



Stefan Burkhardt

Bildungsberatung - Bildungsmanagement

Am Feldwinkel 1
D-40474 Düsseldorf

Telefon +49-211-41 84 605
Telefax +49-211-41 84 606
Mobil +49-173-52 56 556

www.debraco.de
sburkhardt@debraco.de

IT-Security-Experten sind gefragt

Die Aussichten für Sicherheitsexperten sind gut: Die Zahl derer, die auf diesem Feld arbeiten, soll weltweit von heute 1,3 Millionen auf fast 2,2 Millionen im Jahr 2008 steigen. So lauten zumindest die Prognosen von IDC und der Zertifizierungsorganisation (ISC)². In der gemeinsamen "Global Workforce Study", an der rund 5500 Entscheidungsträger aus der Wirtschaft teilnahmen, beurteilen die Security-Profis sowohl ihre Berufsaussichten als auch ihre Verdienstmöglichkeiten als gut bis sehr gut. Auch mit den Weiterbildungsmöglichkeiten sind die Befragten zufrieden: Sie erhalten im Durchschnitt zehn Tage pro Jahr für Zusatztrainings genehmigt. 27 Prozent rechnen für 2005 sogar mit mehr Fortbildung. Mehr als 50 Prozent der Sicherheitsfachleute verdienen eigenen Angaben zufolge im Jahr 80000 Euro und mehr.

Nach Ansicht von Peter Berlich, Security-Manager bei IBM in der Schweiz und Mitglied im europäischen Advisory Board von (ISC)² ist die Rolle des IT-Sicherheitsbeauftragten wichtiger geworden: "In vielen Unternehmen ist diese Funktion mittlerweile in der Umgebung der Geschäftsleitung etabliert." Das liege zum einen an dem stärkeren regulatorischen Druck, den die Kreditvergabe-Richtlinien Basel II bewirkt hätten und zum anderen am US-amerikanischen Sarbanes-Oxley Act, der eine genaue Einhaltung und Überwachung der Sicherheitsmaßnahmen für die meisten größeren Unternehmen notwendig mache. Berlich: "Gleichzeitig hat sich das Risiko-Management als Führungsmethode in den Unternehmen etabliert. Hier geht es nicht mehr um Risikovermeidung, sondern um Risikoabwägung." Kein Unternehmen könne seine operativen Risiken managen, ohne der IT- und Informationssicherheit besondere Aufmerksamkeit zu schenken.

Aus dem IT-Sicherheitsexperten, der bislang komplexe technische Einzelmaßnahmen überwacht und eingeführt habe, ist laut Berlich der Informationssicherheits-Manager geworden, der sich am geschäftlichen Bedarf und nicht an der technischen Machbarkeit orientiert. Um diese Anforderungen erfüllen zu können, müssten die Sicherheitsexperten hervorragend qualifiziert sein. Berlich: "Die Zeiten, in denen derjenige die Security betreute, der gerade Lust und Laune oder nichts anderes zu tun hatte, sind endgültig vorbei. Zudem sind gerade in Deutschland akademische Qualifikationen in der IT gefragt."

Laut der Studie sehen 30 Prozent der befragten Unternehmen eine Berufszertifizierung als sehr wichtiges Einstellungs- und Karrierekriterium an. International haben sich Zertifikate wie der Certified Information Systems Security Professional (CISSP) von (ISC)² und der Certified Information Systems Auditor (CISA) etabliert. In Deutschland begann im vergangenen Jahr die Ausbildung zum Teletrust Information Security Professional (TISP). Daneben haben für Berlich auch herstellerspezifische Zertifikate wie der Cisco Certified Security Professional (CCSP) oder Microsoft Certified Systems Engineer Security (MCSE) im technischen Bereich eine Berechtigung. Der Security-Manager erwartet, dass es bei den Zertifizierungsangeboten künftig noch mehr Wettbewerb geben wird.

Für die Sicherheitsunternehmen selbst spielen Zertifizierungen bei der Personalsuche keine große Rolle. Elmar Haag, technischer Leiter bei Integralis in Heilbronn: "Die Aussagekraft von Zertifizierungen über die tatsächliche Qualifikation eines Kandidaten ist in der Regel sehr begrenzt." Eine Reihe von Kunden indes sehe dies anders und frage zunehmend nach zertifizierten Sicherheitsexperten. Ganz oben auf der Wunschliste ständen herstellerunabhängige Zeugnisse wie CISSP. Haag: "Dass der Bedarf an Security-Profis steigt, erleben wir täglich. Allerdings sind gute Leute am Markt nur schwer zu finden."



