Herzlich willkommen!
Beginn 17:00 Uhr

Umgang mit (IT-)Risiken in der öffentlichen Verwaltung am Beispiel «Cloud»

Frühjahrsanlass des Datenschutzbeauftragten des Kantons Basel-Stadt
7. Mai 2019
Museum der Kulturen, Basel

Umgang mit (IT-)Risiken in der öffentlichen Verwaltung am Beispiel «Cloud»

Datenschutzbeauftragter des Kantons Basel-Stadt

Herzlich willkommen

Herzlich willkommen zum Frühjahrsanlass des Datenschutz-beauftragten des Kantons Basel-Stadt.

Unsere Welt ist voller Risiken – der Weg in die Digitalisierung ist davon nicht ausgenommen. Mit was für (IT-)Risiken sehen sich auf diesem Weg die öffentlichen Verwaltungen konfrontiert? Und wie sollen sie damit umgehen?

An einem Beispiel: Ist die «Cloud» die Lösung für die IT-Probleme der Verwaltung? Oder birgt die «Cloud» Risiken, denen sich die Verwal-tung nicht aussetzen darf?

© 2019 DSB/BS 4

Einstiegsfragen

Die Behörden sind nicht nur verantwortlich, wenn sie selber Daten bearbeiten; sie bleiben es auch, wenn sie Daten durch Dritte bearbeiten lassen (**Auftragsdatenbearbeitung**). Ob eine Auftragsdatenbearbeitung **zulässig** ist, ist nach den entsprechenden Rechtsgrundlagen (Datenschutzgesetze und spezifische Fachgesetze) zu bestimmen, es ist eine Risikoanalyse zu erstellen und die notwendigen Schutzvorkehren sind zu treffen.

→ Leitfaden «Auftragsdatenbearbeitung» des DSB/BS: https://www.dsb.bs.ch/handreichungen/leitfaden-auftragsdatenbearbeitung.html

Ist eine Auftragsdatenbearbeitung zulässig und möglich und sollen Cloud-Technologien verwendet werden, sind **zusätzlich** die **Cloud-spezifischen Risiken** zu beurteilen und die zur Minimierung dieser Risiken notwendigen Massnahmen vorzukehren.

Risiko – Risikoanalyse – risikominimierende Massnahmen ...

© 2019 DSB/BS 5

«Umgang mit (IT-)Risiken in der öffentlichen Verwaltung am Beispiel ‹Cloud›»

Hannes Lubich
Prof. Dr.

Professor für Informatik an der Fachhochschule Nordwestschweiz (FHNW), früher Forscher und Dozent an der ETH Zürich, Chief Information Security Officer bei einer international tätigen Privatbank und Berater in der IT-Industrie [→]

© 2019 DSB/BS 6

Umgang mit (IT)-Risiken in der öffentlichen Verwaltung am Beispiel «Cloud»

Prof. Dr. Hannes P. Lubich

Fachhochschule Nordwestschweiz

7. Mai 2019

8

Was ist ein «Risiko»?

- Ein Risiko ist die *kalkulierte Prognose* eines möglichen *Schadens bzw. Verlustes im negativen Fall (Gefahr)* oder eines möglichen *Nutzens bzw. Gewinns im positiven Fall (Chance)*. Was als Schaden oder Nutzen aufgefasst wird, hängt von **Wertvorstellungen** ab.
- «Management» des Risikos durch eine Mischung aus Vermeidung, Übertragung, Begrenzung, Akzeptanz und/oder Ignoranz
- Abhängig von Risikotyp und Risikokultur
- Beurteilung nach Schadenhöhe und Eintretenswahrscheinlichkeit, sofern genug Daten vorhanden

9

Quellen von Cyber-Risiken

- Extern:
  - Hacker / Cracker
  - Informationssammler
  - Kriminelle Personen oder Organisationen
  - Aufklärungsdienste
  - Partner / Kunden
  - Konkurrenten
  - Fanatiker / Terroristen
  - Militär / Aufklärungsdienste
- Intern:
  - Unzufriedene Mitarbeiter
  - Lieferanten / Wartung
  - System-Spezialisten
  - Kriminelle Personen
  - Unvorsichtige Mitarbeiter

10

Beispiele für aktuelle Cyber-Angriffsvektoren

Ungezielte Angriffe (Typ 1)

