Zeitschrift für Datenrecht und Informationssicherheit

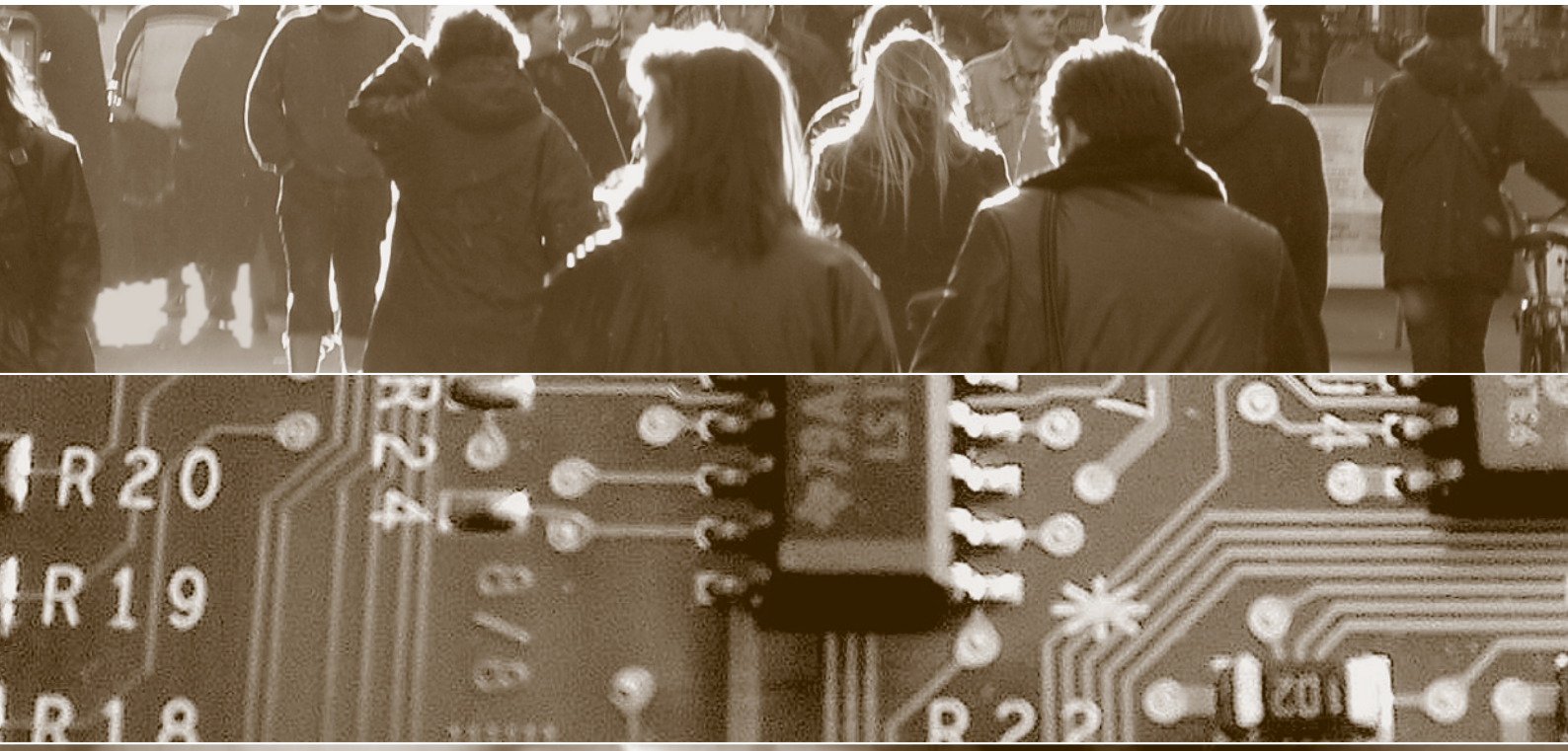
digma

www.digma.info 18. Jahrgang, Heft 2, Juni 2018

Schwerpunkt:

