CYBER SAFE

RW Oberwallis
Regions- und Wirtschaftszentrum Oberwallis AG

Kernkriterien und Herausforderungen

Impulsveranstaltung Cyber-Sicherheit
22. September 2022

Agenda

1. Die Kernkriterien im Kontext: die Risiko Analyse
2. Herausforderungen
3. Ein paar Wörter zum Label

Die Grundlage: die Risikoanalyse

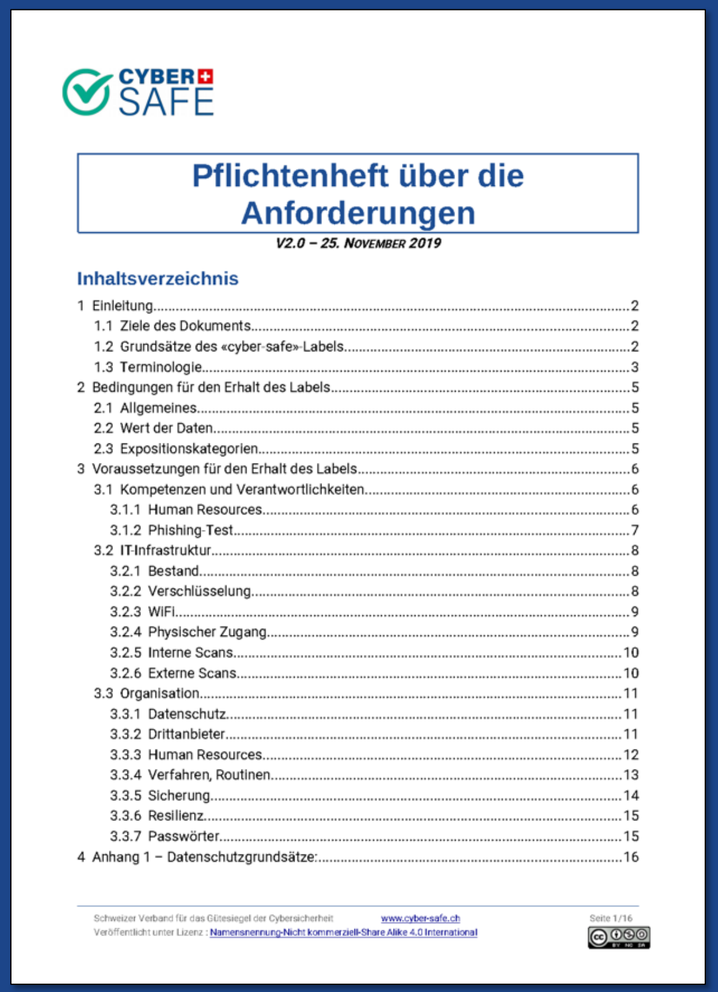
Bevor Sie sich entscheiden, wie Sie sich schützen oder versichern wollen, eine Frage : ***Was haben Sie zu verlieren?***

- Eine komplexe Frage
- Was haben Sie für Datentyp? Verwaltungsdaten, Finanzielle Daten, Daten von Dritten, etc.
- Pro Datentyp, was wären die CIA Auswirkungen:

… **C**onfidentiality (**Vertraulichkeit**)
Wie viel werden Sie verlieren, wenn diese Daten der Öffentlichkeit zugänglich gemacht werden?

… **I**ntegrity (**Integrität**)
Wie viel könnten Sie verlieren, wenn diese Daten geändert werden? (z.B. offenen Rechnungen, Geldbussen, usw.)

