EMPFEHLUNGEN DER GESELLSCHAFT FÜR INFORMATIK E.V. (GI) ZUR BERÜCKSICHTIGUNG VON IT-SICHERHEIT IN DER BERUFLICHEN AUS- UND WEITERBILDUNG

Kurzfassung

Die Sicherheit von IT-Systemen und IT-Infrastrukturen sowie der sichere Umgang mit IT wurden lange Zeit vernachlässigt, werden aber zunehmend als unverzichtbar sowohl für die private Nutzung von IT als auch für die Informationssicherheit in Unternehmen und Institutionen erkannt. Die Gesellschaft für Informatik hat im Oktober 2006 auf das Ausbildungsdefizit bei der IT-Sicherheit hingewiesen und Empfehlungen zur Verbesserung der Ausbildungssituation in Schulen und Hochschulen veröffentlicht. Sie hält es außerdem für erforderlich, dass das Thema in der beruflichen Aus- und Weiterbildung berücksichtigt wird. Drei Bereiche werden identifiziert: Berufliches Schulwesen, berufliche Weiterbildung, Ausbildung zum Datenschutzbeauftragten.

Berufliches Schulwesen: In den Schulformen des beruflichen Schulwesens gibt es unterschiedliche Ausbildungsgänge mit IT-Bezug. Das Thema IT-Sicherheit ist in den entsprechenden Rahmenplänen zu verankern, wobei je nach Schulform unterschiedliche Kompetenzstufen anzustreben sind.

Berufliche Weiterbildung und Zertifizierung: Es gibt bereits Weiterbildungsangebote, die speziell auf IT-Sicherheit fokussiert sind. Allen IT-Fachleuten wird dringend empfohlen, solche Angebote wahrzunehmen. Manche Weiterbildungsgänge mit IT-Bezug berücksichtigen die IT-Sicherheit wenig oder gar nicht. Hier sollten Anpassungen vorgenommen werden, wobei eine Orientierung an den existierenden Angeboten zur IT-Sicherheit empfohlen wird.

Ausbildung zum Datenschutzbeauftragten: Entsprechende Ausbildungsangebote existieren und sollten erheblich mehr als bisher wahrgenommen werden. Leider ist das Qualitätsniveau noch unterschiedlich, weshalb die Einführung einheitlicher Standards empfohlen wird.

1 Einführung

Die Gesellschaft für Informatik hat im Oktober 2006 Empfehlungen zur Berücksichtigung der *IT-Sicherheit in der schulischen und akademischen Ausbildung* herausgegeben [GI 2006b]. Dies geschah aus Sorge über die zunehmend schädlichen Auswirkungen von Angriffen auf unzureichend geschützte IT-Systeme.

Einerseits ist die oft mangelhafte Sicherheit von Systemen auf Defizite in der Ausbildung von Informatikern zurückzuführen, die diese Systeme entwickeln oder einrichten. Andererseits mangelt es Anwendern häufig an dem nötigen Problembewusstsein beim Umgang mit dem Rechner und dem Netz. Daher hält es die GI für dringend erforderlich, dass das Thema IT-Sicherheit in der Ausbildung sowohl von Informatikern als auch von Nichtinformatikern in jeweils angemessener Weise berücksichtigt wird.

Die Empfehlungen vom Oktober 2006 bezogen sich auf die Ausbildung an den Hochschulen und an den allgemeinbildenden Schulen. Die universelle Bedeutung des Themas lässt es geboten erscheinen, dass das Thema auch in die *berufliche Aus- und Weiterbildung* Eingang findet: IT-Infrastrukturen sind heute allgegenwärtig; IT-Sicherheit trägt daher wesentlich zur *Informationssicherheit* in Unternehmen und öffentlichen Institutionen bei.

Die vorliegenden Empfehlungen sollen Initiativen für die berufliche Aus- und Weiterbildung anregen und durch die Benennung wünschenswerter Kompetenzen inhaltlich unterstützen. Der folgende Abschnitt 2 befasst sich mit der Ausbildung an *beruflichen Schulen*. Einen hohen Stellenwert hat das Thema auch im Bereich der *beruflichen Weiterbildung*, wo auch die *Zertifizierung* eine große Rolle spielt. Berufliche Weiterbildung und Zertifizierung sowie die Ausbildung zum *Datenschutzbeauftragten* werden im Abschnitt 3 behandelt.

