Zertifizierung für IT-Sicherheitsspezialisten

Schein der Weisen

Christoph Puppe

Die in den USA längst gängige Zertifizierung für IT-Sicherheitsexperten setzt sich allmählich auch hierzulande durch. *iX* stellt die wichtigsten Zertifikate vor.

Zertifikate sollen einen definierten Qualitätsstandard gewährleisten. Bei Personen trägt der Erwerb eines Zertifikats überdies zur Einschätzung seiner beruflichen Fähigkeiten bei, was sowohl für den Arbeitgeber, als auch für den Mitarbeiter selbst von Vorteil ist – wenngleich die Zertifikate hierzulande in Stellenausschreibungen und Gehaltsverhandlungen noch nicht dieselbe Bedeutung haben wie im „Mutterland", den USA.

Hersteller bieten häufig auf die eigenen Produkte oder Betriebssysteme reduzierte Zertifizierungen an. Ist jedoch der Nachweis umfassender herstellerunabhängiger Kenntnisse der IT-Sicherheit gewünscht, sind Lern- und Prüfwillige bei den Zertifizierungsanbietern ISC2, ISACA, GIAC oder COMPTIA richtig (s. Kasten „Adressen im Web").

Alle vier bieten Zertifikate an, die Aussagen über die Kenntnisse, Praxiserfahrung und teilweise auch Vertrauenswürdigkeit der Zertifizierten treffen. Die Anforderungen in jedem dieser Gebiete und die Zielrichtung unterscheiden sich jedoch teilweise stark von Anbieter zu Anbieter. Die ISACA stellt mit ihrem Certified Information Systems Auditor (CISA) und dem Certified Information Security Manager (CISM) hohe Ansprüche an die Kandidaten und ist weithin anerkannt. Der Schwerpunkt der geprüften Inhalte liegt neben der Technik eher auf organisatorischen Fragen bei Auditierung beziehungsweise Management.

Die ISC2 stellt dagegen mit dem Certified Information Systems Security Professional (CISSP) und dessen „kleinem Bruder" Systems Security Certified Practioner (SSCP) ein stärker auf Technik zugeschnittenes Zertifikat aus. Auch diese beiden berücksichtigen alle Bereiche der Unternehmenssicherheit: Fragen zu Organisation, Brandschutz, Risikomanagement und physikalische Sicherheit müssen die Prüflinge beantworten können.

Die Zertifizierungsorganisation des amerikanischen Sicherheitsinstitutes SANS (www.sans.org), die GIAC, ist zwar erst seit dem Jahr 2000 aktiv, hat in dieser kurzen Zeit jedoch schon 6000 Zertifikate ausgestellt. Sie bietet als einzige ein Modulkonzept an, im Rahmen dessen Themen wie Firewalls und Verschlüsselung als einzelne Zertifikate erhältlich sind. Jedes dieser Einzelzertifikate ist sehr viel praktischer orientiert als der entsprechende Bereich bei den anderen Anbietern. Überdies gehen sie mehr in die Tiefe, was sich etwa daran zeigt, dass Prüflinge nicht nur einen oder zwei Multiple-Choice-Test absolvieren, sondern auch eine auf circa 30 bis 50 Seiten dokumentierte praktische Aufgabe oder eine gleich lange Analyse vorlegen müssen.

Wer hats erfunden?

Erst seit einem Jahr bietet die COMPTIA das Sicherheitszertifikat Security+ an. Es ist in Umfang und Kosten das kleinste der hier vorgestellten. Die Bandbreite der Themen ist vergleichbar mit der des CISSP, allerdings umfasst die Prüfung nur halb so viele Fragen. Die Bekanntheit der

iX-TRACT

- Die Zertifizierung von IT-Sicherheitsexperten ist für den Arbeitgeber, aber auch für den Experten selbst eine hilfreiche Einschätzung seiner Fähigkeiten.
- Anzahl und Akzeptanz der aus den USA stammenden IT-Sicherheitszertifikate haben in den letzten Jahren in anderen Ländern stark zugenommen.
- Eine Gehaltssteigerung, wie sie in den USA für Zertifizierte üblich ist, ist hierzulande noch eher die Ausnahme als die Regel.

COMPTIA, die geringen Anforderungen und das weltweite Netz von Prüfungsstellen haben dazu beigetragen, dass es nach nur einem Jahr schon 5000 Zertifizierte gibt. Ein genauerer Überblick über die thematische Ausrichtung der Zertifikate und die Anzahl der bereits vergebenen findet sich in der Übersichtstabelle auf Seite 116/117.

