SWISS DELUXE HOTELS

SIDLER
Information Security

vom Know-how zum Do-how

Informationssicherheit in der Praxis

SWISS DELUXE HOTELS - 8. ERFA Meeting - 26. Mai 2016 - Hotel Palace Luzern

Wolfgang Sidler

Die «Evil Maid / Böses Zimmermädchen» Attacke

Das böse Zimmermädchen, installiert unbemerkt einen Key-Logger auf dem Notebook (Booten ab USB-Stick). Der Benutzer meldet sich mit dem Benutzername und Passwort an und der Key-Logger schreibt alles im Klartext in den Boot-Loader. Der Benutzer meldet sich an und das Zimmermädchen kommt noch einmal vorbei und liest die Datei auf dem Boot-Loader aus und loggt sich so ein. Dies funktioniert auch bei einem Notebook mit einer verschlüsselten Festplatte (z.B. mit TrueCrypt oder BitLocker).

Die «Evil Maid / Böses Zimmermädchen» Attacke

Effektiver Schutz – Lösung:

Für Sie als Hotelier

- Background Screening der Mitarbeitenden

Für den Gast als Notebook-Benutzer

- Installieren Sie eine Festplatten-Verschlüsselungs-Lösung mit einem Pre-boot-Loader
- Verwenden Sie eine 2-Faktor Autorisierung z.B. mit einer Smart-Karte
- BIOS mit einem Passwort schützen (nur bedingt sicher, macht es dem Angreifer einfach etwas schwerer ☺) Boot ab USB/DVD ausschalten

Risiken und Gefahren für die Hotels

Die Hotelkette White Lodging Services Corporation aus Indiana, zu der auch Marriott Hotels gehören, meldete **Anfang 2015** einen Cyberangriff, der über **sieben Monate** andauerte.

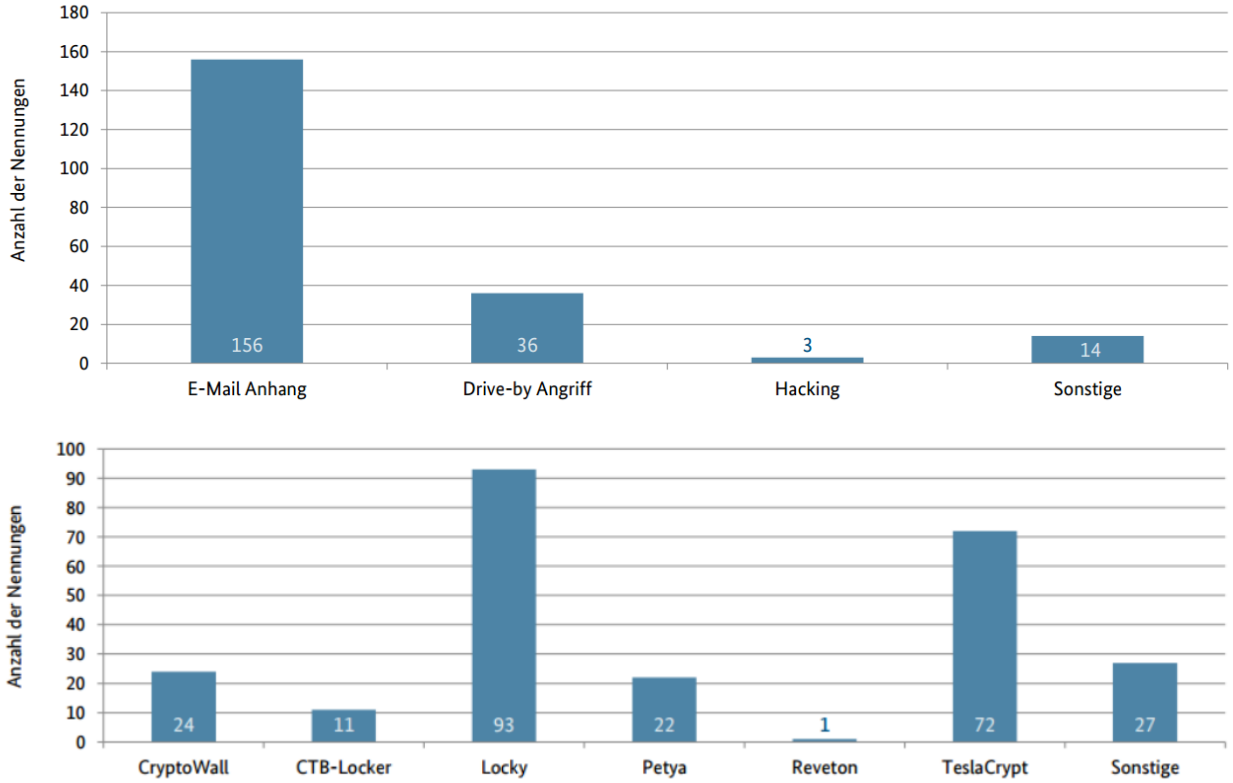
Bei diesem Vorfall war es den Kriminellen gelungen, sich **Zugriff auf das Netzwerk** und die darin enthaltenen Daten zu verschaffen.

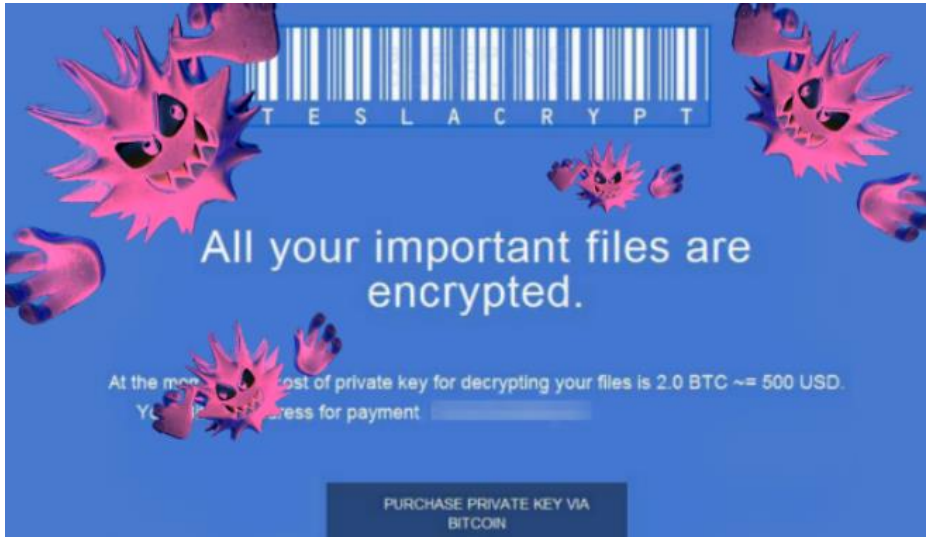
Anfang 2016 war dann die Hyatt-Kette an der Reihe, die massive Abschöpfung von Kreditkarten- und Kundendaten bekannt zu geben. **Weltweit 250 Hotels der Kette waren davon betroffen**.

