Aus dem Hörsaal in den Arbeitsmarkt – Cybersecurity-Ausbildungen in der Schweiz

Viele Schweizer Hochschulen und Universitäten bieten inzwischen Aus- und Weiterbildungen im Bereich Cybersecurity an. Doch wer profitiert von solchen Angeboten und welche Skills erfordert der Markt? Der auf Cybersecurity spezialisierte Personalberater Peter Kosel gibt einen Einblick in den Schweizer Cybersecurity-Arbeitsmarkt. Autor: Maximilian Schenner

Cybersicherheit kann man studieren – seit einigen Jahren auch in der Schweiz. Die Hochschule Luzern (HSLU) rief 2018 als erste Schweizer Hochschule den Bachelor-Studiengang «Information & Cyber Security» ins Leben. Der Studiengang soll das notwendige Fachwissen vermitteln, «um Unternehmen und Verwaltungen vor Hackerangriffen zu schützen und mit einer sicheren IT-Infrastruktur auszustatten», wie die HSLU schreibt. Die Module widmen sich unter anderem den Bereichen Risk Management, Kryptologie und Sicherheit in der Entwicklung. Aber auch Themen wie Datenschutz und Ethik in der Cybersicherheit sind Teil des vierjährigen Studiums.

Die Fernfachhochschule Schweiz (FFHS) bietet ab August 2023 ebenfalls einen Bachelor-Studiengang «Cyber Security» an. Das Studium enthält laut der FFHS eine Vielzahl an spezifischen Modulen zum Thema Cybersicherheit. Dazu zählen etwa Kryptologie, Internet-, Cloud- und Systemsicherheit sowie reaktive Informationssicherheit, IT-Forensik, Secure Coding und Themen zu Trust, Datenschutz und IT-Governance. «Der Praxisbezug ist sehr zentral. So werden die Studierenden die Möglichkeit haben, ihr Können in verschiedenen Hackathons unter Beweis zu stellen», erklärte Oliver Ittig, Leiter des neuen Cybersecurity-Studiengangs, bei dessen Einführung.

An der ETH Zürich gibt es ausserdem einen Master in Cybersecurity zu erwerben. Das entsprechende Studium dauert zwei Jahre – Voraussetzung ist ein abgeschlossenes Bachelorstudium in Informatik.

Es geht auch ohne Studium

Es muss aber nicht gleich ein ganzes Studium sein, wie Cybersecurity-Personalberater Peter Kosel erklärt: «Viele Schweizer Hochschulen und Universitäten bieten Kurse und Programme im Bereich Cybersecurity an, die sich an verschiedene Zielgruppen richten.» Darunter etwa an Risk Manager, Informatiker und Mitarbeitende des öffentlichen Dienstes, aber auch Einzelpersonen, die sich für Cybersecurity interessieren. Kosel ist Gründer von Cyberunity – eine Cyber Security Talent Agency, die einschlägige Fachkräfte an potenzielle Arbeitgeber in Festanstellung vermittelt.

«Besonders hervorzuheben ist die HSLU, die sich mit MAS- und CAS-Angeboten stark auf das Thema Cybersecurity eingestellt hat», sagt Kosel. Auch die Berner Fachhochschule, die ZHAW und die Ostschweizer Fachhochschule bieten derartige Weiterbildungen an.

Private Weiterbildungsträger wie etwa das Swiss Cyber Institute haben ebenfalls Weiterbildungsmöglichkeiten im Bereich Cybersecurity im Angebot. Und auch einige IT-Unternehmen bieten laut Kosel intern oder extern Weiterbildungsmöglichkeiten dazu an, um ihren Mitarbeitenden die Möglichkeit zu geben, ihre Fähigkeiten zu verbessern und sich auf spezielle Bereiche zu spezialisieren. «Es ist wichtig, zu beachten, dass die Qualität und der Umfang der Kurse und Programme, die von verschiedenen Weiterbildungsträgern angeboten werden, variieren können», betont Kosel.

Wer vom Bildungsangebot profitiert

Doch wer profitiert von Bildungsangeboten wie diesen? Laut Kosel bietet sich eine Cybersecurity-Ausbildung vor allem für Arbeitsbereiche an, in denen die Sicherheit des Unternehmens, dessen Daten und Systeme zum zentralen Aufgabengebiet zählen. Dazu zählen laut ihm das Risikomanagement, die Informations- und IT-Sicherheit, die Anwendungsentwicklung, die Netzwerkadministration/Netzwerksicherheit sowie der Datenschutz.

Ein spezifisches Studium zur Cybersicherheit lohnt sich laut Kosel für Personen, die ganz gezielt eine Karriere im Bereich Informationssicherheit anstreben. «Natürlich ist auch für jeden, der gerne sein Wissen erweitern und intensiver in das Thema einsteigen möchte, ein vertieftes Studium wertvoll», sagt Kosel. «Wir können nicht genug Menschen in unseren Unternehmen haben, die dieses zunehmend gefragte Wissen einbringen und sich dafür engagieren, dass eine lebendige Sicherheitskultur zur Normalität wird.»

