

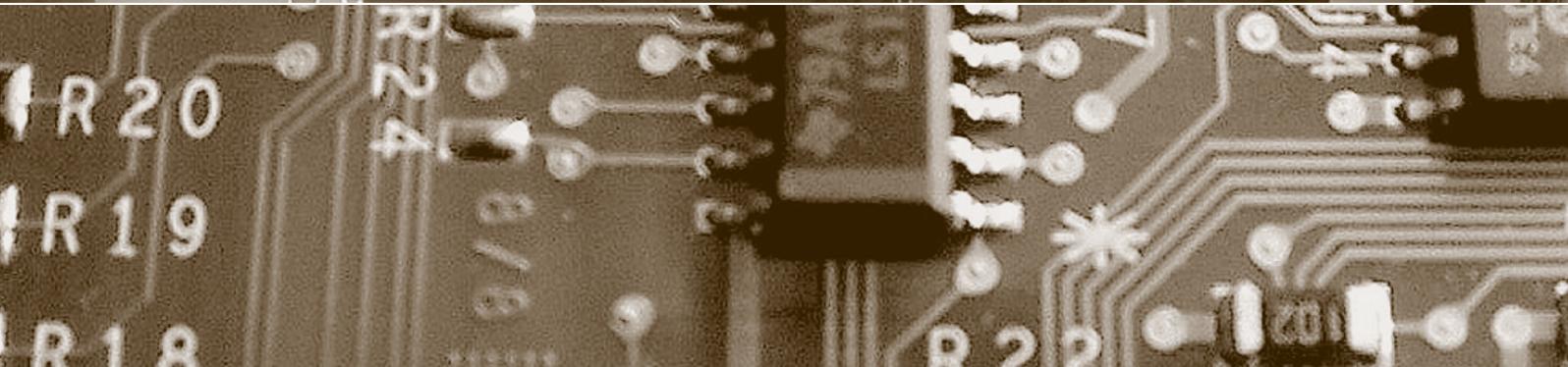
Schwerpunkt:

## 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

## fokus



Schwerpunkt:

### Digitale Demokratie

auftakt

#### Demokratie heisst Betroffene beteiligen

von Balthasar Glättli Seite 37

#### Auf dem Weg zur digitalen Demokratie

von Günter Karjoth Seite 40

#### E-Voting, ein Mehrwert für die Demokratie

von Barbara Schüpbach-Guggenbühl Seite 42

zwischenakt

#### Die Demokratie verträgt nicht das leiseste Misstrauen

von Erich Aschwanden Seite 47

#### E-Voting CH: Das Ende der Demokratie?

von René Droz Seite 50

#### Estland im falschen Blickwinkel

von Bruno Baeriswyl Seite 56

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, ein Mehrwert für die 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.

**E-Voting CH: Das Ende der Demokratie?**

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 Rechtsstaates und seiner Institutionen, der föderalen Demokratie und der Grundrechte orientieren.

**Estland im falschen Blickwinkel**

## impresum

**digma:** Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: [www.digma.info](http://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](mailto: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  
PrintPlus: Jahresabo Inland: CHF 195.00, Jahresabo Ausland CHF 220.00

**PrintPlus:** Das PrintPlus-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](http://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](mailto: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](mailto:service@schulthess.com), [www.schulthess.com](http://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, das 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 ...

### Forschung

**Datenkrake Leak-Checker – Lösung in Sicht?**  
von Susan Gonscherowski/Oliver Vettermann/  
Matthias Wübbeling/Timo Malderle Seite 60

agenda Seite 64

### Datenschutzaufsicht

**Digitalisierung braucht mehr als Feigenblätter**  
von Beat Rudin Seite 66

### Ausbildung

**Cybersecurity Ausbildung – ein Überblick**  
von Bernhard M. Hämmerli Seite 68

### Ausbildung

**Cybersecurity als Bachelor-Studiengang**  
von Sachar Paulus Seite 72

### zwischenakt

**Lasst uns unsere Geheimnisse!**  
von Helmut Stalder Seite 74



### privatim

**Aus den Datenschutzbehörden**  
von Dominika Blonski Seite 76

Der Blick nach Europa und darüber hinaus  
**Welches Recht soll es sein?**  
von Barbara Widmer Seite 78

