« credo ut intelligam non intelligo ut credam »

Ich glaube, dass ich verstehen darf –
Ich verstehe nicht, dass ich glauben darf

Öffentliche Verwaltungen und Klein- & mittlere Unternehmungen als Ziel von Cyberangriffen

- Digitalisierung in den Gemeinden
- Abhängigkeit von funktionierender Informations- und Kommunikationstechnik ist ohne die Verbindung zu externen Dienstleistungsunternehmen nicht mehr möglich.
- Angriffe auf diese Vernetzung und Abhängigkeiten.
- Das Personal bestenfalls reine Anwender.
- Wert der Daten kennen
- Verantwortlichkeiten

Pilotgemeinde im Oberwallis

- Regions- und Wirtschaftszentrum Oberwallis AG

Fragen und Unsicherheiten in Gemeinden im Umgang mit der Digitalisierung

ASSOCIATION SUISSE POUR LE LABEL DE CYBERSÉCURITÉ - Pilotgemeinde im Oberwallis

- Vertragsunterzeichnung und Online-Fragebogen
- Festlegung der Arbeitsplätze und IT-Umgebung
- Start eines Phishing-E-Mail Angriffes über längerem Zeitraum
- Schwachstellen Scanning der IT-Infrastruktur (ca. 2h)
- Bericht auf Basis Fragebogen, Phishing und Scanning
- Abarbeitung der Abhilfemassnahmen
- Durchführung eines Audits
- Labelvergabe

Der Wow – Effekt!

- Erfolgreiche Phishing-Kampagne ✅
- Expositionsniveau durchschnittlich kritisch ❌
- Schutzniveau ist durchschnittlich ❌
- Risikoniveau ❌
- Liste der Zugriffsberechtigung ❌
- Leistungsvereinbarungen mit Dienstleistern ❌
- Passwortkomplexität ❌
- BIT-Locker auf allen Geräten ❌
- IT-Charta Mitarbeiter ❌

Passwortschutz der IT-Geräte

Ein Beispiel:

Mitarbeiter A nutzte als Passwort mit 4 Zahlen, 6 Buchstaben und 1 Sonderzeichen. Das Resultat der Passwortprüfung:

Teilwörter	Typ	Entropie	Rechenzeit
***	Namensliste	13 Bit	
***	Übrige Zeichen	28 Bit	
Aufwandschätzung		42 Bit	32 Sekunden

Mit dem heutigen Passwort: (4 Zahlen, 10 Buchstaben, 1 Sonderzeichen)

Teilwörter	Typ	Entropie	Rechenzeit
***	Übrige Zeichen	100 Bit	
Aufwandschätzung		100 Bit	Mehrere Millionen Jahre

Passwortschutz der IT-Geräte

- Bequemlichkeit und Angst, Passwörter zu vergessen…
  - ➡ Kleiner Trick mit grosser Wirkung:

Man denkt sich eine Geschichte aus:
$eit 2009 bin ich Gemeindeschreiber in Salgesch und habe 3 Kinder

$eit 2009 bin ich Gemeindeschreiber in Salgesch und habe 3 Kinder

$2009biGiSuh3K

Teilwörter	Typ	Entropie	Rechenzeit
***	Datum	15 Bit	
***	Übrige Zeichen	67 Bit	
Aufwandschätzung		82 Bit	Mehrere Millionen Jahre

Audit und Schlussbericht

- Bereitstellung alle Dokumente
- Terminfindung zur Durchführung des Audit durch den Spezialisten der Association Suisse pour le Label de Cybersécurité
- Anwesenheit externer IT-Dienstleiter während des Audit ratsam
- Erstes Audit 3.11.2021 – nicht bestanden
- Lücken schliessen
- Zweites Audit 29.11.2021 – bestanden
- Vertraulicher Audit-Bericht und Zertifikat erhalten
- Entscheid über Kommunikation nach Aussen

Kosten

- Dienstleistungen Association suisse pour le Label de Cybersécurité — Fr. 3’758.00
- IT – Dienstleister der Gemeinde für Support — Fr. 2’540.05
- Anschaffungen IT oder Software — Fr. 1’692.00

« credo ut intelligam non intelligo ut credam »

Ich glaubte zu wissen,
dass unsere Informatik in der Gemeinde sicher ist

Nun weiss ich, dass ich glauben darf,
dass wir gegenwärtig die bestmöglichen
Sicherungen eingebaut haben