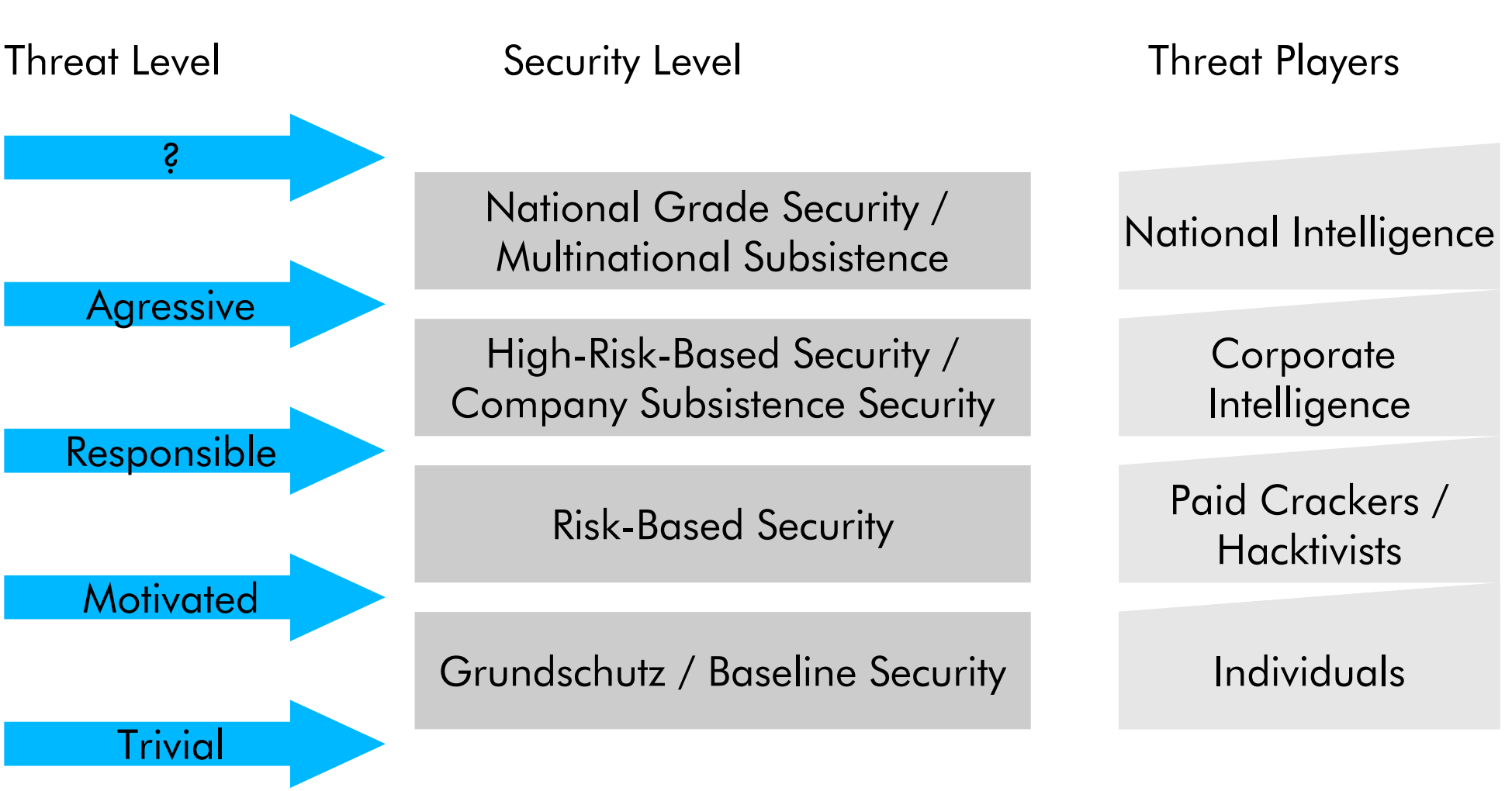
Cloud Security?

21. März 2013, Dr. Marcus Holthaus

- Wie sicher können wir sein?
- Über die Cloud
- Kopf voran in die Cloud!
- Datenschutz im Cloud-Zeitalter

IMSEC GmbH, Sonnhaldenstrasse 87, CH 6331 Hünenberg
+41 41 780 00 11, +41 780 00 21, http://www.imsec.ch, info@imsec.ch, CHE-104.991.590 MWST

