65. Österreichischer Städtetag

10. – 12. Juni 2015 in Wien
„Smart Cities: Menschen machen Städte“

Arbeitskreis V

Städte und Gemeinden im digitalen Zeitalter

Wissen.Offenheit.Bildung.Sicherheit

Österreichischer Städtebund

Städte und Gemeinden im digitalen Zeitalter

Wissen.Offenheit.Bildung.Sicherheit

Moderation:

Mag. Markus Pohanka
Austro Control

Vorsitz:

Mag.ª Ulrike Huemer
Leiterin Gruppe Prozessmanagment und IKT-Strategie der Stadt Wien _____ Seite 5

Vortragende:

Ing. Roland Ledinger
Leitung des Bereiches IKT-Strategie des Bundes,
Geschäftsführer der Plattform Digitales Österreich _____ Seite 15

Mag. Bernhard Krabina
KDZ – Zentrum für Verwaltungsforschung _____ Seite 25

Joanna Schmölz, MA
stellvertretende Direktorin,
Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) _____ Seite 41

Mag.ª Meral Akin-Hecke
Digital Champion Austria _____ Seite 53

Joe Pichlmayr, Geschäftsführer
Sebastian Bachmann
IKARUS Security Software GmbH _____ Seite 57

Städte und Gemeinden brauchen eine Digitale Agenda

Mag.a Ulrike Huemer

CIO von Wien

Städte und Gemeinden brauchen eine Digitale Agenda

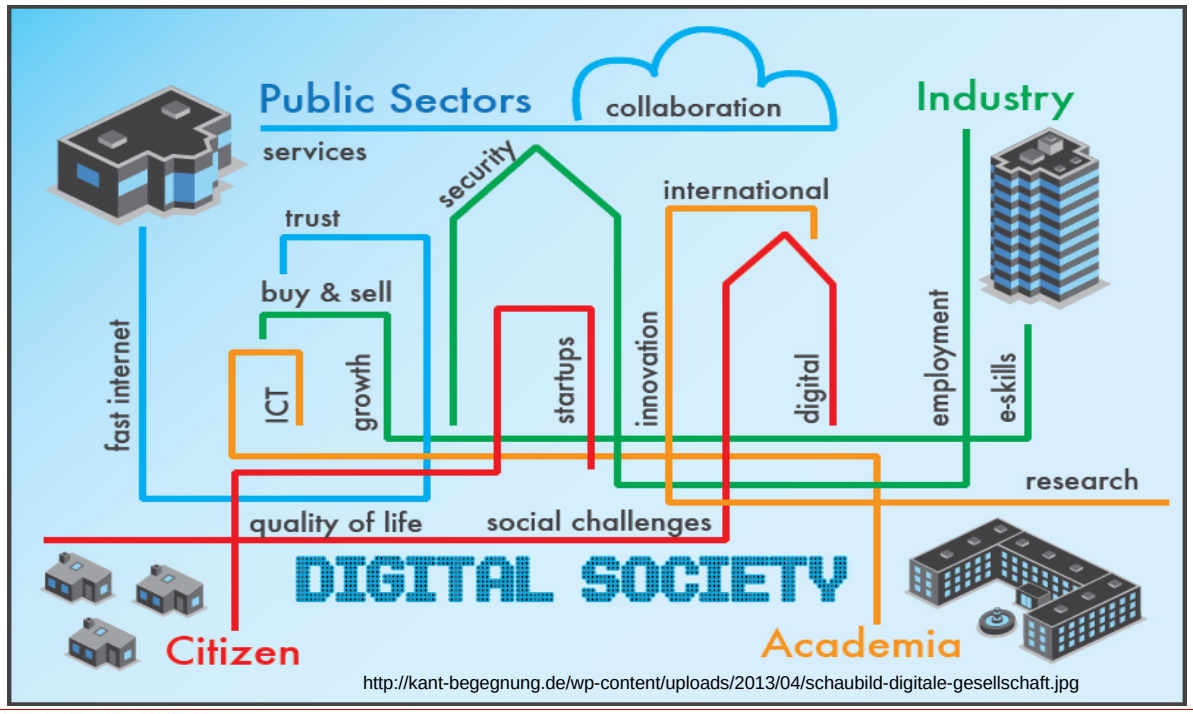
65. Österreichischer Städtetag

11. Juni 2015 in Wien

Ulrike Huemer, CIO von Wien

Magistratsdirektion der Stadt Wien
Geschäftsbereich Organisation und Sicherheit
Prozessmanagement und IKT-Strategie

Herausforderung Digitale Revolution



http://kant-begegnung.de/wp-content/uploads/2013/04/schaubild-digitale-gesellschaft.jpg

Megatrends – Digitale Revolution

- Digital First
- Cloudtechnologien
- Mobility
- Disruption
- Big Data „Krankheiten berechnen aus Gesundheitsdaten“
- BürgerInnenportale (City as a Service)
- Open Government (Human Centric Ansatz)
- Industrie 4.0
- Machine to Machine Communication
- Internet of Everthing

#DigitalesWien

Digitale Agenda Wien

Der Prozess….

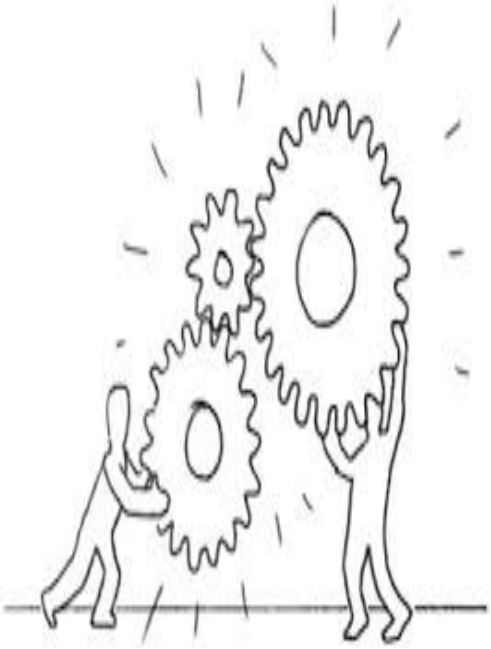
Ideengenerierung (online) :
17.9 - 19.10

Strategietexterstellung
(offline): 10/2014 – 4/2015

Strategiediskussion (online):
4/2015

Revision des Strategietexts
(offline): 5/2015

Veröffentlichung 16.6.2015



DigitalesWien

wien.at

1. Online Phase….

- 478 Registrierungen,
- 172 Ideen,
- 296 Kommentare,
- 2451 Likes/Dislikes

DigitalesWien

wien.at

Offline Phase….

- 5 Arbeitsgruppen
- Open Government: Einbindung der IdeengeberInnen
- Konsolidierung der Ergebnisse der Arbeitsgruppen
- Aus 500 Seiten werden 30 Seiten

Digitalen Agenda - Struktur

- Einführung in die Digitale Agenda
- Vertrauen, Sicherheit und Schutz
- Serviceangebote und Aktivierung der BürgerInnen
- Bildung und Forschung
- IT Standort Wien
- Digitale Infrastruktur
- IT Governance

Die Prinzipien der Digitalen Agenda

Vertrauen und Sicherheit

Vertrauen der Bürgerinnen und Bürger in die Informationssicherheit ist entscheidend für das gesamte Handeln der Stadt Wien und ist die Basis der modernen Stadt. Die Sicherheit von Infrastruktur, Daten und Kommunikation hat oberste Priorität und ist immer zu berücksichtigen.

Transparenz, Offenheit und Beteiligung

Die Stadt Wien entwickelt sich noch stärker als bisher von einem geschlossenen Bürokratie-Modell zu einer offenen und partizipativen Stadt. Die aktive Einbindung der Bürgerinnen und Bürger mit intelligenten IT-Plattformen wird zum Standard in der Stadt Wien und lässt kreative und innovative Lösungen partnerschaftlich entstehen. Transparenz und Offenheit leiten das Verwaltungsdenken und Handeln.

Inklusion und soziale Nachhaltigkeit

Digitale Veränderungsprozesse sind eine große Herausforderung für die Politik, die Verwaltung, die Wirtschaft und für die gesamte Bevölkerung. Die Stadt Wien stellt sicher, dass dabei niemanden zurückgelassen wird und dass alle Services für alle Menschen der Stadt zugänglich bleiben – unabhängig von Bildung und Einkommen. Das Inklusionsprinzip ist daher ein zentrales Anliegen der Smart City Wien.

Gendergerechtigkeit

Frauen und Mädchen sind sowohl in digitalen Berufen wie auch generell in den digitalisierten Lebenswelten unterrepräsentiert. Die Gendergerechtigkeit in diesem wesentlichen Gesellschafts- und Wirtschaftsbereich herzustellen ist eine wesentliche Handlungsanleitung für die Stadt Wien.

BürgerInnenorientierung

Verwaltung ist eine Dienstleistung für die BürgerInnen und Bürger. Die Stadt Wien orientiert sich weitgehend an den Blickwinkeln und Lebenslagen der Bürgerinnen und Bürger. Für deren Anliegen ist sie sieben Tage die Woche 24 Stunden am Tag online verfügbar

Stärkung des Wirtschaftsstandorts

Die IKT-Branche hat sich in den letzten Jahren zu einem der wichtigsten Wirtschaftsfaktoren für die Stadt Wien entwickelt. Diesen gemeinsam weiter auszubauen, ist eine wichtige Aufgabe aller Beteiligten.

Konsolidierung

Die Stadtverwaltung Wien und ihre Unternehmen werden in einer bürgerInnenorientierten Sicht gesamthaft wahrgenommen. Eine koordinierte und konsolidierte Vorgangsweise ist Grundvoraussetzung für eine effiziente und effektive Weiterentwicklung der Informations- und Kommunikationstechnologien der Stadt Wien.

Innovation

In Zeiten von extrem dynamischen Veränderungen, die von neuen Ideen geprägt sind, haben Informations- und Kommunikationstechnologien eine noch stärkere strategische Bedeutung und müssen immer mitgedacht werden. Die Stadt Wien stellt sich dieser Herausforderung, indem sie nicht nur einen zusätzlichen Rahmen für innovative Projekte schafft, sondern auch Innovationskultur im eigenen Haus aktiv unterstützt. Gemeinsam mit der FTI-Strategie „Innovatives Wien 2020" will die Digitale Agenda hierzu einen Beitrag leisten

Flexibilität und Lernen

Um die Herausforderungen der digitalen Transformation zu meistern, bedarf es einer lernenden Organisation, die ein hohes Maß an Beweglichkeit (Agilität), Flexibilität und Veränderungsbereitschaft vorweist. Das bedeutet auch den Einsatz neuer Management-Methoden, die die Innovationskultur in der Stadt Wien unterstützen, die Veränderung von Prozessen und den Einsatz innovativer Technologien des digitalen Zeitalters.