… **A**vailability (**Verfügbarkeit**):
Kosten wenn diese Daten nicht mehr zugänglich sind? (z.B Anzahl Mitarbeiter im Stillstand)



CYBER SAFE

Pflichtenheft über die Anforderungen

V2.0 – 25. November 2019

Inhaltsverzeichnis

1 Einleitung....2
1.1 Ziele des Dokuments....2
1.2 Grundsätze des «cyber-safe»-Labels....2
1.3 Terminologie....3
2 Bedingungen für den Erhalt des Labels....5
2.1 Allgemeines....5
2.2 Wert der Daten....5
2.3 Expositionskategorien....5
3 Voraussetzungen für den Erhalt des Labels....6
3.1 Kompetenzen und Verantwortlichkeiten....6
3.1.1 Human Resources....6
3.1.2 Phishing-Test....7
3.2 IT-Infrastruktur....8
3.2.1 Bestand....8
3.2.2 Verschlüsselung....8
3.2.3 WiFi....9
3.2.4 Physischer Zugang....9
3.2.5 Interne Scans....10
3.2.6 Externe Scans....10
3.3 Organisation....11
3.3.1 Datenschutz....11
3.3.2 Drittanbieter....11
3.3.3 Human Resources....12
3.3.4 Verfahren, Routinen....13
3.3.5 Sicherung....14
3.3.6 Resilienz....15
3.3.7 Passwörter....15
4 Anhang 1 – Datenschutzgrundsätze:....16

Die Kernkriterien

- Grundschutzmassnahen – IT Hygiene
- Nullrisiko gibt es nicht !

➢ **Wahrscheinlichkeiten verringern**

- Z.B. Phishing-Kampagne zur Sensibilisierung der Mitarbeiter

➢ **Auswirkungen verringern**

- Sicherung (Backup)

Herausforderungen – IT Infrastruktur

- **Verschlüsselung**
  - Welche Daten - **Inventar**
    - z.B. Finanzdaten
  - Im **Ruhezustand**
    - z.B. auf dem Laptop
  - Bei der **Übertragung** nach aussen
    - z.B. bei der Übermittlung an der Treuhandgesellschaft

Herausforderungen – IT Infrastruktur

- **Trennung Netzwerke:**
  - **Wi-Fi Gast ≠ Wi-Fi Arbeitsnetzwerk**
  - Segmentierung (Infektion begrenzen)
  - ➢ Technische Einrichtung (IT Partner)
- **Aktualisierung Soft und Hardware**
  - **Vollständigkeit !**
  - Mandatsvertag vs. Leistungsvertrag
  - Budget!

Herausforderungen – IT Infrastruktur

- **Antivirus und Firewall**
  - AV vorhanden und aktualisiert auf alle Geräte: Vollständigkeit!
  - **Sicherheitswarnungen**
    - Zentralisiert…
    - …Regelmässig verarbeitet

Wenn der Feueralarm losgeht, stellen Sie ihn dann einfach ab ?

Wahrscheinlich nicht. Und beim Antivirus?

