

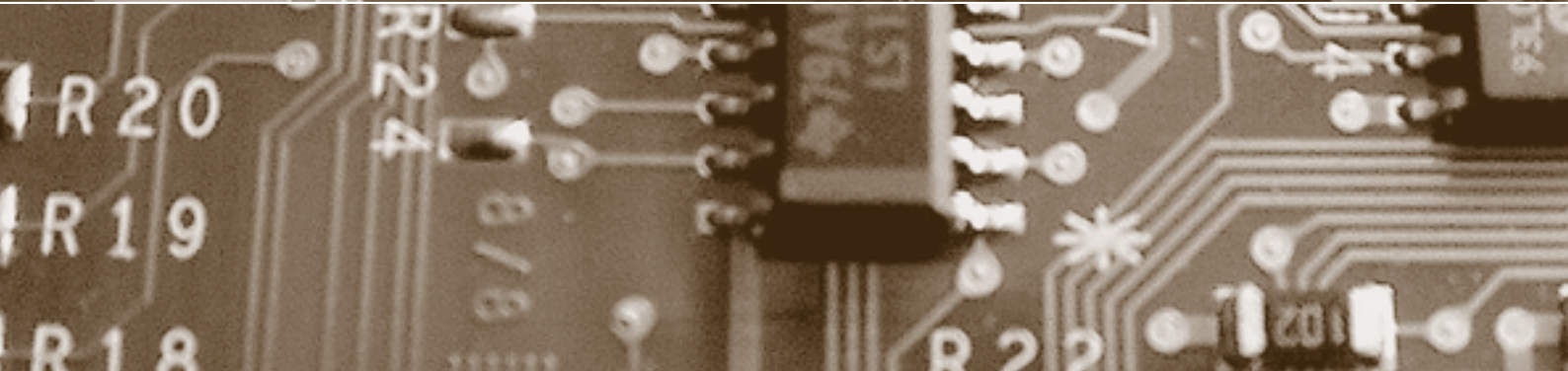
Schwerpunkt:

Sensor-Actor-Netze

fokus: Lagebild für Kritische Infrastrukturen

fokus: Privatsphäre trotz intelligenter Zähler

report: Sicherheit im Cloud Computing



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

fokus

Schwerpunkt:

Sensor-Actor-Netze

auftakt

Prima leben ohne Privatsphäre

Roberto Simanowski Seite 1

Kritikalität von Sensor-Actor-Netzen

von Bernhard M. Hämmerli Seite 4

Lagebild für Kritische Infrastrukturen

von Heiko Borchert/Stefan Brem Seite 6

Schutz der Schweiz vor Cyber-Risiken

von Gérald Vernez Seite 10

Sicherheit im Energienetz der Zukunft

von Sven Garrels Seite 14

PET – ein Konzept harrt der Umsetzung

von Bruno Baeriswyl Seite 18

Privatsphäre trotz Intelligenter Zähler

von Markulf Kohlweiss und Lothar Fritsch Seite 22

Für den Schutz Kritischer Infrastrukturen (SKI) ist der regelmässige Austausch von Informationen zwischen Behörden und Unternehmen unerlässlich. Dieser könnte in einem SKI-relevanten Lagebild gebündelt und aufbereitet werden. Darin können Behörden und Betreiber Informationen zum Schutz Kritischer Infrastrukturen bündeln und die Koordination im Hinblick auf Schutzmassnahmen verbessern.

Lagebild für Kritische Infrastrukturen

Durch den vermehrten Einsatz von ICT und der damit verbundenen erhöhten Anzahl von Schnittstellen im Energienetz entstehen neue Sicherheitsrisiken in Bezug auf Netzverfügbarkeit, Systemintegrität und Datenschutz. Ein Sicherheitskonzept für das intelligente Stromnetz der Zukunft sollte frühzeitig geplant werden.

Sicherheit im Energienetz der Zukunft

Mit «Privacy Enhancing Technology» (PET) sollen neue Anwendungen «datenschutzverträglich» gemacht werden. Die inhärenten Zielkonflikte können nur aufgelöst werden, wenn neben der Technik auch das Datenschutzrecht in die Betrachtung einbezogen wird.