Tipps

- Schulen und sensibilisieren Sie Ihre Mitarbeitenden auf allen Stufen in Bezug auf Phishing und Social Engineering.
- Halten Sie Ihre PC‘s auf dem aktuellsten Software-Stand.
- Führen Sie eine GAP-Analyse durch, um herauszufinden, wie es um Ihre Sicherheit steht
- Führen Sie jedes Jahr einen unabhängigen Security-Audit/Vulnerability-Check durch
- Sparsamer Umgang mit Kreditkarten-Daten. Erstellen Sie ein Inventar über alle Systeme, welche Kreditkarten-Daten speichern.
- Speichern Sie nur Name und Ablaufdatum. Die anderen Merkmale bitte maskieren!
- Ist Ihre Hotel-Management-Software PCI (Payment Card Industry) kompatibel?
- Lassen Sie Kreditkarten-Daten nicht in den E-Mails und kopieren Sie diese direkt ins Hotel-Management-System
- Vernichten Sie nicht mehr benötigte Kreditkarten-Daten, Ausdrucke gehören geschreddert
- Löschen Sie alle Gruppenaccounts (jeder Mitarbeitende hat ein eigener Account mit seinem persönlichen Passwort, Audit-Trail)
- Trennen Sie Gäste-WLAN mit dem Hotel-Office-Netzwerk
- Speichern Sie Ihre Daten nur auf Hardware basierte Verschlüsselungs-Sticks
- Informieren Sie doch Ihre Gäste über mögliche Risiken mit einem netten Info-Schreiben

Verschlüsselungs-Trojaner





Ein neuer Krypto-Trojaner geht um: Die Alpha Ransomware verlangt iTunes-Gutscheine vom Opfer, sonst bleiben die Daten mit AES-256 verschlüsselt. Der Erpresserbrief ist überraschend höflich, verschweigt allerdings wichtige Details. Der Krypto-Trojaner Alpha Ransomware verschlüsselt eine grosse Anzahl von Dateitypen auf dem Rechner der Opfer und fragt dann, äusserst höflich, nach Lösegeld. Statt der Krypto-Währung Bitcoin verlangen die höflichen Erpresser die 400 US-Dollar Lösegeld in Form von iTunes-Geschenkgutscheinen. Erkennen können Betroffene den Schädling an der Dateiendung .encrypt der verschlüsselten Daten.

Verschlüsselungs-Trojaner

Tipps:

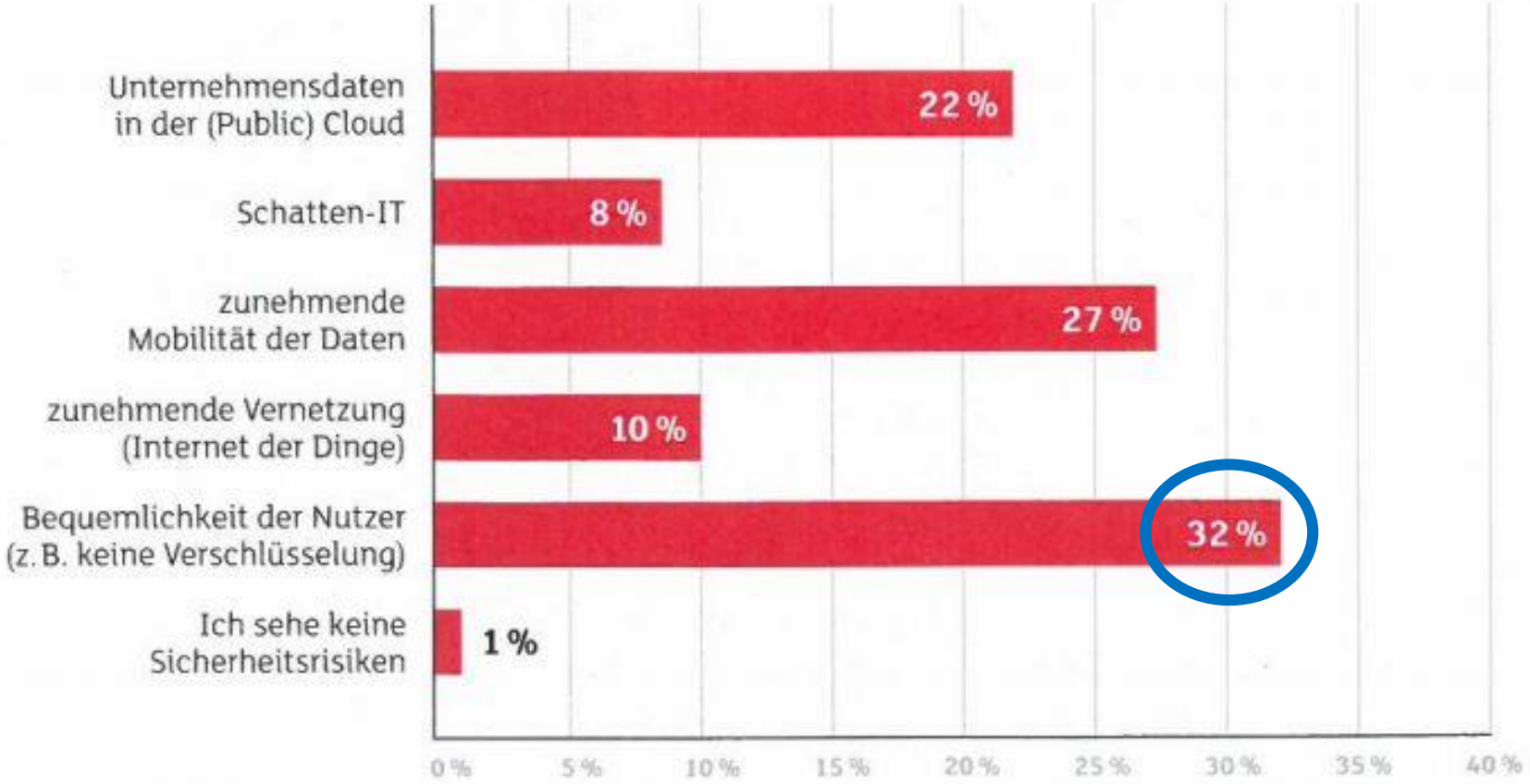
- Browser (Internet Explorer, Firefox, Chrome, etc.)
- Java von Sun
- Adobe Flashplayer
- Adobe Reader
- Quicktime und andere Video-Player
- Und alle Programme, welche direkt mit dem Internet kommunizieren!
- Ein guter Echtzeit-Virenschutz inkl. Browser-Schutz und Anti-Phishing-Schutz
- Macro-Ausführung in den Office-Anwendungen deaktivieren oder einschränken
- Gesunder Menschenverstand und etwas Misstrauen
- Regelmässige Datensicherung inkl. Restore-Test

Aktuelle Top-Gefahren

SWISS IT 2015

DIE GRÖSSTEN GEFAHREN FÜR UNTERNEHMENSDATEN

Die IT-Verantwortlichen orten im Verhalten der Mitarbeitenden den grössten Gefahrenherd. Bequemlichkeit und Mobilität fördern das Risiko. Quelle: Computerworld Swiss IT 2015 (CIOs, n = 433)



Quelle: Swiss IT (April 2015)

SIDLER Information Security

Aktuelle Top-Gefahren

Quelle: Swiss IT (April 2015)

Weitere Top-Risiken

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**

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

SIDLER
Information Security

Menschliches Fehlverhalten

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

2001
- 62‘000 Handys (3 pro Taxi)
- 2’900 Notebooks
- 1‘300 PDAs

2004
- 63‘135 Handys
- 4‘973 Notebooks
- 5‘838 PDAs

ZürcherInnen verlieren über 3000 Handys!
In Zürich wurden von Januar bis Juli 2012 **3'250 Handys** und **200 Laptops** im städtischen Fundbüro abgegeben.

Fundsachen 07. Januar 2014 08:06; *Akt: 07.01.2014 10:19*

Pendler haben 12'000 Handys im Zug vergessen

100'000 Gegenstände haben Schweizer 2013 in Zügen und Bahnhöfen liegen lassen – vom Rollstuhl über Sexspielzeug bis zur Urne. Nur wenig mehr als die Hälfte davon holten sie ab.

