



## Schutz von Identitäten und Zugangsberechtigungen

Argomed eHealth Forum 2019

Pius Graf, Director Sales, Thales, Schweiz

**THALES**

**gemalto**  
a Thales company

# Agenda

- ✦ Identitäten und Daten
- ✦ Organisatorische und technische Massnahmen

**Identitäten und Daten müssen  
geschützt werden**

## Nicht alle Leute finden alle Lösungen gut



"On the Internet, nobody knows you're a dog." Updated for a Post-Snowden world  
by [drewSaysGoVeg](#) Aug 14 2015



Es ist (nur) eine Bit Sequenz



# Clouds Over IT

Februar 2019 gestohlene Accounts/ Identitäten

8fit (20 million)

500px (15 million)

Animoto (25 million)

Armor Games (11 million)

Artsy (1 million)

BookMate (8 million)

CoffeeMeetsBagel (6 million)

DataCamp (700,000)

Dubsmash (162 million)

EyeEm (22 million)

Fotolog (16 million)

HauteLook (28 million)

MyFitnessPal (151 million)

MyHeritage (92 million)

ShareThis (41 million)

Whitepages (18 million)



## Zwei wesentliche Faktoren bei Cyber Angriffen

Hauptangriffsziel

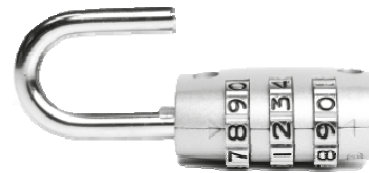
### Identitätsdiebstahl

**69%** der Angriffe  
zielen auf die  
Identität der  
Personen



Hauptgrund für Schäden

### Unverschlüsselte Daten



**95%** der Angriffe  
stehlen  
unverschlüsselte Daten

Eigentlich wissen wir es Alle - handeln wir entsprechend!

## Nächster Schritt: Sabotage kritischer Infrastruktur





## Wie kommen die Angreifer rein?

- ✦ Über 90% der Malware kommt über Email rein
- ✦ Phishing / Spear phishing
  - ✦ 15%-30% aller Phishing Emails werden geöffnet. Auch bei uns in der Firma!
- ✦ Bis zu 10% der User geben (unabsichtlich) ihre Zugangsinformation weiter (UserID & Password)

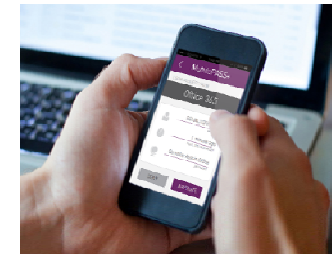
## Ich habe (zu) viele Anmeldungen...

- ✦ Power On Password (1)
- ✦ Disk Encryption (1)
- ✦ Windows Logon (1)
- ✦ Intranet Logon (1)
  - ✦ Email (1)
  - ✦ Reisekosten (1)
  - ✦ Personaldaten (1)
  - ✦ Interne Applikationen (3)
- ✦ Virtual Machine Logon (1)
- ✦ Internet via Browser
  - ✦ Website logon (5)
- ✦ Cloud services
  - ✦ Office 365 (1) , Sharepoint (1) , Business Anwendungen (5)

23 Anmeldungen

## Anmelden mit 2 Faktoren

- ✧ Unterschied **Authentisierung** und **Authorisierung**.
- ✧ Authentisieren mit 2 Faktoren (Besitz und Wissen).
- ✧ Benutzerfreundlichkeit durch Einmal-Anmeldung und Weiterleitung (Single Sign On).
- ✧ Der Benutzer soll so wenige Passwörter wie möglich wissen, oder nachschauen müssen.
- ✧ Benutzerkomfort mit gleichzeitig hoher Sicherheit



## Organisatorische und technische Massnahmen

## Mit wenig Aufwand möglichst viel erreichen

- ✧ Regeln Sie Aufgaben, Kompetenzen und Verantwortlichkeiten und setzen Sie damit den Grundstein für Ihren Cybersecurity Minimal-Schutz.
- ✧ Nutzen Sie die vorhanden Hilfsmittel welche vom Bund und den ICT Verbänden speziell für KMU's entwickelt wurden.
- ✧ Machen Sie Cybersecurity zum Thema mit Ihren Mitarbeitern. Events organisieren. Gemeinsam Awareness erhöhen - Videos schauen, über Mittag, vor einem Apéro, Wettbewerbe ...



## Hilfsmittel für Ihre ICT Strategie

- ✧ **Melani: Melde- und Analysestelle** Informationssicherung gibt das Merkblatt Informationssicherheit für KMUs heraus.
- ✧ **ICT Switzerland:** Hinweise und Informationen für einen minimalen Cybersecurity-Schutz.