Digitale Demokratie

fokus: E-Voting, ein Mehrwert für die Demokratie
fokus: E-Voting CH: Das Ende der Demokratie?
fokus: Estland im falschen Blickwinkel



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth
David Vasella

Schulthess §

inhalt

fokus

Schwerpunkt:
Digitale Demokratie

E-Voting, ein Mehrwert für die Demokratie

E-Voting aus Sicht einer Befürworterin: Es ermögliche die zeit- und ortsunabhängige Stimmabgabe, erfülle strengste Anforderungen, ermögliche den Stimmberechtigten, durch mathematische Verfahren die eigene Stimmabgabe nachzuvollziehen, und gewährleiste den kantonalen Wahlbehörden, jegliche Veränderung im Abstimmungsverfahren erkennen und gegebenenfalls reagieren zu können.

E-Voting CH: Das Ende der Demokratie?

E-Voting aus Sicht eines Skeptikers: Ist es realistisch, darauf zu vertrauen, dass die Bürger bei E-Voting nicht einfach blind der Applikation folgen, sondern den Code überprüfen? Zweifel an der Korrektheit der Abstimmungsergebnisse würden das Vertrauen der Bürger in unseren Staat tief erschüttern.

Estland im falschen Blickwinkel

In staatlichen Digitalisierungs-Strategien wird gerne auf Estland verwiesen. Doch sind die estnischen Erfahrungen unbesehen übertragbar? Auch dort ist die Digitalisierung nicht von der Technologie, sondern durch das Recht gesteuert. Schweizerische Strategien zur Digitalisierung sollten sich deshalb auch an klaren Zielen wie der Stärkung des Rechtstaates und seiner Institutionen, der föderalen Demokratie und der Grundrechte orientieren.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Prof. Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. (em.) Dr. iur. Rainer J. Schweizer, Prof. Dr. Günter Karjoth, Dr. iur. David Vasella

Redaktion: Dr. iur. Bruno Baeriswyl und Prof. Dr. iur. Beat Rudin

Rubrikenredaktor(inn)en: Dr. iur. Barbara Widmer, Dr. iur. Dominika Blonski

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Inland: CHF 174.00, Jahresabo Ausland: CHF 199.00, Einzelheft: CHF 48.00
PrintPlu§: Jahresabo Inland: CHF 195.00, Jahresabo Ausland CHF 220.00

PrintPlu§: Das PrintPlu§-Abonnement bietet die Möglichkeit, bequem und zeitgleich zur Printausgabe jeweils das PDF der ganzen Ausgabe herunterzuladen. Detaillierte Informationen finden Sie unter www.schulthess.com/printplus.

Anzeigenverkauf und -beratung: Fachmedien Zürichsee Werbe AG, Laubisrütistrasse 44, CH-8712 Stäfa,
Tel. +41 (0)44 928 56 11, pietro.stuck@fachmedien.ch

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach 2218, CH-8021 Zürich
Tel. +41 (0)44 200 29 29, Fax +41 (0)44 200 29 28, service@schulthess.com, www.schulthess.com

Datenkrake Leak-Checker – Lösung in Sicht?

Die existierenden Konzepte zur Information von Betroffenen bei einer Datenschutzverletzung sind ungeeignet, um einen wirklichen Schutz zu bieten. Notwendig ist daher ein neu gedachtes Konzept, dass datenschutzfreundlich arbeitet und dabei proaktiv und umfassend informiert.

Digitalisierung braucht mehr als Feigenblätter

Digitalisierung bringt viel mehr Datenbearbeitungen und damit Risiken für die Grundrechte der Bürgerinnen und Bürger. Sollen die Chancen der Digitalisierung genutzt werden können, müssen die Risiken minimiert werden. Das ist u.a. Aufgabe der Datenschutzbehörden – doch sind sie mehr als Feigenblätter? privatim schlägt Alarm.