DigitalesWien

Digitalen Agenda - Struktur

- Leuchtturmprojekte (z.B. BürgerInnenportal)
- Ideen referenziert
- Annex

DigitalesWien

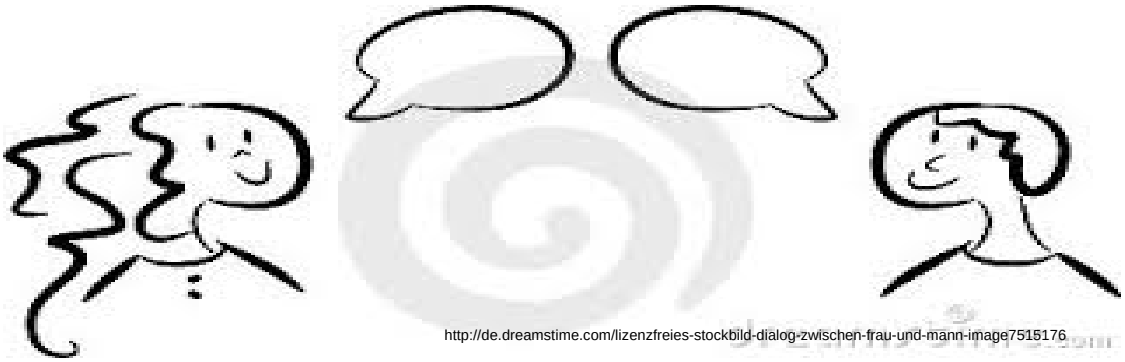
Online Phase II

- Text wird auf www.digitaleagenda.wien zur Diskussion gestellt
  - 622 Registrierungen
  - 313 Kommentare
  - 2999 Likes/Dislikes

- Veröffentlichung 16. Juni 2015

DigitalesWien

Der Dialog…



http://de.dreamstime.com/lizenzfreies-stockbild-dialog-zwischen-frau-und-mann-image7515176

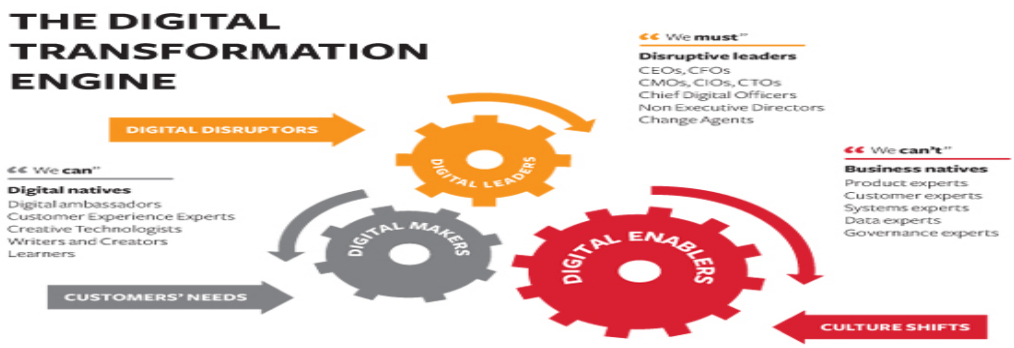
- Plattform www.digitaleagenda.wien bleibt aufrecht
- Einmal jährlich wird der Partizipationsprozess mit den BürgerInnen neu angestoßen werden
- Arbeitsgruppen entwickeln die Ideen laufend weiter
- Umsetzung der Maßnahmen wird regelmäßig reflektiert

DigitalesWien

Die Erfahrung …

- Wir haben viel über uns gelernt…
- Wir haben die Ressource Partizipation schätzen gelernt…
- Wir verändern uns dadurch….

Die Nächsten Schritte



- Von der Digitalen Agenda zur IT-Strategie
- Applikationsstrategie, Infrastrukturstrategie, Sourcing-Strategie, Innovationsstrategie, Sicherheitsstrategie
- IT Projekte sind Businessprojekte!
- Disruption und Agilität

Wir bringen IT in die Organisations- und Personalentwicklung!

Herzlichen Dank
für Ihre
Aufmerksamkeit!

Diese Präsentation der Stadt Wien steht unter einer Creative Commons Namensnennung 3.0 Österreich Lizenz.
Die Namensnennung der Stadt Wien als Rechteinhaberin hat in folgender Weise zu erfolgen:
"Datenquelle: Stadt Wien"

digitale Gesellschaft, digitale Wirtschaft, digitaler Staat, digitale Zukunft?

Ing. Roland Ledinger

Bundeskanzleramt Österreich - Bereich IKT-Strategie

digitale Gesellschaft, digitale Wirtschaft, digitaler Staat, digitale Zukunft?

Herausforderungen an Politik und Verwaltung

Roland Ledinger

Bundeskanzleramt - Österreich
Bereich IKT-Strategie

Ballhausplatz 2, 1014 Wien

ikt@bka.gv.at
www.bka.gv.at

DIGITALES ÖSTERREICH

die großen Ziele

ein leichteres Leben der Menschen, mehr Möglichkeiten und Chancen

Rahmenbedingungen für eine kreative IKT-Branche mitten in Europa

die modernste Verwaltung Europas, das leistungsfähigste e-Government

die digitale Welt verändert unsere Leben

Bildung
IKT fit von klein auf

Partizipation
gemeinsam gestalten

Arbeit
flexibler und mobiler werden

Crowd-Sourcing
Ideen für das Gemeinwesen

.....

Mobilität Älterer
Teilhabe am gesell. Leben

DIGITALES ÖSTERREICH

eine kreative IKT-Branche

Infrastruktur
Standort-vorteile

Ausbildung
Qualitative MitarbeiterInnen

Innovation
fördern und leben

Investition
Sicherstellung privat + öffentl.

.....

Kollaboration
Plattform für Gemeinsames

Die modernste Verwaltung sichern

- **Technologie** führend
- **Vernetzt** über Organisations -grenzen
- **BürgerInnen im Mittelpunkt**
- **Unter-nehmen entlasten**
- **Behörden als Service-Units**
- **.....**

Themen 2015 aus der Bund-Länder-Städte -Gemeinden-Kooperation

Digitale Gesellschaft
- BürgerInnenportal
- BürgerInnenzentriertes eGov
- Cockpit/Status der Verfahren
- Verwaltungsapp
- Partizipation
- Mobilität
- One-Stop-No-Stop

Digitale Wirtschaft
- Elektronische Zustellung
- E-Procurement
- eID für Wirtschafts-anwendungen

Digitale Zukunft
- Big Data
- Cloud
- Elektronischer Dienstleister
- OGD[2]/PSI[3]/ UI[4]

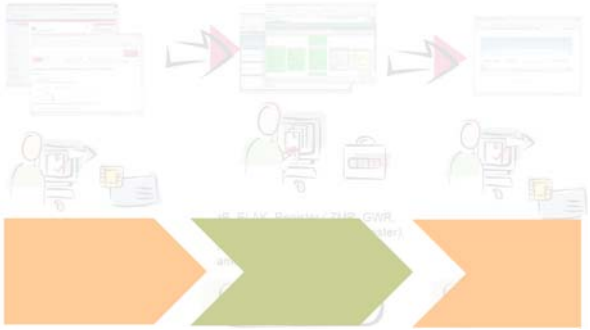
Digitaler Staat
- Amt der Bundesregierung
- Bundesclient und Alternativszenarien
- Einsparungsoptionen
- Register
- Gewerbeinformationssystem
- Verwaltungsstrafen

BürgerInnen im Mittelpunkt

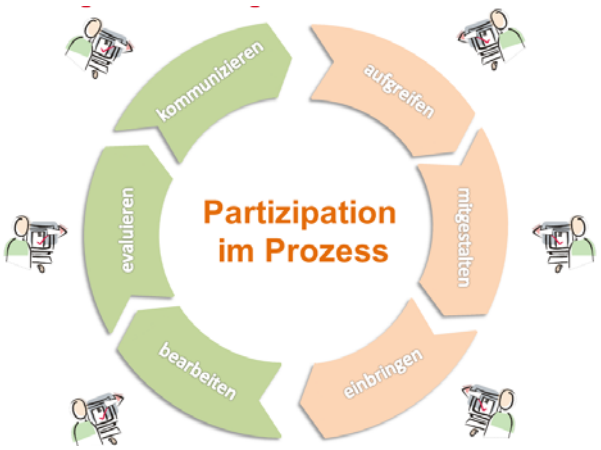
- Recht auf elektronischen Abwicklung (vom Antrag, Statusabfrage, bis zur Zustellung)
- Beteiligung am Prozess (Verwaltung der eigenen Daten, Ideen- und Meinungsbildungsprozesse)
- One und NoStop, pro-aktives E-Government
- Transparenz und Recht auf Zugang zu eigene Daten
- Registerabfrage statt Vorlage von bekannten Daten
- wirksames Datenschutzkonzept

BürgerInnen im Mittelpunkt
Beteiligung am Prozess

- weg von Input-/Output hin zu partizipativen Prozessen



Input-/Output



Behörden als Service-Units

Transparenz - Rohdatenlieferant

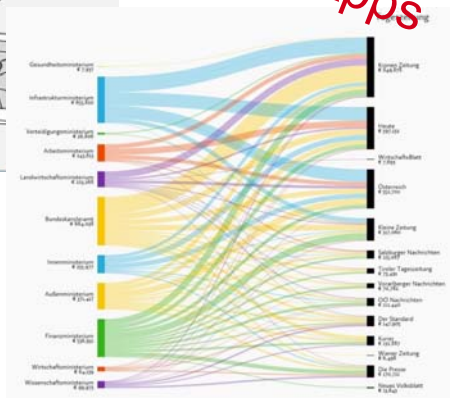
- Open Government Data wird der Normalfall, es werden keine Anwendungen sondern nur mehr Rohdaten bereitgestellt
- Community und die Wirtschaft sorgen für die Visualisierung und Apps
- Verwaltung konzentriert sich auf die Qualitäts-sicherung der Daten
- Synergien mit Daten aus der Wirtschaft erhöhen die Wertschöpfung

„Verwaltung stellt **NUR NOCH** die Rohdaten zur Verfügung“

„Community bzw. Wirtschaft stellt der Verwaltung Apps/Präsentation für den Gebrauch in der Verwaltung zur Verfügung“

Gemeinsam Daten bereitstellen und verwerten!

