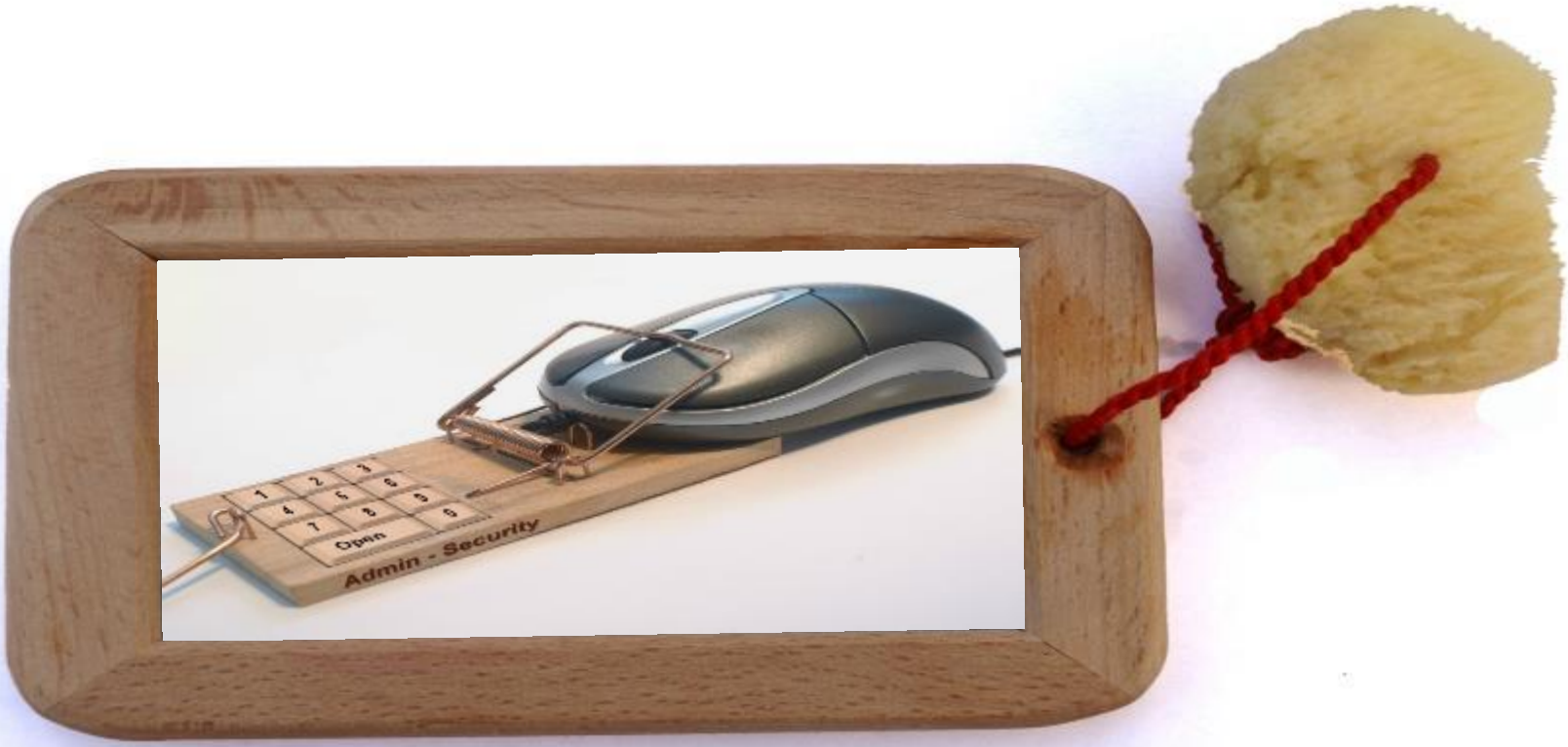


IT-Security für KMU – ein Widerspruch?

Grundlagen – Begriffe – Status Quo – Problemstellungen - Lösungsansätze

HolisticSec
securing is our business

alldata

Vortrag im Rahmen des E-Day 2014– Wien 6.3.2014

Rüdiger Linhart - linhart@alldata.at
Florian Brunner - florian.brunner@holisticsec.com

„I think, there will be a market for maybe five computers“

Thomas J. Watson (CEO IBM, 1943)