Cybersecurity als Bachelor-Studiengang

Der Arbeitsmarkt fordert immer mehr Security-Fachpersonal. Neue Varianten von Informatik-Studiengängen bereiten darauf vor. An der Hochschule Mannheim wird ab Wintersemester 2018/19 ein Bachelor zu «Cybersecurity» angeboten. Seine Interdisziplinarität, spezielle Inhalte zu Automatisierung und ein hoher Praxisanteil sind interessante Aspekte dieses Studiengangs.

Aus den Datenschutzbehörden

Wo wird das Bedrohungsmanagement neu im Polizeigesetz geregelt? Und wo hat das kantonale Verwaltungsgericht die Verwaltungsgerichtsbeschwerde des Datenschutzbeauftragten bezüglich Drohnenaufnahmen in einer Gemeinde gutgeheissen und die Gemeinde angewiesen, sämtliche Luftaufnahmen der betroffenen Grundstücke zu löschen?

Das Stimmgeheimnis beim E-Voting

Die Stimmabgabe nachvollziehbar sicher machen und das Stimmgeheimnis wahren – geht das? Anonym ist verdächtig …

report

forum

Ausbildung

Cybersecurity-Ausbildung – ein Überblick

Bernhard M. Hämmerli, Prof. Dr., Studiengangleiter BSc Information & Cyber Security, Hochschule Luzern – Informatik, Rotkreuz
bernhard.haemmerli@hslu.ch

Die Cyber-Bedrohungslage hat sich in den letzten Jahren massiv verschärft. Seit langem verlangen die Information Security Professionals mehr Investitionen in ihrem Bereich. Erfolgreich hatten sich über 20 Jahre die Unternehmen gegen grosse Sprünge an Mehrinvestitionen gewehrt. Die Schadenssumme war zwar individuell empfunden hoch, doch waren es um die Jahrtausendwende einige 100 000 CHF bis wenige Millionen, was bei grossen Firmen durchaus auch getragen werden konnte: Die Beträge waren weder im Vergleich zur Sicherheitsinvestition noch zum Firmenumsatz kritisch. Im Jahr 2014 kam es zum ersten grossen Paukenschlag, als Carbanak[1], ein einziges Stück Malware, einen weltweiten Schaden von 1 Milliarde USD verursachte. In über 30 Ländern waren bis zu 100 Banken von diesem «Advanced Persistent Thread» (APT) betroffen.

Die «kleinen Schäden» sind geblieben und häufiger geworden. Jedoch hat sich innert 14 Jahren die maximale Schadenssumme, verursacht durch eine einzige Malware, um einen Faktor von ca. 1000 erhöht. 2017 waren wir mit der Familie WannaCry[2], Petya[3], NotPetya konfrontiert, einer Malware, die gesamtheitlich einen geschätzten Schaden von 100 Milliarden USD generierte und in Einzelfällen Firmen bis zu 3,5 Milliarden USD gekostet hat[4]. Ursprünglich war die Malware als Erpressungssoftware gedacht; aber mit den letzten Versionen drang die Malware auch in sehr komplexe Systeme ein, und die Kontrolle über die Malware entglitt den Erpressern: Sehr viele Daten wurden verschlüsselt, jedoch gelang es den Erpressern nicht mehr, die verschlüsselten Daten zu dechiffrieren[5]. NotPetya war dann nur noch eine Datenzerstörungssoftware, und die Erpresser konnten am Ende im Vergleich zum angerichteten Schaden nur sehr wenig Geld machen. Die angegebenen Zahlen entsprechen qualifizierten Schätzungen, die in Insiderkreisen bekannt sind. Die Angaben von WannaCry lassen Spielraum; bei Petya ist Maersk[6] mit ca. 250 Millionen USD das öffentlich gehandelte Beispiel.

