Neue Bildungsangebote

Security-Asse gesucht

Security-Fachkräfte sind in der Schweizer ICT-Branche momentan heiss begehrt. Die Nachfrage ist jedoch grösser als das Angebot. Wie werden also die Sicherheits-Experten von morgen ausgebildet?

→ VON LUCA PERLER

Die Revision der Datenschutzgesetze in der Schweiz und Europa sowie die folgenreichen Cyber-Attacken im Sommer des vergangenen Jahres haben bei vielen Schweizer Unternehmen die Sicherheit und Compliance der Informatiksysteme in den Fokus gerückt. Aus Sicht der IT-Entscheider ist das Gewährleisten der IT-Sicherheit und Compliance in diesem Jahr auch die wichtigste Aufgabe der IT-Abteilung, wie die Auswertungen der Swiss-IT-Studie von Computerworld zeigen (vgl. Grafik rechts). Im Vergleich zum Vorjahr ist der Anteil jener, die diese Aufgabe als wichtig oder sehr wichtig bezeichnen, um etwas mehr als vier Prozentpunkte gestiegen. Bei 69 Prozent der Befragten gehören Projekte im Bereich Informatik-Sicherheit zudem zu den fünf wichtigsten im laufenden Jahr (vgl. Grafik Seite 20). Im Vergleich zum Vorjahr entspricht dies einem Zuwachs von etwas mehr als zehn Prozent.

HOHER BEDARF AN SPEZIALISTEN

Wer seine Anstrengungen in der IT-Security erhöhen will, der braucht dafür die nötigen Fachkräfte. Doch in der Informatik Spezialisten zu finden, stellt Schweizer Unternehmen bekanntlich seit Längerem vor Probleme. Dass IT-Fachkräfte generell Mangelware sind – besonders auch IT-Sicherheitsexperten –, das bestätigt Chaib Whiteford, Senior Manager beim Personalberater Robert Half, in Zürich. «Der Bedarf ist ungebremst sehr hoch», sagt er. Speziell Software-Sicherheitsspezialisten und Experten für die EU-Datenschutz-Grundverordnung würden händeringend gesucht. Aufgrund der neuen Datenschutz-Richtlinien der EU bestehe bei vielen Unternehmen akuter Handlungsbedarf. Dazu komme, dass die digitale Transformation die Unternehmen vor neue Sicherheitsanforderungen stelle. «IT-Sicherheit und Datenschutz sind elementare Themen, die bei Schweizer Unternehmen momentan ganz oben auf der Prioritätenliste stehen.»

Wenn das ausgebildete Personal fehlt, dann ist der Bereich Weiterbildung gefragt. Welche Qualifikationen und Fähigkeiten müssen Security-Spezialisten eigentlich mitbringen, damit sie für den Markt interessant sind? Gemäss Whiteford sollten sie grundsätzlich dazu bereit sein, ständig nach neuen Lösungen zu suchen, um die Sicherheit im Unternehmen zu verbessern. Ein gutes Verständnis des Kerngeschäfts des Unternehmens sowie agiles Denken und Agieren seien dabei besonders wichtig. Auch ein gewisses Mass an Erfahrung sei gefragt. «Bei den meisten Jobs im IT-Security-Bereich werden einige Jahre Berufserfahrung vorausgesetzt», weiss Whiteford. Jüngere Menschen würden deshalb eher operative Positionen übernehmen.

GUTE AUSSICHTEN MIT ZERTIFIKATEN

Aus Sicht des Personalberaters von Robert Half sind Zertifizierungen im Bereich IT-Security ideal. Je nach Stelle und Funktion sind jedoch unterschiedliche Qualifikationen gewünscht. Bei den Penetration-Testern hätten Bewerber mit CEH- (Certified Ethical Hacker) oder ECSA-Zertifikaten (EC-Council Certified Security Analyst) sowie einem Examen als EC-Council Licensed Penetration Tester (Master) die besten Jobchancen. Bei Cloud-Security-Experten seien jene mit einer CCSP-Qualifikation (Certified Cloud Security Professional) besonders gut gerüstet. Beliebt seien auch die Zertifizierungen CISSP (Certified Information Systems Security Professional) oder ISO 27001.

Mit Fähigkeiten im IT-Security-Bereich können gemäss Whiteford auch Experten aus anderen Gebieten punkten. «Netzwerkadministratoren mit entsprechenden Weiterbildungen und Zertifikaten stehen attraktive Jobs in der IT-Sicherheit offen», sagt der Personalberater. Bei Leitungspositionen wie etwa dem Chief Security Officer seien neben den fachlichen Qualifikationen zusätzlich auch noch Führungskompetenzen gefragt.

