Heid Schiefer
Rechtsanwälte

UBIT
Unternehmensberater
Buchhalter
IT-Dienstleister

e_Rechtstag 2013
Cloud Computing rechtlich betrachtet: Informationssicherheit und Datenschutz
23.4.2013

Cloud Computing = „Hype“?

News

Gartner: Public cloud market to grow 18.5% this year

Infrastructure as a Service (IaaS) is fastest growing segment of the cloud market, growing at 42% annually

By Brandon Butler, Network World
February 28, 2013 11:20 AM ET

Network World - The global public cloud computing market will grow 18.5% in 2013 to $131 billion, up from $111 billion last year, research firm Gartner predicts.

Through the next three years, cloud spending is predicted to total $677 billion, with almost half of that spending made up of cloud advertising.

(http://m.networkworld.com/news/2013/022813-gartner-public-cloud-267223.html)

Sicherheitsrelevante Gründe gegen Cloud Computing

- **Fehlende Transparenz**
  - Wo befinden sich die Daten genau?
  - Wie wird mit den Daten umgegangen?
  - Wie sind branchenspezifische Anforderungen an Sicherheitsüberprüfungen umsetzbar?
  - Risikoabschätzung?
- **Vermengung von Kunden, Daten und Diensten**
  - Integritätsverlust bei einzelnen Assets kann Auswirkungen auf andere Assets haben
  - Schlecht aufgesetzte Anwendungen können die Sicherheit der Plattform kompromittieren
  - Sind die eingesetzten Komponenten für eine solide Abgrenzung ausgelegt?
- **Verlust der Kontrolle über Daten und Prozesse**
- **Abhängigkeit vom Anbieter**

Sicherheitsrelevante Gründe gegen Cloud Computing

- **Schwierigkeiten von Backups**
  - Backups nur mit erheblichem Aufwand selbständig umsetzbar
  - Ansonsten Abhängigkeit vom Cloud Provider
- **Schwierigkeiten bei Migration**
  - Komplexe Abhängigkeiten und Inkompatibilitäten können Migration aufwändig machen
- **Juristische Konflikte bezüglich Datenschutz**
- **Juristische Eigenverantwortung**
- **Einbußen beim Know-how**
  - Insourcing wird zum kompletten Neuaufbau der IT-Abteilung
- **Zentraler Angriffspunkt**
  - Kompromittierung der Cloud kann potentiell alle ausgelagerten Mechanismen kompromittieren

Risikofaktor Mensch

heise Security

News Hintergrund Erste Hilfe

Security > News > 7-Tage-News > 2013 > KW 13 > Benutzer von Amazon S3 geben unbeabsichtigt Mill

