Neues Informationssicherheitsgesetz – future best practice?

Liliane Mollet

Geschäftsführerin insecor gmbh, Master of Law,
CAS Information Security

8. Tagung zum Datenschutz –
Jüngste Entwicklungen, 27.01.2015

Agenda

1. Einleitung
2. Ausgangslage für neues Informationssicherheitsgesetz (ISG)
3. Ausgewählte Inhalte des ISG und Praxisbeispiele
4. Kritische Würdigung

1. Einleitung

Neues Informationssicherheitsgesetz – future best practice?

© istockphoto

1. Einleitung

Phänomene der heutigen Zeit…

- **Informationsgesellschaft** – Zunehmende Verbreitung/Nutzung und Abhängigkeit von IKT
- **Steigende Komplexität der IKT**
- **Neue Technologien und Trends** – z.B. „SMAC“ (Social, Mobile, Analytics, Cloud)
- Cyberwelt kennt **keine (Staats-)Grenzen**!
- **Alles gratis!** Zu welchem Preis?
- **Digital Natives vs. Digital Immigrants**
- **Steigende Cyberkriminalität**

1. Einleitung

Phänomene der he

1. Einleitung

Phänomene der

Zürich 2°

Neue Zürcher Zeitung

Dienstag 20. Januar 2015 – E-Paper Webpaper

International | Wirtschaft | Finanzen | Schweiz | Zürich | Meinung | Sport | Feuilleton | Wissenschaft | Panor

AMERIKA

Hacker-Angriff via Twitter

Peinlichkeit für das US-Militär

Marie-Astrid Langer 13.1.2015, 11:03 Uhr

So sah die Twitter-Seite des Central Command vorübergehend aus. *(Bild: Reuters)*

Der Terrormiliz Islamischer Staat ist es gelungen, Twitter-und Youtube-Konten des amerikanischen Militärs zu hacken. Für das Verteidigungsministerium ist der Vorfall peinlich.

Für die Terrormiliz Islamischer Staat (IS) ist es ein weiterer Propaganda-Coup, für das amerikanische Militär ein peinlicher Zwischenfall. Am Montag haben sich Aktivisten eines selbsternannten «Cyber-Kalifats» für etwa 30 Minuten in die Twitter- und Youtube-Konten des Zentralkommandos des amerikanischen Militärs (Centcom) gehackt und Propaganda-Bilder darüber vertrieben. So zeigte

GELESEN

Reflexe einer

Der «Franken

Über Geld red

Wirtschaft

Federer probl

Schweizer Bö

Managing Dir
Development
Zühlke Engine

Business Ana
PERSONAL S

Leiter Produk
Network Sele

Head Quality
Engineering M
AG

Buchhalter m
Reporting
Econag Execu

Banking Cons
Infosys Lodes

1. Einleitung

Phänomene der

News Newsticker 7-Tage-News Archiv Foren

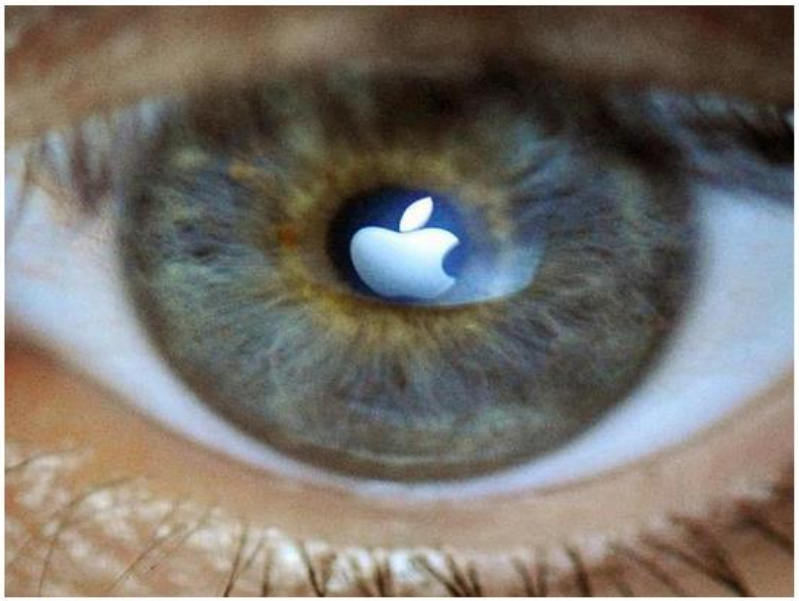
Topthemen: CES Rosetta Windows 10 NSA iPhone 6 Andr

heise online > News > 2015 > KW 4 > NSA-Skandal: iPhone-UDID als Tracking-Tool für das

19.01.2015 15:41 Mac&i « Vorige | Nächste »

NSA-Skandal: iPhone-UDID als Tracking-Tool für das GCHQ

vorlesen / MP3-Download



(Bild: dpa, Daniel Reinhardt/Archiv)

Der britische Nachrichtendienst nutzte nach einem Snowden-Dokument die einzigartige ID von iPhone und iPad zur Analyse von Zielpersonen wie Zielgeräten – über ein Software-Implantat sollten dann Daten ausgelesen werden.