- Viren / Würmer, «intelligente» Spam-Nachrichten, Spyware, Phishing, Trojaner, verseuchte Web-Seiten («drive-by infection»), … (Sammelbegriff: Malware)
- Basiert oft auf «social engineering»-Methoden
- Kommerzielle Mehrfach-nutzung mit stark verteilter Wertschöpfungskette

Gezielte Angriffe (Typ 2)

- «Denial of Service», Sabotage, Erpressung, Aufklärung (kommerziell, militärisch), Identitätsdiebstahl und –missbrauch
- Gezielter Zugriff (Diebstahl oder online) auf Geräte durch Personen im «Nahbereich»
- Gezielte Manipulation von Heimarbeitsplätzen und Heim-Infrastruktur (gilt auch für ver-meintlich «harmlose» Benutzer)

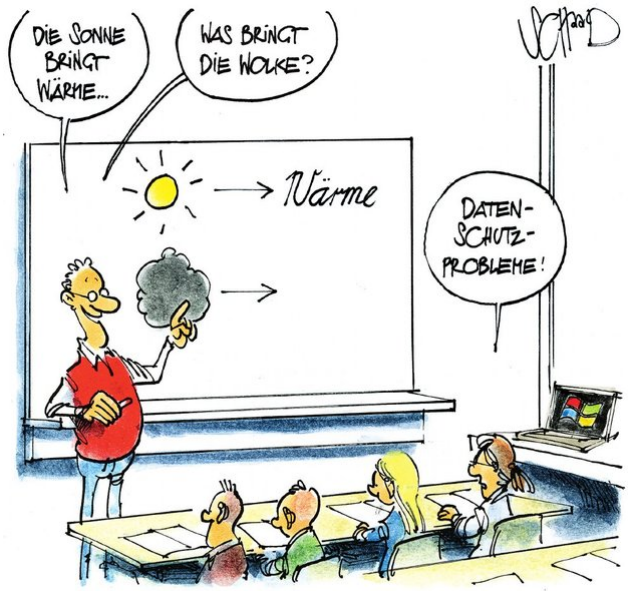
11

Auswirkung auf die Verwaltung

- Teilweise systemkritische Diensterbringung
- Hohe Verfügbarkeits- und Qualitätsansprüche aller Anspruchsgruppen
- Attraktives Angriffsziel → hoher Schutzbedarf für die eigenen und anvertrauten Daten, Systeme und Schnittstellen
- Hohe Sichtbarkeit und öffentliche Empörung im Schadenfall
- Hoher Bedarf an eigenem und extern bezogenem IT-Know-how

12

© 2019 Hannes Lubich (FHNW)



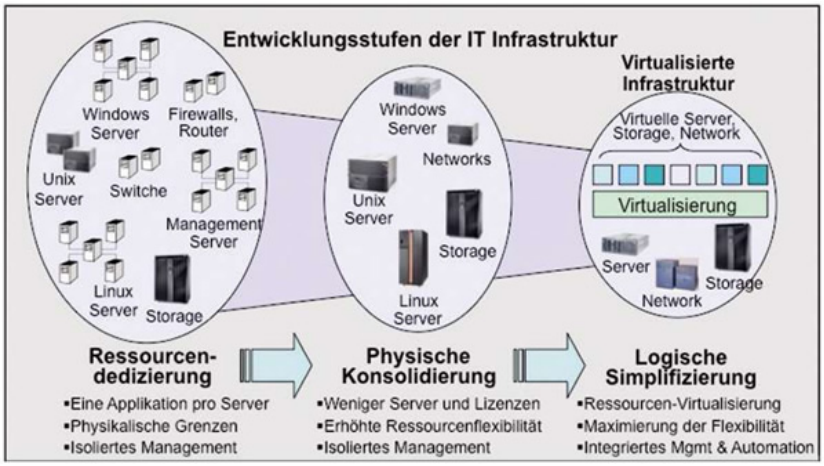
13

Die Cloud in der Verwaltung

- Wachsender Bedarf für das standardisierte Angebot digitalisierter Dienste für die Bevölkerung (eVoting, eSchalter, eUmzug, usw.)
- Plattform für die digitale Transformation interner Abläufe, Prozesse und Hilfsmittel
- Standards und «good practices» (z.B. «eCH-0199: Cloud Referenzarchitektur») gibt es
- Für die Verwaltung geeignete Dienstanbieter sind ebenfalls vorhanden (Abraxas, Bedag, …)

