Neuer Beruf soll Informationssicherheit in Schweizer Unternehmen erhöhen

Cyber-Risiken betreffen nicht nur IT-Sicherheitsberater

Der Verband ICT-Berufsbildung Schweiz hat in Zusammenarbeit mit dem Informatiksteuerungsorgan des Bundes (ISB) das Projekt eidgenössisches Diplom «ICT Security Expert» gestartet. Beteiligt an der Entwicklung des neuen Berufsbildes sind auch namhafte Vertreter aus der Wirtschaft. Dabei sind Microsoft Schweiz, die Schweizerische Post, Swisscom, UBS und der Verband Schweizerischer Elektrizitätsunternehmen (VSE).

Bruno Schnarwiler, Hansjörg Hofpeter

Ziel aller Aktivitäten im Bereich Sicherheit ist es, schädigende Ereignisse für das Unternehmen, seine Mitarbeitenden, Partner und die Umwelt in Häufigkeit und Auswirkung auf ein Minimum zu reduzieren.

Ein System ist dann sicher, wenn es sich zuverlässig, d. h. gemäss den ihm gegebenen Regeln, verhält und gegebenenfalls nicht regelkonformes Verhalten bemerkt sowie die nötigen Gegenmassnahmen zur Kompensation des fehlerhaften Verhaltens einleitet. Eine vollkommene Kongruenz zwischen externer Ordnung und tatsächlichem Verhalten – absolute Sicherheit – eines Systems kann nicht erreicht werden. Die relative Sicherheit lässt sich mit Massnahmen verbessern, die umso aufwendiger werden, je mehr die Nähe zur absoluten Sicherheit erreicht werden soll (sinkender Grenznutzen).

Informationssicherheit wird definiert als das angemessene und dauernde Gewährleisten der Verfügbarkeit, Integrität und Vertraulichkeit der IT-Ressourcen und der damit bearbeiteten oder übertragenen Informationen und dient dem Schutz sämtlicher Informationen ungeachtet der Art ihrer Darstellung und Speicherung.

Die Vertraulichkeit ist gewährleistet, wenn die als schutzwürdig definierten Objekte nur berechtigten Subjekten offenbart werden.

Die Integrität ist dann gewährleistet, wenn nur berechtigte Subjekte (Mensch, System oder Funktion) Schutzobjekte (System, Funktion oder Informationsbestände) zu berechtigten Zwecken korrekt bearbeiten, die Schutzobjekte spezifiziert sind und die Bearbeitung nachvollziehbar ist.

Die Verfügbarkeit ist dann gewährleistet, wenn die berechtigten Subjekte dauernd innerhalb der gemeinsam als notwendig definierten Frist auf die zur Durchführung ihrer Aufgaben benötigten Schutzobjekte zugreifen können, die notwendigen Massnahmen umgesetzt sind, die es bei Störungen erlauben, die Verfügbarkeit fristgerecht wiederherzustellen bzw. zu sichern.

Gesetzliche Anforderungen

Entwicklung, Betrieb und Verwendung von IT-Systemen, Applikationen und Informationen sind gesetzlichen Anforderungen unterworfen. Sichere Informationsbearbeitung heisst auch gesetzeskonforme Informationsbearbeitung.

Ein Bestandteil der Informationssicherheit bildet der Datenschutz, der sich mit dem Schutz der Persönlichkeit der von einer Datenbearbeitung betroffenen Person beschäftigt. Das Datenschutzgesetz des Bundes (DSG) erfasst die automatisierte und die manuelle Bearbeitung von Personendaten. Diese Daten müssen angemessen durch technische und organisatorische Massnahmen vor dem Zugriff Unbefugter geschützt werden (Art. 6 DSG). Die getroffenen Massnahmen müssen grundsätzlich verhältnismässig sein und beachten Zweck, Art und Umfang der Bearbeitung, Schätzung der möglichen Risiken für die betroffenen Personen oder das Unternehmen und den gegenwärtigen Stand der Technik.

