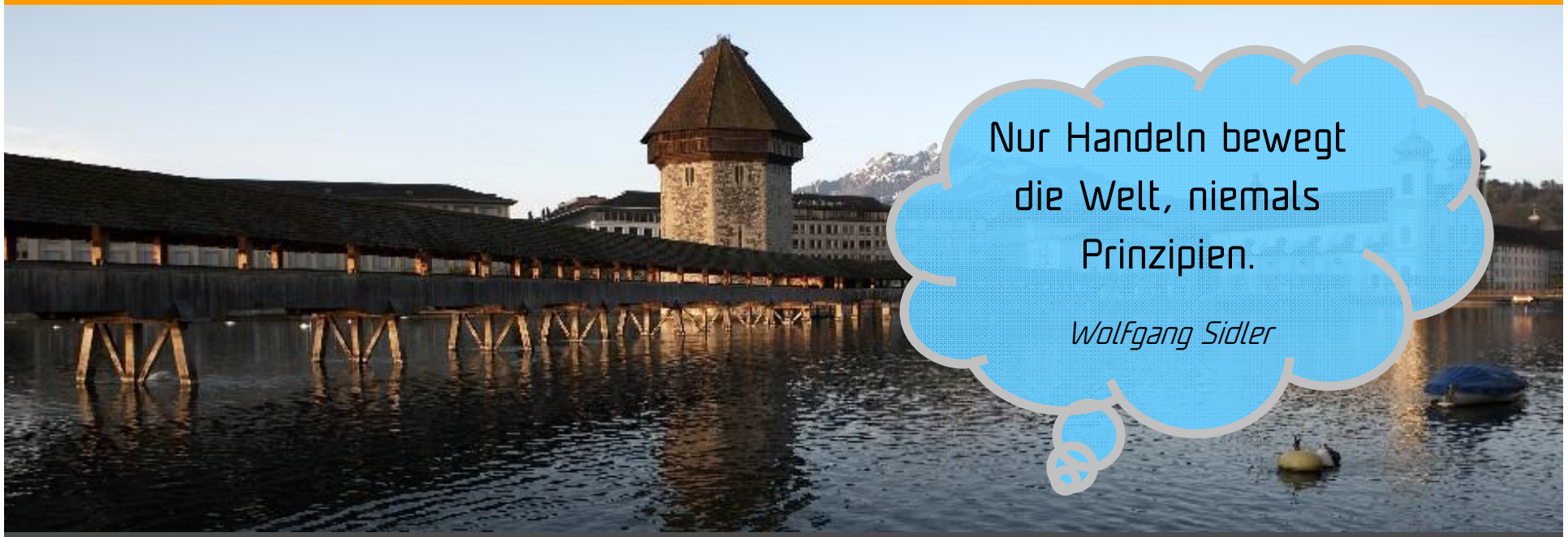
SIVG
Schweizerisches Institut für Verwaltungsräte

Awareness
Datenschutz
Analyse und Audit
Risiko-Management
Interimsmanagement

SIDLER
Information Security



SIDLER Information Security GmbH

vom Know-how zum Do-how

ICT-Governance «Wolfgang Sidler»

KKL Luzern, 6. August 2013

Wolfgang Sidler, CEO

Kontakt
www.sidler-security.ch
wolfgang.sidler@sidler-security.ch

Ausbildung

- Master in Information Security Hochschule Luzern
- eidg. Wirtschaftsinformatiker mit FA
- Certified ISO 27001 Lead Auditor
- ITIL Foundation Certificate
- Microsoft Certified Systems Engineer (MCSE)

Engagement

- Mitarbeiter des Datenschutzbeauftragten des Kantons Luzern (Teilzeitpensum)
- Freier Dozent an der Uni Luzern für Rechtswissenschaften
- Beirat Hochschule Luzern - Wirtschaft (Sicherheit)
- Prüfungsexperte für Informatik-Lehrlinge (Luzern)
- Präsident Verein InfoSurance 2009-2011

Berufserfahrung

- 25 Jahre Informatik-Erfahrung
- Mitautor „IT-Sicherheitshandbuch für die Praxis"
- 6 Jahre IT-Security Officer bei der renommierten Schweizer Privat Bank Julius Bär
- European Security Consultancy Manager bei Zurich Financial Services (ZFS)
- 3 Jahre Erfahrung im Ausland (New York, Muscat) im Bereich Informations-Sicherheit und Projektmanagement

IT-Sicherheitshandbuch für die Praxis ISBN: 3-9521208-3-9

SIDLER Information Security

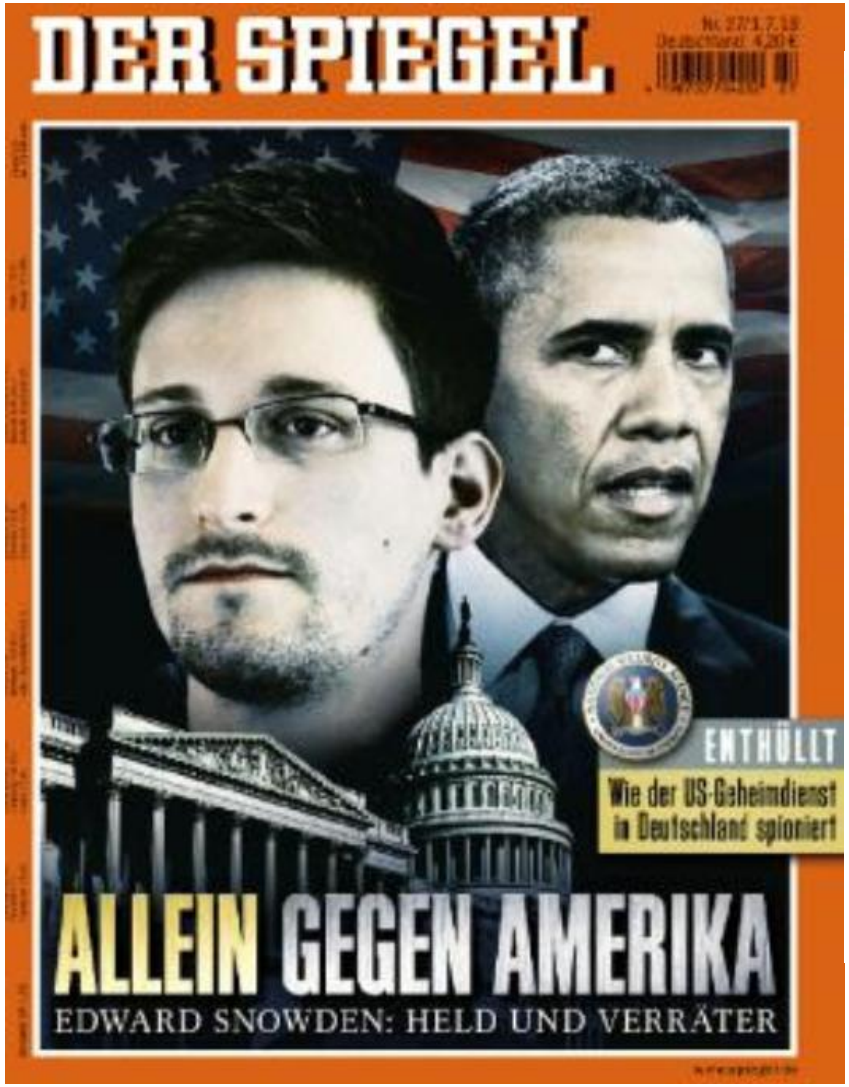
 © 2013 SIDLER Information Security GmbH

Heutige Agenda

- Aktuelle Gefahren und Risiken inkl. Kurz-Video
- Was heisst eigentlich ICT-Governance?
- Treiber für die ICT-Governance und Compliance
- Fragen, die sich Verwaltungsräte stellen sollten
- Aktuelle Herausforderungen
- Was ist IT-Risiko Management? Was ist ein Risiko?
- Tipps für die Umsetzung
- Ihre Verantwortung und Ihr Nutzen
- Unsere ICT-Governance Dienstleistungen

© 2013 SIDLER Information Security GmbH

NEWS -Orwell grüsst!



Clouds: US-Recht öffnet Türen

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)

Verschiedene US-Gesetze, wie der Patriot-Act geben den US-Justiz- und Sicherheitsbehörden «weitreichende Möglichkeiten» um die Herausgabe von Daten in Clouds verlangen zu können. Der Glaube, dass nationale Datenschutzbestimmungen höher gewichtet sind als das amerikanische Recht, sei irreführend. Zu diesem Schluss kommt eine aktuelle **[1] Studie** des **[2] Instituts für Informationsrecht der Universität Amsterdam**. Anscheinend spiele es keine Rolle, wo der Datenserver physisch steht. Es reiche schon aus, wenn ein Cloud-Anbieter seinen Hauptsitz in den USA habe, wie das bei Amazon, Apple, Google oder Microsoft der Fall sei. Auch Partner im Ausland, mit dem der Anbieter «Geschäftsbeziehungen ständiger oder systematischer Natur» pflege, seien nicht vor Zugriffen gefeit.

Wenig substanzielle Barrieren für Geheimdienste

Daten sind in der Cloud nicht vor neugierigen US -Blicken sicher

So gebe es für die US-Geheimdienste «wenig substanzielle Barrieren», um an Informationen in der Cloud zu gelangen. Dabei kommt nicht nur der Patriot-Act zum Tragen, sondern auch das US-amerikanische Anti-Terror-Gesetz. Dieses sei bereits mehrfach ausgedehnt worden und biete der National Security Agency (NSA) weitreichende Kompetenzen, ohne dass Richter ihre Bewilligung dazu geben müssen.

© 2013 SIDLER Information Security GmbH

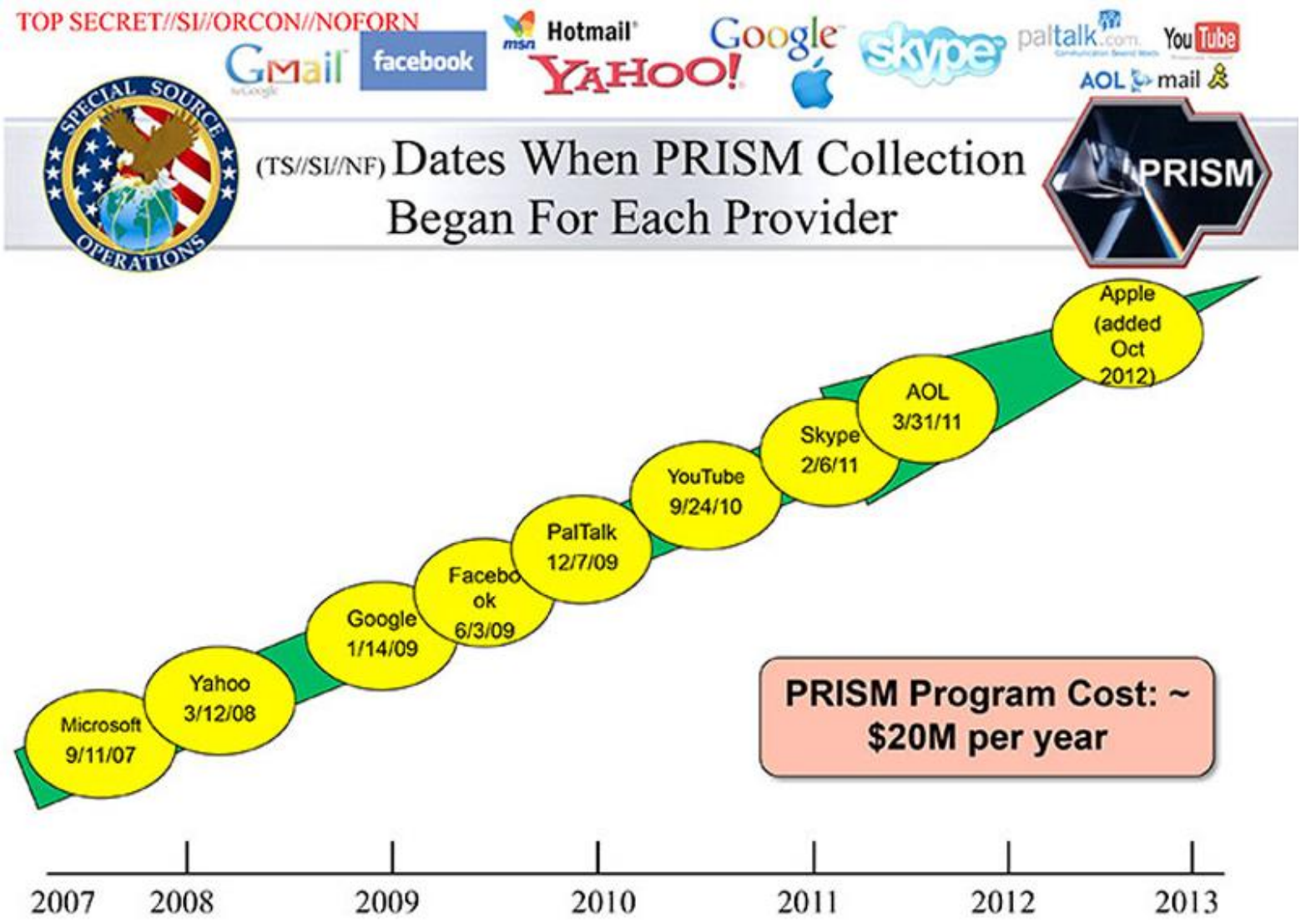
NEWS -Orwell grüsst!