1|2 Ein Metalldetektor, eine Urne, ein Rollstuhl und eine Beinprothese: Roland Widmer von Fundsachenverkauf.ch mit einigen der Fundgegenstände aus dem Jahr 2013.

Bild: hal

ein aus i

Tweet

Taschen, Koffer, Kleider und Elektrogeräte: Im Keller des Fundsachenverkauf.ch in Zürich stapelt sich die Ware auf Holzpaletten und in Kisten mit Aufschriften wie «Spielzeug», «Schmuck», «iPhone» oder «Erotik». Hier landet, was in der Schweiz in Zügen und Postautos sowie an Bahnhöfen und Flughäfen liegen geblieben ist und nicht abgeholt wurde.

Menschliches Fehlverhalten

190,000 mobile phones left in London Taxis every year

Press Association

PUBLISHED
06/10/2014 | 09:02

SHARE

More than 190,000 mobile phones are lost in the back of London taxis each year, in what a security firm has called a technology "black hole". PA photo.

More than 190,000 mobile phones are lost in the back of London taxis each year, in what a security firm has called a technology "black hole".

SIDLER
Information Security

Ungebetene Zuhörer !

SIDLER
Information Security

Ungebetene Zuhörer !

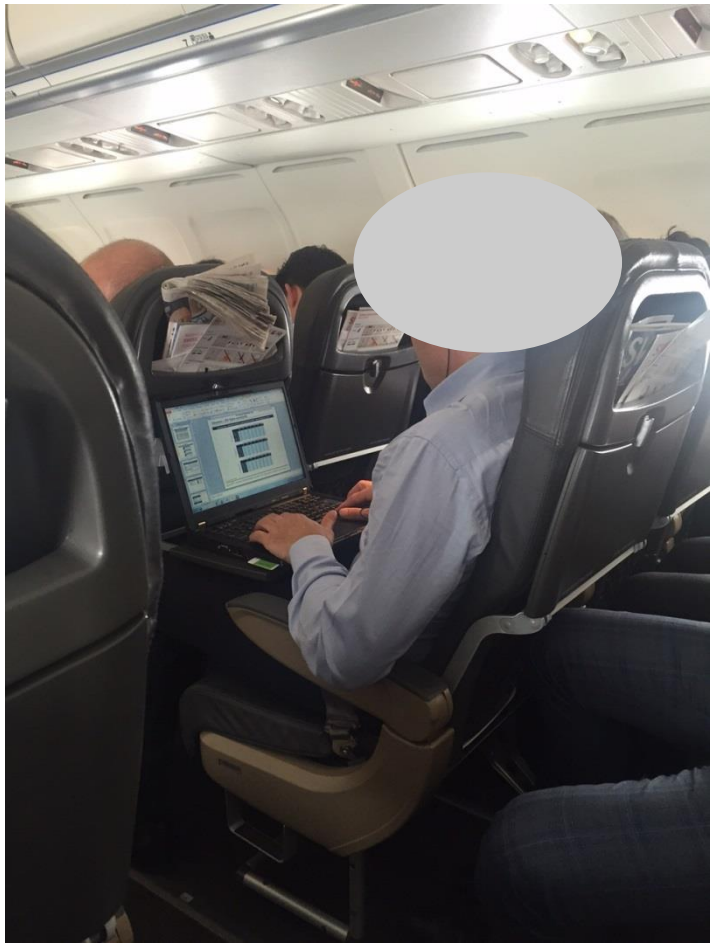
Tipps:

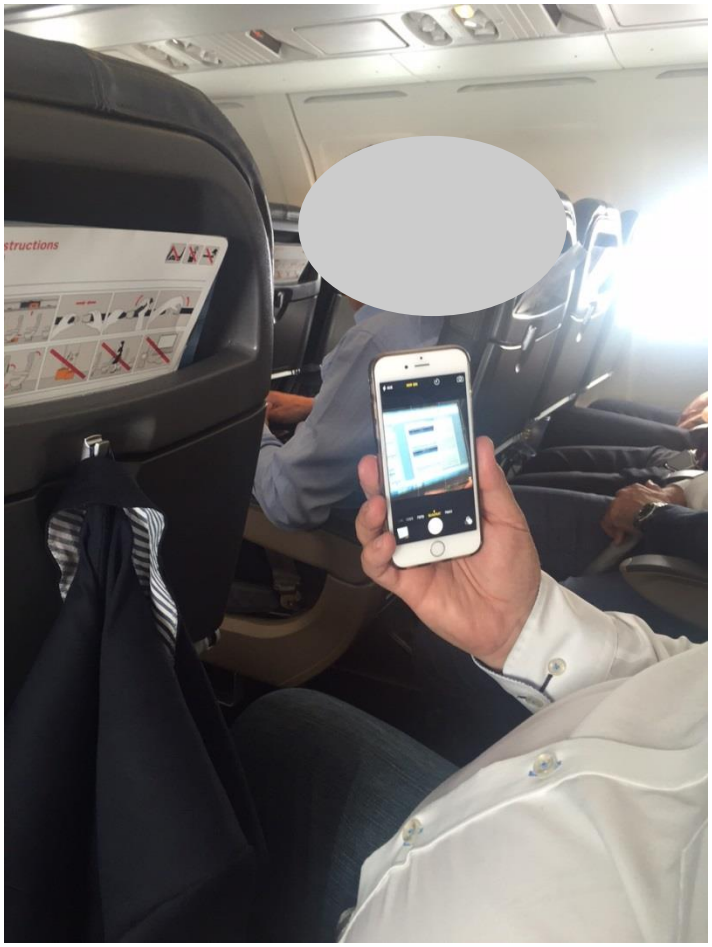
Unternehmen geben Unsummen für teure Sicherheitsmassnahmen aus, verschlüsseln ihre Nachrichten mit VPN, und dann im Zug oder Flugzeug verbreiten sie die Nachrichten freizügig!

- **Behandeln Sie Gäste-Themen wie Namen, etc. in der Öffentlichkeit vertraulich**
- **Lassen Sie andere nicht mithören**
- **Lassen Sie sich nicht aushorchen**
- **Verwenden Sie beim Notebook einen Sichtschutzfilter**

Passagier liest mit!

Swiss Flug von London City nach Zürich am 14.5.2015 (17:05)





SIDLER Information Security

Passagier liest mit!

