acf-fgv
association des communes fribourgeoises
freiburger gemeindeverband

Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg

VILLARS-SUR-GLÂNE

POLICE

Cybersicherheit

Vorbeugen, unterstützen, handeln

23.1.2025

Programm

1. Einführung
2. Prävention: *Welche Verhantensweisen sollte man respektieren?*
3. Audits und Zertifizierungen: *Wie funktionniert das?*
4. Wie reagieren im Falle eines Verdachts, eines Angriffs oder einer Bedrohung?
5. Beispiel einer Gemeinde: *Vorgehen und Ausbildung*
6. Toolbox Cybersicherheit
7. Schlussbemerkungen

Cybersecurity-Sensibilisierung

Jean-Roland Schuler, jean-roland.schuler@hefr.ch

François Buntschu, francois.buntschu@hefr.ch

Michael Mäder, michael.maeder@hefr.ch

Referenzen

[1]: www.ebas.ch (eBanking but secure, DE, FR, IT, EN)

[2]: www.ibarry.ch (Internet security platform, DE, FR, IT, EN)

[3]: www.ncsc.admin.ch (National Cyber Security Center NCSC, DE, FR, IT, EN)

Inhalt

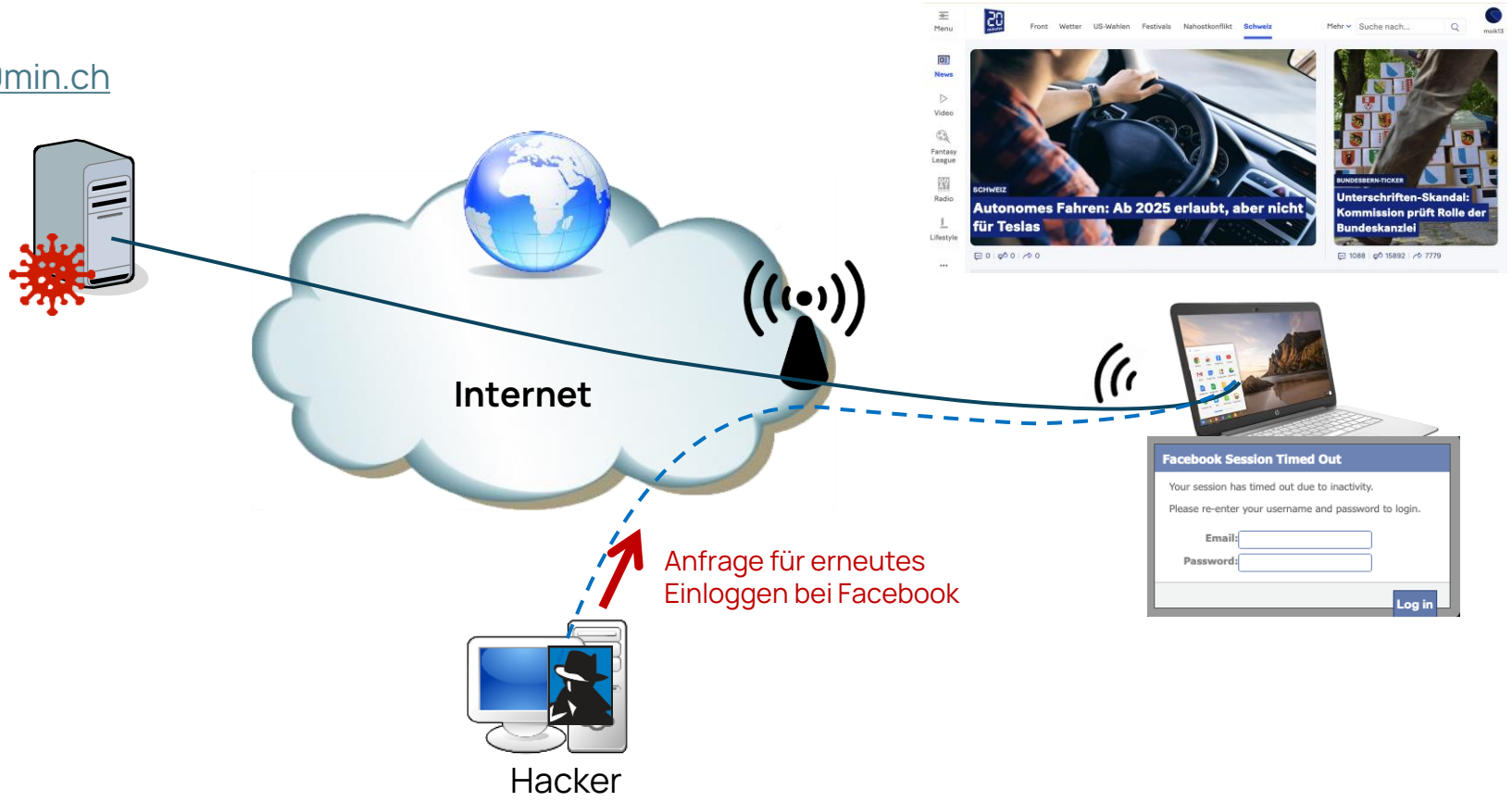
- Demo
- Sicherheitsregeln
- Was ist zu unternehmen im Falle eines Problems?
- Virus, Ransomware, …, wie kann man infiziert werden?
- Passwörter
- HTTPS, VPN