PET – ein Konzept harrt der Umsetzung

Intelligente Zähler versprechen eine bessere Ausnutzung vorhandener Infrastruktur für Netzbetreiber und erhöhte Transparenz für Konsumenten. Kann die Privatsphäre im eigenen Heim bedingungslos geschützt werden, oder folgt auf den gläsernen Mobilfunkkunden nun der gläserne Stromkunde?

Privatsphäre trotz Intelligenter Zähler

impresum

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

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer J. Schweizer, Dr. Günter Karjoth

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

Zustelladresse: Redaktion digma, per Adr. Datenschutzbeauftragter des Kantons Basel-Stadt, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, Fax +41 (0)61 201 16 41, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 131.00 (inkl. Versandkosten), Einzelheft: CHF 42.00

Anzeigenmarketing: Publicitas Publimag AG, Mürtchenstrasse 39, Postfach, CH-8010 Zürich
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, www.publimag.ch, service.zh@publimag.ch

Herstellung: Schulthess Juristische Medien AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 19, Fax +41 (0)44 200 29 08, www.schulthess.com, zs.verlag@schulthess.com

Sicherheit im Cloud Computing

Obwohl in den Medien intensiv über Cloud Computing und entsprechende ökonomische Vorteile berichtet wird, werden die latent vorhandenen Sicherheitsprobleme meist verschwiegen bzw. ignoriert. Muss man den Cloud-Anbietern einfach vertrauen?

E-Learning: Kryptografie und -analyse

Das Open-Source-Projekt CrypTool (CT) hat sich die Aufgabe gestellt, Kryptografie und Kryptoanalyse mit Beispielen und Visualisierungen so darzustellen, dass man ein gutes Verständnis und Awareness für IT-Sicherheit erreicht.

Familie und Arbeitsplatz: heikle Ortung

Location Based Services sind heikel oder unzulässig, wenn sie der Überwachung von Kindern und Arbeitnehmenden dienen. Die gesetzliche Vertretung ist bei älteren Kindern meist nicht befugt, an deren Stelle die Einwilligung zur Datenbearbeitung zu erteilen. Das Arbeitsrecht schränkt die Überwachung von Arbeitnehmenden erheblich ein.

EU: Zu neuen Ufern lockt ein neuer Tag?

Die EU-Kommission hat Entwürfe für eine «Regulation» und eine «Directive» zur Vereinheitlichung des Datenschutzrechts vorgelegt. Mit dem darin enthaltenen «right to be forgotten» und dem Strafenkatalog würde ein bedeutender Schritt in Richtung Harmonisierung des Datenschutzrechts getan. Es ist zu hoffen, dass der Gedanke der Entwürfe in der definitiven Fassung immer noch zu erkennen sein wird.

Aus den Datenschutzbehörden

Wer ist neu zur Datenschutzbeauftragten gewählt worden? Welche Themen haben Datenschutzbehörden im letzten Quartal bearbeitet? Die Unterrubrik berichtet über Personelles und Aktuelles aus der Datenschutzzsene.

report



Sicherheit

Sicherheit im Cloud Computing

von Rolf Oppliger

Seite 28

Lernen

E-Learning:

Kryptografie und -analyse

von Bernhard Esslinger/Sibylle Hick Seite 32

Follow-up: Location Based Services

Familie und Arbeitsplatz: heikle Ortung

von Daniel Kettiger

Seite 36

Rechtsentwicklung

EU: Zu neuen Ufern lockt ein neuer Tag?

von Sandra Husi-Stämpfli

Seite 38

Transfer

Private Smartphones im Geschäftsumfeld

von Roland Portmann

Seite 42

forum



privatim

Aus den Datenschutzbehörden

von Sandra Husi-Stämpfli

Seite 44

ISSS

Jahresprogramm ISSS 2012

von Ursula Widmer

Seite 45

ISSS

Wie sicher sind «sichere» IT-Systeme?

von Sonja Hof

Seite 46

agenda

Seite 47

schlussstakt

In der Gratis-Falle

von Bruno Baeriswyl

Seite 48

cartoon

von Reto Fontana

Lagebild für Kritische Infrastrukturen

Sicherheitsgewinn durch Informationsaustausch zwischen Behörden und Unternehmen



Heiko Borchert,
Dr., Inhaber und
Geschäftsführer,
Sandfire AG,
Luzern
borchert@
sandfire.ch

In einem Lagebild können Behörden und Betreiber Informationen zum Schutz Kritischer Infrastrukturen bündeln und die Koordination im Hinblick auf Schutzmassnahmen verbessern.