Neben dem Datenschutzgesetz sind im Rahmen des IT-Einsatzes auch die Anforderungen des Urheberrechts und der individuellen Geheimhaltungspflichten (Fernmelde-, Bank-, Arztgeheimnis u.a.m.) zu berücksichtigen.

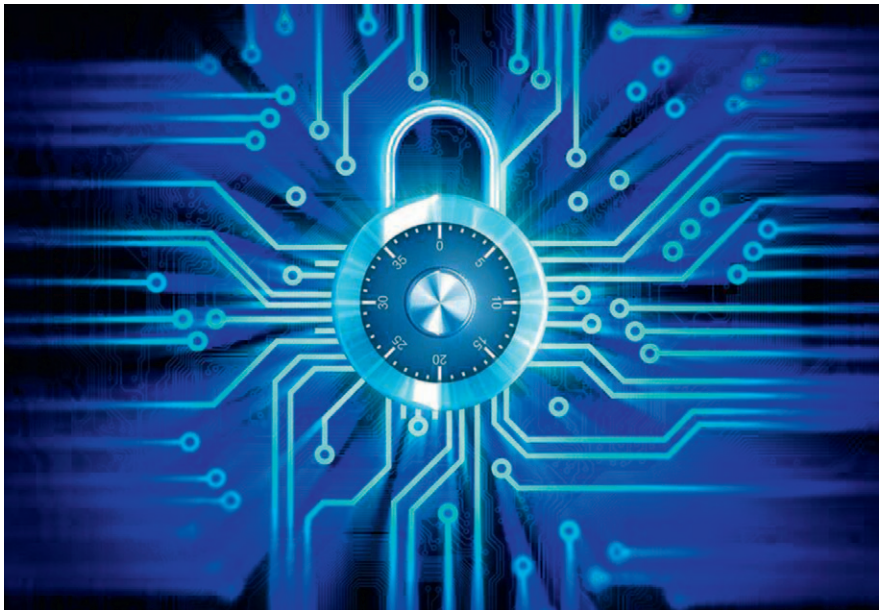

Bild 1 ICT-Security Expert, die staatlich anerkannte Vertrauensperson für Wirtschaft, Politik und Verwaltung.

Bild 2 Der ICT-Security Expert wird den zunehmend schärferen schweizerischen und internationalen Regeln im Bereich Datenschutz und Datensicherheit gerecht.

Weiterhin zu beachten sind in diesem Zusammenhang internationale Regulative (u.a. aktuell die EU-Datenschutzgrundverordnung), die für die einzelnen Unternehmen von Relevanz sein können.

Informationssicherheit als Teil der Integralen Sicherheit

Unter Integraler Sicherheit wird verstanden, dass dem gesamten Bereich Sicherheit konsequent, umfassend, abgestimmt, geplant und effizient in ethisch, wirtschaftlich und rechtlich vertretbarem Rahmen unter Ausnutzung bestehender Synergien begegnet wird. Voraussetzungen dafür sind das Engagement der Unternehmensleitung sowie eine klar formulierte Politik, welche die Verpflichtung der Organisation festlegt und dokumentiert. Notwendig ist auch eine effiziente Aufbau- und Ablauforganisation, die in der Lage ist, die weiteren Schritte zu bewältigen.

Die wichtigsten Anforderungen

Damit neue Regelungen erfolgreich sein können, müssen sie Teil der Unternehmenskultur werden.

Sicherheitspolitik

Das Management muss der Sicherheit einen umfassenden Stellenwert einräumen: Es muss im Unternehmen die Sicherheitskultur etablieren, diese kultivieren und mit den notwendigen Massnahmen Informationssicherheit gewährleisten. Im Rahmen einer Politik sind die Sicherheitsziele zu definieren. Die Grundsätze für die einzelnen Sicherheitsbereiche sind festzulegen. Das beinhaltet den Ablauf der Risikoerkennung, -bewertung und -überprüfung.

Sicherheitskonzept

Das Informationssicherheitskonzept konkretisiert die Politik unter Berücksichtigung der gesetzlichen, vertraglichen und internen Anforderungen. Im Konzept werden Massnahmen festgelegt sowie Aufgaben, Verantwortlichkeiten und Kompetenzen für Funktionen und Gremien definiert.

