

Aus- und Weiterbildung in IT-Sicherheit

Harald Baier¹, Johannes Buchmann², Christoph Busch³

Kurzfassung

Wir stellen Inhalte, Adressatengruppen, Organisation und Angebote der Aus- und Weiterbildung in Deutschland vor.

1 Einleitung

Informationstechnologie (IT) ist das Rückgrat von Unternehmen, Forschungseinrichtungen und öffentlicher Verwaltung. Auch für Privatleute wird die Informationstechnologie immer wichtiger. Sie bekommen wichtige Informationen aus dem Internet, schreiben Emails und kaufen dort ein. Schäden an IT-Systemen und Angriffe auf solche Systeme können zu Ausspähung, Verlust und Veränderung wichtiger Daten, zu erheblicher Beeinträchtigung der Kommunikation, zu Schäden in der Produktion, zu Unfällen und zu vielen anderen schwerwiegenden Problemen mit weitreichenden Folgen führen.

IT-Sicherheit ist also in allen Bereichen der Gesellschaft und Wirtschaft von großer Bedeutung. IT-Sicherheit kann es nur geben, wenn diejenigen, die mit IT-Systemen umgehen, die Bedrohungen einschätzen können, die Gegenmaßnahmen kennen und adäquat umsetzen. Das setzt Aus- und Weiterbildung in IT-Sicherheit voraus. In der Sicherheits-Community hat sich der Slogan „It’s not a product – it’s a process.“⁴ eingebürgert. Damit kommt zum Ausdruck, dass man sich IT-Sicherheit nicht mit einem Produkt oder als Produktpalette kaufen kann. Vielmehr erreicht man IT-Sicherheit erst in einem dauerhaften, dynamischen Prozess, der den Veränderungen sowohl hinsichtlich der eingesetzten IT-Infrastrukturen als auch hinsichtlich erweiterter Bedrohungen gerecht wird. Aus- und Weiterbildung ist ein Baustein in diesem Prozess.

Dieser Artikel will einen Beitrag zu der Frage leisten, welche Möglichkeiten der Aus- und Weiterbildung es heute schon gibt und wie solche Aus- und Weiterbildung adäquat realisiert werden kann.

¹ Darmstädter Zentrum für IT-Sicherheit

² Technische Universität Darmstadt

³ Fraunhofer Institut für Graphische Datenverarbeitung

⁴ Geschützt von der Firma Dignet GmbH

2 Inhalte der Aus- und Weiterbildung

IT-Sicherheit ist heute ein sehr breites Gebiet, in dem viele wissenschaftliche, technische und organisatorische Themen von Bedeutung sind. Wir erläutern im Folgenden Inhalte, die aus unserer Sicht wichtig für die Aus- und Weiterbildung in der IT-Sicherheit sind. Wir stellen zunächst grundlegende Themen dar. Anschließend gehen wir auf den weiterführenden Aspekt der Systemsicherheit ein. Wir schließen dieses Kapitel mit Aus- und Weiterbildungsthemen, die mit konkreten Anwendungen verbunden sind.

Wir beginnen mit einigen grundlegenden Themen.

Kryptographie: Bei der Umsetzung von IT-Sicherheit spielen kryptographische Techniken wie zum Beispiel Verschlüsselung, elektronische Signaturen und Identifikationsverfahren eine wichtige Rolle. Wer solche Techniken anwendet, muss wissen, wie sie funktionieren. Wer über ihren Einsatz entscheidet, muss die richtigen Verfahren auswählen und ihre Sicherheit einschätzen können. Kryptographische Verfahren werden erfunden und nach einiger Zeit gebrochen. Das ist so seit vielen hundert Jahren und es ist nicht absehbar, dass sich das ändert. Darum müssen Anwender ihr kryptographisches Wissen immer wieder aktualisieren. Sie müssen auch wissen, welche Krypto-Standards und rechtlichen Vorschriften (zum Beispiel das Signaturgesetz) es gibt, wie kryptographische Verfahren effizient implementiert werden und welche Implementierungen es schon gibt.