### schlussakt

**Was geschieht mit unserer Gesellschaft?**  
von Beat Rudin Seite 80

### cartoon

von Reto Fontana Umschlagseite 3

## Ausbildung

# Cybersecurity als Bachelor-Studiengang



Sachar Paulus,  
Prof. Dr., Hochschule Mannheim,  
Mannheim,  
Deutschland  
paulus@hs-mannheim.de

Es gibt gegenwärtig eine Vielzahl von Studienangeboten zur IT-Sicherheit, mit sehr unterschiedlichen Profilierungen. Ein Grossteil dieser Studiengänge sind jedoch Masterstudiengänge. Viele Akademiker, die im Security-Bereich forschen und lehren, sagen, dass man zuerst eine fundierte Grundlagenausbildung haben muss – entsprechend ist ein Informatik- oder Wirtschaftsinformatikstudium der richtige Einstieg. Andererseits ist die Nachfrage nach Security-Fachkräften seit Jahren ungebrochen, und so ist es für Hochschulen verlockend, auch für Studienanfänger eine entsprechende Spezialisierung von Anfang an anzubieten.

In Deutschland gab es im November 2017 elf Bachelorstudiengänge mit Security-Profil. Die meisten dieser Studiengänge sind Ableger der Informatik, wo die Informatikausbildung um Aspekte der Sicherheit ergänzt wurde. Sie dauern mindestens sechs Semester und unterscheiden sich durch ihren Fokus auf Technik oder Management, Praxisnähe oder Forschungsorientierung.

An der Hochschule Mannheim wurde ebenfalls ein entsprechender Studiengang entwickelt, der im Wintersemester 2018 zum ersten Mal durch-

geführt wird. Er erhebt den Anspruch, interdisziplinär zu sein und die jungen Menschen auf «Cyber» vorzubereiten.

Dieser Artikel geht der Frage nach, welche Motivation der Einrichtung des Studiengangs zugrunde liegt, welche Kompetenzziele verfolgt werden und wie diese erreicht werden sollen.

## Motivation

Mehrere Faktoren bildeten die Motivation für die Konzeption des neuen Studiengangs. ■ Es gibt in der Rhein-Neckar-Region eine recht grosse Dichte an Firmen, die sich auf IT-Sicherheit spezialisiert haben. Masterangebote sind für die Unternehmen nicht so interessant, da die grösste Chance, neue Mitarbeiter zu gewinnen, eher im Bachelorbereich liegt.

■ Für Professoren sind Masterstudierende mit Security-Schwerpunkt sehr dienlich für die eigene Forschung; jedoch ist die Hochschule Mannheim in einem industriestarken Umfeld angesiedelt, und von interessanten Masterangeboten in der erweiterten Region umgeben (Darmstadt, Kaiserslautern, Karlsruhe). Entsprechend bleiben wenige Informatik-Absolventen mit Bachelorabschluss (oder vergleichbarer Studiengänge) in Mannheim

für ein Masterstudium. Folglich müssen die Professoren früher ansetzen, um Nachwuchs heranziehen zu können.

■ Auf einer Veranstaltung der Bundeswehr im Frühjahr 2017 wurde die (nicht mehr ganz so) neue Cyberstrategie der Bundeswehr vorgestellt, erläutert und an einem Podium gemeinsam diskutiert. Dabei wurde klar, dass die Bundeswehr, auch bei Zusammenlegung aller bestehenden Ressourcen, einen erheblichen Bedarf an Nachwuchskräften hat und dass die neuen Soldaten nicht nur allgemeine Kenntnisse in der IT benötigen, sondern insbesondere auch im Bereich der Cybersicherheit.

Die sich daran anschließende hochschulinterne Diskussion führte zu dem Entschluss, ein entsprechendes Angebot zu konzipieren.

## Inhalt

Die Kernidee ist, den Studiengang interdisziplinär zu gestalten und gleichzeitig auf ein modulares Konzept zu setzen. Die Kompetenzziele sind dabei einerseits an dem sicheren Beherrschen von Automatisierungstechnik («Cyber») und andererseits an modernen Ansätzen der Programmierung und Software-Entwicklung ausgerichtet.

Flankiert werden diese technischen Kernkompetenzen mit Grundlagen aus Soziologie, Recht und Betriebswirtschaft, um die Auswirkungen von Angriffen und Schwach-

## Fussnoten

<sup>1</sup> Im Forschungsvorhaben IUNO, dem Nationalen Referenzprojekt zur IT-Sicherheit in Industrie 4.0, werden Bedrohungen und Risiken für die intelligente Fabrik identifiziert, Schutzmassnahmen entwickelt und exemplarisch in vier Anwendungsfällen umgesetzt. Siehe <<http://www.iuno-projekt.de>>.

stellen geeignet bewerten zu können. Schliesslich wird grosser Wert auf soziale Kompetenzen, speziell die Wahrnehmung ethischer Verantwortung, gelegt, um die Studierenden im Hinblick auf ihre neue Aufgabe entsprechend vorbereiten zu können.

