Talente gesucht – Liaison von Grundlagen mit Aktualität

Was ist professionelles IT-(Governance)-Management? Wie und wo kann man es lernen? Sind Schweizer Unternehmen für die möglichen, künftigen Aufgaben rund um das IT-Management gerüstet? Der Kampf um die raren Talente hat längst begonnen!

DIE AUTORINNEN

Petra Maria Asprion
Leiterin Kompetenzschwerpunkt Cyber Security / Resilience Fachhochschule Nordwestschweiz (FHNW), Hochschule für Wirtschaft

Dörte Resch
Dozentin für Human Resource Management und Organizational Behaviour Fachhochschule Nordwestschweiz (FHNW), Hochschule für Wirtschaft

Im Jahr erhalten wir pro Wochentag teils mehrere informelle Anfragen zur «Talentsuche». Häufig geht es darum, ob wir nicht jemanden wüssten, der oder die eine neue Herausforderung beziehungsweise einen Job im Umfeld von «IT-Governance» oder «IT-Audit» sucht. Dieses komplexe und vielseitige Tätigkeitsfeld umschreiben wir vereinfacht mit «Governance, Risiko, Compliance», kurz GRC-Management; neuerdings hat sich noch «Cybersecurity», als spezialisiertes Fokusfeld dazugesellt.

Die gesuchten Talente sollten aktuelles Wissen rund um GRC mitbringen sowie talentiert und motiviert sein. Sie sollten GRC im Kontext von neuen und bisherigen Geschäftsmodellen etablieren und überwachen, regulatorische Anforderungen in interne Kontrollaktivitäten transformieren, wissen, was es mit neuen Technologien auf sich hat usw. Viele Unternehmen fahnden aktuell nach Personal mit fundierten Kenntnissen zur Umsetzung der neuen EU-Datenschutz-Grundverordnung (EU-DSGVO), die im Mai 2018 in Kraft treten wird. Es werden Studierende und Absolventinnen gesucht, aber auch erfahrene Experten, die kurzfristig Führungsaufgaben und Verantwortung übernehmen können. Insbesondere innovations- und wissensbasierte Unternehmen in der Schweiz, aber auch in den Nachbarländern, suchen verstärkt und intensiv nach Ressourcen, die eine Informatik-/Wirtschaftsinformatik-Ausbildung oder Vergleichbares absolviert haben.

Solche Anfragen nahmen in den letzten Monaten kontinuierlich zu und indizieren eine steigende Nachfrage nach akademisch ausgebildetem Personal rund um GRC und Cybersecurity/-resilienz. Gestützt wird dieser Eindruck auch durch aktuelle Forschungen, wie etwa die Studie «ICT-Fachkräftesituation, Bedarfsprognose 2024» des Berufsverbands ICT-Berufsbildung Schweiz im Jahr 2016 oder die Studie zur «Attraktivität von ICT-Berufen», durchgeführt von der Fachhochschule Nordwestschweiz 2017. Letztere untersuchte, wie der geringe Anteil an Frauen im Berufsfeld (aktuell nur bei zirka 15 Prozent) gesteigert werden könnte, um den Fachkräftemangel zu bekämpfen.

Inspiring the New Generation …

Was inspiriert Teilnehmende unserer Aus- und Weiterbildungen, Inhalte rund um GRC oder Cybersecurity/-resilienz kennenzulernen und zu vertiefen? Wie können wir sie nachhaltig motivieren, diese Themen in den Mittelpunkt ihrer künftigen beruflichen Tätigkeit zu stellen?

Das Interesse an ICT und insbesondere an GRC – als Managementaufgabe – muss immer wieder geweckt werden. Doch wie? Ja, es stimmt, in erster Linie lehren, diskutieren und forschen wir an Grundlagen, wie beispielsweise am ethischen Umgang mit Technik, an der Adaption von Metamodellen, an den Prinzipien der Auditierung oder etwa an den Anforderungen an Datensicherheit und kritische Infrastrukturen. Diese sind nicht immer nur spannend und oft eher grundlegender Natur. Jedoch bilden Grundlagen den Bezugsrahmen für ein professionelles Wissen – und dies ermöglicht uns deren Verknüpfung mit neuen Innovationen wie etwa Bitcoin oder mit (tages) aktuellen Ereignissen.

Wannacry – ein Weckruf

Es ist schon fast wieder in Vergessenheit geraten, dass «Wannacry» im Mai dieses Jahres, an einem Samstag, rund 300 000 Computer in 150 Ländern befiel. Zu den Opfern der Cyberattacke zählte unter anderem die Deutsche Bahn, bei der Anzeigetafeln und Fahrkartenautomaten ausfielen. In Grossbritannien wurden Krankenhäuser attackiert, sodass Patienten abgewiesen und Routineeingriffe abgesagt werden mussten. Die betroffenen Unternehmen und auch Privatpersonen waren alle mit verschlüsselten Daten konfrontiert, flankiert mit Lösegeldforderungen, zahlbar in der Kryptowährung Bitcoin.

