Ohne Sicherheit kein Vertrauen in E-Business und eingebettete Systeme

Die Stellv. Sprecherin und der Sprecher des Fachbereichs „Sicherheit – Schutz und Zuverlässigkeit“ der Gesellschaft für Informatik (GI)

Isabel Münch
BSI
Godesberger Allee 185-189
53175 Bonn
isabel.muench@bsi.bund.de

Manfred Reitenspieß
Fujitsu-Siemens Computers
Otto-Hahn-Ring 6
81793 München
manfred.reitenspiess@fujitsu-siemens.com

Abstract Das Fachgebiet Sicherheit hat sich in den vergangenen Jahren aus verschiedenen Disziplinen der Informatik als Querschnittsthema der Angewandten, Praktischen, Theoretischen und Technischen Informatik entwickelt. Die nachfolgenden Aspekte sollen dieser Entwicklung Rechnung tragen sowie die wachsende Bedeutung der Disziplin Sicherheit mit ihrem Leitbildcharakter für die Entwicklung sicherer Informatiksysteme akzentuieren. Im GI-Fachbereich „Sicherheit – Schutz und Zuverlässigkeit“ wird das Thema Sicherheit in seinem Bezug zur Informationstechnik sowohl wissenschaftlich als auch anwendungsorientiert bearbeitet.

1 Informatik-Themen im Bereich Sicherheit

Die folgende Aufzählung von Bereichen, deren Gliederung nur vorläufig sein kann, zeigt die Vielfalt der Informatik-Themen im Bereich Sicherheit: technische Grundlagen (u.a. Verlässlichkeit von Informatiksystemen, Zutritts-, Zugriffs- und Zugangskontrolle, Integrität von Daten, Infrastruktursicherheit); organisatorische Grundlagen (u.a. gesetzliche Regelungen, Datenschutz, IT-Sicherheitsmanagement, Sicherheitszertifizierungen); theoretische Grundlagen (u.a. Sicherheitsmodelle, Kryptographie, Protokollanalysen) sowie Anwendungen und spezielle Techniken (u.a. Elektronisches Geld, Biometrische Authentifikations- und Identifikationssysteme, Chipkarten, Firewalls, Intrusion Detection Systeme, Virenscanner).

Wichtige Themen sind darüber hinaus die Dienst- und Systemverfügbarkeit, wobei auch die Verfügbarkeit der Sicherheitseinrichtungen selbst relevant ist. Dazu gehören einerseits technologische Aspekte (Zuverlässigkeit, Schutz vor Fehlern, Fehlertolerierende Systeme), aber auch Aspekte der Sicherheit und des Schutzes dieser Systeme, z.B. vor Denial-of-Service Angriffen.

Die genannten Themen betreffen die gesamte Anwendungsbreite informationstechnischer Systeme. Beispielhaft seien genannt:

- der Einsatz von Computern in Fahr- und Flugzeugen,
- die Öffnung vormals dedizierter und abgeschlossener Systeme im Finanz- oder Behördenumfeld durch die Konvergenz von Informations- und Kommunikationstechnik, etwa durch UMTS, WLAN, DSL usw.

Die nachfolgenden Ausführungen skizzieren kurz die Entwicklung des Fachgebietes in den gesellschaftlichen Bereichen der Hochschulen und Wirtschaft.

2 Entwicklungen an den Hochschulen

Während bislang an den Hochschulen nur Teilaspekte der IT-Sicherheit in Lehrstuhlbeschreibungen und Bezeichnungen Niederschlag fanden (Kryptographie, Kommunikationssicherheit) oder IT-Sicherheit von anders lautenden Bereichen (mit)gelehrt wurde („Informatik und Gesellschaft“, „Anwendungen der Informatik in Geistes- und Naturwissenschaften“, „Kommunikation in Rechnernetzen“, „Theoretische Informatik“), sind in letzter Zeit an einigen Hochschulen ganze Lehrstühle und Bereiche für das Gebiet IT-Sicherheit ausgeschrieben worden. Hier lassen sich ein deutlicher „Run“ auf dieses Thema und eine Konsolidierung der Curricula ausmachen.