14

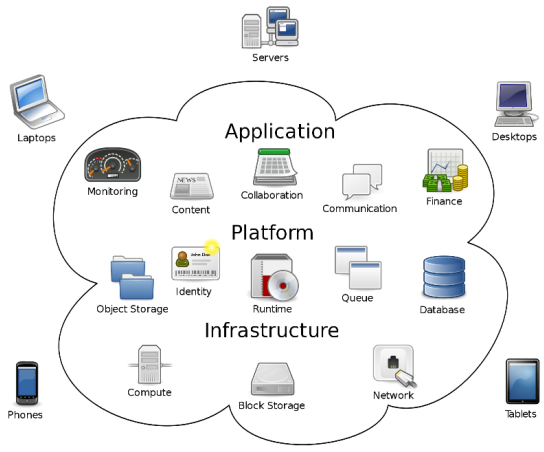
Der Weg zur «Cloud»



http://i.cmpnet.com/informationweek.de/iwk_img/2009/03/iwk_03_10_01.jpg

15

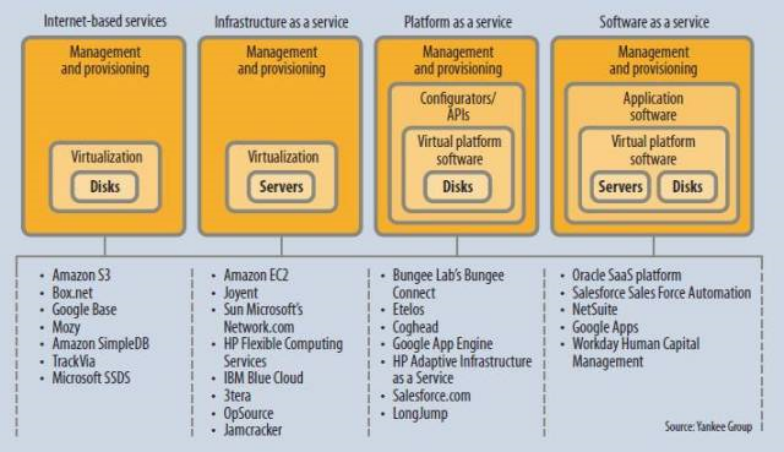
Was meinen wir mit «Cloud»?



http://upload.wikimedia.org/wikipedia/commons/thumb/b/b5/Cloud_computing.svg/2000px-Cloud_computing.svg.png

16

Welche Angebotstypen gibt es?



http://waimingmok.files.wordpress.com/2009/01/yankeegroupcloudservices.jpg

17

Cloud Nutzungsmuster

Private Nutzung:	KMU-Nutzung:	Grosskunden- und Behörden-Nutzung:
E-Mail Services Filesharing Services Musik, Videos etc. Tauschbörsen Dokumentablage Backup, Archivierung	E-Mail Services Backup, Archivierung Dokumentablage	Private Cloud Services Such- / Filter Services (Spam / Content Filter, Data Mining, etc.) Applikationsdienste (CRM, Buchhaltung, Bestellwesen, Shops, eGov)
→ grosse Benutzergruppe, eher kleine Datenmengen pro Person → standardisierte «flat rate» Angebote	→ kleine Benutzergruppe, Angebote noch eher wenig bekannt /genutzt → künftig ggf. «private cloud» pro Branche	→ grosses Volumen, kleine Nutzergruppe → Kooperationsmodell mit den Anbietern

18

Chancen der Cloud-Nutzung

Dienstnehmer

- «economy of scale»
- Kostenflexibilisierung
- Transfer von Risiken
- Komplexitätsreduktion
- Konzentration auf die Kernkompetenzen
- Neue Anwendungen / DIgitalisierung

Dienstanbieter

- Skaleneffekte bei Beschaffung, Betrieb und Wiederverwendung
- Reduktion der Komplexität durch Vereinheitlichung
- Vertieftes Wissen über die Kunden und deren noch abzudeckende Bedürfnisse

19

Risiken der Cloud-Nutzung

Dienstnehmer:

- Abhängigkeitsketten
- Intransparenz
- Transitionskosten
- Rechtliche Unklarheit
- «Monokulturen»
- Sicherheitsbedenken

Dienstanbieter:

- Hohe Verantwortung für die Summe der Anforderungen aller Kunden
- Ausreichender Grundschutz für unterschiedliche Kundensegmente
- Standardisierte Angebote führen zu reduzierter Kundenbindung

20

«Typische» Bedenken

- «Wo sind meine Daten und wer hat Zugriff?»
- «Gehen meine Daten ins Ausland?»
- «Wie ist meine Privatsphäre geschützt?»
- «Wie kann ich zusätzlichen Schutz erhalten?»
- «Woher weiss ich, ob die Cloud sicher läuft?»
- «Was, wenn die Cloud mal nicht läuft?»
- «Die Cloud ist ein Primärziel für Angreifer!»

