

## Thementext

*„Die natürliche Neugierde der Konkurrenz ist auf einmal schachmatt gesetzt durch eine Maschine, mit der Sie all Ihre Dokumente vollständig geheim halten können.“*

*Arthur Scherbius, Erfinder der „Enigma“-Chiffriermaschine*

## Informatik und Sicherheit

In Zeiten zunehmender Globalisierung, steigender Mobilität und wachsender Abhängigkeit der Industrienationen von Informations- und Kommunikationstechnologien gewinnen Aspekte wie Sicherheit und Zuverlässigkeit in der Informatik immer mehr an Bedeutung. Neue technische Möglichkeiten werfen neue Fragen auf: Reichen bestehende Vorstellungen über Sicherheit in einer vernetzten Welt noch aus? Wie sicherheitsbewusst sollte man im 21. Jahrhundert überhaupt sein? Können wir den verwendeten IT-Infrastrukturen vertrauen? Sind persönliche Daten mit den neuen Biometrieverfahren ausreichend geschützt? Oder birgt die Erfassung körperlicher Daten (Iris, Genom) nicht vielleicht sogar neue Risiken?

Sicherheit ist ein Begriff, der in einer vernetzten Welt neue Inhalte bekommt. Ein sicherer Zustand bezeichnet nicht mehr in erster Linie den Schutz von Leben und Gesundheit. Sicherheit im Kontext der Informationsgesellschaft umfasst vielmehr vier Bereiche, die über eine klassische Bedeutung von Sicherheit hinausgehen: die Vertraulichkeit von Informationen, die Verfügbarkeit von Informationssystemen, die Integrität von Daten und der Schutz gegen Vandalismus.

### **Vandalismus: ständige Wachsamkeit gefragt**

Das Bewusstsein über die Notwendigkeit digitaler Schutzmaßnahmen ist in Deutschland relativ groß. Der Schutz von Systemen gegen Vandalismus umfasst im Internetzeitalter vor allem auch die Systeme selbst, die darüber wachen, dass Computerviren oder andere Angriffe so wenig wie möglich Schaden anrichten. Von allen Bereichen der digitalen Sicherheit ist dieser Schutz der am meisten bekannte: Fast 90 Prozent der Unternehmen in Deutschland haben auf jedem Rechner einen Virenschoner installiert, 60 Prozent nutzen eine Firewall und 40 Prozent der beruflichen IT-Nutzer haben eine so genannte Monitorsoftware installiert, die über die Webnutzung und die Angriffe berichtet.

Hinzu kommt, dass sich die Strategie der „Angreifer“ ständig ändert. Eine weitere Tendenz, die sich klar abzeichnet: Hacker verfolgen zunehmend wirtschaftliche Ziele. Im Vordergrund steht nicht mehr der Vandalismus oder das Erlangen von Ruhm, sondern das Gewinnstreben durch den Verkauf vertraulicher Informationen. Für Unternehmen und auch für Privatleute heißt das, eine stetige Wachsamkeit zu entwickeln, um Systeme gegen unbefugte Zugriffe zu schützen.

### **Vertraulichkeit: drei Szenarien**

Die Vertraulichkeit von Daten ist durch eine zunehmende Vernetzung der Computer stark gefährdet. Es gibt viele Szenarien aus unserer alltäglichen Umgebung, die unbefugte Zugriffe auf Daten und damit verbundene Folgen aufzeigen.

Erstes Beispiel: Moderne Arbeitsmethoden in einer Kanzlei sind geprägt von Mobilität. Ein Rechtsanwalt, der Daten eines Mandanten in seinem Laptop speichert, das über einen drahtlosen Internetanschluss verfügt, muss das Risiko bedenken, dass Fremde über Funk Zugang zu seinem Fileserver erhalten können. Das könnte fatale Folgen beispielsweise in einem Prozess haben. Gerade weil die Nutzung des Wireless LAN (WLAN) als drahtlose Erweiterung eines traditionellen lokalen Netzes einen festen Platz in den Zugangstechniken zur IT-Infrastruktur eingenommen hat, müssen dessen Sicherheitsmechanismen umso exakter genutzt werden.