Die Schweiz ist in grossem Masse vom kontinuierlichen Funktionieren Kritischer Infrastrukturen (KI) abhängig, welche die Versorgung mit wichtigen Gütern und Dienstleistungen sicherstellen. Dazu gehören unter anderem die Stromversorgung, der Luftverkehr, die Informationstechnologien oder auch die Abfallentsorgung. Störungen wirken sich rasch auf die Bevölkerung und die Wirtschaft aus und können dominoartig auf andere Kritische Infrastrukturen übergreifen: So beeinträchtigt beispielsweise ein grossflächiger Stromausfall auch die Wasserversorgung, die Telekommunikation und den Schienenverkehr.

Kritische Infrastrukturen in der Schweiz

In der Schweiz werden auf nationaler Ebene zehn Sektoren als kritisch betrachtet. Dazu gehören etwa Energie, Verkehr oder Finanzen. Sie lassen sich unterteilen in 28 Teilsektoren, z.B. Strom-, Erdöl- und Erdgasversorgung im Energie-Sektor. Für einzelne Teilsektoren und insbesondere für darin enthaltene Objekte (wie etwa Unterwerke, Netzleitstellen oder Trafostationen) bestehen zum Teil bereits weit fortgeschrittene Schutzmassnahmen. Lange Zeit fehlten jedoch eine sektorübergreifende Koordination und ein einheitliches Vorgehen auf nationaler Ebene. Aus diesem Grund hat der Bundesrat das Bundesamt für Bevölkerungsschutz (BABS) mit der Koordination der Arbeiten zu dieser Thematik und der Erarbeitung einer nationalen Strategie zum Schutz Kritischer Infrastrukturen (SKI-Strategie) beauftragt.

Erarbeitung einer nationalen Strategie

Die nationale SKI-Strategie wird dem Bundesrat im Frühjahr 2012 unterbreitet. Das übergeordnete Ziel besteht darin, die Funktionsfähigkeit der Kritischen Infrastrukturen aufrechtzuerhalten bzw. das Schadensausmass im Fall von Störungen zu begrenzen. Die Konsultationsversion der SKI-Strategie schlägt insgesamt 16 Massnahmen vor. Dazu zählen etwa die Erstellung und periodische Überprüfung eines Inventars der Kritischen Infrastrukturen oder die periodische Erarbeitung einer priorisierten Übersicht von relevanten Gefährdungen. Der Selbstschutz der Kritischen Infrastrukturen soll gestärkt werden, indem die zuständigen Stellen integrale Schutzkonzepte erarbeiten und umsetzen. Bei den genannten Massnahmen geht es vielfach darum, bestehende Prozesse anzupassen und weiterzuentwickeln, damit die umfassende Koordination und ein abgestimmtes Vorgehen aller Akteure sichergestellt werden können. Dementsprechend erfolgt die Umsetzung der nationalen SKI-Strategie weitgehend dezentral und im Rahmen der bestehenden Zuständigkeiten.

Gemeinsames Verständnis durch SKI-relevante Lagedarstellung

Ein wichtiges Teilziel der SKI-Strategie besteht darin, Risiken und Verletzlichkeiten der Kritischen Infrastrukturen zu kennen, um darauf mit geeigneten Schutzmöglichkeiten zu reagieren. Ein künftig zu erstellendes SKI-Lagebild unterstützt dieses Ziel. Dazu soll ein Prozess zur Erfassung, Bewertung und Verfolgung der SKI-relevanten Aspekte und Entwicklungen etabliert werden. Dieser Prozess soll

- definieren, welche inhaltlichen Aspekte für die SKI-relevante Lagedarstellung systematisch erfasst und beurteilt werden;
- festlegen, wer für den Gesamtprozess und seine Elemente verantwortlich ist;
- aufzeigen, wie die unterschiedlichen SKI-relevanten Anspruchsgruppen in den Prozess der Lagedarstellung eingebunden werden.