Der Unique Device Identifier (UDID) von iPhone und iPad spielte eine wichtige Rolle bei Identifizierung und Tracking von Zielpersonen durch den britischen Nachrichtendienst GCHQ. Dies geht aus einem weiteren Snowden-Dokument hervor, das der *Spiegel* veröffentlicht hat. Die einzigartige und permanente ID der iOS-Geräte

GELESEN

Reflexe einer

Der «Franken

Über Geld red

Wirtschaft

Federer probl

Schweizer Bö

Managing Dir Development Zühlke Engine

Business Ana PERSONAL S

Leiter Produk Network Sele

Head Quality Engineering M AG

Buchhalter m Reporting Econag Execu

Banking Cons Infosys Lodes

2. Ausgangslage für neues Informationssicherheitsgesetz (ISG)

Neues Informationssicherheitsgesetz – future best practice?

2. Ausgangslage für neues ISG

Wichtigste Gründe für ein Informationssicherheitsgesetz (ISG)

- **16.12.2009** **Angriff auf Systeme des EDA**
  Bundesrat beschliesst Erhöhung der Informationssicherheit in der Bundesverwaltung
- **12.05.2010** **Bundesratsauftrag zur Schaffung formell-gesetzlicher Grundlagen**
  für Informationsschutz
- **03.12.2010** **Lybien-Krise**
  Die GPK-S[1] hält in ihrem Bericht fest, dass „(…) in Sachen Informationsschutz und Schutz von technischen Geräten in der Bundesverwaltung grosser Handlungsbedarf besteht (…)“
- **14.01.2011** **Expertengruppe** unter Prof. Dr. iur. Markus Müller wird eingesetzt
- **30.11.2011** **Bundesratsentscheid**
  1) Ausdehnung des Regelungsbereichs auf die Informationssicherheit
  2) Koordination mit Cyber-Defense-Strategie und Strategie Informationsgesellschaft
- **01.02.2012** **Bundesauftrag** betreff. Harmonisierung / Straffung Personensicherheitsprüfungen
- **19.06.2012** **Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)**

[1] GPK-S: Geschäftsprüfungskommission des Ständerates

2. Ausgangslage

Wichtigste Gründe

Handelszeitung

LOGIN SHOP ABOS E

HOME UNTERNEHMEN MANAGEMENT INVEST KONJUNKTUR POLITIK LIFESTYLE

Geheimdienst-Affäre: Tipp kam von der UBS

Der versuchte Datenklau beim Schweizer Geheimdienst sorgt für rote Köpfe. Nun zeigt sich: Die Affäre flog einem Zeitungsbericht zufolge nur dank der Aufmerksamkeit einer Schweizer Grossbank auf.

