Gast. Der IFIP-Kongress in Brisbane bot vom 20. bis 23. September einen Einblick in aktuelle Forschungsergebnisse und State-of-the-Art-Lösungen im Bereich der Informations-, Kommunikations- und Mediensicherheit. Zur Tagung kamen international renommierte Wissenschaftler und Forscher sowie hochrangige Anwendervertreter.

Prof. Dr.-Ing. Kai-Oliver Detken ist Dozent an der Hochschule Bremen im Fachbereich Informatik sowie Geschäftsführer der Decoit GmbH

Schlagwort Security Management: In diesem Bereich wurde die Entwicklung der letzten Computergenerationen aufgezeigt – vom Mainframe-System bis zu verteilten Rechnersystemen. Die Datenverarbeitung findet heute immer mehr dezentral statt. Neben der technischen Entwicklung brachte die Information Security einheitliche Standards wie BS7799 hervor. Auch wurde das Top-Management hierbei zum ersten Mal involviert – nicht länger waren nur technische Lösungen gefragt. Die nächste Generation beinhaltet das Ausrollen der IT-Security-Vorschriften auf der Regierungsebene. Regularien wurden definiert und rechtliche Schritte eingeleitet sowie Verantwortlichkeiten für Geschäftsführer definiert. Die bisher letzte Generation der Computertechnologien beinhaltet das „E-Everything“: Benutzer sind überall und jederzeit mit dem Internet verbunden. Dabei wird aber auch das Web zum Angriffsziel. So kann man heute wesentlich einfacher sensible Daten bzw. Informationen des Endbenutzers bekommen, ohne in ein Unternehmensnetz einbrechen zu müssen. Die Cyber Security ist daher die neue Herausforderung des Internet. Hier sprechen die Zahlen für sich: Heute arbeiten ca. 3,6 Mio. Kriminelle im Cyberspace, und ca. 44.000 Phishing-Websites sind weltweit vorhanden, auf denen Benutzer unwissend ihre Daten eingeben. Die Anti-Phishing Working Group machte seit Juni 2009 einen Anstieg auf 585 % aus. Hinzu kommt, dass nach dem Imperva White Paper von 2010 rund 92 % der Webanwendungen nicht gut genug programmiert sind, um keine Sicherheitsattacken zuzulassen. In der jetzigen Computergeneration sind webbasierte Systeme aber an der Tagesordnung. Die Risiken bei Nutzung dieser Systeme wachsen daher jeden Tag. Der Endbenutzer steht im Mittelpunkt

der Hacking-Bemühungen, was zu immensen Problemen führen wird. So entstand der Begriff des „Battle Management“. Benötigt wird daher mehr Forschung bez. der Benutzersicherheit. Auch sollte die IT-Security mehr in die Software-Entwicklung eingebettet werden. Da dies bisher nicht geschieht, ist es nach Ansicht einiger Experten sogar bereits zu spät, um gegen die neue Bedrohungslage noch etwas zu unternehmen.

IFIP-Steckbrief

Die International Federation for Information Processing (www.ifip.org) ist eine internationale gemeinnützige Informatikorganisation. Sie richtet u.a. verschiedene Konferenzen, wie z.B. den World Computer Congress (WCC) oder die International Conference on Functional Programming (ICFP), aus. Sie dient auch als Dachorganisation für eine Vielzahl nationaler Informatikgesellschaften. Gegründet wurde sie ursprünglich 1960 unter Schirmherrschaft der Unesco als ein Resultat des ersten World Computer Congress in Paris, der 1959 stattfand.

Auch bei neuen Energieversorgungsnetzen spielt die IT-Sicherheit eine entscheidende Rolle. Präsentiert wurde die neue Generation von Smart Meters für die Energieversorgung, die heute bereits im Einsatz sind oder in Zukunft sein werden. Das Energienetz wird sich dadurch von einem zentralen Energienetz zu einem verteilten Energienetz entwickeln, da vor Ort die notwendige Energie erzeugt wird (z.B. durch Sonnenkollektoren). Dafür sind Sensoren nötig, die dezentral verwaltet werden müssen. Dabei beeinflussen diese Sensoren aktiv die Energieversorgung, z.B. durch die Festlegung, wie viel Energie in das Stromnetz ab-

gegeben werden darf. Das heißt, es muss eine Absicherung dieser Sensoren umgesetzt werden, was aber von den Energieversorgern derzeit nicht ausreichend betrachtet wird. Verteilte Infrastrukturen lassen sich zudem schwer managen, da die Energieversorgung unvorhersehbar an verschiedenen Bereichen zu- oder abnimmt. Die Frage ist daher, wie können verschiedene Root of Trusts etabliert werden? Eine Hardware-basierte Sicherheit über einen TPM-Chip wäre für die Smart Grids deshalb wünschenswert. Prototypen für Smart Gateways werden im EU-Projekt SecFutur (www.secfutur.eu) bereits entwickelt.