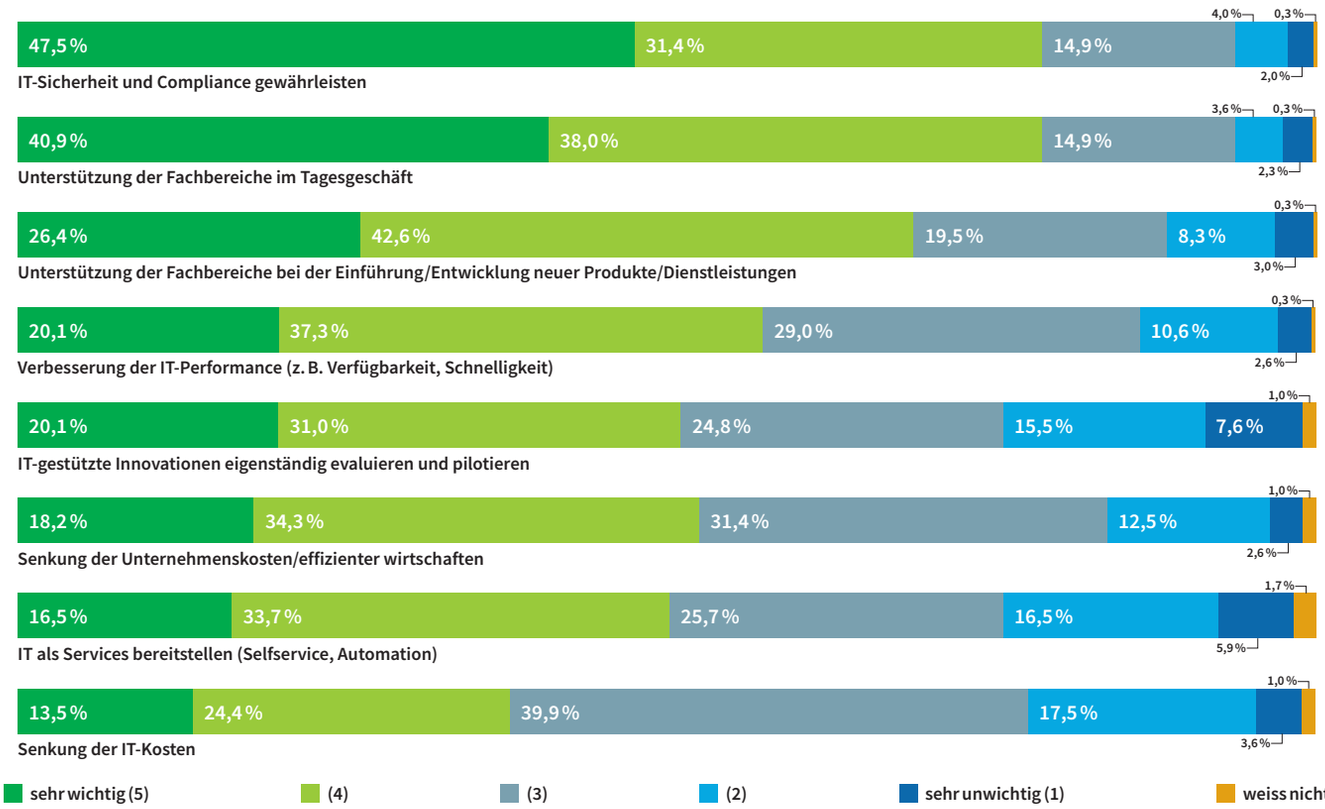
FACHHOCHSCHULEN RÜSTEN AUF

Dass man sich nicht nur mit verschiedenen Zertifizierungen und Weiterbildungen auf den Bereich IT-Security spezialisieren kann, beweisen die Fachhochschulen. Mittlerweile sind auch sie mit Studiengängen und Weiterbildungskursen auf diesem Gebiet in die Bresche gesprungen. Wie beispielsweise die Berner Fachhochschule oder die Fachhochschule Nordwestschweiz, hat auch die Hochschule Luzern (HSLU) seit Längerem Master-Lehrgänge und CAS-Kurse im Angebot. Im kommenden Herbst lanciert das Informatik-Departement der HSLU zusätzlich einen neuen Bachelorstudiengang mit dem Namen «Information & Cyber Security» – der Erste seiner Art in der Schweiz.