ca. 1300 Datenbestände
ca. 200 Apps



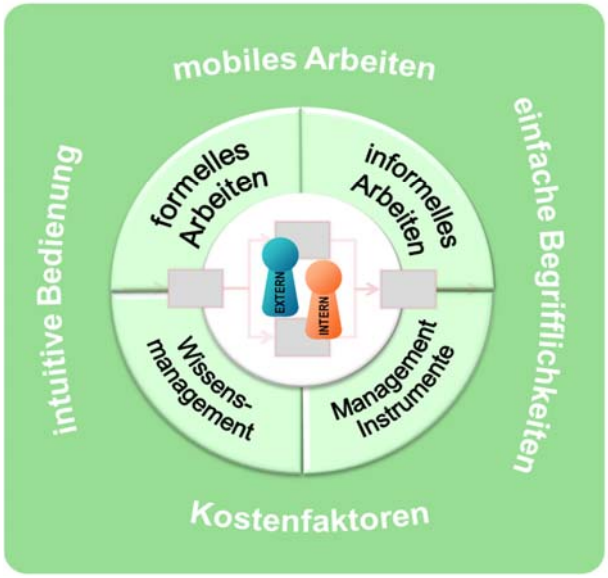
DIGITALES ÖSTERREICH

•Amt der Bundesregierung
•Bundesclient und Alternativszenarien
•Einsparungsoptionen
•Register
•Gewerbeinformationssystem
•Verwaltungsstrafen

Digitaler Staat

Behörden als Service-Units
Arbeitsplatz der Zukunft intern

- Wissens- statt Aktenmanagement (ELAK-APP)
- Wissen teilen und nutzen
- vernetzt statt hierarchisch
- die Amtsstube als Treffpunkt zum Austausch
- mit dem Bürger und Wirtschaft gemeinsam die Verwaltung „bewältigen“
- Fachanwendungen der Verwaltung als Apps auch für unsere MitarbeiterInnen



Arbeitsplatz der Zukunft

DIGITALES ÖSTERREICH

•Amt der Bundesregierung
•Bundesclient und Alternativszenarien
•Einsparungsoptionen
•Register
•Gewerbeinformationssystem
•Verwaltungsstrafen

Digitaler Staat

Unsere MitarbeiterInnen am Collaboration Tisch! Share your place – work together...

DIGITALES ÖSTERREICH

- BürgerInnenportal
- BürgerInnenzentriertes eGov
- Cockpit/Status der Verfahren
- Verwaltungsapp
- Partizipation
- Mobilität
- One-Stop-No-Stop

Digitale Gesellschaft

Behörden als Service-Units
neue Kanäle unterstützen

Auto übernimmt Geschwindigkeitskontrolle

Parkraumbewirtschaftung

DIGITALES ÖSTERREICH

- Elektronische Zustellung
- E-Procurement
- eID für Wirtschafts-anwendungen

Digitale Wirtschaft

Unternehmen entlasten
breitestmögliche elektronische Abwicklung

- Unternehmen wickeln ihre Informationsverpflichtungen den Behörden gegenüber vollkommen elektronisch ab
- Behörden kommuniziert mit Unternehmen nur mehr elektronisch via e-Zustellung; jedes Unternehmen hat ein elektronisches Postfach (nutzbar für Behörden aber auch zwischen den Unternehmen B2B)
- Damit ist Staat Impulsgeber für eine digitale Abwicklung auch B2B (business to business)
- Behörden nutzen die Register für die elektronische Abwicklung und fragen nur mehr nicht bei den Behörden bekannte Daten ab

DIGITALES ÖSTERREICH

Basiselemente
Übersicht

- eine elektronische Identität für Behörden und Wirtschaft (Abschaffung von UserID und Passwort – Handy-Signatur)
- eine E-Zustellung für Behörden und Wirtschaft
- Gemeinsame E-Vertrauensdienste (E-Dokumentenmappe, E-Ausweis, usw.)
- Gesellschaftliche und technologische Trends im Fokus behalten (vorne dabei, aber Beständigkeit wahren)
- Demografische Entwicklung, Digital Gap und Digital Literacy im Fokus halten

DIGITALES ÖSTERREICH

„Weg“ von der Amtsstube hin zu einer digitalen Welt hat schon begonnen!

Danke für Ihre Aufmerksamkeit!

Roland Ledinger
Bundeskanzleramt - Österreich
Bereich IKT-Strategie

Ballhausplatz 1
1014 Wien
ikt@bka.gv.at
www.bka.gv.at

Die offene Stadt - Open Government auf kommunaler Ebene umsetzen

Mag. Bernhard Krabina

KDZ - Zentrum für Verwaltungsforschung

Die offene Stadt

Open Government auf kommunaler Ebene umsetzen

Bernhard Krabina, 11. Juni 2015

Wie entscheiden wir uns?

Wie steuern wir Offenheit?

2010/2011

2012

Wie implementieren wir Open Government?

1. Datentransparenz erhöhen
2. Offene Partizipation verbessern
3. Offene Kollaboration ermöglichen
4. Umfassende Miteinbeziehung realisieren

http://www.kdz.eu/de/open-government-vorgehensmodell

Public Management

Open Government

SMART CITY WIEN

Fokus auf WIE!

- Transparent
- Partizipativ
- Kollaborativ

Fokus auf WAS!

- Lebensqualität
- Ressourcen
- Innovation

Welche Kompetenzen werden wichtiger?

Informations- und Kommunikationskompetenz

Stöcklin, Nando: **Informations- und Kommunikationskompetenz – das «Lesen und Schreiben» der ICT-Kultur**. In: MedienPädagogik – Zeitschrift für Theorie und Praxis der Medienbildung, 22.06.2012. http://www.nandostoecklin.ch/

Kooperationskompetenz

https://www.qualityinconstruction.com/ncr-in-a-construction-project/

Rathje, Stefanie: **Kooperationskompetenz – Cooperation Competence - Toolbox zur Verbesserung der Zusammenarbeit in internationalen Kooperationen**, Verlag Bertelsmann Stiftung, Gütersloh, 2008, ISBN 978-3-86793-007-9

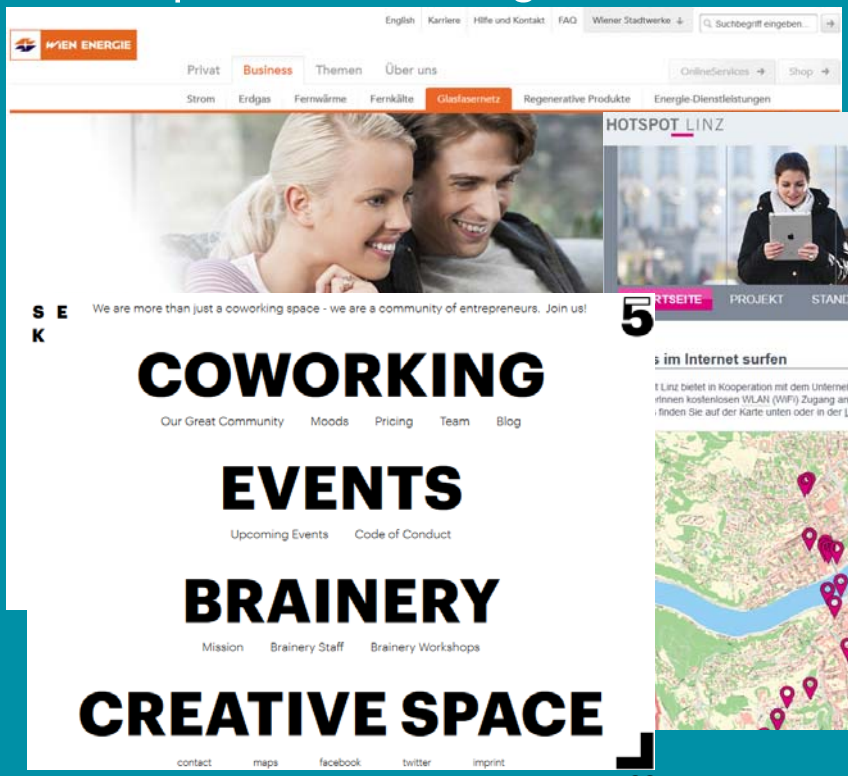
Resilienz

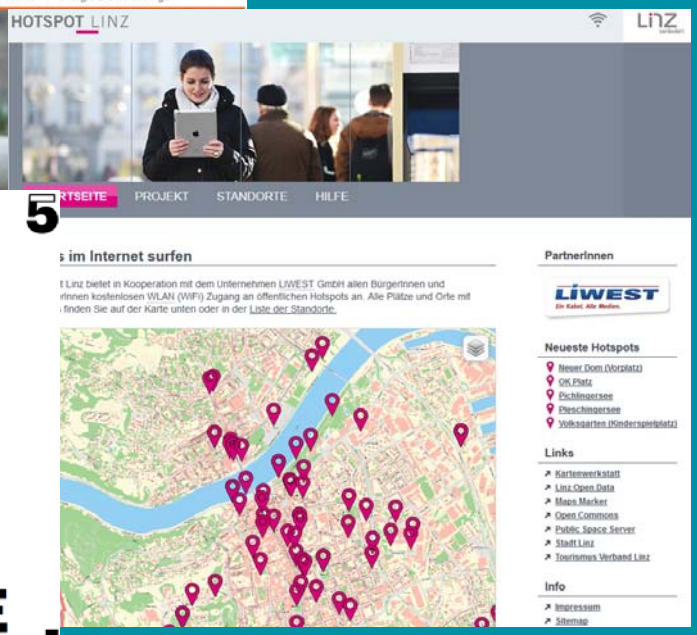
http://blog.team-vision.at/2010/01/02/unwahrscheinlichkeit-der-veranderung/

VÄLIKANGAS, L. (2010). **The Resilient Organization – How Adaptive Cultures Thrive Even When Strategy Fails.** New York: McGraw-Hill.

Welche Basisinfrastruktur brauchen wir?