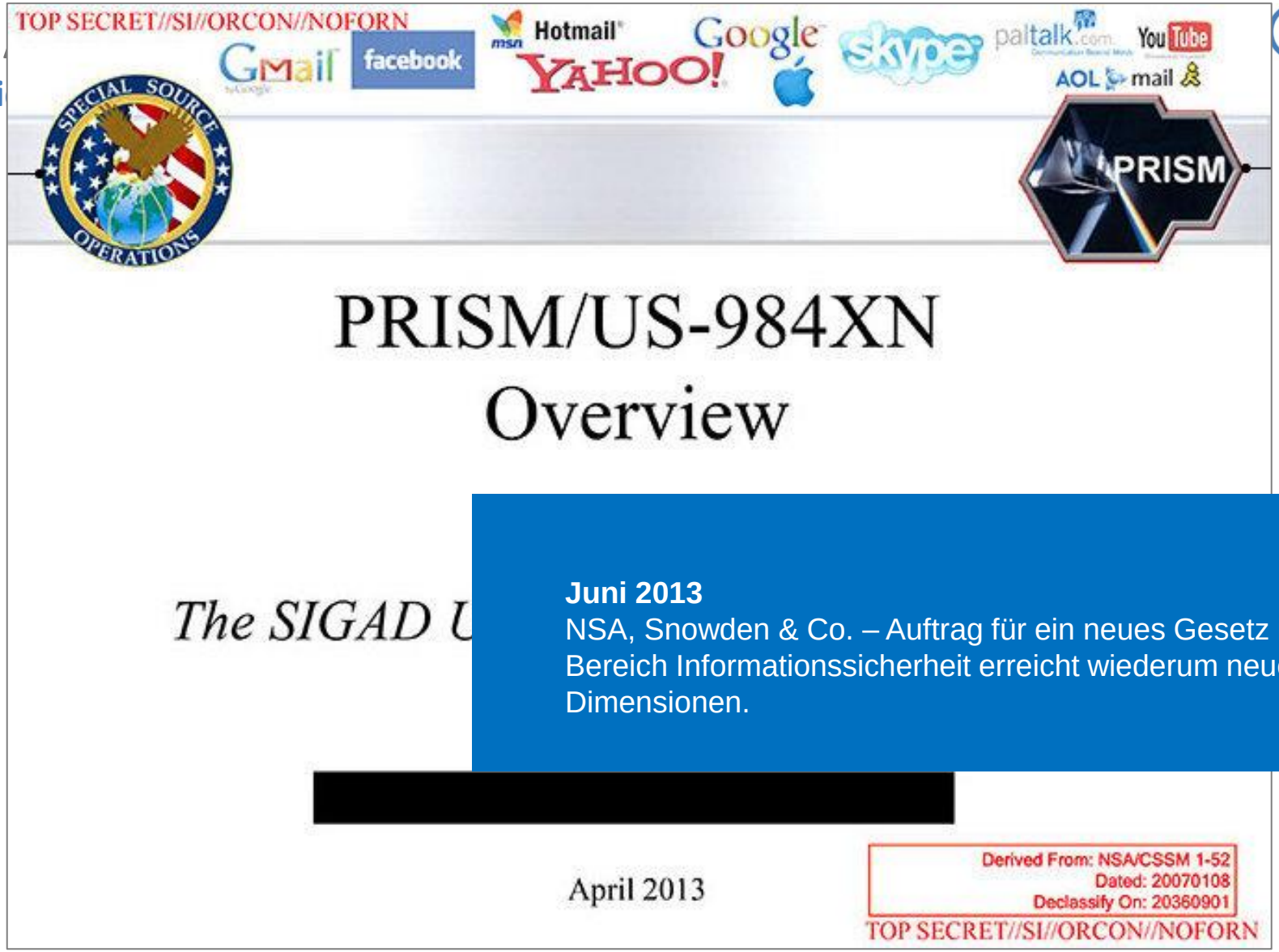
30.09.2012

Die UBS schlug beim Nachrichtendienst Alarm. (Bild: Keystone)

24.10.2012
Bundesrat erteilt Zusatzauftrag: Bericht über Gefahren und Lücken in der Informationssicherheit in der Bundesverwaltung und Vorschläge für Sofortmassnahmen

Siehe Bericht des VBS vom 11.04.2013, Verhinderter Datenabfluss im Nachrichtendienst des Bundes.

2. Wi



Juni 2013
NSA, Snowden & Co. – Auftrag für ein neues Gesetz im Bereich Informationssicherheit erreicht wiederum neue Dimensionen.

2. Ausgangslage für neues ISG

Aktuelle Meilensteine

- **26.03.2014 - 04.07.2014**
  Vernehmlassungsverfahren
- **16.10.2014**
  Bericht über die Ergebnisse des Vernehmlassungsverfahrens
- **Mai 2015**
  Botschaft wird dem Bundesrat vorgelegt
- **Herbst 2015**
  Erstmalige Parlamentarische Beratung
- **01.01.2017**
  Früheste Inkraftsetzung

© Das Schweizer Parlament

3. Ausgewählte Inhalte des ISG und Praxisbeispiele

Neues Informationssicherheitsgesetz – future best practice?

3. Ausgewählte Inhalte des ISG und Praxisbeispiele

Zweck des ISG

Art. 1 Zweck

[1] Dieses Gesetz soll den sicheren Umgang mit Informationen sowie den sicheren Einsatz von Informations- und Kommunikationstechnologien gewährleisten.

[2] Es soll damit die folgende

a. die Entscheidungs-
b. die innere und äuss
c. die aussenpolitische
d. die wirtschafts-, fin
e. die Erfüllung der ge

Bundesbehörden zum

Zum Vergleich: Datenschutzgesetz

Art. 1 Zweck
Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.

Art 2 Geltungsbereich
[1] Dieses Gesetz gilt für das Bearbeiten von Daten natürlicher und juristischer Personen durch:
a. private Personen;
b. Bundesorgane.