Biometrie: Unveränderliche Merkmale von Menschen wie das Gesicht, die Iris oder der Fingerabdruck können zu ihrer Identifikation eingesetzt werden. Solche biometrischen Verfahren haben Vorteile gegenüber geheimen PINs. Wer Biometrie einsetzen will, muss wissen, wie biometrische Erkennung im Prinzip funktioniert, wie man sie technisch umsetzt und in welchem Maße sie akzeptiert wird. Allerdings sind beim Einsatz auch die Grenzen der biometrischen Verfahren zu berücksichtigen: Beim Vergleich vorgelegter biometrischer Merkmale mit den gespeicherten Referenzdaten eines Menschen gibt es keine Bit-genaue Übereinstimmung. Dies macht es notwendig, für die jeweilige Anwendung sinnvolle Fehlertoleranzen zu konfigurieren.

Netzwerkprotokolle: Netzwerkprotokolle wie TCP/IP sind fundamental für Netzwerke. Gleichzeitig sind sie die Achillesferse der IT-Sicherheit. Denn sie stammen aus einer Zeit, in der weitgehend Stand-Alone-Computer oder lokale Netze verwendet wurden. Sicherheitsmechanismen spielten damals keine Rolle. Um die Bedrohungen aus dem Fehlen von Sicherheitseigenschaften der Protokolle einschätzen und beheben zu können, muss man ein grundlegendes Verständnis von Netzwerkprotokollen haben.

Datenschutz: Je mehr Daten über Personen elektronisch gespeichert und verarbeitet werden, desto mehr wächst die Notwendigkeit, diese Daten vor Missbrauch wie etwa die unberechtigte Verknüpfung von Datenbeständen zu schützen. Hier sind zum Beispiel medizinische Daten oder Personaldaten betroffen. Wer sich mit Datenschutz beschäftigt,

muss wissen, wie die rechtlichen Vorschriften für den Datenschutz sind und welche technischen Möglichkeiten es gibt, Datenschutz zu realisieren.

IT-Sicherheit wird jedoch nicht durch die Absicherung einzelner Komponenten erreicht. Das ganze IT-System muss sicher gemacht werden. Im Gebiet der Systemsicherheit mit ihrem dynamischen Charakter sehen wir u.a. folgende, wichtige Aus- und Weiterbildungsthemen:

Security-Engineering: Die Leitfragen im Security-Engineering lauten zum Beispiel: Wie konstruiert man eigentlich sichere IT-Systeme? Wie analysiert und bewertet man die Bedrohungen? Welche Risiken können akzeptiert werden? Welche Maßnahmen muss man ergreifen und welche nicht? Solche grundlegenden Fragen stehen bei der Entwicklung einer Sicherheitspolitik in Unternehmen oder Institutionen im Vordergrund. Wichtig sind auch die Konzepte zur Umsetzung einer Sicherheitspolitik durch organisatorische und technische Maßnahmen.

Netzwerk-Sicherheit: Mögliche Fragen in diesem Themengebiet sind: Wie stelle ich fest, welche Rechner und Dienste des Netzwerks aus dem Internet erreichbar sind? Welche Arten von Firewalls gibt es, wie funktionieren sie jeweils und welche Bedrohungen können sie abwenden? Wie werden Virtual Private Networks konstruiert? Wie können unterschiedliche Firmenstandorte sicher verbunden werden? Diese Fragen spielen überall da eine Rolle, wo Rechnernetze betrieben werden.

Public-Key-Infrastrukturen: Grundlegende Fragen aus dem komplexen Gebiet der Public-Key-Infrastrukturen (PKI) sind: Was leistet eine PKI? Wie wird sie aufgebaut? Welche Sicherheitsanforderungen müssen die einzelnen Komponenten (Registrierung, Zertifizierung, Zertifikatsmanagement) erfüllen? Wie häufig müssen Schlüssel oder Zertifikate erneuert werden? Muss die PKI dem deutschen Signaturgesetz entsprechen? Was besagen das Signaturgesetz und die entsprechende Verordnung?

Mobile Security: Welche Sicherheitsprobleme haben WLANs? Wie vermeidet man sie? Welche Sicherheitsmechanismen gibt es in Bluetooth? Wie vertraulich sind Handy-Gespräche? Welche Sicherheit bieten die neuen Protokolle der dritten und vierten Generation? Je mehr mobile Computer-Infrastrukturen eingeführt werden, desto wichtiger werden solche Fragen für die Anwender und Administratoren.