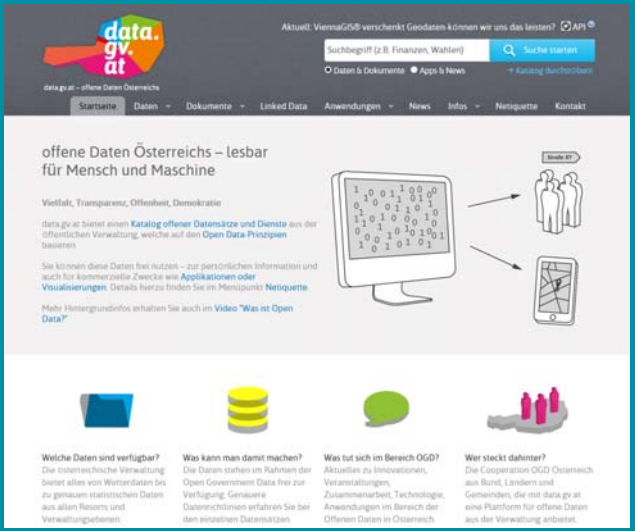
Breitband/Glasfaser/WiFi und Coworking Spaces als digitale Daseinsvorsorge



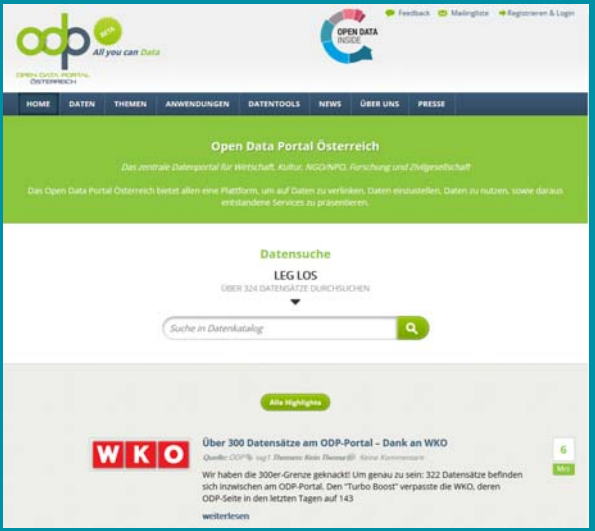


Datenportale

data.gv.at



opendataportal.at



Content

Zivilgesellschaft

Respekt.net
CROWDFUNDING FÜR EINE BESSERE GESELLSCHAFT

FORUM INFORMATIONSFREIHEIT

OPEN KNOWLEDGE FOUNDATION AUSTRIA

Open3 GOVERNMENT DATA SOCIETY

YOUNG CODERS FESTIVAL

FUNKFEUER FREE NET

School of Data Austria

paroli

Open GLAM

OpenGLAM-AT unterstützt kulturellen Einrichtungen (Galerien, Bibliotheken und Museen) in der Veröffentlichung von Daten und Entwicklung neuartiger, partizipative Zugänge zu kulturellen Inhalten.

Informationsfreiheitsgesetz

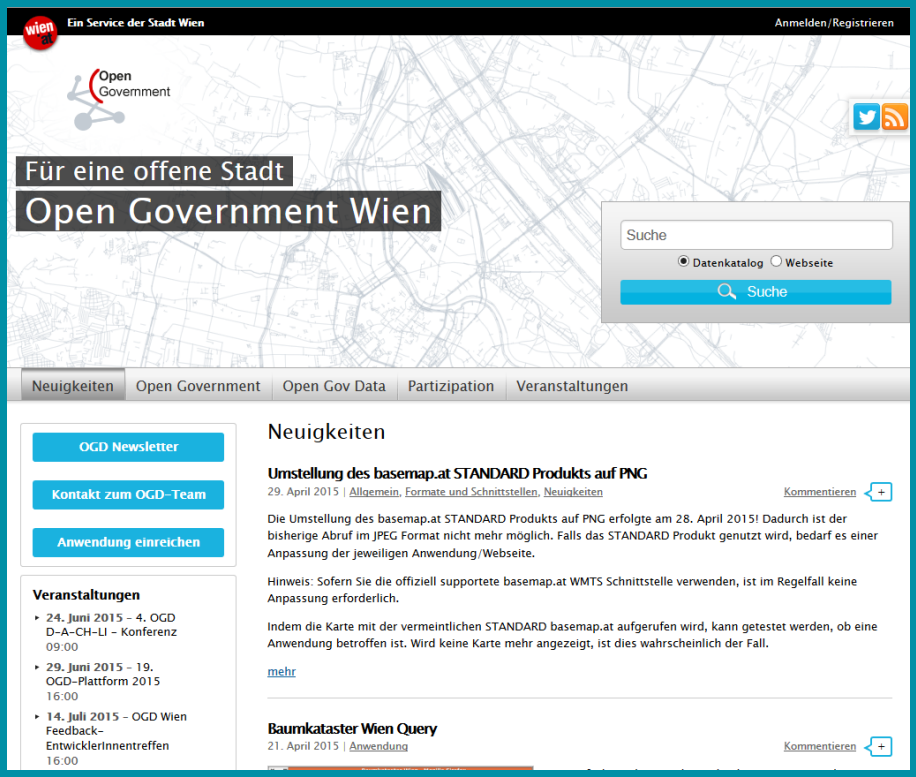
Informationsfreiheitsgesetz ist eine überparteiliche Gruppe, die versucht den Diskurs zwischen den Stakeholdern rund um das Thema Informationsfreiheit zu befördern und zu versachlichen.

netidee powerful innovations

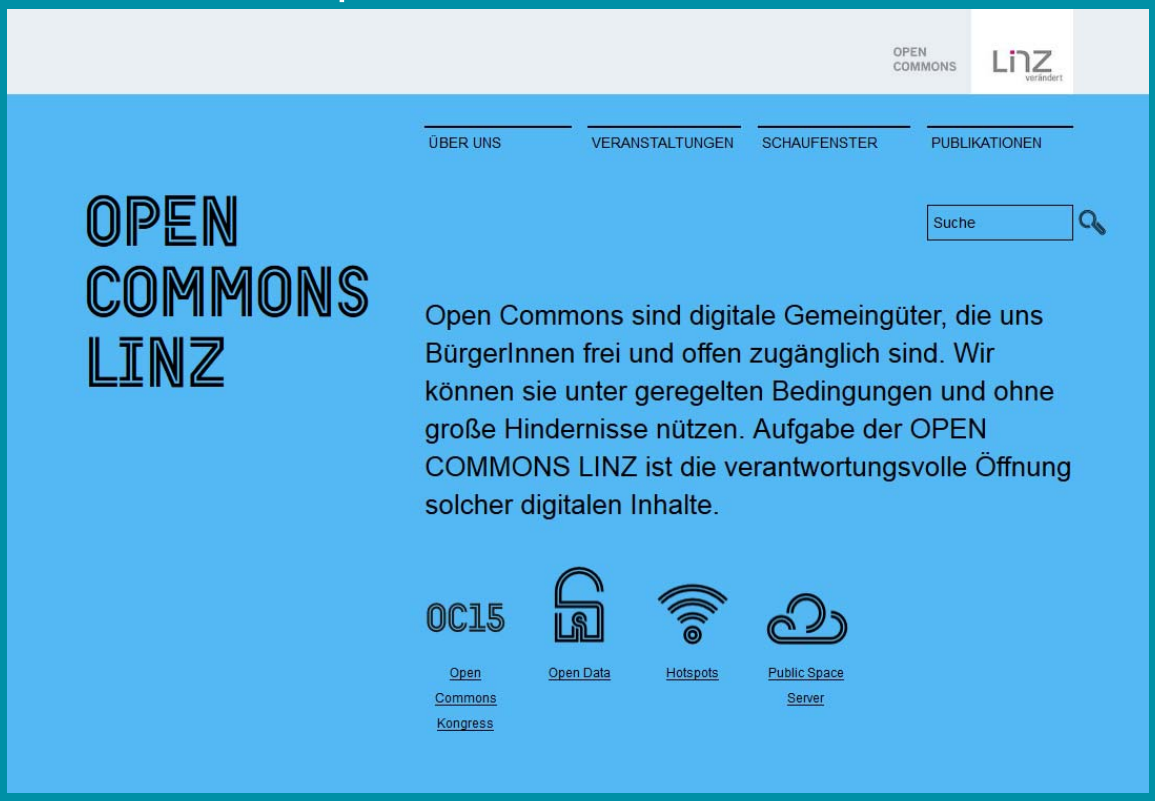
...

Welche Initiativen gibt es?

