BASZ

Awareness
Datenschutz
Analyse und Audit
Risiko-Management
Interimsmanagement

SIDLER
Information Security

www.sidler-security.ch

Swiss Made
Information Security

vom Know-how zum Do-how

NSA - und wie weiter!?

15. Oktober 2013

NEWS -Orwell grüsst!

Clouds: US-Recht öffnet Türen

Eine holländische Studie kommt zum Schluss, dass US-Behörden in Cloud-Daten schnüffeln können, au… …er ausserhalb der USA steht. Einzig der E… …das Recht dazu.

von M…

Verschi… …und Sic… …abe von D… D… …e Recht, se… …es [2]
Ins…
Ans… …t. Es rei… …USA habe, wie… …. Auch Partner im Aus… …iger oder syste… …eit.

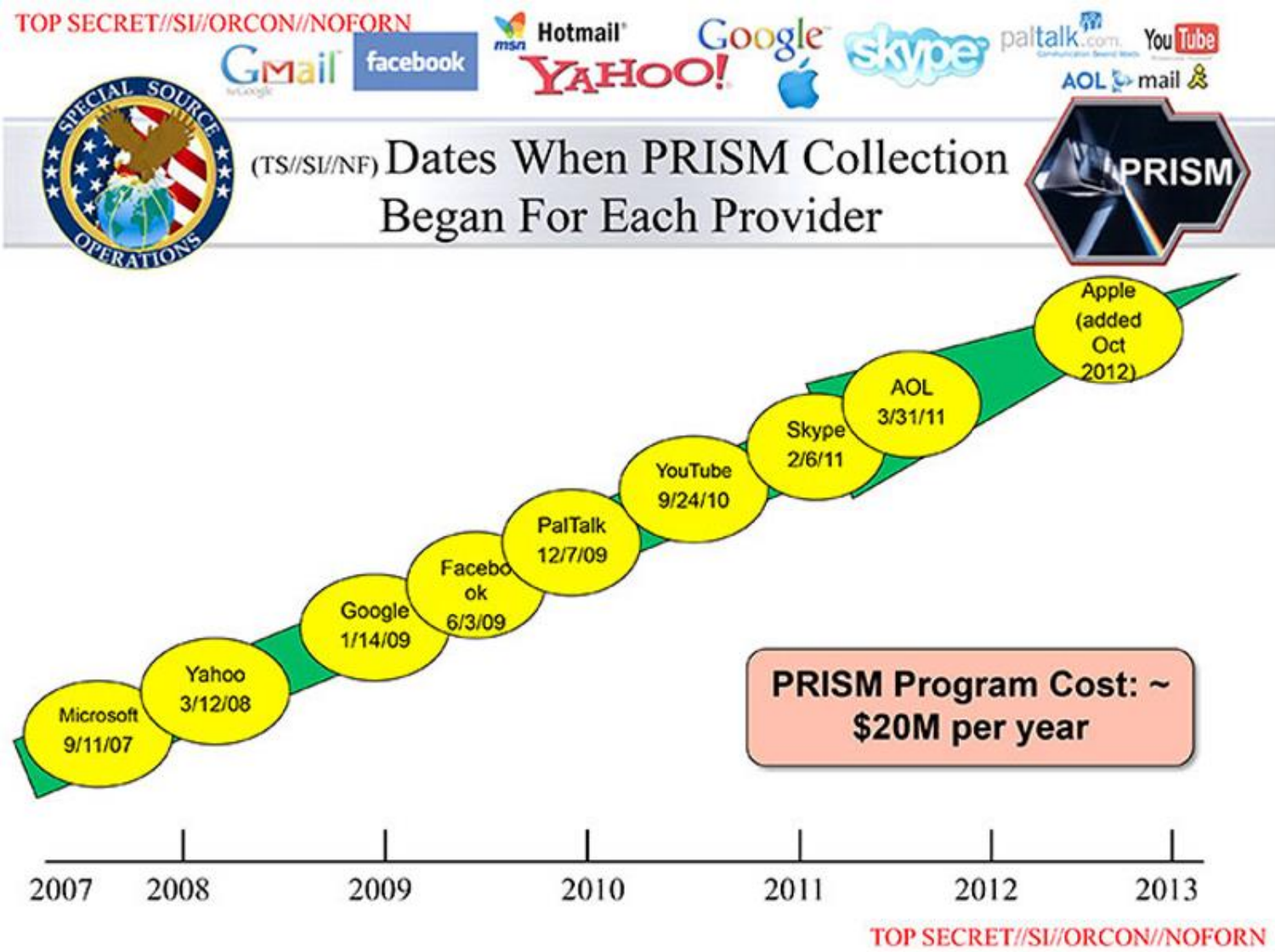
Wenig substa… …dienste

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

…für die US-Geheimdienste «wenig …anzielle 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.