Demo – Szenario

- Gehackte Website ist das Ziel, auf welches ein Opfer geleitet werden soll
- Besuch der Website verbindet im Hintergrund der Browser des Opfers mit dem Hacker
- Der Hacker kann verschiedene Aktionen auf dem Computer des Opfers ausführen lassen (z.B. Credentials abfragen)
- Der Hacker kann die gewonnen Credentials direkt oder auf anderen Services nutzen
- Der Hacker kann mit Username/Email Passwörter versuchen zu knacken

Demo – Passwort-Diebstahl

https://20min.ch



Verhaltensregeln für Computer, Tablets und Smartphones

Regeln für die IT-Abteilung

- Ein aktuelles Antivirenprogramm haben
- Aktualisierungen aller Programme vornehmen
- Erstellen von Backups und Sicherstellen, dass diese auch gelesen werden können. Das Speichermedium muss nach einem Backup wieder getrennt werden
- Den Bildschirm sperren, wenn keine Aktivitäten stattfinden

Regeln für Benutzer

- Verwenden Sie komplexe Passwörter, z. B. *Ifb2j/@aSeVs*. Verwenden Sie nie mehrmals das gleiche Passwort
- Beenden oder sperren Sie die Sitzungen, wenn Sie Ihre Arbeitsstation verlassen
- Verwenden Sie keine unbekannten USB-Sticks
- Benutzen Sie keine öffentlichen WiFis ohne VPN
- Wenn möglich, keine sozialen Netzwerke auf den Arbeitsstationen nutzen
- **Wachsam sein, den gesunden Menschenverstand einsetzen**
- Persönliche Daten nicht weitergeben

Wie man bei einer Cyber-Attacke reagieren soll (1/2)

Isolieren

- Sich vom Internet trennen (Netzwerkkabel ziehen, WiFi deaktivieren)

Kommunizieren

- Kontaktieren Sie Ihren IT-Verantwortlichen
- Informieren Sie Ihre Kollegen und die Verwaltung
- Prüfen Sie, ob Sie die Polizei kontaktieren und eine Strafanzeige erstatten müssen.
- Warten Sie mit der Wiederherstellung der Systeme, bis die Polizei die Spuren gesichert hat. Spezialisten der Polizei beraten und unterstützen Sie bei der Frage, wie Sie vorgehen sollen, sichern die Spuren und ermitteln. Unter www.suisse-epolice.ch finden Sie die Telefonnummer der nächstgelegenen Polizeidienststelle.

Wie man bei einer Cyber-Attacke reagieren soll (2/2)