Waren Sie überrascht?

Fast jedes Land hat einen Geheimdienst und setzt die neuen Technologien zur Überwachung zum eigenen Vorteil ein. Der «kalte Krieg» ist schon länger Realität! z.B. Echelon (2001), Lawful Interception, etc.

 © 2013 SIDLER Information Security GmbH

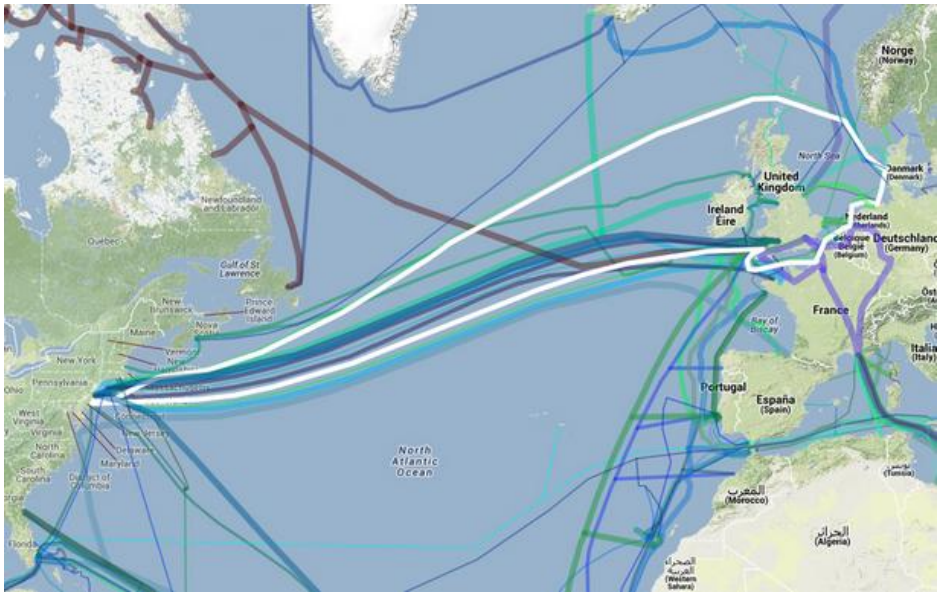
NSA – Überwachung durch die USA



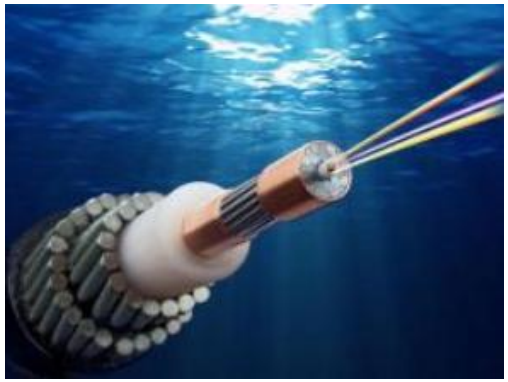
© 2013 SIDLER Information Security GmbH

Auch der Glaserfaser-Kabel im Ozean wurde angezapft!

Darüber wird ein grosser Teil der deutschen Kommunikation mit Übersee abgewickelt. Mit der Unterstützung von Vodafone und BT (British Telecom) habe sich der Geheimdienst in der Küstenstadt Bude Zugang zu den Daten beschafft. Berlin gab sich überrascht und liess den Regierungssprecher mitteilen: **"Eine Massnahme namens 'Tempora' ist der Bundesregierung ausser aus diesen Berichten erst einmal nicht bekannt."**



Glasfaserkabel zwischen Europa und Nordamerika, weiss TAT-14



 © 2013 SIDLER Information Security GmbH

Ist Internet für Sie auch Neuland?

#Neuland Internet

Aktualisiert am 19.06.2013 22 Kommentare

Eine Bemerkung von Angela Merkel aus der gemeinsamen Pressekonferenz mit US-Präsident Barack Obama sorgt auf Twitter für Lacher. Andere pflichten der deutschen Bundeskanzlerin bei.

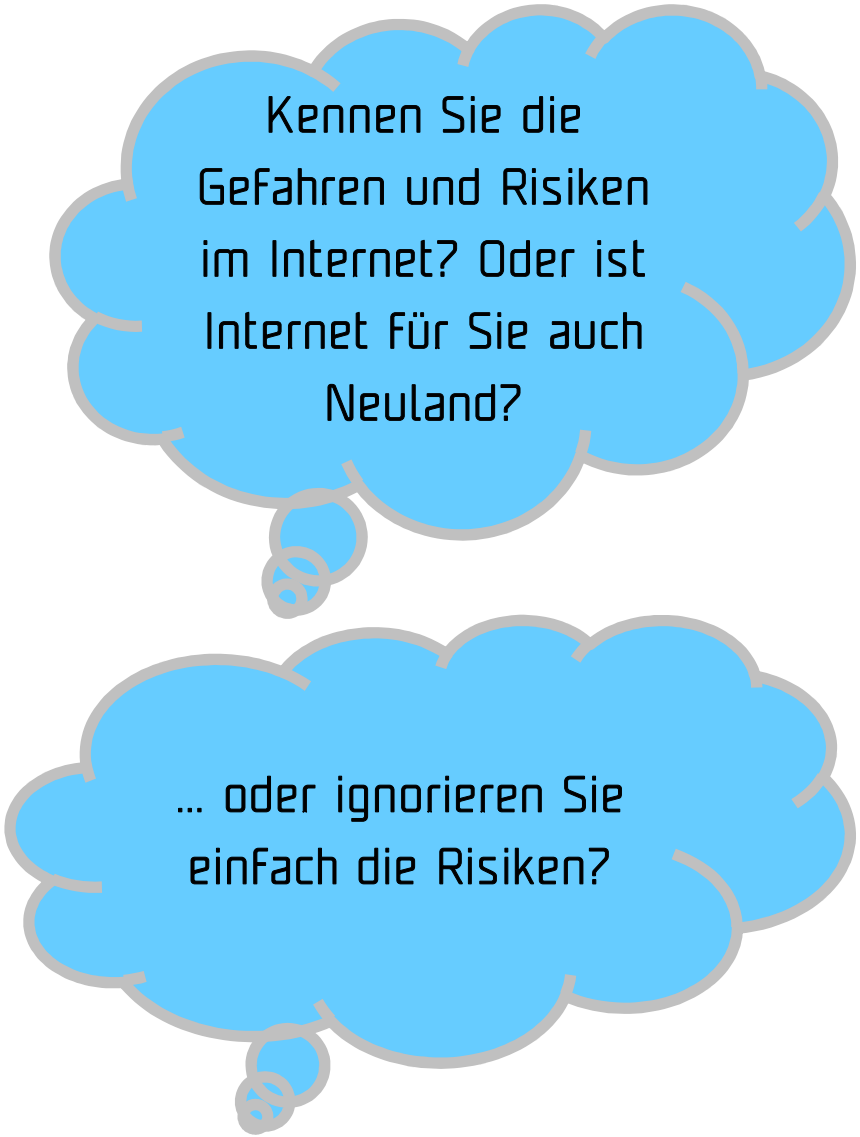
«Das Internet ist für uns alle Neuland»: Angela Merkel kurz vor der Pressekonferenz. (19. Juni 2013)

... ist die politische Führung in Bezug auf die Technik einfach überfordert!?

Quelle: ICT Kommunikation, 19.6.2013

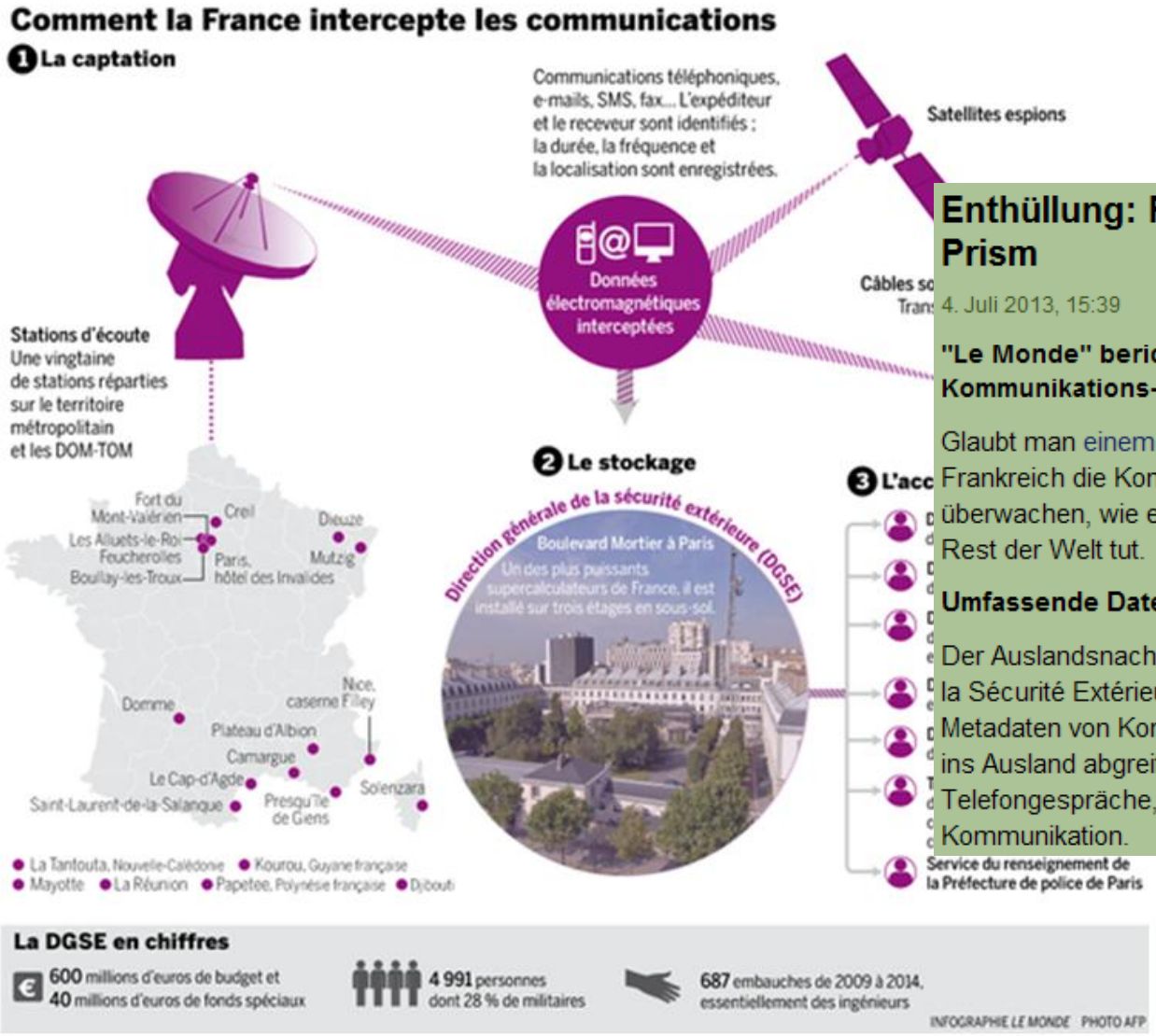
 © 2013 SIDLER Information Security GmbH

Ist Internet für Sie auch Neuland?



 © 2013 SIDLER Information Security GmbH

Auch die Franzosen überwachen! Wer nicht?



Enthüllung: Frankreich hat sein eigenes Prism

4. Juli 2013, 15:39

"Le Monde" berichtet, dass der Geheimdienst DGSE Kommunikations-Metadaten abgreift

Glaubt man einem Bericht der Zeitung "Le Monde", könnte Frankreich die Kommunikation seiner Bürger ähnlich überwachen, wie es das NSA-Programm Prism mit dem Rest der Welt tut.

