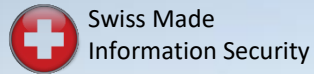


# Firmenpräsentation

[www.sidler-security.ch](http://www.sidler-security.ch)



**SIDLER**  
Information Security



**Nur Handeln bewegt die Welt, niemals**

**Prinzipien.** *Wolfgang Sidler*



**vom Know-how zum Do-how**

**Datenschutz- und Informationssicherheits-Beratung**

# Wolfgang Sidler - Senior Security Consultant & CEO



- Master of Advanced Studies HSLU in **Information Security** und Certificate of Advanced Studies HSLU in **Blockchain**
- **20 Jahre** Informationssicherheits-Erfahrung
- **10 Jahre** Stv. Datenschutzbeauftragter des Kantons Luzern von 2009 - 2018
- **6 Jahre** IT-Security Officer bei der Privatbank Julius Bär in Zürich und New York
- **3 Jahre** internationale Security-Beratung (USA und Oman)

## Mitautor

IT-Sicherheitshandbuch für die Praxis

ISBN: 3-9521208-3-9 [www.sihb.ch](http://www.sihb.ch)

## Kontakt

[www.sidler-security.ch](http://www.sidler-security.ch)

[wolfgang.sidler@sidler-security.ch](mailto:wolfgang.sidler@sidler-security.ch)



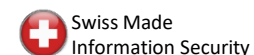
SWISS  
BUSINESS  
PROTECTION

## Wirtschaftsschutz-Schweiz

Member of the Board & Founding Partner

Swiss Business Protection AG

[www.swissbp.ch](http://www.swissbp.ch)



**SIDLER**  
Information Security

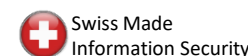
# Unsere Kernkompetenzen und Lösungen

## Beratung

- IT-Security Officer und Datenschutzbeauftragter (DPO) auf Zeit
- Aufbau eines Information Security Management System (ISMS) bis zur ISO 27001 Zertifizierung
- Informationssicherheit für Entscheidungsträger (Coaching)
- Datenschutz (GDPR/DSGVO) und Compliance Beratung
- Cyber-Security Assessment für KMU
- IT-Risiko Management für KMU
- Notfall- und Krisenmanagement (BCM)
- Sicherheits-Sensibilisierung

## Lösungen


- 2 Faktor Authentisierungs-Lösung für Notebooks mit Microsoft BitLocker
- Swiss Secure Mobile Communication (sicheres Telefonieren und Chatten mit iPhone & Android)
- Sichere Datenaustausch-Plattform Cloud-Lösung im Swiss Fort Knox



**SIDLER**  
Information Security

# Ihr Nutzen – Unser Know-how zum Do-how

- Geringere Verwundbarkeit
- Keine falsche Sicherheit
- Bewussterer Umgang mit Information
- Gefahren kennen, Restrisiko ist bekannt
- Sorgfaltspflicht erfüllt
- Bessere Kreditwürdigkeit
- Positive Audits (interne und externe Revision)
- Erhöhtes Kundenvertrauen (ISO 27001 Zertifizierung)
- Einhalten aller Gesetze (IKS, Datenschutz, GebüV, FINMA, Basel II/III etc.)
- Wettbewerbsvorteil -> Sicherheit = Vertrauen
- Reduziert das Risiko einer Geschäftsunterbrechung erheblich (hohe Verfügbarkeit)
- Fördert das „Sicherheitsbewusstsein“ der Mitarbeiter (Sicherheitskultur)
- Steigert die Möglichkeit neue Geschäftsfelder sicher und schneller anzugehen



***Wir sagen nicht,  
was ankommt,  
sondern worauf  
es ankommt!***

# Wie sieht es bei Ihnen aus?

- Wie schätzen Sie Ihre eigene IT-Sicherheit / Datenschutz ein?
- Wissen Sie, was Sie wie schützen müssen?
- Hatten Sie schon mal einen Sicherheitsvorfall?
- Haben Sie eine verantwortliche Person für die Informationssicherheit und den Datenschutz?
- Kennen Sie das Verhalten Ihrer Mitarbeitenden in Bezug auf die Informationssicherheit und den Datenschutz?
- Haben Sie Informationssicherheits- und Datenschutz-Weisungen in Ihrem Unternehmen?
- Haben Sie IT-Services ausgelagert? (Outsourcing oder Cloud-Services)
- Haben Sie vertragliche Informationssicherheits- oder Datenschutz-Auflagen von Kunden?
- Haben Sie einen Notfall- und ein Krisenmanagement-Plan?
- Speichern Sie Ihr Daten extern (Offline Backup)?