Planen

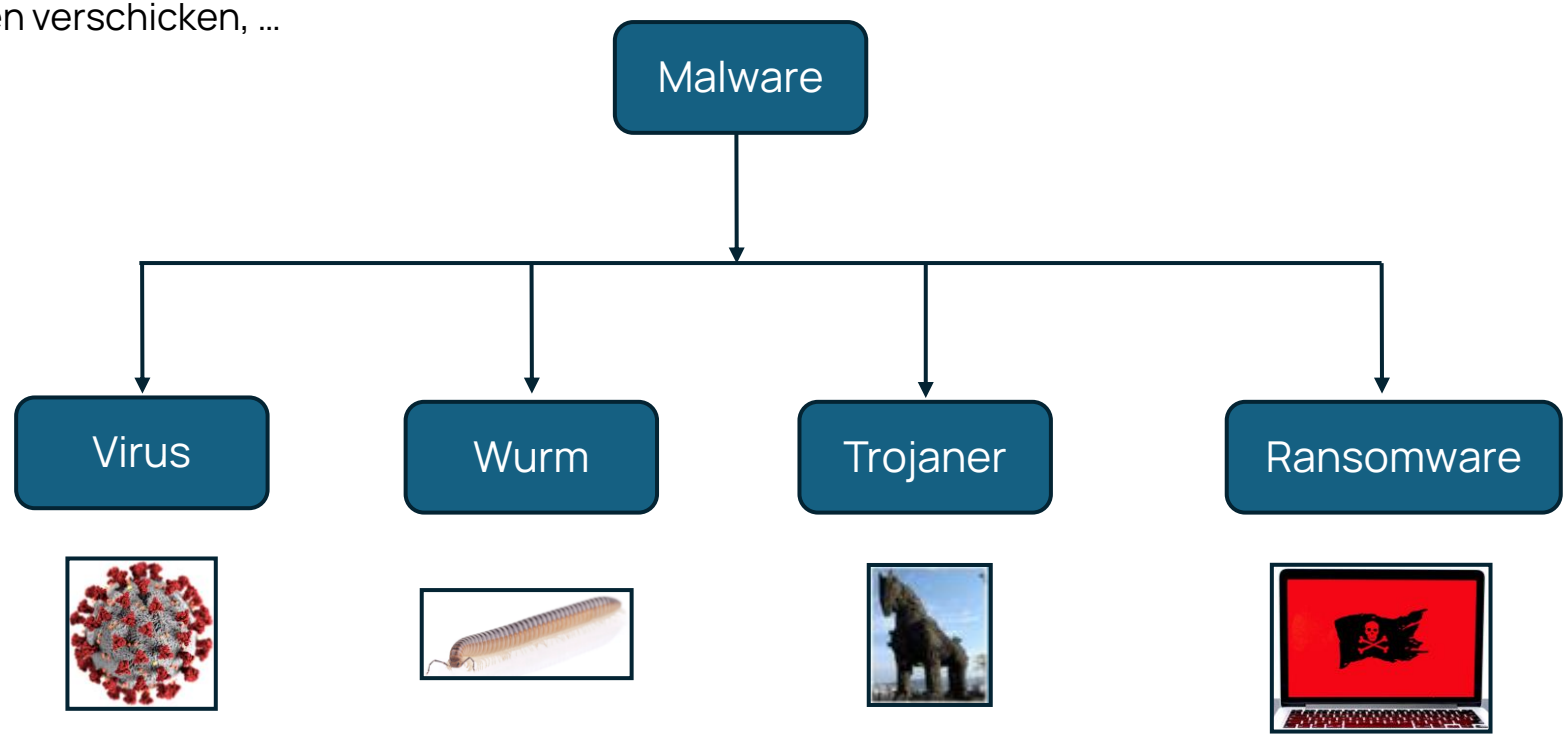
- Schnell und sorgfältig die Reaktion auf den Vorfall und die einzusetzenden Massnahmen (Schutz sensibler Daten, Wiederaufbau von Systemen) ausarbeiten

Vorbereitung / Vorbeugung

- Beurteilen Sie die Massnahmen, die Sie ergreifen müssen, um die Wahrscheinlichkeit eines weiteren ähnlichen Vorfalls zu verringern
- Mitarbeiter schulen

Schadprogramme (Malware)

- Malware ist ein allgemeiner Begriff, der alle bösartigen Programme wie Viren, Würmer, Trojaner, Ransomware und andere umfasst
- Eine Malware kann: verschlüsseln, stehlen, Daten modifizieren, Kamera einschalten, Daten verschicken, …