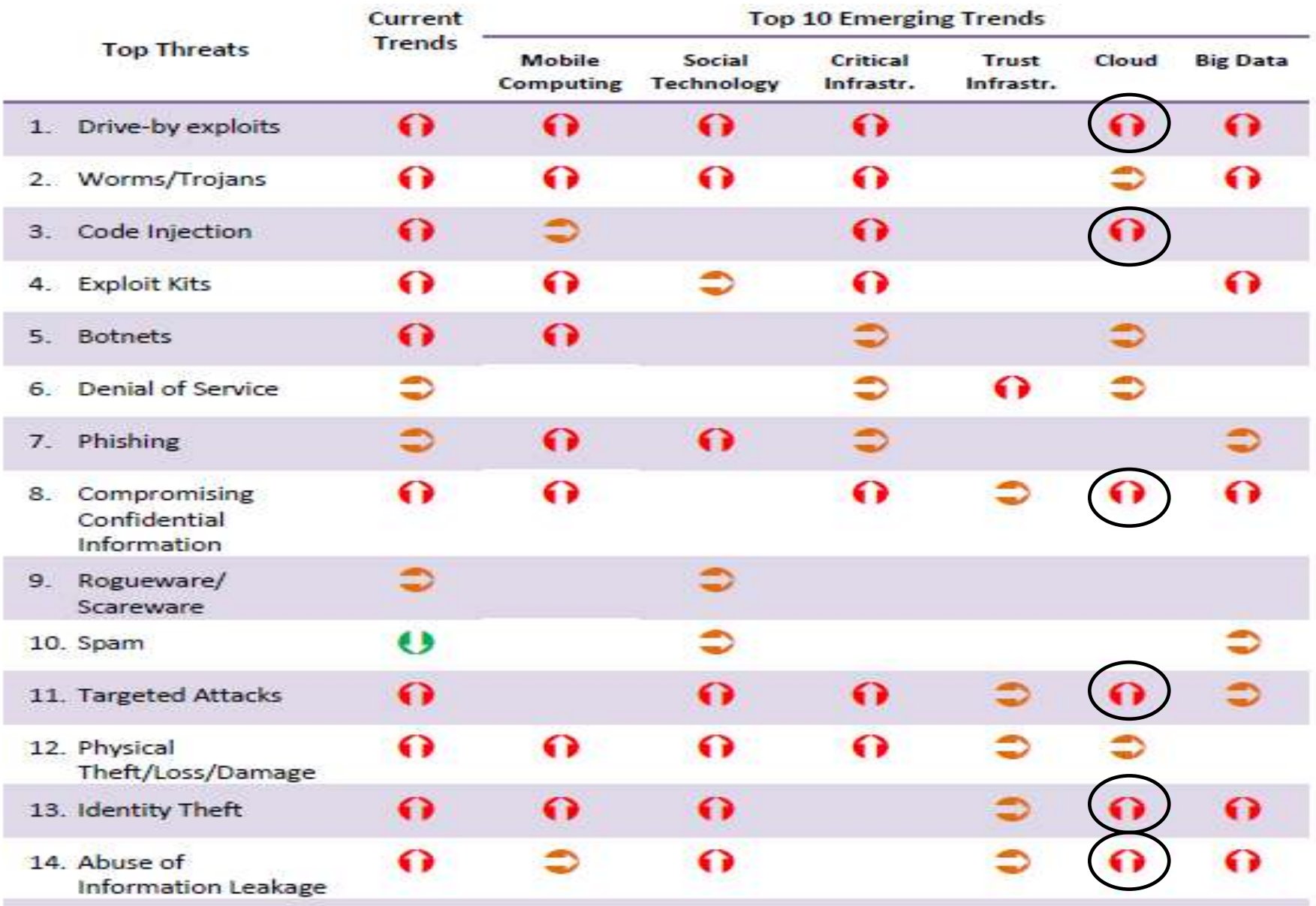
28.03.2013 12:48 « Vorige | Nächste »

Benutzer von Amazon S3 geben unbeabsichtigt Milliarden sensitiver Dokumente frei

vorlesen / MP3-Download

Amazons Simple Storage Service (S3) finden viele Firmen ungemein praktisch. Zu moderaten Preisen steht Speicherplatz im Netz zur Verfügung. Allerdings scheint vielen Benutzern nicht klar zu sein, dass dort gelagerte Daten auch entsprechend geschützt werden müssen. Das ergab jedenfalls eine Untersuchung der Sicherheitsspezialisten von S7, deren Ergebnisse sie auf ihrem Blog veröffentlichten: Von rund 12328 "buckets" (Verzeichnissen) waren 1951, also knapp ein Sechstel, öffentlich zugänglich (public) und 10377 mit einem Zugriffsschutz versehen.

Und das dürfte kaum Absicht sein. Denn in den öffentlich zugänglichen Verzeichnissen befanden sich laut S7 126 Milliarden Dateien mit Daten, die kaum für die Öffentlichkeit gedacht sein dürften. Die Untersuchung einer Stichprobe von 40 000 Files brachte Geschäftsberichte, persönliche Fotos, Zugangsdaten für diverse Dienste und so weiter zu Tage.



ENISA Threat Landscape 2012-09-28, 3

Beispiel Evernote

heise Security

News | Hintergrund | Erste Hilfe

Security › News › 7-Tage-News › 2013 › KW 9 › Notiz-Dienst Evernote wurde gehackt

03.03.2013 11:52 « Vorige | Nächste »

Notiz-Dienst Evernote wurde gehackt

vorlesen / MP3-Download

Die Betreiber des weltweit von 50 Millionen Anwendern genutzten Online-Notizbuchs Evernote haben alle Passwörter zurückgesetzt, nachdem sich Kriminelle Zugang zu sensiblen Daten verschafft hatten. Einigen Berichten zufolge geschah das bereits am 28. Februar. Dabei konnten die Eindringlinge offenbar verschlüsselte Passwörter, E-Mail-Adressen und Nutzernamen der Evernote-Kunden ergattern. In einer Mitteilung an die Anwender heißt es: "Evernotes Ausführungs- und Sicherheitsteam hat eine verdächtige Aktivität im Evernote-Netzwerk entdeckt und blockiert, die als koordinierter Versuch des Zugriffs auf sichere Bereiche des Evernote-Dienstes erscheint."