Wir diskutierten im Kollegenkreis, in verschiedensten Settings mit Studierenden und mit vielen Personen, die unsere Hochschule besuchten. In den folgenden Tagen und Wochen erörterten wir Wannacry: Die Themen drehten sich um kriminelle Hacker, Trojaner, insbesondere um Lösegeldtrojaner und um Kryptowährungen wie Bitcoin. Wir fragten, wer (von uns) solche Bitcoins besitzt und wieso eigentlich. Studierende überlegten Szenarien und präventive Massnahmen, die (vielleicht) nicht einen Angriff, aber eine Infizierung verhindert hätten. Wir spielten Aktivitäten zum Krisenmanagement durch, versuchten den jeweiligen Schaden zu berechnen und spekulierten, wie wohl die Schadensbehebung in den betroffenen Unter-

Bild: gorodenkoff / iStock.com

nehmen aussehen könnte und entwickelten (fiktive) Empfehlungen. Wir beschäftigten uns mit «Forensic Readiness» und identifizierten dieses Themenfeld als eines unserer künftigen Forschungsfelder. Nicht zuletzt suchten wir Schuldige – und entdeckten diese schnell, nämlich die Verantwortlichen für IT-Sicherheit in den betroffenen Unternehmen. Hingegen waren die betroffenen Privatpersonen «selbst schuld», da sie die empfohlenen Updates nicht eingespielt hatten. Wir diskutierten intensiv über die potenziellen Täter – als solche kamen Personen mit guten bis sehr guten Informatikkenntnissen infrage – also wir!

Wer sind «wir»?

Die Disziplin und das (künftige) Berufsfeld unserer Studierenden der Wirtschaftsinformatik und aller, die eine Weiterbildung bei uns besuchen, zeichnet sich durch eine kontinuierliche Verbreiterung der Themenfelder aus – und das in einer atemberaubenden Geschwindigkeit. Vor einigen Jahren lehrten und erforschten wir den Lebenszyklus von ERP-Systemen, was heute weitgehend als Commodity angesehen wird. Manch einer wird sich noch an Nicholas Carr erinnern, der 2003 prognostizierte, dass IT innerhalb von zehn Jahren unsichtbar, eben Commodity sein und in die Bedeutungslosigkeit versinken werde. Ganz so ist es nun doch nicht gekommen. Heutzutage stehen IT-getriebene Innovationen und damit zusammenhängende ökonomische und technische Aspekte im Vordergrund. Eine solche integrierte Betrachtung ist Kern und Alleinstellungsmerkmal der Wirtschaftsinformatik! Was sich wie ein roter Faden durch die Disziplin und das Berufsfeld zieht, ist die kontinuierliche Weiterentwicklung der Governance- und Managementprozesse rund um die Organisation und den Betrieb der IT.

Und Wannacry ist nichts anderes als eine plumpe Warnung, eine Erinnerung, die Sicherheit der ICT, heutzutage eben erweitert um Cybersicherheit, ernst zu nehmen und aktiv in die Unternehmensprozesse zu integrieren. Was Unternehmen daraus lernen (können) ist, dass sie (noch) schneller, noch kreativer sein müssen – und hierfür benötigen sie geeignetes Personal. Wie soll das gehen? Schneller und kreativer sein! Professionelles Personal ist rar und wird künftig noch rarer werden. Die bereits erwähnte Studie des Berufsverbands prognostiziert bis ins Jahr 2024 einen Mangel an 25 000 ICT-Fachkräften. Diese braucht es praktisch in allen Wirtschaftszweigen. Insbesondere werden ICT-Führungskräfte nachgefragt und diese müssen zumindest eine Grundausbildung, ein solides Grundverständnis von GRC und deren Einflussfaktoren haben.

Liaison von Grundlagen mit Aktualität

Wie können wir nun diese eh schon raren ICT-Fachkräfte für die Themenfelder rund um GRC gewinnen? Wir arbeiten daran, indem wir für künftige, aber auch erfahrene ICT-Fachkräfte attraktive Angebote zur Aus- und Weiterbildung gestalten. Nicht nur, aber auch im Themenfeld GRC und natürlich auch zu Cybersecurity und -resilienz. Wir flankieren unsere Angebote mit Forschung, etwa zu den Bedürfnissen der künftigen Generation und wie das Berufsfeld zugänglicher, ja attraktiver gemacht werden kann («Attraktivität von ICT-Berufen», FHNW, 2017). Aktuell ist eine weitere Studie in Vorbereitung, deren Ergebnisse Unternehmen helfen sollen, die begehrten Mitarbeitenden zu gewinnen und langfristig zu binden.

Die Liaison von Grundlagen mit Aktualität ist uns ein Anliegen: Grundlagen sind das Leitmotiv einer akademisch geprägten Ausbildung, darauf wollen und können wir nicht verzichten. Auf diesen bauen wir auf, sie bilden den Bezugsrahmen für theoretisch gestützte Anwendungen und Erweiterungen in unserer Disziplin. Nicht zuletzt sind sie aber auch Anknüpfungspunkte für das «Neue», das «Unbekannte», das «Kreative», das «Innovative», die «Spielwiesen». Letztens diskutierten wir im Rahmen einer Vorlesung das Phänomen der Cyberbedrohungen und deren Auswirkungen auf Unternehmen. Wir trugen Informationen zu Wannacry und dem nachfolgenden Trojaner «EternalRock» zusammengetragen und kauften fiktiv Bitcoins. Mit Argusaugen werden wir von nun an deren Entwicklung verfolgen und alles, was damit technisch zusammenhängt, insbesondere wie sich unsere Bitcoins entwickeln. Was für ein spannendes Themenfeld, in dem wir und hoffentlich (noch) viele andere arbeiten dürfen!