Umfassende Datensammlung

Der Auslandsnachrichtendienst DGSE (Direction Générale de la Sécurité Extérieure) soll dem Bericht zufolge automatisiert Metadaten von Kommunikation im Inland und von Frankreich ins Ausland abgreifen. Betroffen sind nicht nur Telefongespräche, sondern auch internetbasierte Kommunikation.

© 2013 SIDLER Information Security GmbH

Schweizer Nachrichtendienst-Gesetz in Vernehmlassung

Nachrichtendienstgesetz
(NDG)

vom … *Entwurf vom 08.03.2013*

Die Bundesversammlung der Schweizerischen Eidgenossenschaft,
gestützt auf die Artikel 54 Absatz 1, 57 Absatz 2 und 173 Absatz 2 der Bundesverfassung[1],
nach Einsicht in die Botschaft des Bundesrates vom …[2],
beschliesst:

1. Kapitel: Allgemeine Bestimmungen und Grundsätze der Informationsbeschaffung

Art. 1 Gegenstand und Zweck

[1] Dieses Gesetz regelt:

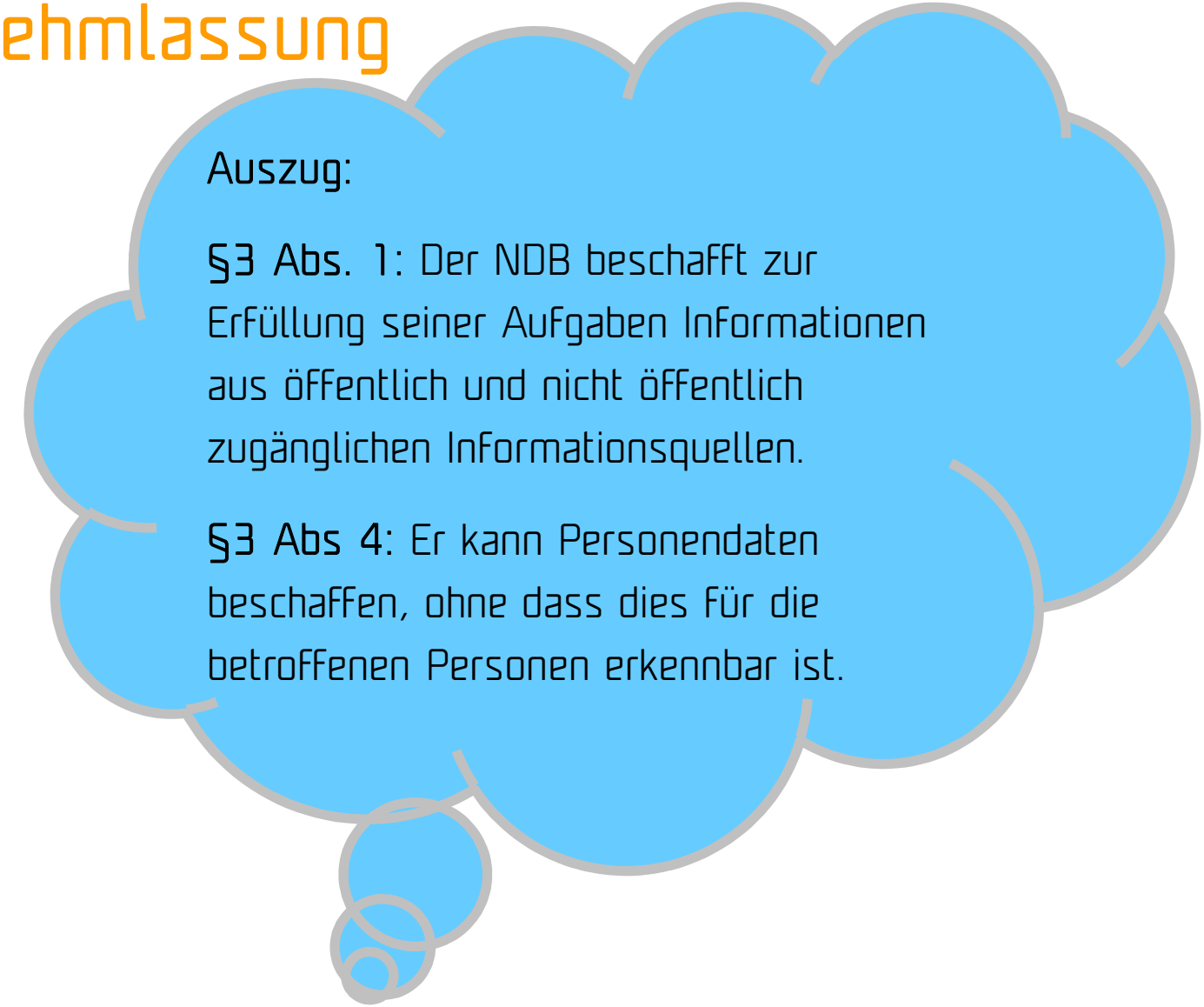
a. die Tätigkeit des Nachrichtendienstes des Bundes (NDB);

b. die Zusammenarbeit des NDB mit anderen Behörden des Bundes, mit den Kantonen, mit dem Ausland und mit Privaten;

c. die übergeordnete Steuerung, Aufsicht und Kontrolle der nachrichtendienstlichen Tätigkeit.

© 2013 SIDLER Information Security GmbH

Schweizer Nachrichtendienst-Gesetz in Vernehmlassung



 © 2013 SIDLER Information Security GmbH

Wie wird heute ein Unternehmen angegriffen?

- Ein Angriff wird heute bestens bis ins Detail vorbereitet.
- Beispiel: Angriff auf **Council of Foreign Relations** www.cfr.org:
  - Die Webseite www.cfr.org wird mit einem Trojaner (Java Script) verseucht.
  - Besucht der Mitarbeitende die versuchte Webseite und hat sein Internet Explorer die bekannte Schwachstelle (Check), wird der "Trojaner" runtergeladen und auf dem PC des Mitarbeitenden ausgeführt.
  - Der Trojaner verbindet sich dann automatisch mit dem Command-and-Control-Server (C&C) oder auch Bot/Zombie-Server genannt.
  - Jetzt kann der Angreifer fast "Alles" auf den PCs der Mitarbeitenden ausführen
  - Der Trojaner verseucht über das Unternehmens-Netzwerk weitere PCs

- FAZIT: Diese sehr gut vorbereiteten Angriffe werden von einem Standard Virenschutz, Firewall und **"Mensch"** nicht mehr erkannt!
- TIPPS: Sensibilisieren Sie Ihre Mitarbeitenden in Bezug auf die Internet Gefahren und Risiken...Schützen Sie Ihren Webauftritt und patchen Sie Ihre Systeme... etc.

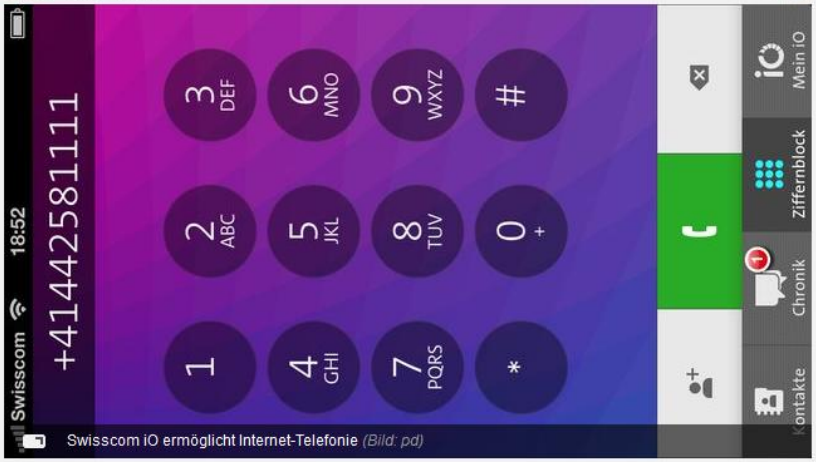
© 2013 SIDLER Information Security GmbH

Es ist nicht immer drin, was drauf steht!

Konkurrenz für Skype und WhatsApp

iO übermittelt Daten in die USA

Digital Dienstag, 17:49 3



Swisscom iO ermöglicht Internet-Telefonie *(Bild: pd)*

Der neue Messenger schickt Daten an US-Unternehmen. Swisscom sieht darin auch vor dem Hintergrund der jüngst publik gewordenen Überwachungsaktivitäten kein Problem.

hes. Kürzlich lancierte die Swisscom ihren Messenger iO, der Diensten wie Skype und WhatsApp Konkurrenz machen soll. Er zählt mittlerweile rund 270'000 Nutzer. Grossen Wert wurde bei der Präsentation darauf gelegt, die Öffentlichkeit darauf hinzuweisen, dass sämtliche Daten in der Schweiz liegen. Hintergrund sind die jüngst publik gewordenen US-Überwachungsaktivitäten rund um Prism.

Blogger François Charlet wies nun allerdings auf folgenden Passus in den Nutzungsbedingungen hin: «Swisscom arbeitet im Hinblick auf die Auswertung des Nutzungsverhaltens mit ausländischen Firmen zusammen, weshalb Daten ins Ausland übermittelt werden. Swisscom stellt sicher, dass die von ihr beauftragten Firmen dem Datenschutz und der Datensicherheit in gleichem Masse verpflichtet sind wie Swisscom selbst.»

Quelle: NZZ, 11. Juli 2013

 © 2013 SIDLER Information Security GmbH

Die Top 6 Cyber-Risiken

1. DDoS-Angriffe mit Botnetzen, um die Erreichbarkeit von Webservern und anderen IT-Services zu stören oder die Netzanbindung der betroffenen Unternehmen zu unterbrechen.
2. Drive-by-Exploits zur breitflächigen Schadsoftware-Infiltration beim Surfen mit dem Ziel, die Kontrolle der betroffenen Rechner (inkl. Notebooks und Tablets) weltweit zu übernehmen um das Unternehmen auszuspionieren.
3. Gezieltes Hacking von Webservern, um dort Schadsoftware zu platzieren oder weitergehende Spionageangriffe in angeschlossenen Netzen oder Datenbanken vorzubereiten.
4. Gezielte Schadsoftware-Infiltration per E-Mail und mittels von Social Engineering mit dem Ziel der Kontrollübernahme des betroffenen Rechners und anschliessende Spionage.
5. Ungezielte Verteilung von Schadsoftware via Spam oder Drive-by-Exploits mit Fokus Identitätsdiebstahl.
6. Mehrstufige Angriffe, bei denen zum Beispiel zunächst Ihr Zu-Lieferant oder der externe Sicherheitsanbieter (Managed Security Service) kompromittiert werden, um in weiteren Schritten dann die eigentlichen Ziele anzugreifen.

© 2013 SIDLER Information Security GmbH

Menschliches Fehlverhalten

Innert **6 Monaten** verloren gegangene mobile Geräte in **London-Taxis**:

2001

- 62'000 Handys (3 pro Taxi)
- 2'900 Notebooks
- 1'300 PDAs

2004

- 63'135 Handys
- 4'973 Notebooks
- 5'838 PDAs

2006

- 54'872 Handys
- 3'179 Notebooks
- 4'718 PDAs
- 923 Memory Sticks

ZürcherInnen verloren 2012 über 3'250 Handys und 200 Notebooks
Quelle: Städtisches Fundbüro Zürich

© 2013 SIDLER Information Security GmbH

Aussagen des Hackers «Blackhat» Adam

- Viele Nutzer wissen ja nicht einmal, dass ihre E-Mail-Adressen über ihre Facebook-Profile öffentlich einsehbar sind und sich wunderbar an Spammer verkaufen lassen. Das Abgreifen lässt sich natürlich automatisieren und damit Geld verdienen.

- Ich kann Ihnen nicht die Einzelheiten erzählen, aber nach dem 11. September 2001 haben wir **Millionen** verdient.

- Anfänger suchen einfach nach «inurl:money.php?id=» - dann werden sie schon fündig. Da das aber besonders auf grossen Sites nicht immer funktioniert, ist schon etwas mehr Recherche nötig. Ich schaue gerne Finanznachrichten im Fernsehen. Die dort vorgestellten **Start-ups** sind schnell erfolgreich, haben aber selten Admins, die wirklich Ahnung von Sicherheit haben. Also sind sie verwundbar. Häufig patchen Sie ihre SQL-Datenbank, haben aber ihr DNS nicht im Griff, was den Schutz vor Cache Poisoning angeht. Ein geräuschloser Einbruch in deren Datenbank ist in weniger als einer Stunde vollzogen.