Allen Zertifikaten gemein ist, dass sie aus den USA stammen und für einen europäischen Prüfling ungewohnte Fragen zu Recht, Standards und Methoden stellen. Hier ist das Lernen der amerikanischen Vorgaben notwendig, auch wenn diese für die Praxis in Europa nur bedingt anwendbar sind.

Der starke amerikanische Fokus schlägt sich nicht nur in Themen und Sprache der Prüfung wieder, auch stammen die meisten Zertifizierten aus den USA (s. Abb. 1). So sind etwa lediglich 20 % der CISA-Absolventen aus Europa/Afrika. Unter den etwas über 22 100 CISSP-Zertifizierten sind gerade einmal 93 deutsche, bei insgesamt 8 % Europäern. Demgegenüber stehen 15 000 US amerikanische und 1300 kanadische Absolventen. Asien und Europa liegen etwa gleichauf, immerhin 19 % der CISAs und circa 12 % der CISSPs kommen aus asiatischen Ländern.

Dementsprechend höher sind Anerkennung und Bekanntheitsgrad der Zertifikate in den USA, was sich etwa beim Vergleich von Stellenangeboten zeigt. Von 450 Ergebnissen bei der Stichwortsuche „CISSP“ bei einem weltweit operierenden Online-Dienst (www.monster.de) sind nur 17 aus Europa – davon keiner aus Deutschland – und 350 aus den USA. Der CISA wird in Europa 27-mal gesucht, in Deutschland keinmal und in den USA 630-mal, bei weltweit 720 Angeboten. Entgegen diesem Trend scheint der CISSP in Deutschland mehr Beachtung als der CISA zu finden. Darauf deutet zumindest die immerhin doppelte Anzahl der deutschen Webseiten zu diesem Thema hin.

Der GIAC Security Expert (GSE) ist noch zu jung, um in Stellenanzeigen Beachtung zu finden, die weiteren Zertifikate der GIAC werden dort nur selten explizit gesucht. Das Modulkonzept erschwert es, eine für alle Zertifikate geltende Einschätzung bezüglich ihrer Bedeutung zu treffen.

Auch wenn in einer Stellenausschreibung kein spezielles Zertifikat gefordert ist, kann der Nachweis des Wissens auf diese Art hilfreich sein. Selbst wenn nicht gewährleistet ist, dass der deutsche Personalchef oder der Abteilungsleiter der IT-Abteilung schon davon gehört haben oder sich des Schwierigkeitsgrades der jeweiligen Prozedur bewusst sind. Ob auch hierzulande Gehaltssteigerungen von circa 10 % möglich sind, wie dies nach Studien von Foote and Partners (www.lfpltd.com) in den USA mit dem CISA der Fall ist, hängt wohl mehr vom eigenen Verhandlungsgeschick ab.

Sicherheit ist vielleicht das komplexeste Thema der IT und damit auch der Zertifizierung von IT-Kräften. Ein Überblick über alle verwendeten Komponenten, ihr Zusammenspiel und die organisatorischen Abhängigkeiten und Bedingungen sind notwendig, um eine sichere Infrastruktur in einem Unternehmen aufzubauen, zu verwalten oder zu überprüfen. Eine seriöse Zertifikatsprüfung muss jeden dieser Aspekte berücksichtigen. Alle Zertifikate stellen überdies an den Prüfling Anforderungen, die in puncto Berufspraxis und Kenntnisse über die eigentlichen Prüfinhalte hinausgehen.

Komplexes Wissen gefragt

Umfassende Kenntnisse verlangen auch Hard- und Softwarehersteller für ihre eigenen Zertifikate, die hier nur kurz erwähnt werden sollen. Sie setzen häufig den Erwerb mehrerer ihrer Zertifikate für die Prüfung zum Sicherheitsadministrator ihrer Produkte voraus. Meistens muss der Prüfling sich mit einem Querschnitt der angebotenen Produkte und den dazugehörenden organisatorischen sowie planerischen Aufgaben unternehmensweit auskennen und dies in vorangegangenen Prüfungen nachgewiesen haben. Durch die Behandlung unterschiedlicher Bereiche und technischer Themen kann man davon ausgehen, dass ein derart Zertifizierter über ausreichend Praxiserfahrung verfügt, um spezielle Sicherheitsfragen nicht nur auf dem Papier beantworten zu können.

