

### **Frage 7: Entwicklung von IT-Sicherheitstechnologien in Deutschland**

Wie sehen Sie die Lage der Entwicklung von IT-Sicherheits-Technologie in Deutschland? Was sind Hindernisse für positive Entwicklungen? Wie könnten Hindernisse beseitigt werden (z.B. durch Forschungsförderung, Verbandsarbeiten?) Was kann man aus Erfahrungen in anderen Ländern lernen? Wie sehen Sie die Kooperation zwischen Forschung und Wirtschaft? Wer ist an den neuen Technologien am meisten interessiert: Wissenschaftler, Produktanbieter, Endnutzer?

#### **Sven Müßig (IBM Global Services):**

Solange nichts passiert, nimmt IT-Sicherheit niemand wahr und darum ist auch kaum jemand bereit, in sie zu investieren. Das ist eines der größten Hindernisse für die IT-Sicherheit in Deutschland. Wir haben es mit einer unsichtbaren Gefahr zu tun. Manager können die Auswirkungen und das mögliche Bedrohungspotential der heutigen Kommunikationsmöglichkeiten nur schwer beurteilen oder fachlich in ihrem ganzen Umfang abschätzen.

Viele denken beim Thema IT-Sicherheit nur an Hacker, Virenattacken, Gebäudekontrolle, fehlerhaftes IT-Equipment oder Datenverluste. Diese sind zwar die hauptsächlich in der Öffentlichkeit genannten Themen, allerdings gibt es Gefahren im Hintergrund, die weitaus höhere Schäden verursachen. Wirtschaftsspionage gehört beispielsweise dazu. In der heutigen Zeit wird es potentiellen Datendieben durch die ständige Miniaturisierung, etwa durch Mobiltelefone mit integrierter Kamera, Hacktools aus dem Internet oder ähnlichen Hilfsmitteln immer einfacher gemacht, Daten zu stehlen. Von diesen Schäden wird man allerdings kaum etwas in der Zeitung lesen, da die geschädigten Firmen kein Interesse an deren Publizierung haben.

Die Erfahrungen in den USA zeigen, dass umfangreiche Investitionen des Staates in neue Bereiche wie Homeland Security im gesamten Land ein ganz anderes Bewusstsein für Sicherheit innerhalb kürzester Zeit geschaffen haben. Der Staat hat durch diese Investitionen Wirtschaftsunternehmen, die in diesen Bereichen tätig sind, zu ganz neuen technologischen Entwicklungen animiert und dadurch eine technologische Führungsrolle in der Welt übernommen. Diese Technologien werden nun wiederum in anderen Ländern nachgefragt und bewirken ein starkes Wirtschaftswachstum in dieser Branche.

Die Entwicklungen in den USA und anderen Ländern führen nun auch immer mehr in Europa zu einem gesteigerten Sicherheitsbewusstsein. Das beginnt in den meisten Firmen mit einem erhöhten Basis-Sicherheitsbewusstsein. Welche Firewall installiere ich? Setze ich ein Virtual Private Network (VPN) ein? Existiert eine Security Policy in meinem Unternehmen? Derzeit hört die Entwicklung bei den komplexeren IT-Sicherheits-Anwendungen wie beispielsweise Signaturkarten und Biometrie auf.

Wichtig ist, mit einer detaillierten Risikoanalyse zu beginnen. Darufhin folgt die Erstellung der Security Policy und deren direkte und konsequente Umsetzung. Die Anwendung neuer Technologien wie etwa Biometrie für die Zugangskontrolle, ID-Chip-Aktivierung durch Personalisierung in Laptops, kann hierbei zusätzlich helfen, den Sicherheitslevel weiter anzuheben. Das Bewusstsein muss allerdings beim Management geweckt werden. Wenn ein RZ-Leiter die Vorgabe bekommt, die IT Ausgaben um 20 Prozent zu senken, wird er kaum Geld für Sicherheit einplanen wollen, wenn dies nicht ein Anliegen des Managements ist.