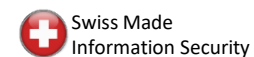
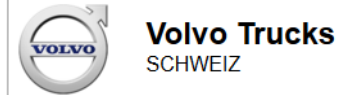


# Herausforderungen

- Cloud-Dienste, IoT Geräte, und Abhängigkeiten zu IT-Lieferanten und Schnittstellen
- Keine internen Weisungen und Sicherheitskonzepte
- Kein Notfall- und Krisenkonzept
- Hohe Komplexität – additive Probleme – neue Gesetze (DSG, DSGVO, etc.)
- Hohe Mobilität der Benutzer – Daten überall, zu jeder Zeit und auf jedem Endgerät
- Zuwenig Awareness, viel Halbwissen und Ignoranz
- Mehr und breiter motivierte/ausgerüstete Angreifer
- Mehr vernetzte Werte/höheres Schadenpotential
- Ressourcen-Mangel und Schnelligkeit des Wandels

- *Produkte lösen keine Management/Führungsprobleme*
- *Bevor Sie einen Cloud-Dienst verwenden, klären Sie wie «sicher» dieser Cloud-Service ist.*
- *Haben Sie immer einen Plan «B» und hinterfragen Sie neue Services und Produkte in Bezug auf die Informationssicherheit und den Datenschutz*

# Auszug Referenzen



# Unsere Success-Stories

Dienststelle Informatik  
informatik.lu.ch



Schutzbedarfsanalyse  
Kanton Luzern

PILATUS



IT-Security-Management-  
Handbuch und  
IT-Risiko Management

Landis  
Gyr+  
manage energy better



EAL4+ Common Criteria  
Zertifizierung  
Smart Metering



IT-Sicherheit im Swiss Fort Knox  
SIAG erlangt ISO 27001 Zertifizierung mit SIDLER Information Security GmbH

Die zwei grossen hochrechen Data Center (Data Fort Knox) in den Schweizer Bergen werden von der Firma SIAG betrieben. Der Betrieb und die Überwachung der physischen und logischen Infrastrukturen wird von zwei Security Operation Center (SOC) aus Norditalien (Der Hauptort der SIAG ist in Zug in der Schweiz, angliedert wurde SIAG im Jahr 2004)

SIAG ist der weltweit anerkannte Spezialist für Management und das zuverlässige und hochrechen Aufwachen und Ausbauen von digitalen Informationen über den gesamten Lebenszyklus hinweg. Erfahrung und professionell angelegte Security Operation Center die Kunden mit der Risiko-Identifizierung bis hin zur Erfassung und effektiven Risikominimierung.

Im Zentrum der Leistungserbringung der SIAG steht die Qualität, aber auch die effiziente und kostenreduzierende Gestaltung von IT-Sicherheitskonzepten. SIAG bietet anspruchsvolle Kunden in der ganzen Welt, SIAG-Lösungen und immer international anwendbar, existiert und auf die Bedürfnisse der Kunden massgeschneidert. Unsere Spezialisten überwachen dabei rund um die Uhr die physischen Strukturen von Standorten des Kunden bis in die parallel geführten hochrechen Swiss Fort Knox Data Center.

Für diese innovativen Sicherheitsanforderungen werden nur Technologien eingesetzt, welche die strengen Evaluationskriterien der SIAG bestmöglich erfüllen.

Die Informationssicherheit ist für die SIAG AG ein wichtiger Pfeiler. Diese orientiert fordern gesetzliche und regulatorische Anforderungen sowie führen Risiken durch Wirtschaftstätigkeit ein erhöhtes Sicherheitsniveau. Andererseits verlangen auch Kunden spezielle IT-Sicherheitsstandards. Diese Adressieren Technischer Leiter der SIAG AG und Swiss Fort Knox Rechenzentrum-Operatoren müssen sich die "ITC-Sicherheitsstandards" erfüllen um so unsere Verantwortung gegenüber unseren Kunden nachweisen zu können. Dadurch hat Sicherheit bei uns die höchste Priorität.

Intelligenter Aufbau und Zertifizierung eines Information Security Management Systems (ISMS) nach ISO 27001.

Die SIAG AG entschloss sich im Jahr 2018 ein ISMS einzuführen und zertifizieren zu lassen. Der Beginn war mit dem Rechenzentrumsleiter Eber, dass er dabei auf die Unterstützung eines externen IT-Security-Experten zählen wollte. Diese Adrian Schürli: "Für die Umsetzung sollten wir zunächst der richtigen Messuren, insbesondere werden wir die Projekt selbstständig realisieren. Der Beitrag eines externen-Experten sollte zudem die sein, dass der Prozess unabhängig und neutral beurteilt wird und wesentliche Punkte nicht übersehen werden und wir uns auf den besten-für-uns-konzepte konzentrieren können."

Nach der Umsetzung hat die SIAG auf die Sidler Information Security GmbH aus Hünenberg, Auszugstestung dafür war das Wichtige Sidler, Gründer und CEO der Firma, neben seinen anspruchsvollen und langjährigen Security-Know-How



ISO 27001  
Zertifizierung