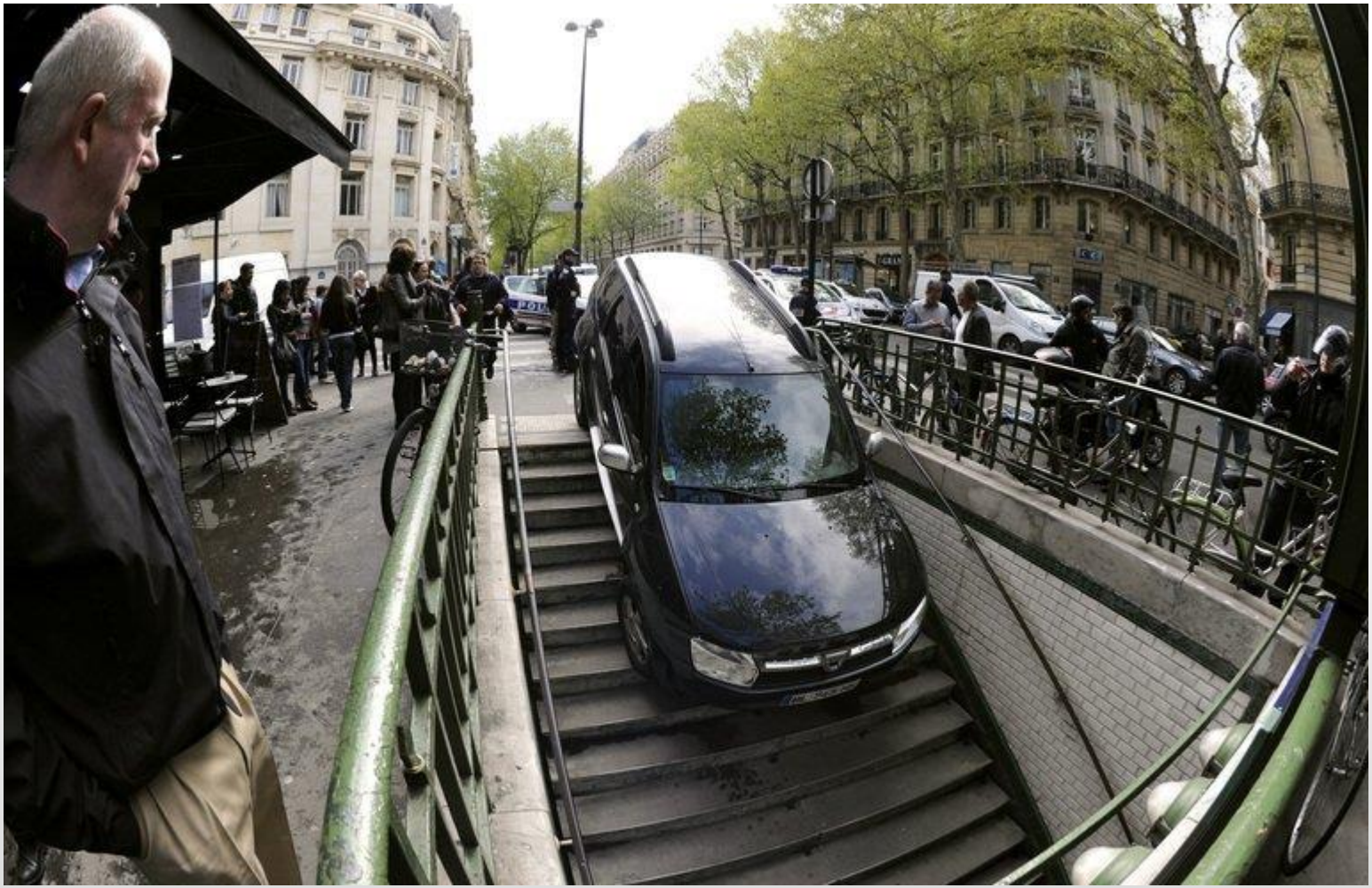
IT- und Datensicherheit bei KMU?

98 % Internetnutzung

85 % Website

Q: STATISTIK AUSTRIA, Europäische Erhebung über den IKT-Einsatz in Unternehmen 2013. Erstellt am 21.10.2013
http://www.statistik.at/web_de/statistiken/informationsgesellschaft/ikt-einsatz_in_unternehmen/022195.html

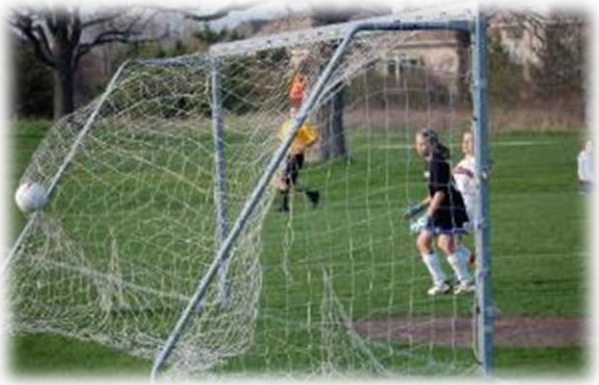
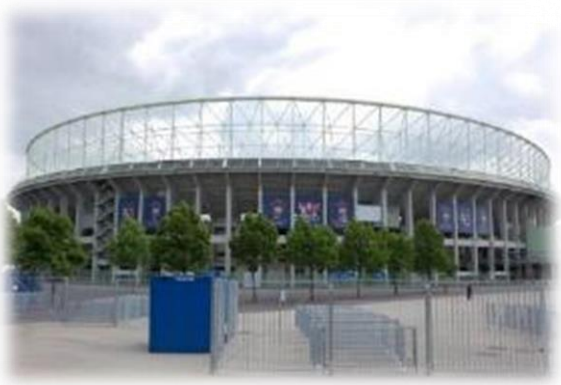
Haben KMU ein Problem?



