VDI Forum „Innovative Sicherheitstechnik" 25.11 2011

Beinahe täglich erreichen uns Meldungen über kleine und große Unfälle, neue Bedrohungen im Internet, Terrordrohungen oder gar Katastrophen. Und jeder denkt: Sicherheit tut not. Auch der VDI widmete dem Thema Risiko ein Forum: Innovative Sicherheitstechnik. Durch eine glückliche Hand bei der Auswahl der Vortragenden wurde es eine sehr anregende Veranstaltung.

Einführung

Prof. Dr. Reinhard Höpfl, Vorsitzender des VDI Landesverbands Bayern begrüßte die Funktionsträger aus Behörden, Wissenschaft und Wirtschaft und natürlich die anwesenden VDI-Mitglieder. Er wies darauf hin, dass wir alle nach Sicherheit suchen, aber zwecks Wahrnehmung von Chancen trotzdem Wagnisse eingehen müssten. Sicherheit schaffe Vertrauen und sei für eine Gesellschaft essentiell.
Der gastgebende TÜV wurde durch Walter Reithmaier von der Geschäftsführung TÜV SÜD Automotive vertreten. Er zitierte die Satzung des TÜV, die diesen auf den Schutz von nicht nur materiellen Werten verpflichte. Mit mittlerweile 16.000 Mitarbeitern weltweit kümmert sich der TÜV daher auch zunehmend um Safety und Security von Strukturen, Verfahren und Prozessen aller Art.
Der Vorsitzende des VDI Bezirksvereins München, Prof. Dr. Bernd-Robert Höhn, übernahm dann die Moderation und beschrieb als Ziel der Veranstaltung einen Überblick über die gesamte Bandbreite der Sicherheitstechnik.

Bedeutung der Sicherheitsforschung

Einen Überblick über das große Feld der Sicherheitsforschung gab Prof. Dr. Klaus Thoma vom Fraunhoferinstitut für Kurzzeitdynamik, Ernst-Mach-Institut, Freiburg.
Das Programm „Forschung für die zivile Sicherheit" des Bundesministeriums für Bildung und Forschung (BMBF) untersucht mit verschiedenen Partnern umfassend die Probleme der Security für Mensch und Infrastruktur, wobei auch Safetyaspekte nicht ausgeklammert werden (security = Schutz vor absichtlichen, von Menschen ausgelösten Angriffen; safety = Schutz vor zufälligen, unbeabsichtigten Schäden; d. Red.). Sicherheit ist eines der großen Themen der Zukunft neben Energie, Mobilität, Umwelt, Gesundheit und Kommunikation.

Warum ist Sicherheitsforschung so wichtig? Weil Gefahren immer und überall drohen. Zwar hat die Technik einerseits immer mehr Sicherheit ermöglicht, andererseits aber auch die Voraussetzungen für eine immer leistungsfähigere und komplexere Infrastruktur zur Versorgung mit Gütern und Information geschaffen, die einer neuartigen Verletzlichkeit unterliegt. Das wurde bisher zu wenig erkannt und beachtet (Ausnahme Brandschutz). Wegen zunehmender Bevölkerungskonzentration in Megacities und der Vernetzung in globalem Ausmaß können Terrorangriffe, organisierte Kriminalität, Cyber Crime, Großunfälle, Naturkatastrophen oder Epidemien verheerende Effekte ausüben. Die Forschung soll kritische Strukturen definieren (Verkehr, Versorgung, Behörden, Banken, Information) und mit einem holistischen Sicherheitsansatz eine resiliente (fehlertolerante) Gesellschaft ermöglichen. Ziel ist Security by Design, indem möglichst alle für ein Projekt wichtigen Risiken von vornherein berücksichtigt werden.
Die Forschung wird sowohl auf EU- wie auch auf nationaler Ebene betrieben. Neu ist, dass nicht nur die klassischen technischen Felder bearbeitet werden, sondern dass querschnittlich u.a. auch Soziologie, Recht, Ethik, Medien und vor allem die Endnutzer wie die Feuerwehr einbezogen werden.
Als konkrete Anwendungsbeispiele wurden ein Hochhauskonzept mit einsturzgeschütztem Kern und SOGRO, ein Projekt zur Sofortrettung bei Großunfällen vorgestellt.