Risiken werden mit standardisierten und regelmässigen Methoden identifiziert. Sicherheitsregeln werden festgelegt, um künftige Risiken zu minimieren.

Regelwerk

Zum Informationsschutz sind Sicherheitsmassnahmen zu definieren, die in einem Regelwerk zusammengefasst werden können. Ein solches Regelwerk kann ungefähr 80 Prozent der Risiken abdecken. Für die verbleibenden Risiken sind Analysen durchzuführen, deren Resultate in das Regelwerk zurückfliessen.

Weitere zu regelnde Punkte sind Organisation, Krisen und Notfälle in Unternehmen, Krisenstab IT, Notfallhandbuch, Klassifizierung, Sicherheit in Projekten oder auch Awareness resp. Sensibilisierung.

Was war, ist und wird

In der Vergangenheit musste man sich in Sachen Datenübertragung, Archivierung und Verschlüsselung (Informationsschutz im weitesten Sinne) mit Brieftauben, Ton-, Wachs- und Bambustäfelchen befassen. Es genügte ein Skytale zur Verschlüsselung. Der Abakus war für Rechenaufgaben vollkommen ausreichend. Lange ging dann die Entwicklung im Vergleich zu heute in allen Informatikbereichen nur im Schneckentempo vorwärts.

Im 20. Jahrhundert betraten dann erstmals «Computer» in grösserem Stile das Rampenlicht. Anfangs waren diese Maschinen gross, vergleichsweise leistungsschwach und nahezu unerschwing-

Bilder: iStock-Foto

Bild 3 Der ICT-Security Expert ist die Fachperson bei zunehmenden Bedrohungen (inkl. soziale Faktoren), Wirtschaftsspionage & -kriminalität und Cyberangriffen.

lich. Heute können wir auf eine um ein Vielfaches grössere Leistungspalette zurückgreifen – zu einem Bruchteil der Kosten bei erheblich weniger Platzbedarf. Hier sei unter anderem an Moore's Gesetz erinnert.

Heute müssen sich nebst IT-Sicherheitsbeauftragten auch andere Unternehmensbereiche wie etwa die Entwicklungsabteilungen mit dem Thema Sicherheit befassen. Dazu zählen das Internet per se, neuerdings auch das Internet of Things (IoT), BYOD, SaaS, Phishing oder Telearbeit. Die bereits bekannten Angriffsarten auf die Informationen und Daten eines Unternehmens und eine kritische Betrachtung der Infrastruktur dürfen nicht fehlen.

Weshalb Informations- und IT-Sicherheit?

Adäquate IT-Sicherheit ist aus vielen Gründen wichtig für Unternehmen: Der Wettbewerbsdruck zwingt sie zum rigorosen Einsatz von Informatikmitteln. Die damit einhergehende zusätzliche Vernetzung erhöht jedoch das Bedrohungspotenzial von innen und von aussen. Die Abhängigkeit von IT vergrössert sich bei gleichzeitigem Wegfall eines Fall-Backs bei einem Ausfall ebendieser – dabei zählen Daten und Informationen zu den wertvollsten Einheiten von Unternehmen. Die bestehende Gesetzgebung und tiefe ethische Barrieren wirken zu wenig abschreckend. Und die Möglichkeiten einer effektiven Kontrolle sind mangelhaft oder fehlen gänzlich.

Schwierigkeiten im Bereich Informationssicherheit

Bei der Realisierung von Informationssicherheit sind wir mit vielerlei Problemen konfrontiert. Dazu gehört, dass kein anerkanntes und fundiertes Grundwissen dazu besteht. In Ausbildungsprogrammen fehlt Informationssicherheit wegen erforderlichem Einbezug verschiedener Disziplinen sowie Abteilungen und zudem ein Bewusstsein für die Bedrohung (Awareness). Dazu kommt, dass weltweit keine akzeptierten Definitionen und Standards sowie Qualifikationsmerkmale bestehen. Als weitere Hürde fungieren die unklaren Verantwortlichkeiten innerhalb des Betriebs. Auch ist die Kosten-Nutzen-Relation problematisch. Die bestehenden Hilfsmittel sind nicht benutzerfreundlich und nicht zuletzt erschwert hoher Realisierungs- und Termindruck die Entwicklung der Systeme zur Erhöhung der Informationssicherheit.

