Zeitschrift für Datenrecht und Informationssicherheit

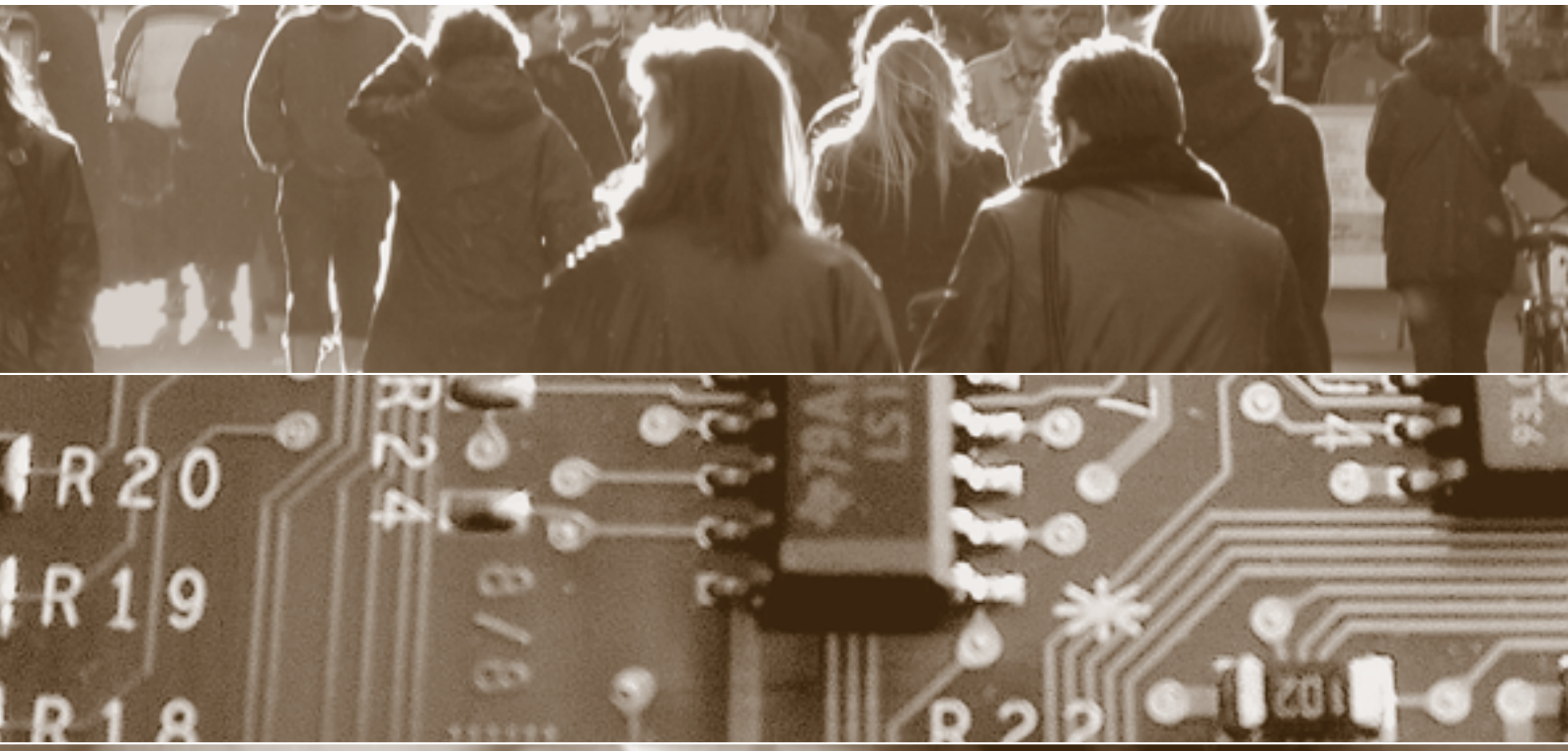
digma

www.digma.info 12. Jahrgang, Heft 1, April 2012

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

Schulthess §

inhalt

fokus

Schwerpunkt:
Sensor-Actor-Netze

Lagebild für Kritische Infrastrukturen

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.

Sicherheit im Energienetz der Zukunft

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.

PET – ein Konzept harrt der Umsetzung

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.

