Schweizer
Kader
Organisation

Das Kompetenzzentrum für Führungskräfte

SIDLER
Information Security
www.sidler-security.ch

Swiss Made
Information Security

**Nur Handeln bewegt die Welt, niemals Prinzipien.** *Wolfgang Sidler*

## vom Know-how zum Do-how

# Informationssicherheit und Datenschutz

**Wolfgang Sidler – 27. März 2019 - Zug**

# Wolfgang Sidler - Senior Security Consultant & CEO

## Ausbildung

Master of Advanced Studies HSLU in Information Security

Certificate of Advanced Studies HSLU in Blockchain

eidg. Wirtschaftsinformatiker mit FA

Certified ISO 27001 Lead Auditor

ITIL Foundation Certificate

Microsoft Certified Systems Engineer (MCSE)

## Berufserfahrung

34 Jahre Informatik-Erfahrung

19 Jahre Informationssicherheits-Erfahrung

6 Jahre IT-Security Officer bei der Privatbank Julius Bär in Zürich und New York

3 Jahre internationale Security-Beratung (2 Jahre New York, 1 Jahr für die Regierung in Oman)

1 Jahr European Security Consultancy Manager bei Zürich Financial Services

Mitautor
„IT-Sicherheitshandbuch für die Praxis“ www.sihb.ch

## Engagement

Stv. Datenschutzbeauftragter des Kantons Luzern von 2009 - 2018

Freier Dozent an der Uni Luzern für Rechtswissenschaften

Fachlicher Beirat MAS/CAS Information Security an der Hochschule Luzern – Wirtschaft (HSLU)

18 Jahre Prüfungsexperte für Informatik-Lehrlinge im Kanton Luzern von 1999 - 2017

Mitbegründer der ERFA IT-Sicherheit Zentralschweiz

Co-Organisator Lucerne Law & IT Summit (LITS) der Universität Luzern (seit 2017)


**IT-Sicherheitshandbuch für die Praxis**
ISBN: 3-9521208-3-9 www.sihb.ch

**Kontakt**

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

Swiss Made Information Security

SIDLER Information Security

# Was ist IT-Sicherheit eigentlich?

## 1. Schutz der Vertraulichkeit

- Eine bestimmte Information gilt nur für eine befugte Person oder Personen
- Vertraulichkeitsvereinbarung (NDA), Berufsgeheimnis, Postgeheimnis, etc
- Datenschutz (DSGVO/GDPR)

## 2. Schutz der Integrität

- Unversehrtheit und Korrektheit der Daten und Informationen
- korrekte Funktionsweise von Systemen und Software
- Das Erkennen von Modifikationen

## 3. Schutz der Verfügbarkeit

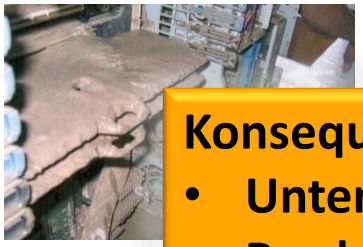
- Die Information zur rechten Zeit und am rechten Ort
- Die Verfügbarkeit wird in SLAs geregelt. Also vertragliche Abmachung zur Verfügbakreit von Systemen und Anwendungen.

Swiss Made Information Security

SIDLER Information Security

# Gefahren und Risiken - Konsequenzen



**Höhere Gewalt**
Feuer, Blitz, Sturm, Überschwemmung, Stromausfall, Krankheit, …

**Konsequenzen:**
- **Unterbruch der Geschäftsprozesse**
- **Produktions-Ausfall, Auslieferungs-Verzug**
- **Projekt-Verzögerung**
- **Verlust von vertraulichen Daten oder Know-how**
- **Bussen (juristische Konsequenzen)**
- **Verstoss gegen vertragliche Geheimhaltungsvorschriften**
- **Image Schaden**
- **Wiederherstellungskosten**

Zutrittskontrollen, falsche Zugriffsrechte, Abgang von Schlüsselpersonen (Know-how-Verlust), Versagen der Prozesse, …

**Vorsätzliche Handlungen**
Manipulation, Diebstahl, Missbrauch, Sabotage, Spionage, Hacking, Erpressung, Viren, organisierte Kriminalität, ...