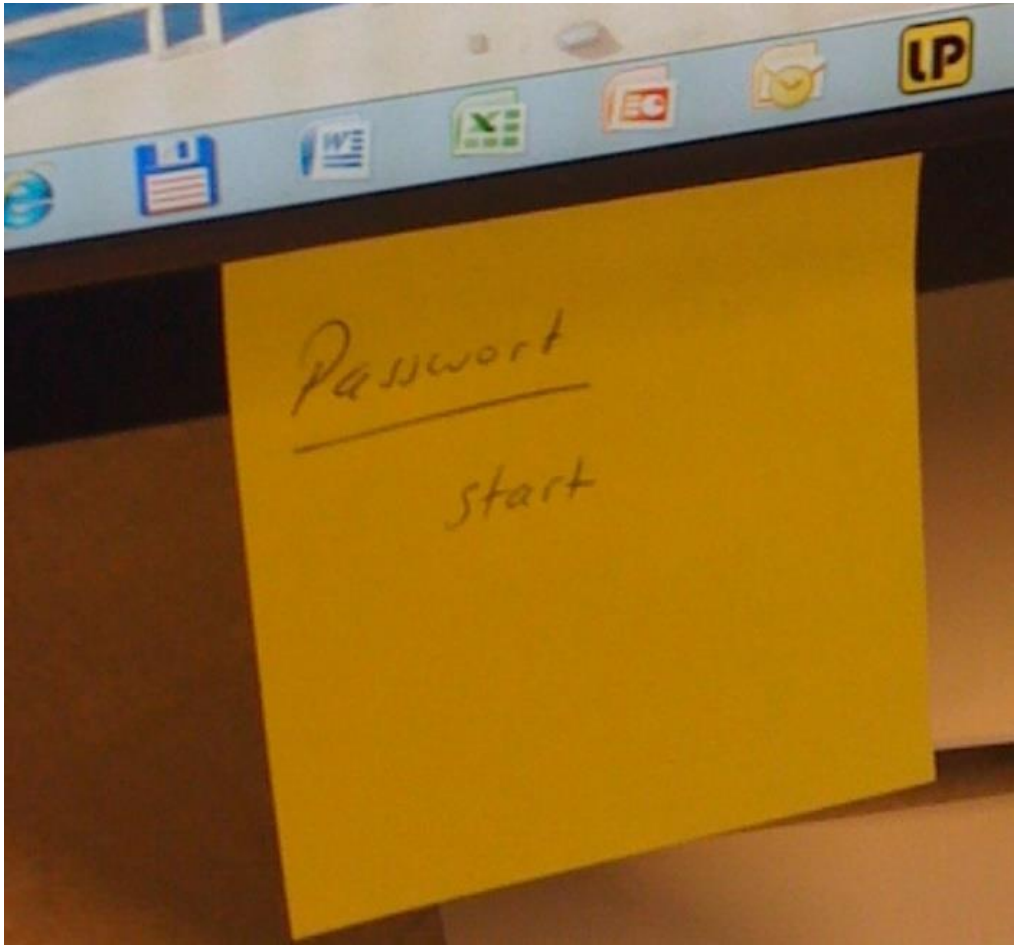
Wir konnten ohne Probleme die Präsentation lesen. Es war eine M&A Transaktion einer Medical-Company im Auftrag einer Grossbank.

Tipps:

- Sichtschutzfilter für Notebook-Bildschirm
- Geräte «nie» mit Namen und Firma anschreiben!!! → macht neugierig!

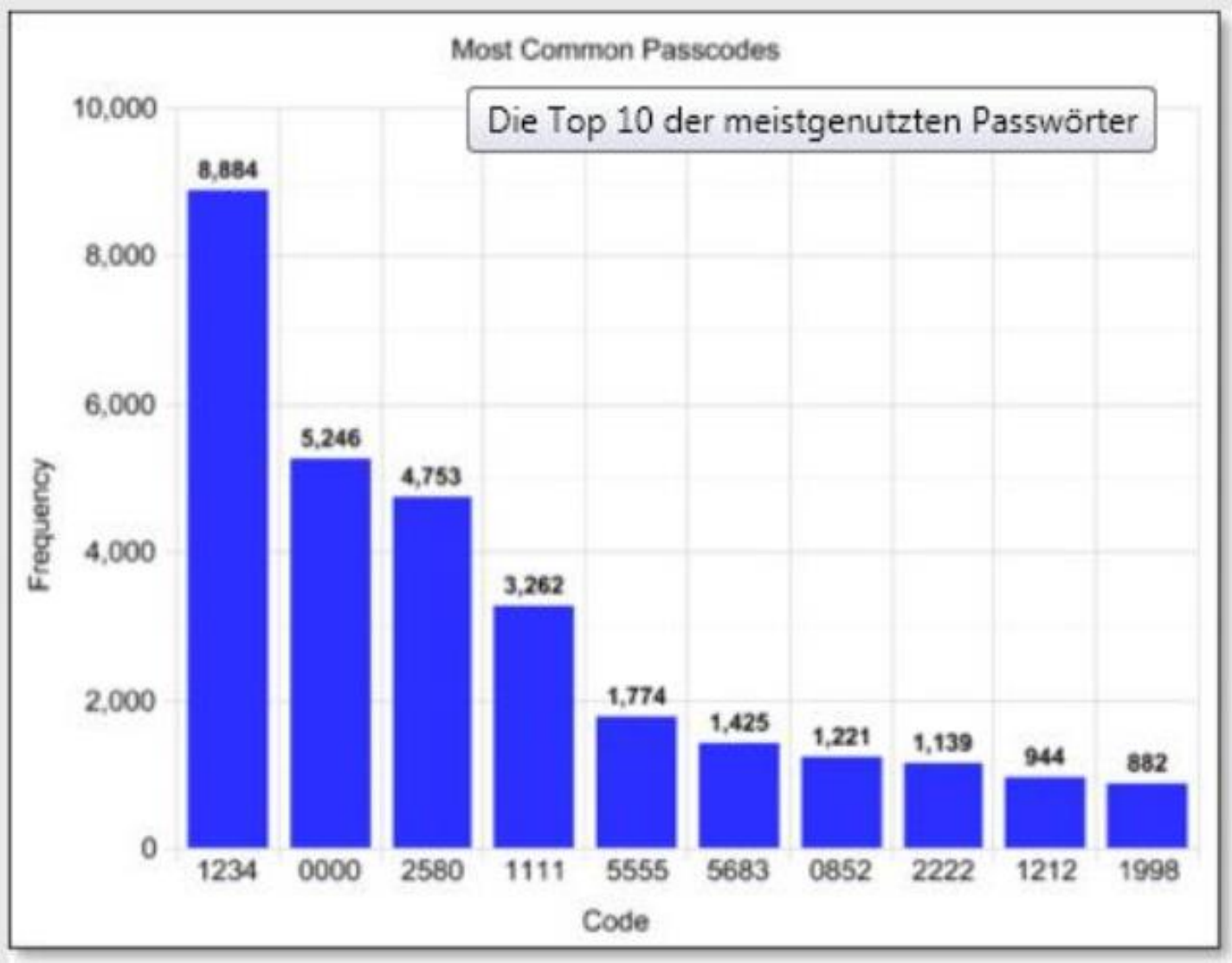
SIDLER Information Security

Umgang mit Passwörter!



SIDLER
Information Security

Umgang mit Passwörter!



SIDLER
Information Security

Achtung: WebCam aktiv!

Bund empfiehlt das Abkleben von Webcams
Die Melde- und Analysestelle Informationssicherung des Bundes (Melani) empfiehlt, alle Webcams temporär abzukleben. Dadurch schütze man sich vor unerwünschten Zuschauern.

Wie bereits letzten November bekannt wurde, fielen Tausende von Webcambesitzer einem Hackerangriff zum Opfer. Darunter befanden sich nach neusten Erkenntnissen auch **141 Webcams aus der Schweiz**.

Watch Linksys camera in
Switzerland
Schaffhausen

Watch Panasonic camera in
Switzerland
Zurich

Tipp:
Default Passwort ändern!

Country:	Switzerland. You can see other **online cameras** in Switzerland.
Country code:	CH
Region:	Zurich
City:	Zurich. **View CCTV online** in Zurich.
Latitude:	47.366670
Longitude:	8.550000
ZIP:	8045
Timezone:	+02:00
Channels:	1
Manufacturer:	Panasonic

GSM Mini-Sender

Der Akku versorgt den Mini-Sender bis zu **einer Woche lang im Standby** mit Strom. Eine dauerhafte Übertragung des Signals kann bis zu 2 Stunden lang erfolgen. Rufen Sie den GSM Sender an und hören Sie in das Umfeld hinein. Auch können Sie eine SMS an den Sender senden, nach deren Empfang der Audiosender Sie zurückruft.