Security Levels



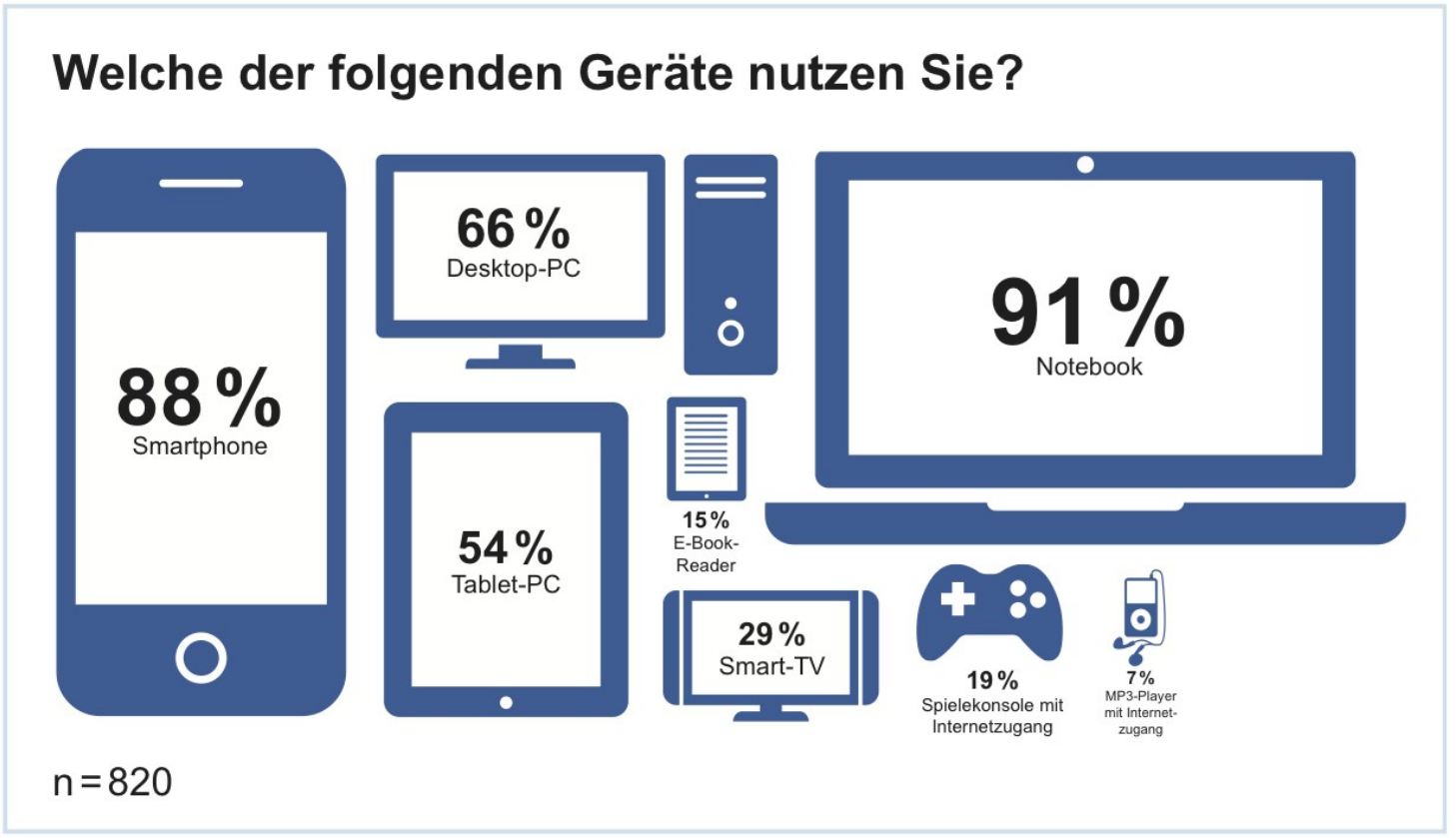
IMSEC

Wo steht Ihr Provider?

Security-Realitäten KMU

- Typischerweise massiver Projektstau
- Überrant mit BYOD und BYOS (Doodle, Dropbox etc.)
- Zugelassene Heterogenität (Macs, iPads, diverse Tablets, Linux-Clients)
- Gewünschte Flexibilität von Arbeitsort und Arbeitszeit führt zu fehlenden Off-Zeiten der zentralen Systeme
- Hohe Anforderungen an internes Zugriffskontrollsystem, v.a. hinsichtlich Dynamik
  - oft: „alle dürfen alles“ oder „viele dürfen vieles“
  - oft auch „Chef darf alles“ oder „Admin darf alles“
- Interne IT selten gross genug für
  - ISO 27000 / ISMS
  - Service Management / ITIL / ISO 20000
- Externe IT-Provider selten zertifiziert und selten aware
  - Unterschiedliche Branchenanforderungen
- Fazit
  - Gute Security ist aufwändig!
  - Gute Security lässt den Mitarbeiter seine Arbeit unbeeinträchtigt ausführen – das ist ein hehres Ziel und steht oft im Widerspruch zu Flexibilität und Dynamik.
  - Die meisten technologischen Probleme lassen sich durch Cloudsourcing lösen.

Geräte-Nutzung



Quelle: ibi research / Internet World Messe 2013: Digitalisierung der Gesellschaft (www.ibi.de) ; zitiert nach http://bernetblog.ch/2013/03/21/mobile-website-die-k-o-kriterien/

Security-Realitäten KMU

- Schwachstellen auf allen Ebenen
  - Netzwerk-Devices
  - Betriebssystem
    - Der Patch-Level von Windows-Systemen lässt zu wünschen übrig!
    - Usability vs. Security beim Patchen
  - Libraries
    - Selten Patches für Libraries
      - vgl. Schwachstelle in Universal Plug and Play (UPnP)
  - Anwendungen
    - Viele Hersteller proprietärer Software verteilen keine Patches
    - Programmierer beachten Application Security Hints oft nicht
    - Web-Anwendungen ständig angreifbar
  - Mitarbeiter
    - gemessen an Dynamik, Flexibilität, Leistung – selten an sicherem Verhalten
- Kein Sensorium
  - Logs höchstens zur Fehlerbehebung, selten für proaktive Angriffserkennung
    - Keine SIEMs
  - Selten: Definierte Kommunikationsmatrizen und interne Firewalls
  - Sicherheitslöcher werden nur wahrgenommen, wenn sie Funktionalitäten stören
  - Bei Störungen wird zuerst Sicherheit ausgeschaltet, weil sie die Funktionen verkompliziert
  - „Never change a running system“
- Security-Vorfälle haben in der Regel keine Konsequenzen

Security-Realitäten KMU

- Virenscanner erkennen nicht alle Schädlinge, v.a. nicht ganz neue!
  - (Quelle: c't, 5/2013, S. 81) --- bezieht sich nur auf Trojaner!

Alter	Avira	Avira (free)	McAfee	Symantec	Eset	Kaspersky	Avast (free)	Avast	Trend Micro	Bitdefender	F-Secure	G Data	AVG	AVG (free)	Microsoft	Panda	Anzahl
> 1 Jahr	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
≥ 1 Woche	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	81
≥ 1 Wo., 1 neu	0	0	0	0	0	0	0	0	0	0	0	0	0,5	0,5	0	0	13
≥ 1 Wo., 1 neu	0	0	1	1	1	0	0	0	0	0	0	1	0,5	0,5	1	0	12
< 1 Tag	0	0	0	1	2	5	2,5	4	1	3	0	7,5	10,5	10,5	11	19	25
< 1 Tag	1	1	2	3	1	2	4,5	5,5	0	7	6	5,5	7,5	7,5	7	6	29
< 1 Tag	0	0	0	0	1	3	1,5	1,5	0	2	2	3	2	2	3	3	3
< 1 Tag	0	0	0	0	2	0	1	1	0	0	0	1	1	1	0	2	2
< 1 Tag	0	0	0	0	0	1	0,5	0,5	0	1	0	1,5	1,5	2	3	3	4
< 1 Tag	0	0	0	0	0	0	0,5	0,5	2	0	2	0,5	0	0	2	2	2
< 1 Tag	0	0	0	0	1	0	0,5	0,5	0	0	1	0,5	0,5	0,5	0	0	1
< 1 Tag	0	0	0	0	0	0	12,5	11,5	24	25	36	29	41	42	43	43	74
Summe	1	1	3	5	8	11	23,5	25	27	38	47	49,5	65	66,5	70	78	248

Der Übersichtlichkeit halber wurden alle älteren Samples zu einer Zeile zusammengefasst. Die anderen wurden ganz grob anhand von Ähnlichkeit des Codes in Familien gruppiert. Ein erkannter und gestoppter Trojaner gab eine 0; ein infiziertes System eine 1. Überließ der Wächter dem Anwender die Entscheidung, wurde dies mit 0,5 bewertet.