Die Einhaltung von regulatorischen Vorgaben, Datenschutzfragen oder Zertifizierungen spielen hinsichtlich Corporate Governance (GRC) eine wichtige Rolle.

NSA - Überwachung durch die USA

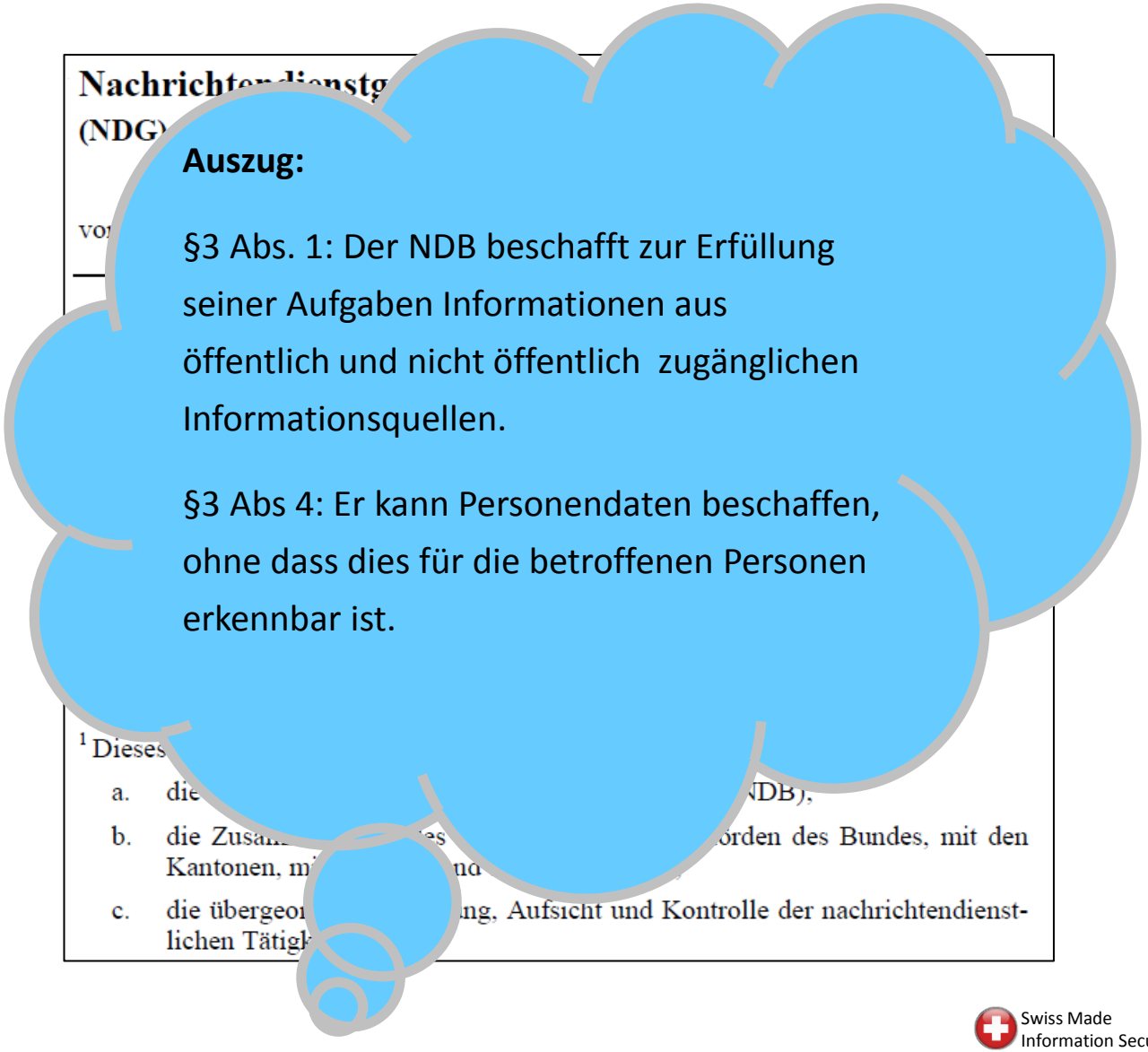


Swiss Made Information Security

SIDLER Information Security

www.sidler-security.ch

Und die Schweiz?



Auszug:

§3 Abs. 1: Der NDB beschafft zur Erfüllung seiner Aufgaben Informationen aus öffentlich und nicht öffentlich zugänglichen Informationsquellen.

§3 Abs 4: Er kann Personendaten beschaffen, ohne dass dies für die betroffenen Personen erkennbar ist.