Swiss Made Information Security

SIDLER Information Security

# Aktuelle Top-Risiken

Die folgenden Top-Risiken wurden aktuell 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) → Phishing** | **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: 6'924 Unternehmen in Deutschland wurden im Auftrag von TÜV befragt. 10.9% der Befragten Unternehmen waren Banken, Finanzdienstleistungen und Versicherungen.

Swiss Made Information Security

SIDLER Information Security

# 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".

**In Zürich wurden in einem halben Jahr 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

Tweet

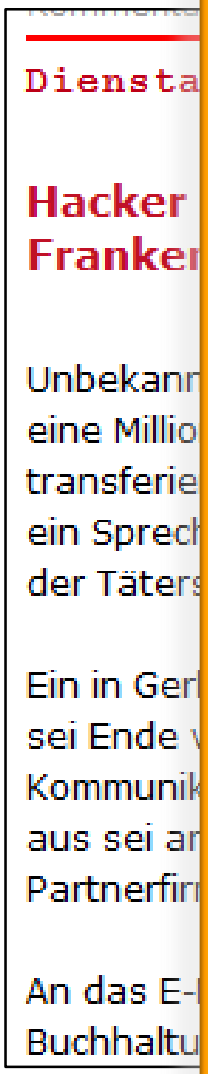
Taschen, Koffer, Kleider und Elektrogeräte: Im Keller des Fundsachenverkauf.ch in Zürich stapelt sich die Ware auf Holzpaletten und in Kisten mit Aufschriften wie «Spielzeug», «Schmuck», «iPhone» oder «Erotik». Hier landet, was in der Schweiz in Zügen und Postautos sowie an Bahnhöfen und Flughäfen liegen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

Swiss Made Information Security

SIDLER Information Security

# Die CEO Phishing Falle!


Dienst

Hacker
Franke

Unbekann
eine Millio
transferie
ein Sprec
der Täter

Ein in Ger
sei Ende
Kommunik
aus sei ar
Partnerfir

An das E-
Buchhaltu

**Tipps**

- Es gibt kein Unternehmen, welches die Passwörter ihrer Kunden per E-Mail erfragt.
- Ignoriere E-Mail-Aufforderungen Dein Passwort zu ändern.
- Öffne bei **«verdächtigen»** E-Mails nie ein angehängtes Dokument oder Programm und klicke auf keine darin angegebenen Links.
- Gib keine Kundendaten oder Personendaten unberechtigten Dritten Personen bekannt.
- Benutzernamen und Passwörter sind **vertraulich, persönlich und nicht übertragbar.**
- Notiere Deine Passwörter niemals auf einen Zettel, die in der Umgebung Deines Arbeitsplatzes kleben.
- Verwende für Deine Arbeit und Privat unterschiedliche Passwörter.
- Bei einer Geld-Transaktion immer telefonisch zurückfragen und sich über die Transaktion informieren.

**Gute Security-Seiten: www.ebas.ch und www.melani.admin.ch**

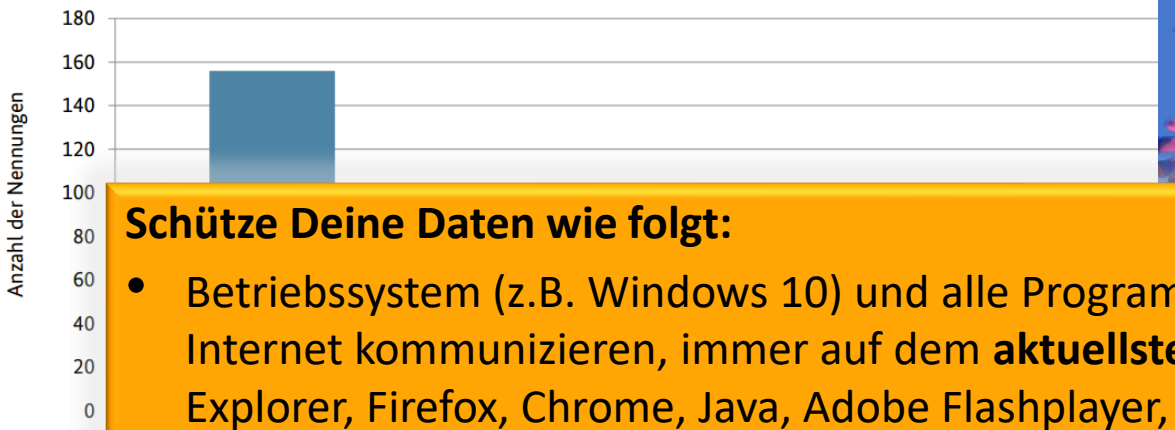
**Hier könnt Ihr prüfen, ob Euer Passwort schon gehackt wurde:**
**https://haveibeenpwned.com/Passwords**