Besonderes Highlight ist aber die **Geräuschaktivierung**: Registriert der Mini Audiosender im Umfeld z.B. ein Gespräch, werden Sie automatisch angerufen. Damit ergeben sich viele Einsatzmöglichkeiten im Bereich der Langzeit-Raumüberwachung.

Durch seine geringen Abmessungen findet der Audio-Sender überall Platz und kann auch jederzeit mitgenommen werden. Ist der Akku einmal leer, wird dieser per Netzteil geladen.

Spionage-Cams

Videos, Fotos, Tonaufnahmen. Zugleich USB-Stick und elegantes Schreibgerät.

Auf den ersten Blick ein elegantes Schreibgerät. Doch im Inneren dieses genialen Tools ist eine 1,3-MegaPixel-Kamera eingebaut. Klippen Sie den Pen einfach an Ihre Brusttasche und schalten Sie ein. So gelingen Ihnen unauffällig wahre Live-Mitschnitte, Sie verpassen nie mehr einmalige Momente – und haben dennoch beide Hände frei. Ideal auch zur Beweissicherung, als Gedächtnisstütze beim Meeting, bei Vorträgen, …

Nicht grösser als ein Stecknadelkopf, versteckt sich das Fix-Focus-Objektiv oberhalb des Clips.
Aus bis zu 4 Metern Entfernung schiessen Sie Fotos (mit einer Auflösung von 1280 x 1024 Pixel) und drehen Farbvideos im avi-Format (640 x 480 Pixel). Auch ein Mikrofon ist eingebaut. Auf den integrierten 2-GB-Speicher passen bis zu 5 Stunden Bild- und Tonaufnahmen.

Ebenfalls über den USB-Stecker laden Sie den eingebauten Lithium-Polymer-Akku auf (Ladekabel mitgeliefert; Ladezeit 2 Stunden). Schreibt mit handelsüblicher Mine. Aus lackiertem Metall. Wiegt nur 37g.

Schutz Ihrer Geschäftsprozesse

Geschäftsprozess

Anwendungen

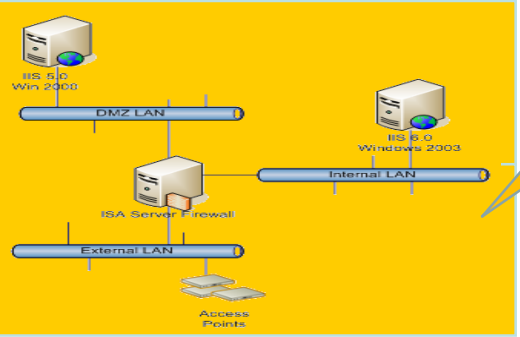
Betriebssysteme

Hardware (Server)

Netzwerk (intern)

Telekommunikation (extern)

Cloud-Computing



Energie

Sicherheit

Sicherheit

Sicherheit

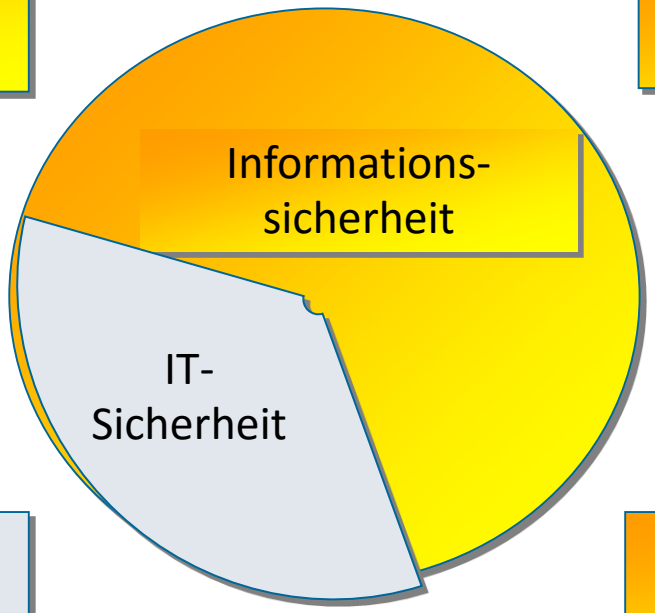
Sicherheit

Querschnittsfunktion

SIDLER Information Security

IT-Sicherheit und Informationssicherheit

Eine technische Massnahme muss immer mit einer organisatorischen Massnahme kombiniert werden!