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.

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.

- 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.

Ist Internet für Sie auch Neuland?

#Neuland Internet

Aktualisiert am 19.06.2013 22 Kommentare

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

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

Kennen Sie die Gefahren und Risiken im Internet? Oder ist Internet für Sie auch Neuland?

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

… oder ignorieren Sie einfach die Risiken?

Quelle: ICT Kommunikation, 19.6.2013

Fragen, die Verwaltungsräte sich stellen sollten

Kennen Sie die Schwachstellen und Risiken Ihrer IT-Umgebung?

Welchen Schaden kann eine Sicherheitslücke für unsere Unternehmensreputation und Markenwahrnehmung bedeuten?

Wie schütze ich mein Unternehmen vor Wirtschaftsspionage?

Kennen Sie die aktuellen externen Risiken und Gefahren?

Haben Sie einen IT-Risiko-Management-Prozess?

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 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.

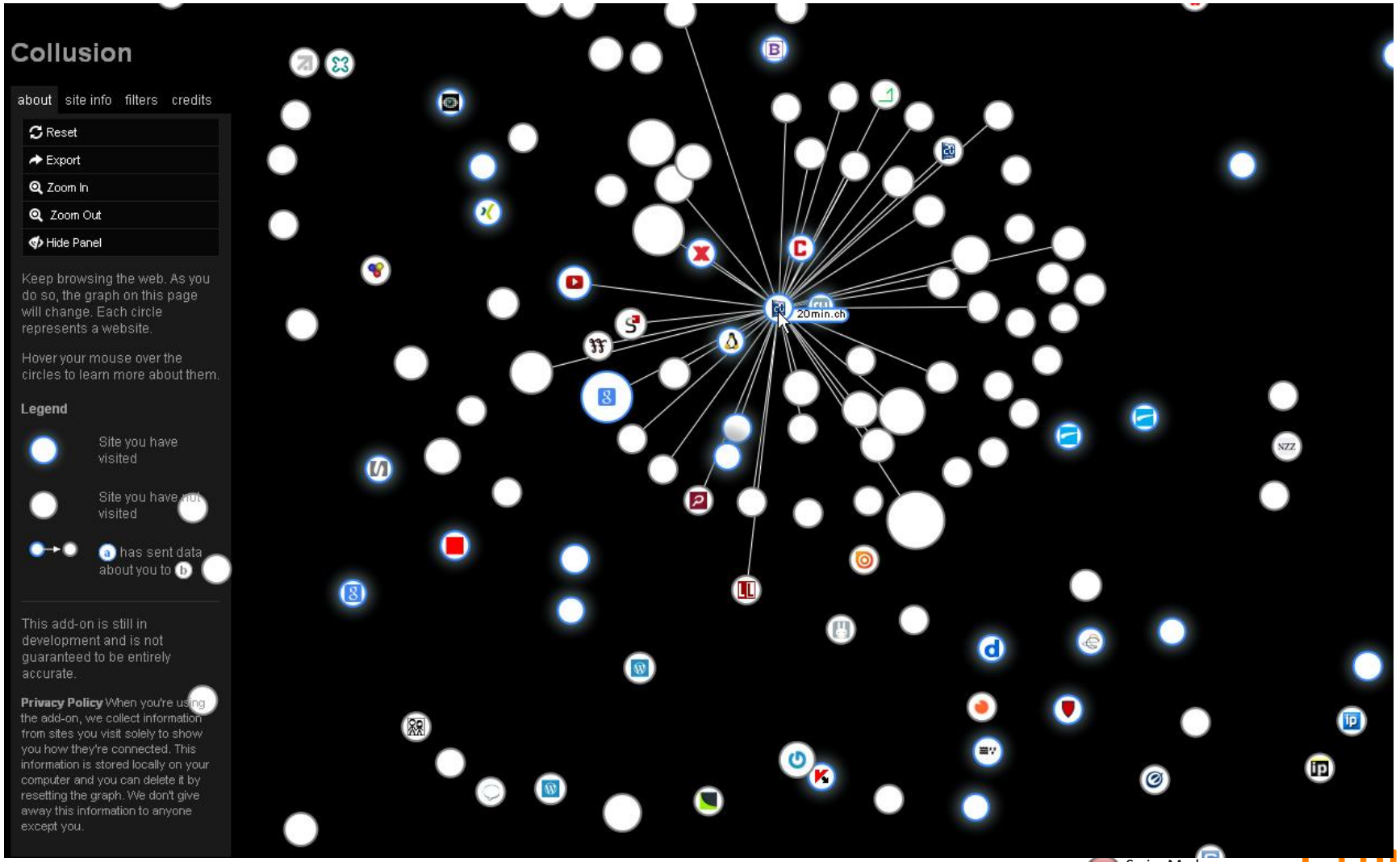
Umgang mit Geschäftsdaten ! ?