Stefan Brem, Dr.,
Chef Risikogrundlagen und
Forschungs- und
Koordinationskoordination,
Bundesamt
für Bevölkerungsschutz,
Bern
stefan.brem@
babs.admin.ch

Das SKI-relevante Lagebild dient der Erarbeitung einer integralen, gegenwarts- und zukunftsorientierten Lagedarstellung zum Schutz Kritischer Infrastrukturen in der Schweiz. Hierfür zeichnen sich vier inhaltliche Schwerpunkte ab:

Gefährdungs- und Bedrohungsentwicklungen

Ein wichtiger Aspekt der Lagedarstellung resultiert aus der Frage, welche Ereignisse und Entwicklungen den Schutz Kritischer Infrastrukturen gefährden und bedrohen¹. Auf Bundesebene bestehen bereits zahlreiche Initiativen zur Gefährdungs- und Bedrohungsanalyse². Diese Analysen verfolgen jedoch unterschiedliche Zielsetzungen. Daher besteht die wesentliche Herausforderung darin, aus den Analysen die für den KI-Schutz relevanten Aspekte zu filtern und die gewonnenen Erkenntnisse so konkret wie möglich auf die Bedürfnisse der jeweiligen KI-Unternehmen auszurichten. Die daraus resultierende SKI-spezifische Gefährdungs- und Bedrohungsanalyse bzw. -bewertung legt damit den Grundstein für einen öffentlich-privaten SKI-Informationsaustausch z.B. im Hinblick auf mögliche Gefährdungen durch unsichere Informations- und Kommunikationstechnologie oder Wirtschaftsspionage. Neben sektorspezifischen Aussagen sollte das Augenmerk der staatlichen Seite vor allem auf den sektorübergreifenden Gefährdungen und Bedrohungen liegen.

Technologieentwicklungen

Der technologische Durchdringungsgrad moderner Infrastrukturen nimmt laufend zu. Diese Entwicklung ist unerlässlich, um die wachsenden Anforderungen an Infrastrukturen (z.B. Kosteneffizienz, Berücksichtigung umwelt- und klimapolitischer Anliegen, Steigerung der Leistungsfähigkeit) erfüllen zu können. Gleichzeitig steigt dadurch aber auch die Abhängigkeit von verschiedenen Infrastrukturkomponenten, die in den unterschiedlichen KI-Sektoren zum Einsatz kommen. Das kommt insbesondere bei der Verwendung von Informations- und Kommunikationstechnologie als Querschnittstechnologie in allen KI-Sektoren zum Ausdruck. Der Blick auf künftige Technologieentwicklungen spielt daher für die SKI-relevante Lage eine wichtige Rolle und sollte in eine SKI-spezifische technische Vorausschau münden. Zwei Fragestellungen sind dabei besonders wichtig:

■ Welche Technologieentwicklungen gefährden in welcher Form den Schutz der Kritischen Infrastrukturen?

■ Welche technologischen Entwicklungen tragen dazu bei, den Schutz und die Widerstandsfähigkeit Kritischer Infrastrukturen zu verbessern?

Infrastrukturentwicklungen

Informationen über die langfristigen Pläne und Vorhaben zur künftigen Infrastrukturentwicklung in der Schweiz sind ein weiterer Baustein der SKI-Lagedarstellung, weil darüber der

Der Blick auf künftige Technologieentwicklungen spielt daher für die SKI-relevante Lage eine wichtige Rolle und sollte in eine SKI-spezifische technische Vorausschau münden.