IMSEC

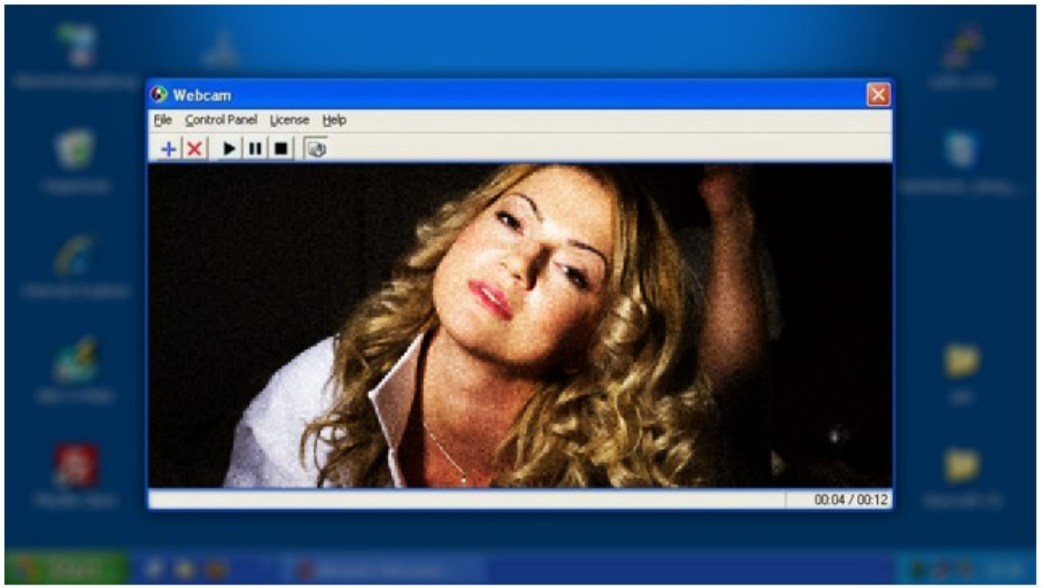
Sicherheit und Stabilität lokaler IT?

Meet the men who spy on women through their webcams

The Remote Administration Tool is the revolver of the Internet's Wild West.

by **Nate Anderson** - Mar 11 2013, 1:30am CET

HACKING INTERNET CRIME 217



Aurich Lawson / Thinkstock

"See! That shit keeps popping up on my fucking computer!" says a blond woman as she leans back on a couch, bottle-feeding a baby on her lap.

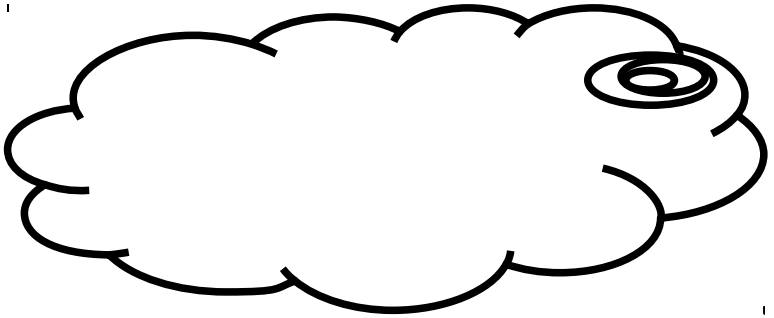
Wann wurde in Ihrer Firma zuletzt ein Backup durchgeführt?

Wo lagert das Backup extern? Ist es verschlüsselt? Wer kann darauf zugreifen oder hat den Schlüssel?

Wann wurde letztmals ein erfolgreicher Restore-Test durchgeführt?