Quelle: Computerworld Nov. 2012

CH-Umfrage: Werden Sie abgehört?

Quelle: Computerworld, Juni 2013

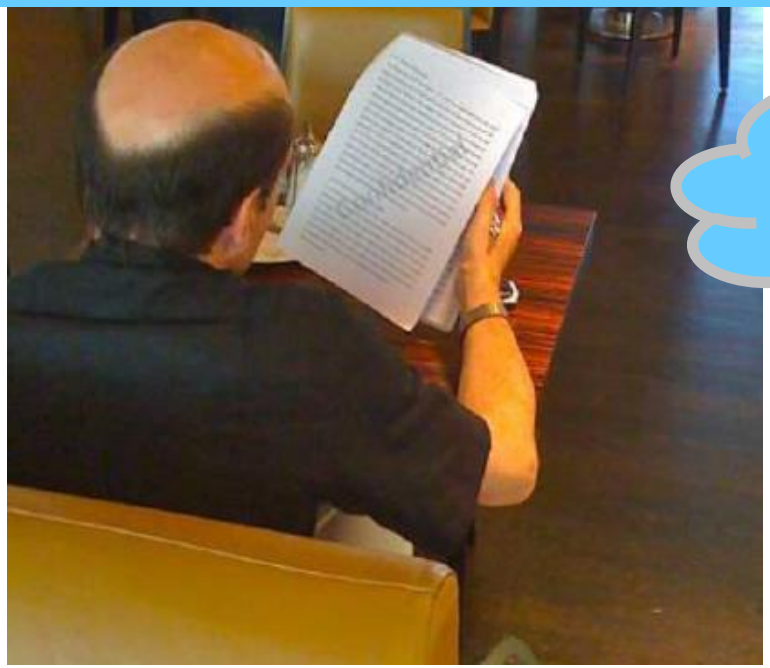
Nicht nur die NSA sammelt Benutzerdaten!



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

Kurz-Video "Wirtschaftsspionage"

Die Top 9 Risiken

Die aktuellen 9 Top-Risiken (Studie)

Die folgenden Top-Risiken wurden im Jahr 2012 in Deutschland in einer aufwendigen Studie identifiziert. Über **20 Prozent** aller Unternehmen hatten in den letzten drei Jahren einen konkreten Spionagevorfall.

Konkrete Handlung (Risiken)	In %
Bewusste Informations- oder Datenweitergabe. Datendiebstahl durch eigene Mitarbeitende.	47.8
Abfluss von Daten durch externe Dritte wie Zulieferer, Dienstleister oder Berater	46.8
Hackerangriffe auf die IT-Systeme und Geräte (Server, Notebook, Tablet, Smartphone)	42.4
Diebstahl von IT-Geräten (Notebook, Tablet, Handy)	32.7
Social Engineering (geschicktes Ausfragen von Mitarbeitenden)	22.7
Sonstiger Informationsabfluss ausserhalb der Firma durch unbedachte Kommunikation, Home-Office, Cloud-Dienste wie Dropbox, etc.	15.5
Abhören und Mitlesen von elektronischer Kommunikation wie unverschlüsselte E-Mails	12.2
Einbruch in Gebäuden bzw. Diebstahl von Dokumenten, Unterlagen, etc.	11.2
Abhören von Besprechungen, Telefonaten, Mitlesen von Faxen oder Ausdrucke	6.5
Sonstiges	0.4

Studie 2012: 6'924 Unternehmen in Deutschland wurden 2012 im Auftrag von TÜV befragt. 10.9% der Befragten Unternehmen waren Banken, Finanzdienstleistungen und Versicherungen.

Einschätzung der künftigen Risiken (Studie)

Welche Entwicklungen sehen Sie als zunehmendes Risiko für Ihr Know-how?

Künftige Risiken (Risiko-Trends)	In %
Zunehmende Verwendung mobiler Geräte wie Tablets und Smartphones	63.7
Sinkende Sensibilität von Mitarbeitenden beim Umgang mit vertraulichem Know-how	54.3
Zunehmendes Outsourcing von Dienstleistungen	52.4
Zunehmender Einsatz von Cloud-Services	47.7
Zunehmende Aktivitäten staatlich gelenkter Hackergruppen (organisierte Kriminalität bzw. individueller Angriff)	44.1
Zunehmende IT-technische Verflechtung mit Kunden und Lieferanten	35.2
Sinkende Loyalität von Mitarbeitenden	26.1
Zunehmende Verlagerung von Geschäft in Auslandniederlassungen	19.9
Sonstiges	5

Studie 2012: 6'924 Unternehmen in Deutschland wurden 2012 im Auftrag von TÜV befragt. 10.9% der Befragten Unternehmen waren Banken, Finanzdienstleistungen und Versicherungen.