Das zentrale Problem ist die fehlende Sensibilisierung auf Stufe Top-Management mit dem Thema IT-Sicherheit. Es hat keine ernsthafte Vorstellung von den Risiken, die vom IT-Einsatz ausgehen. Das Top-Management ist sich oft auch nicht im Klaren über das Ausmass der Abhängigkeit von einer einwandfrei funktionierenden IT. Meist kennt es die möglichen Mechanismen der Risikobeeinflussung nicht. Es sieht oft nur den externen Angreifer und fühlt sich aufgrund dieser irreführenden Annahme in Sicherheit. Es handelt sich aber um eine Scheinsicherheit, der nur mit sensibilisierenden und aufklärenden Massnahmen begegnet werden kann. Das ist aber keine einfache Aufgabe, denn das Top-Management sieht Sicherheitsvorkehrungen als Kostenfaktoren. Das wird auch dadurch bestärkt, dass Sicherheit keinen sichtbaren Gewinn generiert. Sie ist erfolgreich, wenn Gefahren nicht eintreten. Dabei kann nicht einmal nachgewiesen werden, ob dies auf die Sicherheitsvorkehrungen zurückzuführen ist oder ob es schlicht dem Zufall zu verdanken ist.

Zu den wichtigsten Aufgaben zählt demnach, das Top-Management laufend und intensiv auf die konkreten Unternehmens-Risiken aufmerksam zu machen.

Ein Diplom für ICT-Security entsteht

Eine durch ICT-Berufsbildung Schweiz durchgeführte Marktanalyse zeigt:

- Das Thema ICT-Security hat eine hohe Sichtbarkeit und Relevanz und ist in der Schweiz trotzdem nur ein Nischenthema.
- Ein neues Berufsbild für ICT-Security gewinnt im Markt Beachtung, wenn neben fachlichen Kompetenzen auch die interpersonellen Kompetenzen im Vordergrund stehen.
- Es existieren bereits zahlreiche internationale und kantonale Ausbildungen und Zertifikate.

Jährlich kommen über 250 neue Diplom- und Zertifikatsabschlüsse dazu.