3. Ausgewählte Inhalte des ISG und Praxisbeispiele

Begriffe (1)

Erläuternder Bericht, S. 34

„(…) Der Begriff "Information" wird im vorliegenden Informationssicherheitsgesetz (ISG) nicht definiert, da im Erlass auf Legaldefinitionen verzichtet wird und der Begriff im ISG sich mit dem umgangssprachlichen Gebrauch deckt. (…) „

3. Ausgew… …ele
Begriffe (2…

Art. 7 DSG / Art. 8 Abs. 1 VDSG Datensicherheit
«Wer (…) Personendaten bearbeitet ode… Datenkommunikationsnetz zur Verfügun… sorgt für die Vertraulichkeit, die Verfügba… die Integrität der Daten, …»

Art. 3 Abs. 8 BinfV IKT-Sicherheit
«Die IKT-Sicherheit umfasst Massnahmen zum Schutz der Integrität und Verfügbarkeit der IKT-Systeme sowie zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten, die in diesen Systemen gespeichert, verarbeitet und übertragen werden.»

Art. 3 Bst. i ISchV Informatiksicherheit
«die Informatiksicherheit stellt die Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit bei der elektronischen Bearbeitung von Informationen sicher»

ISO 27000:2014
Information security (is the) preserva… confidentiality, integrity and availabil… information.

BSI Standard: Cyber-Sicherheit
Cyber-Sicherheit «umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schliesst darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Damit wird praktisch die gesamte moderne Informations- und Kommunikationstechnik zu einem Teil des Cyber-Raums.»

3. Ausgewählte Inhalte des ISG und Praxisbeispiele

Begriffe (3)

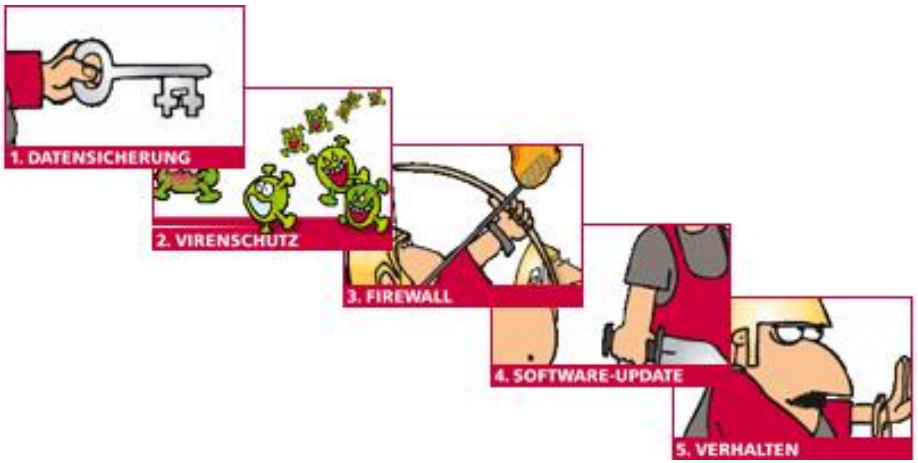
- **Informationen**
  Informationen können sowohl auf Papier, in Rechnersystemen oder im Kopf gespeichert sein.
  Quelle: Definition gemäss dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI)

- **Beispiele**
  Kundendaten (Bankkundendaten, Steuerdaten, Krankenakten, usw.), Sitzungsprotokolle, Geschäftsberichte, Erfindungen, Ideen, Unternehmensstrategien, usw.

© istockphoto

3. Ausgewählte Inhalte des ISG und Praxisbeispiele

Begriffe (4)



© Informatiksteuerungsorgan des Bundes (ISB)

© istockphoto

Informationssicherheit

«Sämtliche Anforderungen und Massnahmen, die zum Schutz der Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von Informationen dienen, und zwar unabhängig davon, ob die Informationen elektronisch, mündlich oder in Papierform bearbeitet werden» (vgl. Erl. Bericht zum ISG; vgl. auch Art. 8 VDSG)

Datenschutz

Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden (vgl. Art. 1 DSG).

3. Ausgewählte Inhalte des ISG und Praxisbeispiele

Klassifizierung von Informationen

- **Art der Daten?** Personendaten, Geschäftsberichte, Erfindungen, …?
- **Klassifizierungsstufen (Art. 14)** „INTERN“, „VERTRAULICH“ und „GEHEIM“
- **Nur für „Informationen“.** Doch welche sind gemeint? Auch Personendaten?
- **EU-Verschlusssache:** Einfluss europäischer Vorgaben, z.B. Schengen/Dublin

Klassifizierung ist die Basis entsprechender organisatorischer und technischer (Schutz-)Massnahmen.