Ein anderes Beispiel: Eine Psychologin mit umfangreicher Patientendatei spielt eines Tages eine Musik-CD auf ihrem Praxis-Computer ab. Dabei wird ein Programm auf der Festplatte installiert, das ein illegales Kopieren der CD verhindern soll. Das Programm bleibt von allen gängigen Virencannern unbemerkt. Später findet ein Hacker über das Internet dank des unsichtbar installierten Programms leichten Zugang zu den Patientenakten und somit streng vertraulichen Daten.

Ein weiteres Szenario: Ein High-Tech-Unternehmen hat eine neue Erfindung auf dem internen Server gespeichert. Die Daten sind kryptographisch verschlüsselt, und das interne Netzwerk ist gut abgesichert gegen einen Zugriff über das Internet. Das WLAN ist digital verriegelt und die Firma leistet sich regelmäßig neue Software zur Datensicherheit. So weit wurden alle technischen Schutzmaßnahmen berücksichtigt. Alle Mitarbeiter des Unternehmens haben jedoch freien Zugang zum Serverraum. Ohne größere Mühe wäre es möglich, in kurzer Zeit alle Kenntnisse über die Erfindung, die Preislisten und Kalkulationen auf einem USB-Stick zu speichern. Das benötigte Passwort befindet sich auf einem Zettel neben dem Monitor. Besonders unter

den Bedingungen eines sich verschärfenden Wettbewerbs kann dies fatale Folgen haben.

Diese Beispiele zeigen, dass der Schutz von gesamten IT-Landschaften immer wichtiger wird. Dabei muss die Gefahr nicht immer von dem PC oder Laptop ausgehen. Die Sicherheitslücken betreffen jetzt auch Mobiltelefone und andere mobile digitale Geräte, die per Funk erreichbar sind.

Eine geänderte Gesetzeslage trägt dazu bei, die Sensibilität für IT-Sicherheitsthemen zu erhöhen: Vorstände und Geschäftsführer sind persönlich für Versäumnisse und mangelnde Risikovorsorge verantwortlich. Für bestimmte Berufsgruppen wie Ärzte, Rechtsanwälte oder Angehörige sozialer Berufe gibt es neuerdings Sonderregelungen im Strafgesetzbuch, die sogar Freiheitsstrafen vorsehen, wenn vertrauliche Angaben von Patienten, Mandanten oder Klienten ohne Einwilligung öffentlich gemacht werden (§ 203 StGB). Bereits ein fahrlässiger Umgang mit Informationstechnik kann diesen Tatbestand unter Umständen verwirklichen. An der Schnittstelle zwischen Hochfrequenztechnik, Nachrichtentechnik und Elektronik liefert die Informatik die Konzepte zur „abhörsicheren“ digitalen Informationsübertragung. Sie entwickelt Risikoanalysen, die untersuchen, wie wahrscheinlich das Eintreten eines bestimmten Schadensszenarios ist, neue Verfahren zur Authentifizierung der Identität von Personen und neue mathematische Methoden, mit denen Daten sicherer digital verschlüsselt werden.

### **Verfügbarkeit: das Informationsherz der Gesellschaft**

Benutzer von Informationssystemen sind darauf angewiesen, dass Dienstleistungen, Funktionen oder auch Informationen zum geforderten Zeitpunkt zur Verfügung stehen. Für viele Firmen ist dies von entscheidender Bedeutung.

Heute sind mit der Verfügbarkeit von Informationen nicht mehr ausschließlich die klassischen Kernbereiche der Informationsgesellschaft betroffen. Die Informatik gewinnt auch eine immer größere Bedeutung in Fabriknetzwerken, Steuerungssystemen, wie etwa in Aufzug oder Klimaanlage, und in industriellen Anlagen. Bisher blieben diese von den Risiken aus dem PC-Bereich weitgehend verschont, da sie Daten über spezielle Industrienetze austauschten.