Sicherheitsniveaus: Wir sehen zu diesem Thema folgende Leitfragen: Welche Sicherheitsstufen gibt es? Wie stelle ich meinen Schutzbedarf fest? Welche Inhalte stellt das Grundschutzhandbuch des BSI dar, wie arbeite ich mit diesem und welchen Schutz bietet es? Was unterscheidet das Grundschutzhandbuch von internationalen Standards wie ISO/IEC 17799 (BS 7799)? Was besagen Sicherheitsevaluationen nach Kriterienwerken wie ITSEC oder den Common Criteria? Wir machen darauf aufmerksam, dass diese Fragen einen wesentlichen Inhalt des Security-Engineering ausmachen.

Spezielle Sicherheitsbedrohungen: Auch Aus- und Weiterbildungsmaßnahmen zu speziellen, aber doch sehr verbreiteten Bedrohungen sind sinnvoll. Zum Beispiel sind Angriffe durch Viren, trojanische Pferde oder (Distributed) Denial of Service Attacken verbreitet. Man sollte daher ihre Funktionsweise verstehen und gängige Abwehrmaßnahmen kennen und anwenden.

Von großer Bedeutung ist die Sicherheit konkreter IT-Anwendungen:

Digital-Rights-Management: Wie kann das Copyright auf digitale Daten geschützt werden? Das ist eine zentrale Frage für alle, die elektronische Bücher, Zeitschriften oder Musikdateien anbieten. Welche Möglichkeiten zum Nachweis der Urheberschaft an solchen Werken gibt es und wie können solche Nachweise trotz der weiterbestehenden Medienbrüche zur analogen Welt geführt werden. Wie können im Handel mit elektronischen Waren die Interessen aller Beteiligten im Sinne einer mehrseitigen Sicherheit gewahrt werden.

Bezahlen: Besonders sicherheitskritisch ist das Bezahlen im Internet. Es gibt viele verschiedene Bezahlverfahren, die unterschiedlich sicher sind. Manche erlauben anonymes Bezahlen, andere nicht. Sowohl Anbieter als auch Anwender sollten die Sicherheitsvor- und -nachteile des eingesetzten Verfahrens kennen.

Email: Wodurch werden Emails authentisch? Was garantiert ihre Unverfälschtheit? Welche Verfahren machen eine Email verbindlich? Das sind wichtige Fragen, wenn Email zu einem wichtigen Kommunikationsmedium wird.

SAP: Software von SAP wird von vielen Unternehmen und Verwaltungen eingesetzt. Zentrale Fragen für Unternehmenssoftware sind: Wie wird der Zugriff (lesend bzw. schreibend) auf Daten in SAP-Systemen gesichert? Wie erkenne ich Manipulationen? Wie erreiche ich Revisionsfähigkeit meines SAP-Systems?

Auch wenn man mit der Funktionsweise eines Sicherheitsverfahrens vertraut ist, so bedeutet dies nicht automatisch, dass man das entsprechende Produkt adäquat bedienen kann. Je nach Komplexität der Soft- oder Hardware kommen daher Produktschulungen in Betracht. Diese sollen in den richtigen Umgang mit speziellen Produkten wie Firewalls, Anti-Virus-Programmen oder PKIs einführen.

3 Zielgruppen der Aus- und Weiterbildung

In diesem Abschnitt gehen wir der Frage nach, wer Aus- und Weiterbildung in IT-Sicherheit braucht.

IT-Sicherheitsverantwortliche: In Ihrer Hand liegt die Entwicklung von Strategien, Konzepten und Maßnahmen zur Umsetzung von IT-Sicherheit im Unternehmen. Sie müssen die technischen, rechtlichen und organisatorischen Grundlagen der IT-Sicherheit

kennen, weil sie ja geeignete Maßnahmen vorschlagen sollen. Sie müssen in der Lage sein, zu beurteilen, ob Produkte ihren Anforderungen entsprechen.

Administratoren: In jeder Gruppe von Administratoren, die ein IT-System betreuen, muss es Fachleute für IT-Sicherheit geben. Diese IT-Sicherheitsexperten brauchen gute Kenntnisse der ganzen Palette der IT-Sicherheit Auch Sie müssen mit den technischen Grundlagen der IT-Sicherheit vertraut sein. Sie müssen die Weiterentwicklung der Angriffe auf IT-Systeme verfolgen und angemessen darauf reagieren. Gerade in diesem Bereich gibt es viele überraschende Entwicklungen, weil Mathematiker, Informatiker und Hacker mit großem Ehrgeiz versuchen, IT-Sicherheitssysteme zu brechen. Daher brauchen solche Administratoren eine solide Grundausbildung in der IT-Sicherheit und ständig berufsbegleitende Weiterbildung.