Sicherheitshalber habe man alle Anwender-Passwörter zurückgesetzt. Die Untersuchungen hätten ergeben, dass weder Inhalte kopiert, geändert oder gelöscht noch Bezahlinformationen für Premium- oder Geschäftsdienste gestohlen worden seien.

Sicherheitsrelevante Gründe für Cloud Computing

- **Skaleneffekte: effiziente Implementierung von Sicherheitsmaßnahmen für Cloud Provider einfacher**
- **Reduzierung der Anzahl der Angriffspunkte**

Datenschutzrechtliche Anforderungen

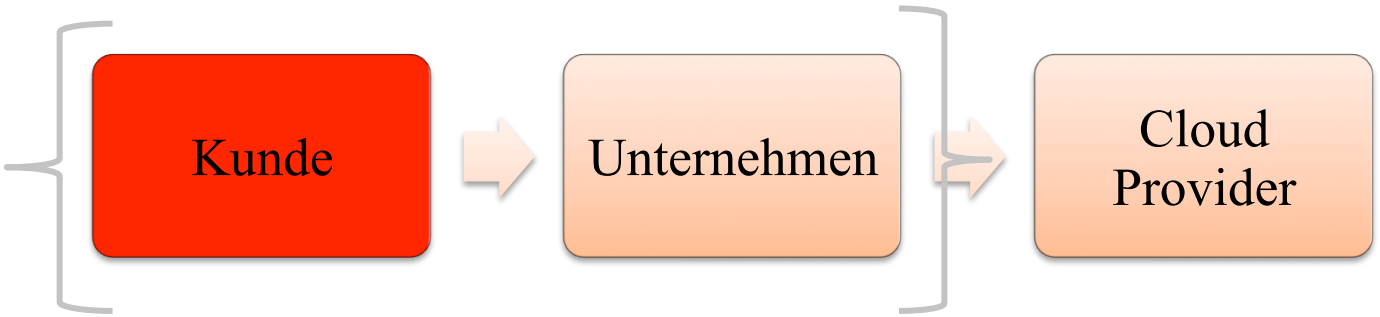
- **Cloud Provider muss ausreichende Gewähr für rechtmäßige und sichere Datenverwendung bieten**
- **AG hat entsprechende Vereinbarungen zu treffen und sich zu überzeugen, dass Cloud Provider tatsächlich entsprechende Maßnahmen getroffen hat (§ 10 Abs 1 DSG)**
- **Datenübermittlung genehmigungsfrei**
  - in den EU/EWR-Raum
  - in sichere Drittstaaten (zB Schweiz, Israel)
  - an US-Unternehmen, die sich Safe Harbour-Statuten unterworfen haben

Vertraglich zu klären

- **Zertifizierungen des Cloud Providers**
- **Definition der Rechenzentren und Subunternehmer**
- **Verpflichtung von Mitarbeitern und Subunternehmer zur Einhaltung des Datengeheimnisses**
- **Abgrenzung der datenschutzrechtlichen Verantwortlichkeiten und Kontrollrechte des Auftraggebers**
- **Release Management**
- **Service Levels**
- **Keine einseitigen Vertragsänderungen**
- **Information bei Wechsel von Subunternehmern**
- **Mitwirkung des Cloud Providers bei der Datenrückgabe nach Vertragsbeendigung, Datenformate**
- **….** (vgl EuroCloud / WKÖ / ADV / ASI, Leitfaden Cloud-Verträge)

Rechtsdurchsetzung

Ansprüche Kunde => Unternehmen



Ansprüche Kunde => Unternehmen

- **Cloud Provider ist Erfüllungsgehilfe**
- **Erfüllungsgehilfenhaftung § 1313a ABGB**

Vertragliche Haftungsbeschränkungen?