Eine Stellungnahme der GI zur *IT-Weiterbildung generell* findet man in einem Positionspapier vom August 2006 [GI 2006a].

2 Berufliches Schulwesen

Bei den beruflichen Schulen gibt es eine Reihe verschiedener Schulformen. Im Folgenden wird zunächst die Teilzeitberufsschule betrachtet; anschließend wird auf weitere Schulformen eingegangen.

2.1 Teilzeitberufsschule: Duale Berufsausbildung

In der dualen Berufsausbildung beziehen sich diese Empfehlungen auf die folgenden Ausbildungsberufe:

1. IT-Systemelektroniker
2. Fachinformatiker Fachrichtung Systemintegration
3. Fachinformatiker Fachrichtung Anwendungsentwicklung
4. IT-System-Kaufmann
5. Informatik-Kaufmann

Es wird empfohlen, das Thema IT-Sicherheit in den Rahmenlehrplänen dadurch zu verankern, dass in den betreffenden Lernfeldern der Aspekt *Sicherheit* stärker hervorgehoben wird. Dies muss möglichst umgehend, spätestens aber bei einer Neuordnung der Ausbildungsgänge geschehen. Die Formulierung eines eigenen Lernfeldes zur IT-Sicherheit wird als nicht sinnvoll angesehen, da Fragen zur IT-Sicherheit in der Berufsschule besser als integraler Bestandteil eines übergeordneten Themas behandelt werden können.

Die typischen Handlungsfelder der Auszubildenden lassen sich in drei Bereiche unterteilen: Entwicklung von Anwendungssystemen, Konfiguration von Betriebssystemen, Einrichtung von Netzen. In jedem dieser Handlungsfelder sollte die Aufgabenstellung in der Schule und im Betrieb unter Berücksichtigung der kritischen Geschäftsprozesse

- die Gefahrenlage im Bereich der IT-Sicherheit behandeln,
- eine Diskussion über geeignete Abwehrmaßnahmen einbeziehen,
- auf die Bedeutung sicherer Software-Entwicklungsprozesse hinweisen,
- die Beachtung von rechtlichen Vorgaben berücksichtigen,
- die Dokumentation dieser Bereiche behandeln.

Die genannten Anforderungsbereiche lassen sich in ein *Kompetenzraster*[1] überführen, das in Abb. 1 gezeigt ist. Die Stufung der Kompetenzen eines Kompetenzbereichs drückt das Niveau der Anforderung an den Auszubildenden aus.

	A1	A2	B1	B2	C1	C2
Kritische Geschäftsprozesse erkennen	Ich kann zu schützende Vermögen benennen	Ich kann Beispiele für kritische Geschäftsprozesse aufzählen	Ich kann Geschäftsprozesse eines Unternehmens von Entscheidern erfragen	Ich kann für einen gegebenen Geschäftsprozess die Kritikalität ermitteln	Ich kann bewerten, welche Geschäftsprozesse kritisch sind	Ich kann die Abhängigkeit der Geschäftsprozesse untereinander in die Risikoanalyse einbeziehen
Risiken einschätzen und vermeiden	Ich kann Risiken und ihre Ursachen (Malware, Software-Schwachstellen) benennen	Ich kann die Auswirkungen von Risiken beschreiben und Präventions- und Schutzmaßnahmen aufzählen	Ich kann die Notwendigkeit für eine Schutzmaßnahme erläutern und begründen	Ich kann die Mechanismen von Risiken sowie ihre Vermeidung durch sichere Entwicklung beschreiben	Ich kann entscheiden, gegen welche verbleibenden Risiken Schutzmaßnahmen zu ergreifen sind	Ich kann solche Risiken einschätzen und am Markt verfügbare Lösungen auswählen
Abwehrmaßnahmen ergreifen	Ich kann Abwehrmaßnahmen und zugehörige Werkzeuge benennen	Ich kann die Funktionsweise einer Abwehrmaßnahme erläutern	Ich kann eine Abwehrmaßnahme im Netz installieren und konfigurieren	Ich kann Abwehrmaßnahmen überwachen. (Logfiles auswerten)	Ich kann prüfen, ob meine Abwehrmaßnahme erfolgreich ist	Ich kann Schwachstellen im Netzwerk erkennen und beheben
Rechtliche Vorgaben berücksichtigen	Ich kann rechtliche Vorgaben benennen	Ich kann zu einer rechtlichen Vorgabe die techn. notwendigen Umsetzungen aufzählen	Ich kann zu einer rechtlichen Vorgabe die techn. notwendigen Umsetzungen erläutern		Ich kann rechtliche Vorgaben fachgerecht technisch umsetzen	Ich kann technische Umsetzungen für rechtliche Vorgaben bewerten
Dokumentation erstellen	Ich kann eine gegebene Dokumentation lesen		Ich kann anhand einer gegebenen Dokumentation Aspekte der Netzwerksicherheit erläutern		Ich kann eine Dokumentation nach Kundenwunsch erstellen und erweitern	