Quelle: http://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/

Cloud-Begriffe

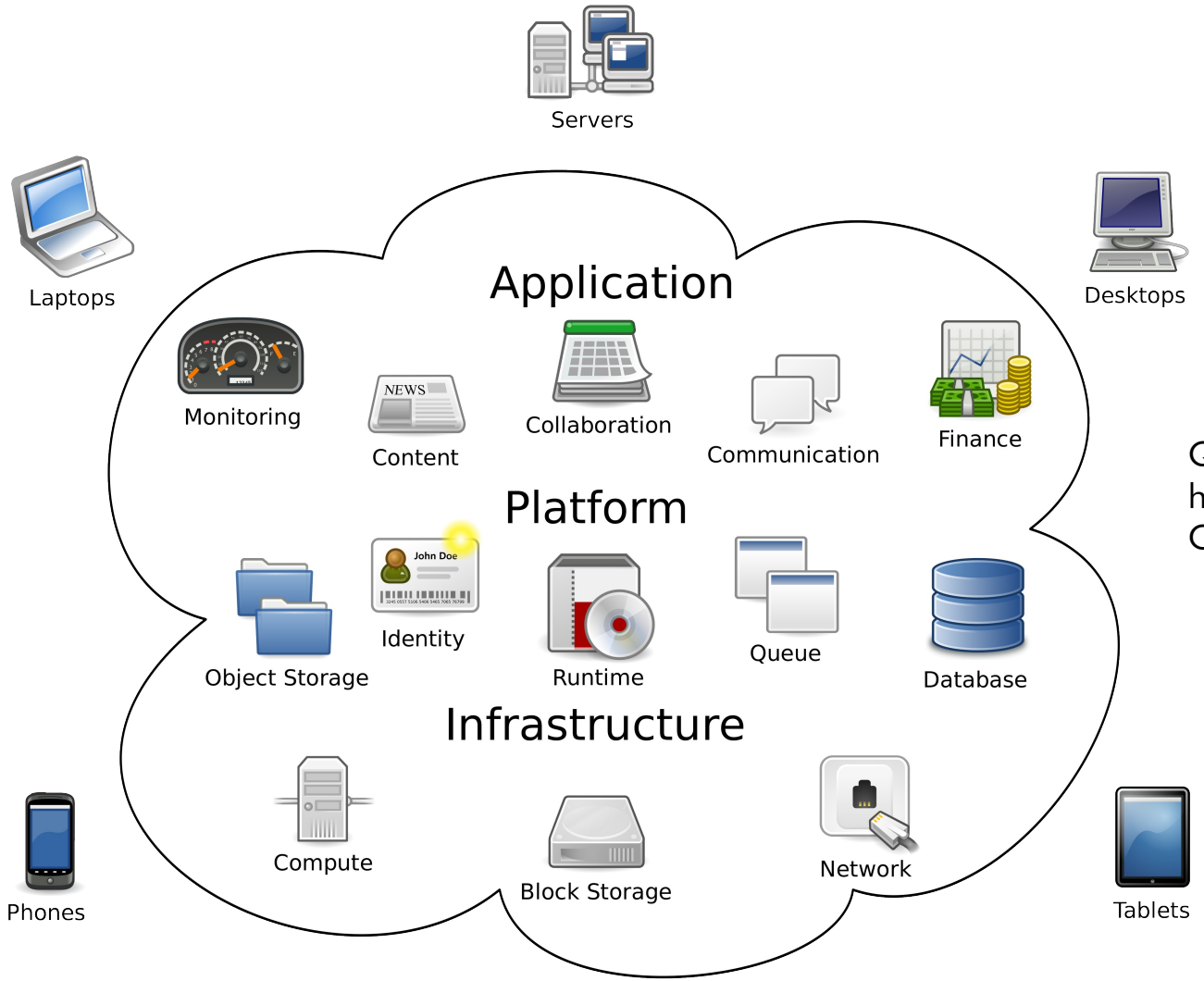


Technologie-Sicht

Kunden-Sicht

	Infrastructure as a Service (Iaas)	Platform as a Service (Paas)	Software as a Service (Saas)
Application Hosting			X
System Hosting		X	X
Virtualisierung	X	X	X
Housing	X	X	X

Cloud-Computing Komponenten



Quelle:
http://de.wikipedia.org/wiki/Cloud_Computing

Cloud-Nutzung und Trend

Cloud Computing: Jedes dritte Unternehmen nutzt die Wolke

Kategorien: News | 28.02.2013

Cloud Computing setzt sich durch

Im Jahr 2012 hat gut ein Drittel (37 Prozent) aller Unternehmen in

Quelle:https://www.it-sicherheit.de/startseite/news/cloud-computing-jedes-dritte-unternehmen-nutzt-di/

Swisscom baut «Cloud für die Schweiz»

Cloud Computing ist für Unternehmen mehr eine Chance als ein Risiko. Das wollen die Veranstalter des 4. Swiss IT Sourcing Forums mit einer Konferenz im April zögernden Unternehmen nahebringen.

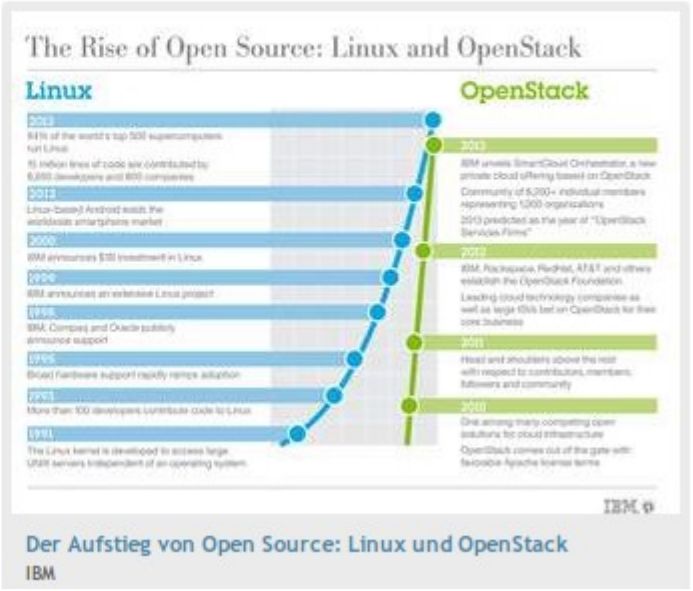
Quelle: http://www.computerworld.ch/news/it-services/artikel/swisscom-baut-cloud-fuer-die-schweiz-62596/

IBM mit neuer Open-Cloud-Strategie

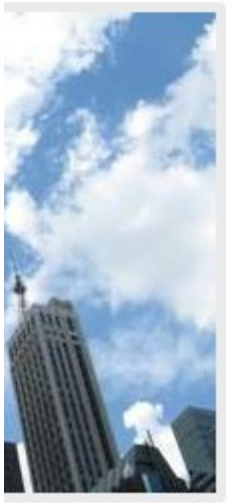
Big Blue plant alle Cloud Services und Software auf Open-Source-basierte Architekturen zu bringen

» Von Fabian Vogt , 06.03.2013 16:11.

IBM will alle seine Cloud Services und Software in Zukunft auf der Grundlage einer offenen Cloud-Architektur anbieten. Damit will das Unternehmen sicherstellen, «dass Innovationen im Bereich Cloud Computing nicht durch 'proprietäre Inseln' gehemmt werden», wie es in einer Medienmitteilung heisst. Als ersten Schritt hat IBM das Cloud-Angebot «IBM SmartCloud Orchestrator» angekündigt, das auf offenen Cloud-Standards, insbesondere OpenStack, basiert und die Verwaltung einer Unternehmenscloud einfacher und schneller machen soll. «Die Vergangenheit hat gezeigt, dass Open Source und offene Standards Endkunden enorme Vorteile bringen und ein echter Katalysator für Innovation sind», sagt Robert LeBlanc, Stellvertretender Software-Chef bei IBM. «Gewinner sind Kunden, die in Zukunft frei wählen können, welche Plattform mit welchen Services am besten für sie passt, ohne einen



Der Aufstieg von Open Source: Linux und OpenStack
IBM



Quelle: http://www.computerworld.ch/news/software/artikel/ibm-mit-neuer-open-cloud-strategie-62775/?utm_source%3DRSS%26utm_medium%3DFeedreader%26utm_campaign%3DRSSFeed

Sicherheit und Stabilität der Cloud?

Home » News » Security

Studie: US-Behörden können in der Cloud schnüffeln

Eine holländische Studie kommt zum Schluss, dass US-Behörden in Cloud-Daten schnüffeln können, auch wenn der Server ausserhalb der USA steht. Einzig der Firmensitz in den USA gebe ihnen das Recht dazu.

» Von Marcel Hauri . 07.12.2012 11:41.

Quelle: http://www.computerworld.ch/news/security/artikel/studie-us-behoerden-koennen-in-der-cloud-schnueffeln-62022/?utm_source%3DRSS%26utm_medium%3DFeedreader%26utm_campaign%3DRSSFeed

IM DOSSIER

» Dossier - Cloud Computing

be, dass nationale
d als das amerikanische Recht,
aktuelle Studie des Instituts
m.