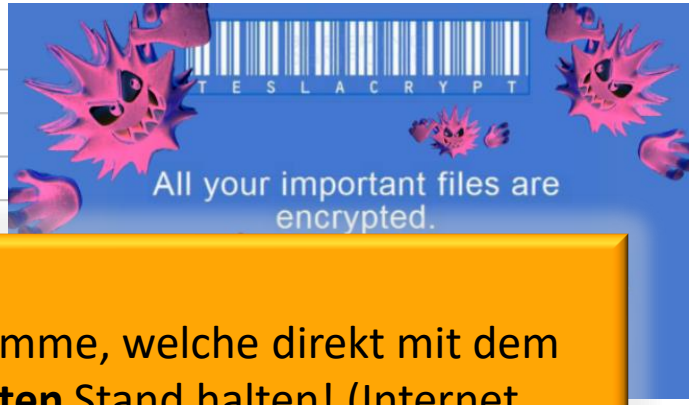
Swiss Made Information Security

SIDLER Information Security

# Verschlüsselungs-Trojaner




**Schütze Deine Daten wie folgt:**

- Betriebssystem (z.B. Windows 10) und alle Programme, welche direkt mit dem Internet kommunizieren, immer auf dem **aktuellsten** Stand halten! (Internet Explorer, Firefox, Chrome, Java, Adobe Flashplayer, Adobe Reader, etc.)
- Einen guten **Echtzeit-Virenschutz und zusätzlich z.B. Malwarebytes**
- Gesunder Menschenverstand und etwas Misstrauen an den Tag legen
- Ein regelmässiges **Backup** Deiner Daten auf eine externe USB-Disk oder –Stick (z.B. wöchentlich) und **offline** aufbewahren! Und eine Online-Sicherung Deiner Firmen-Daten direkt vom Server z.B. in einen Bunker in den Schweizer-Bergen (z.B. Mount 10)

Die
256
Re
ver
Ge
ver

Swiss Made Information Security

SIDLER Information Security

# Weisungs-Paket für KMU

Die folgenden Weisungen bieten Ihnen einen Basis-Compliance Grundschutz:

- Leitlinie zur Informationssicherheit und Datenschutz (DSGVO)
- IT-Nutzungsweisung für alle Mitarbeitenden inkl. Anhang Mobile Datenträger
- Security Awareness Flyer
- Etc.


Ziel ist, dass Sie Ihre **Verantwortung** zum Thema Informationssicherheit & Datenschutz dokumentieren und die Weisungen durchsetzen.

Swiss Made
Information Security

SIDLER
Information Security

# Inhalt einer IT-Nutzungsweisung

**Inha**



### E-Mails und Anhänge

**Viren** und sonstige bösartige Software werden am häufigsten verbreitet über
- E-Mails (verseuchte Anhänge)
- USB-Sticks
- Internet-Webseiten

**Phishing** ist eine Methode von Betrügern, um sich Informationen von ihren Opfern zu beschaffen, die zur persönlichen Bereicherung eingesetzt werden können. Phishing-Angriffe erfolgen oft via E-Mails, in denen Benutzer mit möglichst glaubhaften Geschichten dazu gebracht werden sollen, dem Absender vertraulichen Informationen auszuhändigen.