Um sich gegen eine Bedrohung erfolgreich schützen zu können, muss man sich zuerst mit möglichen Quellen für die Bedrohungen beschäftigen. Wer die Risiken kennt, kann mit ihnen umgehen und entsprechende Vorkehrungen treffen, um sie zu vermeiden oder zu vermindern.

### **Gerold Hübner (Microsoft Deutschland GmbH):**

Ich bin der Meinung dass deutsche Anbieter von IT-Sicherheits-Technologie sich absolut nicht verstecken müssen. Es gibt gerade in Deutschland eine ganze Reihe sehr leistungsfähiger und innovativer Anbieter von Sicherheitstechnologie. Auch sehe ich, dass der Know How Transfers von Fachhochschulen und Universitäten hinein in flexible, dynamische Unternehmen der IT-Sicherheitsbranche im Großen und Ganzen recht gut funktioniert, auch wenn es im Detail Verbesserungsbedarf gibt. Wünschenswert wäre z. B. eine größere Durchlässigkeit für den Wechsel von Hochschullehrern und Führungskräften in den Unternehmen in beide Richtungen.

Probleme sehe ich bei einigen deutschen Anbietern noch im Hinblick auf die fehlende Weltmarktorientierung. In Zeitalter der globalen Vernetzung kann man großen Märkte mit einer rein lokalen Ausrichtung von Produktportfolios und Marktstrategien nicht mehr nachhaltig gewinnen. Auch die an vielen technischen

Fakultäten einseitig an der Philosophie der Open Source Gemeinde orientierte Ausbildung ist häufig nicht marktgerecht.

Eines der größten Probleme der gesamten IT-Sicherheitsbranche dürfte aber sein, dass entgegen der immer zu hörenden Beteuerungen, die Ausgaben der Unternehmen für IT-Sicherheits-Technologie würden kräftig wachsen, in der Praxis doch verhältnismäßig wenig Budget für IT-Sicherheits-Projekte vorhanden ist. Ein Grund dafür ist sicher, dass es grundsätzlich sehr aufwendig und damit teuer ist, Sicherheit in bestehen Umgebungen nachträglich messbar zu verbessern. Reine IT-Sicherheits-Projekte, wie z. B. den Aufbau eine Public Key Infrastruktur oder die Einführung von Smartcards für die Authentifizierung von Anwendern sind deshalb vergleichsweise selten. Derartige Sicherheitstechnologien werden meist erst bei der Neukonzeption einer IT-Umgebung berücksichtigt.

### **Dr. Sachar Paulus (SAP AG):**

Die deutsche IT-Sicherheitsbranche konzentriert sich aus historischen Gründen sehr stark auf nationale Bedürfnisse. So hat das Signaturgesetz und dessen technische Folgen eine hohe Innovations- und Investitionsbereitschaft in deutschen Technologieunternehmen zur Folge gehabt. Dennoch erreichen deutsche Sicherheitsprodukte oft nicht den „Commodity“-Status, d.h. sie werden überall gebraucht und verwendet (etwa Firewalls), und wenn, sind sie nur regional erfolgreich. In diesem Punkt sind uns gerade U.S.-Amerikaner und Israelis deutlich voraus. Gründe dafür sind vielfältig. Ein wesentlicher Grund ist sicherlich die starke Betonung der deutschen Sicherheitsforschung auf technologieintensive Themen, die häufig nicht zu praktikablen Lösungen in Produkten führen. Ein engerer Austausch mit der Konzentration auf Probleme der Praxis ist aber schon in vielen neueren Kooperationen zu sehen.

### **Klaus Martin (Siemens Business Services Deutschland):**

Im Moment kommt ein Großteil der Sicherheitstechnologien aus den USA. Durch die teilweise unterschiedlichen Anforderungen in Europa, beispielsweise bei Verschlüsselungstechnologien, muss aber auch vermehrt in Deutschland Entwicklung betrieben werden. Wichtig dabei ist, dass in den einzelnen Wirtschaftsregionen keine Insellösungen entstehen. Es sollte nicht sein, dass in den USA, in Europa und in Asien unterschiedliche Sicherheitstechnologien im Einsatz

sind. Dies widerspricht dem globalen Charakter der Unternehmen und bietet der Cyber-Kriminalität verstärkt Angriffspunkte. Wir müssen eigene Technologien im weltweiten Kontext entwickeln. Nur so hat der international agierende Anwender – auf den es letztendlich ankommt – den größten Nutzen.