Einen ähnlichen Ansatz verfolgt die GIAC mit dem GSE. Für diesen Abschluss müssen fünf der normalen Zertifikate, die sich jeweils auf einen Teilbereich der IT-Sicherheit konzentrieren (Firewalls, IDS, Incidents, Unix und Windows) erworben werden. Da jedes einzelne dieser Zertifikate mit erheblichem Aufwand verbunden ist, können sich erst zwei Absolventen mit dem Titel GSE schmücken. Weitere Zertifikate der GIAC wenden sich teilweise direkt an Einsteiger. Weitergehende Nachweise sind generell nicht erforderlich.

Ein anderer Ansatz ist die Berücksichtigung von Berufserfahrung in relevanten Positionen. Hier verlangt die ISACA mit fünf Jahren nachgewiesener Erfahrung deutlich mehr als die ISC2, die erst 2003 den nachzuweisenden Zeitraum von drei auf vier Jahre erhöht hat. Der COMPTIA reichen gar zwei Jahre Berufserfahrung, und selbst das ist nur eine Empfehlung, nicht Bedingung. ISC2 und ISACA rechnen den Kandidaten für schon erreichte Abschlüsse und Titel einige Berufsjahre an. ISACA überprüft den Lebenslauf anhand der genannten Arbeitgeber, bei der ISC2 erfolgt die Überprüfung lediglich in Form von Stichproben und einer Bestätigung durch einen anderen CISSP. Dieser muss dem Prüfling professionelles Verhalten und die Einhaltung gewisser Grundregeln bescheinigen.

Da die Prüflinge in ihrer Arbeit eine besondere Vertrauensstellung innehaben und ihre neuen Arbeit- und Auftraggeber ihnen aufgrund der Zertifizierung häufig einen Vertrauensvorschuss entgegenbringen, versuchen die Zertifizierungsanbieter auch hier, einen für Absolventen gültigen Standard zu setzen. GIAC, ISC2 und ISACA verlangen vom Prüfling, dass er sich ihrem „Code of Ethics“ unterwirft. Dieser verlangt, dass der zukünftig zertifizierte Sicherheitsexperte nur Aufträge annimmt, für die er auch qualifiziert ist, dass er durch sein Verhalten weder seinen, noch den guten Ruf anderer schädigt, dass er keine strafbaren

Handlungen vornimmt und so weiter. Die Grundsätze variieren leicht, je nach Anbieter. Bei nachgewiesenen Zuwiderhandlungen kann der Anbieter das Zertifikat aberkennen, was etwa die GIAC nach eigenen Aussagen schon bei 95 Personen getan hat.

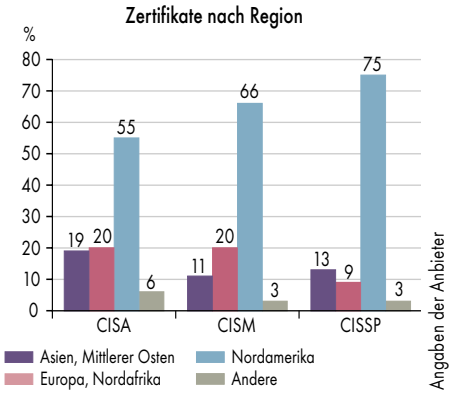
Ohne Fleiß …

Für jedes Zertifikat gibt es Schulungsanbieter, die entsprechende Kurse im Programm haben. Sie sind teilweise auch von den Zertifizierern anerkannt. Am besten schaut man sich im Vorfeld die Schulungskräfte genau an und entscheidet, ob man sie sympathisch findet, ihnen vertraut und so weiter. Dass angesichts des umfangreichen Stoffes eine fünftägige Schulung nur ein Teil der Vorbereitung sein kann, versteht sich fast von selbst. Wer sich jedoch unsicher ist, ob er die Sicherheitskonzepte und die Vorgehensweisen zu ihrer Erstellung verstanden hat, findet hier Unterstützung.