Quelle: Betrand Guay - AFP

Haben KMU ein Problem?

Viren	Trojaner	Backdoors	Scareware
Spyware	Adware	Hacker	Ex-Mitarbeiter
Physische Zerstörung	NSA & Co	Phishing	Fehlbedienung


KMU und EPU

Kategorie	Angestellte	Umsatz oder	Bilanzsumme
Micro	< 10	≤ € 2.0 mio	≤ € 2.0 mio
Small	< 50	≤ € 10.0 mio	≤ € 10.0 mio
Medium-Sized	< 250	≤ € 50.0 mio	≤ € 43.0 mio

Fußballtor. Quelle: http://www.flickr.com/photos/keithminer CC-BY-2.0
Ernst Happel Stadion: Cha già José from Vienna, Austria (Ernst-Happel-Stadion Uploaded by darkweasel94) CC-BY-SA-2.0
Sotschi Quelle: Team Evergreen/nextstop.at

KMU und EPU - Statistikwerte

KMU-Daten für Österreich — Beschäftigtendaten

Dezember 2012	Beschäftigtengrößengruppen	Anzahl der Unternehmen [1]	*Anteil in %*	Anzahl der unselbständig Beschäftigten [2]	*Anteil in %*
WIRTSCHAFTSKAMMERBEREICH		404.690	*100,0*	2.272.260	*100,0*
	0 - 9	372.895	*92,1*	351.468	*15,5*
	10 - 49	25.754	*6,4*	513.338	*22,6*
	50 - 249	4.952	*1,2*	500.805	*22,0*
	250 und mehr	1.089	*0,3*	906.649	*39,9*

Bei diesen Daten handelt es sich um Ergebnisse einer Unternehmensauswertung, wobei die Klassifikation der Unternehmen nach dem Tätigkeitsschwerpunkt erfolgt.

[1] die Daten der WKO-Beschäftigungsstatistik für den Bereich der Wirtschaftskammern sind das Ergebnis einer breit angelegten Transformation von ÖNACE-basierten Daten auf solche nach der Kammersystematik. Im Vergleich zu den Statistiken des Hauptverbandes der Sozialversicherungsträger, die nur sog. Arbeitgeberbetriebe, also Betriebe mit mindestens einem unselbständig Beschäftigten ausweisen, beinhalten die Ergebnisse der WKO-Beschäftigungsstatistik (Basis Registerdaten) auch Unternehmen ohne unselbständig Beschäftigte. Diese Gruppe von Unternehmen war im Jahr 2010 durch Änderungen in den Aufnahme- und Bestandskriterien im verwendeten Unternehmensregister (UR) von einem massiven Anstieg der erfassten Einheiten betroffen. Während für Unternehmen mit unselbständig Beschäftigten die Kriterien für den Status ‚wirtschaftlich aktiv' im UR in etwa die gleichen sind wie für die Mitglieder der WKO, ist dies für Unternehmen ohne unselbständig Beschäftigte auf Grund der genannten Änderungen nicht der Fall. Dadurch müssen weitere Kriterien zur Masseeingrenzung vorgegeben werden, damit das Verhältnis der aktiven Mitglieder der WKO zur Zahl der aktiven Unternehmen im UR gewahrt bleibt. Für die Referenzperioden 2010 bis 2012 bedeuten diese Änderungen, dass die Zahl der Arbeitgeberunternehmen sehr wohl mit den jeweiligen Ergebnissen früherer Jahre vergleichbar ist, die Zahl der Unternehmen ohne unselbständig Beschäftigte hingegen nicht.

[2] Beschäftigungsverhältnisse (ohne geringfügig Beschäftigte, ohne öffentlicher Dienst)