Stefan Burkhardt

Bildungsberatung - Bildungsmanagement

Am Feldwinkel 1
D-40474 Düsseldorf

Telefon +49-211-41 84 605
Telefax +49-211-41 84 606
Mobil +49-173-52 56 556

www.debraco.de
sburkhardt@debraco.de

Die Sicherheitsunternehmen suchen zum einen strategische und zum anderen technische Berater. Während von den strategischen Consultants Kenntnisse in den Bereichen Betriebswirtschaftslehre, Management und IT erwartet werden, sollten die so genannten Junior-Berater "so richtige PC-Freaks" sein. Haag: "Das sind die klassischen Hochschulabgänger, die auch in ihrer Freizeit am PC sitzen. Sie müssen allerdings noch lernen, dass Projektarbeit beim Kunden vor allem Stress bedeutet. Damit umzugehen ist am Anfang gar nicht so einfach." Die Suche nach Senior-Beratern, also Kandidaten mit mehrjähriger Produkt- und Projekterfahrung im Security-Bereich, gestaltet sich zumeist noch weitaus schwieriger, da nur ein relativ kleiner Kreis an Arbeitskräften in Deutschland sich mit den einschlägigen Spezialprodukten genug auskenne.

Gute Chancen haben nach Meinung des Integralis-Managers momentan die Sicherheitsbeauftragten. Ihre Aufgabe sei es, Sicherheitslücken weniger auf der technischen als auf der organisatorischen Ebene zu schließen. Dazu müssten sie zwar über technischen Background verfügen, aber nicht unbedingt wissen, wie eine Firewall konstruiert und installiert wird. Oberste Aufgabe sei es, die Mitarbeiter für die Sicherheitsproblematik zu sensibilisieren. Der Integralis-Consultant: "Aufgrund der großen Anforderungen ist diese Position in den Konzernen zumeist in der Management-Ebene aufgehängt."

Das sieht Wolfram Funk, Senior Consultant bei der Meta Group in Ismaning bei München, ähnlich: "In großen Unternehmen ist der Sicherheitsbeauftragte in der Tat in der Topetage zu finden. Bei kleineren und mittleren Unternehmen dagegen kann es vorkommen, dass er irgendwo in der Netzwerkgruppe integriert ist." Wenn der Sicherheitsbeauftragte hierarchisch so weit unten stehe, habe er naturgemäß keine größeren Befugnisse.

Funk bemängelt, dass sich das Sicherheitsbewusstsein in den Unternehmen lediglich in den Bereichen geändert habe, in denen die Probleme offensichtlich seien. Bekannt seien die Gefahren durch Viren, Würmer, Spyware oder Hacker-Attacken. Der Meta-Consultant: "Über diese Sicherheitsprobleme wird nicht nur ständig in den Medien berichtet - etliche Unternehmen können selbst ein Lied davon singen." Für Funk steht fest, dass Sicherheitsexperten in ihrem Job vor allem über Erfahrung verfügen müssen: "Da der IT-Markt nicht statisch ist, wird es sich zwischen Internet-Kriminellen und Security-Profis immer um eine Art Hase-und-Igel-Wettlauf handeln." Neue Techniken wie Web-Services oder Mobile Computing hätten ihre eigenen Sicherheitslöcher. Der Marktanalyst erkennt zwar in vielen Unternehmen ein zunehmendes Bewusstsein für die möglichen Schäden, dem stünden aber fast immer knappe Budgets gegenüber. Funk: "Zur Abwehr von Gefahren gehört eine detaillierte Risikoanalyse. Da diese aber nur in den wenigsten Unternehmen stattfindet, haben wir es allzu oft mit Flickwerk zu tun."