IT-Entscheider: Diejenigen, die über Strategien und Investitionen im Bereich der Informationstechnologie entscheiden, brauchen entsprechende Grundkenntnisse in IT-Sicherheit. Sie müssen die IT-Sicherheitsrisiken (auch die langfristigen) und ihre Lösungsmöglichkeiten grundsätzlich kennen. Sie müssen einschätzen können, welchen Aufwand die Absicherung von IT-Systemen bedeutet, um angemessene Budgets bereitstellen zu können. Die IT-Entscheider müssen in der IT-Weiterbildung Verfahren kennenlernen, um ein Return on Security Investment (ROSI) für Ihren Verantwortungsbereich berechnen zu können. Diese Kennzahl soll den Kosten-Nutzen-Effekt von Investitionen in IT-Sicherheit ausdrücken. Mit Hilfe des ROSI hat der IT-Entscheider ein Zahlenwerk zur Hand, das das obere Management vom Sinn des Budgets der IT-Sicherheit überzeugt.

Anwender: Sind IT-Sicherheitssysteme installiert, müssen sie von Anwendern angenommen und angemessen benutzt werden. Das ist dann die zentrale Voraussetzung für eine wirkliche Umsetzung von IT-Sicherheit. Anwender müssen zum Beispiel lernen, wie sie mit geheimen Passwörtern umgehen, wie sie ihre Chipkarten vor Missbrauch schützen, wann sie Emails verschlüsseln und signieren. Dazu sind entsprechende Schulungen nötig, die einerseits ein Grundverständnis für die Sicherheitsmechanismen wecken und andererseits die Verwendung der Sicherheitstechniken einüben. Ziel der Schulungen ist es, beim Anwender ein grundlegendes Sicherheitsbewusstsein (Security Awareness) aufzubauen. Solche Schulungen müssen regelmäßig wiederholt werden. Diese Weiterbildungsmaßnahmen bilden ferner einen guten Rahmen, um Mitarbeiter mit den Sicherheitsrichtlinien ihres Arbeitgebers vertraut zu machen. Oft scheitert das Einhalten von vorgeschriebenen Sicherheitsmaßnahmen beim Anwender aus schlichter Unkenntnis der Richtlinien.

Politiker: Die Umsetzung von Sicherheit im Internet ist auch eine politische Aufgabe. Gesetze wie zum Beispiel das deutsche Signaturgesetz oder die europäische Signaturrechtlinie können Rahmenbedingungen für die sichere Nutzung des Internets schaffen. Andererseits können in öffentlich finanzierten Projekten geeignete Verfahren

und Produkte entwickelt und deren Akzeptanz gefördert werden. Politiker müssen entscheiden, wie solche Gesetze aussehen und welche Projekte finanziert werden. Dazu müssen Sie Bedrohungen, auch längerfristige, erkennen und einschätzen können. Sie müssen auch wissen, welche Gegenmaßnahmen geeignet sind. Im Bereich der Kryptographie ist zum Beispiel absehbar, dass Quantencomputer in etwa zwanzig Jahren die heute bekannten PKI-Techniken unsicher machen werden. Die Entwicklung von alternativen Verfahren bis zur Standardisierung, Produktreife und Einführung dauert viele Jahre. Damit muss heute begonnen werden. Die Politiker, die darüber zu entscheiden haben, müssen ein kryptographisches Grundverständnis haben, um rechtzeitig wichtige Themengebiete zu fördern.

Datenschützer: Hauptamtliche Datenschützer, Datenschutzbeauftragte, Personalvertreter und andere, die den Missbrauch von Computerdaten verhindern sollen, müssen die Missbrauchsmöglichkeiten einschätzen können. Sie müssen auch beurteilen können, welche Gegenmaßnahmen adäquat sind. Das ist besonders wichtig, weil solche Maßnahmen manchmal die Benutzung unkomfortabler machen.

4 Organisation der Aus- und Weiterbildung in IT-Sicherheit

Wir gehen in diesem Kapitel der Frage nach, wie die Aus- und Weiterbildung in IT-Sicherheit organisiert werden soll. Wir stellen zunächst vor, welchen Ausbildungshintergrund ein hauptamtlich Verantwortlicher für IT-Sicherheit haben sollte. Da IT-Sicherheit ein sehr dynamisches Gebiet mit vielen neuen Erkenntnissen ist, muss jeder, der mit IT-Systemen umgeht, dauerhaft in IT-Sicherheit weitergebildet werden. Welche Organisation die Weiterbildung haben kann, darauf gehen wir anschließend ein.