Sofern derzeit die wissenschaftliche „Community“ noch als überschaubar gelten kann, ist mittelfristig mit einer personellen Vergrößerung, verbunden mit einer stärkeren Ausdifferenzierung und Gruppierung der (fachlichen) Interessen, im gesamten Bereich der Sicherheit (Security und Safety) zu rechnen.

Trotzdem bleibt Sicherheit ein Querschnitts- bzw. Anwendungsthema, wobei einzelne Teilaspekte von anderen Bereichen der Informatik (Verifikation von Hard- und Software, Kommunikation in Netzen), Mathematik (Zahlentheorie, Kryptographie) aber auch von Ingenieurdisziplinen (physikalischer Schutz, z.B. Stromversorgung, Brandschutz, Zutrittsschutz, Fehlertoleranz, Softwarediversität usw.) detailliert untersucht und in die Thematik Sicherheit eingebunden werden.

3 Sicherheit im betriebswirtschaftlichen und industriellen Umfeld

Zuverlässigkeit und „Safety“ haben im wirtschaftlichen Bereich eine lange Tradition, da die Zuverlässigkeit und Verfügbarkeit von Systemen unmittelbar den Geschäftserfolg beeinflussen (Telekommunikation, Kraftwerke). Teilweise wurde „Safety“ von Systemen auch institutionalisiert und einer staatlichen Überwachung unterworfen, u.a. durch Luftfahrt-Bundesamt, Eisenbahn-Bundesamt, Kraftfahrt-Bundesamt, usw.

Auch das Bewusstsein um die Bedeutung der IT-Sicherheit hat sich gerade im industriellen Umfeld in den letzten Jahren erheblich vertieft. Dazu gehört nicht nur der Einsatz von Virenscannern oder Firewall-Programmen. Es gibt kaum noch Anwendungen, die ohne Zugriffsschutz oder verschlüsselte Übertragung auskommen. Authentizität, Integrität, Vertraulichkeit und Nachweisbarkeit von Kommunikationsvorgängen

in und zwischen Unternehmen sind heute unabdingbar.

Entwicklungen in sicherheitskritischen Bereichen werden schon seit langem durch geeignete Risikobewertungen und Maßnahmenpakete begleitet. Neu hinzugekommen sind Standardisierungsarbeiten im Verfügbarkeitsbereich wie zum Beispiel dem „Service Availability™-Forum“.

Mittelfristig wird ein besonderes Augenmerk auf die Administration und die Benutzung von Sicherheitsverfahren gelegt werden, so dass ihre Nutzung einfach und selbstverständlich wird. Die wachsende Zahl von integrierten Informations- und Kommunikationssystemen erfordert Konzepte und Mechanismen für ihre weitgehende autonome Funktion und der Sicherstellung ihrer Überlebensfähigkeit. Dazu gehören neben klassischen Zuverlässigkeits- und „Safety“-Aspekten (Ausfallsicherheit, Funktionssicherheit) auch der Schutz vor Angriffen physikalischer oder logischer Natur. Dies fand auch Eingang in das von GI und VDE/ITG vorgestellte Konzept des „Organic Computing“ als Systemparadigma 2010. Zuverlässigkeit und Schutz sind grundsätzliche Eigenschaften eines solchen Systems.

4 Lehre, Ausbildung und Vernetzung im Bereich IT-Sicherheit

In den Gebieten der IT-Sicherheit ist neben der Wissensvermittlung an Hochschulen in den letzten Jahren auch auf dem privaten Sektor eine Verstärkung der Aus- und Weiterbildung zu beobachten, die teilweise durch Zertifizierungsprogramme institutionalisiert und qualitätsgesichert werden. Die an Zahl wachsenden IT-Sicherheitskonferenzen sind teilweise überfüllt.