3. Ausgewählte Inhalte des ISG und Praxisbeispiele

Klassifizierung von Informationen

Klassifizierung (ISchV)	KT-Sicher-heitsstufe	Anwendung beim Umgang mit Personendaten (DSG)	Anwendung beim Umgang mit anderen Informationen in der BV
GEHEIM	Erhöhter Schutz	Personendaten, deren Miss-brauch das Leben der betrof-fenen Person gefährden kann.	wie unter Ziff. 1 erwähnt wird darauf nicht Bezug genommen
VERTRAULICH	Erhöhter Schutz	Personendaten, deren Miss-brauch zu einer schweren Beeinträchtigun lichen Situation schaftlichen Ste kann (besonde werte Personer Persönlichkeits	Geschäftsgeheimnisse der Verwaltung, die durch eine
INTERN	Grund-schutz	Personendaten brauch die wirts Situation oder d liche Stellung d Person beeinträ	
Nicht klassifiziert	Grund-schutz	Personendaten brauch in der R betroffene Pers besonderen Folgen hat.	

«Creating groups of information with similar protection needs and specifying information security procedures that apply to all the information in each group facilitates this.»

ISO 27002:2013, 8.2.1 Classification of Information

© ISB – Gegenüberstellung der verschiedenen Klassierungen, Version 1.0, 9.12.2013

3. Ausgewählte Inhalte des ISG und Praxisbeispiele

Personensicherheitsprüfung

- **Personensicherheitsprüfung (ISG)** – erst **nach** Unterzeichnung des Vertrags (Arbeitsvertrag, Dienstleistungsvertrag) zulässig
- **Zugang zu EU-Verschlusssachen** – Personensicherheitsprüfung erst **nach** Unterzeichnung des Vertrags (Arbeitsvertrag, Dienstleistungsvertrag) zulässig
- **ISO 27002:2013, A.7.1** - Human Resource Security: „**Prior** to employment“
  - Screening
- Noch zeitgemäss?

Human Factor nie unterschätzen!
Vgl. die jüngsten Terror-Anschläge in Paris. ☹

3. Ausgewählte Inhalte des ISG und Praxisbeispiele

Human Factor

- **Beispiel: Verantwortlichkeiten für die Klassifizierung**
  - Was ist genau schützenswert? Welche Information? Welche Kriterien?
  - Verantwortung hierfür nicht mehr beim Verfasser bzw. der Verfasserin, sondern NEU bei einer dafür bezeichneten Stelle/Funktion mit entsprechendem Fachwissen (vgl. Art. 13 ISG)
  - Anders: ISO 27002:2013
    „Owners of information assets should be accountable for their classification“.

3. Ausgewählte I

Human Factor

29.12.2014 11:39 « Vorige | Nächste »

Offenbar Spionagesoftware Regin auf Rechner im Kanzleramt entdeckt UPDATE

vorlesen / MP3-Download

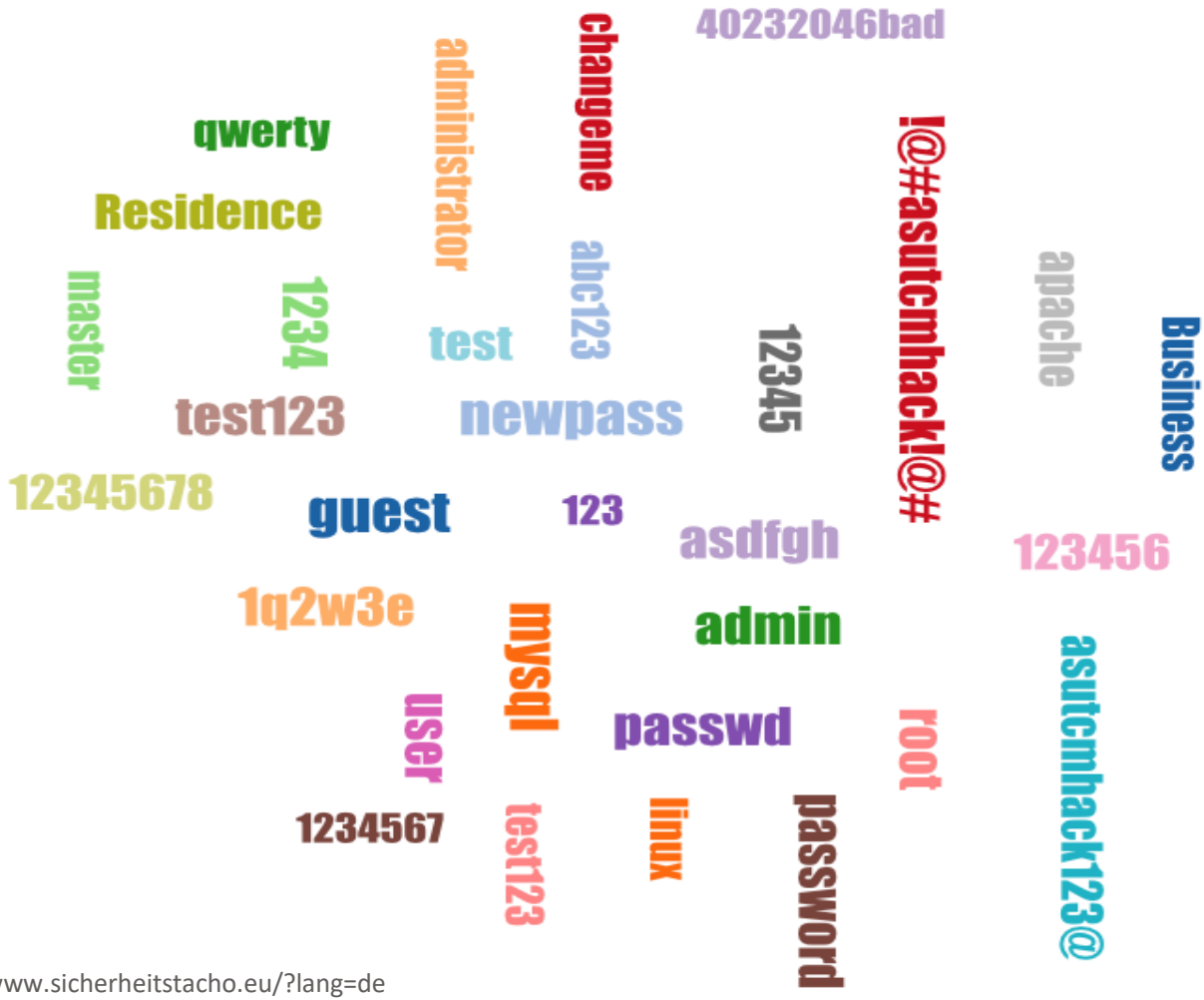
(Bild: dpa, Karl-Josef Hildenbrand)