Eine Ausnahme in diesem Punkt bildet die GIAC. Da sie aus einer Organisation hervorgegangen ist, die schon seit vielen Jahren Schulungen zur IT-Sicherheit anbietet, sind die einzelnen Zertifikate sehr gut auf die Schulungsangebote abgestimmt. Bei ausreichendem Vorwissen sollten die Kurse den Teilnehmenden in die Lage versetzen, die Prüfung zu bestehen. Allerdings muss der Prüfling zusätzlich noch eine schriftliche Arbeit zu einer praktischen Aufgabe abliefern – und diese Fähigkeit lässt sich kaum in einer Schulung auf die Schnelle erwerben.

Details und Faktenwissen sollte man mit den verfügbaren Büchern und Online-Ressourcen erwerben. Hier ist allerdings Vorsicht geboten: Selbst das Durcharbeiten eines mehrere hundert Seiten starken Buches ist noch keine Garantie dafür, dass man besteht. Schließlich gibt es bei allen Prüfungen jedes Jahr neue Fragen, und die Themen werden teilweise in einer Tiefe abgefragt, die ein Buch alleine selten vermitteln kann.

Vorbereitungsfragen für die Prüfung erhält man auf drei Arten: In guten Büchern finden sich nach jedem Kapitel Fragen zum behandelten Stoff, die sich in der Regel allerdings nur auf die im Buch enthaltenen Themen beziehen. Auch entsprechen diese Fragen nicht immer dem Schwierigkeitsgrad der Prüfung. Die fehlerfreie Beantwortung kann einen in der trügerischen Sicherheit wiegen, das Thema bereits ausrei-



Noch dominieren die USA bei allen Zertifikaten. Der Anteil der Zertifizierten aus den anderen Erdteilen ist in den letzten Jahren allerdings stark angestiegen (Abb. 1).

INTERNATIONALE ZERTIFIKATE FÜR IT-SICHERHEITSEXPERTEN

Zertifizierung	CISSP (Certified Information Systems Security Professional)	SSCP (Systems Security Certified Professional)	CISA (Certified Information Systems Auditor)	CISM (Certified Information Security Manager)
Anbieter	ISC2	ISC2	ISACA	ISACA
URL	www.isc2.org	www.isc2.org	www.isaca.org	www.isaca.org
Umfang/Inhalte	Access Control; Systems & Methodology; Applications & Systems Development; Business Continuity; Planning; Cryptography; Law, Investigation & Ethics; Operations Security; Physical Security; Security Architecture & Models; Security Management Practices; Telecommunications, Network & Internet Security	Access Controls; Administration; Audit & Monitoring; Risk, Response & Recovery; Cryptography; Data Communications; Malicious Code/Malware	Management, Planning & Organization of Information Security; Technical Infrastructure & Operational Practices; Protection of Information Assets; Disaster Recovery & Business Continuity; Business Application; System Development; Acquisition; Implementation & Maintenance; Business Process; Evaluation and Risk Management; Information Security Audit Process	Information Security Governance; Risk Management; Information Security Programme Management; Information Security Management; Response Management
Multiple Choice-Fragen	250	125	200	200
Thesenpapier	nein	nein	nein	nein
ausgestellte Zertifikate	22 000	430	30 000	4900
Kosten der Prüfung	599 US-$	469 US-$	495 US-$	495 US-$
Kosten pro Jahr für Erhalt	85 US-$	65 US-$	keine direkten	keine direkten
Jahre Erfahrung vorausgesetzt	4	1	5	5
Erhalt des Zertifikates	120 CPE[1] in drei Jahren	60 CPE[1] in drei Jahren	120 Stunden Fortbildung in drei Jahren	120 Stunden Fortbildung in drei Jahren

[1] CPE – Continuing Professional Education

chend zu beherrschen. Fragenkataloge gibt es auch in Form von Software. Hier ist darauf zu achten, dass die Antworten so gut kommentiert sind, dass man gleich für alle dieses Detail betreffenden Fragen gewappnet ist. Eine Fragenkatalogsoftware sollte eine Prüfungssimulation, ausreichend Fragen sowie die Möglichkeit, nur bestimmte Themen auszuwählen und in vorherigen Durchgängen falsch beantwortete Fragen zu wiederholen, enthalten. Neben den kostenpflichtigen Produkten gibt es Websites, die diese Vorbereitung zumindest teilweise bieten und als dritte Quelle dienen können. Empfehlenswert ist etwa www.lostclusterz.com.

Weltweite Anerkennung

Die Prüfungen bestehen bei allen Anbietern aus Multiple-Choice-Fragen in englischer Sprache – dafür sind die Zertifikate allerdings auch international anerkannt. Überdies sind alle relevanten Konferenzen sowie ein Großteil des Materials zum Erhalt des Wissens in Englisch, sodass man sich besser gleich an die Fremdsprache gewöhnt.