	Vorsatz / Grobe Fahrlässigkeit		Leichte Fahrlässigkeit	
	AGB	**Aus-gehandelt**	**AGB**	**Aus-gehandelt**
Unter-nehmer	**Nein** (OGH 29.5.1996, 3 Ob 2004/96z)	**Ja**, außer bei krasser Sorglosig-keit (KBB § 879 Rz 11 lit g)	Grundsätzlich **Ja** (OGH 29.5.1996, 3 Ob 2004/96z) **Nein**, soweit dem Vertragspartner das Risiko eines technischen Missbrauchs innerhalb der eigenen Sphäre durch Dritte zugewiesen werden soll (vgl OGH 29.6.2000, 22 Ob 133/99y)	**Ja**
Ver-braucher	**Nein** (§ 6 Abs 1 Z 9 KSchG)		**Nein** bei generellem Ausschluss (OGH 20.3.2007, 4 Ob 221/06p)	**Ja**

Ansprüche Unternehmen => Cloud Provider

Ansprüche Unternehmen => Cloud Provider

- "Most legal issues involved in cloud computing will currently be resolved during contract evaluation (ie, when making comparisons between different providers) or negotiations. The more common case in cloud computing will be selecting between different contracts on offer in the market (contract evaluation) as opposed to contract negotiations. However, opportunities may exist for prospective customers of cloud services to choose providers whose contracts are negotiable."
  (ENISA, Cloud Computing – Benefits, risks and recommendations for information security, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment)

Ansprüche Unternehmen => Cloud Provider

- "Standard contract clauses may deserve additional review because of the nature of cloud computing. The parties to a contract should pay particular attention to their rights and obligations related to notifications of breaches in security, data transfers, […]. Because the cloud can be used to outsource critical internal infrastructure, and the interruption of that infrastructure may have wide ranging effects, the parties should carefully consider whether standard limitations on liability adequately represent allocations of liability"
  (ENISA, Cloud Computing – Benefits, risks and recommendations for information security, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

Ansprüche Unternehmen => Cloud Provider

- WE … WILL NOT BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE … WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE THE SERVICES, INCLUDING AS A RESULT OF ANY (I) TERMINATION OR SUSPENSION OF THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS, … (III) WITHOUT LIMITING ANY OBLIGATIONS UNDER THE SLAS, ANY UNANTICIPATED OR UNSCHEDULED DOWNTIME OF ALL OR A PORTION OF THE SERVICES FOR ANY REASON, INCLUDING AS A RESULT OF POWER OUTAGES, SYSTEM FAILURES OR OTHER INTERRUPTIONS; (… (D) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR CONTENT OR OTHER DATA. (http://aws.amazon.com/de/agreement/)

Ansprüche Unternehmen => Cloud Provider

- 13.11 Governing Law; Venue. The laws of the State of Washington, without reference to conflict of law rules, govern this Agreement and any dispute of any sort that might arise between you and us. Any dispute relating in any way to the Service Offerings or this Agreement where a party seeks aggregate relief of $7,500 or more will be adjudicated in any state or federal court in King County, Washington. You consent to exclusive jurisdiction and venue in those courts. We may seek injunctive or other relief in any state, federal, or national court of competent jurisdiction for any actual or alleged infringement of our, our affiliates, or any third party's intellectual property or other proprietary rights. The United Nations Convention for the International Sale of Goods does not apply to this Agreement. (http://aws.amazon.com/de/agreement/)

Ansprüche Unternehmen => Cloud Provider

- **„Take it or leave it“ - Vertragsbedingungen**
- **Anwendbares Recht**
  - Rechtswahl (Art 3 Rom I-VO)
  - Recht des Staates, in dem der Dienstleister den gewöhnlichen Aufenthalt hat (Art 4 Abs 1 lit b Rom I-VO)
  - => idR nicht Österreich
- **Gerichtsstand**
  - Vertraglich vereinbarter Erfüllungsort (Art 5 EuGVVO)
  - => idR nicht Österreich
- **=> Rechtsdurchsetzung auf Grundlage ausländischen Zivilrechts im Ausland**

Weiterführende Informationen

- **www.eurocloud.at**

Heid Schiefer
Rechtsanwälte

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Ralf Blaha LL.M.

Heid Schiefer Rechtsanwälte OG E-Mail: office@heid-schiefer.at Internet: www.heid-schiefer.at

Kanzleisitz: 1030 Wien, Landstraßer Hauptstraße 88/2-4
Tel: +43 (0)1 9669 786, Fax: +43 (0)1 9669 790

Niederlassung Klagenfurt: 9020 Klagenfurt, Domplatz 1
Tel: +43 (0)463 5002 32, Fax: +43 (0)463 2655 26 4945

Niederlassung Salzburg: 5020 Salzburg, Rainbergstraße 3a
Tel: +43 (0)662 8406 48, Fax: +43 (0) 662 8450 33

Sprechstelle St. Pölten: 3100 St. Pölten, Niederösterreichring 2, Haus D
Tel: +43 (0)2742 233 55, Fax: +43 (0)2742 233 55 10