künftige Infrastrukturbedarf abgebildet wird. Informationen dazu werden unterschiedlich aufbereitet, z.B. in Form von Sachplänen, die für verschiedene KI-Sektoren³ erstellt werden, oder langfristigen Planungsdokumenten wie dem 2010 veröffentlichten Bericht «Zukunft der nationalen Infrastrukturnetze in der Schweiz». Für die SKI-relevante Lage sollten die darin enthaltenen Informationen ergänzt und auf folgende drei Aspekte zugeschnitten werden:

- Stärkere wechselseitige Betrachtung der Konsequenzen, die sich aus spezifischen Infrastrukturentwicklungen in einem Sektor für die davon abhängenden anderen Sektoren ergeben können (Vernetzung);
- Betrachtung der besonderen Risiken des zunehmenden Trends der Infrastrukturkollokation (z.B. Nutzung von Abwasserrohrleitungen für das Verlegen von Glasfaserkabeln)⁴;
- Definition der Anforderungen an die Sicherheit der Infrastrukturen nicht nur im Sinne der

Kurz & bündig

Für den Schutz Kritischer Infrastrukturen (SKI) ist der regelmässige Austausch von Informationen zwischen Behörden und Unternehmen unerlässlich. Dieser könnte in einem SKI-relevanten Lagebild gebündelt und aufbereitet werden. Das Lagebild würde Auskunft geben über vier Themenfelder: Gefährdungen und Bedrohungen, Technologie, Infrastruktur und regulatorische Entwicklungen. Die Erkenntnisse aus dem SKI-relevanten Lagebild könnten einmal jährlich in einer Veranstaltung der Behörden und den KI-Eigentümern/-Betreibern diskutiert werden, um gemeinsam den daraus resultierenden Schutzbedarf zu erörtern. Eine elektronische Plattform könnte die Arbeiten unterstützen, indem in einem geschützten Umfeld der Dialog zwischen den Beteiligten vertieft und relevante Informationen sowie Dokumente bereitgestellt werden.

Versorgungsqualität aus Konsumentensicht, sondern auch der Resistenz gegen Störungen, der Redundanz im Bereich der Vorbereitung/Prävention sowie der Wiederherstellungsfähigkeit (Recovery) im Ereignisfall.

Angesichts des hohen inhaltlichen Verknüpfungsgrades mit anderen Politikfeldern ist die Erstellung der SKI-relevanten Lage anspruchsvoll.

Regulatorische Entwicklungen

Schliesslich gilt es, das regulatorische Umfeld auf der nationalen und internationalen Ebene in seiner Bedeutung für SKI zu verfolgen. Von besonderer Bedeutung ist dabei die rechtsfelderübergreifende Betrachtung von vier zentralen Aspekten:

- Versorgungsziele (Grundschnitzniveau);
- Schutz- und Sicherheitsstandards;
- Anforderungen an Sicherheitsmassnahmen für KI-Unternehmen (z.B. Erarbeiten von Sicherheitsplänen, spezifische Anforderungen an besonders kritische Infrastrukturelemente);
- Überwachungs- und Verifikationsregimes.

Ziel sollte es sein, ein die sektorspezifischen Unterschiede berücksichtigendes kohärentes

regulatorisches Umfeld herzustellen, das dazu beiträgt, sektorübergreifende Aspekte (z.B. Sicherheit der Informations- und Kommunikationstechnologie) einheitlich zu behandeln. Hierbei spielt ein nationaler Regulatordialog eine besondere Rolle, um SKI-relevante Aspekte in koordinierter Weise in die Arbeit der sektorspezifischen Regulierungsbehörden einfließen zu lassen.

Dabei sind auch regulatorische Initiativen internationaler Organisationen zu beachten. Im europäischen Umfeld sind neben den Initiativen der Europäischen Kommission (z.B. Programm zum Schutz Europäisch Kritischer Infrastrukturen) auch die Arbeiten der sektorspezifischen Verbände und Organisationen (z.B. European Network of Transmission System Operators for Electricity, European Railway Agency) von Bedeutung. Diese internationalen Entwicklungen sollten ebenfalls in den nationalen Regulatordialog einfließen. Dabei wird auch zu klären sein, wie und durch wen internationale regulatorische Entwicklungen bereits erfasst werden, um Doppelspurigkeiten zu vermeiden. Die einzelnen Verbände könnten dabei eine wichtige Rolle spielen, indem sie Informationen aus dem Monitoring der Entwicklung in ihren Zuständigkeitsbereichen in diesen Dialog einfließen lassen.