Die Informationsebene des Cyberspace wird durch Fake News und Manipulationen eingesetzt, um sich auf verschiedensten Gebieten Vorteile zu verschaffen. Wahlbetrug in der Präsidentschaftswahl in USA und beim Brexit im UK sind Beispiele auf staatlicher Ebene. Die Aufklärung der vorgefallenen Sachverhalte braucht Cybertalente, die in komplexen Systemen die Spuren lesen können und diese hinsichtlich der Täter auswerten können. Fälle von Wirtschaftsspionage werden beinahe täglich publiziert: Die daraus entstehenden finanziellen Nachteile sind schwierig zu beziffern. Die Tatsache, wie oft Vorfälle aufgedeckt werden, zeigt, wie lohnenswert dieses Vorgehen für Täter sein muss.

Mangel an Fachkräften

Aufgrund der oben beschriebenen Lage nahm der Druck unerwartet rasch zu, Massnahmen zu ergreifen, wie z.B. die Installation fortschrittlicher Cyber-Defence-Techniken und deren Überwachung mit Personal. Und nun wollen alle Regierungen und Betriebe gleichzeitig den Cybersecurity-Bereich aufbauen. Nur fehlen die qualifizierten und vertrauenswürdigen Cybersecurity Professionals und -Experten. Kritisch ist auch deren Vertrauenswürdigkeit: Oft sind Sicherheitsprüfungen notwendig, die dann nur wenige Nationalitäten für einen spezifischen Markt zulassen. Daraus lässt sich ableiten, dass die Ausbildung der Information & Cybersecurity Workforce eine nationale Aufgabe ist, die nur bedingt in Billiglohnländer ausgelagert bzw. auch nur sehr bedingt von Personen anderer Nationalität verantwortet werden kann.

Sucht man in Google nach offenen Stellen im Information-&-Cybersecurity-Bereich und zählt die offen Stellen der grössten drei Jobportale zusammen, so kommt man je nach Zeitpunkt auf 500–700 offene Stellen: Das bedeutet eine wirkliche Knappheit an Fachkräften, die nicht rasch behoben werden kann. Es lohnt sich demnach, einen Blick auf das Schweizer Aus- und Weiterbildungssystem zu werfen.

Ausbildungsgänge

In der Schweiz können heute auf unterschiedlichen Ebenen Qualifikationen im Information & Cybersecurity-Bereich erworben werden.

Höhere Fachprüfung

Der Verband ICT-Berufsbildung Schweiz entwickelte ein Programm zum «ICT Security Expert» (Eidgenössisches Diplom ED, Stufe höhere Fachprüfung)[7]. Dieses Diplom kann mit mindestens drei Jahren Berufserfahrung und drei bis vier Semestern Teilzeitunterricht erworben werden. Bei bestandenem Diplom erstattet der Bund 50% der Ausbildungskosten. Handlungskompetenzen liegen primär in der Informationssicherheit, Sicherheitsstrategie, Awareness und ISMS Incident Response. Die erste Diplomprüfung findet im Herbst 2018 statt.

Bachelor

Alle sieben öffentlich-rechtlichen Fachhochschulen und die zwei vom Bund genehmigten Fachhochschulen mit privater Trägerschaft bieten Informatikstudiengänge auf Bachelor-Level an. Diese bieten innerhalb des Studienganges Vertiefungsrichtungen an, die typischerweise 10% bis maximal 15% des gesamten Studiums ausmachen. Damit können sicherlich wesentliche Fähigkeiten im Bereich Sicherheit als Zusatz erworben werden, jedoch bleibt die Kernqualifikation im angestammten Gebiet.

Master

Die Schweizer Fachhochschulen haben in der grundständigen Ausbildung nur einen Master of Science, der eine gewisse Spezialisierung in Sicherheit erlaubt, aber nicht vollständig auf Information & Cybersecurity ausgerichtet ist.

Die ETH Zürich bietet ebenfalls nur eine Vertiefungsrichtung in Informationssicherheit an. Die Kurse sind mehr auf die Forschung ausgerichtet und haben eine geringe Ausbildungszahl. Die EPFL bietet ebenfalls eine Spezialisierung in Informationssicherheit (ab September 2018: Cybersecurity) an.