Sicherheitspolitik

Sicherheitsprozesse

Sicherheitsmanagement

Firewalls / Virenschutz

IS-Risikomanagement

VPN-Zugang

Sicherheitsrichtlinien
& -standards

Verschlüsselung

Security-Awareness

Security-Audits

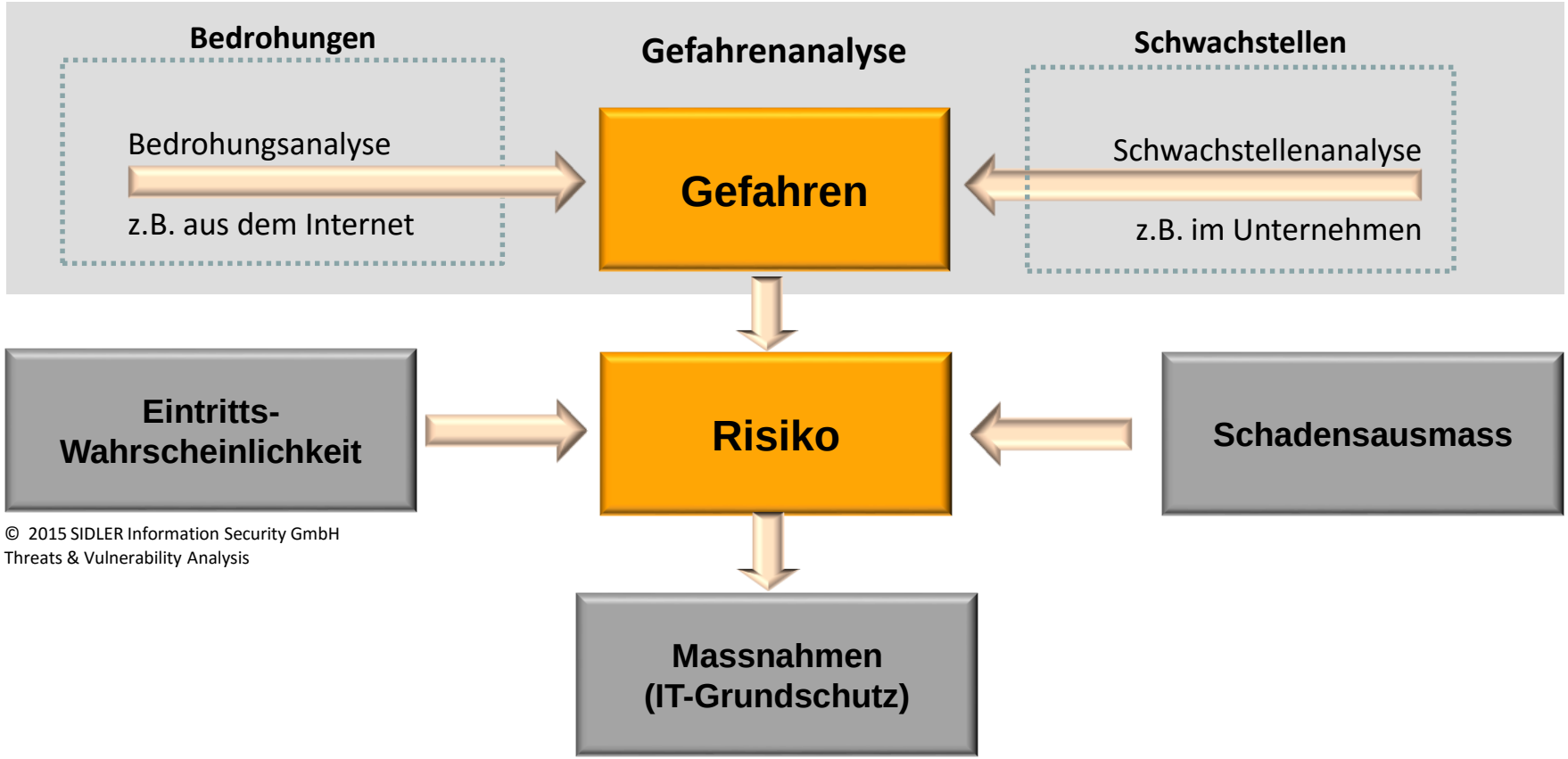
Sicherheit

ist nur 20% Technologie!!!

SIDLER
Information Security

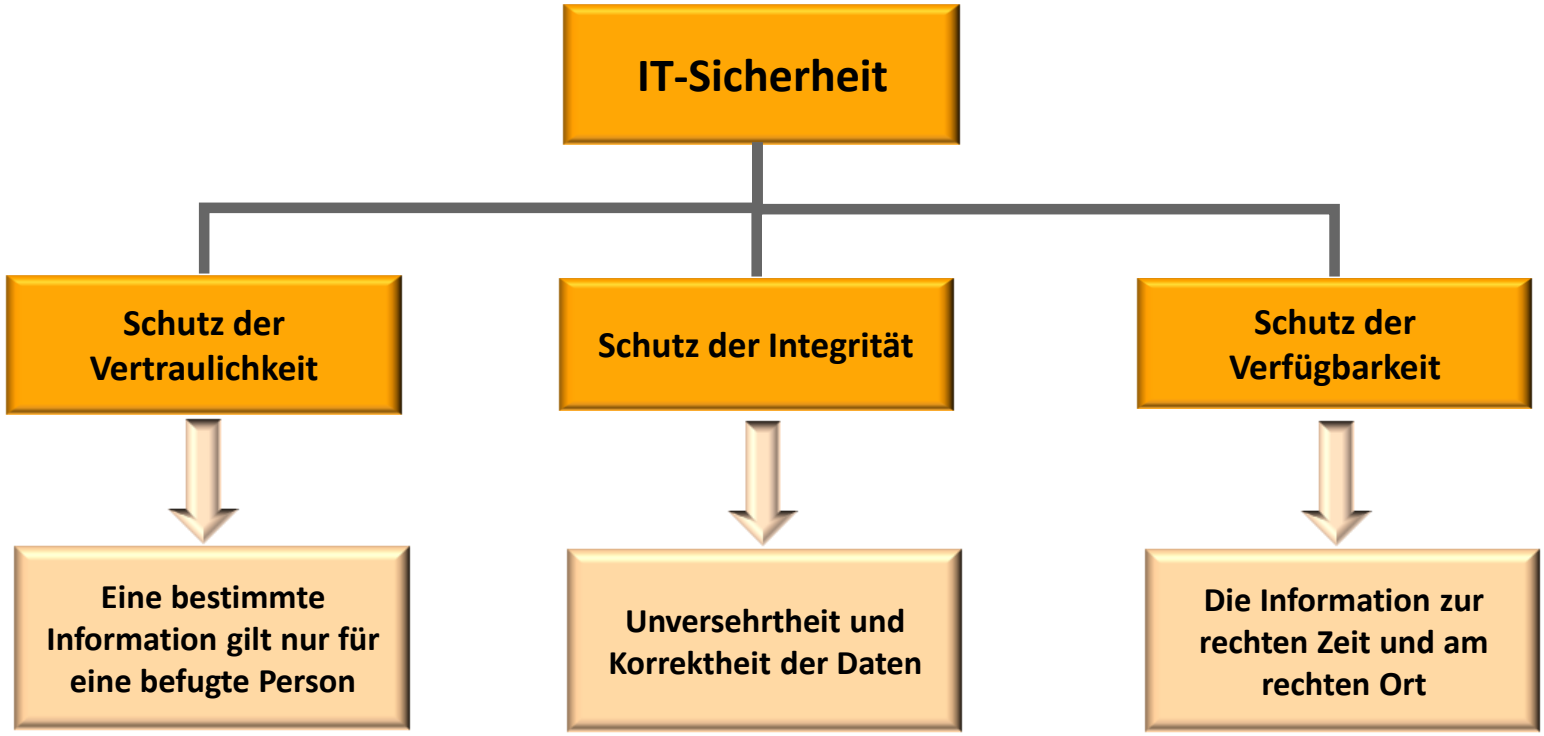
Wie entsteht ein Risiko?

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



SIDLER Information Security

3 Pfeiler der IT-Sicherheit



« Sie haben durchschnittlich 243 Tage lang Eindringlinge in ihrem Unternehmen, bis es jemandem auffällt. »