Das Aus- und Weiterbildungsangebot im Cybersecurity-Bereich hält Kosel für derzeit ausreichend. Es mangle eher an genügend Bewerberinnen und Bewerbern, um die Nachfrage nach Sicherheitsspezialisten abzudecken.

Jobchancen: Vom Techie bis zum Security Manager

Die Jobaussichten in der Cybersecurity sind hierzulande vielfältig, wie Kosel erklärt: «Wir reden hier über die gesamte Bandbreite: vom Network-Security Engineer über den Cloud-Security-

Peter Kosel, Gründer von Cyberunity.

Architekten oder Crypto Engineer bis zum Data Protection und Chief Information Security Officer.» Die Kompetenzen, die der Jobmarkt erfordert, seien ebenso vielfältig: «Vom Techie bis zum Security Manager ist alles dabei», sagt Kosel. Das umfasse etwa die Bereiche Application Security, Network Security, Cloud Security sowie die Information Security als ganzheitliche, umfassende Sicht auf das Thema Informationssicherheit.

Je nach Bereich gebe es dann wiederum sehr vielfältige und spezifische Kompetenzen. Wer etwa in der Application Security arbeiten will, muss laut Kosel Software-Engineering-Erfahrungen in der Kombination mit Security mitbringen. Das Stichwort laute hier «Security by Design» – also das sichere Entwickeln von Beginn an. Das Segment Network Security erfordere hingegen Kenntnisse über die Netzwerkadministration, kombiniert mit Netzwerksicherheit.

Fingerspitzengefühl gefragt

Abgesehen von den technologischen Erfahrungen sind Kosel zufolge vermehrt interpersonelle Skills respektive emotionale Intelligenz gefragt. Dies gelte besonders für all jene, die eine Position als Security Manager oder Information Security beziehungsweise Chief Information Security Officer (CISO) anstreben. Hierbei gehe es etwa um Erfahrungen, die sich um das Etablieren eines umfassenden Informations- und Risikomanagements drehen: «Das Thema Security ist in Unternehmen noch keine Selbstverständlichkeit und muss auf eine positive Art und Weise nach und nach in den Köpfen der Menschen etabliert werden», erklärt Kosel. «Da hilft neben logischen Argumenten vor allem Einfühlungsvermögen und Fingerspitzengefühl, verbunden mit smarten Ideen, die die Menschen motivieren, das Thema Sicherheit aktiv in den Arbeitsalltag einzubinden.»

Standards für alle

Auch die Unternehmensleitung kommt nicht ohne grundlegende Cybersecurity-Kenntnisse aus, wie Kosel sagt. CEOs und andere Führungskräfte sollten etwa die verschiedenen Bedrohungsarten und damit verbundenen Risiken kennen und verstehen. Dazu zählen unter anderem Hackerangriffe, Datendiebstahl und Malware. Des Weiteren liege es an der Firmenleitung, Sicherheitsrichtlinien für das gesamte Unternehmen zu etablieren und Sorge zu tragen, dass diese auch eingehalten werden. Die Entwicklung eines lebendigen und positiven Sicherheitsbewusstseins falle ebenfalls in das Aufgabenfeld der Unternehmensspitzen.

Cybersecurity-Kompetenzen seien für Unternehmen jeder Grösse relevant, wenn man davon ausgehe, dass alle Firmen der gleichen Bedrohungslage ausgesetzt seien, sagt Kosel. Gerade KMUs würden sich aber wohl oftmals zu Unrecht in Sicherheit wähnen: «Einige Unternehmer neigen dazu, zu denken, dass sie nicht auf der ‹Shoppingliste› der Hacker stünden, da sie sich als zu klein und damit nicht relevant erachten.» Dieser Trugschluss habe schon so manches KMU viel Geld respektive die Existenz gekostet.

Alle anderen Personen im Unternehmen müssten ebenfalls gewisse Sicherheitsstandards erfüllen, meint Kosel – die hinlänglich bekannten Basics, auf die immer wieder hingewiesen wird. «Sie sollten mittlerweile Standard sein, doch auch hier gibt es immer wieder Verbesserungspotenzial», sagt der Experte. «Es steht und fällt mit der erwähnten Unternehmensleitung und deren Sicherheitsbewusstsein und -verständnis.» Als «Klassiker» nennt Kosel etwa das Verwenden sicherer und einzigartiger Passwörter sowie deren regelmässige Aktualisierung. Auch für die Aktualisierung von Antivirus-Software seien die Mitarbeitenden verantwortlich. Als weiteren wichtigen Punkt nennt er das Klicken – oder besser gesagt das «Nicht-Klicken» – auf verdächtige Links und Anhänge, ein beliebter Weg für Cyberkriminelle, um Malware auf Firmensystemen zu installieren. Gerade hier brauche es Aufklärungsarbeit, sagt Kosel. «Von heute auf morgen bewegt sich da nur sehr wenig – Geduld, viel Verständnis für Menschen und smarte Begleitung sind angesagt.»

Den Artikel finden Sie auch online
www.swisscybersecurity.net