Doch seitdem verstärkt Anwendungen und Übertragungssysteme aus dem Büroumfeld in der Produktion eingesetzt werden, ist auch die Verfügbarkeit von Industriesystemen betroffen. Die klassischen Informationssysteme in Maschinen und Geräten werden immer mehr von einem Netzwerk ersetzt, das

kompatibel ist zu dem Informationsprotokoll, auf dessen Basis auch das Internet funktioniert, das TCP/IP. Damit sind Produktionshallen, Prozessleitsysteme und Steuerungseinheiten für die gleichen Sicherheitslücken im Datennetz wie der PC auf dem Schreibtisch anfällig geworden. Und laut VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) haben nur 14 Prozent aller Betriebe, die ihre Prozessleitsysteme und Steuerungen ans Internet angeschlossen haben, diese ausreichend gegen schädliche Einflüsse geschützt. Das ist ein großes Sicherheitsrisiko, da das ganze übergeordnete System ausfallen kann, wenn nur eine Steuereinheit oder ein Sensor betroffen ist.

Das Internet ist mit mehreren Millionen Benutzern und weltweiter Ausbreitung eine Quelle für mögliche Angriffe auf die Verfügbarkeit der angeschlossenen Rechner. Technische Anlagen sind für Hacker zwar derzeit noch keine so interessanten Ziele, aber ein Virus, der sich vom Rechner eines Mitarbeiters auf das interne Netzwerk verbreitet, könnte eine ganze Produktionslinie stilllegen. Problematisch wird es, wenn terroristische Motive eine Rolle spielen: mit dem Internet verfügen Terroristen weltweit über immer mehr Möglichkeiten, von außen wichtige Anlagen anzugreifen. Neben der Funktionalität und Leistungsfähigkeit sollte also auch im Produktionsbereich die Verfügbarkeit der IT-Systeme als gleichrangiges Ziel bereits bei der Entwicklung und beim Erwerb eines Rechnersystems berücksichtigt werden.

Die Aufgabe der Informatik besteht darin, Strategien zu entwickeln, die die Verfügbarkeit der Informationssysteme gewährleisten. Einerseits besteht diese aus konkreten Maßnahmen wie etwa die doppelte Ausstattung von Hardware oder die Entwicklung von Software, die automatisch Sicherheitskopien erstellt oder systematisch die Zugriffsrechte für verschiedene Nutzer des Netzwerks definiert. Andererseits gehört auch die wissenschaftliche Fragestellung zur Informatik, wie Menschen und Organisationen auf Computersysteme und ihre Verfügbarkeit vertrauen.

### **Integrität: die Richtigkeit der Information**

Mit der Integrität von Daten ist gemeint, dass die bereitgestellten Informationen vollständig sind, vom angegebenen Absender stammen und dass die Daten nach dem Versand durch den Absender inhaltlich unverändert geblieben sind. Der Verlust der Integrität bedeutet, dass Informationen unerlaubt verändert wurden. Ohne Schutzvorkehrungen ist einer digitalen Datei nicht anzumerken, ob diese drei Kriterien der Integrität erfüllt sind. Dies ist ein Grund, warum ein digitaler Kontoausdruck für das Finanzamt keine Beweiskraft hat. Denn es ist

nicht zweifelsfrei ersichtlich, ob die darin enthaltenen Daten vollständig sind, ob sie von der angegebenen Bank stammen und ob die Zahlen nicht nachträglich manipuliert wurden.