Quelle: WKO Beschäftigungsstatistik in der Kammersystematik; 1. Aufarbeitung

Quelle: wko.at/Statistik/kmu/WKO-BeschStatk.pdf, Abgerufen 2014-02-25

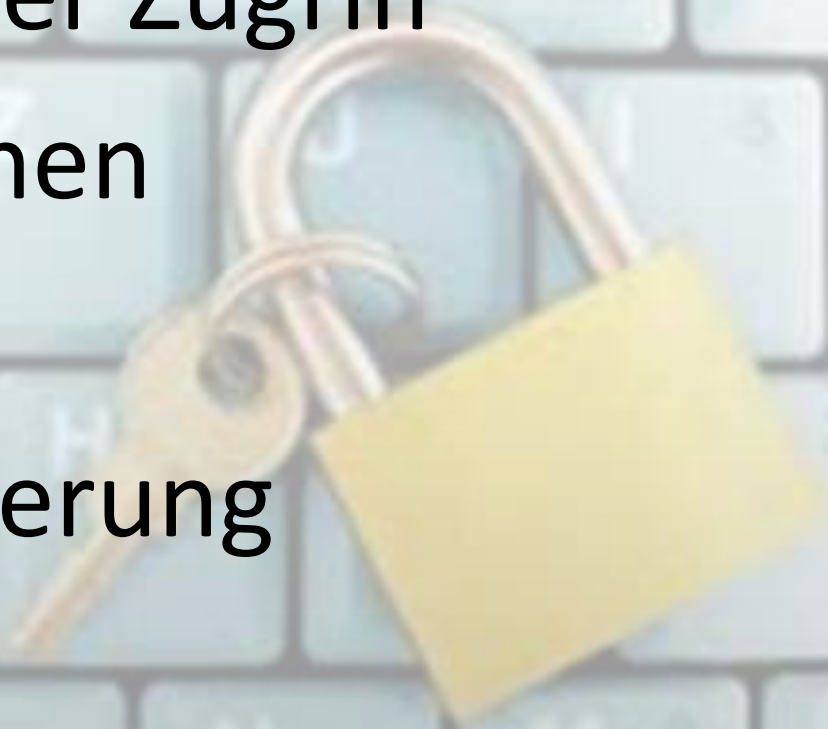
Problemstellungen bei KMU?

Mangel an IT-Know-How

- Fachpersonal
- Mitarbeiterbindung
- Ausbildungsbudget
- Aufgabenverteilung
- Intern/extern
- Schnelllebigkeit

Datensicherheit

- unberechtigter Zugriff
- Manipulationen
- Datenverlust
- Risikominimierung



Andrea & Bernd (alias Alice & Bob)

- Vertraulichkeit
- Integration
- Authentizität
- Nichtabsteitbarkeit
- Authentifizierung
- Verfügbarkeit