21

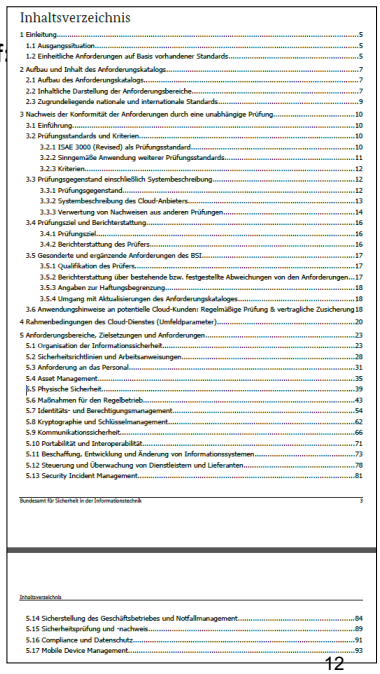
Handlungsbedarf

- Nachvollziehbare Bedürfnisabklärung und Entscheidungsfindung
- Nutzung etablierter Standards und «good practices»
- Realistischer Migrationsplan inklusive Chancen-/Risiken-Abschätzung und klaren Meilensteinen
- Betrieb, Überwachung, Wartung, Weiterentwicklung und Partner unter eigener «Governance»
- Realistischer und eingeübter «Plan B» für die Aufrechterhaltung des notwendigen Betriebs und hoheitlicher Funktionen bei längeren Ausfällen und Unterbrüchen

22

© 2019 Hannes Lubich (FHNW)

Für Firmen ohne formellen Zertifizierungsbedarf:
BSI Anforderungskatalog Cloud Computing (C5)
– Kriterien zur Beurteilung der Informations-sicherheit von Cloud-Diensten


Inhaltsverzeichnis

1 Einleitung ... 5
1.1 Ausgangssituation ... 5
1.2 Einheitliche Anforderungen auf Basis vorhandener Standards ... 5
2 Aufbau und Inhalt des Anforderungskatalogs ... 7
2.1 Aufbau des Anforderungskatalogs ... 7
2.2 Inhaltliche Darstellung der Anforderungsbereiche ... 7
2.3 Zugrundeliegende nationale und internationale Standards ... 9
3 Nachweis der Konformität der Anforderungen durch eine unabhängige Prüfung ... 10
3.1 Einführung ... 10
3.2 Prüfungsstandards und Kriterien ... 10
3.2.1 ISAE 3000 (Revised) als Prüfungsstandard ... 10
3.2.2 Sinngemäße Anwendung weiterer Prüfungsstandards ... 11
3.2.3 Kriterien ... 12
3.3 Prüfungsgegenstand einschließlich Systembeschreibung ... 12
3.3.1 Prüfungsgegenstand ... 12
3.3.2 Systembeschreibung des Cloud-Anbieters ... 13
3.3.3 Verwertung von Nachweisen aus anderen Prüfungen ... 14
3.4 Prüfungsziel und Berichterstattung ... 16
3.4.1 Prüfungsziel ... 16
3.4.2 Berichterstattung des Prüfers ... 16
3.5 Gesonderte und ergänzende Anforderungen des BSI ... 17
3.5.1 Qualifikation des Prüfers ... 17
3.5.2 Berichterstattung über bestehende bzw. festgestellte Abweichungen von den Anforderungen ... 17
3.5.3 Angaben zur Haftungsbegrenzung ... 18
3.5.4 Umgang mit Aktualisierungen des Anforderungskataloges ... 18
3.6 Anwendungshinweise an potentielle Cloud-Kunden: Regelmäßige Prüfung & vertragliche Zusicherung 18
4 Rahmenbedingungen des Cloud-Dienstes (Umfeldparameter) ... 20
5 Anforderungsbereiche, Zielsetzungen und Anforderungen ... 23
5.1 Organisation der Informationssicherheit ... 23
5.2 Sicherheitsrichtlinien und Arbeitsanweisungen ... 28
5.3 Anforderung an das Personal ... 31
5.4 Asset Management ... 35
5.5 Physische Sicherheit ... 39
5.6 Maßnahmen für den Regelbetrieb ... 43
5.7 Identitäts- und Berechtigungsmanagement ... 54
5.8 Kryptographie und Schlüsselmanagement ... 62
5.9 Kommunikationssicherheit ... 66
5.10 Portabilität und Interoperabilität ... 71
5.11 Beschaffung, Entwicklung und Änderung von Informationssystemen ... 73
5.12 Steuerung und Überwachung von Dienstleistern und Lieferanten ... 78
5.13 Security Incident Management ... 81
Bundesamt für Sicherheit in der Informationstechnik 3
Inhaltsverzeichnis
5.14 Sicherstellung des Geschäftsbetriebes und Notfallmanagement ... 84
5.15 Sicherheitsprüfung und -nachweis ... 89
5.16 Compliance und Datenschutz ... 91
5.17 Mobile Device Management ... 93