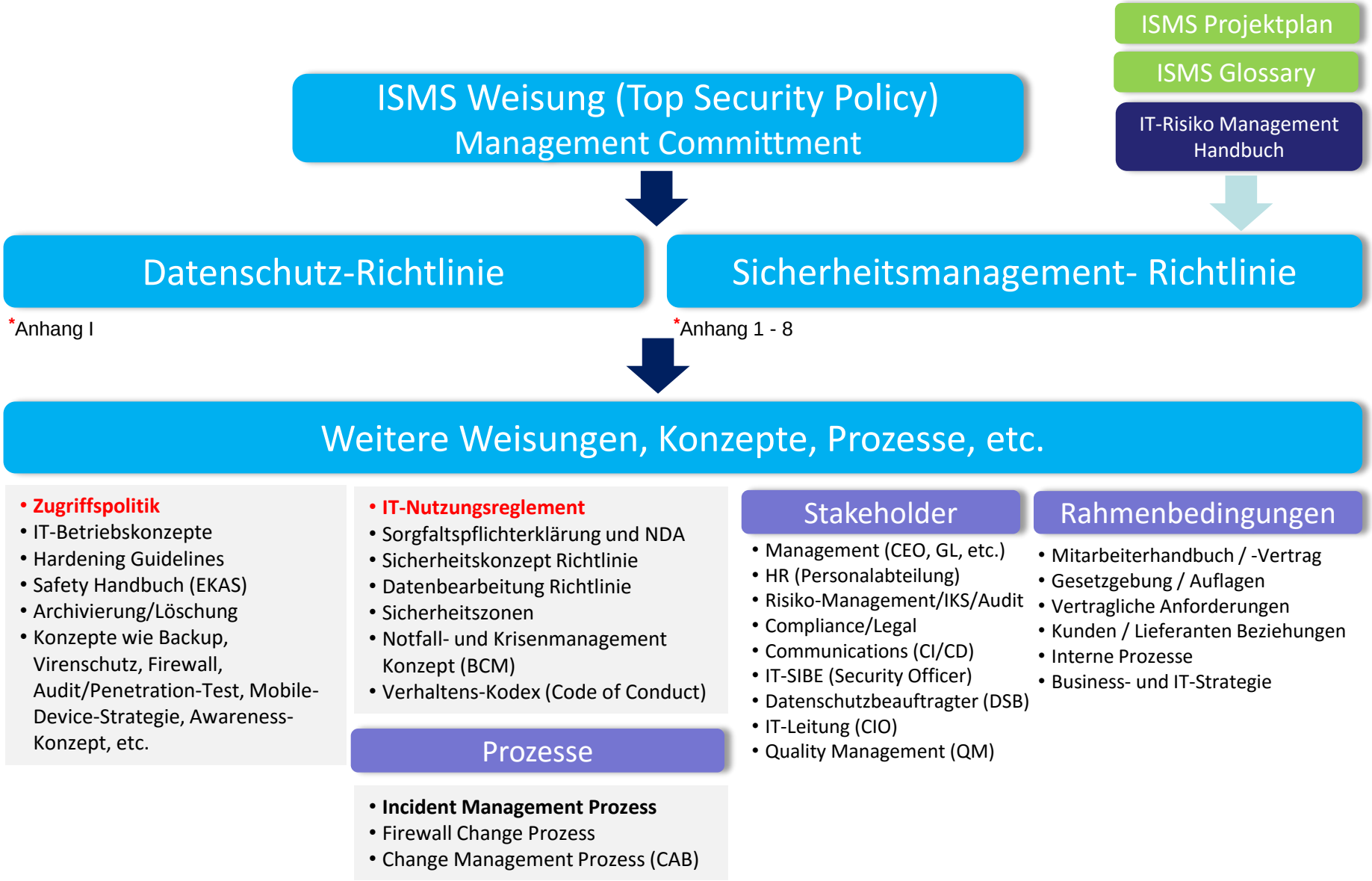
Microsoft-Sicherheitschef Paul Nicholas

SIDLER
Information Security

Ziele der Informationssicherheit - Ihr Nutzen

- Geringere Verwundbarkeit
- Keine falsche Sicherheit
- Bewusster Umgang mit Informationen und Daten
- Gefahren kennen, Restrisiko ist bekannt
- Sorgfaltspflicht erfüllt
- Bessere Kreditwürdigkeit (Basel II und III, gilt nur Finanz-Institute)
- Sie erhalten positive Audits (interne und externe Revision)
- Erhöhtes Kundenvertrauen (z.B. mit einer ISO 27001 Zertifizierung)
- Einhalten aller Gesetze (IKS, Datenschutz, GebüV, FINMA, etc.) → gute Compliance
- Wettbewerbsvorteil → Sicherheit schafft Vertrauen
- Reduziert das Risiko einer Geschäftsunterbrechung erheblich (hohe Verfügbarkeit)
- Fördert das „Sicherheitsbewusstsein“ der Mitarbeiter (Sicherheitskultur)
- Steigert die Möglichkeit neue Geschäfts-Felder sicher und schneller anzugehen

Weisungs-Framework



SIDLER Information Security

Inhalt einer IT-Nutzungsweisung

Inhaltsverzeichnis

SIDLER
Information Security

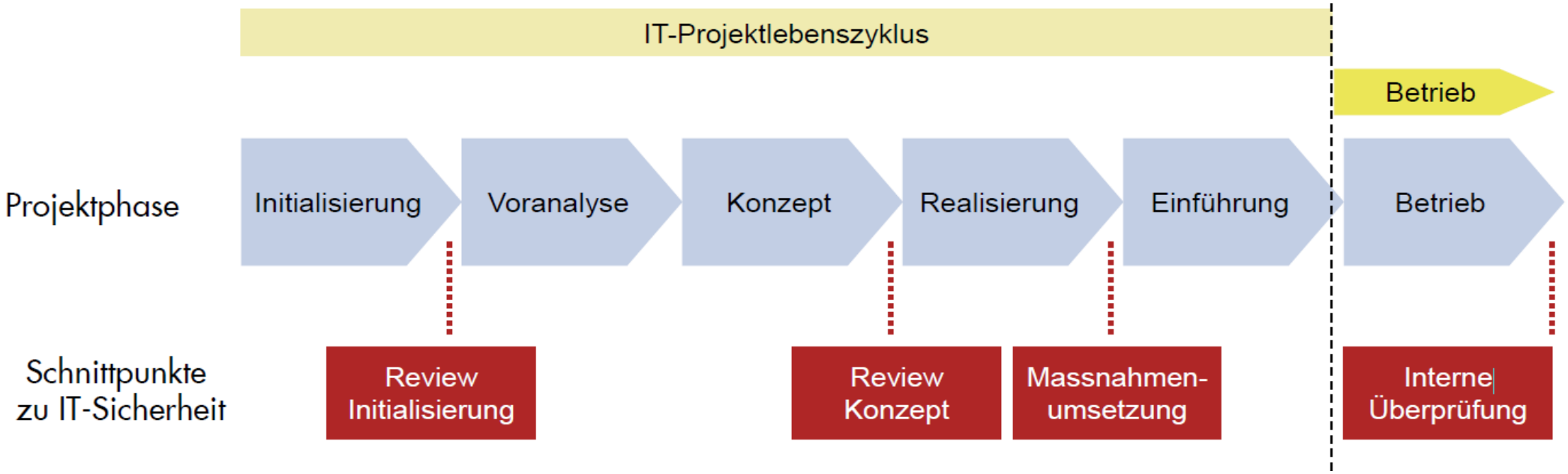
Wie anpacken?

- Kommittent vom Management (Ressourcen zur Verfügung stellen) → Top-Down Approach
- Informationssicherheitsstrategie (Awareness, Weisungen, Konzepte, etc.) erstellen
- Rollen und Verantwortlichkeiten festlegen
- IT-Risiko Analyse durchführen (Risiko-basierter Ansatz)
- Sich immer verbessern (Audits und Pen-Tests durchführen)
- Allumfassende Sicht (integraler Ansatz)
- IT-Sicherheit in den IT-Projekten von Beginn an miteinbeziehen
- Besser 5 umgesetzte als 20 geplante Sicherheitsmassnahmen (80/20 Regel)
- Denken Sie in Szenarien (Welche Bedrohungen bzw. Risiken betreffen mein Unternehmen?)

Sind Ihre Sicherheitsmassnahmen effektiv?