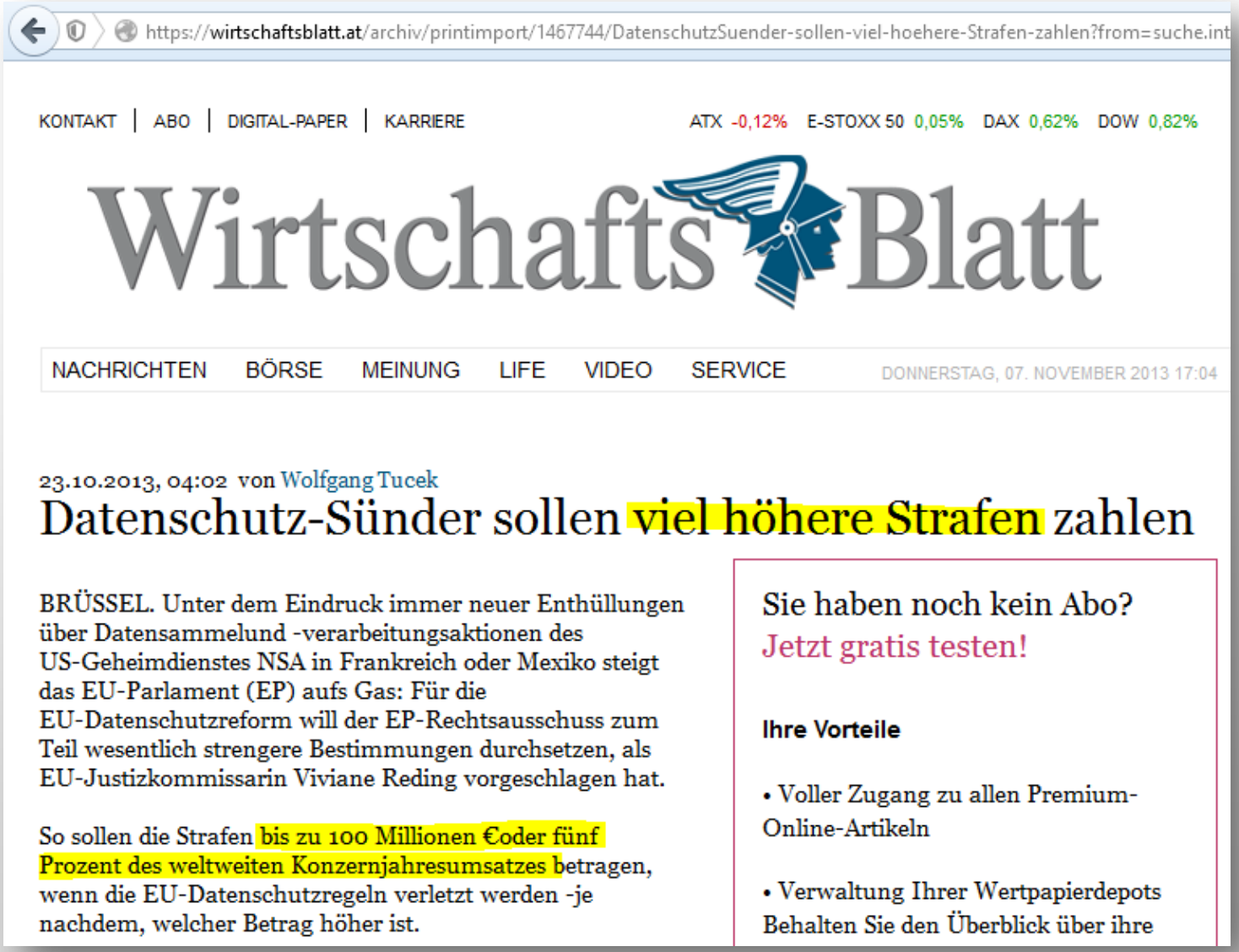
Verfügbarkeit

Hochwasser 2002/Schwertberg © GWB
Linz, Flussdialog Oberösterreich

Datenschutz

Datenschutz bezeichnet die notwendigen Maßnahmen, um den **Einzelnen** davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem **Persönlichkeitsrecht** verletzt wird.

Datenschutz



https://wirtschaftsblatt.at/archiv/printimport/1467744/DatenschutzSuender-sollen-viel-hoehere-Strafen-zahlen?from=suche.int

KONTAKT | ABO | DIGITAL-PAPER | KARRIERE ATX -0,12% E-STOXX 50 0,05% DAX 0,62% DOW 0,82%

Wirtschafts Blatt

NACHRICHTEN BÖRSE MEINUNG LIFE VIDEO SERVICE DONNERSTAG, 07. NOVEMBER 2013 17:04

23.10.2013, 04:02 von Wolfgang Tucek

Datenschutz-Sünder sollen viel höhere Strafen zahlen

BRÜSSEL. Unter dem Eindruck immer neuer Enthüllungen über Datensammelund -verarbeitungsaktionen des US-Geheimdienstes NSA in Frankreich oder Mexiko steigt das EU-Parlament (EP) aufs Gas: Für die EU-Datenschutzreform will der EP-Rechtsausschuss zum Teil wesentlich strengere Bestimmungen durchsetzen, als EU-Justizkommissarin Viviane Reding vorgeschlagen hat.

So sollen die Strafen bis zu 100 Millionen €oder fünf Prozent des weltweiten Konzernjahresumsatzes betragen, wenn die EU-Datenschutzregeln verletzt werden -je nachdem, welcher Betrag höher ist.

Sie haben noch kein Abo?
Jetzt gratis testen!

Ihre Vorteile

• Voller Zugang zu allen Premium-Online-Artikeln

• Verwaltung Ihrer Wertpapierdepots Behalten Sie den Überblick über ihre

Recht haben oder nicht?

Wollen Sie mit dem

CHEF

sprechen?

Oder mit Jemand der sich

auskennt?

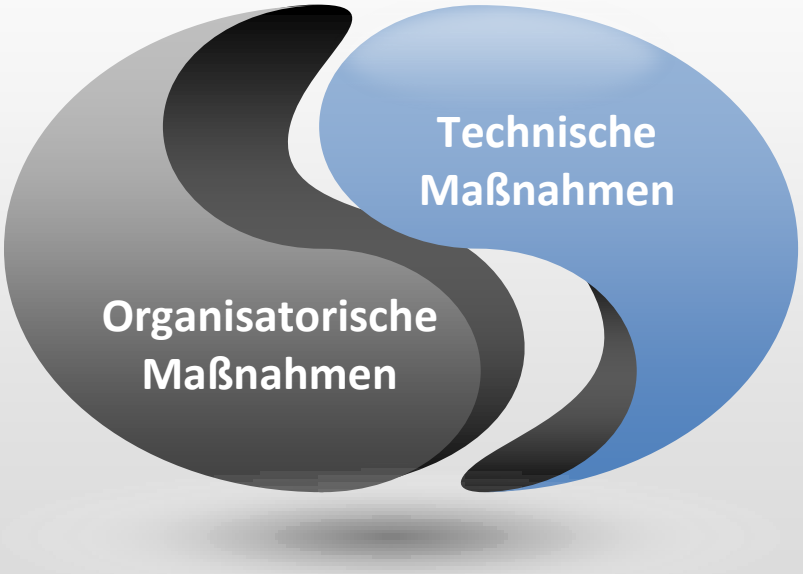
© RAHMENLOS München

Problembeispiele

Virenschutz veraltet	WLAN – Geräte	Router vom Provider offen	Software wird einfach installiert
Überall das gleiche Passwort	Surfverhalten	Datensicherung nur auf USB-Stick	Phishing – „Glaube an das Gute“
Handies/Tablets sind auch Computer	Adminrechte	„Firewall stört“	Konfigurations-fehler