Wer hauptamtlich für IT-Sicherheit oder Datenschutz zuständig ist, sollte eine grundständige Ausbildung in IT-Sicherheit haben. Die Ausbildung kann dabei einerseits in Form eines Hochschul- oder Fachhochschulstudiums absolviert werden. Andererseits sehen wir auch die Möglichkeit, entsprechende Kenntnisse im Rahmen der berufsbegleitenden, arbeitsprozessorientierten Weiterbildung zum operativen oder strategischen Professional zu erwerben. Wichtig ist aber, dass hinreichend viele Themengebiete der IT-Sicherheit behandelt werden. Da der IT-Sicherheit in den Rahmenlehrplänen der Ausbildung zum Fachinformatiker (oder ähnlicher Berufe) nur sehr wenig Platz eingeräumt wird, ist unserer Ansicht nach eine grundständige Ausbildung in IT-Sicherheit in diesem Rahmen nicht möglich.

Zunächst zu den Hochschulen bzw. Fachhochschulen. Diese können in Studiengängen wie Mathematik, Informatik, Wirtschaftsinformatik, Elektrotechnik oder Rechtswissenschaft einen Studienschwerpunkt IT-Sicherheit anbieten. Dabei ist darauf zu achten, dass auch die nicht-technische Ausbildung etwa im Bereich Recht und Wirtschaft einen angemessenen Platz erhält. Die Absolventen sind dann Diplom-Informatiker, Diplom-Mathematiker, Diplom-Wirtschaftsinformatiker oder Diplom-Ingenieure. In

gesonderten Zertifikaten kann die (Fach-)Hochschule den Studienschwerpunkt IT-Sicherheit bestätigen. Hochschulen können aber auch eigene interdisziplinäre Studiengänge in IT-Sicherheit anbieten. In einem solchen Studiengang lernen die Studierenden schwerpunktmäßig die IT-Sicherheit in ihren Grundlagen und Anwendungen kennen. Ihr Abschluss heißt zum Beispiel Diplom-Ingenieur für IT-Sicherheit. Ein solcher Studiengang bietet eine wirklich vertiefte Ausbildung in IT-Sicherheit. Aber im Gegensatz zu Diplom-Mathematikern mit Studienschwerpunkt IT-Sicherheit sind Diplom-Ingenieure IT-Sicherheit spezialisierter. Ihre Beschäftigungsmöglichkeiten erscheinen potenziell geringer. Daher ist nicht klar, welche Akzeptanz solche Studiengänge finden werden.

Eine sehr praxisorientierte Ausbildung wird von einigen Berufsakademien (unter anderem der BA Mannheim) angeboten. Dabei werden die in Vorlesungen kommunizierten Inhalte durch praktische Erfahrungen ergänzt, die in einem Ausbildungsbetrieb vermittelt werden. Die arbeitsprozessorientierte Weiterbildung ist noch im Entstehen. Wir sehen hierin die alternative Möglichkeit für Berufstätige, eine grundständige Ausbildung in IT-Sicherheit zu erhalten.

Kommen wir nun zur Weiterbildung. Sie ist von fundamentaler Bedeutung für alle, die mit IT-Systemen arbeiten. Für alle, die eher grundsätzliche Kenntnisse in IT-Sicherheit brauchen oder IT-Sicherheit nur anwenden wollen, sind einführende Schulungen, Kurse und Workshops das geeignete Format. Tutorials wie z.B. Kryptographie oder Datenschutzrecht werden von Hochschulen oder Forschungseinrichtungen angeboten. Die Mitarbeiter dieser Einrichtungen sind aufgrund ihrer Tätigkeit in der Forschung immer auf dem wissenschaftlich und technisch aktuellen Stand. Angewandte Themen wie Security-Engineering können auch von IT-Sicherheitsunternehmen angeboten werden. Spezielle Anwendungen und Produktschulungen bleiben den Herstellern der Produkte oder von diesen zertifizierten Anbietern vorbehalten.