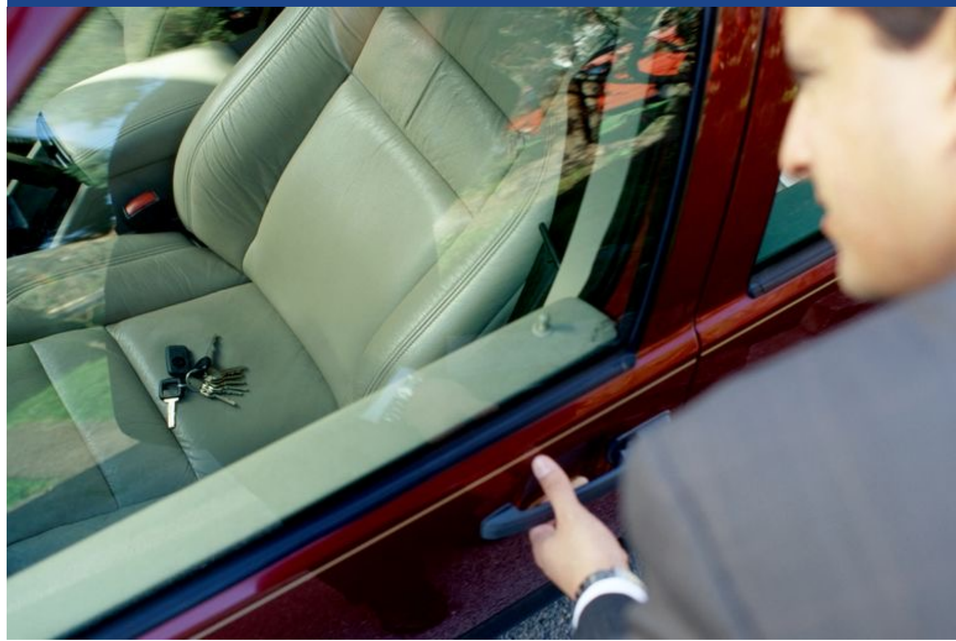
Herausforderungen – IT Infrastruktur

- **Datensicherungsystem**
  - Daten und System Sicherung; Frequenz? Verweildauer?
  - Vollständigkeit – alle Daten inbegriffen?
  - Daten im Cloud
  - **Nicht zugänglich Mitarbeiter / Administratoren**
  - **Regelmässige Überprüfung**

Ihr Backup ist nur wertvoll, wenn Sie es wiederherstellen können!!!

3 - 2 - 1 - 0 Regel

- **3 Kopien**
- **2 Formate**
- **1 Kopie ausserhalb des Standorts**
- **0 Fehler beim Wiederherstellungstest**



Herausforderung – Org. Massnahmen

- **Drittanbieter**
  - Wer sind die verschieden Anbieter?
  - Wer macht was?
    - Unklarheiten identifizieren und regeln!
- **Berechtigungsplan…**
  - Administrator: möglichst wenig!
  - Beim Austreten (Mitarbeiter, Praktikant)
- **… und Benutzercharta**
  - **Private Geräte** (Telearbeit, Smartphone, etc.), auch in Zusammenhang mit gewählte **Gemeindeexekutive**!

Herausforderung – Org. Massnahmen

- **Passwortrichtlinien**
  - Mindestanforderungen können technisch bestimmt werden
  - Länge und Komplexität
  - Passwortmanager
  - Passphrase:
    - Mein Auto hat 2 Türen, 1 Motor und 4 Räder -> MAh2T,1Mu4R (aus dem Web, nicht benutzen!)

Platz	Anzahl	Passwort
1	2600	123456
2	708	1234
3	498	123456789
4	428	12345678
5	381	12345
6	289	111111
7	266	hallo
8	215	passwort
9	175	soleil
10	162	password

«ein Freiwilliger für Cybersicherheit?»

Chappatte, Le Temps, 28.01.2022

Kompetenzen und Verantwortung

1. **Verantwortung auf der Ebene des Managements / Gemeinderat**
   - Entscheidungen > Kompetenzen !
2. **Kontaktperson** innerhalb der Organisation:
   - Kontaktstelle
   - Zugang zu den Kompetenzen
   - Feedback?
3. **Bereichsübergreifende** Dimension der Cybersicherheit
   1. Operative Leistungen
   2. Marketing
   3. HR
   4. Etc.

Phishing- Identifizierung

- **Inhalt der E-Mail bewerten**
  - überraschende, dringende oder unerwartete Anfrage? Schreibfehler? Anfragen zu persönlichen Informationen und Zugangsdaten?

- **Absender der E-Mail mit Sicherheit identifizieren**
  - Bei Unsicherheit, durch andere Kommunikationskanäle bestätigen

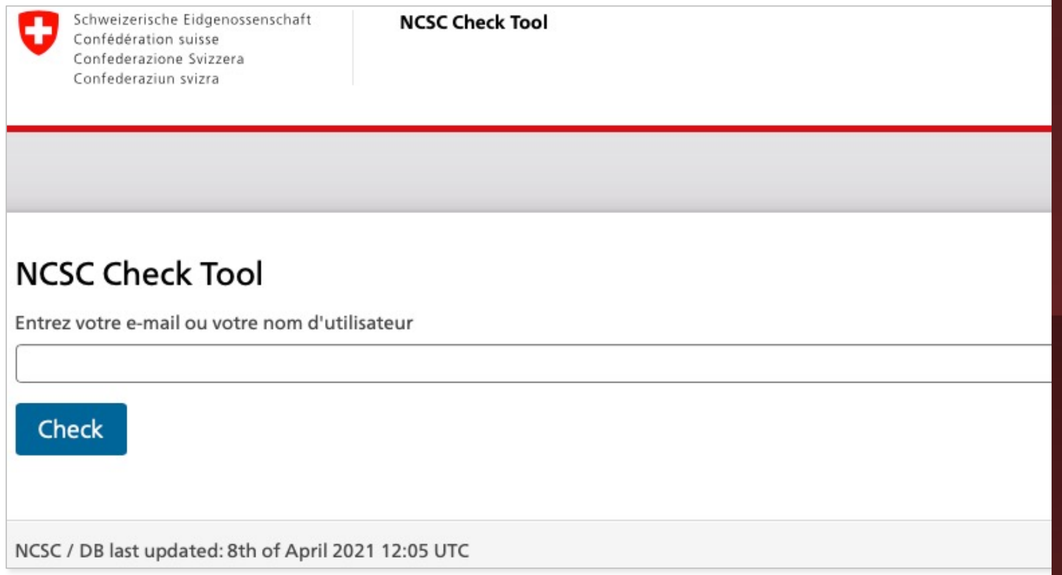
- **Identifizieren Sie verdächtige Links in der E-Mail**