12

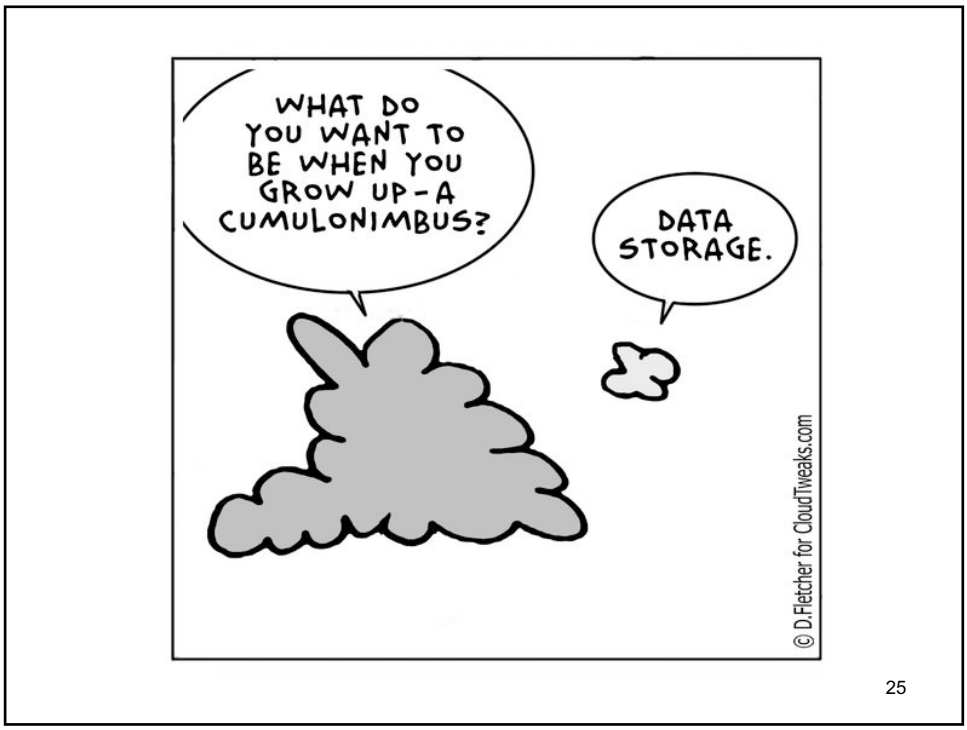
Zukünftige Entwicklungen

- Virtualisierung von einzelnen Applikationen und Bereitstellung aus der Cloud (Citrix usw.)
- Noch kleinere Bausteine (Docker / Container),
- Verteiltere Funktionen in der Ende-zu-Ende-Wertschöpfungskette mittels Intermediären

Aber auch:

- Erhebliche Anspruchshaltung der Anwender
- Öffentlichkeitswirksame Unterbrüche/Angriffe

24


WHAT DO YOU WANT TO BE WHEN YOU GROW UP - A CUMULONIMBUS?
DATA STORAGE.
© D.Fletcher for CloudTweaks.com
25

privatim-Merkblatt «Cloud-spezifische Risiken und Massnahmen»

privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Der Einsatz von Cloud-Lösungen ist im konkreten Einzelfall zu beurteilen. Es muss eine **umfassende Risikoanalyse** durchgeführt werden, die neben der Art der Datenbearbeitung insbesondere auch die Fragen des *anwendbaren Rechts* und des *Gerichtsstandes*, des *Orts der Datenbearbeitung* (Serverstandort) und des *Geheimnis-schutzes (Verschlüsselung, Schlüsselmanagement)* in den Fokus stellt.