Wir erachten eine Zweiteilung der Weiterbildung zu den wichtigen Themen der IT-Sicherheit als sinnvoll. Zunächst gibt es Einführungskurse (Tutorials), die für die jeweilige Adressatengruppe ohne spezielle Vorkenntnisse verständlich sind. Weiterhin werden Workshops angeboten, die auf diesen Grundkursen aufbauen und den aktuellen Wissensstand im jeweiligen Gebiet vermitteln. Im Bereich PKI zum Beispiel wird ein Tutorial über PKI angeboten, das Grundlagen von Public-Key-Verschlüsselung, elektronischen Signaturen, dem Aufbau einer PKI und ihren Vor- bzw. Nachteilen behandelt. Auf dem zugehörigen PKI-Workshop werden aktuelle Entwicklungen von PKI-Techniken vorgestellt und diskutiert.

5 Aus- und Weiterbildungsangebote

In diesem Kapitel stellen wir vor, welche Aus- und Weiterbildungsangebote in Deutschland es bereits gibt. Es stellt sich heraus, dass der klassische Unterricht im

Rahmen von Präsenzseminaren die dominierende Lehrmethode ist. Inhaltlich stehen technische und organisatorische Themen im Vordergrund.

Wir beginnen mit der Ausbildung. Im vorigen Kapitel haben wir mögliche Ausbildungsansätze erwähnt. Im Hochschulbereich werden sowohl der Studienschwerpunkt IT-Sicherheit als auch der Diplom-Studiengang IT-Sicherheit angeboten. Die Technische Universität Darmstadt (TU Darmstadt) hat sich für den Weg des Studienschwerpunkts entschieden. Studierende aller Fachrichtungen können ein ‚Zertifikat IT-Sicherheit‘ erwerben, wenn sie eine gewisse Anzahl von Pflicht- und Wahlpflichtveranstaltungen (Vorlesungen, Seminare, Praktika, Workshops) erfolgreich besucht haben. Voraussetzung zur Teilnahme an den Zertifikatsveranstaltungen ist lediglich die Immatrikulation an der TU Darmstadt. Inhaltlich wird das Zertifikat vom Darmstädter Zentrum für IT-Sicherheit [DZI] gestaltet. Eine wichtige Aufgabe des DZI ist die Förderung der Ausbildung im Bereich IT-Sicherheit an der TU Darmstadt.

Die Ruhr-Universität Bochum verfolgt den anderen Ansatz. Sie bietet den Studiengang ‚Sicherheit in der Informationstechnik‘ an. Dieser wird nach 10 Semestern mit dem Diplom oder Master abgeschlossen. Die mit IT-Sicherheit befassten Arbeitsgruppen der Ruhr-Universität Bochum haben sich zum Horst Görtz Institut [HGI] zusammengeschlossen.

Mit der arbeitsprozessorientierten Weiterbildung (operative und strategische Ebene) liegen noch keine Erfahrungen für eine grundständige Ausbildung in IT-Sicherheit vor.

Eine Motivation der besonderen Art für Studenten und Auszubildende stellt der Förderpreis des Competence Center for Applied Security Technology [CAST] aus Darmstadt dar, der jährlich vergeben wird. Er prämiert innovative Arbeiten zur IT-Sicherheit. In zwei Kategorien können sich zum Einen Auszubildende und zum Anderen Studenten von Berufsakademien, Fachhochschulen und Universitäten um den Preis bewerben. Bewertet wird sowohl die schriftliche Arbeit als auch die Präsentation der Ergebnisse im Rahmen eines Vortrags.

Das Weiterbildungsangebot ist vielfältig. Besonders bekannt sind die Workshops des Competence Center for Applied Security Technology [CAST]. Die meist eintägigen Workshops von CAST behandeln ein Gebiet der IT-Sicherheit. Experten stellen aktuelle Entwicklungen vor und diskutieren diese mit dem Plenum. Um auch dem Bedarf nach einführenden Schulungen zu verschiedenen Themen nachzukommen, bietet CAST jetzt komplementär zu den Workshops auch Tutorials z.B. zu PKI, Mobile Security oder Recht und IT-Sicherheit an. Dabei wechseln sich Phasen des Unterrichts mit Praxisübungen ab. Die Teilnehmer wenden so ihr theoretisches Wissen in praktischen Übungen an. Damit deckt CAST die vollständige Palette grundlegender Themen für die verschiedenen Adressatengruppen ab. CAST kooperiert eng mit dem Darmstädter Zentrum für IT-Sicherheit [DZI].