Abb. 1: Kompetenzraster zum Thema IT-Sicherheit.

[1] http://www.learningfactory.ch/downloads/dateien/artikel_lernen%20als%20dauerbaustelle.pdf

Die Zeilen entsprechen den Kompetenzbereichen; die Spalten entsprechen den Kompetenzstufen. Von links nach rechts nimmt das Niveau der Kompetenz zu. (A: grundlegende Kompetenz, B: mittlere Kompetenz, C: fortgeschrittene Kompetenz.) Dieses Raster ist für die Hand des Schülers bestimmt.

Eine getrennte Betrachtung der einzelnen Berufe wird in dieser Empfehlung als nicht notwendig erachtet. Die genannten Berufsbilder verbindet eine starke Fokussierung auf Geschäftsprozesse, die eine Betrachtung des Themas IT-Sicherheit mit einschließen muss.

Angesichts der Tatsache, dass die Auszubildenden zwei Drittel ihrer Zeit im Betrieb verbringen, kommt dem praktischen Umgang mit Sicherheitsmechanismen und -werkzeugen am Arbeitsplatz eine große Bedeutung zu. Die betrieblichen Ausbildungsordnungen sind daher um Aspekte der IT-Sicherheit zu ergänzen, und in den betrieblichen Projekten sind Fragen zur IT-Sicherheit stärker zu berücksichtigen. Eine Orientierung am Kompetenzraster aus Abb. 1 wird empfohlen.

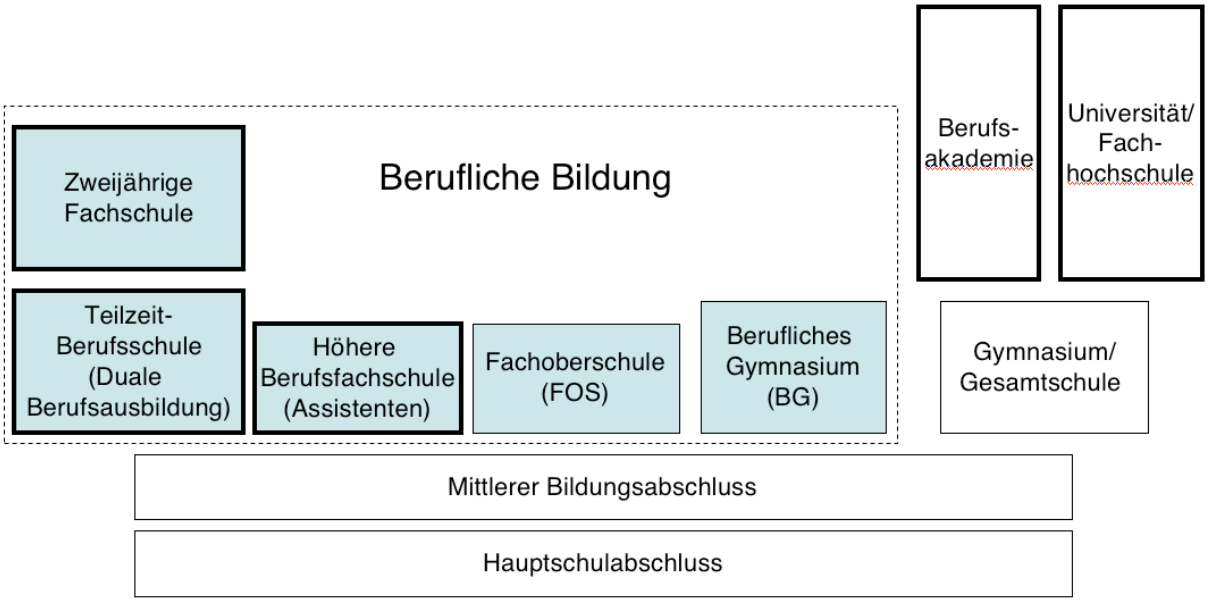

Abb. 2: Bildungswege im beruflichen Schulwesen
Die zeitliche Abfolge verläuft von unten nach oben.
Berufsqualifizierende Abschlüsse sind durch fette Umrandung gekennzeichnet.
Die Schulformen im beruflichen Schulwesen sind grau hinterlegt.
Die vorliegende Empfehlung richtet sich an diese Schulformen.