Schlussfolgerungen

Angesichts des hohen inhaltlichen Verknüpfungsgrades mit anderen Politikfeldern ist die Erstellung der SKI-relevanten Lage anspruchsvoll. Von der Gesamtverantwortung für diesen Prozess ist die inhaltliche Zuständigkeit in Form der Beiträge zu den vier oben genannten Schwerpunkten zu unterscheiden. Die Prozessverantwortung beschreibt lediglich die Aufgaben, die mit dem Sicherstellen des Prozesses an und für sich verbunden sind. Die inhaltlichen Zuständigkeiten sollten davon – soweit sinnvoll – nicht berührt werden.

Ein wesentlicher Aspekt der Prozessverantwortung besteht in der Konkretisierung der Art und Weise, wie die unterschiedlichen Akteure für das SKI-relevante Lagebild zusammenarbeiten sollten. Dabei sind folgende Punkte zu berücksichtigen:

- Die SKI-relevante Lage sollte *mindestens einmal jährlich* aktualisiert werden, wobei sich zumindest in der Anfangsphase die Arbeiten auf jene Bereiche beschränken könnten, in denen bei der Umsetzung der SKI-Strategie der grösste Handlungsbedarf festgestellt wird. Dabei ist die enge Abstimmung mit den sektorspezifischen öffentlichen und privaten Partnern erforderlich.

Literatur

Die Informationen zu diesem Artikel basieren auf einer internen Studie des BABS:

- HEIKO BORCHERT, Öffentlich-Private SKI-Kooperation. Sicherheitsarchitektur und Sicherheitsdialog: Bestandaufnahme und Entwicklungsoptionen, Luzern: Sandfire AG, 2011.
- Weiterführende Informationen zum SKI-Programm: <www.infraprotection.ch>.

Fussnoten

- ¹ In Einklang mit der Definition des BABS wird Gefährdung als ein Ereignis oder eine Entwicklung mit negativen Auswirkungen, die Bedrohung als eine akute und manifeste Gefährdung definiert.
- ² Ohne Anspruch auf Vollständigkeit können genannt werden: Berichte zur Sicherheitspolitik (Bereich Sicherheitspolitik, VBS), Sicherheit Schweiz: Jahresberichte des Nachrichtendienstes des Bundes (NDB, VBS), Risiken Schweiz (BABS), SKI-Programm (BABS), Gefährdungs- und Verwundbarkeitsanalysen der wirtschaftlichen Landesversorgung (BWL), Perspektiven 2025 (Perspektivstab Bundeskanzlei), Krisenmanagementausbildung (Bundeskanzlei), Risikomanagement Bund (Eidg. Finanzverwaltung, EFD).
- ³ Es gibt z.B. Sachpläne für den Strassen-, Schienen- und Luftverkehr, für Übertragungsleitungen im Bereich der Stromwirtschaft, für Windenergieanlagen sowie für Geologische Tiefenlager. Im Bereich der Kommunikationsanlagen hat das BAKOM Empfehlungen für die Koordination der Planungs- und Bewilligungsverfahren erarbeitet: <<http://www.are.admin.ch/themen/raumplanung/00240/01406/index.html?lang=de>> und <<http://www.are.admin.ch/themen/raumplanung/00242/01413/index.html?lang=de>> (3.3.2012).
- ⁴ «Eine Bündelung [der Infrastrukturen in Korridoren, Anm. d. Verf.] scheint vor allem bei Strassen-, Schienen-, Kabel- und Rohrleitungsnetzen vielversprechend zu sein»; Generalsekretariat UVEK, Zukunft der nationalen Infrastrukturnetze in der Schweiz, Bericht des Bundesrates vom 17. September 2010, Bern 2010, 61, Fn. 139.