© 2013 SIDLER Information Security GmbH

Aussagen des Hackers «Blackhat» Adam

- Whois war einst unerlässlich zum Informationensammeln. Mittlerweile holen sich alle die Daten über **Facebook, Twitter** etc. Damit lassen sich beispielsweise Amazon-Konten schnell übernehmen und mit fremden Kreditkarten shoppen gehen. Das erfordert lediglich ein Telefonat mit dem Kundenservice für das Zurücksetzen des Passworts. Auch wenn Amazon nach eigenen Angaben diese Art Identitätsdiebstahl schon vor zwei Jahren unmöglich gemacht hat, sind deren Mitarbeiter doch immer noch sehr vertrauensselig und wollen nicht viele Daten zur Verifizierung haben. Also Amazon, trainiert eure Angestellten!

- Zero-Day. Direkt dahinter Cross-Site-Scripting (XSS). Beides wohlbekannt, aber niemand kümmert sich ums Patchen. Distributed Denial of Service (DDoS) lässt sich eher nicht als Exploit bezeichnen, stellt aber unser monatliches Grundeinkommen sicher.

© 2013 SIDLER Information Security GmbH

Nur Prinzipien und Weisungen!?

«Geheimhaltungsverpflichtungen (NDAs) gehören häufig zum Standard, eine sichere Datenaustauschplattform für vertrauliche Dokumente oder verschlüsselte E-Mails dagegen nur bei jedem zehnten Unternehmen.»

«Die meisten Unternehmen gehen bei Geschäftsreisen ins Ausland viel zu sorglos mit ihren Informationen um»

Zürich Flughafen – Business Lounge

 © 2013 SIDLER Information Security GmbH

Was heisst eigentlich «ICT-Governance?

*" The system by which the current and future use of ICT is **directed** and **controlled**. It involves evaluating and directing the **plans** for the use of ICT to support the organisation and **monitoring** this use to achieve plans. It includes the **strategy** and **policies** for using ICT within an organisation."*

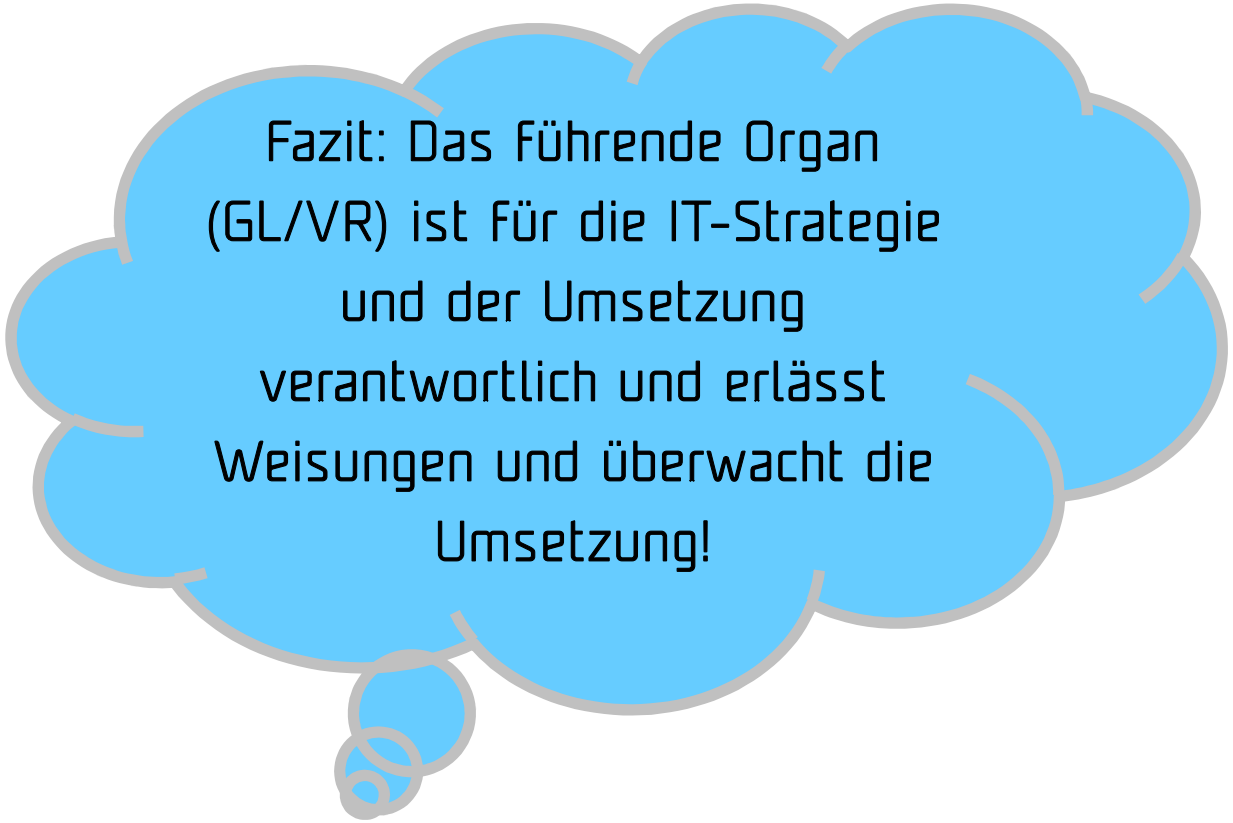
Quelle: Australian Government, Wikipedia

Stellen wir uns die folgenden 5 Fragen:

- Wie sieht's in unserem Unternehmen aktuell in Bezug auf die IT-Sicherheit aus?
- Welche Entscheidungen/Massnahmen müssen getroffen werden?
- Wer soll die Entscheidungen treffen?
- Wie sollen diese umgesetzt und überwacht werden?
- Welche Mittel stehen mir für die Umsetzung zur Verfügung?

© 2013 SIDLER Information Security GmbH

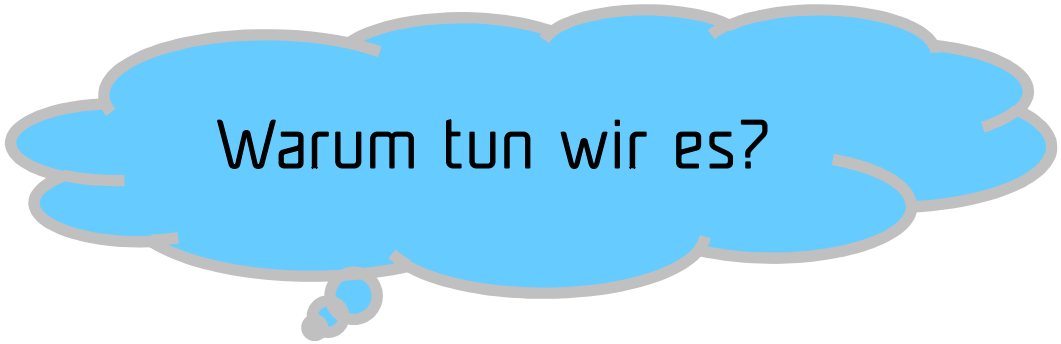
Was heisst eigentlich «ICT-Governance?



 © 2013 SIDLER Information Security GmbH

ICT-Governance- und Compliance-«Treiber»

- Risiko-Beurteilung des Verwaltungsrates (OR 663b, Ziffer 12)
- IKS inkl. Risiko-Management (OR 728a und 728b)
- Interne Unternehmens-Weisungen (Corporate-Policies)
- Einhaltung Schweizerisches Datenschutzgesetz (DSG)
- Einhaltung Urheberrecht (UR)
- Vertragliche Anforderungen
- Anforderungen seitens Kunden
- Archivierung (GebüV)
- Einhaltung der FINMA Vorgaben und BASEL II/III
- Zertifizierung im Bereich Datenschutz (DSMS)
- ISO Zertifizierungen (ISO 9001, ISO 14000, ISO 20000, ISO 27001)



© 2013 SIDLER Information Security GmbH

Schützen Sie Ihr Know-how!

Schweiz bleibt innovativstes Land der Welt

Eine Studie bescheinigt der Schweiz unter 142 Ländern mit grossem Vorsprung den Spitzenplatz in Sachen Innovation. Damit wird der Titel aus dem Vorjahr verteidigt, was auch ein Verdienst der Tech-Firmen ist.

» Von Fabian Vogt , 02.07.2013 11:47.

Das Ranking gereicht dem Namen nicht zu Ehren: Im «Global Innovation Index 2013» sind die Neuerungen ausgeblieben. Die ersten 25 Länder sind unter sich geblieben, belegen nur neue Positionen. Wie Grossbritannien, die von 5 auf 3 sprangen. Ganz nach vorne reichte es den Briten aber nicht, da liegen nach wie vor Schweden und - mit grossem Vorsprung - die Schweiz.

In fast allen Bereichen belegt die Schweiz einen Spitzenplatz, der Titel aus dem Vorjahr konnte dadurch souverän verteidigt werden. Vor allem beim Innovationsoutput, zu dem unter anderem der Anteil an High-Tech-Firmen und die Zahl der Firmengründungen zählt, führt die Schweiz deutlich. Auch mit hohen Investitionen in Forschung und Entwicklung der Unternehmen und der engen Vernetzung zwischen den Hochschulen und der Wirtschaft konnte die Schweiz punkten.

Quelle: Computerworld, 2. Juli 2013

 © 2013 SIDLER Information Security GmbH

Ihr Unternehmen ist exponiert!

- Ihr Unternehmen mit Niederlassungen z.B. in China, Middle East und Indien sind zunehmend mehr exponiert für Cyber- und andere Angriffe.
- Auch die Zunahme Ihrer Zu-Lieferanten und das mobile Arbeiten (BYOD) von überall sind weitere Risiken, welche angemessen kontrolliert werden müssen.

Über **20 Prozent** aller Unternehmen in Deutschland hatten in den letzten drei Jahren einen konkreten Spionagevorfall.

Am häufigsten sind die Finanzwirtschaft und der **Maschinenbau** betroffen.

Die **Geschäftstätigkeit im Ausland** erhöht das Risiko deutlich.

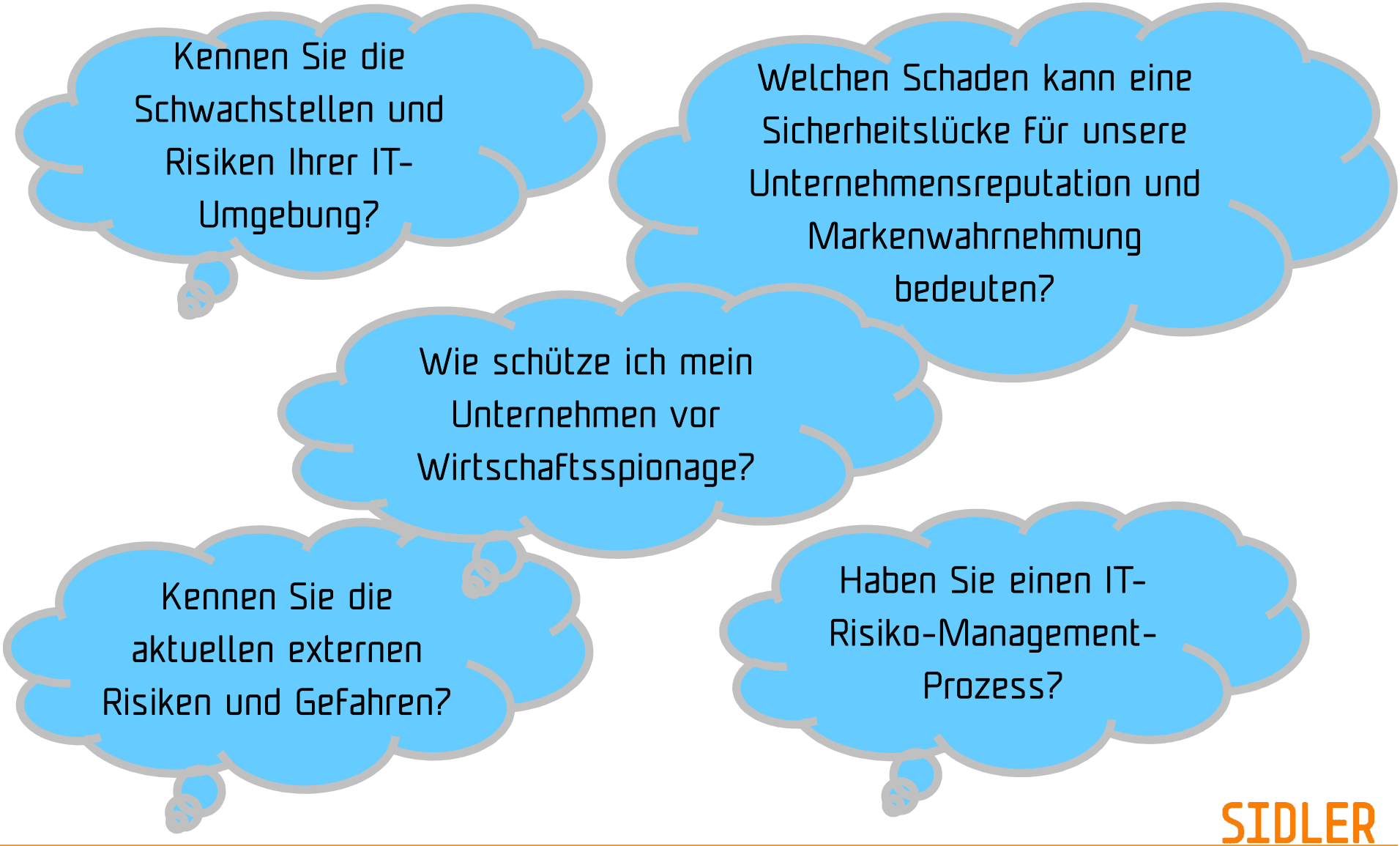
Schäden entstehen vor allem durch **eigene Mitarbeiter** sowie externe **Geschäftspartner** und Hackerangriffe.