Die Informatik hat die theoretischen und praktischen Verfahren zur Verfügung gestellt, die Integrität von elektronischen Dokumenten sicherzustellen. Die Methoden sind technisch seit einigen Jahrzehnten bekannt, es mangelt allerdings noch an ihrer allgemeinen Anwendung. Die Aufgabe der Informatik besteht also jetzt darin, die existierenden Verfahren einfacher zu gestalten und bei hoher Sicherheit auch nutzerfreundlich zu sein.

In einer vernetzten Welt hat die Integrität von Information eine neue Bedeutung erhalten. Im Internet kann jeder Nutzer Informationen verbreiten, ohne dabei Rücksicht auf ihre Vollständigkeit oder Richtigkeit zu nehmen. Für Projekte wie freie Enzyklopädien, in die jeder sein Wissen eintragen kann, ergibt sich daher eine besondere Aufgabe der Informatik: das Verfügbarmachen von „Metadaten“, eine automatische und akribisch geführte Buchhaltung darüber, wer wann welche Informationen zugefügt, gelöscht oder verändert hat. Nur so kann Wissen im Netz zur Erhöhung der Datenintegrität beigetragen.

Integrität ist aber nicht nur eine Frage von digitalen Signaturen und Metadaten. Schon einer der Pioniere der theoretischen Informatik, der niederländische Wissenschaftler Edsger Wybe Dijkstra, warf in den siebziger Jahren die Frage auf: „Wenn ein automatischer Computer Ergebnisse produziert, warum sollten wir diesen Vertrauen schenken? Und so wir dies schon machen, welche Maßnahmen können wir ergreifen, damit wir das Vertrauen darin, dass die Ergebnisse tatsächlich die gemeinten Resultate darstellen, zunimmt?“ Die Informatik als Wissenschaft widmet sich auch Fragen wie diesen. Sie stellt die abstrakten Kriterien auf, die festlegen, wann bei einer automatischen Speicherung, Verarbeitung und Präsentation von Informationen mit Hilfe der Informationstechnik die Integrität der Daten sichergestellt ist. Vertrauen ist ein elementares soziales Bedürfnis. Die Informatik trägt dazu bei, dass es auch bei komplexen Systemen nicht zu einem Vertrauensbruch zwischen Mensch und Technik kommen muss.

Alles in allem ist Sicherheit im digitalen Zeitalter mehr als ein Produkt. Sie ist vor allem eine Vertrauensfrage. Nur wenn Anwender aufgrund entsprechender Schutzvorrichtungen das Gefühl haben, dass sie mehr unterstützt als behindert werden, werden Sicherheitsvorkehrungen in der Praxis angenommen. Digitale Sicherheit im 21. Jahrhundert ist demnach nicht nur eine technische Angelegenheit. Der Schlüssel zu diesem Thema ist eine eher ganzheitliche Vision: Es ist das Zusammenspiel aus neuen Technologien und wirtschaftlichen, menschlichen und gesellschaftlichen Kräften, das Sicherheit ermöglicht. Das

fordert von allen Beteiligten Voraussicht, Um- und Weiterdenken. Eine gut informierte breite Öffentlichkeit ist die beste Allianz für Sicherheit im Informationszeitalter.

**Abdruck honorarfrei, Belegexemplar erbeten.  
Für weitere Informationen wenden Sie sich bitte an:**

**Team Informatikjahr**

Susanne Kumar-Sinner  
Neue Schönhauser Straße 3-5  
10178 Berlin  
Tel.: 030 / 590 04 33 - 11  
Fax: 030 / 590 04 33 - 51  
E-Mail: [kumar@informatikjahr.de](mailto:kumar@informatikjahr.de)  
[www.informatikjahr.de](http://www.informatikjahr.de)

Tiziana Zugaro-Merimi  
Neue Schönhauser Straße 3-5  
10178 Berlin  
Tel.: 030 / 590 04 33 - 54  
Fax: 030 / 590 04 33 - 51  
E-Mail: [zugaro@informatikjahr.de](mailto:zugaro@informatikjahr.de)  
[www.informatikjahr.de](http://www.informatikjahr.de)