Michael Dickopf, IT-Experte beim Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn, sekundiert ihm: "Wie das Thema gehandhabt wird, hängt von der Größe des Unternehmens ab. So haben mittlere Firmen zwar oft eine Firewall installiert, aber keinen Sicherheitsprofi, der für deren Überwachung zuständig ist. Dementsprechend werden Hacker-Angriffe oftmals überhaupt nicht registriert." Firmen wüssten zwar über solche Gefahren besser Bescheid als noch vor ein paar Jahren, bei der Abwehr hapere es jedoch nach wie vor an der praktischen Umsetzung: "Natürlich wollen die Unternehmen den Angreifern mit qualifizierten Sicherheitsprofis Paroli bieten - aber die gibt es nicht fertig gebacken." Nach seinen Erfahrungen sollten die Security-Experten neben ihrem Computer-Know-how über Zusatzqualifikationen im Bereich IT-Sicherheit verfügen. "Im Idealfall", erklärt der BSI-Fachmann, "sind noch organisatorische Fähigkeiten sowie soziale Kompetenzen vorhanden."



Stefan Burkhardt

Bildungsberatung - Bildungsmanagement

Am Feldwinkel 1
D-40474 Düsseldorf

Telefon +49-211-41 84 605
Telefax +49-211-41 84 606
Mobil +49-173-52 56 556

www.debraco.de
sburkhardt@debraco.de

Hans Boos, Geschäftsführer des Frankfurter Sicherheitsdienstleisters Arago, hat die Erfahrung gemacht, dass die Kunden eher Security-Profis mit Organisations- und Management-Know-how als reine Techniker suchen: "Das ist verständlich, denn sie müssen komplexe Sicherheitsprozesse in den Griff bekommen, von den Anwendern eine Änderung ihrer Arbeitsweise verlangen sowie Sicherheitsüberprüfungen und Change-Management umsetzen." Für all diese Prozesse sei neben einer fundierten technischen Wissensbasis ein großes Organisationsverständnis erforderlich. Der Arago-Vorstand: "Was man im Sicherheitsbereich nicht gebrauchen kann, ist ein Hansdampf in allen Gassen - also jemand, der von allem ein bisschen und nichts richtig kann. Ein erfolgreicher Sicherheits-Manager muss in allen Sparten der Technik fit sein."

Für Boos steht fest, dass nicht nur die Zahl der Hacker-Angriffe massiv zugenommen hat - die Attacken seien auch gefährlicher geworden. Der Frankfurter Security-Consultant: "Je intelligenter und komplexer die Angriffe, desto professioneller müssen die Sicherheitsexperten sein." Der Arago-Chef hat deshalb kein Problem damit, auch ehemalige Hacker einzustellen. Das sind Mitarbeiter, für die das Ganze in erster Linie ein Spiel darstellt, in dem das System geschlagen, aber nicht zerstört werden soll. "Wer Schaden verursachen will, hat bei uns keine Chance", stellt er klar.

Dass Sicherheitsprofis vor allem im Bankenbereich gesucht werden, darin sind sich alle einig. Klaus Thoma von der Deutschen Bank in Frankfurt bestätigt diesen Trend: "Bei uns besteht in der Tat Bedarf. Da wir es hier mit einem hochsensiblen Bereich zu tun haben, müssen die besten Leute eingesetzt werden."

Das zunehmende Sicherheitsbewusstsein hat seiner Meinung nach unter anderem auch viel mit den aktuellen rechtlichen Regularien zu tun. Thoma: "Die größten Chancen auf einen Job haben Sicherheitsprofis, die rechtliches Know-how, methodisches Wissen über Risiko-Management sowie IT-Kenntnisse mitbringen."

Strenge Gesetze

Die Rechtsvorschriften für die Unternehmensvorsorge haben sich verschärft. Ein Beispiel ist das KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich). Geschäftsführung und Vorständen werden hierin neue persönliche Verantwortlichkeiten zugeschrieben. Sie sind zur Risikoversorge für das Unternehmen verpflichtet. Werden in der IT und anderswo keine geeigneten Sicherheitsmaßnahmen getroffen, haften Vorstand beziehungsweise Geschäftsführung unter Umständen persönlich. Darüber hinaus kann das Unternehmen nach den allgemeinen zivilrechtlichen Schadensersatzregelungen verantwortlich sein, wenn seine IT-Infrastruktur für Angriffe auf andere missbraucht wird. Auch steuerrechtlich können Rechtsfolgen entstehen - nämlich dann, wenn die Infrastruktur nicht revisionsfähig ist und somit die Besteuerungsgrundlagen nicht nachvollziehbar sind.

Von Ina Hönicke, COMPUTERWOCHE 10.02.2005
Ina Hönicke arbeitet als freie Journalistin in München.