Open Government Wien

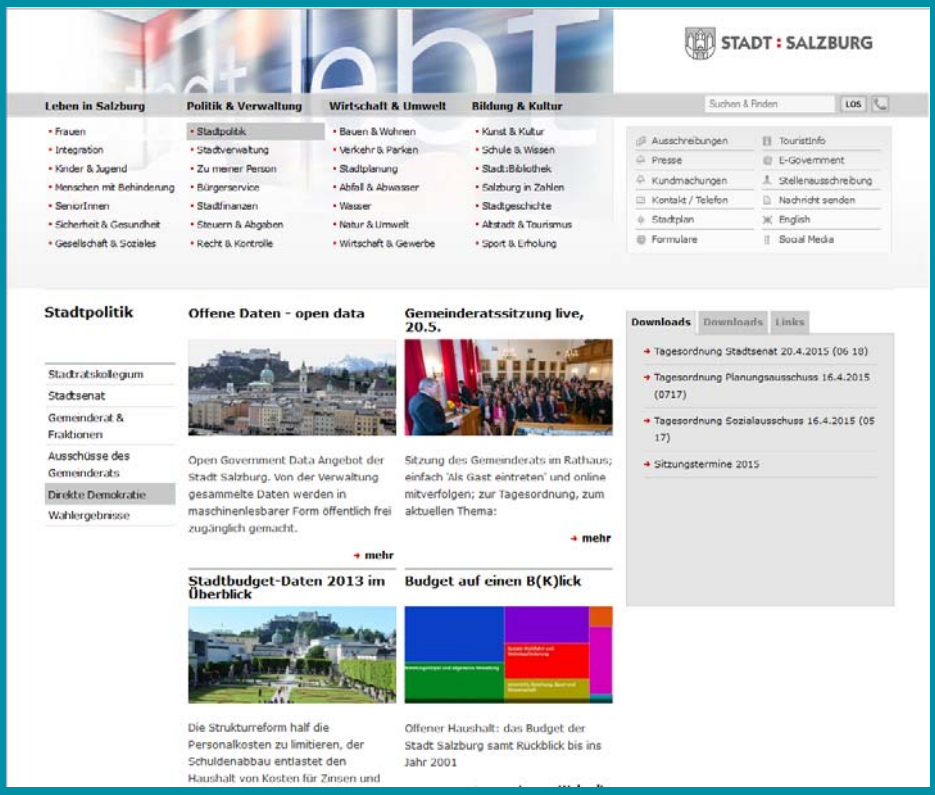


Open Commons Linz

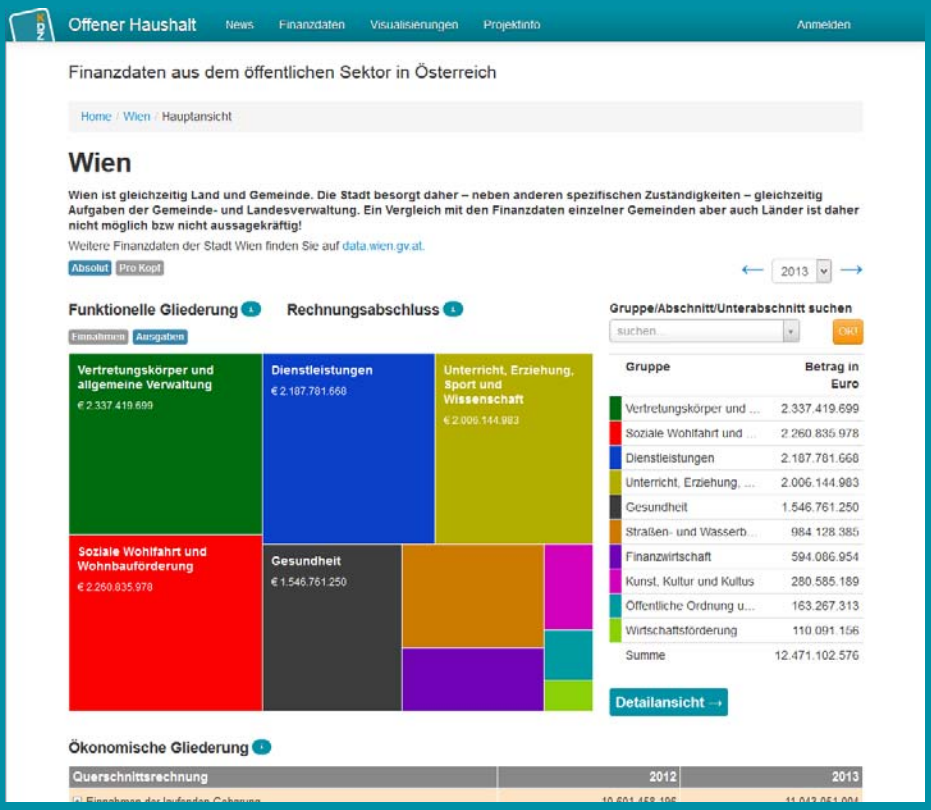


BürgerInnenbeteiligung Graz

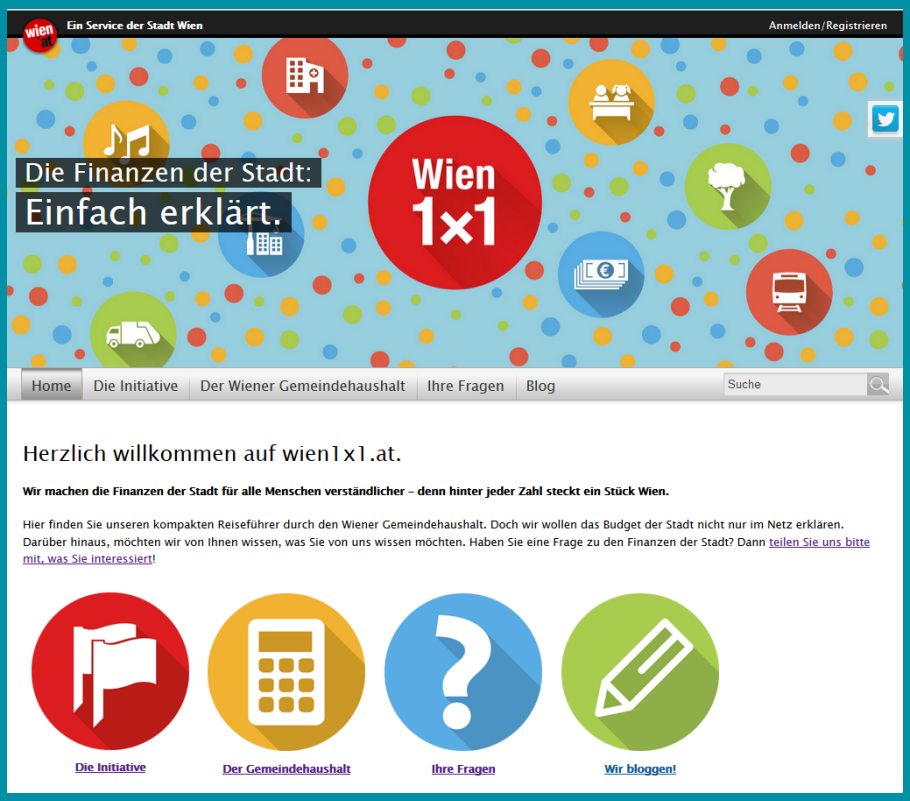
Salzburg macht auf!



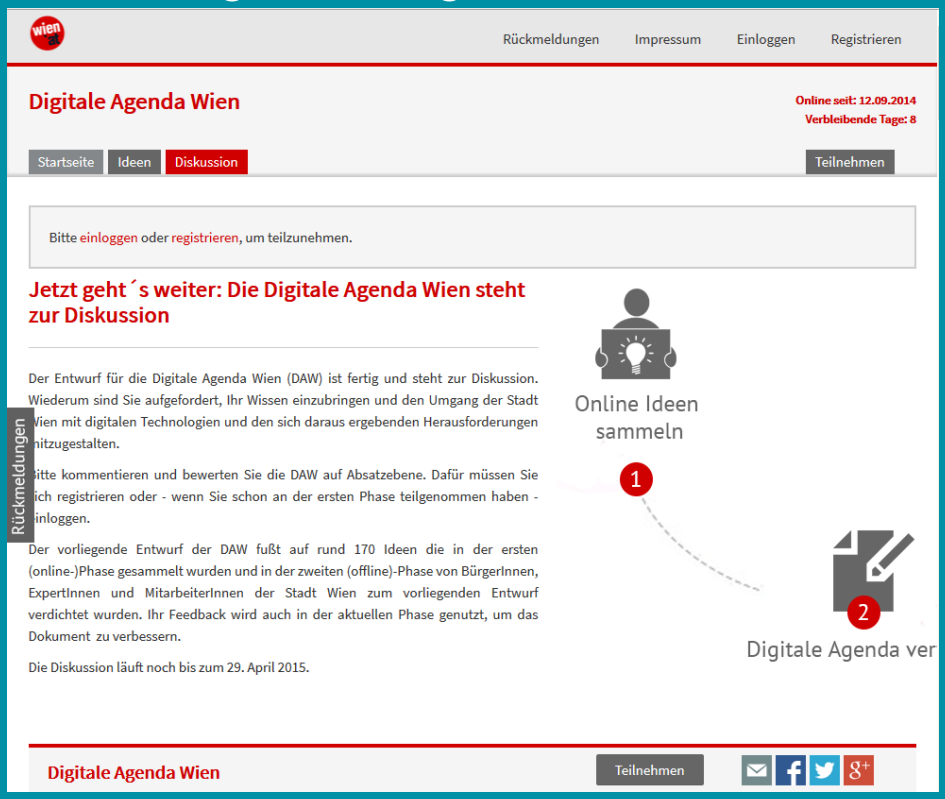
Offener Haushalt.at



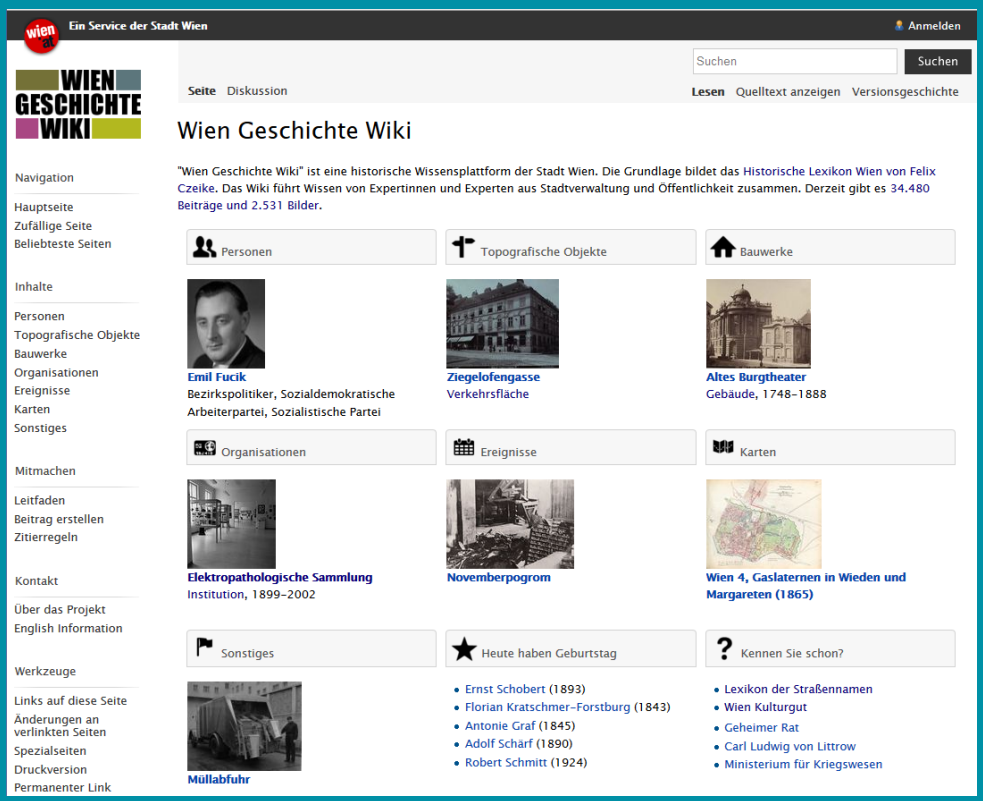
Wien 1x1



Digitale Agenda Wien



Wien Geschichte Wiki



Was wir (nicht) brauchen...

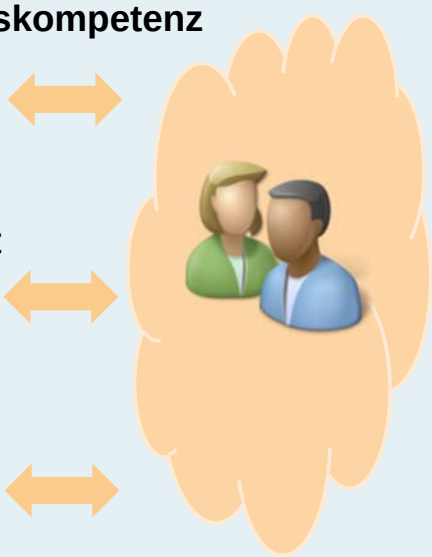
Was wir nicht brauchen...