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

Reduzieren Sie die Komplexität Ihrer IT-Infrastruktur.

Eine Sicherheitsmassnahme darf nicht mehr kosten als das Risiko.

Cyber-Defense Strategie

Ziele der Cyber Defense Strategie

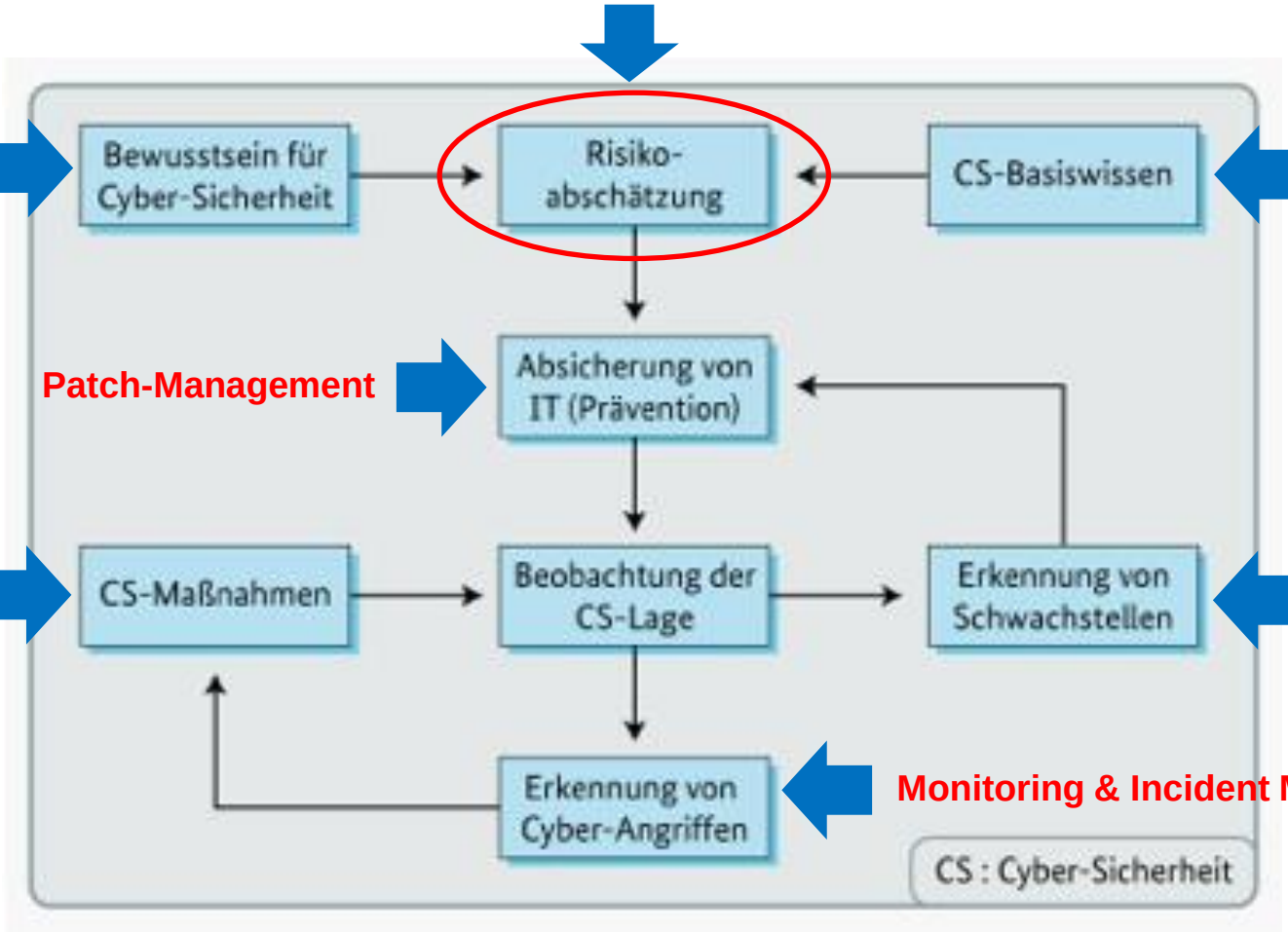
- Frühzeitige Erkennung der Bedrohungen & Gefahren
- Erhöhung Widerstandsfähigkeit Ihrer IT-Infrastruktur
- Wirksame Reduktion von Cyber-Risiken
- Kennen, kommunizieren und akzeptieren der Rest-Risiken