2.2 Weitere Schulformen

Neben der dualen Berufsausbildung in der Teilzeitberufsschule umfasst das berufliche Schulwesen weitere Schulformen mit Schwerpunkten auf dem Gebiet der Informationstechnik (siehe Abb. 2). Die im Abschnitt 2.1 genannten Kompetenzbereiche der IT-Sicherheit gelten hier entsprechend. Lediglich die zu erreichenden Kompetenzstufen unterscheiden sich bei den einzelnen Schulformen:

1. Die *Fachoberschule* führt im Anschluss an den mittleren Bildungsabschluss (Realschulabschluss) auf die Fachhochschulreife hin. Als Vertiefungsrichtung kann z.B. Informationstechnik gewählt werden.

	A1	A2	B1	B2	C1	C2
Kritische Geschäftsprozesse erkennen						
Risiken einschätzen und vermeiden	*	*	*	*		
Abwehrmaßnahmen ergreifen	*	*	*	*		
Rechtliche Vorgaben berücksichtigen	*	*				
Dokumentation erstellen						

2. Das *Berufliche Gymnasium* stellt eine eher technikorientierte Alternative zum allgemein bildenden Gymnasium bzw. zur Gesamtschule dar. Es bietet technikorientierte Leistungskurse z.B. im Bereich Informationstechnik an.

	A1	A2	B1	B2	C1	C2
Kritische Geschäftsprozesse erkennen						
Risiken einschätzen und vermeiden	*	*	*	*		
Abwehrmaßnahmen ergreifen	*	*	*	*		
Rechtliche Vorgaben berücksichtigen	*	*				
Dokumentation erstellen						

3. Die *Höhere Berufsfachschule* (z.B. *für Informationsverarbeitung)* ist eine Schulform im beruflichen Schulwesen, die im Anschluss an den mittleren Bildungsabschluss (Realschulabschluss) vollschulisch zu dem berufsqualifizierenden Abschluss *staatlich anerkannter Assistent* (z.B. *für Informationsverarbeitung)* führt. Ausbildungsbegleitend ist es möglich, die Fachhochschulreife zu erwerben.

	A1	A2	B1	B2	C1	C2
Kritische Geschäftsprozesse erkennen	*	*				
Risiken einschätzen und vermeiden	*	*	*			
Abwehrmaßnahmen ergreifen	*	*	*			
Rechtliche Vorgaben berücksichtigen	*	*				
Dokumentation erstellen	*		*			

4. Die *Zweijährige Fachschul*e (z.B. Fachrichtung Informationstechnik, Schwerpunkt Computersystem- und Netzwerktechnik) ermöglicht mit der Ausbildung zum *staatlich geprüften Techniker* den Erwerb einer gehobenen Qualifikation nach einer abgeschlossenen Berufsausbildung und einigen Jahren im Beruf, die zwischen dem Facharbeiter und dem Ingenieur angesiedelt ist.

	A1	A2	B1	B2	C1	C2
Kritische Geschäftsprozesse erkennen	*	*	*	*	*	*
Risiken einschätzen und vermeiden	*	*	*	*	*	*
Abwehrmaßnahmen ergreifen	*	*	*	*	*	*
Rechtliche Vorgaben berücksichtigen	*	*	*		*	*
Dokumentation erstellen	*		*		*	

3 Berufliche Weiterbildung und Zertifizierung

In den Unternehmen ist die *Informationssicherheit* wegen Mängeln in der IT-Sicherheit von immer neuen Gefährdungslagen und Angriffen bedroht. Somit sind die Mitarbeiter herausgefordert, sich Wissen und Handlungskompetenzen im Bereich Informationssicherheit zu erarbeiten und damit die Profitabilität des Unternehmens zu erhalten und zu stärken.