Geprüft wird bei den meisten Anbietern in speziellen Prüfungszentren. Nur die GIAC macht hier eine Ausnahme: Per Web vom heimischen PC aus kann man die Prüfungsfragen beantworten. Das mag auf den ersten Blick zu einfach erscheinen. Man darf aber nicht vergessen, dass die GIAC den Kandidaten noch das Schreiben eines Papiers abverlangt und diese Eigenleistung wird kontrolliert – zumindest daraufhin, dass die Arbeit von keiner anderen Publikation abgeschrieben ist. Anders sieht es für die Zertifizierung zum GSE aus: Eine viertägige Prüfung während einer SANS-Konferenz mit praktischen Aufgaben, Multiple Choice, mündlichem Vortrag und dem Verfassen eines Paper unterstreichen den Anspruch der GIAC, das praxisnächste Zertifikat anzubieten.

COMPTIA und ISC2 führen mehrmals im Jahr Prüfungen durch, Termine und Anmeldeformulare finden sich auf ihren Webseiten. Die ISACA ist auch hier ein wenig schärfer als die anderen, da die Prüfung weltweit nur einmal im Jahr – in diesem Jahr am 12. Juni – abgelegt werden kann.

Die in der Übersichtstabelle genannten Preise der einzelnen Zertifikate sind jeweils ohne Rabatte für

Aus deutschen Landen

Alternativ zu den internationalen Zertifikaten bietet die International Security Tuition Association (ISTA; www.ista.org) in deutschsprachigen Landen die Zertifizierung zum Certified Information Security Officer (CISO) an. In einem vierwöchigen Schulungslehrgang, der einmal jährlich (in diesem Jahr vom 7.6. bis 3.7.) stattfindet, wird ein relativ umfassendes, praxisorientiertes Themenspektrum behandelt. 40 Absolventen von deutschen Behörden und Unternehmen haben bislang ein Zertifikat erworben. Die Prüfung basiert nicht auf Multiple Choice, sondern auf der ausformulierten Beantwortung von 40 zum Teil komplexen Fragen. Eine internationale Ausrichtung durch die zusätzliche Schulungs- und Prüfungssprache Englisch (derzeit ausschließlich Deutsch) ist nach Aussagen des Anbieters geplant. Ein weiteres in Deutschland ausgegebenes Zertifikat ist der „IT-Grundschutzauditor“ des Bundesamtes für Sicherheit in der Informationstechnik (mehr Informationen unter www.bsi.de).

GSE (GIAC Security Expert)	GIAC Module (33 stehen zur Auswahl)	Security+
GIAC	GIAC	COMPTIA
www.giac.org	www.giac.org	www.comptia.org
Voraussetzung sind folgende Zertifikate: GIAC Certified Firewall Analyst; GIAC Certified Intrusion Analyst; GIAC Certified Incident Handler; GIAC Certified Windows Security Administrator; GIAC Certified Unix Security Administrator	GIAC Security Essentials Certification (GSEC); GIAC Certified Firewall Analyst (GCFW); GIAC Certified Security Leadership (GSLC); GIAC Certified Intrusion Analyst (GCIA); GIAC Certified Incident Handler (GCIH); GIAC Certified Windows Security Administrator (GCWN); GIAC Certified Unix Security Administrator (GCUX); GIAC Information Security Fundamentals (GISF); GIAC Systems and Network Auditor (GSNA) und weitere	General Security Concepts; Communication Security; Infrastructure Security; Basics of Cryptography; Operational/Organizational Security
ja, zusätzlich zu praktischen Aufgaben, mündlicher Vortrag	75 – 90	100
ja	ja	nein
2	6000	5000
noch nicht bekannt	250 US-$	250 US-$
wie die Teilzertifikate	60 US-$ Prüfungskosten	keine
–	–	2 (Soll, kein Muss)
noch nicht bekannt	Prüfung alle 2 Jahre; 120 US-$ für alle eines Jahres	–

Mitgliedschaften oder Frühbucherrabatte an. Wer sich beispielsweise der ISACA anschließt, kann bis zu 180 US-Dollar sparen. Alle anderen bieten ausschließlich Frühbucherrabatte an.