Inhalt Cyber Defense Strategie/Konzept

- Einführung in die Thematik Cyber-Crime
- Analyse der aktuellen und zukünftigen Bedrohungslage bzw. -Szenarien
- Bewertung der Bedrohungs-Szenarien (IT-Risiko Management)
- Definieren von möglichen Sicherheitsmassnahmen (technisch und organisatorisch)
- Definition Vorgehen bei einem Incident inkl. Krisen-Management
- Aufbau Unternehmens-CERT inkl. IT-Infrastruktur-Monitoring
- Kooperation mit der Behörde (MELANI, GovCERT, etc.)

Cyber Defense Governance

bestehender IT-Risiko Katalog mit Cyber- und anderen Szenarien ergänzen



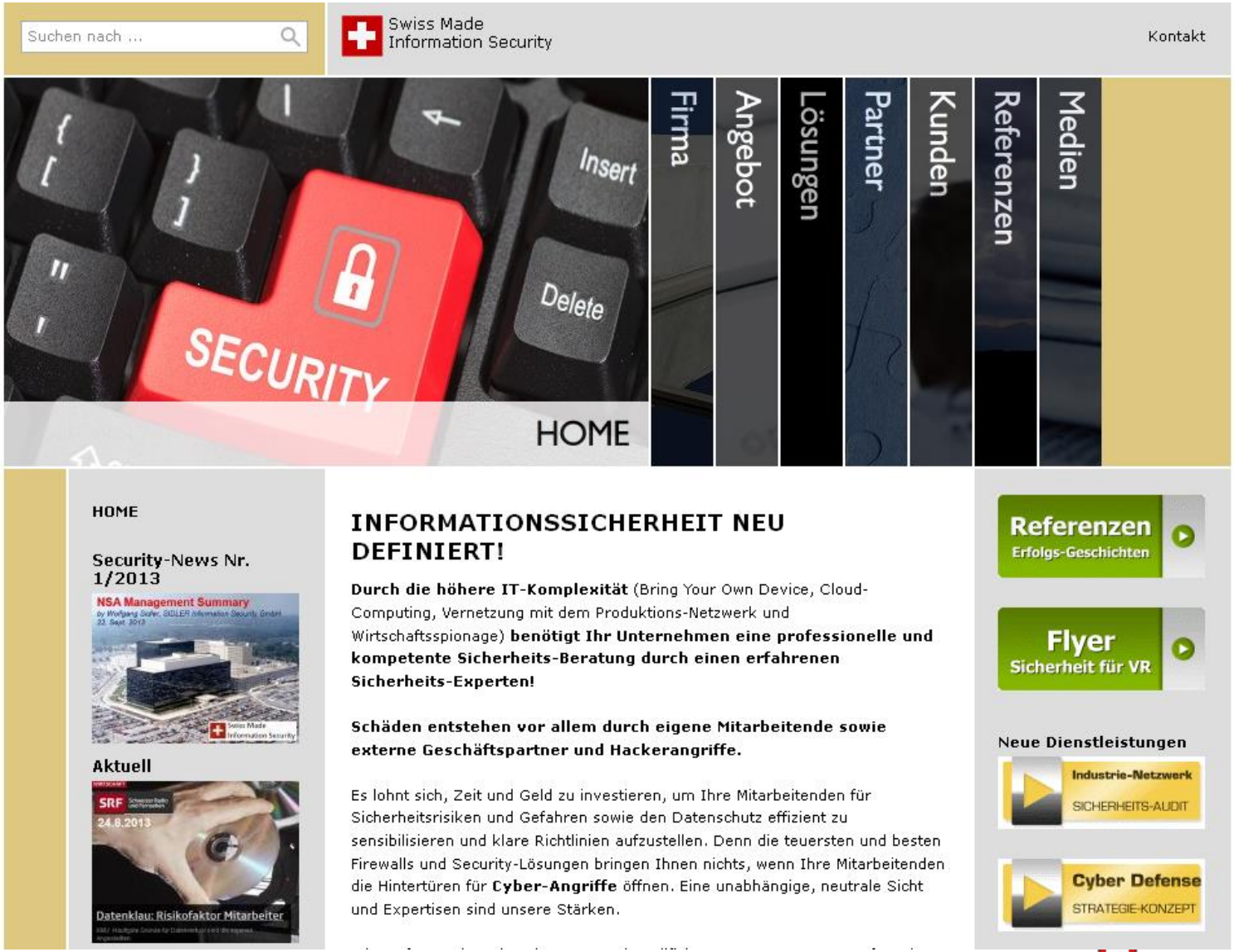
Unsere "Secure" Lösungen

"Secure" Cloud-Lösung

"Secure" Datenaustausch-Plattform

"Secure" Online-Backup

Unser neuer Web-Auftritt



Unsere Success-Stories

PILATUS

IT-Sicherheit wird beim Flugzeughersteller Pilatus Flugzeugwerke AG nicht dem Zufall überlassen

Pilatus Flugzeugwerke AG hat mit einer umfassenden IT-Risiko-Analyse die gesamte Informationssicherheit nachhaltig erhöht. Beratend zur Seite stand dem Unternehmen dabei die Sidler Information Security GmbH.