Zunehmend werden berufsbegleitende Aus- und Weiterbildungen angeboten, die verstärkt auf lebenslanges Lernen ausgerichtet sind. Diese Ausrichtung wird politisch durch Europäische Integrationsmaßnahmen unterstützt, insbesondere durch das in Entwicklung befindliche Modell des *European Qualifications Framework* (EQF)[2] . Inhaltlich stärkt das EQF die Bedeutung der beruflichen Handlungskompetenz gegenüber der Aneignung von theoretischem Wissen. Im Auftrag des BMBF wurde das APO-IT entwickelt, ein Konzept für die Arbeitsprozessorientierte Weiterbildung im Bereich der Informationstechnik, auf dem die staatlich anerkannten und im Berufsbildungsgesetz verankerten Bildungsprofile für IT-Spezialisten beruhen.

Im Gegensatz zur universitären und beruflichen Erstausbildung steht die berufliche Weiterbildung in der IT- und Informationssicherheit *nicht* unter dem Primat eines pädagogischen Bildungsauftrags. Im Vordergrund steht vielmehr der Bedarf und der Nutzen für den Mitarbeiter und das Unternehmen, weshalb hier auch eine lediglich punktuelle oder modulare Ausrichtung von Weiterbildungsprofilen sinnvoll sein kann. Die persönliche Entwicklung und soziale Reifung ist in den verschiedenen Profilen nur insofern von Bedeutung, als sie notwendiger inhaltlicher Bestandteil der Weiterbildung ist; so unterliegen Fachkräfte besonderen Anforderungen hinsichtlich Vertrauensbildung und verantwortlichen und vorbildhaften Verhaltens.

Aufgrund der verschiedenen Interessenlagen sind die angebotenen Weiterbildungsprofile vielfältig. Folgende unterschiedliche Ausprägungen lassen sich erkennen:

- staatlich anerkannte Ausbildung (in der Gesetzgebung verankert), thematisch *mit* oder *ohne* besonderen Fokus auf IT- und Informationssicherheit (Erwachsenenstudiengänge, anerkannte berufliche Weiterbildung),
- thematische Ausbildung ohne Fokus auf IT-Sicherheit, gefördert durch *Institutionen* oder *Produkthersteller*,
- IT-sicherheitsspezifische Ausbildung, gefördert durch *Institutionen* oder *Produkthersteller*.

3.1 Standards, Normen und Zertifikate

Mit der zunehmenden Professionalisierung der IT nimmt auch die Bedeutung der einschlägigen Standards, Normen und auf Normen basierenden *Zertifikaten* zu, nicht zuletzt auf Druck des Gesetzgebers, der mit der Einhaltung von Normen beim Betrieb von informationstechnischen Anlagen strafbewehrte Sanktionen verbindet (z.B. KonTraG[3], SOX[4]). Die international wichtigste Organisations-Norm im Bereich der Informationssicherheit ist die ISO-2700x-Familie[5], welche sich zum Teil noch in Entwicklung befindet. Die anerkannte Norm zur Füh-

[2] http://www.bibb.de/de/wlk18242.htm
[3] http://www.bgblportal.de/BGBL/bgbl1f/b198024f.pdf
[4] http://www.soxlaw.com
[5] http://www.27000.org

rung einer Personalzertifizierungsstelle und damit zur Zertifizierung von Personal ist die ISO 17024. Diese Norm unterstreicht im übrigen das Prinzip des lebensbegleitenden Lernens, indem der ständige Kompetenzerhalt und -nachweis durch *Rezertifizierung* erzwungen wird.

3.2 Profile mit allgemeinem Informatik-Bezug

Neben den spezifischen Fähigkeiten, die jeder benötigt, um seinen Beruf auszuüben, werden in den meisten Unternehmen Fähigkeiten benötigt, die in Hochschulen selten zum Lehrplan gehören. Neben Präsentations- und Rhetoriktechniken gibt es einige, die eine hohe IT-Durchdringung mit sich bringen, hauptsächlich im Management-Bereich. Typische Weiterbildungsprofile beziehen sich auf das *Projektmanagement*, das *Service Management* oder das *Qualitätsmanagement*.