Per USB-Stick gelangte vergangene Woche offenbar der hochentwickelte Trojaner Regin auf einen Rechner im Bundeskanzleramt. Die Software wird mit westlichen Geheimdiensten in Verbindung gebracht.

Auf einem Computer im Bundeskanzleramt ist laut einem Medienbericht die Spionagesoftware Regin entdeckt worden. Eine Referatsleiterin aus der Europapolitik-Abteilung habe ein Dokument auf einem privaten USB-Stick mit nach Hause genommen, berichtete die Bild-Zeitung am heutigen Montag ohne nähere Angaben zu Quellen zu machen. Dort habe sie auf ihrem Privat-Laptop an dem Dokument weitergearbeitet und den Speicher danach wieder ins Kanzleramt mitgenommen. Als die Frau ihn dann in ihren Dienst-Laptop steckte, habe dessen Viren-Scanner wegen Regin Alarm geschlagen. Daraufhin seien alle Hochsicherheitslaptops im Kanzleramt untersucht worden – ohne weitere Funde.

3. Ausgewählte Inhalte des ISG und Praxisbeispiele

In Angriffen genutzte Passwörter…



Quelle: http://www.sicherheitstacho.eu/?lang=de

insecor

“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.”

Bruce Schneier, Vorwort von "Secrets and Lies", 2000

Vgl. auch den Bericht des VBS vom 11.04.2013 „Verhinderter Datenabfluss im Nachrichtendienst des Bundes“

3. Ausgewählte Inha

Unterstützung der krit

insecor

Liste der kritischen Infrastrukturen

Sektoren	Teilsektoren
Behörden	Diplomatische Vertretungen und Sitze internationaler Organisationen
	Forschung und Lehre
	Kulturgüter
	Parlament, Regierung, Justiz, Verwaltung
Energie	Erdgasversorgung
	Erdölversorgung
	Stromversorgung
Entsorgung	Abfälle
	Abwasser
Finanzen	Banken
	Versicherungen
Gesundheit	Ärztliche Betreuung und Spitäler
	Labors
Industrie	Chemie- und Heilmittelindustrie
	Maschinen-, Elektro- und Metallindustrie
Information und Kommunikation	Informationstechnologien
	Medien
	Postverkehr
	Telekommunikatio
Nahrung	Lebensmittelversor
	Wasserversorgung
Öffentliche Sicherheit	Armee
	Blaulichtorganisati
	Zivilschutz
Verkehr	Luftverkehr
	Schienenverkehr
	Schiffsverkehr
	Strassenverkehr