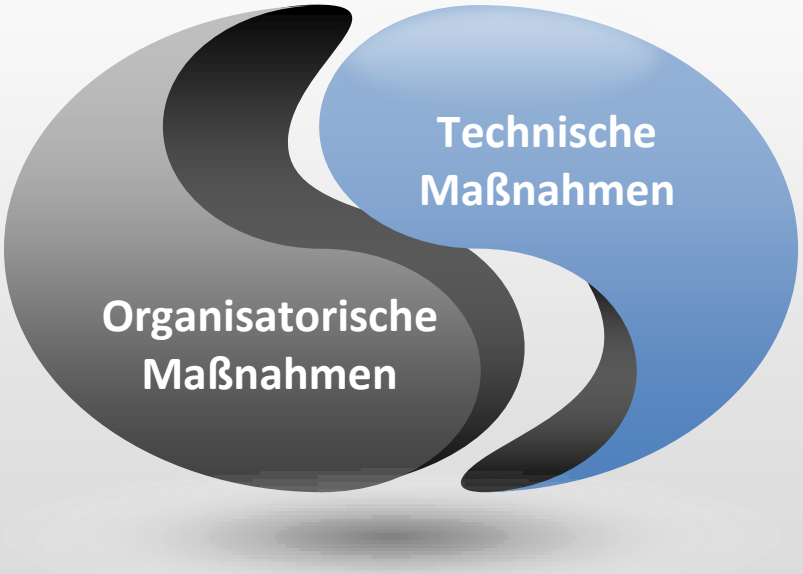
Lösungsansatz - Awareness - Bildung

- **Öffentliche und private Aufgabe !!!**
- **Unterschiedliche Organisationen**
  - Bundeskanzleramt (Sicherheitshandbuch)
  - Cyber Security Austria
  - Wirtschaftskammern
  - Expertengruppen
  - Schulen
  - Fachhochschulen
  - Universitäten
  - Unternehmen
  - Hersteller



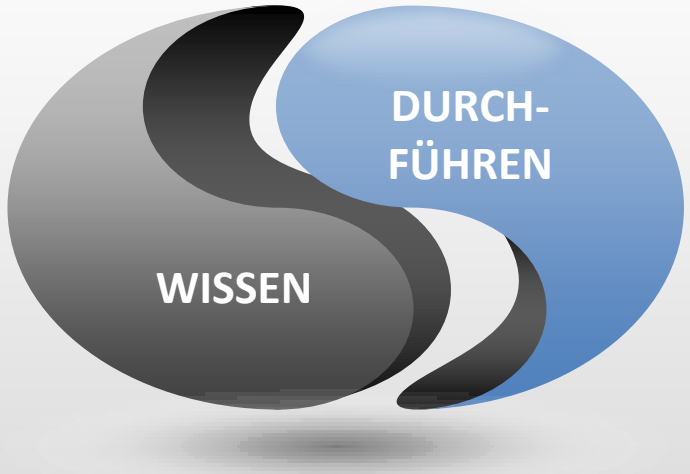
Lösungsansatz - Awareness - Bildung

- IT-Kosten haben Versicherungscharakter
- IT ist geschäftskritisch
- Schaden kann sehr hoch sein
- 80/20-Regel