- Die SKI-relevante Lage könnte in einer neuen *Veranstaltung* präsentiert werden. Zu den Teilnehmern gehören die Verantwortlichen der KI-Unternehmen und die Vertreter der relevanten Behörden auf Stufe Bund und Kantone. Der gewählte Delegierte des Sicherheitsverbundes Schweiz könnte ebenso eingeladen werden wie die Spitzen wichtiger kantonaler Gremien (z.B. Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren [KKJPD], Regierungskonferenz Militär Zivilschutz Feuerwehr [RK MZF]).
- Das BABS könnte diese Veranstaltung in Zusammenarbeit *mit anderen Bundesämtern* gemeinsam organisieren. Naheliegend ist z.B. die enge Abstimmung mit dem Bundesamt für wirtschaftliche Landesversorgung. Jahresveranstaltungen beider Ämter könnten miteinander kombiniert werden, um das SKI-relevante La-gebild vorzustellen.
- Vertreter des *Nachrichtendienstes des Bundes* (NDB) spielen bei diesen Veranstaltungen ebenfalls eine wichtige Rolle. Sie könnten beispielsweise die Erkenntnisse des Jahresberichts

«Sicherheit Schweiz» für die Bedürfnisse der KI-Unternehmen konkretisieren, diesen die Bedrohungslage darlegen und mit diesen gemeinsam mögliche Schutzmassnahmen erörtern.

- Darüber hinausgehende Informationen sowie weiterführende Grundlagendokumente könnten dem Nutzerkreis der KI-Eigentümer/-Betreiber

Der Nachrichtendienst des Bundes könnte die Erkenntnisse für die Bedürfnisse der KI-Unternehmen konkretisieren, die Bedrohungslage darlegen und mögliche Schutzmassnahmen erörtern.

auch über eine *geschützte elektronische Plattform* zur Verfügung gestellt werden, soweit dazu aus Sicht der Nutzer ein Bedarf besteht. Diese Plattform könnte zudem auch für den regelmässigen Dialog zwischen den Behörden und den KI-Eigentümern/-Betreibern genutzt werden. ■

Neuerscheinung aus dem Schulthess Verlag



Von der Lochkarte zum Mobile Computing

20 Jahre Datenschutz in der Schweiz

Datenschutz-Forum Schweiz (Herausgeberschaft)

Das Datenschutz-Forum Schweiz hat aus Anlass des 20-jährigen Jubiläums des Schweizer Datenschutzgesetzes eine Festschrift herausgegeben. Nicht erst seit 20 Jahren ist Datenschutz ein Thema, sondern bereits in den 70er-Jahren kam in der Schweiz die Diskussion auf. In der vorliegenden Publikation werden in einem Rückblick die Anfänge des schweizerischen Datenschutzes sowohl aus juristischer als auch technischer Sicht erläutert. Weiter wird auf aktuelle Themen eingegangen – Internet-Veröffentlichungen, Gesundheitswesen, Arbeitswelt – und untersucht, inwiefern das Bauchgefühl bei Datenschutzentscheiden eine Rolle spielt. Bei der Autorenschaft wurde auf eine ausgewogene Vertretung von Privaten, Politik, Wirtschaft und Wissenschaft geschaut. Die Beiträge geben einen guten Überblick über 20 Jahre Datenschutz – und einen Ausblick auf die weitere Entwicklung.

Herausgeberschaft:
Datenschutz-Forum Schweiz

Erschienen	April 2012
ISBN	978-3-7255-6495-8
	162 Seiten, broschiert
Preis	CHF 58.00

Schulthess Juristische Medien AG
Zwingliplatz 2, Postfach, CH-8022 Zürich/Switzerland
Telefon +41 44 200 29 29, Fax +41 44 200 29 28
buch@schulthess.com, www.schulthess.com

Schulthess §

Meine Bestellung

- 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 131.00** (inkl. Versandkosten)

Name _____ Vorname _____

Firma _____

Strasse _____

PLZ _____ Ort _____ Land _____

Datum _____ Unterschrift _____

Bitte senden Sie Ihre Bestellung an:

Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich

Telefon +41 44 200 29 19

Telefax +41 44 200 29 18

E-Mail: zs.verlag@schulthess.com

Homepage: www.schulthess.com

Schulthess 