Immer mehr Mitarbeiter setzen ihr **privates Mobilgerät** auch für Firmenzwecke ein.

6'924 Unternehmen in Deutschland wurden 2012 im Auftrag von TÜV befragt.

© 2013 SIDLER Information Security GmbH

Fragen, die Verwaltungsräte sich stellen sollten



© 2013 SIDLER Information Security GmbH

Aktuelle Herausforderungen

Cloud-Computing

Wo sind Ihre Daten?

Wer hat Zugriff auf Ihre Daten?

«Immer mehr Mitarbeitende setzen ihr privates Mobilegerät auch für Firmenzwecke ein (BYOD)!»

Wirtschaftsspionage

«Über die Hälfte aller Unternehmen besitzt keine Sicherheits-Policy mit klaren Regeln für den Informationsschutz!»

«Drei Viertel aller Unternehmen versäumen es, ihre Mitarbeitenden auf die Gefahren von Social Engineering vorzubereiten!»

© 2013 SIDLER Information Security GmbH

Was ist IT-Risk Management?

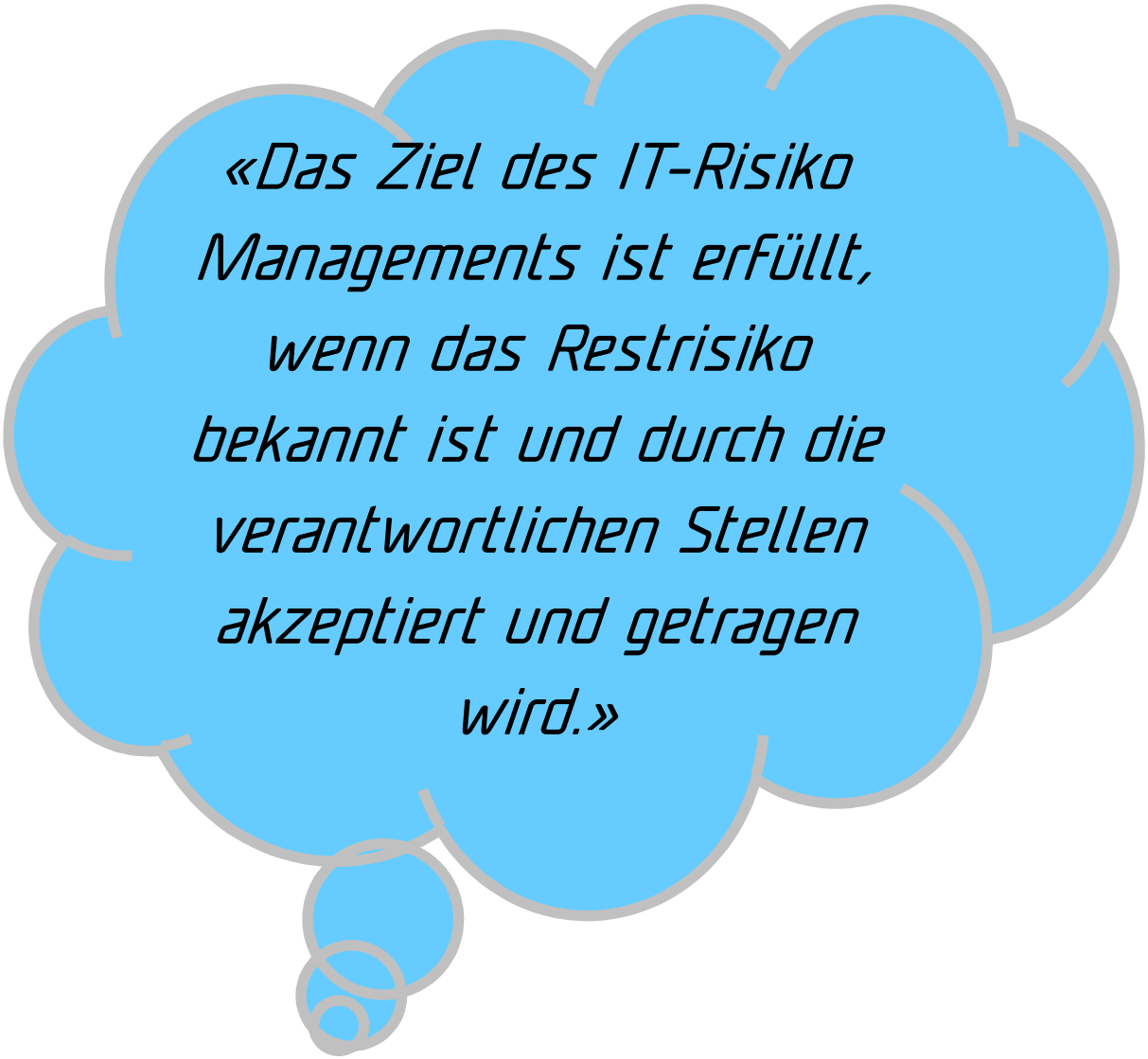
- **Gefahren** und **Schwachstellen** im Unternehmen erkennen,
- Potentielles **Schadens-Ausmass** abschätzen,
- Adäquate **Schutz-Massnahmen** (IT-Grundschutz) umsetzen,
- Periodische Überprüfung der Massnahmen und
- Ausschau halten nach **neuen** Schwachstellen (in Szenarien denken).

Umsetzung

- Die Top 20 IT-Risiken identifizieren und bewerten
- Entsprechende Massnahmen ableiten und priorisieren
- Eine Massnahmen-Pendenzenliste inkl. Risk-Owner nach ihrer jeweiligen Bedeutung und Dringlichkeit erstellen

© 2013 SIDLER Information Security GmbH

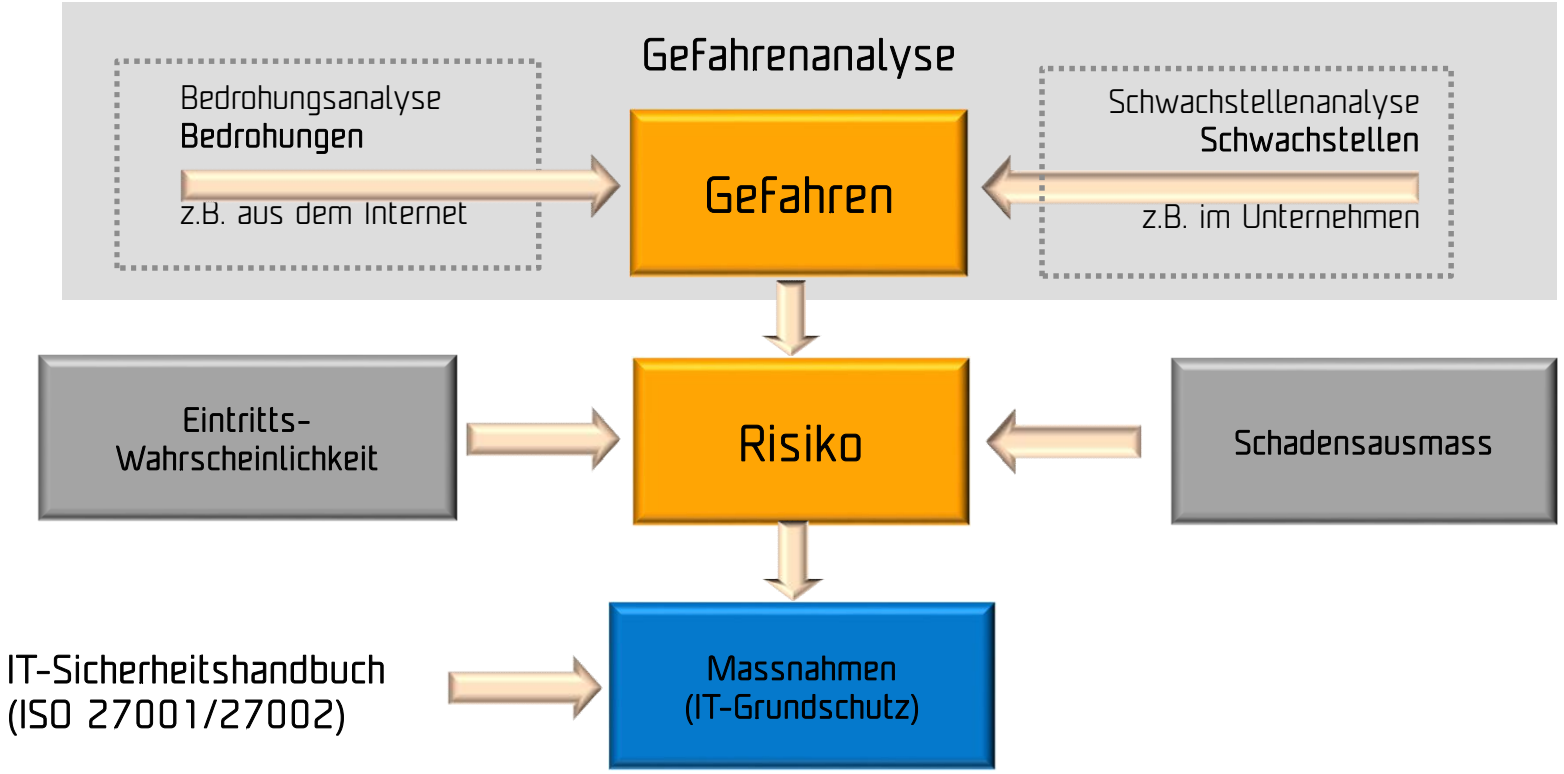
Was ist IT-Risk Management?