Pilatus Flugzeugwerke AG mit Hauptsitz in Stans und Niederlassungen in Altenrhein (CH), Broomfield (USA) und Adelaide (Australien), ist führend in der Herstellung von einmotorigen Turboprop-Flugzeugen und die einzige Schweizer Firma, die Trainingssysteme und Flugzeuge für die zivile und militärische Luftfahrt entwickelt, baut und weltweit verkauft. Sorgfalt, Zuverlässigkeit, Leistungsfähigkeit, ausserordentliche Qualität und ein exzellenter Kundenservice sind grundlegende Aspekte, die das Unternehmen dabei auszeichnen. Die Einhaltung höchster Sicherheitsstandards ist ein zusätzliches Muss mit oberster Priorität. Umfassende Sicherheit kann jedoch nur dann erreicht werden, wenn neben einer exzellenten Produkt- und Servicequalität auch die Rahmenbedingungen der Informationssicherheit im Bereich der Forschung, der Entwicklung, der Herstellung und Montage, im Vertrieb und in der Verwaltung stimmen. Denn einerseits fordern gesetzliche und regulatorische Anforderungen sowie höhere Risiken durch Wirtschaftsspionage ein erhöhtes Sicherheitsniveau. Andererseits verlangen auch Kunden spezielle ICT-Sicherheitsstandards. Dazu Christoph Büeler, Head of ICT, Pilatus Flugzeugwerke AG: «Als Technologiekonzern und speziell als Lieferant, müssen wir nicht nur verschiedenste ICT-Sicherheitsstandards erfüllen, sondern auch unsere Vertrauenswürdigkeit gegenüber unseren Kunden, die unter anderem aus dem Regierungs- und Militärumfeld stammen, nachweisen. Sicherheit hat bei uns deshalb nicht nur in der Luft, sondern auch am Boden, sprich bei der gesamten ICT-Infrastruktur, höchste Priorität.»

Mit einer Mehrfachstrategie zum Erfolg

Um sicherzustellen, dass die Anforderungen vollumfänglich erfüllt werden und keine Schlupflöcher bestehen, entschloss sich Pilatus Flugzeugwerke AG, eine ICT-Risiko-Analyse durchzuführen. Ziel der Analyse war es, mögliche Bedrohungsszenarien im Bereich der Informations-Sicherheit aufzuzeigen, die Auswirkungen für das Unternehmen bezogen auf die Kerngeschäftsprozesse zu identifizieren, um daraus die geeignetsten Sicherheits-massnahmen abzuleiten und zu treffen. Von Beginn an war dem Flugzeughersteller klar, dass sie dabei auf die Unterstützung eines externen IT-Security-Dienstleisters zählen wollten. Dazu Christoph Büeler: «Für die Umsetzung fehlten uns damals einerseits die nötigen Ressourcen, andererseits wollten wir das Projekt schnellstmöglich realisieren. Der Beizug eines Sicherheits-Experten hatte zudem den Vorteil, dass das Projekt unabhängig und neutral beurteilt wird, wesentliche Punkte nicht vergessen werden, wir uns nicht auf Nebenschauplätze verlieren, sondern uns auf das Wesentliche konzentrieren konnten.» Nach der Offertphase fiel die Wahl auf die Sidler Information Security aus Hünenberg. Ausschlaggebend dafür war, dass Wolfgang Sidler, Gründer und CEO der Firma, neben seinem ausgewiesenen und langjährigen Security-Know-how, als Security-Experte international tätig war und mit den verschiedenen Kulturen und der Mentalität dort ansässiger Unternehmen vertraut ist.

Treuhand Gesundheit Finanz Industrie Verwaltung Legal Ausbildung

praktisch konkret angemessen

SIDLER Information Security
www.sidler-security.ch
Holzhäusernstrasse 5a
6331 Hünenberg / Zug

Landis+Gyr manage energy better

Landis+Gyr sorgt Für Sicherheit im Smart Metering

Schutzprofil Für Smart-Meter-Gateway nach Common Criteria umgesetzt.

