Dataspace Switzerland 2022

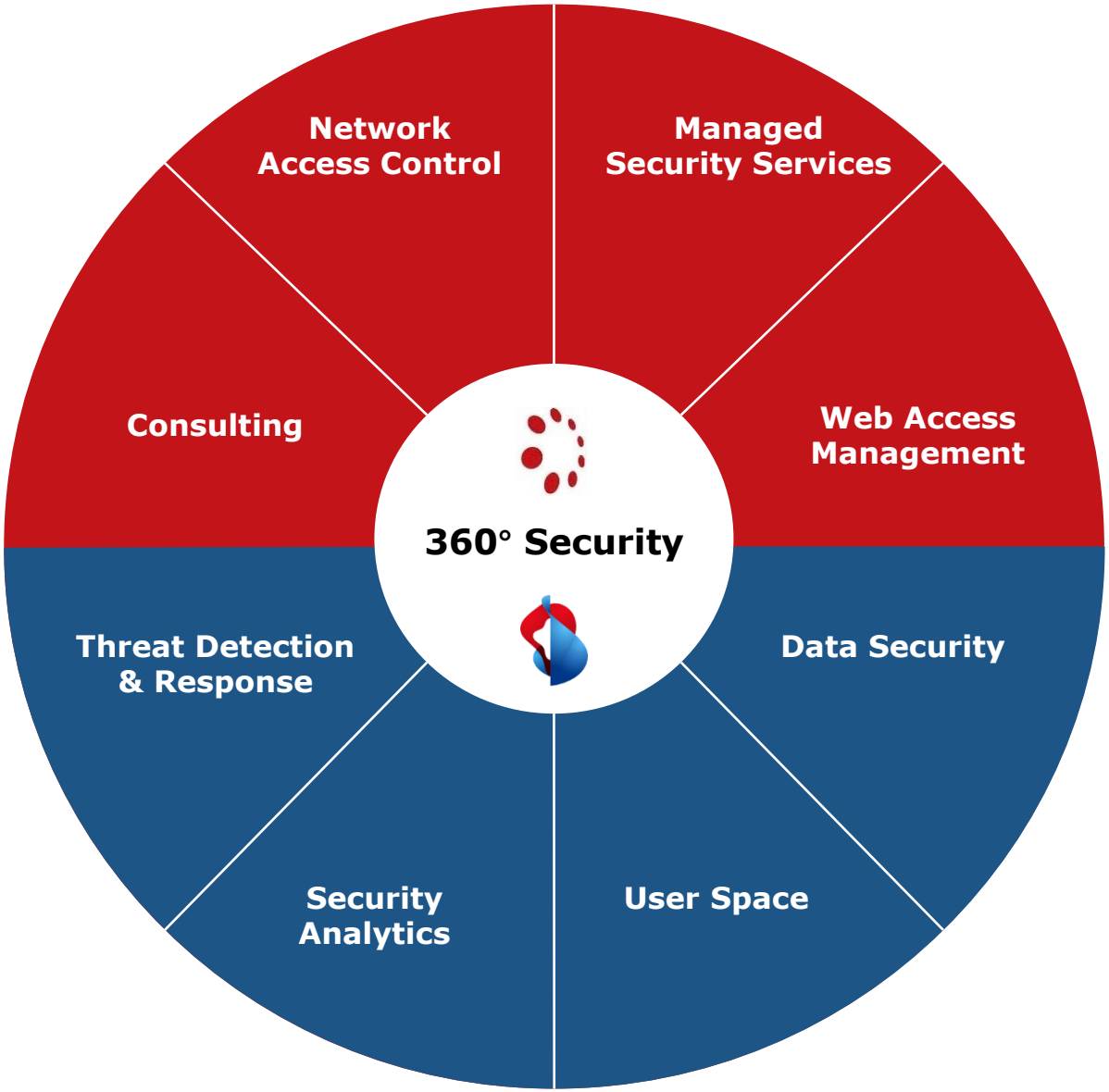
UNITED SECURITY PROVIDERS

Wie Data Compliance in der Cloud in drei einfachen Schritten erreicht wird

Dorothée Troyanov
IT Security Consultant

Wir schaffen Sicherheit für Unternehmen

United Security Providers und Swisscom

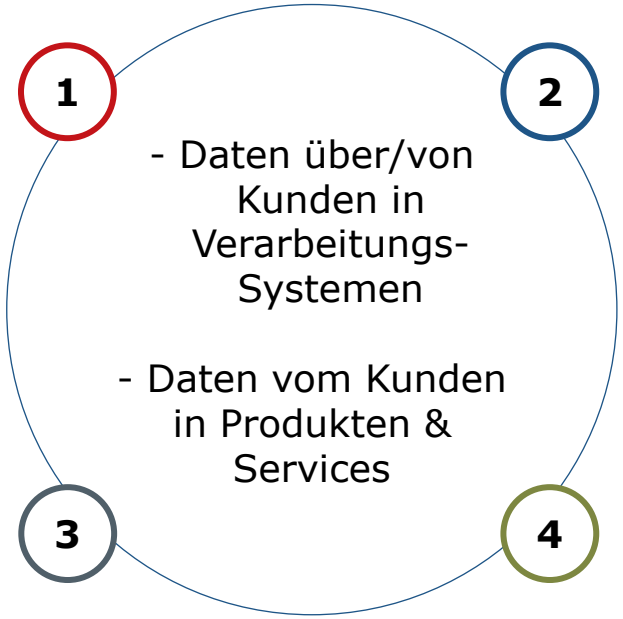


I. Wissen, welche Daten(arten) vorhanden sind

II. Wissen, welchen Compliance Vorgaben meine Daten unterstellt sind

Kundenvertrag
Im Vertrag mit dem Kunden können sich gewisse Datenschutzvorgaben befinden, z.B. Datenspeicherung in der Schweiz.

Gesetzliche Geheimhaltungspflichten (StGB)
Mitarbeitende müssen sich bezüglich der Bearbeitung von Daten an den geltenden gesetzlichen Vorgaben (DSG, BankG, FINMA) und die Internen Richtlinien halten.



Cloud Act (DSGVO Non compliant)