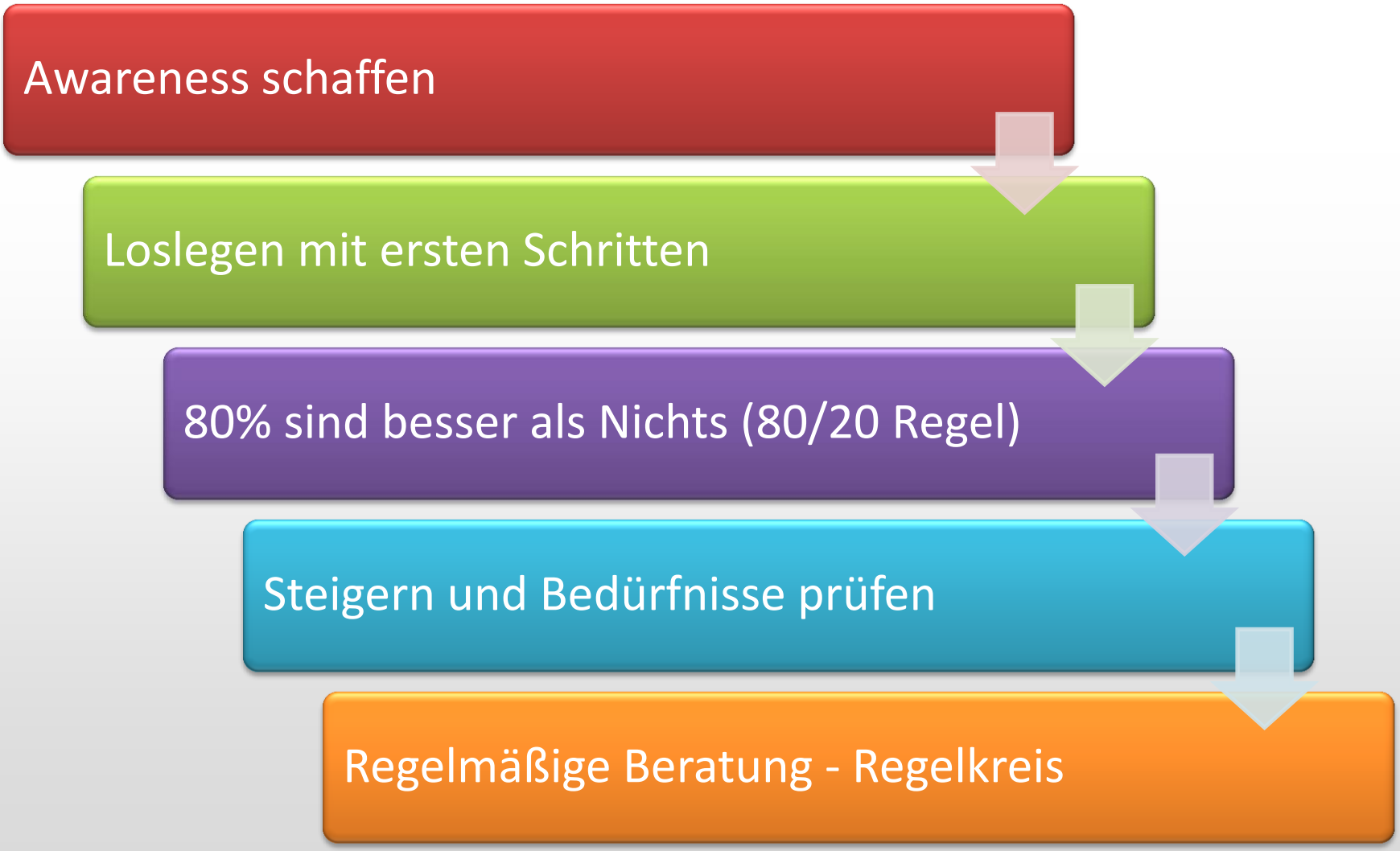
Lösungsansatz - Beratung

- **Problemstellung muss BEWUSST sein!!!**
- **Spezielle Kompetenzen notwendig**
  - Umfassendere Beratung
  - „Eigene Sprache“ notwendig
  - Langjährige Beziehung von Vorteil
  - Gesamtheitliche Sicht nötig
  - Unternehmenswerte erheben
  - Pragmatischer Ansatz von Vorteil
- Viele KMU sind auch eine Chance!



- **Nische besetzen und ausfüllen!**

Lösungsansatz – Loslegen und Tun!



0. Berater auswählen

- Zum Steuerberater geht man auch, bevor das Finanzamt anklopft ...
- **WKO ExpertsGroup IT-Security**
- **Know-How ehrlich bewerten**
  - Habe ich das Know-How im Haus
  - Wieviel Unterstützung brauche ich?
- **Rahmen festlegen**
  - **Was wollen wir gemeinsam erreichen?**

1. Awareness schaffen

- **Sicherheitsaspekte berücksichtigen**
- **Alternative Ansätze bedenken**
  - Mangelnde Ressourcen
  - Umständliche Vorhaben
  - Mangelnde Akzeptanz
  - Widerspruch zur Unternehmenskultur
  - Pragmatischer Ansatz von Vorteil
- **Ziele festlegen**
  - **Maßnahmen definieren und prüfen**

2. Loslegen mit ersten Schritten

- **Handlungsplan mit klaren Prioritäten**
- **Chaos vermeiden**
  - Klare Zuständigkeiten und Verantwortlichkeiten festlegen
  - Bestehende Richtlinien bekannt machen
  - Informationssicherheit regelmäßig überprüfen
- **Zweckmäßigkeit und Effizienz**
  - **Nicht nur Sicherheitsaspekte prüfen**
  - **Einsparungspotential**
  - **Reduzierte Komplexität erhöht die Sicherheit**

3. Mehr Sicherheit mit wenig Aufwand

- **80 % Erfolg durch 20 % Aufwand**
- **Sicherheitsniveau erhöhen**
  - Bestehende Richtlinien dokumentieren
  - Vorhandene Schutzmaßnahmen nutzen
  - Minimale Privilegien
  - Administratorrechte sinnvoll einschränken
  - Nicht benötigte Funktionalität entfernen
  - Verschlüsselung aktivieren, ...
- **Sicher machen was sicher gehört**
  - **Handbücher, Dokumentation und Empfehlungen lesen**

4. Steigern und Bedürfnisse prüfen

- **Security als Business-Enabler**
- **Anforderungen erheben**
  - Kundenbedürfnisse an Sicherheit
  - Verschlüsselte Kommunikation
  - Verfügbarkeiten und Ausfallszeiten
  - SLAs, Verträge, Gesetze und Mitbewerb als Anhaltspunkt
- **Regelmäßigkeit vorbereiten**
  - **Sicherheitsmanagement betreiben**
  - **Sicherheit ist kein Produkt, sondern ein Prozess!**