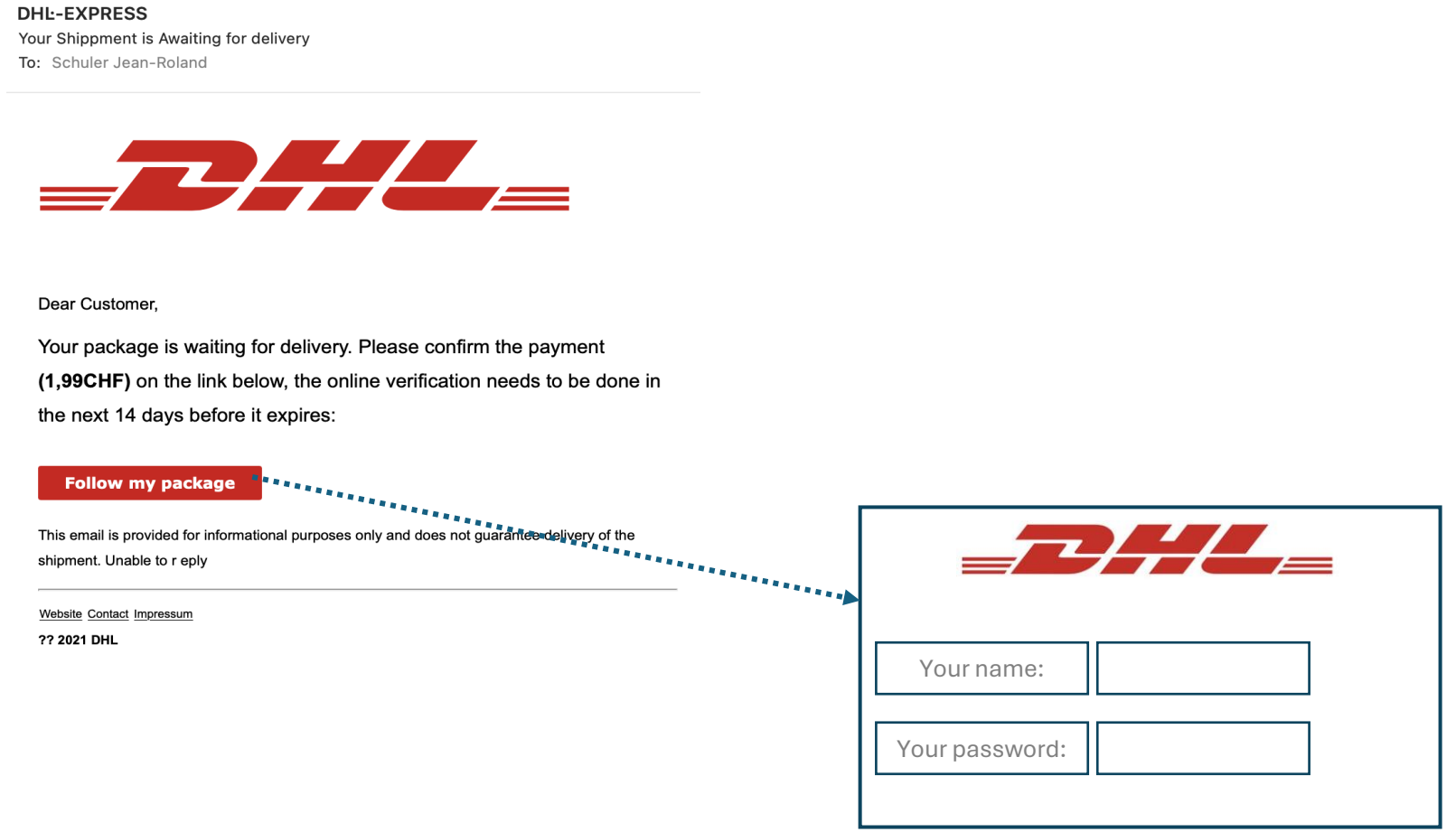


Einige Zahlen [2]

- Gegen 400k neue, detektierte Malwares / Tag (Ger)
- 50 Millionen kompromittierte Facebook-Accounts
- 91% der Cyberangriffe beginnen mit einer betrügerischen E-Mail, um Passwörter zu stehlen (Spear Phishing) und dann eine "Ransomware" zu installieren.
- Etwa 1-2 Millionen Angriffstests pro Tag auf weniger bekannte Websites
- Cyberangriffe können alle betreffen! Unternehmen, Personen, … und **Gemeinden**

Wie wird mein Gerät infiziert?