Wie Bernhard Hämmerli, der Leiter des neu geschaffenen Studiengangs, erklärt, reagierte das Informatik-Departement der HSLU damit auf ein klares Marktbedürfnis: «Wer im Netz die ersten drei Stellenportale nach Vakanzen für Cyber-Security-Professionals abgrast, der findet bestimmt rund 700 offene Stellen», sagt er. Seitens der Wirtschaft sei der Bachelorstudiengang deshalb sehr willkommen. «Wir erhalten dazu einzig den Kommentar, warum nicht heute schon Absolventinnen und Absolventen da sind.» Denn gross angelegte Cyber-Angriffe wie «NotPetya» im vergangenen Jahr hätten aufgezeigt, wie teuer dies für betroffene Unternehmen heute werden könne – der Verschlüsselungstrojaner verursachte bei einzelnen Firmen Verluste von 300 bis 400 Millionen US-Dollar.

Die wichtigsten Aufgaben der IT-Abteilung aus Sicht der CIOs

Viele IT-Entscheider bewerten das Gewährleisten von IT-Sicherheit und Compliance aktuell als die wichtigste Aufgabe der Informatikabteilung. Verschärfte Datenschutzrichtlinien und die grossen Cyber-Attacken aus dem letzten Jahr dürften ihren Beitrag dazu geleistet haben.



Computerworld Swiss IT/2018

Quelle: Swiss IT Computerworld/IDC 2018; CIOs, n = 303

«Das bezahlt man nicht mehr einfach so aus der Portokasse – das schlägt auf die Bilanz und zwar massiv», erläutert Hämmerli.

BREITE UND FLEXIBLE AUSBILDUNG

Mit dem Bachelor wolle man jungen Menschen Eintrittschancen in den Job sowie die Mitarbeit in einer technischen Security-Abteilung ermöglichen. «Wie für Fachhochschulen üblich, ist auch hier das Ziel, dass unsere Absolventen vom ersten Tag an produktiv arbeiten können.» Wie Hämmerli erklärt, können sich Studierende im Verlauf des Studiums mit der Wahl eines Hauptfachs entweder auf die Technologie oder das Management spezialisieren. Studierende auf der technologischen Seite eignen sich unter anderem Wissen zur Sicherheit von Betriebssystemen und Applikationen, zur Network- sowie Cyber-Defence oder auch zu kritischen Infrastrukturen an. Das Management konzentriert sich dagegen etwa auf die Security-Awareness, das Durchführen von Audits oder das Erstellen von Security-Richtlinien. «So wollen wir bei unseren Leuten eine gesamtheitliche, breite und solide Grundlage schaffen, damit sie sich auf einer höheren Stufe in der Wirtschaft in einem der zirka 50 hauptsächlichen Security-Berufsrichtungen einbringen können.»

Wer sich für den Studiengang einschreiben will, muss entweder eine Berufslehre mit technischer oder wirtschaftlicher Berufsmatur oder eine Matura mit einjährigem Praktikum mitbringen. Generell können Studierende den Bachelor in Information & Cyber Security in drei Zeitmodellen – Vollzeit, berufsbegleitend oder Teilzeit – absolvieren und diese auch während des Studiums wechseln.

AUSBILDUNG UND UMSCHULUNG

Für den Start im Herbst konnte Hämmerli bereits eine erste Laborklasse von 25 Personen füllen. Nun holte er bei der Departementsleitung bereits die Bewilligung für eine Doppelführung ein. Auf diese Weise kann die Hochschule weitere Studierende aufnehmen. Laut dem Studiengangleiter finden sich unter den bereits angemeldeten Personen einerseits junge, andererseits aber auch erfahrene Informatiker, die in einer späteren Phase ihrer Karriere noch eine Umschulung in Angriff nehmen. Hinzu kämen schliesslich noch die «Digitalisierungsopfer», die in administrativen Bereichen gearbeitet haben und deren Stellen ausgelagert wurden oder der Digitalisierung zum Opfer fielen. «Wir sehen, dass der Druck durch die Digitalisierung gerade auf KV-Stellen spürbar grösser wird. Eine Umschulung mit dem neu geschaffenen Bachelorstudiengang kann ihnen dabei helfen, einfacher eine Stelle zu finden.»

VIELE OFFENE TÜREN

Wie Studiengangleiter Hämmerli erklärt, stehen den Absolventen nach der Ausbildung zahlreiche Türen offen – neben vielen anderen Optionen seien etwa Tätigkeiten denkbar wie die Arbeit in einem Security Operation Center, das Durchführen von Penetration-Tests oder das Betreuen von Security-Awareness-Kampagnen. Dass die Nachfrage der Wirtschaft nach gut ausgebildeten Security-Fachkräften auch in Zukunft nicht abflachen wird, da sind sich Hämmerli und Whiteford einig. Hämmerli sagt dazu: «Zumindest in den nächsten zehn Jahren wird der Bereich IT-Sicherheit noch enorm stark wachsen, dabei werden sich zahlreiche Karriere- und Weiterbildungsmöglichkeiten auftun. Wer weiter in die Zukunft prognostiziert, ist aus meiner Sicht unseriös.» ←