Evernote hacked: Emails, encrypted passwords stolen

Quelle: http://j.mp/12jDMgf

Chris Davies, Mar 2nd 2013 **Discuss [17]**

+1 1k Tweet 524 Like 460

Der Dotnet-Doktor 23.02.13

Weltweiter Ausfall bei Windows Azure

Microsoft verzeichnet einen gravierenden Ausfall bei Windows Azure: D
Dienst, der tabellarische Daten und BLOBs speichert und die Grundlag
und Kunden-Anwendungen darstellt, ist seit Freitagabend 22:44 Uhr we
Zugriff über SSL/HTTPS verfügbar. Ursache laut Windows Azure Servi
abgelaufenes Zertifikat ("a worldwide outage impacting HTTPS operati
expired certificate"). Es bleibt unklar, warum Microsoft so lange braucht

Von dem Ausfall betroffen sind alle Azure-Kunden, die den Table Stora
HTTPS nutzen. In Deutschland ist das zum Beispiel die Hochwasservo
Niedersachsen. Aber auch Microsoft-Dienste wie die Cloud-basierte Qu
Foundation Service sind betroffen. Als Workaround könnten Kunden, di
ablegen, auf das unverschlüsselte HTTP umstellen und damit die Verfü
Anwendung wiederherstellen.

Quelle: http://m.heise.de/developer/artikel/Weltweiter-Ausfall-bei-Windows-Azure-1809377.html?from-classic=1

•IMSEC

InfoWorld Home / The Industry Standard / Tech's Bottom Line / When is your data not your data? When it's

MARCH 07, 2013

When is your data not your data? When it's in the cloud

With Verizon's aid, police arrest a man for storing illegal porn in the cloud, which raises questions about how much privacy cloud users can expect

By Bill Snyder | InfoWorld

Follow @BSnyderSF

Print | 7 Comments +1 More

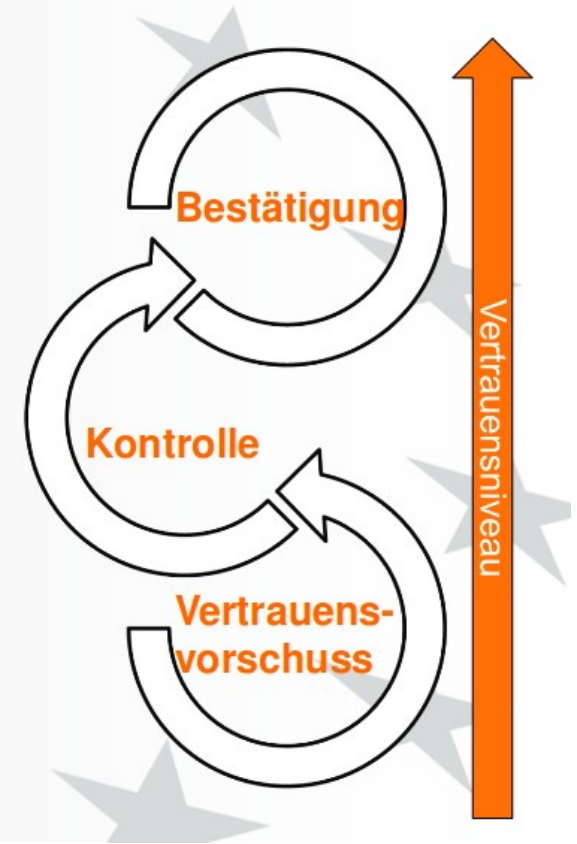
nk the data you upload to a cloud storage site is private? Not necessarily. At least a dozen of the

Quelle: http://www.infoworld.com/d/the-industry-standard/when-your-data-not-your-data-when-its-in-the-cloud-213988

they find it, they're obligated by federal law to blow

Akzeptanzfaktoren

- „Viele Kunden wissen nicht, dass Daten ausgelagert werden → keine Störgefühle der Mandanten“



aus einer Studie der Universität Aschaffenburg zum Thema Cloud Akzeptanz in Kooperation mit EuroCloud Deutschland
http://www.eurocloud.de/files/2012/07/120628_Abschlusspra%CC%88sentation_Cloud_Akzeptanz_Summary.pdf

Vertrauensbildende Massnahmen

Quelle: http://www.eurocloud.de/files/2012/07/120628_Abschlusspra%CC%88sentation_Cloud_Akzeptanz_Summary.pdf

Pro / Contra Cloudsourcing

Pro:

- Economies of Scale
  - Zentrale Standard-Lösung vs. dezentrale Individuallösung
- Cloud-Anbieter konzentrieren sich auf die Aktivität → Professionalität, Qualität, Sicherheit
- Sicherheit im lokalen Betrieb wird immer schwieriger zu gewährleisten (Komplexität, Projektstau, Fachkräftemangel, Kosten)
- Vendor-Lock-In der Software-Hersteller / Wechsel auf Standard-Lösungen mit offenen Schnittstellen
- Schweizer Angebot wächst / Cloudsourcing innerhalb CH ist möglich (Compliance)
- Transparente Kostenrechnungen
- Governance-Schnittstellen zur Kontrollierbarkeit

Contra:

- Abhängigkeit von Dritten
  - Dienstleister
  - Verbindung / Connectivity
  - Software-Anbieter
- Mögliches Vendor-Lock-In der Cloud-Betreiber
  - reduziert durch weitestgehende Akeptanz / Unterstützung von OpenStack
- Potentiell teurerer Betrieb durch konsequente Verrechnung
  - interner Betrieb oft quersubventioniert
  - Frage der internen Betriebsqualität
- Kontrollverlust
- Mangelnde Abgrenzung
- Compliance Risiken
- Zugriff von ausländischen Behörden

teilweise gemäss Leitfaden EDöB zu Cloud Computing
http://www.edoeb.admin.ch/datenschutz/00683/00877/index.html

Wie sicher ist die Cloud und wie prüft man das?