Eine fundierte wissenschaftliche Weiterbildung in IT-Sicherheit bietet die TU Darmstadt in Zusammenarbeit mit CAST an. Berufstätige können in vier Semestern ein ‚Zertifikat IT-Sicherheit‘ erwerben, wenn sie in dieser Zeit eine vorgegebene Anzahl von Pflicht- und Wahlpflichtveranstaltungen erfolgreich besucht haben. Dieses Zertifikat wird inhaltlich gemeinsam von CAST und DZI gestaltet. Die Teilnehmer hören die regulären Vorlesungen an der TU Darmstadt. Durch speziell auf Berufstätige abgestimmte Unterlagen und Übungen werden die Inhalte aufbereitet und vertieft. Aktuelle Entwicklungen praktisch relevanter Themen erhalten die Zertifikatsteilnehmer im Rahmen der CAST-Workshops.

Ein weiterbildendes Studium ‚IT-Sicherheit: Administration und Sicherheit von IT-Systemen und –netzwerken‘ führt das Weiterbildungszentrum der Ruhr-Universität Bochum [WBZ] im März 2003 ein. Das Studium ist berufsbegleitend organisiert. In einem Gesamtzeitraum von ca. einem Jahr werden in ein- bis viertägigen Präsenzseminaren grundlegende Themen der IT-Sicherheit behandelt. Begleitend zur Weiterbildung entwickeln die Teilnehmer die Grundstruktur eines Sicherheitskonzepts.

Tutorials, Workshops und Produktschulungen werden auch von einer Reihe von Firmen angeboten. Sehr aktiv auf dem Markt der Weiterbildung ist die Gesellschaft für IT-Sicherheit [GITS] in Bochum. GITS bietet Veranstaltungen aller drei Klassen in Form von Präsenzseminaren an. Das GITS-E-Learning Programm rundet das Angebot ab. Die IT-Beratungsfirma Secorvo Security Consulting [SSC] aus Karlsruhe bietet im Rahmen ihres Secorvo Colleges eine Reihe von Weiterbildungsseminaren zu verschiedenen Themen der IT-Sicherheit an (Public-Key-Infrastrukturen, IT-Security Management, Lotus Notes Security). Ein weiterer Anbieter von IT-Sicherheitsweiterbildung ist die secunet Security Networks AG [Sec] aus Essen. secunet bietet Schulungen zu Themen wie symmetrische Verschlüsselung, Intrusion Detection und Datenschutz an.

Die Firma Dignet GmbH [Dig] bietet in Kooperation über die Studiengemeinschaft Darmstadt [SGD] zwei jeweils dreitägige Workshops zum Themengebiet IT-Sicherheit an. Der Workshop ‚Internet Security‘ legt den Schwerpunkt auf die Gestaltung sicherer Internetprozesse, während der zweite Workshop ‚IT-Sec 1‘ bzw. ‚IT-Sec 2‘ Themen des IT-Sicherheitsmanagements und die Umsetzung des IT-Grundschutzkonzepts behandelt.

Eine vierwöchige blockbasierte Ausbildung wird von der Summer University Informationssicherheit angeboten, die im Rahmen einer praxisorientierten Grundausbildung den Erwerb eines Zertifikats ‚Certified Information Security Officer‘ ermöglicht [SUM]. Das Angebot wird von dem Unternehmen Lessing&Partner GmbH in Kooperation mit der Fachhochschule Bonn-Rhein-Sieg in St. Augustin gestaltet.

Interessant für Firmen und Verwaltungen sind auch bedarfsorientierte Schulungen. Der Auftraggeber gibt hierbei die Inhalte vor. Der Schulungsanbieter entwickelt auf Basis dieser Vorgabe eine individuelle Schulung. Von großem Vorteil bei diesem Ansatz ist, dass die Lehrinhalte speziell auf die Teilnehmer zugeschnitten sind. Bedarfsorientierte

Schulungen werden von allen oben genannten Einrichtungen angeboten. Außerdem sei das breite Angebot der Darmstädter Fraunhofer Institute SIT und IGD [SIT], [IGD] genannt. Die Institute bieten z.B. Schulungen und Seminare zu Sicherheitsmanagement, Bedrohungs- und Risikoanalysen oder Sicherheitskonzepten an.