# Melanie: Informationssicherheit für KMUs

- ✧ Merkblatt ist unterteilt in zwei Massnahmen-Bereiche:

**Organisatorische**

Technische

- ✧ Verantwortlichkeiten bezüglich IT, insbesondere der IT-Sicherheit, sind geregelt.
- ✧ Die Zuständigkeiten bezüglich IT-Sicherheit zwischen Ihrem Unternehmen und Ihrem IT-Dienstleister sind klar geregelt.
- ✧ Regelmässige Schulung der Mitarbeitenden im Umgang mit der IT-Infrastruktur hinsichtlich der IT-Sicherheit.
- ✧ Umgang mit sensiblen Daten
- ✧ Passwort-Policy

 Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun Svizra

Edgewardische Finanzdepartement EPD  
Informationskennungsgesamt Bund ISB  
Melde- und Analysestelle Informationssicherung MELANI

---

## Merkblatt Informationssicherheit für KMUs

MELANI

---

Version:	v2.0
Autor:	MELANI
Zuletzt aktualisiert:	25. Mai 2018



# ICT Switzerland: Minimaler Cybersecurity-Schutz

1. Aufgaben, Kompetenzen, Verantwortlichkeiten.
2. Sensibilisierung von Mitarbeitenden, Kundinnen und Kunden, Lieferanten und Dienstleistern.
3. Datenschutz-Richtlinien.
4. Passwort-Richtlinien und Benutzeradministration
  - ✦ Schwache und/oder mehrfach verwendete Passwörter.
  - ✦ Zugangs- und Administratorenrechte für jeden Dienst mit einem anderen Passwort nutzen.
  - ✦ Verwenden Sie einen Passwortmanager.
  - ✦ Nutzen Sie wo möglich Zwei-Faktor-Authentifizierung, vor allem wenn es um Geld geht.
  - ✦ Regeln Sie den Zugriff auf Daten durch eine übergeordnete Benutzeradministration. Löschen Sie diese beim Austritt von Mitarbeitenden aus dem Unternehmen.

## ISSS

Starke Passwörter verwenden

[Informationssicherheit für KMU, Punkt 6](#)

Zugriffsschutz auf Daten regeln

[Informationssicherheit für KMU, Punkt 12](#)

## MELANI

Wie schütze ich mich?

Verhaltensregeln

[Portal MELANI](#)

## Passwortcheck

So testen Sie die Stärke Ihrer Passwörter

[Portal Passwortcheck.ch](#)

## Alle Mitarbeiter sind im Fokus

- ✦ Es betrifft Alle, Vorgesetzte, Mitarbeiter, Dritte.
- ✦ Bedienung der Programme sollen einfach und Anmeldungen unkompliziert und schnell sein.
- ✦ Die Passwörter und der Schutz der Identität sind zentral.
- ✦ Email Risiken thematisieren.
- ✦ Fremde Datenträger sind ein grosses Risiko.
- ✦ Vermischung von Geschäft und Privat (BYOx).
- ✦ Browser Einstellungen und Handhabung beachten.

**Checktools, Hilfsmittel, Ideen.**



# Cybersecurity Schnelltest für KMU



[www.cybersecurity-check.ch](http://www.cybersecurity-check.ch)

# Passwordcheck

Das zu prüfende Passwort lautet:  ☐ Passwort anzeigen

Das eingegebene Passwort wird lokal überprüft und nie an den Server übermittelt.