	Sehr grosse Kritikalität*
	Grosse Kritikalität*
	Reguläre Kritikalität*

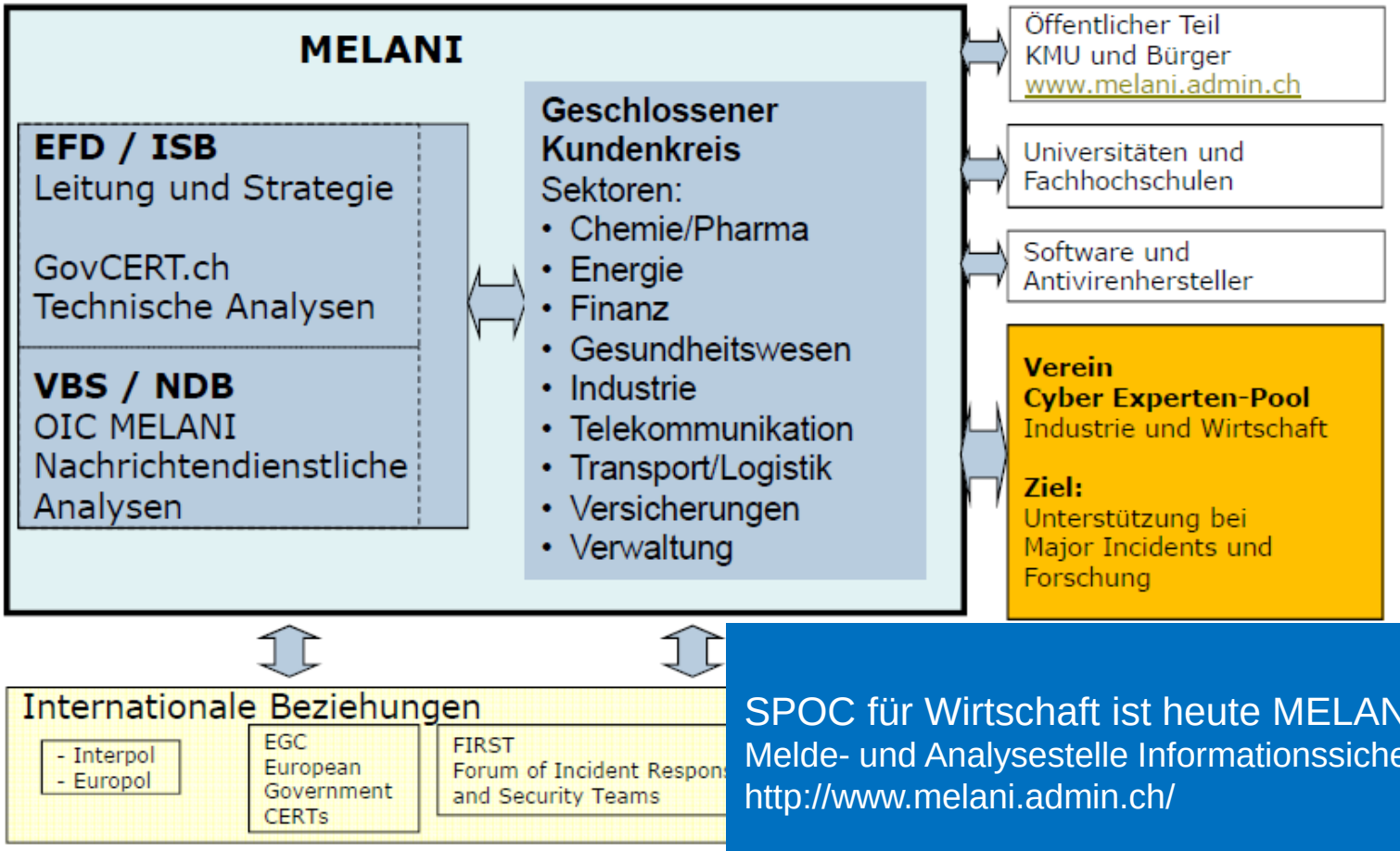
* – Die Kritikalität steht für die relative Bedeutung des Teilsektors bezüglich Bevölkerung, Wirtschaft und Dependenzen (≠ absolute Bedeutung). Zur Ableitung eines allfälligen Handlungsbedarfs sind zusätzlich jeweils die konkrete Bedrohungslage und die Verletzlichkeit der kritischen Infrastrukturen zu berücksichtigen.
– Die Gewichtung macht keine Aussagen über die Kritikalität von Einzelobjekten.
– Die Gewichtung orientiert sich an einer normalen Gefährdungslage.

Nationale Strategie zum Schutz kritischer Infrastrukturen vom 27. Juni 2012
-> Koordination Staat, Wirtschaft und Gesellschaft wichtig!

3.

Org

Das MELANI-PPP-Netzwerk



SPOC für Wirtschaft ist heute MELANI
Melde- und Analysestelle Informationssicherung,
http://www.melani.admin.ch/

© Informatiksteuerungsorgan des Bundes (ISB), aus Präsentation am SPIK 2014

4. Kritische Würdigung

Neues Informationssicherheitsgesetz – future best practice?

5. Kritische Würdigung

Neues ISG: Alles klar?