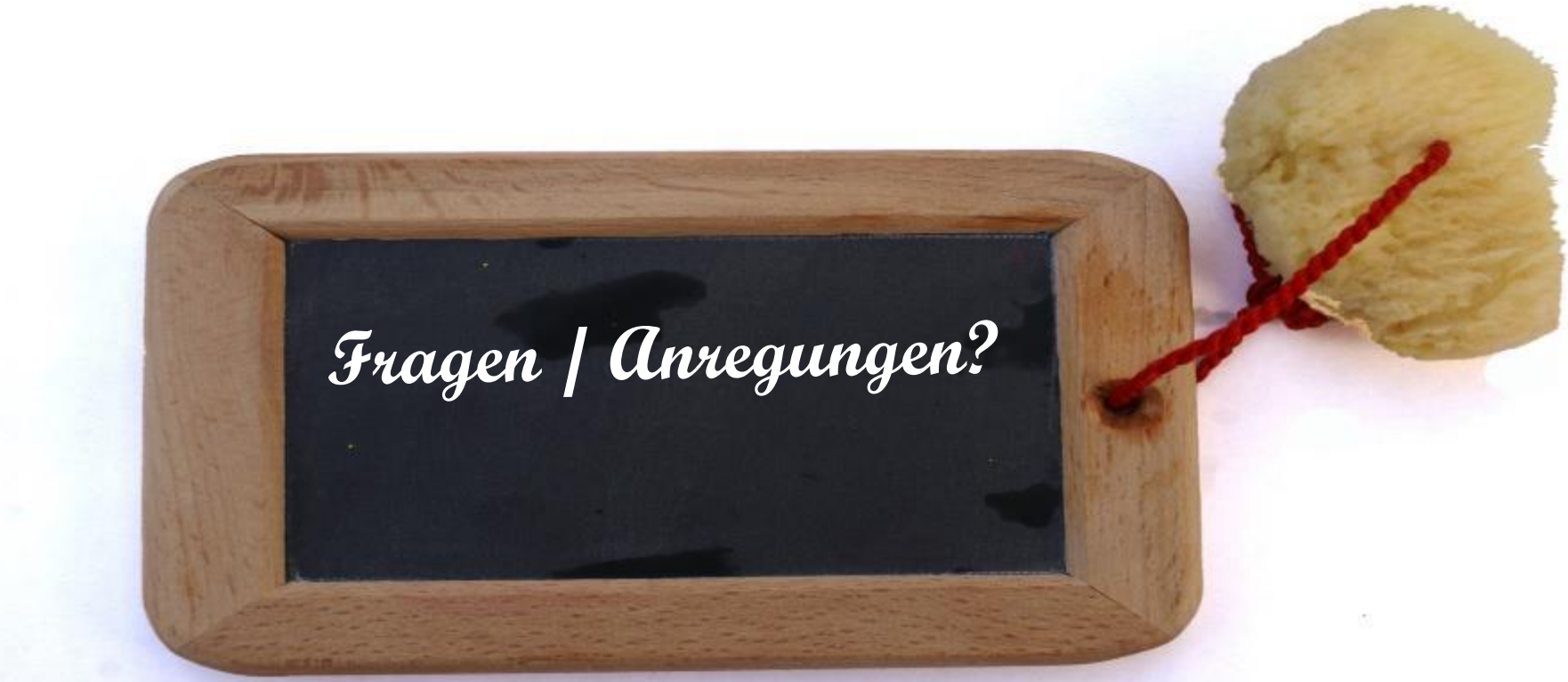
5. Regelmäßige Beratung - Regelkreis

- **Security wird gelebt**
- **PDCA – Sicherheit wird zum Prozess**
  - Plan Anforderungen, Maßnahmen und Ziele
  - Do Implementierung und Richtlinien
  - Check Regelmäßige Prüfung (Zweck, Sicherheit, Effizienz)
  - Act Reagieren und Adaptieren
- **Ehrliche Selbsteinschätzung notwendig**
  - **Expertenrat hinzuziehen**
  - **Sicherheit muss messbar gemacht werden**
  - **Sicherheitsentwicklung aufzeigen**

Zusammenfassung

- Besondere Bedürfnisse
- Awareness beim Kunden
- Awareness beim Berater
- Öffentliche und private Aufgabe
- Spezielle Lösungen nötig
- Von Herstellern bereits tlw. erkannt und umgesetzt!

→ ES IST MÖGLICH!



IT-Security für KMU – ein Widerspruch?

Grundlagen – Begriffe – Status Quo – Problemstellungen - Lösungsansätze

HolisticSec
securing is our business

alldata

Vortrag im Rahmen des E-Day 2014 – Wien, 6. März 2014

Rüdiger Linhart - linhart@alldata.at
Florian Brunner - florian.brunner@holisticsec.com