### **Stefan Strobel (cirosec GmbH):**

IT-Sicherheits-Technologie made in Germany ist im internationalen Vergleich leider nicht so häufig wie beispielsweise Technologien aus Israel oder den USA. Dennoch hat auch Deutschland einige international erfolgreiche Firmen in diesem Bereich vorzuweisen.

Eine starke treibende Kraft für neue Sicherheitstechnologie sind in anderen Ländern meist junge Startup-Unternehmen. Gerade Startup-Firmen aus Israel und den USA sind uns mit völlig neuen Ideen weit überlegen. Das hat viele Gründe. Beispielsweise ist schon die ganze Venture Capital Kultur in Israel und den USA sehr viel ausgeprägter als in Deutschland. Dazu kommt, dass eine Ausbildung im IT-Sicherheitsbereich an deutschen Universitäten nicht sehr häufig angeboten wird, während das Thema in Israel ständig präsent ist.

Um hier vorwärts zu kommen, müsste IT-Sicherheit zunächst stärker in der Ausbildung gefördert werden. Dazu gehört nicht nur die Theorie von Verschlüsselung, sondern auch die Sicht der Angreifer, denn nur mit diesem Wissen können gute neue Ideen für innovative Technologien entstehen.

Die Forschung und Kooperation zwischen Forschung und Wirtschaft ist selbstverständlich ein weiterer wichtiger Baustein.

### **Gernot Hacker (Sophos GmbH):**

Infineon ist ja Contributor-Mitglied der TCG, somit aktiv an der Gestaltung von neuen Technologien beteiligt. Prinzipiell ist der Sicherheitsmarkt jedoch sehr am nordamerikanischen Markt angesiedelt, da dies der weltweit größte IT-Markt ist. Gepaart mit der Tatsache, daß es dort gängig ist, zu heimischen Produkten zu greifen. Eine deutsche Firma tut sich gerade im sicherheitskritischen Bereich schwer, in den USA Fuß zu fassen. Weiterführende Aussagen zu dieser Thematik vermag ich jedoch mangels konkreter Unterlagen nicht zu treffen.

### **Prof. Dr. Hartmut Pohl (FH Bonn- Rhein- Sieg):**

Es wäre leicht hier zu jammern, wer was nicht tut oder auch versäumt.

Wir haben an der Fachhochschule Bonn– Rhein– Sieg ein Labor für Informationssicherheit errichtet, in dem wir mit Studierenden u.a. erfolgreich Sicherheitsprodukte und auch umfangreiche Sicherheitssysteme anhand objektiver Kriterien testen. Das ist für die Studierenden hochinteressant deswegen, weil sie lernen die (durchaus unterschiedliche) Qualität von Sicherheitsprodukten zu bewerten. Für die Produktlieferanten und Hersteller ist das Verfahren auch ganz nützlich.

### **Norbert Luckhardt (<kes> - Die Zeitschrift für Informations- Sicherheit):**

Es gibt in Deutschland eine beträchtliche Zahl guter Leute, guter Ideen und guter Produkte zur IT-Sicherheit. Die Interessens- und Tätigkeitsschwerpunkte differieren dabei in verschiedenen Bereichen. So entstammen neue Ansätze beispielsweise zu Kryptographie und Datenschutz eher dem akademischen Umfeld, während sich die Anbieter von Sicherheitslösungen verständlicherweise vorrangig dem widmen, wofür der Markt aktuell einen konkreteren Bedarf hat. Für den Endanwender dürfte es dabei bisweilen schwierig sein, noch den Überblick über die Vielzahl der Angebote, Technologien und „Buzzwords“ zu behalten.