Mit diesem Kompetenzprofil sollten den jungen Menschen dann Positionen in den verschiedensten Bereichen zugänglich sein: im Bereich der Steuerung von Informationssicherheit und Datenschutz, im Bereich der sicheren Softwareprogrammierung oder im Bereich der Sicherheitsberatung und -dienstleistung.

Realisiert wird dieser Studiengang durch eine überfakultäre Zusammenarbeit – die Lehrveranstaltungen rund um Automatisierungstechnik (Microcontrollertechnik, Industrie 4.0, sichere Heimautomatisierung) werden von der Fakultät für Elektrotechnik erbracht; die technischen Inhalte rund um Systeme, Netzwerke und Protokolle kommen von der Fakultät für Informationstechnik (vormals Nachrichtentechnik) und die Programmier- und Software-Entwicklungs-Module werden von der Fakultät für Informatik übernommen.

Der Studiengang gliedert sich in drei Phasen:

■ In der Grundlagenphase werden innerhalb von drei Semestern die Studierenden mit den erforderlichen Grundlagen versorgt.

■ In der Praxisphase befinden sich ein Projektsemester, währenddessen die Studierenden in Teams Sicherheitslösungen für reale Kunden entwickeln müssen, und das in Baden-Württemberg übliche 6-monatige Praxissemester.

■ In der zweisemestrigen Abschlussphase haben die Studierenden die Möglichkeit, Wahlpflichtmodule nach eigenem Interesse zusammenzustellen.

### Reflektion

Ist nun dieses Studienangebot geeignet, den Bedarf der Industrie zu bedienen? Sind die Ausbildungsinhalte und Kompetenzziele vollständig genug, um in der Wirtschaft (oder auch für die Bundeswehr) von Interesse zu sein? Die Antwort kann natürlich erst wirklich gegeben werden, wenn die ersten Absolventen auf den Arbeitsmarkt kommen. Dennoch gibt es Anlass zu der Vermutung, dass dies zutreffen könnte.

Im Wintersemester 2017/18 wurde das Projektsemester des Studiengangs «Unternehmens- und Wirtschaftsinformatik» mit der Security-Firma Accessec GmbH und den produzierenden Unternehmen HOMAG und TRUMPF durchgeführt. Aufgabe war es, Lösungen zu entwickeln, mit denen ein produzierendes mittelständisches Unternehmen seine Informationssicherheitsrisiken (im Rahmen der Digitalisierung und Industrie 4.0)

leicht erfassen und steuern kann.

Die Ergebnisse waren – auch aus Sicht der erfahrenen Dozenten der Hochschule – sehr gut. Die Erkenntnisse aus dem Projektsemester sind in das Nationale Referenzprojekt IUNO<sup>1</sup> eingeflossen. Ausserdem erhielten die Studierenden Einladungen, ihre Ergebnisse an verschiedenen Veranstaltungen zu präsentieren, unter anderem auf der Hannover Messe. Einigen Studierenden wurde zudem schon am Ende des vierten Semesters eine Festanstellung angeboten.

Diese erste Erfahrung zeigt, dass Studierende mit einer angemessenen «Grundausbildung», problembasierten Lehrkonzepten mit Praxisbezug und einer entsprechenden Betreuung durch erfahrene Lehrpersonen auch schon ab dem vierten Semester für Sicherheitsaufgaben einsetzbar sind (natürlich nicht alle gleich gut). Insofern ist es durchaus anzunehmen, dass ein Cybersecurity-Bachelorabschluss «funktioniert». ■

### Kurz & bündig

Der Arbeitsmarkt fordert immer mehr Security-Fachpersonal. Neue Varianten von Informatikstudiengängen 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.



# 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](mailto:service@schulthess.com), Fax: +41 (0)44 200 29 28.



# A

Nicht frankieren  
Ne pas affranchir  
Non affrancare

Geschäftsantwortung Invio commerciale-risposta  
Envoi commercial-réponse



Schulthess Juristische Medien AG  
Kundenservice  
Zwingliplatz 2  
Postfach 2218  
8021 Zürich