Alle Ausbildungseinrichtungen haben hervorragende Kompetenzen in verschiedenen Bereichen der Informationssicherheit und bieten entsprechende Kurse an – jedoch ist kein Master voll auf Information & Cybersecurity ausgerichtet.

Promotion

Eine Promotion ist nur an den universitären Hochschulen möglich. Doktorierende schliessen mit den betreuenden Professoren eine Vereinbarung über ihr Forschungsthema ab. Insbesondere Professoren an den beiden ETH unterstützen Doktorate im Bereich Information & Cybersecurity.

Weiterbildung

Die Weiterbildung ist ein Leistungsbereich der Universitäten und Fachhochschulen, der wirtschaftlich selbstragend sein muss. Die Weiterbildung richtet sich an Personen mit mindesten fünf Jahren Berufspraxis, die entweder Kompetenz in einem Spezialgebiet ausweisen können oder sich in ein neues Gebiet umschulen wollen.

Die Ausbildungsgänge werden in Credits bemessen, wobei ein Kreditpunkt einer Studierendenleistung von 30 Stunden entsprechen soll. Das «Certificate of Advanced Studies» (CAS) hat meistens 10 bis 15 Credits, das «Diploma of Advanced Studies» (DAS) ca. 30 Credits und der «Master of Advanced Studies» (MAS) 60 bis 90 Credits.

Die CAS-, DAS und MAS-Ausbildungen zeichnen sich durch klare berufliche Profile aus, welche für die Wirtschaft interessant sind – nur diese Profile erlauben es, genügend Teilnehmende zu rekrutieren, so dass die Studiengänge durchgeführt werden können.

Angebote der Fachhochschulen

Die Berner Fachhochschule (BFH) bietet drei CAS an: in «Security & Privacy», in «Security Incident Management» und «Networking & Security». Studierende erhalten einen MAS-Titel, wenn sie drei CAS besuchen und mit einer Masterarbeit ergänzen.

Die Fachhochschule Nordwestschweiz (FHNW) bietet das CAS «Information Security & Risk Management» an, das auch als Zertifizierungsvorbereitung zum «Certified Information System Security Professional» (CISSP) geeignet ist.

Die Hochschule Luzern (HSLU) bietet seit 1996 CAS im Security-Bereich an und die Produkte wurden in mehrjähriger Vorbereitungsarbeit innerhalb der Information Security Society Switzerland (ISSS) bzw. der Vorgängerorganisation entwickelt. Es werden zwei CAS angeboten, die den Pflichtteil zum MAS ausmachen: CAS «Information Security – Technology», CAS «Information Security – Management». Das dritte CAS kann

Kurz&bündig

Die Wirtschaft sucht dringend Fachkräfte im Bereich Information & Cybersecurity. Die Lage ist dermassen prekär, dass verschiedene parallele Initiativen aus Wirtschaft und Verwaltung bezüglich Information-&-Cybersecurity-Ausbildungen laufen. Die erforderlichen Fähigkeiten für Cybersecurity Professionals steigen aufgrund der Komplexität rasch an, weshalb die Grundausbildung einen engeren Fokus auf die Cybersecurity legen muss, um das Ziel einer erhöhten Sicherheit zu erreichen.

gewählt werden, wobei sich im Security-Bereich die folgenden beiden CAS anbieten: CAS «Information Security Advanced», CAS «Data Privacy Officer». Nach drei besuchten CAS führt ebenfalls eine Masterarbeit zum MAS-Titel. Das MAS «Information Security» der HSLU eignet sich als Zertifizierungsvorbereitung für den «Certified Information Security Manager» (CISM).

Die Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) bietet den Master of Advanced Studies in «Integrated Risk Management» an. Der Titel setzt voraus, dass die folgenden fünf CAS erfolgreich bestanden sind: CAS «Integriertes Risikomanagement», CAS «Notfall- und Krisenmanagement», CAS «Risikoanalytik und Risiko-Assessment», CAS «Risiko- und Krisenkommunikation» und CAS «Risikomanagement & Recht».