*Das Wichtigste in Kürze:*

- ☐ Misstrauen Sie E-Mails, deren Absender Sie nicht kennen oder deren Inhalt Ihnen verdächtig vorkommt.
- ☐ Fahren Sie mit dem Mauszeiger über die Internet-Adresse in der E-Mail, **ohne** zu klicken; so sehen Sie, auf welche Website der Link führt.
- ☐ Öffnen Sie bei verdächtigen E-Mails nie ein angehängtes Dokument oder Programm und wählen Sie keine darin angegebenen Links.
- ☐ Öffnen Sie keine Anhänge, die zwei Endungen aufweisen (z. B. foto.jpg.vbs).
- ☐ Seriöse Unternehmen fragen nie per E-Mail nach persönlichen Daten.
- ☐ Ignorieren Sie E-Mail-Aufforderungen, Ihr Passwort zu ändern.

### Sorgfaltspflicht

Ihr Arbeitgeber stellt Ihnen einen gut eingerichteten Arbeitsplatz zur Verfügung, der Ihnen die tägliche Arbeit erleichtern soll. Bitte behandeln Sie die Geräte sorgfältig und mit dem nötigen Respekt.

Bearbeiten Sie Daten, so sind Sie in Ihrem Bereich für die Einhaltung von Datenschutz und Datensicherheit verantwortlich.

Fragen Sie den Technischen Leiter, bevor Sie eine Aktion starten, bei der Sie sich über den Ausgang nicht sicher sind.

### Informationen und Kontakt

*Bei Fragen:*
Wenden Sie sich an den Technischen Leiter.

*Für allgemeine Informatikfragen und für die Meldung von verdächtigen Vorfällen:*
Wenden Sie sich an den Technischen Leiter
[redacted]

*Informationen:*
Aktuelle Informationen zum Thema Datenschutz und Informatiksicherheit finden Sie in der IT-Nutzungsweisung.

*Gesetzliche Grundlage:*
Schweizerisches Datenschutzgesetz (DSG)

### Informationssicherheit bei [redacted]

*Merkblatt für den Alltag*
*und weiterführende Hinweise*


**Liebe Mitarbeiterinnen, liebe Mitarbeiter**

Der Einsatz von PC, Notebook und anderen Informations- und Kommunikationsmitteln ist für uns alle eine selbstverständliche Notwendigkeit, die aber auch Risiken birgt.

Ihr Sicherheitsbewusstsein und Ihr verantwortungsvolles Verhalten ist die wichtigste Grundlage, dass diese Risiken nicht eintreten.

Dieser Flyer soll Ihnen helfen, die Risiken zu erkennen und sich richtig zu verhalten.

***Ihr Technischer Leiter***[redacted]
Oktober 2017

Swiss Made
Information Security

SIDLER
Information Security

# EU-Datenschutz-Grundverordnung

Jedes Unternehmen, das personenbezogene Daten von in einem EU-Mitgliedstaat wohnhaften Bürgern speichert oder verarbeitet, muss die DSGVO einhalten, auch wenn es keinen eigenen Sitz in der EU hat. Unternehmen, die eines oder mehrere der folgenden Kriterien erfüllen, müssen die Verordnung einhalten:

- ein Sitz in einem Mitgliedstaat der EU
- kein Sitz in einem Mitgliedstaat der EU, aber Verarbeitung personenbezogener Daten von in der EU wohnhaften Bürgern

Wenn also Ihr Unternehmen in der EU tätig ist oder Mitarbeiter oder Kunden aus der EU hat, müssen Sie ab dem **25. Mai 2018** die DSGVO einhalten.

**Die alte Welt**

- EU-Datenschutz vor der digitalen Welt (veraltet)
- Keine Audits und nur wenige Untersuchungen
- Wurde nicht konsequent in Europa umgesetzt
- Kleine Bussen, wenn überhaupt!

**Die neue Welt - keine Änderungen in Bezug auf den IT-Grundschutz, aber:**

- Bussen bis 4% des globalen Unternehmens-Umsatz
- EU Bürger haben neu viel mehr Rechte
- Nachweispflicht der Umsetzung (Compliance)

DSGVO = Datenschutz-Grundverordnung
GDPR = EU General Data Protection Regulation

Swiss Made Information Security

SIDLER Information Security