Diese Weiterbildungen ohne expliziten Bezug zur IT-Sicherheit berühren zwar bisweilen IT-Sicherheits-Aspekte, bezeichnen sie aber nicht so; meist ist von Risiken und Risikomanagement die Rede. In der Regel werden die Risiken nur unvollständig betrachtet. So geht es eher um Zeit- und Budgetprobleme; Mängel bei der Erreichung von IT-Schutzzielen wie Vertraulichkeit, Integrität, Verfügbarkeit werden häufig vernachlässigt. Zudem werden offensichtlich sicherheitsrelevante Betriebsprozesse oft nicht als solche gesehen: Benutzerverwaltung beispielsweise wird häufig nur als Passwortvergabe verstanden, obwohl neben der Authentisierung auch die Autorisierung organisiert werden muss.

Es wird daher empfohlen, die genannten Weiterbildungsprofile so auszurichten, dass Grundkenntnisse von *Angriffen und Angriffstypen* und der zur Abwehr geeigneten individuellen *Verhaltensweisen* und organisatorischen *Maßnahmen* vermittelt werden, ferner ein Überblick über die verfügbaren *technischen Mittel* zur Erhöhung der Sicherheit. Zur Sicherstellung dieser Qualifikation wird die Behandlung der folgenden Themen empfohlen:

- Gesetzeslage zur Informationssicherheit
- Kritische Geschäftsprozesse und Risikomanagement
- Angriffstypen: Ausspionieren, Manipulation und Zerstörung von Daten, betrügerische Transaktionen im Netz, Betriebsstörungen (z.B. *denial of service*)
- Schwachstellen von Software (und Hardware) als Einfallstor für Angriffe; sichere Programmierung zur Vermeidung von Software-Schwachstellen; Notwendigkeit von *patches* bei erkannten Schwachstellen
- Schadsoftware wie Viren, Würmer, Trojanische Pferde (auch als Skript-Code in Dokumenten)
- Unwissenheit und/oder Nachlässigkeit von Benutzern und Systemverwaltern
- Schutzmaßnahmen: widerstandsfähige Passwörter, sorgfältiger Umgang mit Dateischutz-Mechanismen, Vorsicht bei der Übernahme unbekannter Software und unbekannter Dokumente, Einsatz kryptographiebasierter Techniken (z.B. *ssh* statt *telnet)*, Umgang mit Zertifikaten, Fähigkeiten von Firewalls.

Es wird oft genügen, wenn diese Themen ohne theoretische Fundierung rein phänomenologisch und praxisorientiert behandelt werden. Entscheidend ist hier weniger die technische Detailkompetenz als eine umfassende Sensibilisierung für die möglichen Gefahren und ein Überblick darüber, wie man diesen Gefahren begegnen kann.

3.3 Spezielle Profile im Bereich IT-Sicherheit

Weiterbildungsprogramme, die explizit der IT-Sicherheit gewidmet sind, genießen relativ hohe Anerkennung. Der Grund dafür ist in der Unabhängigkeit der Inhalte von Produkten und in der Vermittlung von methodischem und strukturiertem Vorgehen zu suchen. Als weiterer Erfolgsfaktor hat sich die Rezertifizierung durch Praxisnachweise herausgestellt. Der Wert eines Zertifikates liegt eben auch darin begründet, dass es verfällt, wenn der Inhaber sich nicht um eine Rezertifizierung kümmert.

Von zertifizierten Sicherheitsexperten sollte man ein Qualifikationsniveau erwarten können, wie es durch die erfolgreiche Teilnahme an Lehrveranstaltungen zur IT-Sicherheit vermittelt wird. Empfohlen wird die Teilnahme an mindestens drei Modulen im Kernbereich der IT-Sicherheit (z.B. *Systemsicherheit, Netzsicherheit, Kryptographie* aus 2.2.1 der erwähnten GI-Empfehlungen von 2006) sowie an einem Praktikum zum Sicherheitsmanagement, alternativ eine äquivalente Weiterbildung außerhalb der Hochschule. Jenseits der oben unter 3.2 geforderten Qualifikation müssen die Absolventen in der Lage sein, *eigenverantwortlich* Sicherheitsanalysen und -beratungen durchzuführen, Sicherheitstechnik erfolgreich zum Einsatz zu bringen und Sicherheitsstrategien zu entwickeln.