Professionelle Zertifizierungen

Professionelle Zertifizierungen sind eine geeignete Möglichkeit, Innovationen zeitgerecht folgen zu können, weil die privaten Organisationen flexibler sind und zeitnah agieren können. Professionelle Zertifizierungen sind breit abgestützt in einer Fachorganisation und beinhalten wesentliche Fähigkeitszusammenstellungen, welche geprüft werden. Professionelle Zertifizierungen sind mehr als die Angebote der Kursanbieter, die in wenigen Tagen minimale Kenntnisse zu einem Spezialthema vermitteln.

Das «International Information System Security Certification Consortium» (ISC)[2] hat das Zertifikat «Certified Information System Security Professional» (CISSP) definiert, eines der ganz wesentlichen Fachzertifikate, das eine breite Ausbildung in IT- und Information Security nachweist.

Nach dem Erfolg der CISSP-Zertifizierung wurden acht weitere Zertifizierungen entwickelt, deren drei wichtigste sind: «Information Systems Security Architecture Professional» (CISSP-ISSAP), «Information Systems Security Engineering Professional» (CISSP-ISSEP) und «Information Systems Security Management Professional» (CISSP-ISSMP).

Die Information Systems Audit and Control Association (ISACA) ist ein internationaler Verband für Spezialisten aus dem IT-Audit-Bereich mit über 140 000 Mitgliedern. Ihre «Certified Information Systems Auditor»-(CISA)-Zertifizierung stammt aus der Prüfung der Grundsätze ordentlicher Verarbeitung bei der Buchführung. Vier weitere Zertifizierungen wurden danach entwickelt: «Certified in the Governance of Enterprise IT», «Certified Information Security Manager», «Certified in Risk and Information Systems Control» und Cybersecurity Nexus «Professionalität als Cyber Security Experte».

Eine erfolgreiche Zertifizierung hat eine starke neutrale Organisation als Träger, deckt ein Bedürfnis ab und ist im Interesse sowohl des Arbeitnehmers, der sich zertifiziert, wie des Arbeitgebers, dem ein Teil seiner Sorgfaltspflicht bei der Prüfung der Fähigkeit beim Anstellen oder bei der Vergabe von Mandaten abgenommen wird.

Firmenzertifikate, wie zum Beispiel von Firmen wie CISCO, Checkpoint, Microsoft und Palo Alto, versichern dem Arbeitgeber, dass seine Mitarbeiter ausreichend auf ihren Produkten ausgebildet sind. Auch verbessern diese Zertifikate für den Arbeitnehmer seine Position im Markt.

Ausblick

Die Security-Technologie hat sich massiv über die Zeit gewandelt. Zu Beginn in den neunziger Jahren waren primär Kryptologen IT-Security-Spezialisten, dann Netzwerksicherheitsspezialisten, dann Systemspezialisten und erst später kam die Verwaltung und Führung der Sicherheit (ISMS) in der breiten Information-Security-Gemeinschaft in den Fokus.

Traditionell ist die Security-Technologie an den technischen Hochschulen beheimatet. Dabei muss der Forschungscharakter «Entwicklung von neuen Technologien», ein Thema bei den universitären Spitzenschulen, und «Anwendung von Technologien zur Sicherung von Unternehmen», ein Thema primär der Fachhochschulen, unterschieden werden. In beiden Bereichen hat die Schweiz herausragende Professoren, die viel zur Entwicklung der Sicherheit in der Schweiz beigetragen haben.