Clarifying Lawful Overseas Use of Data Act: Erlaubt US-Behörden den Zugriff auf die Daten von US-Unternehmen und deren Niederlassungen im Ausland (Verschlüsselung nicht ausreichend).

Serverstandort
Die Dateien bei gewissen Funktionalitäten & Services (oder durch diese erzeugt) werden auf Server ausserhalb der Schweiz gespeichert. Dies ist z.B. inkompatibel mit einer Datenspeicherung CH Zusicherung.

Konsequenzen bei nicht Einhaltung

- Datenleck
- Kontrollverlust über die Daten
- Klage gegen das Unternehmen
- Schadensersatz bei Vertragsbruch
- Persönliche Verantwortung des Mitarbeiters – Strafverfolgung
- Konsequenzen für das Unternehmen:
  - Busse
  - Behördliche Untersuchung
  - Reputationsschaden
  - Kundenverlust

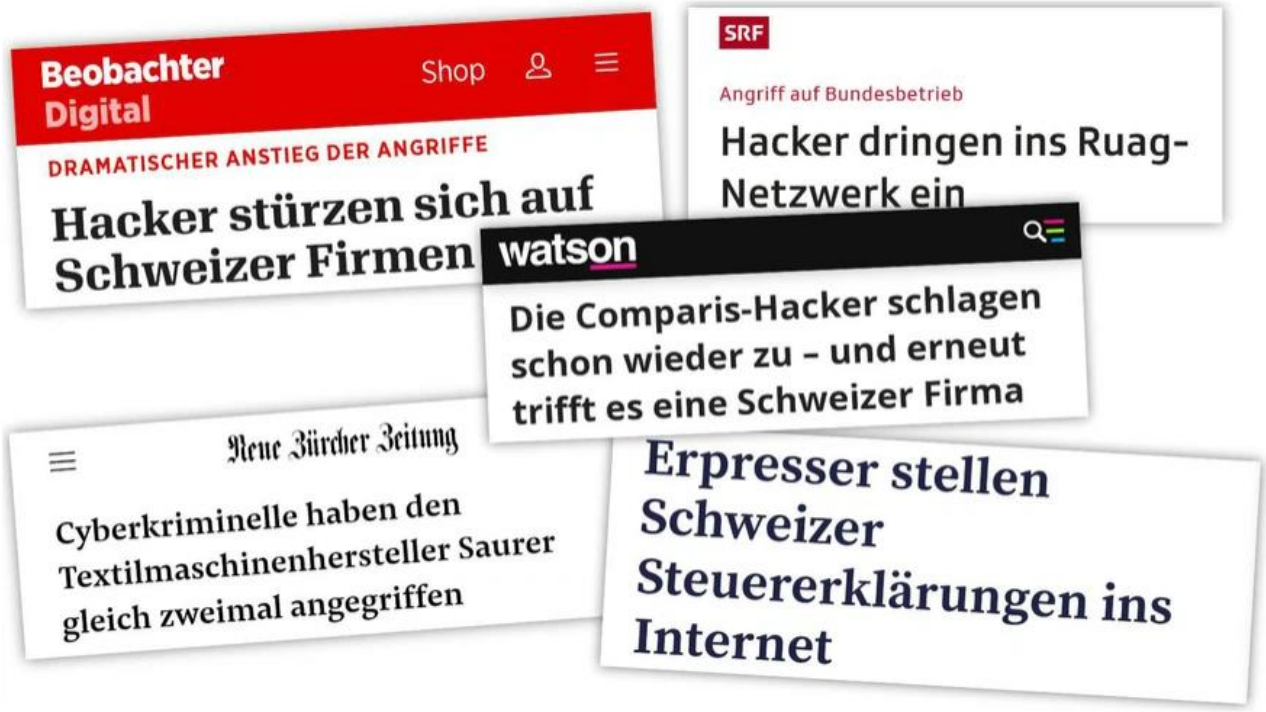
Was kostet ein grosses Dataleak durchschnittlich?