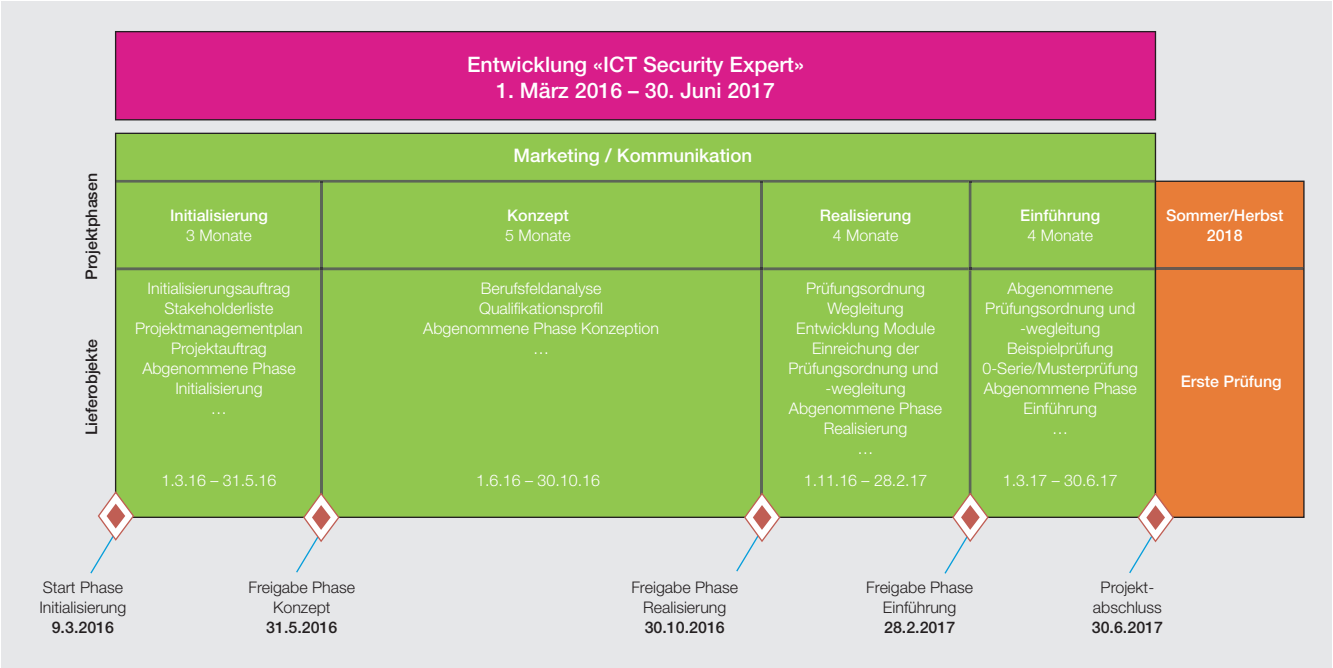

Tabelle 1 ICT-Security Experten werden erstmals 2018 ihr eidgenössisches Diplom erhalten.

- Durch die Heterogenität der verschiedenen Abschlüsse fehlt jedoch beim Thema ICT-Security aktuell ein einheitliches Profil.
- Neben technischen Kompetenzen sind Recht, Veränderungsmanagement und Kommunikation gefragt. Marktnähe, Praxisbezug und Anlehnung an nationale Rechtsnormen und internationale Standards sind die wichtigsten Faktoren bei der Gestaltung eines neuen Berufsbildes.
- Eine stärkere Gewichtung der ICT-Security durch klare Signale aus Wirtschaft und Politik gewährt dem Abschluss/Titel/Diplom mehr Bedeutung am Markt.

Bedeutend für die Entwicklung des neuen Diplomabschlusses ist, dass der Bundesrat 2012 die «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)» gutgeheissen hat. Mit dieser Strategie will der Bundesrat in Zusammenarbeit mit Behörden, Wirtschaft und den Betreibern kritischer Infrastrukturen die Cyber-Risiken minimieren, welchen sie täglich ausgesetzt sind.

Als wesentlich für die Reduktion von Cyber-Risiken bezeichnet die Strategie das Handeln in Eigenverantwortung und die nationale Zusammenarbeit zwischen der Wirtschaft und den Behörden sowie die Kooperation mit dem Ausland. Diesen Handlungsbedarf deckt die Strategie mit 16 Massnahmen ab, die bis 2017 umzusetzen sind.

In der Bildung und Forschung wurden drei Massnahmen definiert, welche allfällige Lücken bei der Kompetenzbildung schliessen sollen. Bezüglich des geplanten Diplomabschlusses ICT-Security Expert ist insbesondere die Massnahme 8 der Nationalen Strategie hervorzuheben: «Förderung der Nutzung der Bildungsangebote und Schliessen allfälliger Lücken».

Seitens des Informatiksteuerungsorgans des Bundes (ISB) und ICT-Berufsbildung in Kooperation mit Partnerorganisationen wie Microsoft Schweiz, die Schweizerische Post, Swisscom, UBS und der Verband Schweizerischer Elektrizitätsunternehmen (VSE), Abraxas Informatik, Alpiq, Armasuisse, Compass Security, die InselGruppe Bern, Information Security Society Switzerland (ISSS), KPMG, Mobiliar, PwC, Ruag, die Schweizerische Akademie der Technischen Wissenschaften, Switch, die Wirtschaftsinformatikschule Schweiz (WISS) und die Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) wurden daraufhin Arbeiten aufgenommen, die zum Ziel haben, einen Diplomabschluss zu schaffen, welcher die oben genannten Problemfelder bearbeiten wird. Dies bedeutet im Detail:

- Abdecken der zunehmenden Bedrohungen (inkl. soziale Faktoren), Wirtschaftsspionage & -kriminalität und Cyberangriffe
- Schlüsselrolle durch die hohe Akzeptanz von Wirtschaft, Politik und Verwaltung
- Wird den zunehmend schärferen schweizerischen und internationalen Regeln im Bereich Datenschutz und Datensicherheit gerecht
- Verlangt von dessen Inhabern ethische Handlungsgrundsätze
- Geht auf die zunehmende Mobilität und dezentrale Informationsbearbeitung sowie Outsourcing ein
- Baut auf bekannten Abschlüssen auf und integriert diese

Wie entsteht ein neues Berufsbild?

Die Prüfungsträgerschaft für das Berufsfeld der Informations- und Kommunikationstechnologie (ICT) ist die Organisation der Arbeitswelt, der Verein ICT-Berufsbildung Schweiz. Sie geht neue Wege gemeinsam mit der Wirtschaft und dem Bund bei der Entwicklung des neuen Berufsbildes zum ICT-Security Expert mit eidgenössischem Diplom. Für die Entwicklung des Qualifikationsprofils arbeiten im Rahmen des Projektes die oben genannten Partnerfirmen mit ICT-Berufsbildung zusammen. Es werden sämtliche relevanten Kompetenzen und Schwerpunkte des zukünftigen Berufsbildes gemeinsam erarbeitet. Das Kernstück dieser Arbeit bildet in erster Linie die Entwicklung des Berufsbildes und das Definieren des Qualifikationsprofils. In diesem werden die Kompetenzbereiche mit den jeweiligen Handlungskompetenzen definiert. Methodische Unterstützung bei der Entwicklung des Profils erhalten die Beteiligten durch das Eidgenössische Hochschulinstitut für Berufsbildung.

Es herrscht unter den beteiligten Partnerfirmen und Institutionen eine einheitliche Meinung über die Positionierung und Handlungskompetenzen des neuen Berufsbildes. Die zukünftigen ICT-Security Experten sind Ansprechpartner des obersten Managements, sie sollen befähigt werden, als «staatlich anerkannte Vertrauenspersonen» wichtige Funktionen im Zusammenhang mit der ICT-Sicherheit in Wirtschaft, Politik und Verwaltungen zu übernehmen.

Der erste Entwurf eines Qualifikationsprofils ergab die folgenden Kompetenzbereiche:

- Verankern der Sicherheitsstrategie im Unternehmen
- Managen von Sicherheitsrisiken
- Führen von Fachspezialisten und Managementsystemen
- Führen von Sicherheitsprogrammen

Résumé

Une nouvelle profession pour augmenter le niveau de la sécurité de l'information dans les entreprises suisses

Les cyberrisques ne concernent pas seulement les conseillers en sécurité informatique

En 2012, le Conseil fédéral a approuvé la « Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) ». À travers cette stratégie, il veut réduire les cyberrisques auxquels les autorités, les milieux économiques et les exploitants d'infrastructures critiques sont exposés quotidiennement, en étroite collaboration avec ces acteurs. L'association ICT-Formation professionnelle Suisse a ensuite lancé le projet de diplôme fédéral « ICT Security Expert » en collaboration avec l'Unité de pilotage informatique de la Confédération (UPIC). Des représentants renommés de l'économie ont également participé au développement de ce nouveau profil professionnel, parmi lesquels Microsoft Suisse, la Poste Suisse, Swisscom, UBS et l'Association des entreprises électriques suisses (AES). Les futurs « ICT Security Experts » occuperont, en tant que « personnes de confiance reconnues par l'État », des fonctions importantes en lien avec la sécurité informatique dans le monde économique et politique, ainsi qu'au sein des administrations. L'une des principales tâches consiste ainsi à rendre les hauts dirigeants attentifs aux risques d'entreprise concrets, en continu et intensivement. Mais leur rôle ne se réduit pas à cela: aujourd'hui, en plus des personnes chargées de la sécurité informatique, d'autres secteurs de l'entreprise doivent également s'intéresser au thème de la sécurité, comme par exemple les départements de développement, et ce, en raison de l'Internet traditionnel, mais aussi de l'Internet des objets (ou Internet of Things, IoT), de l'approche BYOD (Bring your own device/apportez vos appareils personnels), du SaaS (software as a service/logiciel en tant que service), du phishing (hameçonnage) ou encore du télétravail.