- **Beispiel: DDoS-Angriffe**
  Sie gehören zu den am häufigsten beobachteten Sicherheitsvorfällen im Cyber-Raum. Kriminelle haben hieraus bereits entsprechende Geschäftsmodelle entwickelt und vermieten Botnetze verschiedener Größen (…).
  Quelle: Allianz für Cybersicherheit

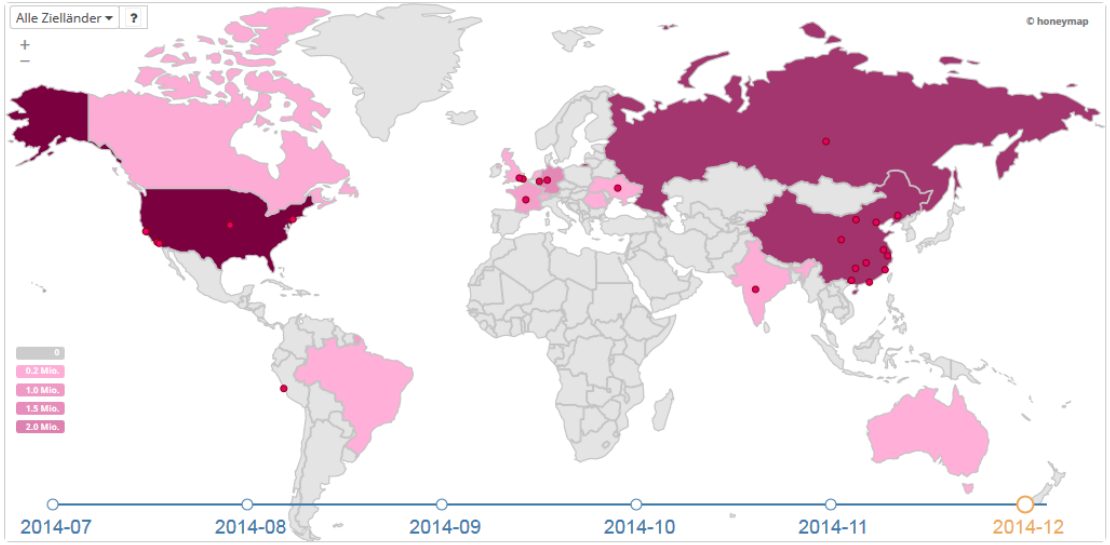
5. Kritische Würdigung

Beispiel: DDos-Angriffe

ERLEBEN, WAS VERBINDET.

ÜBERSICHT | STATISTIKEN | INFO | DOWN

Übersicht über die aktuellen Cyberangriffe (aufgezeichnet von 180 Sensoren)



Top 15 der Ursprungsländer von Angriffen (2014-12)

	Quelle	Anzahl
	Vereinigte Staaten	7.218.795
	China	5.151.994
	Russische Föderation	5.049.609
	Deutschland	1.689.178
	Sonderverwaltungszone Hongkong	845.954
	Frankreich	779.623
	Kanada	259.256
	Vereinigtes Königreich	237.392
	Indien	220.652
	Schweiz	195.358
	Ukraine	194.849
	Australien	149.302
	Niederlande	148.690
	Rumänien	144.767
	Brasilien	137.518

Trendanalyse (Kurzfrist, letzte 24h)

Netzwerkdienste	11835
Konsole/Shell	2031
Webseite	1403
	21
Smartphone	16

Live-Ticker

Datum	Ursprung	Ziel	Angriff auf	Parameter
2015-01-20 21:27:10	China	Deutschland	Netzwerkdienste	honeytrap.pcap.port.5632
2015-01-20 21:27:08	China	Deutschland	Netzwerkdienste	honeytrap.pcap.port.5632
2015-01-20 21:27:06	China	Deutschland	Netzwerkdienste	honeytrap.pcap.port.5632
2015-01-20 21:27:03	China	Deutschland	Netzwerkdienste	honeytrap.pcap.port.5632
2015-01-20 21:27:02	China	Deutschland	Netzwerkdienste	honeytrap.pcap.port.5632

5. Kritische Würdigung

Fazit

- Gesamtheitliche Betrachtung der Informationssicherheit notwendig (Mensch, Organisation, Technik)
- Enge Zusammenarbeit von Staat, Wirtschaft und Gesellschaft
- Staat muss Spielregeln festlegen: für Informationssicherheit und Cybersicherheit / Internet
- Internet macht vor der Staatsgrenze nicht halt: internationale Zusammenarbeit gefragt
- **Human Factor:** Praktikabilität und Aktualität von Sicherheitsmassnahmen laufend hinterfragen!

"Watch the little things;
a small leak will sink a great ship.“
Benjamin Franklin

Besten Dank!

Liliane Mollet
insecor gmbh
Länggassstrasse 8
3012 Bern
Schweiz

Tel: +41 31 302 09 18
E-Mail: l.mollet@insecor.ch
http://www.insecor.ch