- Sperren von sozialen Medien am Arbeitsplatz
- Auslagerung/Verlagerung des „Problems“
  - **von der Politik an die Verwaltung**
  - **in der Verwaltung an IT- oder PR-Abteilung**
  - **an Agenturen**
  - **die „jungen“**

Open Government betrifft den Kern von Politik und Verwaltungshandeln!

Was wir brauchen...

- Kompetenzen
  - **Informations- und Kommunikationskompetenz**
  - **Kooperationskompetenz**
  - **Resilienz**
- Infrastruktur
  - **Netze und Vernetzungsmöglichkeit**
  - **Daten und Content**
  - **Zivilgesellschaft**
- Open Government
- Public Value
- Wissensmanagement



Bernhard Krabina

krabina@kdz.or.at

www.kdz.or.at

www.okfn.at

www.schoolofdata.at

www.km-a.net

Twitter: @krabina

"Brauchen wir für das digitale Zeitalter eine neue Werteordnung?"

Joanna Schmölz, MA

DIVSI - Deutsches Institut für Vertrauen und Sicherheit im Internet

"Brauchen wir für das digitale Zeitalter eine neue Werteordnung?"

Wien, 11. Juni 2015
Joanna Schmölz

DIVSI Deutsches Institut für Vertrauen und Sicherheit im Internet

Papstwahl 2005

DIVSI

Papstwahl 2013

DIVSI

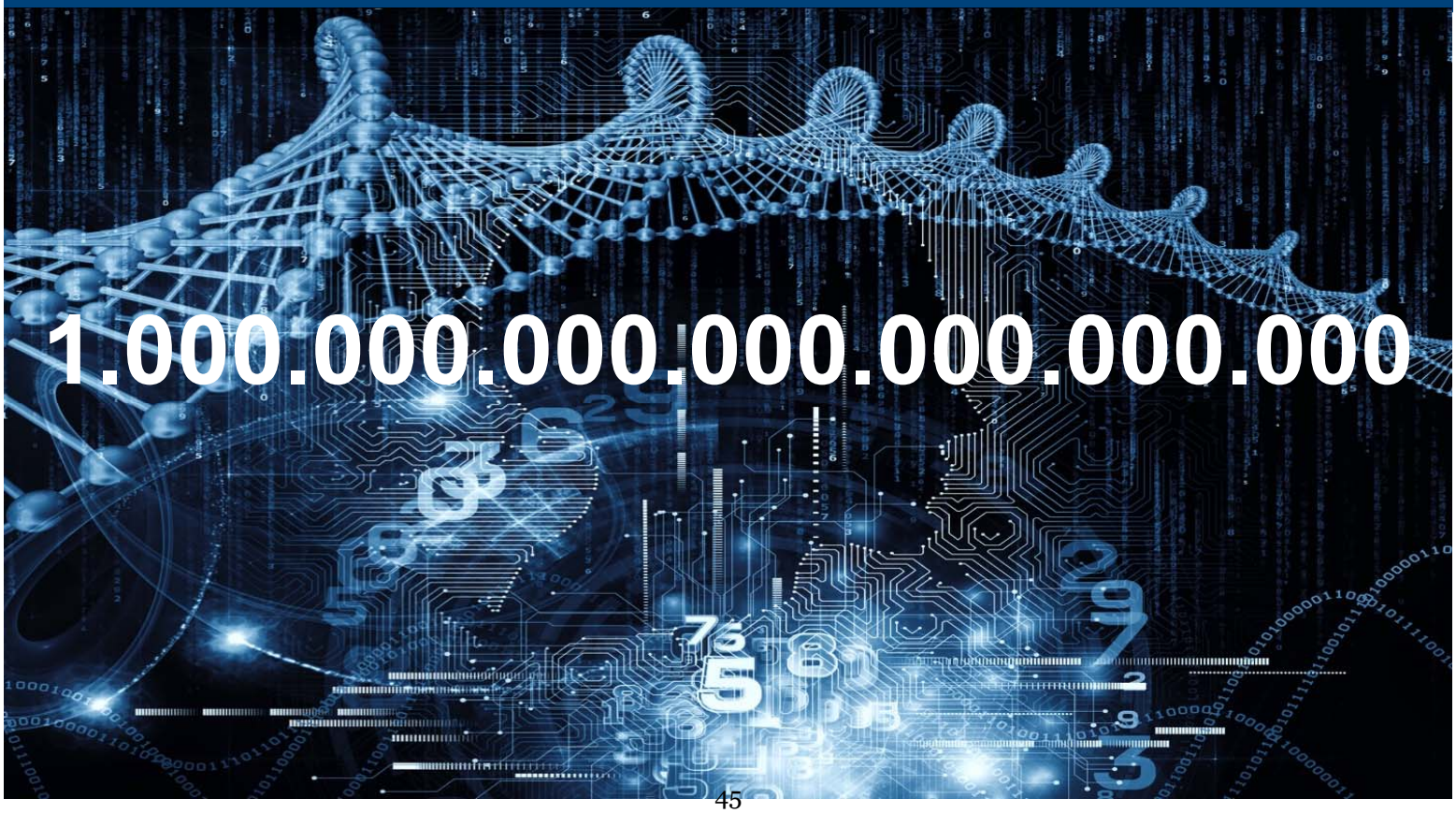
Quelle: Der Spiegel: Digitale Erleuchtung 2013

DIVSI

Digitalisierung: alle Lebensbereiche in allen Lebensphasen

DIVSI

Big Data = a lot of data



Quantified Self - (Selbst)Erkenntnis durch Zahlen?

DIVSI

- Schlafrhythmus und -qualität
- Mentale Leistungsfähigkeit
- Medikamenteneinnahme
- Aktivität / Bewegung
- Puls, Herzfrequenz
- Flüssigkeitszufuhr
- Aufenthaltsorte
- Gewohnheiten
- Produktivität
- Ernährung
- Stimmung
- Konsum
- Gewicht
- ...

Chancen?

Risiken?

Quellen: Apple; © Michael Cogliantry 2012 / The Human Face of Big Data

Aber: Was genau ist „gesund“?

DIVSI

Versicherungsrabatte für „gesund Lebende“

Quelle: shutterstock

Big (Health) Data

DIVSI

Memorial Sloan Kettering & IBM Watson: Advancing the Future of Personalized Cancer Care

Memorial Sloan-Kettering Cancer Center and IBM are developing a powerful tool built upon IBM Watson to help doctors everywhere create individualized cancer diagnostic and treatment recommendations for their patients.

Working with Memorials Sloan-Kettering, IBM Watson will be used to cull through mountains of medical data, helping doctors identify diagnosis and treatment options suited to each patient's specific needs.

Memorial Sloan-Kettering Cancer Center

It can understand 200 million digital pages, and deliver an answer within three seconds.

Together Memorial Sloan-Kettering Cancer Center and IBM will develop a resource built on IBM Watson that incorporates the clinical expertise of MSKCC's cancer experts as well as an extensive library of current published literature on cancer care.

Physicians could tap the system to access relevant cancer care information in order to customize diagnosis and treatment plans for their individual patients. Regardless of where a patient lives or a physician practices, they can have access to a comprehensive source of information.

Chancen

- Bessere und schnellere Diagnosen
- Optimierte Therapien
- Förderung medizinischer Forschung
- Senkung von Gesundheitskosten

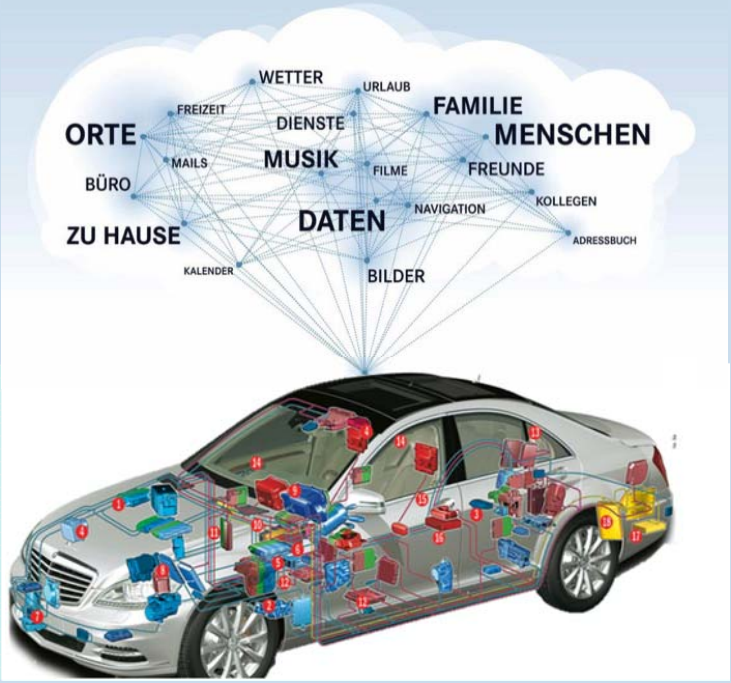
Risiken

- Transparenz des Einzelnen
- Gefahr der Stigmatisierung
- Verlust des „Ausnahmefalls“

IBM

Das vernetzte Auto (connected car)

DIVSI



„Unsere Autos sind heute schon **rollende Rechenzentren** mit 1,5 km Kabeln, mehr als 50 Steuergeräten und der Rechnerleistung von 20 modernen PCs.“

Martin Winterkorn
Vorstandsvorsitzender der Volkswagen AG

Quellen: Daimler; Mercedes-Benz © sueddeutsche.de/Pressinform/gf/goro

self driving car & car-to-x communication

DIVSI

Quelle: BMW

„Das Auto der Zukunft wird mehr und mehr zum digitalen Begleiter. Das bedeutet gleichzeitig, dass es nicht nur verkehrs- und betriebssicher, sondern auch datensicher sein muss.“

Prof. Dr. Thomas Weber
Mitglied des Vorstands der Daimler AG

Mercedes-Benz F 015 Luxury in Motion Self-Driving Car
Quelle: The Verge via http://hypebeast.com

Predictive Policing

DIVSI

„Wenn Einbrecher Ihr Haus ausrauben und in diesem Moment die Polizei vorbeifährt, dann ist das verdammtes **Glück** …
...oder **Big Data**.“

Tobias Schrödel
Ich glaube es hackt; Big Data – Das Ende von Glück und Vielfalt

Quelle: http://ich-glaube-es-hackt.de/wp-content/uploads/2015/03/Cyber-Polizei.jpg

Wenn Algorithmen in Schubladen denken

DIVSI

„Your recent Amazon purchases, tweet score and location history make you 23,5 % welcome here.“

Joanna Schmölz
Stellv. Direktorin DIVSI
joanna.schmoelz@divsi.de
@divsi_info @joschmoelz

+49 40 226 36 98 98 ▪ Mittelweg 110 B ▪ 20149 Hamburg ▪ www.divsi.de

5 Thesen zu Vertrauen und Sicherheit im Internet

DIVSI

1. Das Internet ist eine Kulturleistung der Menschheit von historischer Bedeutung.
Es revolutioniert unsere Arbeit und die Freizeit, unser Denken und die Kommunikation. Deshalb geht das Internet uns alle an – ob wir es schon nutzen oder (noch) nicht.