Sicherheit im Internet
Prof. Dr. Claudia Eckert (TU München, Fakultät für Informatik und Fraunhofer-Institut für Sichere Informationstechnologie) startete ihren Vortrag mit der provokanten Aussage „Sicherheit im Internet gibt es nicht“, setzte aber gleich hinzu, man dürfe natürlich nicht aufgeben. Die Informationsverarbeitung und -vernetzung schreitet rasend schnell voran und Daten sind sowohl Wirtschaftsgut als auch Steuerungselemente. Das macht sie interessant für Ausspähen und Manipulation. Cyberangriffe sind wegen geringem Risiko, hoher Effektivität und möglichen großen Gewinnen sehr attraktiv. Es besteht dringender Handlungsbedarf sowohl bei der Technologie wie beim Problembewusstsein. Ziel muss wiederum sein: Design for Security, was sich sowohl auf die Technik wie auf die Bedienabläufe bezieht. Die Systeme müssen über ihren gesamten Nutzungszeitraum immer wieder getestet werden, da sich die Bedrohungen weiterentwickeln. Die Anwender müssen es ein umfassendes Risikomanagement betreiben. Vor allem müssen die Mitarbeiter intensiv geschult werden, da der Mensch das schwächste Glied der Kette bleibt. Aktuelle Problemfelder sind u.a. Smart Grids und Cloud Computing.

Sicherheitstechnik als gesellschaftspolitische Säule der Industrie
Aus der Praxis berichtete höchst anschaulich Rainer von zur Mühlen von der VON ZUR MÜHLEN'SCHE GmbH, einer auf Sicherheitsberatung und Risk-Management spezialisierten Consulting-Gesellschaft. Er betonte, dass es keine Schadensereignisse gibt, sondern Auslöser und Prozesse, an deren Ende ein Schaden steht. Und für jeden Verantwortlichen gilt die Beweislastumkehr, er muss gegebenenfalls nachweisen, dass er alles Nötige zur Unterbindung von Schadensprozessen getan hat. Der Eintritt von Schäden muss verhindert (z.B. kein brennbares Material vorhanden), behindert (Videoüberwachung), rechtzeitig entdeckt (Sensorik) und geeignet bekämpft (Sprinkleranlage) und im schlimmsten Fall eindeutig nachgewiesen werden. Häufig besteht zu wenig Risikobewusstsein und die Berufung auf Bestandsschutz und daher unterbliebene Investitionen z.B. in Brandschutz können gewaltige Kosten nach sich ziehen. Wenn wegen einer undichten Wasserleitung mit nachfolgendem Kurzschluss schließlich ein Hochhaus total abbrennt, Gesamtschaden 30 Mio. Euro, hat das schon einen hohen Anschauungswert. Laut von zur Mühlen ist das Risikomanagement oft unsystematisch. Je nach Gegebenheit müsse man entweder konsequent die Eintrittswahrscheinlichkeit oder die Schadenshöhe eines möglichen Vorfalles reduzieren. Und vor allem: Sicherheit muss als Querschnittsthema angegangen und als Unternehmensziel definiert werden.

Podiumsdiskussion
Die abschließende Podiumsdiskussion mit den Referenten leitete Prof. Höhn. Klare Antwort auf die Eingangsfrage: Sind Handy und Onlinebanking sicher? Keinesfalls. Gibt es Sicherheitszertifikate für Datengeräte? Nein, auch keine transparente Prüfung von

„Apps“. Das ist zu teuer, Zertifizierung ist zu kompliziert. Kann man Hochhäuser nachträglich sicherer machen? In gewissem Ausmaß ja durch Anwendung spezieller Materialien. Wie lange sind „sichere“ Systeme sicher? Das Hase-und-Igel-Spiel läuft ewig. Ziel des Risikomanagements ist vorausschauendes Handeln, beweisbar ist Sicherheit aber nicht. Für kritische Anwendungen muss man segmentierte Inselkonfigurationen vorsehen, was aber nicht durch die Mitarbeiter durchlöchert werden darf. Auch wird die EU eine neue Richtlinie erlassen, damit bei Auslieferung von Kommunikationsgeräten alle Sicherheitsfunktionen aktiviert sind. Manche Firmen machen dies aber bei Updates zum Teil rückgängig. Security by Design gibt es noch zu selten wegen fehlender Vorschriften, hier ist die Politik gefordert. Prof. Höhn beendete die Diskussion mit der Bemerkung, bei der Ingenieurausbildung sei die Rechnergläubigkeit zu bekämpfen und stattdessen kritisches Mitdenken einzufordern. Prof. Höpfl dankte dann allen Referenten und Zuhörern und leitete zum geselligen Teil über. Die spannenden Vorträge und das attraktive Buffet animierten noch viele der Besucher zu langen Diskussionen.

Gerhard Grosch
Redaktion TiB