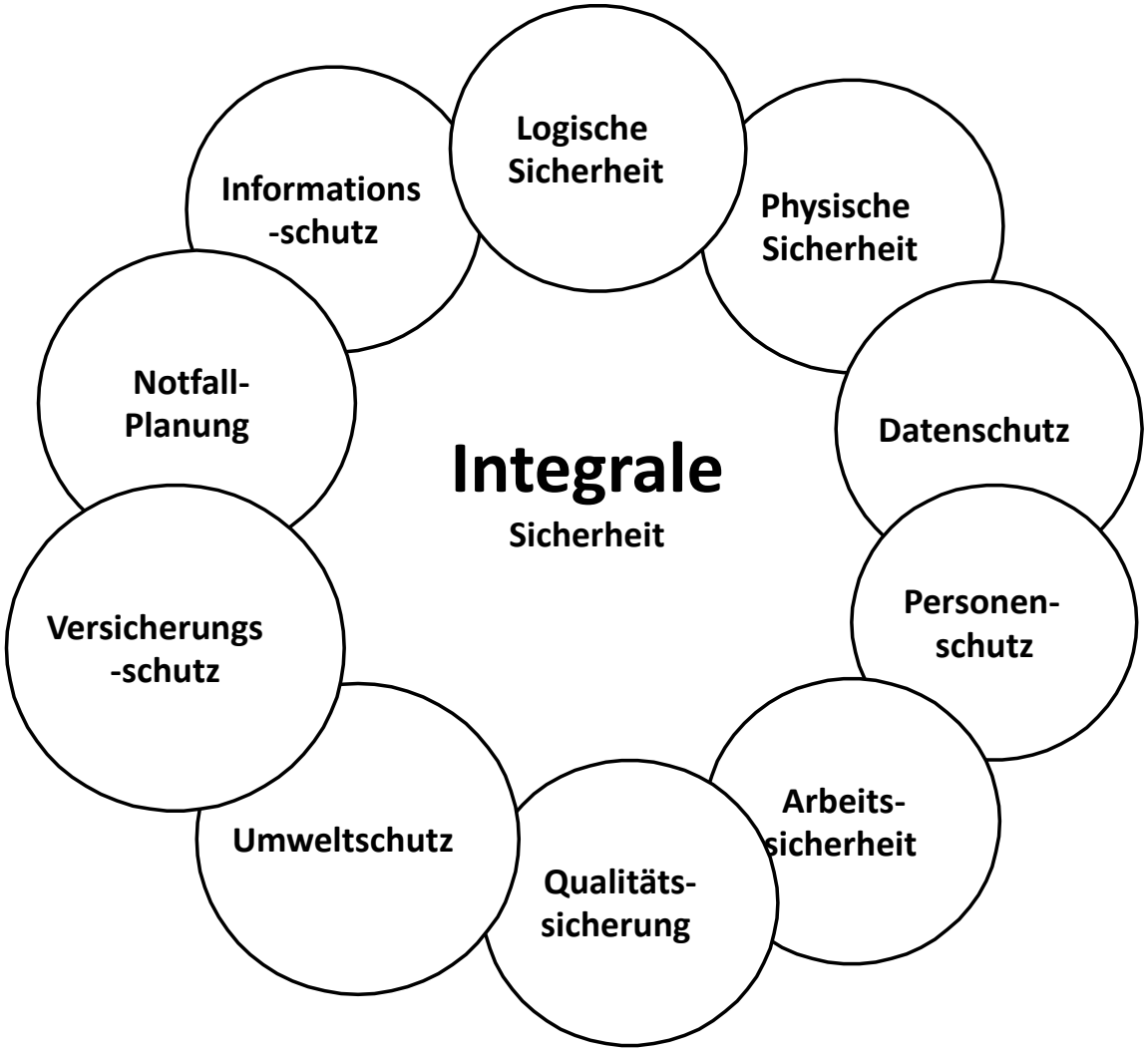
SIDLER
Information Security

IT-Sicherheit im Projektzyklus



Ziel: Einhaltung des IT-Grundschutzes

Integrale Sicherheit - Zusammenspiel



SIDLER Information Security

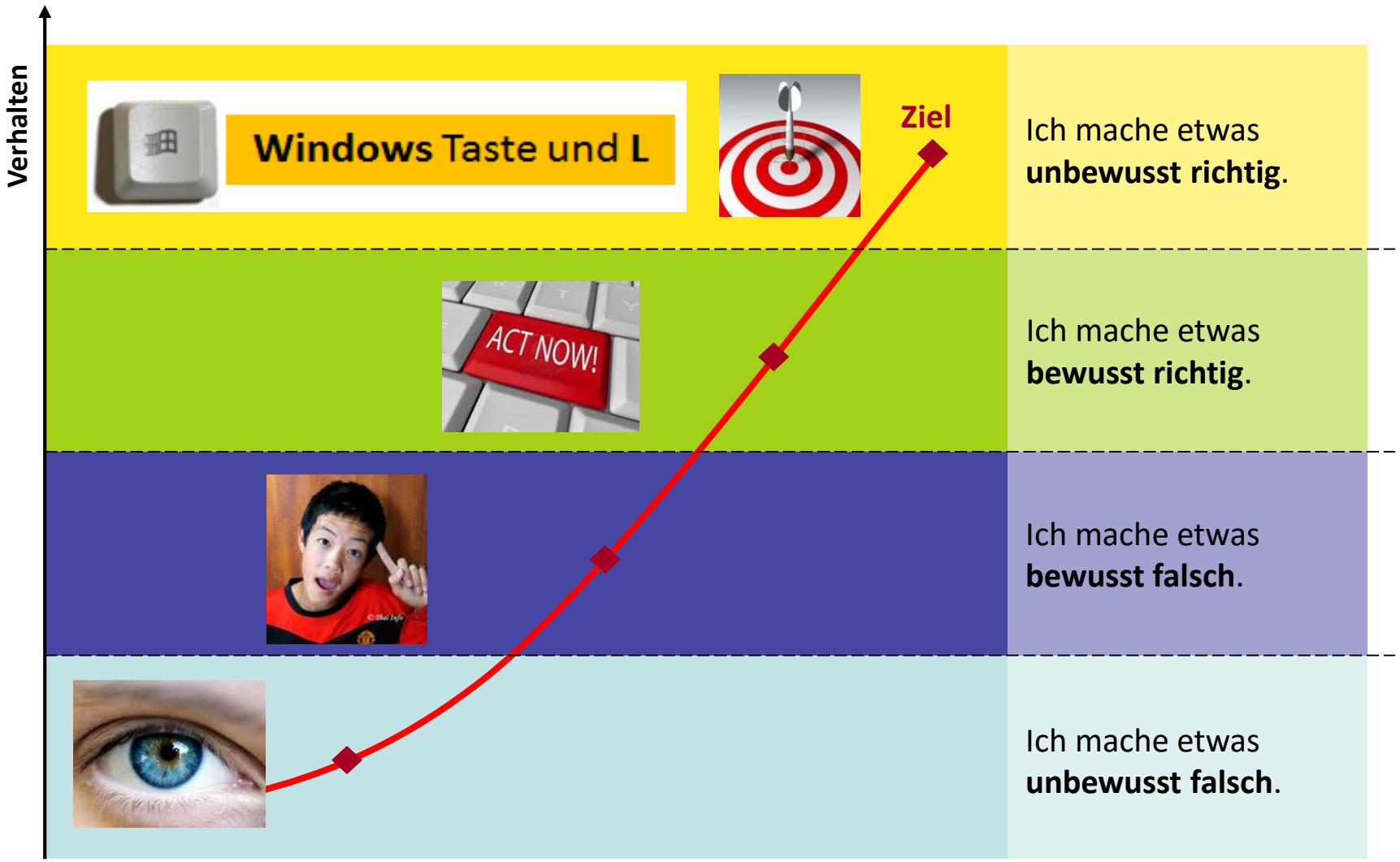
Ahnungslos? Sweet Deal!

Wie viele Personen hätten Ihr geheimes Passwort für ein Stück Schokolade bekanntgegeben?

More than 70% of people would reveal their computer password in exchange for a bar of chocolate, a survey has found.

Quelle: http://news.bbc.co.uk/1/hi/technology/3639679.stm

Entwicklungsstufen der Sicherheitskultur



SIDLER Information Security

So einfach sollten Sie es dem Angreifer nicht machen!

Live getestet am 20. Juli 2013 im Kanton Luzern - Hotel «geheim» - und es funktioniert! **War kein Swiss Deluxe Hotel** ☺

Doch leider wird oft schon beim Einbau geschlampt – wie wir schon in mehr als diesem einen Fall selbst feststellen mussten. Viele Hotels vergessen einfach, den vom Hersteller vorgegebenen **Mastercode (00000)** zu ändern.

Fragen?

SIDLER Information Security