Privatsphäre trotz Intelligenter Zähler

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?

impressum

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. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Publicitas Publimag AG, Mürtschenstrasse 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 Datenschutzszene.

report

forum

Transfer

Private Smartphones im Geschäftsumfeld

Roland Portmann, Prof., Dozent für IT-Security, Hochschule Luzern – Technik & Architektur, externer Fachexperte bei ISO/IEC 27001 Zertifizierungen, Luzern
roland.portmann@hslu.ch

Moderne Smartphones verdrängen die klassischen Mobiltelefone. Über 50% der verkauften Geräte unterstützen neben der Telefonie den Zugriff auf Internet. Die Mail- und Kalenderapplikationen werden vom firmeneigenen Mail-Server auf aktuellem Stand gehalten, tausende von Apps versprechen Unterstützung in allen Lebenssituationen. Die firmeninternen Regelungen bezüglich der Verwendung der Smartphones sind häufig veraltet und adressieren die aktuelle Risiko-Situation nur ungenügend.

BYOD («Bring your own Device») hat Eingang in die IT-Strategie vieler Firmen gefunden. Damit wird die Problematik adressiert, dass heute zunehmend Arbeitnehmer für verschiedene Arbeitgeber arbeiten. Mit den Smartphones und den Tablets gewinnt diese Entwicklung zusätzlich an Aktualität und erfordert entsprechende Regelungen und Massnahmen zur Gewährleistung eines ausreichenden Sicherheitsniveaus.

Technische Möglichkeiten

Die technischen Möglichkeiten der modernen Smartphones (iPhone, Android, Windows Phone 7) sind fantastisch. Die Durchsatzrate der Internetanbindung kann private ADSL-Internet-Anbindungen durchaus übertreffen. Die E-Mail- und Kalender-Applikationen sind übersichtlich und einfach zu bedienen. Der Abgleich mit Mail-Servern von Firmen und Cloud-Anbietern kann auch von technisch nicht versierten Personen konfiguriert werden und funktioniert in der Regel sehr zuverlässig. Für jede Lebenssituation gibt es eine App. Die Multimedia-Funktionen sind überwältigend. Die Social Networks sind nahtlos integriert. Die Integration und Zusammenarbeit der verschiedenen Apps ist weitaus enger, als man es von modernen Arbeitsplatzbetriebssystemen gewohnt ist.

Der moderne Arbeitsmensch

Diese Geräte unterstützen die Mobilität des modernen Arbeitsmenschen, der zunehmend keinen festen Arbeitsplatz mehr besitzt, der gleichzeitig an vielen Projekten und für mehrere Arbeitgeber arbeitet, der keine fixen Arbeitszeiten kennt und durchaus auch an Sonntagen geschäftliche E-Mails beantwortet und dafür unter der Woche auf dem Tennisplatz anzutreffen ist. Das Smartphone erleichtert diese Arbeitsweise und auch das Freizeitverhalten: Neben den erwähnten Kalender- und E-Mail-Funktionalitäten, werden die Fahrpläne von Zügen unter Berücksichtigung allfälliger Verspätungen effizient online abgefragt, das SBB-Ticket wird mit einer App gekauft, das gute Restaurant in der Nähe findet man mit den Location Based Services, über die Wetter- und Skiverhältnisse geben spezialisierte Apps Auskunft, Wartezeiten überbrückt man mit dem Lesen der topaktuellen News der verschiedenen Anbieter, Zeichnung auf Whiteboards in Sitzungen werden rasch fotografiert und direkt an Arbeitskollegen übermittelt, Finanztransaktionen werden durchgeführt und vieles mehr. In Zukunft wird das Smartphone auch zu einem wichtigen Zahlungsmittel.

Zugriff auf Firmeninfrastruktur

In der Praxis erlauben viele Firmen den Zugriff von privaten Smartphones auf die firmeneigene Exchange-Infrastruktur (E-Mail und Kalender). Die Firmen wollen von der besseren Erreichbarkeit der Mitarbeiter auch ausserhalb der Arbeitszeiten profitieren. Mittels VPN können Netzwerkverbindungen in Firmennetzwerke aufgebaut werden. Für Mitarbeiter können auch weitere Dienste, insbesondere Cloud-Angebote interessant und effizient sein. Dropbox erlaubt beispielsweise die Synchronisation von Dateien auf dem Arbeitsplatzrechner mit dem Smartphone. Viele Firmen setzen die Smartphones zudem als Security-Device beispielsweise für den Passwort-Rücksetzungsprozess ein. Angebote von diversen Providern erlauben heute die interne Telefonie auf Smartphones zu migrieren. Dies erspart die Anschaffung einer Telefonieanlage und unterstützt mobile Arbeitsplätze nahezu ideal.