 © 2013 SIDLER Information Security GmbH

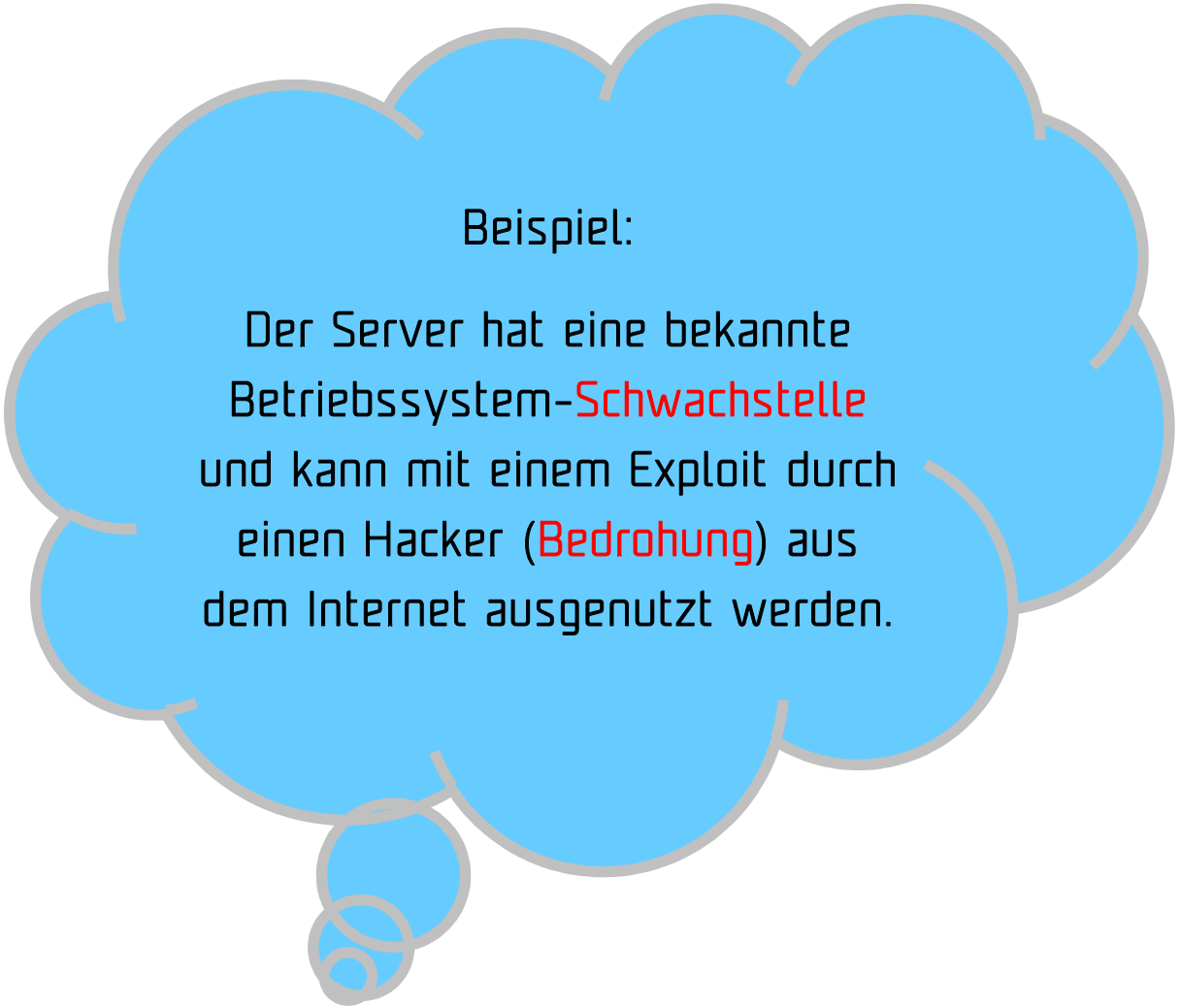
Was ist ein IT-Risiko?

- Risiko ist die Gefahr, dass ein Ereignis eintrifft, das zu einem **Schaden/Verlust** führen kann.
- Risiko ist die Gefahr, dass ein Ereignis eintrifft, das die Erreichung der Unternehmensziele **beeinträchtigen/verhindern** kann.



© 2013 SIDLER Information Security GmbH

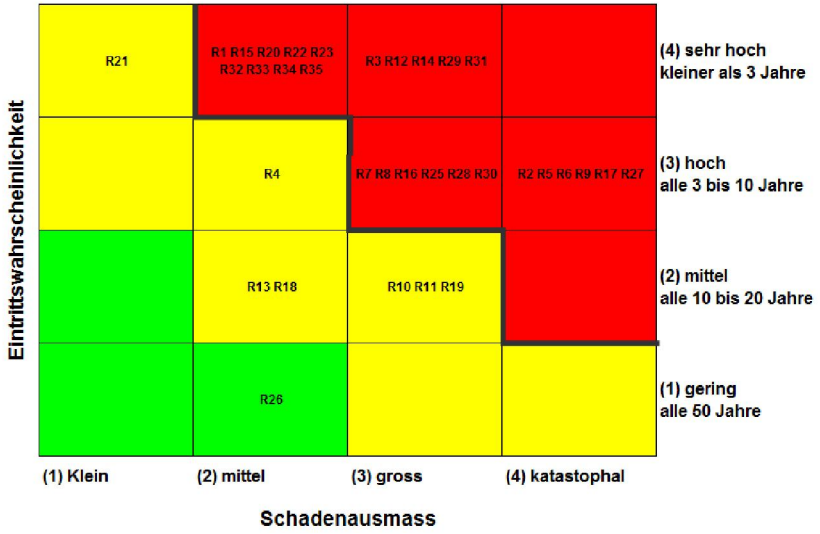
Was ist ein IT-Risiko?



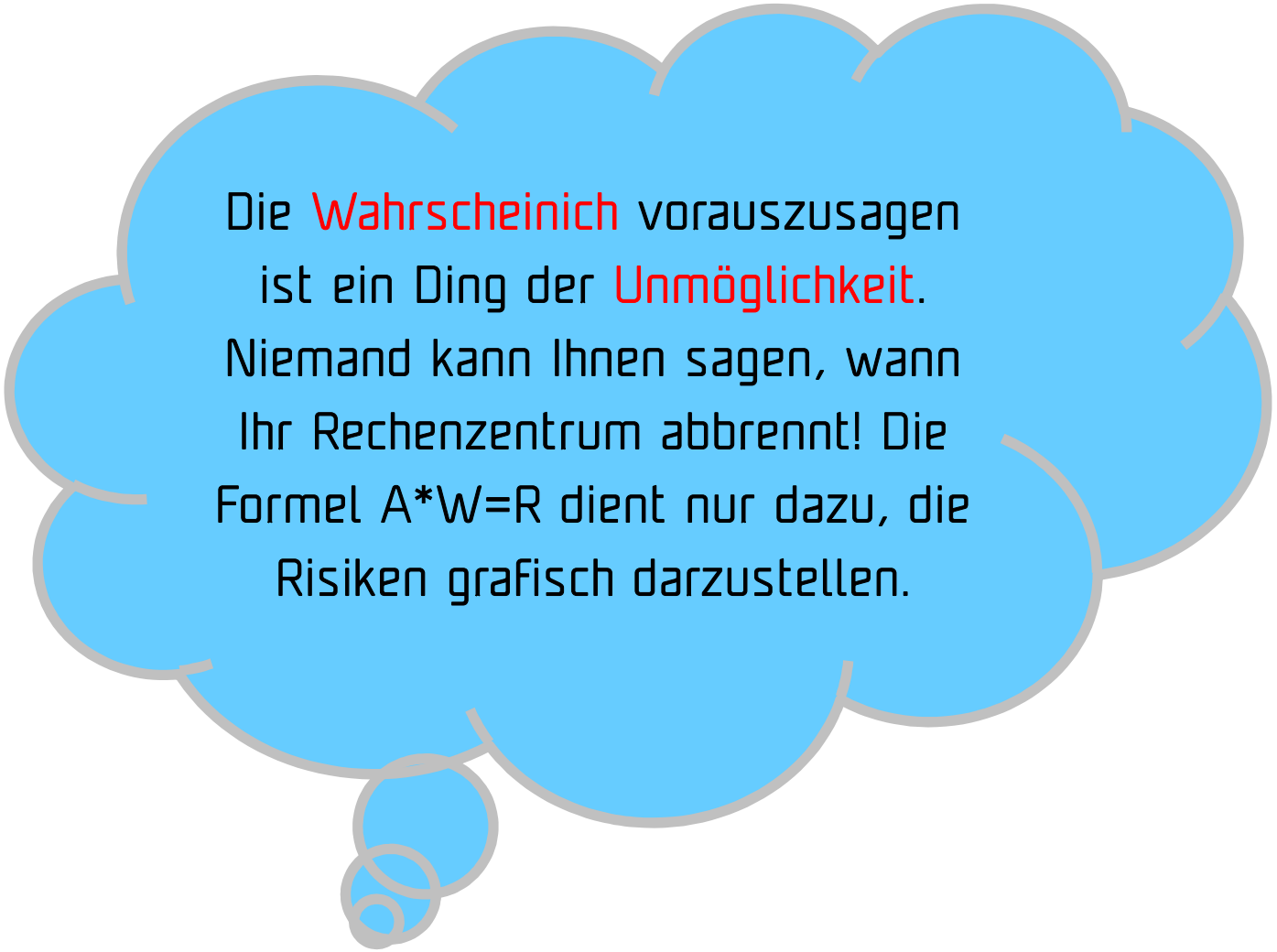
 © 2013 SIDLER Information Security GmbH

IT-Risiko Analyse

		Risiko/Asset	Wahrschein-lichkeit 1 - 4	Risiko: Schadens-Ausmass 1 - 4	Risiko: Risiko Kategorie A*W=R	Risiko Owner	spezifische Bedrohung	Schadensszenario	Bemerkungen
R1		Verlust oder Diebstahl eines USB-Sticks	4	2	8		Veröffentlichung von Kundendaten durch fahrlässigen Umgang mit Daten auf USB-Stick oder USB-Festplatten. - Unverschlüsselt grosses Risiko - Verschlüsselt kleines Risiko	Kundendaten gelangen an Öffentlichkeit	
R2		unverschlüsselte eMails	4	3	12		Veröffentlichung von Kundendaten durch fahrlässigen Umgang mit eMail	Kundendaten werden per eMail verschickt und gelangen an die Öffentlichkeit	
R3		Verlust oder Diebstahl eines Smartphones	3	2	6		Veröffentlichung von Kundendaten durch fahrlässigen Umgang mit Daten auf dem Smartphone	Kundendaten gelangen an Öffentlichkeit	
R4		mangelende RZ-Versorgung (Klima)	3	4	12		Durch nicht korrekte Klimatisierung des RZ können die Server einen Schaden erleiden und daher ausfallen	Plötzlicher Ausfall der Server bzw. der Applikationen und somit Störung der Geschäftsprozesse	
R5		mangelende RZ-Versorgung (Strom)	3	3	9		Wenn die Notsromversorgung bei einem Stromausfall nicht funktioniert, können die Server einen Schaden erleiden und daher ausfallen	Plötzlicher Ausfall der Server bzw. der Applikationen und somit Störung der Geschäftsprozesse	



IT-Risiko Analyse



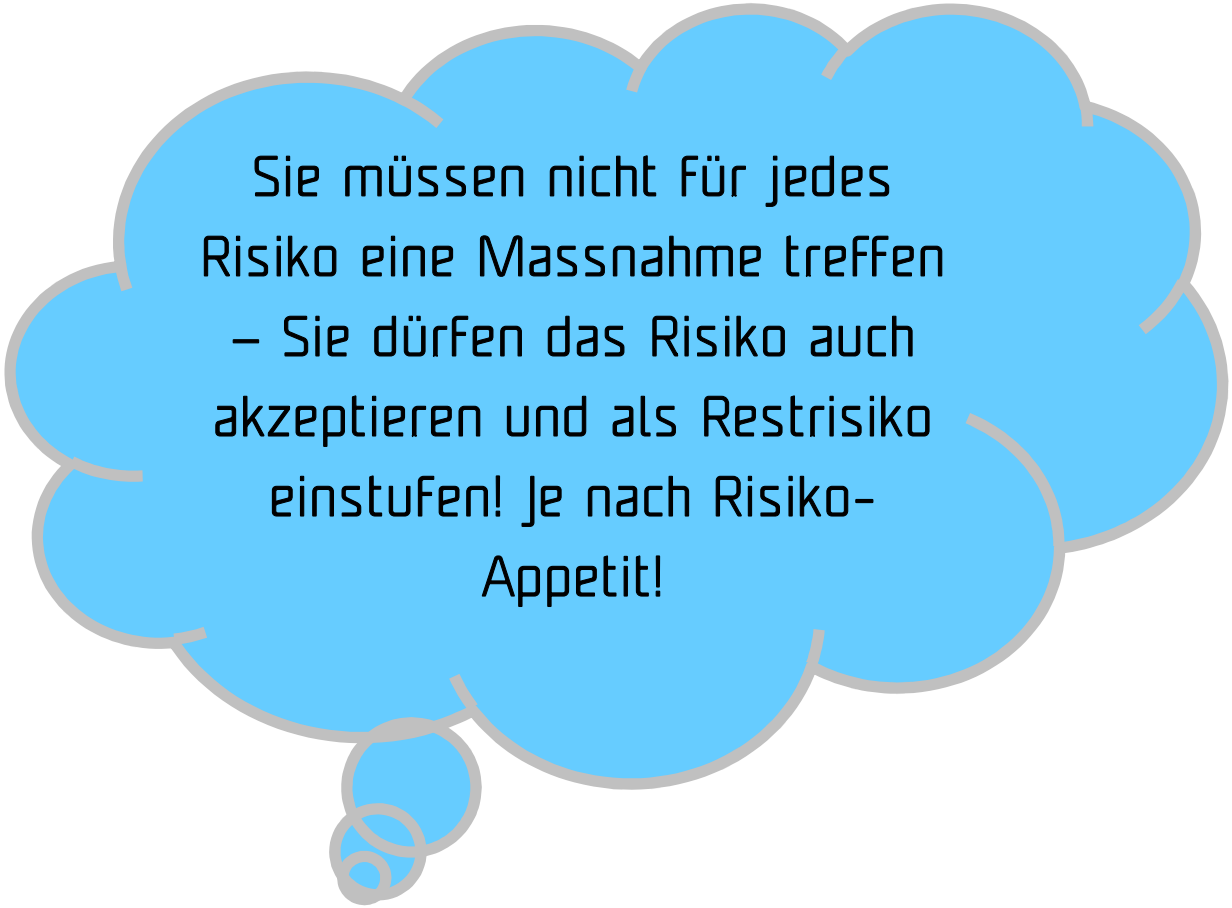
 © 2013 SIDLER Information Security GmbH