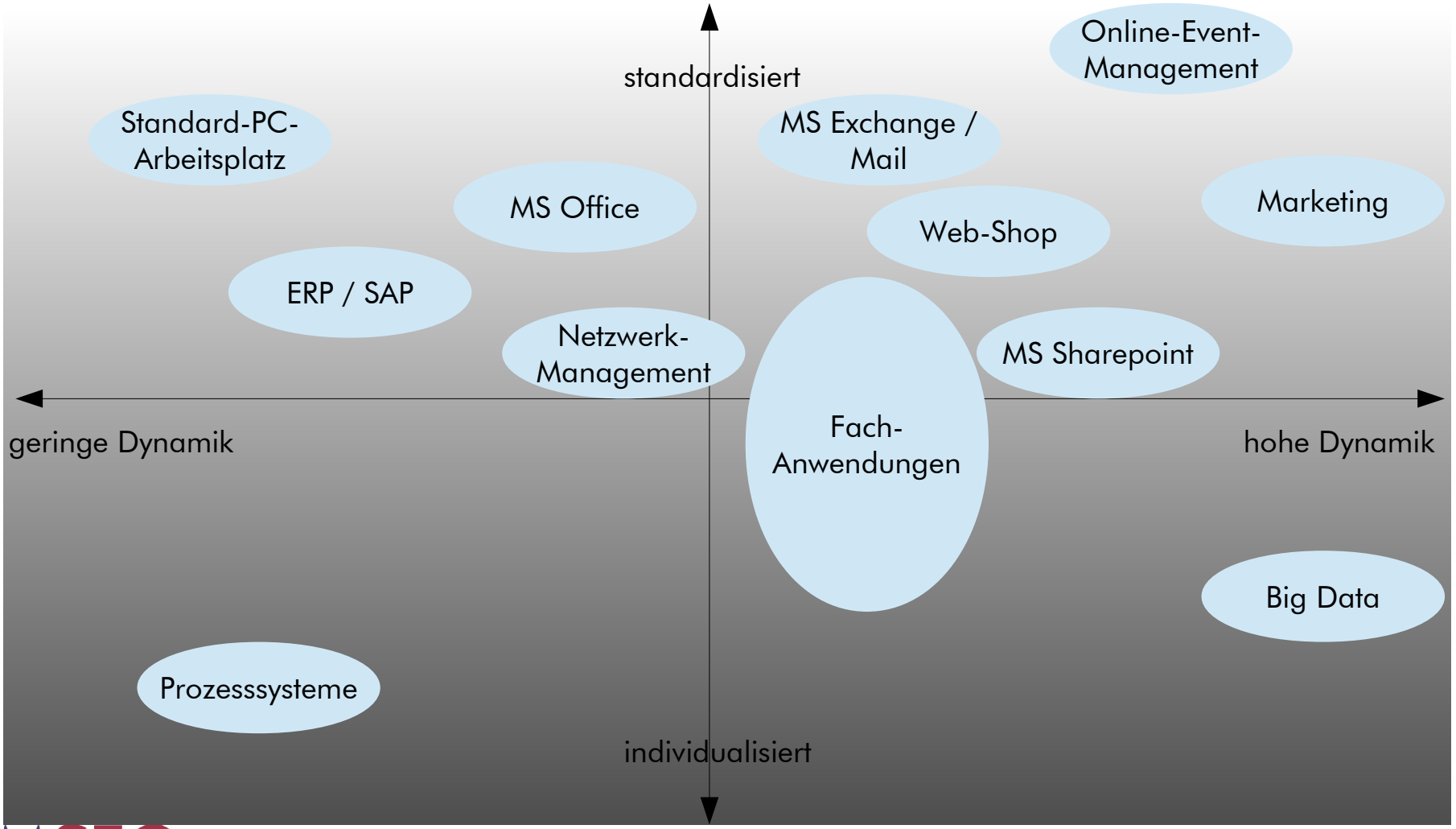
- ISO 27000 Zertifikat
- Prüfdokumente SAS70
- Eigene Revisionen bei genügender Kundengrösse

- Swisscom IT Serives: „The data centres from where we provision our services comply with the highest security requirements. Swisscom IT Services is certified to ISO 9001, ISO 14001, ISO/IEC 20000-1 and ISO/IEC 27001."
  http://www.swisscom-cloud-computing.ch/en/package/
- Green: „Die green.ch-Datacenter werden gemäss ISO 27001, dem umfassenden Standard für Informationssicherheit, betrieben und sind durch SQS und IQ NET national sowie international zertifiziert."
  https://www.greenserver.ch/files/ueberuns.php

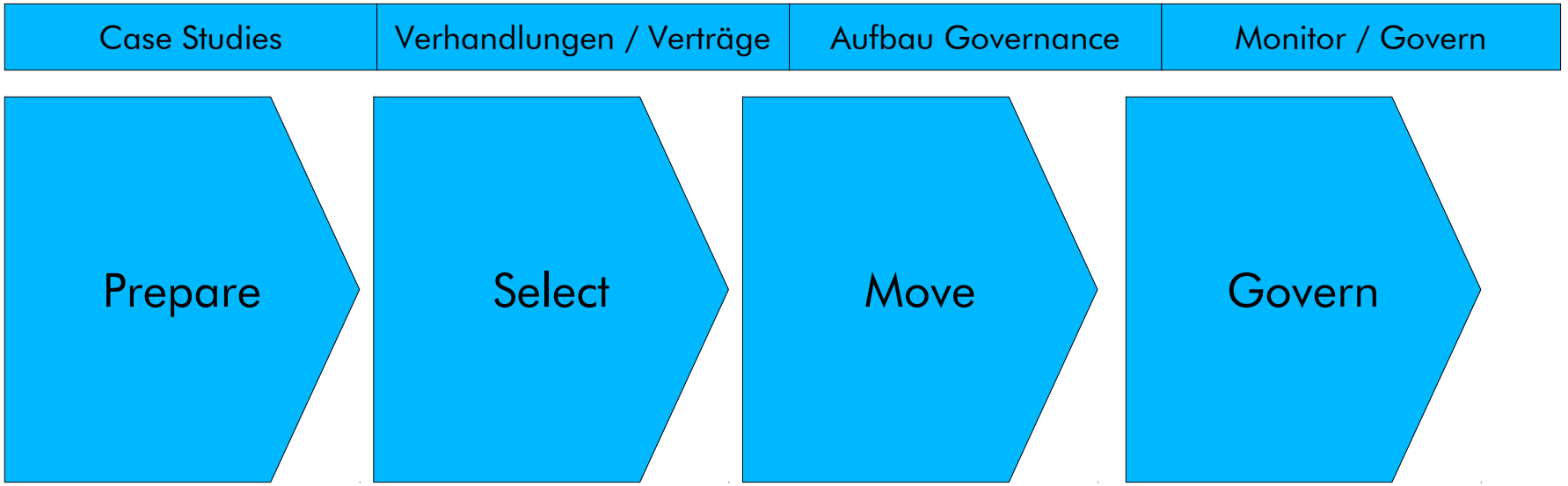
- Microsoft Azure Security Center: „These geographically dispersed data centers comply with key industry standards, such as ISO/IEC 27001:2005, for security and reliability."
  http://www.windowsazure.com/en-us/support/trust-center/security/
- IBM Cloud Security: „To further enhance our security standards and the protection offered to our customers, IBM has completed the necessary steps to earn ISO 27001 Certification."
  http://www-935.ibm.com/services/us/en/cloud-enterprise/tab-details-security.html
- Amazon Web Services (AWS) Security: „AWS hat bereits mehrere Audits gemäß SAS70 Type II erfolgreich durchlaufen. Jetzt veröffentlicht AWS einen SOC 1-Bericht (Service Organization Controls), Typ 2, gemäß den Standards SSAE 16 und ISAE 3402 sowie einen SOC 2-Bericht. Darüber hinaus hat AWS die ISO 27001-Zertifizierung erhalten und wurde für den Datensicherheitsstandard der Kreditkartenbranche (DSS/PCI) als Level 1 Service-Anbieter bestätigt."
  https://aws.amazon.com/de/security/

Cloud-Kandidaten

(sehr individuell!)