- **Zweifel oder haben einen Phishing-Versuch erkannt?**
  - Fragen, informieren und kommunizieren

Benutzerkonten überprüfen

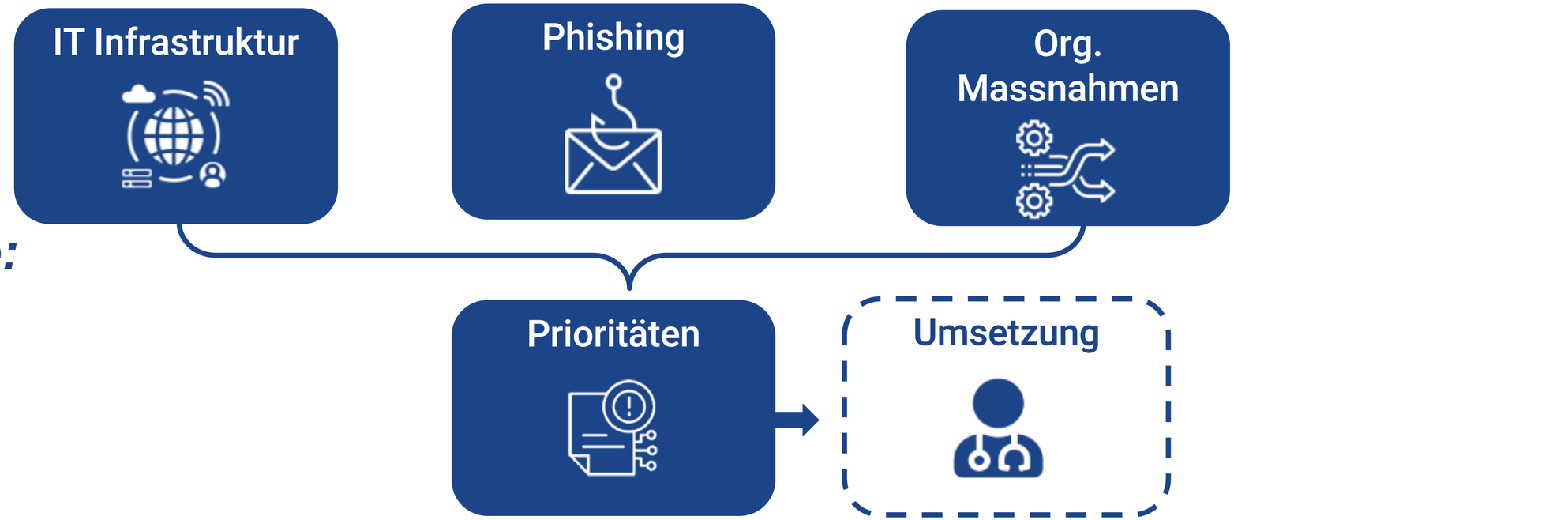
https://haveibeenpwned.com/

https://www.checktool.ch



Label Cyber Safe: Übersicht

1.Diagnose:



2.Überprüfung:

Danke für Ihre Aufmerksamkeit

Fragen?

info@cyber-safe.ch