3.4 Produktbezogene Zertifizierungen

Die meisten Hersteller bieten Trainings und Zertifizierungen zu ihren Produkten an, um Anwendern die komplexe Bedienung zu vereinfachen. Auch hier teilt sich das Feld in allgemeine IT-Produkte und IT-Produkte mit Sicherheitsbezug. Produktbezogene Kurse waren wegen ihrer Praxisnähe ursprünglich sehr beliebt, werden aber mittlerweile auch kritisch gesehen, und zwar wegen ihrer recht technischen Ausprägung und ihrer Schwächen in Bezug auf Methodenkompetenz (im Vergleich zu den produktunabhängigen Ausbildungen, wie zuvor erwähnt). Sie erhöhen für die Teilnehmer das persönliche Bildungsrisiko, da mit dem Wechsel einer Produktgruppe im Unternehmen oder dem Wechsel in ein Unternehmen, das ein anderes Produkt einsetzt, die Bildungsleistung verfällt bzw. die Arbeitsplatzmobilität des Arbeitnehmers eingeschränkt wird. Als punktuelle Maßnahmen, eingebettet in ein Gesamtkonzept, haben aber auch diese Bildungsprofile als Reaktion auf konkrete unternehmerische Anforderungen ihre Berechtigung.

Für Kurse mit Sicherheitsbezug wird empfohlen, bei der Behandlung der konkreten produktspezifischen Materie Verbindungen zu den jeweils einschlägigen *Prinzipien* der IT-Sicherheit herzustellen und auf entsprechende Literatur zu verweisen. Bei produktbezogenen Kursen ohne expliziten Sicherheitsbezug sollte auf die *Sicherheitsaspekte des jeweiligen Produkts* – einschließlich potentieller Sicherheitslücken – eingegangen werden.

3.5 Ausbildung zum Datenschutzbeauftragten

Der hohe Standard im Datenschutz in Deutschland und das gesetzlich vorgeschriebene Amt des Datenschutzbeauftragten in Behörden und Unternehmen verlangen nach einer qualifizierten Ausbildung zum Datenschutzbeauftragten. Entsprechende Lehrgänge (im Umfang von wenigen Tagen bis zu einigen Wochen) werden von verschiedenen Institutionen angeboten. Obwohl es Bemühungen zur Vereinheitlichung der Kursinhalte gibt, gibt es bisher weder eine geschützte Bezeichnung noch eine Teilnahmeverpflichtung. Dieser Missstand sollte umgehend beseitigt werden.

Im Idealfall ist der Datenschutzbeauftragte in den beiden Bereichen *Datenschutz* und *IT-Sicherheit* gleichermaßen kompetent und kennt sich auch in der betrieblichen Organisation aus. Er muss technische und organisatorische Schwachstellen im betrieblichen Datenschutz erkennen können, und er muss zu juristischer Beratung in der Lage sein. Eine entsprechende Mehrfach-Qualifikation zu fordern – etwa die eines Informatikers *und* die eines Rechtspflegers – ist allerdings unrealistisch. Wegen der technischen Komplexität des Bereichs IT-Sicherheit sollte der Datenschutzbeauftragte ein IT-Experte sein (so auch das Ulmer Landgericht in seinem Urteil zur Fachkunde von Datenschutzbeauftragten, Az. 5T 153/90-01 LG Ulm). Unter dieser Voraussetzung sollte eine 3-wöchige Weiterbildung mit Konzentration auf Sicherheits- und Datenschutzfragen eine ausreichende Qualifikation sicherstellen können. Aufbauend auf den informatischen Vorkenntnissen sollten folgende Themenbereiche behandelt werden:

- sichere Verarbeitung personenbezogener Daten in allen Phasen (von der Datenerhebung bis zur Löschung, von der Konzeption von Verfahren bis zum Betrieb),
- typische Schwachstellen von Systemen sowie Angriffsmöglichkeiten im Netz,
- aktuelle Sicherheitstechnologien und -werkzeuge,
- datenschutzfördernde Technik (z.B. Anonymisierung, Pseudonymisierung),
- Risikomanagement.

Gesetze und Rechtsprechung zum Datenschutz sind für Informatiker häufig eine spröde Materie. Man sollte sich dafür Zeit nehmen und dem Themenbereich mindestens eine Woche widmen. Die Themen *datenschutzfördernde Technik, informationelle Selbstbestimmung* (BVerfG 1983), *Vertraulichkeit und Integrität* (BVerfG 2008) können dabei gut als Bindeglied zwischen technischem und juristischem Stoff genutzt werden.