Sicherheitsmassnahmen basierend auf der IT-Risiko-Analyse

Laufende Nummer	Risiko Nummer zuordnen	Sicherheitsbedürfnis / Anforderung	No	Massnahme	Umgesetzt Ja/Nein	Verantwortung Umsetzung	verantwortliche Person	Restrisiko	Bemerkungen	Termin	überprüft (SIBE)	abgenommen (SIBE)
1	R1	Daten auf USB-Sticks müssen verschlüsselt sein.	M1	Weisung (XY): Die Mitarbeiter dürfen nur noch den von der IT empfohlene und verschlüsselte USB-Stick einsetzen.	JA	Abteilung	Name Vorname	Nicht allle Mitarbeitenden halten sich an die Weisung	Weisung mit mehr Kraft Top-Down durchsetzen (Linienführung)	31.08.2012		
2	R2	E-Mail mit sensitiven bzw. vertraulichen Inhalt dürfen nur verschlüsselt versendet werden.	M4	IT Nutzungsrichtlinie: Umgang mit E-Mail	JA	Abteilung	Name Vorname	Nicht allle Mitarbeitenden halten sich an die Weisung	Weisung mit mehr Kraft Top-Down durchsetzen (Linienführung)	12.09.2012		
			M5	Projekt: Evaluation und Einführung einer E-Mail Verschlüsselungs-Lösung	tbd	Abteilung	Name Vorname					
			M6	Projekt: Evaluation und Einführung eines E-Mail Content-Scanners, welcher auf bestimmte Key-Wörter die E-Mail scannt. (Technische Lösung)	tbd	Abteilung	Name Vorname	Das Restrisiko wird kleiner, da diese Lösung eine Kombination einer organisatorischen und technischen Lösung ist.	Compliance-Officer hat Einsicht in das E-Mail Archiv.(Bei End 2 End Encryption müsste die Verschlüsselung wieder aufgehoben werden > Gefahr)			
	R3	Daten auf geschäftlichen Smartphones müssen verschlüsselt sein und die Smartphones müssen über ein zentrales Management Tool verwaltet und kontrolliert werden können (z.B. remote Wipe)	M7	Weisung (xy): Umgang mit Smartphones	JA	Abteilung	Name Vorname	geschäftliche Daten werden auf privaten Smartphones unverschlüsselt gespeichert	Weisung mit mehr Kraft Top-Down durchsetzen (Linienführung)			
			M8	Projekt: Evaluation und Einführung einer zentralen Smartphone Verwaltungs-Lösung	tbd	Abteilung	Name Vorname					

© 2013 SIDLER Information Security GmbH

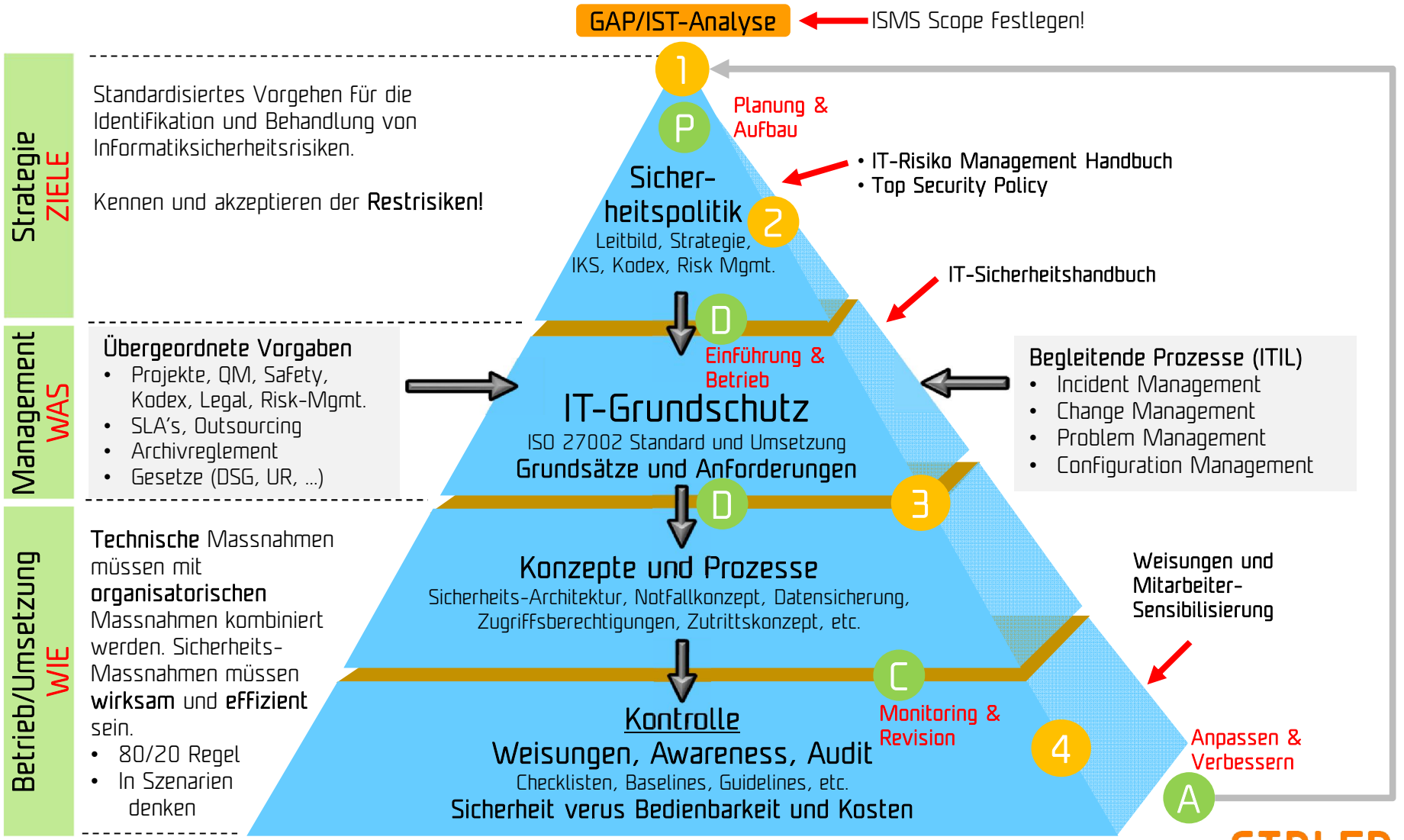
Sicherheitsmassnahmen basierend auf der IT-Risiko-Analyse



 © 2013 SIDLER Information Security GmbH

Umsetzung in der Praxis

P D C A
Plan Do Check Act



© 2013 SIDLER Information Security GmbH - Informationssicherheits-Management-System (ISMS)

SIDLER Information Security
www.sidler-security.ch

Unsere ISMS & GRC Framework-Lösung

Vorgaben

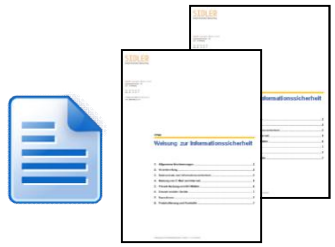
- Management Committment
- Unternehmens-Strategie
- Standards (ITIL, etc.)
- Sicherheitspolitik
- Health & Safety
- Firmen-Kodex
- Weisungen
- Gesetze (IKS)
- QM/TQM

Audit

Ausgangslage
- GAP/IST-Analyse
- Stakeholder-Analyse z.B. auf Ebene GL/VR

1 P

IT-Risiko Management



IT-Risiko Management Handbuch & Top Security Policy

2 D

Umsetzung Sicherheits-Massnahmen

IT-Sicherheitshandbuch (ISO 27002)
- Konzepte (BCM, IAM, NSP, etc.)
- IT-Forensik
- Physische Sicherheit
- Penetration-Test & Vulnerability-Scan

Projekt-Governance

- Security Risiken
- Projekt-Risiken
- Datenschutz
- IT-Architektur
- Quality-Mgmt.

Betrieb OCC

C

Operations Control Center
- Monitoring
- Incident Management

20/80 Regel Szenarien

Hilfsmittel:
- ISO 27002/27005
- BSI Grundschutz

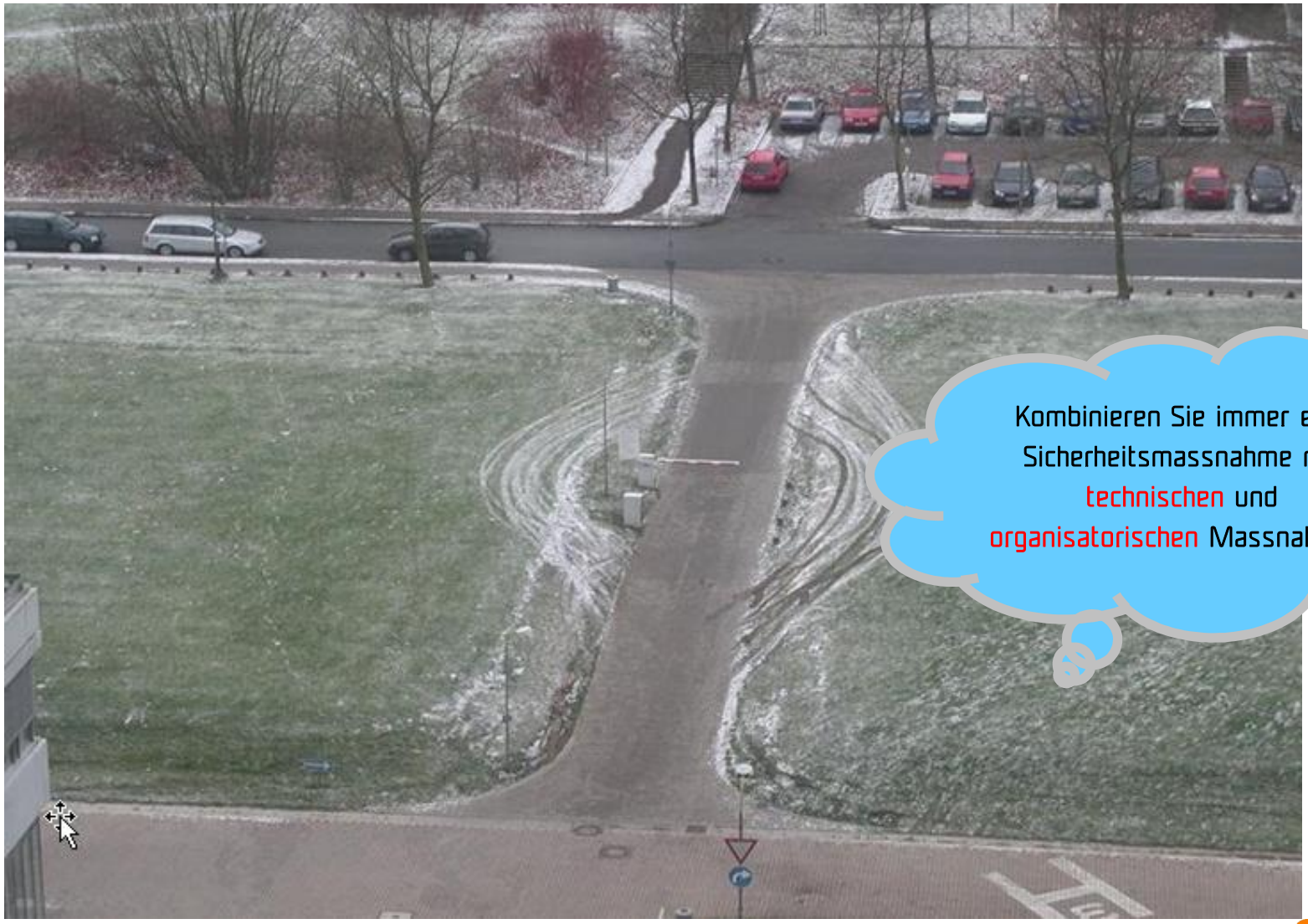
Awareness & Schulung

4 A

C 3

© 2013 SIDLER Information Security GmbH

Sind Ihre Sicherheitsmassnahmen effektiv?