Gesamtbeurteilung: Ist die Verwendung von Cloud-Technologien bei einer bestimmten behördlichen Datenbearbeitung *vertretbar* oder ist aufgrund der nicht zu beseitigenden oder nicht reduzierbaren Risiken darauf zu *verzichten*?

Der Entscheid ist *transparent zu dokumentieren*, so dass das verantwortliche öffentliche Organ (nicht der IT-Dienstleister) die *Risiken kennt* und das verbleibende **Restrisiko bewusst übernehmen und verantworten** kann.

→ privatim-Merkblatt: https://www.dsb.bs.ch/handreichungen/privatim-merkblatt-cloud.html

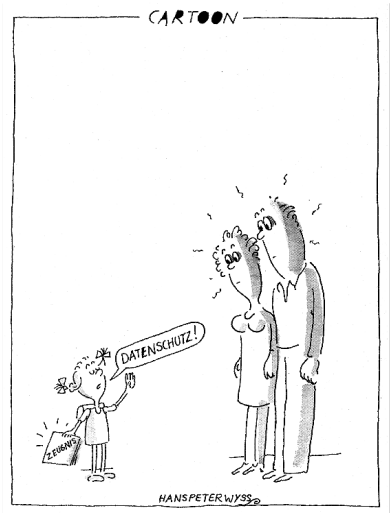
© 2019 DSB/BS 27

Besten Dank für Ihr Interesse und Ihre aktive Teilnahme!

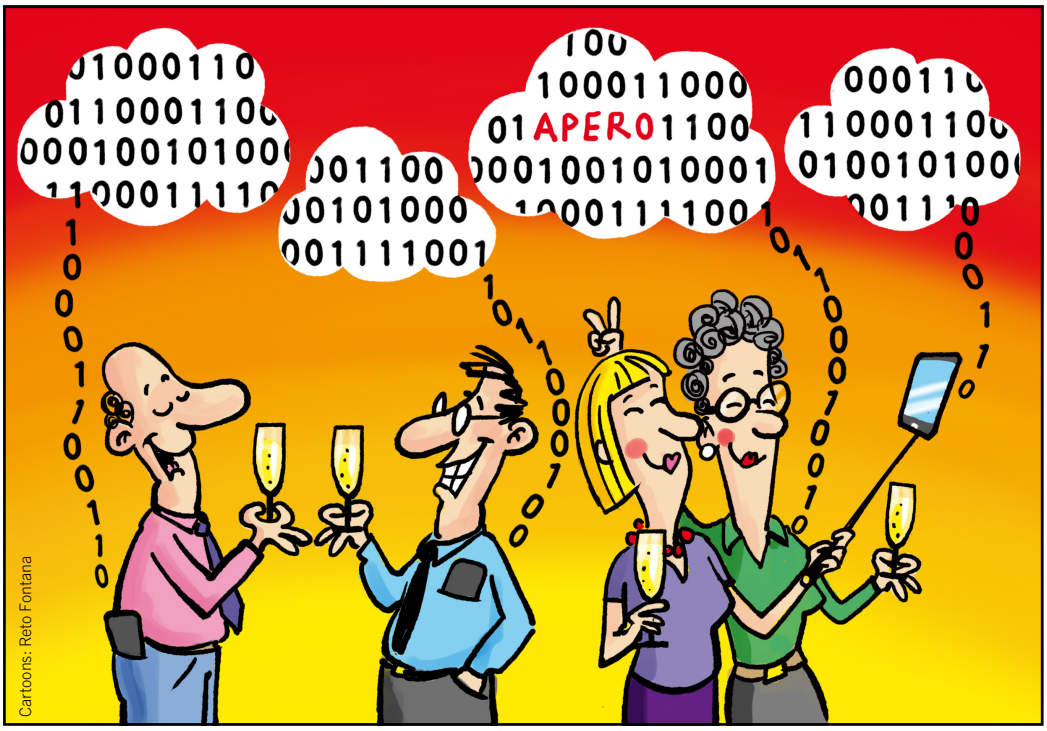
Die Folien werden diese Woche zum Download aufgeschaltet: <http://www.dsb.bs.ch/ueber-uns/Veranstaltungen.html>

Wir sind gerne für Sie da – auch später bei konkreten Fragen.

Datenschutzbeauftragter
des Kantons Basel-Stadt
Henric Petri-Strasse 15
4010 Basel
T 061 201 16 40
datenschutz@dsb.bs.ch
<http://www.dsb.bs.ch>



© 2019 DSB/BS 28


APERO
Cartoons: Reto Fontana