In einer bis zum letzten Platz belegten Session wurde das Projekt des BMBF Vogue (www.vogue-project.de) vorgestellt und auf die neuen Anforderungen an mobile Endgeräte hingewiesen. Dies hängt auf der einen Seite mit den neuen Leistungsmöglichkeiten von Smartphones zusammen, die wie kleine Computer arbeiten, und auf der anderen Seite mit der wachsenden Zahl von Viren, die für Smartphones entwickelt werden. Diesen neuen Anforderungen werden heutige Administratoren nicht gerecht, da sie meistens die mobilen Endgeräte nicht in die Security Policy des Unternehmens integrieren. Hinzu kommt eine Vielfalt an mobilen Betriebssystemen und mobiler Hardware. Das Vogue-Projekt will durch den TNC-Ansatz (Trusted Network Connect) die Sicherheit mobiler Systeme erhöhen, in-



Die Hauptziele einer IFIP-Konferenz – die Förderung internationaler Zusammenarbeit, die Anregung von Forschung und Entwicklung, die Förderung von Bildung und die Verbreitung von Information – konnten alle in den vier Konferenztagen mehr als ausreichend erfüllt werden, da sich auch auf dieser 21. Konferenz wieder ein reger Austausch zwischen den Teilnehmern entwickelte
(Fotos: Detken)

dem neben dem Benutzer auch die Hardware abgefragt wird. Zusätzlich werden verschiedene statische Security Policies unterstützt, damit sich der mobile Benutzer in verschiedenen Firmen sicher aufhalten kann. Vogue nutzt den TNC-Ansatz, um einen einheitlichen NAC-Ansatz (Network Access Control) zu verfolgen und Android als Smartphone-Beispiel einzubinden. Ein Demonstrator wird nach derzeitigem Projektstatus Ende des Jahres vorhanden sein.

Die „Wolke“ kritisch gesehen

Am zweiten Konferenztag stand u.a. Cloud Computing auf dem Programm. Dabei wurde die dezentrale IT-Struktur kritisiert, die heute einen Mehraufwand an administrativen Tätigkeiten beinhaltet. Jedes Unternehmen muss heute eine eigene komple-

xe Infrastruktur aufbauen, incl. der damit verbundenen Fachleute. Das IT-Budget für IT-Equipment stieg deshalb um ein Vielfaches von 2 % auf 48 % im Gegensatz zur Mainframe-Area. 52 % der Unternehmen nutzen heute bereits Cloud Computing, um Kosten einzusparen, während 1 % bisher kein Interesse haben. Das liegt auch daran, dass Bandbreite und Rechenkapazität nach den Gesetzen von Grove und Moore immer weiter anwachsen. Allerdings lässt sich auch nicht verleugnen, dass man sich mit der Cloud neue Probleme ins Haus holen kann, was etwa die Verfügbarkeit und Security angeht.

Rechtsfragen

Auf der Konferenz präsentierte sich auch das Europäische Patentamt als Aussteller und mit verschiedenen Vorträgen. Das intellektuelle Recht in der Softwarebranche wird jedoch nicht von allen positiv gesehen. So kam es am Rande zu einer „Kleindemo“ von Richard Stallmann, in der gegen Softwarepatente und die nicht mehr freie Nutzung protestiert wurde. Unklar ist heute nämlich, was eine Software-Erfindung beinhaltet und wie sich diese gegen andere abgrenzt. Zudem können sich ein Patent nur Großunternehmen leisten, die auch bei evtl. Gegenklagen genug „Sitzfleisch“ besitzen würden. Der Mittelstand bleibt hierbei auf der Strecke. Stallmann setzt daher auf freie Open-Source-Entwicklungen. (we)