Wandel ist die einzige Konstante der IT und besonders der IT-Sicherheit. Die Anbieter reagieren darauf mit Vorgaben zur ständigen Auffrischung des Wissensstandes, um ein Zertifikat zu behalten. Auch hier ist es die ISACA, die die höchsten Anforderungen stellt: 120 Stunden Fortbildung in drei Jahren, wobei eine Schulstunde ohne Pause gerechnet wird. Längere Unterbrechungen darf es nicht geben, es müssen jedes Jahr mindestens 20 Stunden nachgewiesen werden. Die ISC2 hat hier fast die gleichen Anforderungen. Bei beiden kann man sich sowohl den Besuch als auch die Durchführung von Schulungen, das Lesen von Fachbüchern, das Verfassen von Fachartikeln und weitere qualifizierende Maßnahmen anrechnen lassen. Grundlage der Berechnung sind so genannte CPE-Punkte (Continuing Professional Education), von denen innerhalb von drei Jahren 120 für CISSPs und 60 für SSCPs nachzuweisen sind.

Die GIAC verlangt, dass für jedes einzelne Zertifikat alle zwei Jahre erneut eine Prüfung abgelegt wird. Der Zertifizierte zahlt dafür 120 Dollar pro (Prüfungs-)Jahr, unabhängig von der Anzahl der Prüfungen – es empfiehlt sich also, alle Zertifikate entweder in geraden oder in ungeraden Jahren zu erwerben, andernfalls könnte der Erhalt teuer werden. Mit dieser Preispolitik ist die GIAC preiswerter als ISC2 und ISACA, die eine Gebühr von 65 beziehungsweise 85 Dollar pro Jahr verlangen. Bei der COMPTIA müssen die Zertifikate nicht aufrechterhalten werden, es bleibt beim einmaligen Erlangen.

Fazit

Hat man sich zu einer Zertifizierung entschlossen, gilt es zunächst zu überlegen, welche Zertifikate für die eigene Karriere die richtigen sind: ob man sich etwa auf einen Hersteller festlegen oder lieber ein unabhängiges und umfassenderes Zertifikat erlangen möchte. Auch im letzten Fall ist es schwierig, eine Empfehlung zu geben, da die Zertifikate unterschiedliche Zielrichtungen und Themenschwerpunkte verfolgen. Ein genauer Vergleich der Prüfungsinhalte mit den eigenen Karrierezielen ist unerlässlich. Grundlegend lässt sich sagen, dass die Zertifikate der ISACA und ISC2 international einen guten Ruf haben. Die Chancen stehen also gut, dass auch Arbeitgeber hierzulande sie bei Jobsuche und Gehaltsverhandlung anerkennen.

Wer ein umfassendes Wissen nachweisen möchte, ist mit dem CISSP, CISA und GSE sicherlich gut bedient. CISM, CISSP oder entsprechende Module der GIAC sind eher für Sicherheitsbeauftragte oder -manager geeignet. Wer sein Betätigungsfeld eher bei Revision und Audit sieht, bevorzugt voraussichtlich den CISA oder die passenden Module der GIAC. Für Techniker, die sich intensiv mit dem Thema Sicherheit beschäftigen wollen, ist der GSE mit seiner Detailliertheit und Tiefe sicherlich eine gute Wahl. Auch CISSP und CISA sind für Techniker geeignet, sofern sie bereit sind, sich mit organisatorischen und Verwaltungsaspekten zu befassen. Möchte man sich als Techniker auf einen Bereich konzentrieren, sind die Module der GIAC die einzige herstellerneutrale Möglichkeit, eine Zertifizierung zu erlangen. Für Berufsein- und -umsteiger ist der SSCP und der Security+ eine gute Wahl.

Wer nur sein Wissen testen möchte, sei auf Websites mit Testfragen verwiesen oder auf die Anbieter von reinen Online-Zertifikaten, die man sich auch „in schön“ gedruckt nach Hause schicken lassen kann. Ob ein Arbeitgeber diese jedoch anerkennt, ist fraglich. (ur)

CHRISTOPH PUPPE

ist Security Consultant bei der Hisolutions AG in Berlin.

ADRESSEN IM WEB

International Information Systems Security Certification Consortium (ISC2)	www.isc2.org
Information Systems Audit and Control Association (ISACA)	www.isaca.de
Global Information Assurance Certification (GIAC)	www.giac.org
Computing Technology Industry Association (COMPTIA)	www.comptia.de