Risiken

Dieser Einsatz von privaten Smartphones bringt eine Reihe von Risiken mit sich. In viele Firmen ist es beispielsweise erlaubt und üblich, im internen E-Mail-Verkehr vertrauliche Informationen zu versenden. Auch E-Mails an externe Empfänger können durchaus sensitive Informationen enthalten. Diese E-Mails sind auf Smartphones weit weniger gut geschützt, als in internen IT-Infrastrukturen oder auf Notebooks, die einen State-of-the-art-Schutz (z.B. verschlüsselte Harddisks) besitzen. Generell können Smartphones weit weniger gut geschützt werden als moderne Notebooks. Zudem sind auf den Smartphones die Credentials (Name und Passwort) zu den internen E-Mail-Accounts gespeichert. Auch weitere Informationen wie Fotos von Handy-Kameras (z.B. von Whiteboards in Sitzungen), mit Dropbox synchronisierte Dateien, Adress- und Kalenderinformationen können, wenn sie in falsche Hände geraten, grossen Schaden anrichten. Diese Informationen können nicht nur durch den Verlust des Smartphones in falsche Hände gelangen. Stark steigend ist das Risiko, dass über Market-Places installierte Apps unerwünschte Datentransfers durchführen. Die Gefahr einer Verseuchung der Smartphones mit Viren ist gross geworden. Weitere Risiken entstehen durch die enge Verknüpfung der verschiedenen Apps mit den Social-Network-Funktionen. Die Vermischung von Informationen des privaten und des geschäftlichen Umfeldes mag nicht in allen Fällen gewünscht und sinnvoll sein.

Massnahmen

Als wichtigste Massnahme muss die Verwendung von Smartphones im geschäftlichen Umfeld geregelt werden. Ein Reglement kann die folgenden Punkte enthalten:

- Der Bildschirm des Smartphones muss mit einer PIN oder einem Entsperrmuster gesperrt sein.
- Es ist verboten, die Sicherheitsmechanismen eines Smartphones zu umgehen (Jailbreak eines iPhones, Rooten eines Android Phones), da damit viele Sicherheitsmechanismen ausgeschaltet werden.
- Es muss sichergestellt werden, dass keine älteren Betriebssystemversionen eingesetzt werden, da diese grössere Sicherheitslücken aufweisen können. Daher können in einem Reglement die minimale Version für iOS, Android und Windows Phone 7 festgelegt werden.
- Daten auf einem Smartphones können gelöscht werden, falls die E-Mails über einen Exchange-Server synchronisiert werden. Daher muss das Vorgehen bei einem Verlust des Smartphones klar geregelt sein.
- Ein Reglement kann Empfehlungen enthalten, welche Apps installiert werden dürfen und auf welche Apps verzichtet werden muss.
- Es können Vorschriften oder Empfehlungen bezüglich zu installierenden Antiviren-Programmen für Smartphones ins Reglement aufgenommen werden.

Da Smartphones meistens auch als E-Mail-Client verwendet werden, kann es sinnvoll sein, die Verwendung von E-Mail generell neu zu regeln. Insbesondere kann es notwendig sein, restriktivere Regelungen bezüglich dem internen Versenden von vertraulichen Informationen zu erlassen. Alternativ könnte eine Verschlüsselung von vertraulichen E-Mails eingeführt werden, da diese nicht ohne Weiteres auf einem Smartphone gelesen werden können (ausser man importiert das Verschlüsselungszertifikat auf das Smartphone).

Moderne Exchange-Versionen und/oder Zusatz-Produkte erlauben die Definition und die Durchsetzung von Sicherheitspolicies bei der Anbindung von Smartphones. So kann beispielsweise auch bei privaten Geräten durchgesetzt werden, dass E-Mails nur synchronisiert werden können, wenn eine Bildschirmsperre eingerichtet ist.

Zusammenfassung

Es ist in vielen Umgebungen nicht sinnvoll und zeitgemäss, die Verwendung von Smartphones für geschäftliche Zwecke zu verbieten. Die stark zunehmenden mobilen Arbeitsformen werden durch die Möglichkeiten des Smartphones stark unterstützt. Bei einem korrekten Einsatz können die Vorteile überwiegen und die Risiken in viele Firmen auf ein akzeptables Niveau gesenkt werden. ■

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info
erscheint vierteljährlich

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 §