Md

- Pflege eines fachlichen und vertrauenswürdigen Netzwerkes (Beziehungen)
- Managen und beraten von unterschiedlichen Stakeholdern (z.B. Compliance)
- Schaffen von Awareness (stufengerecht)
- Unterstützen beim Bewältigen von Ereignissen

Die besondere Herausforderung bei der Definition der Kompetenzen ist, dass zwar die heutigen Sicherheitsaspekte und deren Massnahmen bekannt sind, dabei die Gefahren und Bedrohungen für die Zukunft im Auge zu behalten.

Die Anforderungen und Profile werden weiterentwickelt und dem sich ändernden Umfeld angepasst.

Dieses Qualifikationsprofil muss anschliessend beim Bund (Staatssekretariat für Bildung, Forschung und Innovation) das eidgenössische Anerkennungsverfahren durchlaufen.

Geplant ist, dass die Entwicklung und Umsetzung dieses neuen Diploms auf die Anforderungen der Industrie, des Bundes, der Kantone und weiterer öffentlicher Organisationen zugeschnitten wird. Erste Prüfungen sind im Jahr 2018 geplant.

Grundsätzlich für alle offen

Der Weg zur höheren Fachprüfung (eidg. Diplom) steht allen offen, welche die reglementarischen Zulassungsbedingungen erfüllen.

Die Hauptzielgruppe werden erfahrene Informatiker/-innen aller Bildungsstufen sein, egal ob mit Universitäts- oder Fachhochschulabschluss, dem Abschluss einer höheren Fachschule oder einem eidgenössischen Fachausweis.

Die Zulassungsbedingungen werden im Rahmen des Projekts ausgearbeitet. Es wird eine Mischung aus Berufserfahrung und früheren Abschlüssen sein.

Link

www.ict-berufsbildung.ch

Autoren

Bruno Schnarwiler, Managing Consultant und Member of the Executive Board, bearbeitet bei der Swiss Infosec AG Mandate in den Bereichen Risiko- und Sicherheitsmanagement, Informationssicherheit, Business Continuity- und Krisenmanagement und Integrale Sicherheit. Er ist eidg. dipl. Wirtschaftsinformatiker, dipl. Projektmanager, CISA und ISO 27001 Lead Auditor. Er verfügt über mehr als 30 Jahre Erfahrung in den Bereichen Wirtschaftsinformatik, Integrale Sicherheit, Risikomanagement, Business Continuity Management und Krisenmanagement.

Swiss Infosec AG, 3011 Bern
bruno.schnarwiler@infosec.ch

Hansjörg Hofpeter, Leiter höhere Berufsbildung, ist seit 2011 unter anderem als Prüfungsleiter der eidg. Berufs- und höheren Fachprüfungen beim Trägerverband ICT-Berufsbildung Schweiz tätig. Er ist zuständig für die Qualität und Weiterentwicklung der eidg. Fachausweise und eidg. Diplome. Zuvor war Hofpeter während über 30 Jahren als Lehrer der Sekundarstufe 2 an einer Privatschule tätig. Er hat dort diverse Ausbildungsgänge mitgestaltet und aktiv durchgeführt. Der Verband ICT-Berufsbildung Schweiz wird getragen vom Dachverband ICTswitzerland sowie den kantonalen und regionalen ICT-Lehrbetriebsorganisationen.

ICT-Berufsbildung Schweiz, 3011 Bern
hansjoerg.hofpeter@ict-berufsbildung.ch