Die Ausbildung von Personen ohne gute informatische Vorkenntnisse ist problematisch, weil die IT-Sicherheit in diesem Fall nur rein phänomenologisch behandelt werden kann. Das Fehlen eines vertieften technischen Verständnisses kann den Datenschutzbeauftragten zum zahnlosen Tiger machen, der einer dem Datenschutz eventuell abträglichen Argumentation eines IT-Experten wenig entgegensetzen kann. Die Gefahr ist dann auch, dass der Datenschutzbeauftragte in kritischen Fällen eher als „Bremser und Bedenkenträger“ auftritt, als dass er mit konstruktiven Vorschlägen überzeugen kann.

4 Schlussfolgerungen

Ein Mitarbeiter in einem Betrieb, der im Rahmen seiner Berufsausbildung Wissen und Kompetenzen im Bereich IT-Sicherheit erworben hat, ist heute noch die absolute Ausnahme. Angesichts der drängenden Sicherheitsprobleme ist dies eine auf Dauer unhaltbare Situation. Im IT-Bereich sind daher gezielte Weiterbildungsmaßnahmen angezeigt, wie sie durch entsprechende Programme und Zertifizierungen gemäß 3.3 realisiert werden. *Allen IT-Fachleuten wird dringend empfohlen, solche Weiterbildungsangebote wahrzunehmen. Entsprechendes (gemäß 3.5) gilt auch für die Datenschutzbeauftragten.*

Bei Weiterbildungsprogrammen, die nicht auf IT-Sicherheit fokussiert sind, ist häufig ein vollständiges Fehlen von Sicherheitsaspekten festzustellen. Solche Programme können heute eigentlich nicht mehr guten Gewissens empfohlen werden. *Stattdessen geht hier eine dringende Empfehlung an die Veranstalter, ihre Programme so zu erweitern, dass auch die für den jeweiligen Einsatzbereich relevanten IT-Sicherheits-Kompetenzen vermittelt werden, wie in 3.2 erläutert. Die Weiterbildung der Datenschutzbeauftragten sollten durch die Einführung einheitlicher Standards auf eine neue Qualitätsstufe gestellt werden.*

Im beruflichen Schulwesen ist die Situation ähnlich wie in den allgemeinbildenden Schulen und den Hochschulen: die Einsicht in die Notwendigkeit, das Thema IT-Sicherheit in den Lehrstoff einzubeziehen, wächst; bei der systematischen Umsetzung bestehen aber noch Defizite. *Es wird empfohlen, diese Umsetzung in allen Schulformen zu beschleunigen und sich dabei am Kompetenzraster aus Abb. 1 zu orientieren.*

Eine letzte Bemerkung zur Weiterbildung aus nationaler Sicht: Es fällt auf, dass anerkannte Bildungsprofile zur IT- und Informationssicherheit vornehmlich im Ausland entwickelt wurden und vom Ausland her vermarktet werden. Bildungsprofile, die in der Bundesrepublik Deutschland entwickelt wurden, konnten international bisher keine Bedeutung erringen. Es sei darauf hingewiesen, dass Bildungsprofile und die dazugehörigen Personalzertifizierungen längst auch als Wirtschaftsgut einer globalisierten Dienstleistungsgesellschaft anzusehen sind. In Deutschland entwickelte Bildungsprofile müssen daher nicht nur mit den Methoden der Bildungspolitik, sondern auch mit den Methoden der Wirtschaftsförderung unterstützt und zur internationalen Marktreife weiterentwickelt werden.

Mitglieder des Arbeitskreises: Bernd Donabauer, Werner Dostal, Dietmar Johlen, Klaus-Peter Löhr (Sprecher), Dirk Schadt. Beiträge auch von Marit Hansen und Gerhard Weck.

Schriftenverzeichnis

[GI 2006a] Gesellschaft für Informatik: Positionspapier der Gesellschaft für Informatik e.V. zur IT-Aus- und -Weiterbildung. August 2006.
www.gi-ev.de/fileadmin/redaktion/Download/IT-WB_Positionspapier2006.pdf

[GI 2006b] Gesellschaft für Informatik: IT-Sicherheit in der Ausbildung – Empfehlungen zur Berücksichtigung der IT-Sicherheit in der schulischen und akademischen Ausbildung. Oktober 2006.
www.gi-ev.de/service/publikationen/empfehlungen