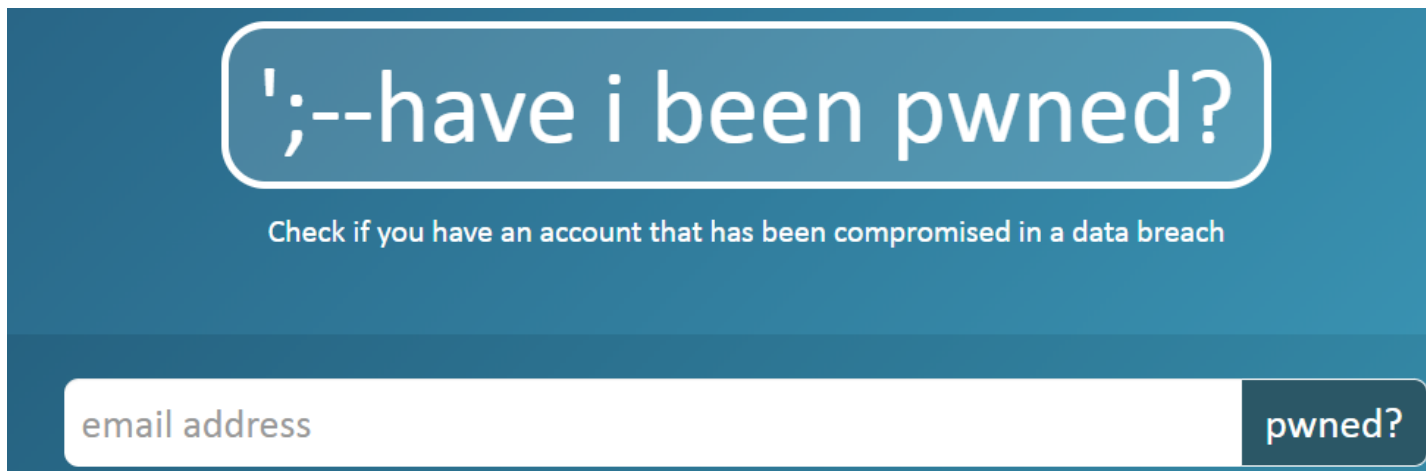
Ausgewählte Wörterbücher

☒ Deutsch ☐ Französisch ☐ Italienisch  
☐ Rätoromanisch ☐ Englisch

Kriterium	Messung	Punkte
Länge des Passworts (0)	5 Punkte pro Zeichen	0
0 Zeichen im Wörterbuch gefunden	-2 Punkte pro Zeichen	0
Bewertung der übrigen Zeichen, welche nicht in der Wörterliste vorkommen.		
Kleinbuchstaben	15 Punkte, falls Kleinbuchstaben vorhanden	0
Grossbuchstaben	15 Punkte, falls Grossbuchstaben vorhanden	0
Zahlen	10 Punkte, falls Zahlen vorhanden	0
Sonderzeichen	10 Punkte, falls Sonderzeichen vorhanden	0
Total Punkte		0

- Wie länger umso besser.
- Passwortmanager verwenden.
- Passwörter stehlen (Phishing, Malware) ist einfacher als ausprobieren (brute force).
- 2-Faktor Authentisierung. Zwingend bei Finanz-Anwendungen.





';--have i been pwned?

Check if you have an account that has been compromised in a data breach

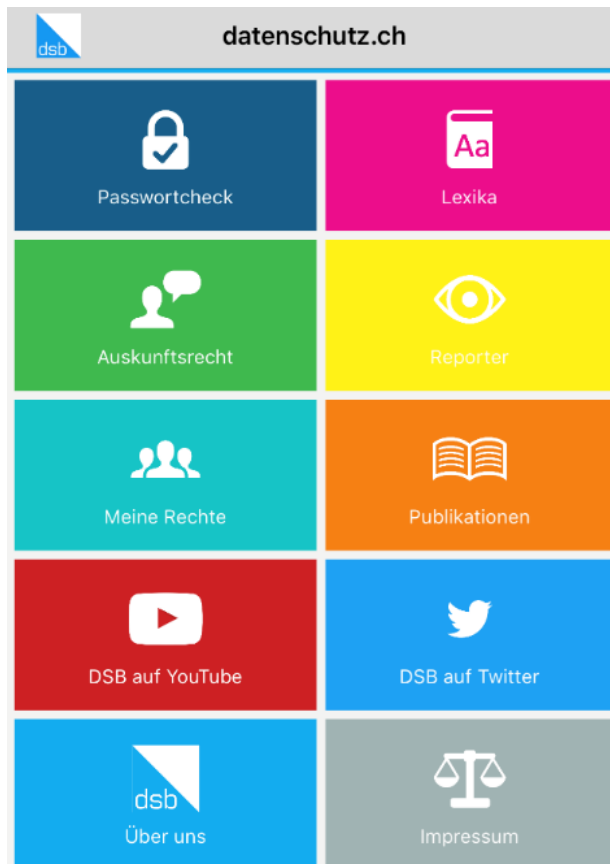
email address pwned?

Ob Ihre E-Mail-Adresse oder Ihr Benutzername gehackt worden ist, können Sie mit verschiedenen online Checktools überprüfen:

- <https://haveibeenpwned.com/> (Betreiber: Sicherheitsforscher Troy Hunt, enthält Datensätze aus verschiedenen Hackerangriffen inkl. «Collection #1-5»)
- <https://sec.hpi.uni-potsdam.de/ilc> (Betreiberin: Hasso-Plattner-Institut, enthält Datensätze aus verschiedenen Hackerangriffen)
- <https://www.checktool.ch> (Betreiberin: MELANI, enthält Datensätze aus verschiedenen MELANI gemeldeten Hackerangriffen)
- Sollte Ihre E-Mail-Adresse in einem der Dienste gelistet sein, empfehlen wir umgehend das entsprechende Passwort zu ändern und wo immer möglich die Zwei-Faktor Authentisierung zu aktivieren.

Quelle: [www.melani.admin.ch](http://www.melani.admin.ch)

# App des DSB Kanton Zürich



- Wettbewerb mit Mitarbeitern machen.
- Begeistern für Datenschutz.

Quelle: DSB Zürich

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

Kontakt Daten:

Pius Graf

Thales, Cloud Protection & Licensing

Hintere Bahnhofstrasse 12, 5001 Aarau

Pius.Graf@thalesgroup.com