Wie aufgezeigt, gibt es aber keinen direkten Einstieg in die Information & Cyberse-

Fussnoten

1 <http://de.wikipedia.org/wiki/Carbanak>.
2 <http://en.wikipedia.org/wiki/WannaCry_ransomware_attack>.
3 <http://en.wikipedia.org/wiki/Petya_(malware)>.
4 Diese Angaben stammen aus zuverlässiger Quelle: Quellenschutz.
5 <https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b>.
6 <https://www.heise.de/newsticker/meldung/NotPetya-Maersk-erwartet-bis-zu-300-Millionen-Dollar-Verlust-3804688.html
7 <https://www.ict-berufsbildung.ch/berufsbildung/ict-weiterbildung/ict-security-expert-ed/>.
8 <https://www.hslu.ch/de-ch/informatik/studium/bachelor/information-and-cyber-security/>.
(Alle URL letztmals kontrolliert am 24.5.2018.)

curity. Diese Möglichkeit gibt es jedoch schon seit einiger Zeit im Ausland. Einrichtungen in Deutschland, Österreich, Norwegen, im UK etc. bieten Bachelor-Studiengänge im Bereich Information, IT und Cybersecurity an.

In der Schweiz startet die Hochschule Luzern – Informatik zum Herbstsemester 2018 als erste Ausbildungsstätte einen Bachelor-Studiengang mit 5400 studentischen Arbeitsstunden, der vollständig auf den Berufseinstieg in Information & Cybersecurity ausgerichtet ist[8]. Heute sind in der Information & Cybersecurity mindestens 50 unterschiedliche Berufsprofile in der Praxis verankert, mit der Tendenz, dass durch den Technologiefortschritt noch weitere Berufe entstehen. Obwohl der Studiengang zwei Security-Vertiefungen anbietet («Technologie» und «Management»), bleibt er generalistisch, um den Einstieg in möglichst viele Berufsfelder zu ermöglichen.

Dieser Studiengang ist eine Antwort auf die grosse Nachfrage an Spezialisten, verursacht durch die stetig steigende Bedrohungslage. Nur mit einer vollen thematischen Ausrichtung können die heutigen und künftigen Anforderungen der Wirtschaft fachlich und professionell erfüllt werden. ■

BSc Information & Cyber Security

Hochschule Luzern – Informatik
Beginn des neuen Studiengangs: 13. September 2018
Informationen und Anmeldung: <http://www.hslu.ch/bachelor-ics>
Anmeldung bis zum 1. September 2018 möglich
Leitung: Prof. Dr. Bernhard M. Hämmerli

Schulthess §

Herausgeber:
Dr. iur. Bruno Baeriswyl,
Prof. Dr. iur. Beat Rudin,
Prof. Dr. Bernhard M. Hämmerli,
Prof. (em.) Dr. iur. Rainer J. Schweizer,
Prof. Dr. Günter Karjoth, Dr. iur. David Vasella

Redaktion:
Dr. iur. Bruno Baeriswyl, Prof. Dr. iur. Beat Rudin

Sprache: deutsch

☑ **JA,** ich profitiere vom **Mini-Abo** von **digma** und erhalte **2 Ausgaben** zum Kennenlernpreis von nur **CHF 58.–** (inkl. MWST und Versandkosten).

Vorname/Name

Firma

Strasse/Nr.

PLZ/Ort

E-Mail

Datum/Unterschrift

Abonnement-Bedingungen

Wenn ich digma danach weiterlesen möchte, muss ich nichts weiter tun und erhalte im Jahresabonnement 4 Printausgaben zum Preis von CHF 174.00 (inkl. MWST, zzgl. CHF 6.00 Versandkosten). Falls ich digma nicht weiter beziehen möchte, melde ich mich spätestens 7 Tage nach Erhalt der 2. Testausgabe bei Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach 2218, CH-8021 Zürich, E-Mail: service@schulthess.com, Fax: +41 (0)44 200 29 28.

A

Nicht frankieren
Ne pas affranchir
Non affrancare

Geschäftsantwortsendung Invio commerciale-risposta
Envoi commercial-réponse

Schulthess Juristische Medien AG
Kundenservice
Zwingliplatz 2
Postfach 2218
8021 Zürich