5 Wachsende volkswirtschaftliche Bedeutung der IT-Sicherheit

Es besteht ein starkes volkswirtschaftliches (und staatliches) Interesse an einer funktionierenden und sicheren Informationsverarbeitung, da durch die zunehmende Vernetzung von IT-Systemen auch deren Verletzlichkeit zugenommen hat. Sofern nicht durch IT-Sicherheitsprozesse, Schutz- und Notfallmaßnahmen innerhalb der betroffenen Institutionen aufgefangen, können sich sicherheits-verletzende Ereignisse ausbreiten und in ihrer Gesamtheit im Extremfall auch schwere volkswirtschaftliche Folgekosten verursachen. Die gemeinsamen Anstrengungen von Behörden und Unternehmen zur Jahr 2000-Problematik sowie die Folgekosten der Ausbreitung von E-Mail-Viren und -Würmern sind nur einige Beispiele hierfür.

Zu nennen sind auch Industrieinitiativen im Bereich der Verfügbarkeit (Raumfahrt, Telekommunikation, E-Commerce). Bei Betrachtung der volkswirtschaftlichen Bedeutung des Electronic Business wird deutlich, dass eine koordinierte Vorgehensweise ganz wesentlich auch zum wirtschaftlichen Erfolg beitragen kann (Bewusstseinsbildung, Ausschreibungen, gesetzliche Anforderungen).

6 Laufende Aktivitäten im Fachbereich Sicherheit

Der im Februar 2002 neu gegründete Fachbereich „Sicherheit - Schutz und Zuverlässigkeit“ besteht mittlerweile aus 15 Fachgruppen zum Thema Sicherheit. Diese haben bereits eine Vielzahl von Aktivitäten und Veranstaltungen durchgeführt. Ein Überblick hierüber findet sich auf den Webseiten des Fachbereichs. Hierzu gehören beispielsweise:

- Arbeitsgruppe „Sicherheit in der Informatik-Ausbildung“: Um dem Bedürfnis nach mehr Sicherheit in der Ausbildung Rechnung zu tragen, werden Empfehlungen erarbeitet, in denen die Mindestanforderungen zur Integration von Sicherheit in der Informatik-Ausbildung formuliert werden.
- Arbeitsgruppe „Begriffsbildung“: Hier soll eine inhaltliche Abstimmung der im Umfeld Sicherheit gebräuchlichen (deutschen) Begriffe stattfinden, so dass das Gebiet Sicherheit mit einer einheitlichen Begriffswelt arbeiten kann.
- Bewusstseinsbildung für Sicherheit bei allen Anwendern von Informations- und Kommunikationstechnik.
- Mitgestaltung der GI-Jahrestagung 2003: Der Fachbereich und seine Fachgruppen bilden mit einem breiten Programm den Schwerpunkt „Sicherheit – Schutz und Zuverlässigkeit“ des 33. GI-Jahreskongresses.

7 Ausblick

Als „wichtigen Beitrag auf dem Weg zur Informationsgesellschaft“ hat daher Prof. Heinrich C. Mayr, Präsident der Gesellschaft für Informatik e.V. (GI) die Einrichtung des Fachbereichs „Sicherheit – Schutz und Zuverlässigkeit“ in der GI bezeichnet. „Zwar haben sich die Fachleute in der GI auch bisher schon intensiv mit den beiden Seiten des Themas Sicherheit beschäftigt. Mit der Einrichtung eines eigenen Fachbereiches tragen wir aber den gestiegenen Anforderungen an die Sicherheit von Informationssystemen und deren breiter Bearbeitung Rechnung.“

Weiterführende Links

- Webseiten des GI-Fachbereichs „Sicherheit – Schutz und Zuverlässigkeit“ unter www.gi-fb-sicherheit.de
- Fachgruppe Security (FGSec) der Schweizer Informatiker Gesellschaft (SI) unter www.fgsec.ch
- Arbeitskreis IT-Sicherheit in Österreich der Österreichischen Computer Gesellschaft unter www.ocg.at/ueber-uns/arbeitskreise/akit.html