Ein erheblicher Dataleak bei einem Grossunternehmen kostet ungefähr CHF

2–3 Millionen.

+ über 1000 Arbeitsstunden, um den Schaden zu beheben.

Presseberichte



Blick auf den Hauptsitz der CPH-Gruppe und die Papierfabrik in Perlen, Luzern. *bild: cph-gruppe*

Hacker legen einzige Zeitungspapierfabrik der Schweiz lahm – Folgen nicht absehbar

Bekannte Ransomware-Angriffe:

- IKRK
- Rolle
- Apotheke zur Rose
- Bad Zurzach
- Bubendorf
- Ruag

(Quelle: Hacker schlagen in der Schweiz zu: Die unfassbar lange Opfer-Liste, watson.ch)

III. Schutzmassnahmen implementieren

Organisatorische Massnahme: Datenklassifizierung

Öffentlich

Daten, die frei mit allen geteilt werden können

Beispiele

- Verzeichnisse
- Medienmitteilungen
- Marketingmaterial
- Kontaktinformationen
- Preislisten

Intern

Daten, die nicht für die Öffentlichkeit bestimmt sind

Beispiele

- Arbeitspläne
- Budgets
- Projektpläne
- Strategien
- Geschäftsprozesse

Vertraulich

Sensible Daten, die bei Kompromittierung den Betrieb beeinträchtigen können

Beispiele

- Verträge mit Anbietern
- Regulierte Daten (personenbezogene Daten, Gesundheits-informationen)
- Personalakten
- Finanzdaten

Streng vertraulich

Hochsensible Unternehmensdaten, die ein finanzielles oder geschäftliches Risiko für das Unternehmen darstellen, wenn sie kompromittiert werden

Beispiele

- Passwörter
- Hochregulierte Daten
- M & A Pläne
- Kritisches IP
- KK Infos

III. Schutzmassnahmen implementieren

Technische Massnahme: Verschlüsselung

Verschlüsselungslösungen:

- Vendor Verschlüsselung
- ByOE (Bring your Own Encryption): eigene Verschlüsselung
- ByOK (Bring your Own Key): eigenen Schlüssel für die Verschlüsselung generieren
- HyOK (Hold your Own Key): eigenen Schlüssel für die Verschlüsselung generieren und behalten

Datenarten bei einer Verschlüsselung:

- Data at Rest: Daten werden in einem Server oder Speicherort gehalten
- Data in Transit: Daten verkehren von einer Applikation/ einem Ort zu einer/m anderer/n
- Data at Use: die Daten werden in einer Applikation oder für einem Prozess benutzt


Fragen?

Wie Data Compliance in der Cloud in drei einfachen Schritten erreicht wird

UNITED SECURITY PROVIDERS

Vielen Dank.

Dorothée Troyanov
IT Security Consultant
United Security Providers AG
dorothee.troyanov@u-s-p.ch
+41 79 885 65 50