2. Sicherheit und Stabilität der Internet-Infrastruktur – beides ist unabdingbar.
Sie ist zu einem elementaren Bestandteil des gesamten Wirtschafts- und Sozialraums geworden.

3. Das Internet bietet Möglichkeiten zur Beteiligung an der Gestaltung von Staat und Gesellschaft.
Es fördert Wohlstand, Bildung, Chancengerechtigkeit und Informationsfreiheit. Seine enorme gestalterische Kraft braucht jedoch das Vertrauen der Menschen, damit sie sich entfalten kann.

4. Nutzer, Wirtschaft und Staat haben eine gemeinsame Pflicht, Grundregeln für den Umgang miteinander im Internet auszuhandeln und für deren Verbindlichkeit zu sorgen.
Dabei sind Wirtschaft und Staat gefordert, die Nutzer in die Lage zu versetzen, dieser Verantwortung gerecht zu werden.

5. Freiheit und Sicherheit sind Grundbedürfnisse – auch im Internet.
Voraussetzung dafür ist das Vertrauen darauf, dass der Staat und alle anderen Internet-Akteure diese Grundbedürfnisse mit geeigneten Maßnahmen angemessen ausbalancieren.

„DIE“ digitale Gesellschaft? – Gibt es nicht!

DIVSI

Zwei Männer mit vielen Gemeinsamkeiten...

...leben in unterschiedlichen Lebenswelten...

...und würden auf die meisten Fragen, vermutlich nicht gleich antworten.

1948 geboren, in Großbritannien aufgewachsen, verheiratet, mit inzwischen erwachsenen Kindern, beruflich erfolgreich und vermögend, urlauben vorzugsweise im Alpenraum

Die Zukunft des Digitalen liegt in unserer Hand

Mag.a Meral Akin-Hecke

Digital Champion Austria

Städte und Gemeinden im digitalen Zeitalter
Wissen.Offenheit.Bildung.Sicherheit

Präsentation: Mag. Meral Akin-Hecke, Digital Champion Austria

Die Zukunft des Digitalen liegt in unserer Hand

Nur eine Gesellschaft, die die digitalen Kompetenzen als Grundlage der heutigen Zeit begreift - wie lesen, schreiben und rechnen - schafft auch die Voraussetzungen für technische Innovation, wirtschaftliche Konkurrenzfähigkeit und eine digital selbstbestimmte Gesellschaft. Das erfordert aber ständige Weiterbildung. Darum muss die Schließung der digitalen Kluft das vorrangige Ziel der österreichischen und europäischen Politik sein.

Die Digitalisierung öffnet jedem einzelnen Menschen ein Meer an Möglichkeiten. Möglichkeiten wie sie keine Generation davor hatte. Doch um die Möglichkeiten auch zu nutzen, braucht es die nötige digitale Kompetenz.

Das beste Mittel um sich konkurrenzfähig zu halten ist immer noch Bildung. Nur wer genug über all die digitalen Möglichkeiten und Herausforderungen weiß, kann die richtige Entscheidung treffen, wie er damit umgehen möchte. Darum muss Österreich die digitale Kluft schließen und für die Weiterbildung aller seiner Bürgerinnen und Bürger sorgen. Nur so weiß man welche Möglichkeiten - und welche Alternativen man hat.

Um sich aktiv bei den zukünftigen Diskussionen zu digitalem Wandel und digitaler Transformation einzubringen bzw. um Gefahren und Risiken im Vorfeld zu erkennen und sich darauf vorbereiten zu können, ist es wichtig die Fähigkeiten, die dazu notwendig sind, im Vorfeld zu erlernen, und das kritische Denken, das dafür erforderlich ist, anzutrainieren. Sonst bleiben wir immer nur passive „Nutzer_innen“ der Plattformen oder „Abhängige“ von Webdiensten.

Was Europa stark macht, sind ihre Werte, um diese Werte auch im Digitalen leben zu können, müssen wir uns von der Nutzungsabhängigkeit lösen und die Produzenten Rolle einnehmen.

Um diesen Weg einzuschreiten bietet WerdeDigital.at allen eine Anschlussmöglichkeit an, sich über den Leitfaden „Das neue Arbeiten im Netz“ das Wissen zunächst in Buchform zu holen (Leitfaden als e-Book / pdf zum Download bzw. als Buch zu bestellen unter leitfaden.werdedigital.at). In weiterer Folge können sich Interessierte durch die wöchentliche WerdeDigital.at Webinarreihe die Praxis aneignen, sich mit anderen austauschen, so Ängste abbauen und konkrete Szenarien austesten.

Mag. Meral Akin-Hecke, Digital Champion Austria

Meral Akin-Hecke ist Österreichs erste Botschafterin für digitale Medienkompetenz. Sie wurde auf Ersuchen der EU Kommission für die Digitale Agenda, im Jahr 2013 vom österreichischen Bundeskanzleramt bestellt. Sie schafft österreichweites Bewusstsein für die Wichtigkeit digitaler Medienkompetenz und berät die EU Kommission zur digitalen Agenda für Europa. Ihre Aufgabe ist es möglichst vielen ÖsterreicherInnen den Weg ins Netz zu ebnen und sie beim Umgang mit digitalen Medien zu unterstützen. Der Verein „Institut zur Förderung digitaler Mediennutzung“, dem Meral Akin-Hecke vorsteht, will mit dem vorliegenden Projekt einen Beitrag zu den Zielen der „Digital Champions“ leisten.

Von 2007 bis 2013 leitete sie die gemeinnützige Initiative Digitalks - das österreichische Netzwerk für digitale Medien - um EndanwenderInnen und Firmen über neue digitale Technologien, Social Media und mobiles Arbeiten aufzuklären und zu informieren. Im Executive Board der Open Knowledge Foundation Austria unterstützt sie den Open Knowledge Gedanken. Zuvor war die Wirtschaftsinformatikerin als Anwendungsberaterin und Projektleiterin bei SAP Österreich und ORF tätig.

https://www.digitalchampion.at
https://www.werdedigital.at

"Wie sicher bin ich im mobilen Netz?"

Joe Pichlmayr (Geschäftsführer)
Sebastian Bachmann

IKARUS Security Software GmbH

Social Media und Fake Profile

Ohne Social Media Profil können sich viele Menschen ein Leben im Internet nicht mehr vorstellen. Die aktuelle Stimmung, Fotos vom Essen und neuste Errungenschaften werden in Sozialen Netzen geteilt und so einer großen Masse von Personen zur Verfügung gestellt.
Auch Promis und Personen des öffentlichen Interesses finden Gefallen an solchen Seiten, da sich hier eine breite Masse an Personen sehr einfach und ohne große Kosten ansprechen lässt.

Wer allerdings wirklich hinter einem Profil im Internet steht lässt sich nur schwer erahnen. Natürlich gibt es Fotos der Nutzer, doch wer stellt sicher, dass dies echte Fotos sind oder sie nicht mit Photoshop geschönt wurden? Sucht man nach einer gewissen Person im Internet, so finden sich sehr viele mit dem gleichen Namen und da die Fotos nicht unbedingt von der gesuchten Person stammen müssen, ist es sehr schwer überhaupt einer Person ein bestimmtes Profil zuzuordnen.

Informationen im Internet verbreiten sich meist wie ein Lauffeuer und sind kaum aufzuhalten wenn sie sich einmal den Weg durch diverse Foren und Social Media Seiten gebahnt haben. So ist es zum Beispiel sehr schwer Falschmeldungen zu revidieren und Zeitungsenten bleiben ewig in den Netzen hängen.

Was also nun passiert wenn Fake-Profile eine solche Falschmeldung herausbringen kann man sich ausmalen. Dennoch lassen sich solche Falschmeldungen meist relativ leicht erkennen, da sie eher Humoristisch gemeint sind und oft auch von der Presse als solche entlarvt werden.
Problematisch wird es allerdings, wenn nicht mehr Humor im Vordergrund steht sondern die Schädigung einer Person. Stellen Sie sich vor einer Ihrer Freunde im Sozialen Netzwerk schreibt auf einmal Botschaften wie „Ich hasse euch alle!“. Würden Sie darauf tippen, dass sein Account übernommen wurde, dass die Person wohl eher ein wenig zu viel getrunken hat oder dass sie es gar ernst meint?
Noch viel Problematischer wird es, wenn das Profil welches diese Botschaften schreibt gar nie gekapert wurde, sondern von vorne hinein als Fake Profil erstellt wurde und sich einfach nur wie die Person verhält, welche es ausgibt zu sein.
Die Angreifer verfahren hier nach einem sehr einfachen Schema: Zunächst wird ein Profil einer bekannten Person angelegt. Dann werden Freunde akquiriert. Am Anfang ist dieser Prozess mühsam, danach wird es jedoch sehr viel einfacher, denn wenn sie einer Person eine Freundschaftsanfrage schicken welche bereits einen gewissen Freundeskreis mit ihnen teilt, ist die Chance sehr viel höher, dass Sie diese annehmen werden.

Doch solche Fake Profile werden nicht nur mit dem Namen von bekannten Personen angelegt um diese öffentlich bloßzustellen. Eine weit verbreitete Masche in sozialen Netzwerken ist es, durch gut gestaltete Fake Profile besonders viele Freunde zu bekommen und dann Schadsoftware an diese zu verteilen. Dies funktioniert besonders gut, wenn das Vertrauen der Freunde groß ist. Umso besser das Profil dabei gestaltet ist und umso besser man sich mit dem Profil identifizieren kann, desto besser wird dies funktionieren.

Doch damit nicht genug. Durch geschicktes Social Engineering können Sie ihr Opfer auch dazu bringen ihnen Geld zu überweisen oder Tätigkeiten auszuführen. Denken Sie etwa daran, wenn Ihnen ein vermeintlich „guter Freund“ schreibt er ist gerade knapp bei Kasse und bräuchte dringend 500€ um dringende Rechnungen zu zahlen.

Oder eine „Person aus der Personalabteilung“ ihrer Firma schreibt Ihnen dass sie demnächst gekündigt werden. Mit welchem Gefühl würden Sie dann am nächsten Tag ins Büro gehen?