Die Herstellung intelligenter Stromzähler, sogenannte Smart Meter, unterliegt rechtlichen Vorgaben und muss strenge Sicherheitsanforderungen erfüllen, deren Einhaltung geprüft und zertifiziert wird. Mit Unterstützung der Sidler Information Security GmbH hat der Smart-Meter-Pionier Landis+Gyr ein dafür erforderliches Informationssicherheitskonzept erstellt und so den Weg zu sicheren Smart-Meter-Lösungen geebnet. Das erste, nach neustem Standard entwickelte Smart-Meter-Gateway konnte Landis+Gyr im Juli 2013 zur Zertifizierung anmelden.

Landis+Gyr mit Hauptsitz in Zug und Niederlassungen rund um den Globus, ist weltweiter Leader auf dem Gebiet des Smart Metering und führender Anbieter von integrierten Energiemanagementlösungen. Das Unter-nehmen ermöglicht es nicht nur Versorgungs-unternehmen und Endkunden ihre Energieeffizienz zu verbessern, Energiekosten zu senken und zu einer nachhaltigen Nutzung der Ressourcen beizutragen. Nachhaltige Werte schaffen, zukunftsfähige Lösungen entwickeln und diese dabei mit den energiepolitischen Herausforderungen in Einklang bringen, gehört mit zum Tagesgeschäft des Branchenführers.

Rechtlich Anforderungen umsetzen

Der Einsatz intelligenter Stromzähler bzw. Smart Meter gilt als grundlegende Voraussetzung für die Umsetzung des "Aktionsplans für Energieeffizienz in Europa". Dieser sieht vor, dass mindestens 80 Prozent der Verbraucher aller EU-Mitgliedsstaaten bis zum Jahr 2020 mit intelligenten auszustatten sind. Im Rahmen der unter Berücksichtigung Deutschland eine Vorreiterrolle ein und hat durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein Schutzprofil (BSI-CC-0073) nach den "Common Criteria" für ein Smart Metering Gateway und die dazugehörigen Sicherheitsmodule herausgegeben. Für Hersteller wie Landis+Gyr stellten die umfangreichen Anforderungen des BSI-Schutzprofils und die damit verbundenen rechtlichen Vorgaben, die in den elektronischen Zählern und Smart-Meter-Gateways umgesetzt werden müssen, vor neuartige Herausforderungen. Denn nicht nur das Produkt an sich wird hinsichtlich Sicherheitsanforderungen dieser Zertifizierung unterzogen. Bestimmte Mindestanforderungen müssen auch im Entwicklungsprozess, in der Dokumentation, bei der Unterstützung des Produktlebenszyklus, bei Tests sowie der Schwachstellenanalyse erfüllt werden. Und nur wenn das Gesamtumfeld dieser Auditierung standhält, erhält das Produkt ein Zertifikat. Dazu Thomas Mosel, Head of Information Security EMEA, bei Landis+Gyr: «Das Schutzprofil nach den international anerkannten IT-Sicherheitsrichtlinien der Common Criteria beinhaltet eine grosse Anzahl von Sicherheitsanforderungen. Uns war schnell klar, dass wir für die Umsetzung dieses umfassenden Anforderungskatalogs, im speziellen für den IT-Sicherheitsbereich, jemanden mit entsprechendem Know-how beiziehen mussten. Auf der Suche nach einem Experten sind wir auf Wolfgang Sidler von der Sidler Information Security gestossen. Sein enormes Sicherheitswissen passte perfekt auf das bevorstehende Projekt. So sind wir ins Gespräch gekommen und haben ihn für die Umsetzung des Projektes verpflichtet.»

Bereichsübergreifende GAP-Analyse von A bis Z

Im April 2012 starteten Thomas Mosel und Wolfgang Sidler mit einer eingehenden Bestandsaufnahme mittels GAP-Analyse, in der die bestehende Informationssicherheit gegenüber dem vorliegenden Anforderungskatalog abgeglichen wurde.

Treuhand Gesundheit Finanz Industrie Verwaltung Legal Ausbildung

praktisch konkret angemessen

SIDLER Information Security
www.sidler-security.ch
Holzhäusernstrasse 5a
6331 Hünenberg / Zug

Angebot nur für BASZ Mitglieder

Alle **BASZ Mitglieder** erhalten einen umfassenden IT-Schwachstellen Scan (Vulnerability Scan) gemäss Flyer statt für **CHF 2’500.-** für nur

1'900.- (-24%)exkl. MWST

gültig bis 31. Dezember 2013 (Bestellung)

Swiss Made Information Security
www.sidler-security.ch
SIDLER Information Security

Danke für Ihre Aufmerksamkeit