Neben den genannten Weiterbildungsangeboten findet man auch spezielle praktische Trainingsangebote. Diese richten sich an Personen, die IT-Systeme bedienen müssen. Zum Beispiel bietet das Information Technology Transfer Office [ITO] an der TU Darmstadt seinen ‚Hacker-Contest‘ jetzt auch für Berufstätige an. In praktischen Phasen, die einer theoretischen Vorbereitung folgen, lernen die Teilnehmer das Vorgehen von Hackern kennen. Auch das Secorvo College [SSC] bietet solche praktische Schulungen an.

6 Was fehlt?

Im vorangegangenen Kapitel haben wir festgestellt, dass bei den Aus- und Weiterbildungsveranstaltungen inhaltlich die technischen, wissenschaftlichen und organisatorischen Themen der IT-Sicherheit im Vordergrund stehen. Aus unserer Sicht fehlen weitgehend Veranstaltungen, in denen die Teilnehmer eine Kosten-Nutzen-Rechnung für IT-Sicherheit erlernen. Eine solche Kennzahl könnte der oben genannte Return on Security Investment (ROSI) sein.

Erste Ansätze dazu sind im Entstehen: Die Gesellschaft für IT-Sicherheit [GITS] aus Bochum und das Secorvo College [SSC] bieten Weiterbildungsseminare zu diesem Thema an.

In Bezug auf die Lehrmethoden steht bei allen Anbietern der klassische Frontalunterricht im Vordergrund. Das Angebot von E-Learning-Methoden steckt noch weitgehend in den Kinderschuhen. Wir erhoffen uns für die Zukunft eine gute Kombination aus Präsenzunterricht und E-Learning-Phasen. Insbesondere Web-Based-Training-Angebote sollten in Zukunft ausgebaut werden. Im Bereich des Web-Based-Training für IT-Sicherheit ist z.B. die Firma digital spirit GmbH [DS] aus Wiesbaden tätig. Erwähnenswert ist auch die multimediale Lern-CD des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein [ULD].

Weitere Verbesserungsmöglichkeiten der Weiterbildung gibt es bezüglich der internationalen Vernetzung der ausbildenden Institutionen. Im Hinblick auf eine internationale Anerkennung der Schulungsinstitutionen und der erteilten Zertifikate ist die Entwicklung des Schulungsstandards *Security+* durch die Non-Profit-Organisation CompTIA [CTA] ein wichtiger Schritt. Unter Einbindung großer Unternehmen wie Microsoft, Sun Microsystems und IBM wurde ein Aus- und Weiterbildungsstandard definiert, der die in diesem Beitrag behandelten Schulungsthemen umfasst. Eine durch diesen Standard forcierte, weltweite Anerkennung von in Deutschland erworbenen IT-

Sicherheitszertifikaten ist in der Zeit global operierender Unternehmen eine wichtige Qualifizierung für die ausgebildeten Sicherheitsexperten.

7 Weitere Informationen

Wir stellen Quellen für weitere Informationen zu den im Dokument erwähnten Einrichtungen zusammen:

[CAST] Competence Center for Applied Security Technology, www.cast-forum.de

[CTA] Computing Technology Industry Association,
www.comptia.org/certification/security/default.asp

[Dig] Diginet GmbH, www.diginet.de

[DS] digital spirit GmbH, www.digital-spirit.de

[DZI] Darmstädter Zentrum für IT-Sicherheit, www.dzi.tu-darmstadt.de

[GITS] Gesellschaft für IT-Sicherheit AG, www.gits-ag.de

[HGI] Horst Görtz Institut, www.ruhr-uni-bochum.de/hgi

[IGD] Fraunhofer Institut IGD, www.igd.fhg.de/igd-a8

[ITO] Information Technology Transfer Office, www.ito.tu-darmstadt.de

[SGD] Studiengemeinschaft Darmstadt, www.sgd.de

[Sec] secunet Security Networks AG, www.secunet.de

[SIT] Fraunhofer Institut für Sichere Telekooperation, www.sit.fhg.de

[SSC] Secorvo Security Consulting GmbH, www.secorvo.de

[SUM] Summer University, www.summeruniversity.de

[ULD] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,
www.datenschutzzentrum.de/projekte/schul-cd

[WBZ] Weiterbildungszentrum der Ruhr-Universität Bochum,
www.ruhr-uni-bochum.de/wbz/wwb/it-sicherheit.html