Cloud-Migrationen



Service-Katalog

Service-Angebote der Dienstleister

Prioritätenliste

Auswahl

Match

Migrationsprojekt

Migrationsprojekt

Migrationsprojekt

Umschulung Betriebspersonal

Datenmigrationen

Laufende Abrechnung

IMSEC

Verlagerungen durch Cloudnutzung

Outgesourced wird:

- Technikbetrieb
- Beschaffung
- technische Konfiguration
- Monitoring
- technisches Security Management
- Service Delivery
- Qualitätsmanagement Servicebetrieb
- Staffing + Staff IT-Management und IT-Administration
- Support / Hotline für Technik- und Applikationsbetrieb

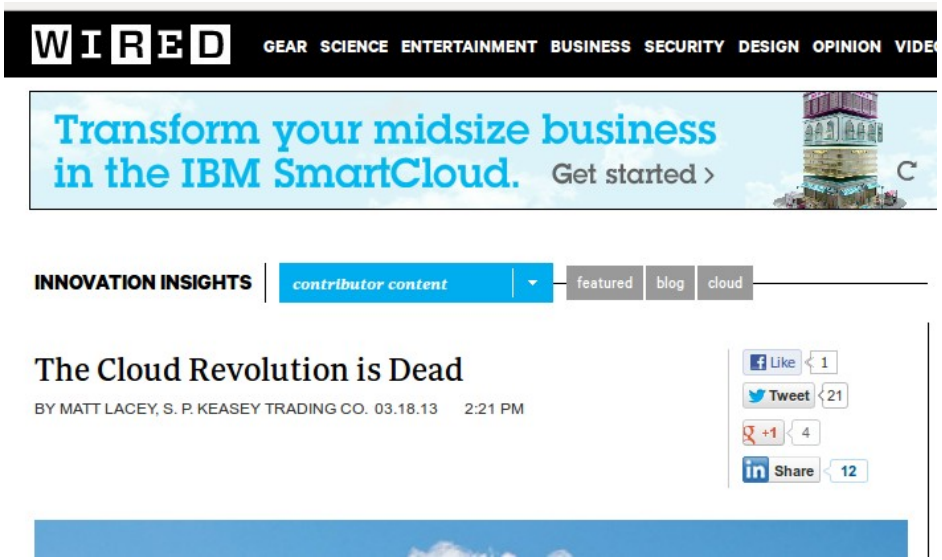
Inhouse verbleibt und wird gestärkt:

- IT-Management
- IT-Governance
- Information Management
- Security und Risk Management
- IT-Architektur & Design
- Service Management Supervision
- Qualitätsmanagement Kerngeschäft
- Financing und Budgeting
- Staffing Information Management
- Support für Business Prozesse

- jeweils in Abhängigkeit von den Cloud-Varianten
  - Private Cloud – Public Cloud – Hybrid Cloud – Community Cloud
  - Government Cloud
  - IaaS, PaaS, SaaS

Fazit 1

- Wir können Security-„Compliance“ erreichen. Compliance ist nicht unbedingt identisch mit realer Security.
- Lokaler IT-Betrieb ist aufwändig und fehleranfällig. Teilverlagerungen in die Cloud führen tendenziell zu Kosteneinsparungen und Qualitätsgewinnen.



Quelle: http://www.wired.com/insights/2013/03/the-cloud-revolution-is-dead/

Datenschutz im Cloud-Zeitalter

- Datenschutzregelungen
  - Schweiz à la Europa; Europäische Datenschutzrichtlinie
  - Amerikanisches Modell der „Privacy“
  - „Safe Harbor“- Prinzip
- Datenbestände
  - Personendaten vs. Verkehrsrahmendaten
  - Suchabfragen und Tracking
  - Selbst online hinterlassene Daten
  - eindeutige Identifikation jedes PCs
    - Heuristiken zur Bestimmung des realen Benutzers
  - Verstösse gegen Safe Harbor
  - Illegal aus der Schweiz und aus Europa exportierte Datensätze
    - Hehlerware „Konsumenten-Daten“
- Trojaner und Phishing

Jeder der compliant sein will, setzt Datenschutz so gut wie möglich um. International ist europäischer Datenschutz aber de facto nicht umzusetzen!

  - Aus amerikanischer Sicht ist Datenschutz ist ein europäischer Standort-Nachteil!
- Big Data als Ressource für gezieltere Werbung

Quelle: https://twitter.com/@bglaettli

Datenschutz im Cloud-Zeitalter

Die wesentlichen Daten lokaler Nutzer (Private und Businesses) sind bereits online erhältlich, auch zeitnah (im darknet).