 © 2013 SIDLER Information Security GmbH

Tipps für die Umsetzung der Sicherheitsmassnahmen

Sensibilisieren Sie Ihre Mitarbeitenden und setzen Sie die neuen Sicherheits-Technologien gezielt ein!

Antivirus-Programme, Firewalls etc. schützen Sie heute wenig vor den gezielten Angriffen!

Organisatorische Massnahmen können effektiver und effizienter sein als rein technische Massnahmen!

«Kein Vertrauen – keine Cloud-Lösung»

 © 2013 SIDLER Information Security GmbH

Handeln Sie jetzt!

10% Ihres IT-Budget sollten Sie für die IT-Governance (IT-Security) einsetzen.

Besser 5 umgesetzte Sicherheitsmassnahmen als 20 geplante!

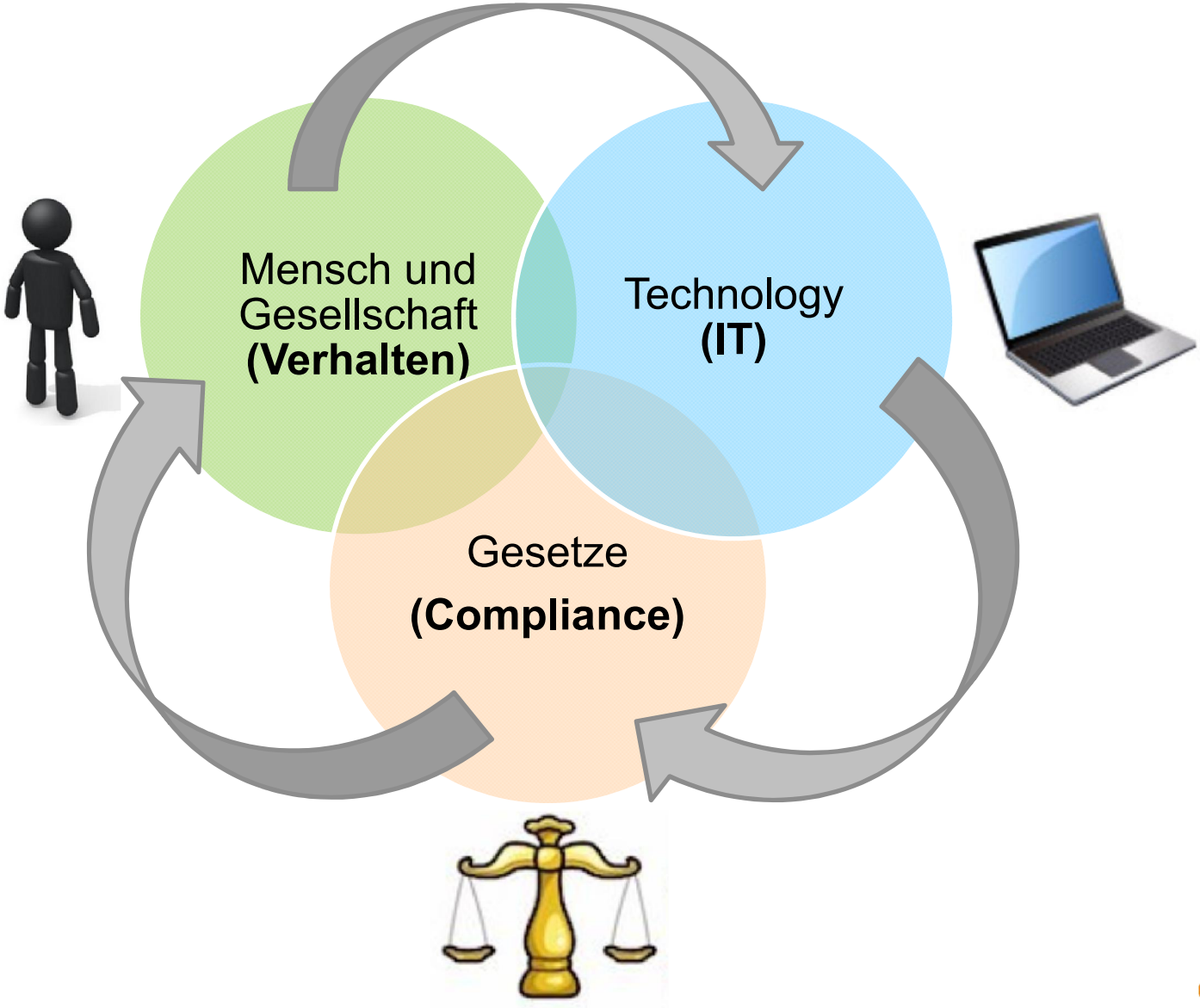
Vertrauen durch Sicherheit und ICT-Governance
"Security und Quality made in Switzerland"

Reduzieren Sie die Komplexität Ihrer IT-Infrastruktur.

Eine Sicherheitsmassnahme darf nicht mehr kosten als das Risiko.

© 2013 SIDLER Information Security GmbH

Zusammenspiel - Handlungsfelder

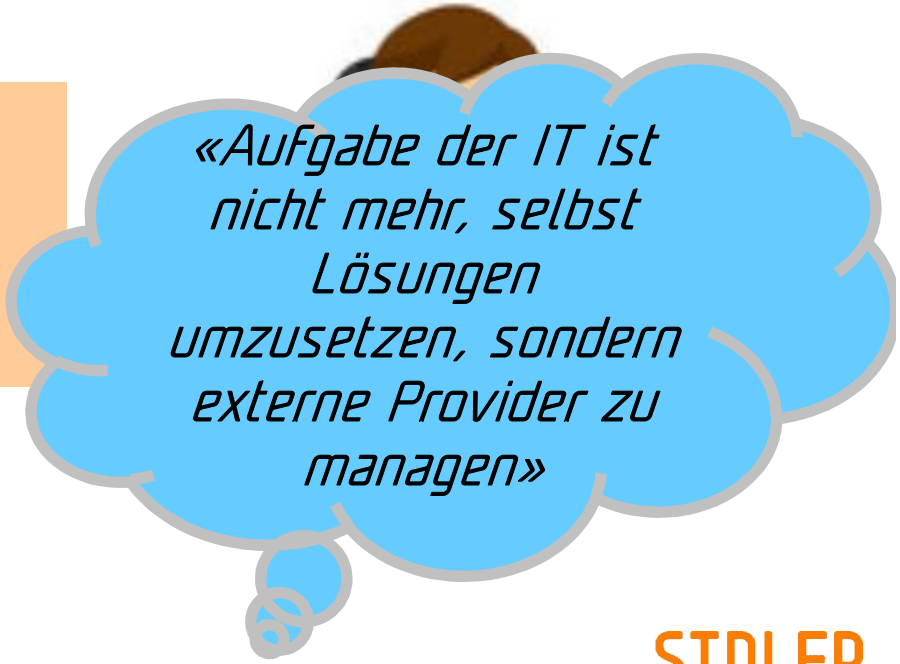


 © 2013 SIDLER Information Security GmbH

Ihre Management-Verantwortung

- Geschäftsfortgang aufrechterhalten
- Sorgfaltspflicht des Managements einhalten
- Verantwortung kann nicht delegiert werden
- Kennen und akzeptieren Sie die Rest-Risiken!

ICT-Governance und Informationssicherheit ist Chefsache!



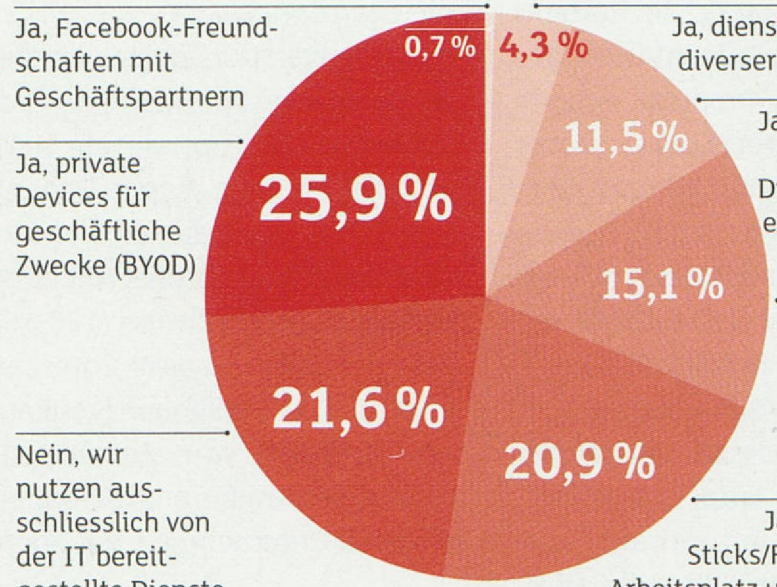
 © 2013 SIDLER Information Security GmbH

Schatten-IT?

«Oder möchten Sie all Ihre Geschäftsinformationen in der Dropbox gespeichert haben, ohne zu wissen, wer Zugriff hat?

UMFRAGE DER WOCHE:

Existiert in Ihrem Unternehmen eine Schatten-IT?



Ganz klar: Die Schatten-IT existiert. Lediglich rund 22 Prozent der von uns befragten Unternehmen setzen ausschliesslich offizielle, von ihrer IT bereitgestellte Geräte und Dienste ein. Die grosse Mehrheit nimmt sich auch mal selbst, was sie braucht: private Geräte (26 %), Speichermedien (21 %), Maildienste aus dem Web (15 %) und mehr.

Quelle: Computerworld 25. Jan. 2013

© 2013 SIDLER Information Security GmbH

Unsere Compliance (GRC)-Dienstleistungen

- Informationssicherheit für Entscheidungsträger
- Informationssicherheits-Audit
- IT-Security Officer auf Zeit
- IT-Risiko Management
- Sensibilisierungs-Aktionen
- ...

© 2013 SIDLER Information Security GmbH

Ihr Nutzen – unser Know-how

- Geringere Verwundbarkeit
- Keine falsche Sicherheit
- Bewussterer Umgang mit Information
- Gefahren kennen, Restrisiko ist bekannt
- Sorgfaltspflicht erfüllt
- Bessere Kreditwürdigkeit (Basel III)
- Positive Audits (interne und externe Revision)
- Erhöhtes Kundenvertrauen (ISO 27001 Zertifizierung)
- Einhalten aller Gesetze (IKS, Datenschutz, GebüV, FINMA, Basel III etc.)
- Wettbewerbsvorteil -> Sicherheit = Vertrauen
- Reduziert das Risiko einer Geschäftsunterbrechung erheblich (hohe Verfügbarkeit)
- Fördert das „Sicherheitsbewusstsein" der Mitarbeiter (Sicherheitskultur)
- Steigert die Möglichkeit neue Geschäfts-Felder sicherer und schneller anzugehen

© 2013 SIDLER Information Security GmbH

IT-Trends – Herausforderungen

- Der Mensch – Umgang mit der Technologie - Awareness (Sensibilisierung)
- Cloud-Computing und Virtualisierung (Vertragsrecht, etc.)
- Compliance (GebüV, IKS, Datenschutz, etc.)
- Bring Your Own Device (BYOD) oder Bring Your Own Everything!

  Konsumerisierung der IT (Private Geräte im Unternehmen) Laut der IDC-Studie werden etwa die Hälfte der weltweiten Consumer-Geräte sowohl für Geschäfts- als auch private Zwecke genutzt.
  Unternehmensinformationen werden dabei ungehindert mit den persönlichen Daten der Nutzer gemischt.
- Big-Data (Datenvolumen wächst laufend!)
- 3D-Drucker und Nano-Technik
- Zugriffsberechtigungen (IAM = Identity Access Management)
- Secure File-Transfer mit Kunden und E-Mail Verschlüsselung
- Umgang mit Social Media (Facebook & Co.)
- Management (MDM) von mobilen Endgeräten (Notebook, Tablet`s, USB-Memory Sticks, Smartphones)

© 2013 SIDLER Information Security GmbH

Danke für Ihre Aufmerksamkeit

© 2013 SIDLER Information Security GmbH