All diese Angriffsmethoden haben einen Namen: Joe-Jobs. Der Name kommt vom Administrator Joe Doll, unter dessen Namen Mails verschickt wurden um dessen Ruf zu schädigen.
Die gleichen Prinzipien wenden heute Angreifer im Social Media Kontext an.

Doch wie schützt man sich nun gegen solche Angriffe? Die Lösung zu diesem Problem ist sehr einfach: Nehmen sie nur Kontakte an, welche sie auch schon im realen Leben „verifiziert“ haben. Wenn Sie eine Kontaktanfrage bekommen, rufen Sie die Person einfach an und fragen nach ob das korrekt ist.
Die meisten sozialen Netze bieten zudem auch eine Verifikation von Profilen an. Bei Twitter etwa gibt es verifizierte Accounts, das bedeutet das die Person welche ausgibt dieser Account zu sein, auch tatsächlich diese Person ist. Natürlich schützt diese Verifikation nicht davor, dass der Account einmal gehacked wird und darüber Rufschädigung betrieben wird.
Daher gilt hier, nicht immer alles glauben was im Internet geschrieben wird. Wenn man die Person kennt, sollte man Sie am einfachsten persönlich darauf ansprechen.

Sicherer Umgang im Internet und in WLAN Hotspots

Das Internet ist heute allgegenwärtig. Fast jede Software benötigt einen Zugang zum Netz und viele Prozesse lassen sich nur so effizient mit der IT umsetzen da Daten zu jeder Zeit zur Verfügung stehen. So ist es nicht verwunderlich dass in Hotels und öffentlichen Plätzen immer häufiger WLAN Hotspots angeboten werden, auf denen man gratis surfen kann.
Diese Hotspots erfreuen sich großer Beliebtheit, kann man doch auch im Ausland, wo mobile Datentarife sehr teuer sind, trotzdem im Internet surfen.

Doch haben WLAN Hotspots auch einen entscheidenden Nachteil: Jeder der in einem solchem WLAN Netzwerk eingewählt ist, kann die Daten der anderen Teilnehmer ebenfalls lesen. Denn WLAN verhält sich so wie jede andere Funktechnologie auch, jeder der eine Antenne hat und sich in Reichweite des Senders befindet kann die Signale empfangen.
Somit kann ein Angreifer sehr leicht an den gesamten Datenverkehr zwischen Endgerät und Access Point kommen. Überlegen Sie einmal welche Seiten Sie ansurfen, wenn Sie sich in einem WLAN befinden.
Lesen Sie Nachrichten? Loggen Sie sich in Social Media Seiten ein? Verwenden Sie Online Banking? All diese Seitenzugriffe können von einem Angreifer prinzipiell mitgelesen werden. Wenn dabei Zugangs- oder sogar Nutzdaten unverschlüsselt übertragen werden, kennt diese nun ein Angreifer ebenfalls.
Was ein Angreifer mit diesen Daten weiß niemand so genau. Manche Angreifer sehen darin eine Art Sport, so viele Opfer wie möglich zu finden. Andere verkaufen die Daten an dritte weiter und manche Angreifer schlagen selber Profit aus den gewonnenen Informationen.

Doch sind wir überhaupt noch sicher im Netz unterwegs? Spätestens seit den Enthüllungen von Edward Snowden ist klar, dass auch ganze Staaten das Internet systematisch überwachen und es kaum einen Schutz dagegen gibt. Auch steigt die Zahl der sogenannten Cybercrime Angriffe stetig an. Viele Angriffe sind mittlerweile automatisiert und versuchen einfach so viele Systeme wie möglich zu übernehmen um diese Zombies dann zu verkaufen. Ein großer Schwarzmarkt existiert schon seit einigen Jahren, auf dem gekaperte Server, Kreditkartendaten und Kundendaten verkauft werden. Auf

den gleichen Märkten lassen sich im Übrigen auch gleich Exploits und Malware Kits kaufen, mit denen man selber Systeme angreifen kann.
Eine wirklich genaue Antwort kann man auf diese Frage leider nicht geben, denn vor staatlicher Überwachung kann man sich leider nicht wirklich schützen. Dennoch gibt es eine große Menge an Möglichkeiten wie man sich vor dem „Alltagshacker“ oder der „Internetmafia“ schützen kann.

Das Verfahren scheint profan, jedoch ist es auch eines der wirksamsten um sich vor Datendieben zu schützen: Verwenden Sie ein VPN (Virtual Private Network). Bei einem VPN werden die Daten verschlüsselt zu einem Server, welcher in einem Sicheren Netz steht, übertragen und erst von hier zum Zielserver weitergeleitet. Der große Vorteil ist, dass Daten auch über unsichere Kanäle wie eine WLAN Verbindung verschlüsselt übertragen werden und ein Angreifer nun keine Chance hat an diese Daten zu kommen.

Auch die Absicherung des eigenen Rechners ist wichtig. So sind ein aktueller Virenscanner und eine aktive Firewall Pflicht. Vergleicht man einen PC mit einem Haus, so wäre die Firewall mit den Fenstern und Türen zu vergleichen. Wenn man Fenster und Türen schließt, kann von außen niemand mehr hinein, man selber kann das Haus jedoch immer verlassen. Hat man selber einen Schlüssel zur Tür, kann man auch wieder hinein. Eine Firewall erfüllt den gleichen Zweck, in dem sie Daten welche an den PC gesendet werden nur „hinein“ lässt, wenn dies erlaubt wurde. Ebenfalls gibt es Firewalls, welche den Datenverkehr nach außen regeln. Hier ist das umgekehrte Prinzip, es werden nur Verbindungen nach außen gelassen, welche vorher vom Benutzer oder dem IT Administrator erlaubt wurden.
Der Virenschutz könnte man in unserem Hausbeispiel am ehesten mit einem Hausmeister vergleichen, welcher regelmäßig nachschaut ob die Wasser- und Stromleitungen noch in Ordnung sind oder ob sich irgendwo Schädlinge niedergelassen haben. Entdeckt er zum Beispiel Küchenschaben, kann er diese entfernen.
Virenschutz und Firewalls sind im Übrigen nur dann wirksam, wenn sie regelmäßig aktualisiert werden und auch aktiv am System laufen. Ein Hausmeister wird Ihnen nichts über die Küchenschaben Plage berichten können, geschweige etwas dagegen tun, wenn er im Urlaub ist.

Aber auch die beste Verschlüsselung, der beste Virenschutz und Firewall wird nichts bringen, wenn Sie Angreifer aktiv auf Ihr Gerät lassen. Oft passiert das unwissentlich, etwa durch Exploits in Programmen wie Flash oder Java, welche von präparierten Webseiten ausgenutzt werden um Trojaner zu installieren.
Auch Links und Anhänge von Phishing Mails können sich sehr schnell auf einem Gerät ausbreiten.

Gegen diese Art von Angriff hilft nur das eigene Misstrauen zu schärfen und nicht jedem Mail zu glauben. Ist etwas ungewöhnlich, sollte man zunächst mit Misstrauen an die Sache herangehen. Besser man klickt einen Link nicht an, als einmal zu viel. Leider werden Angreifer immer kreativer in der Art wie sie Angriffe planen. Es gibt heutzutage sogar schon Phishing Mails welche eine eigene Telefonhotline besitzen und mit einem die notwendigen Schritte zur Infektion des eigenen Rechners am Telefon durchgehen.

Dennoch erkauft man sich mit allen Sicherheitsmaßnahmen immer nur mehr Zeit, welche der Angreifer braucht um zum Beispiel ein Verschlüsselungsverfahren zu knacken.
Dies ist wie bei einem Fahrradschloss: Alle auf dem Markt befindlichen Schlösser lassen sich irgendwie knacken. Es kommt nur darauf an wie lange der Angreifer braucht und mit welchem Werkzeug er es versuchen muss. An einem gewissen Punkt sind die Kosten für Werkzeug und Zeit zu

hoch und der Angriff lohnt sich wirtschaftlich einfach nicht mehr.
Die Zeit um moderne Verschlüsselungen zu knacken liegt zwar bei einigen Millionen Jahren Rechenzeit, allerdings passieren immer wieder Fehler welche die Zeit sehr weit heruntersetzen können. Und einen Monat Rechenzeit aufzuwenden um etwa geheime Unterlagen zu stehlen ist nicht so abwegig.

Somit ist es ebenfalls wichtig sich Gedanken darüber zu machen, was passiert wenn es doch mal passiert? Es mag zum Beispiel sein, dass ein Laptop perfekt abgesichert über das Internet kommuniziert, sollte er jedoch gestohlen werden sind alle Daten auf der Festplatte für den Angreifer ebenfalls auslesbar, es sei denn die Festplatte ist ebenfalls verschlüsselt.
Ebenfalls sehr unterschätzt sind Passwörter. Denken Sie einmal nach, auf wie vielen Webseiten Sie das gleiche Passwort verwenden. Was würde passieren, sollte einmal eine dieser Webseiten gehacked werden und ihre Login Daten den Weg in die Öffentlichkeit finden. Könnte sich ein Angreifer Zugang zu Ihren Mails verschaffen?
Passwörter sollten nicht nur regelmäßig geändert werden, sondern auch variiert. Im Idealfall hat man für jede Webseite, jeden Dienst und jedes Gerät das man verwendet andere Passwörter. Sie fragen sich nun vielleicht wie man sich das alles merken soll. Dafür gibt es extra Programme, welche genau für diesen Zweck geschrieben wurden – sogenannte Passwortsafes, wie etwa KeePass.

Zusammenfassend kann man folgende Verhaltenshinweise geben, welche einen sichereren Umgang im Internet und in WLAN Hotspots ermöglichen:

- In öffentlichen Netzen immer VPN verwenden
- Alle Endgeräte verschlüsseln. Diese Möglichkeit bieten alle PC und Smartphone Betriebssysteme an!
- Alle Endgeräte mit sicheren PINs oder Passwörtern schützen
- Aktuellen Virenschutz und Firewalls verwenden
- Verwenden von unterschiedlichen Passwörtern und Benutzernamen (Anwendung von Passwortsafes)
- Regelmäßiges ändern von Passwörtern
- Idealerweise kein Flash und Java verwenden
  Falls doch benötigt unbedingt immer Updates installieren und höchste Sicherheitsstufen einstellen (auch „Click to Play“ aktivieren)
- Misstrauen gegenüber ungewöhnlichen Mails und Webseiten
  Keine Links anklicken oder Dateien öffnen, besser an IT weiterleiten und analysieren lassen

NOTIZEN