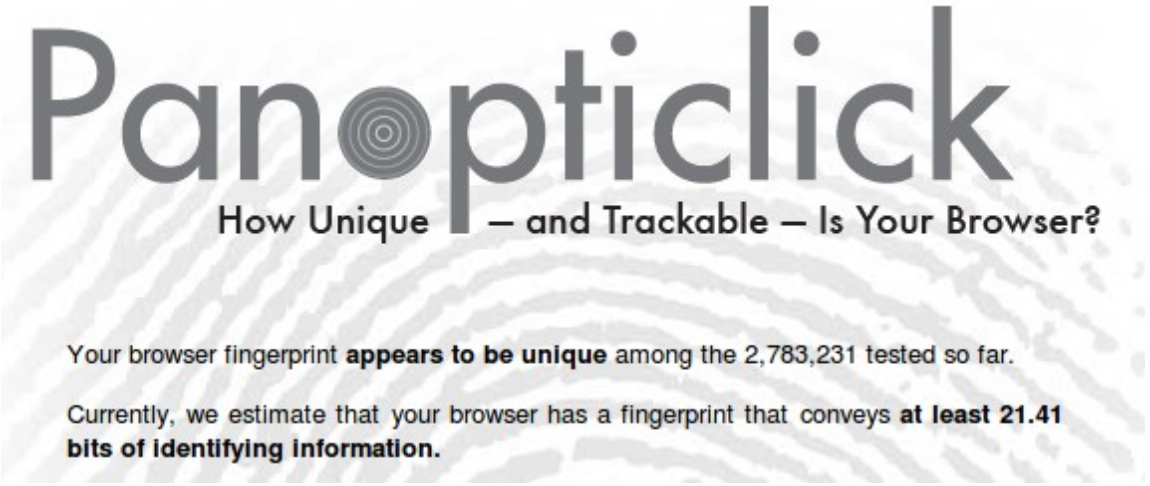
Dark Net 101

By Rogi kalomni / June 13, 2012 / 5 Comments

Freedom or Anarchy? Good or Evil? For the novice we do a quick easy to understand intro into Dark Net, the hidden Internet.

Quelle: http://askthecomputerguy.com/opinions/dark-net-101/

„Einer der dunkelsten „Tor Hidden Services" ist die „Silk Road" – auch bekannt als „Amazon für Drogen". Mit einem Mausklick gibt es dort hauptsächlich illegale Drogen aller Art zu kaufen, davon abgesehen aber auch einfach alles, was die menschliche Natur an Perversem hervorbringt. Zu den harmloseren Angeboten gehören da noch geklaute Kreditkartendaten, Hehlerwaren, gefälschte Papiere, Filesharing oder Waffen."
Quelle: http://securityblog.switch.ch/2013/03/21/deep-web-das-netz-unter-dem-netz-teil-4/



Quelle: https://panopticlick.eff.org/

- Jeder Browser ist eindeutig identifizierbar – auch diejenigen innerhalb von Firmen

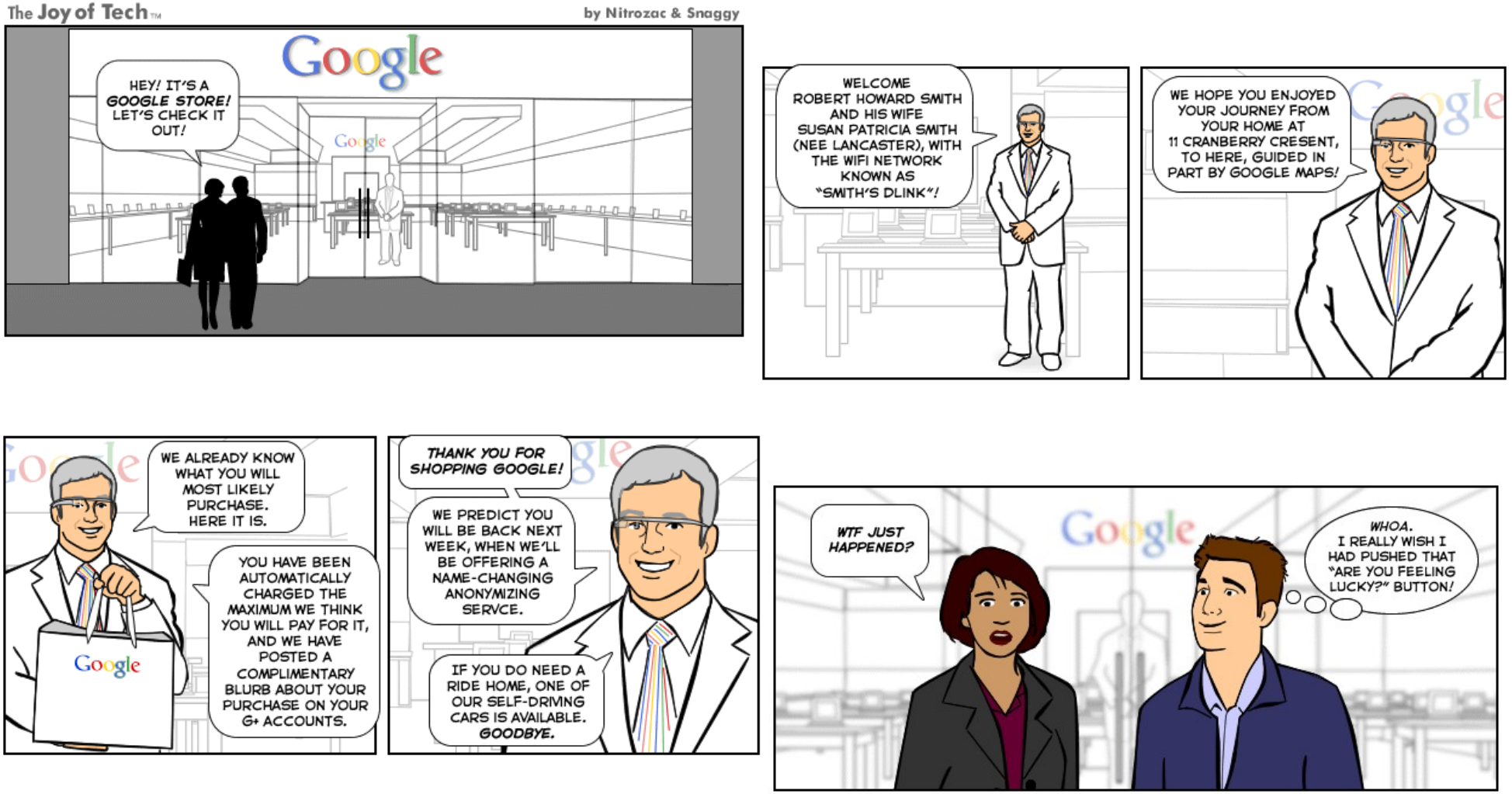
Fazit 2

- „We know where you are. We know where you've been. We can more or less know what you're thinking about."
- "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."
  (beide: Eric Schmidt, Google CEO, zitiert nach http://de.wikiquote.org/wiki/Eric_Schmidt)
- EDÖB zu Cloud:
  http://www.edoeb.admin.ch/datenschutz/00683/00877/index.html

Fazit 2:

- Schweizer oder europäischer Datenschutz ist international nicht durchzusetzen.
- Das Internet fördert Transparenz – und fordert uns zunehmend im Umgang mit Informationen über uns selbst und über unsere Mitmenschen!

The Google Store Experience



Quelle: http://allthingsd.com/20130222/the-google-store-experience-comic/