- Phishing: Anhänge und Links in E-Mails



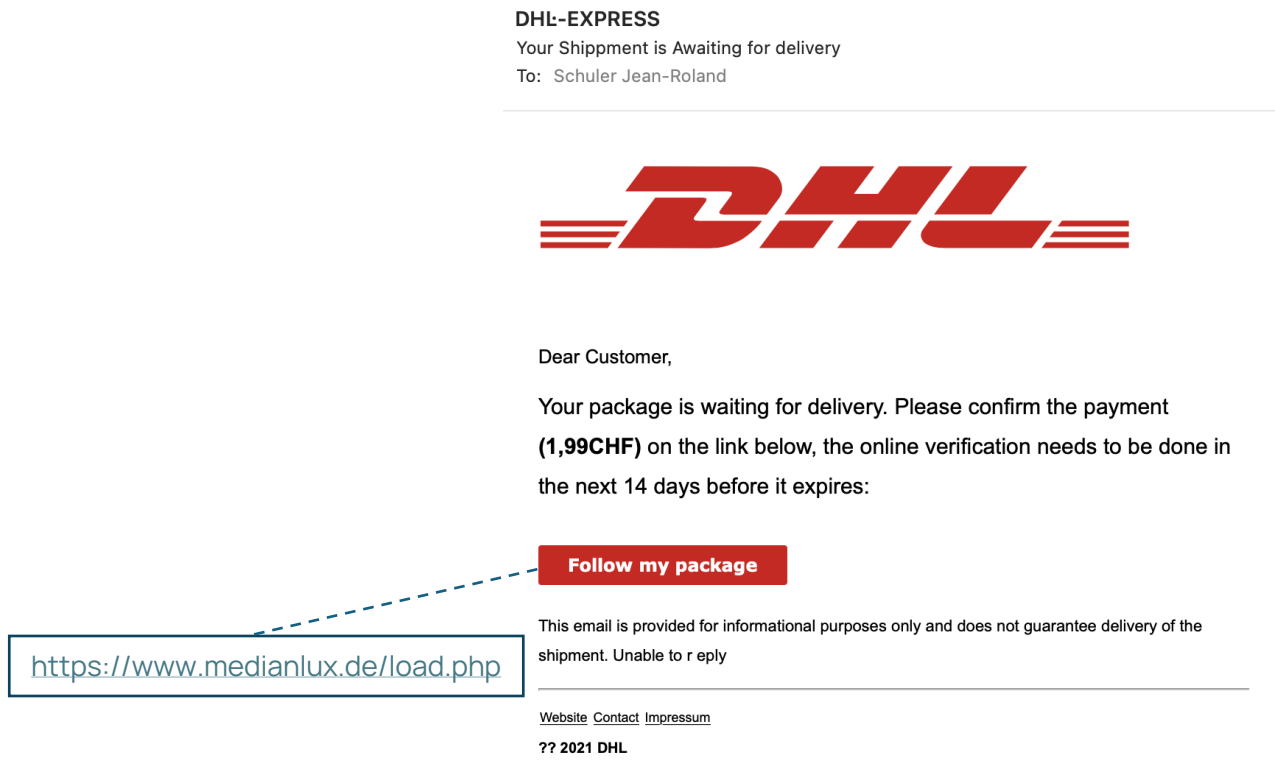
Phishing

- Verweis auf ein bekanntes Unternehmen
- Ankündigung eines bevorstehenden Problems (Empfang eines Pakets, Sperrung eines Kontos, …)
- Gefälschte E-Mail Adresse einer meist bekannten Person

Regeln:

- Niemals auf einen Link klicken
  Nur auf PC (nicht Smartphone, Tablet): Wenn man mit der Maus über den Hyperlink fährt und nicht klickt, dann sieht man die Ziel-Adresse).

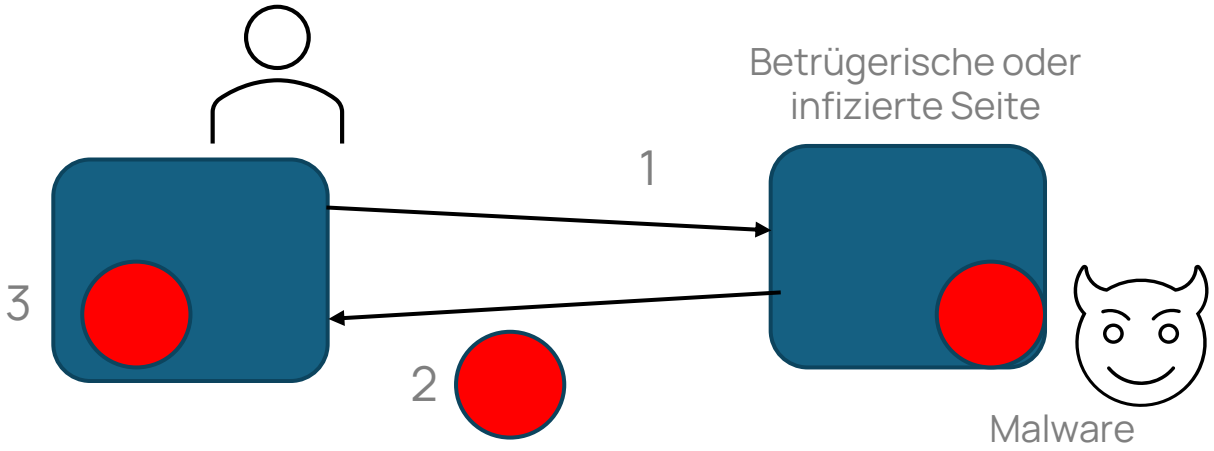
- Gut überlegen, bevor man eine Aktion ausführt



Infektion durch eine Malware

Herunterladen von einer betrügerischen oder infizierten Webseite

1) Der Benutzer verbindet sich auf eine infizierte Webseite
2) Die Malware wird auf den Computer des Benutzers geladen
3) Die Malware wird gestartet, sie kann:
   - Die Harddisk verschlüsseln
   - Protokollieren aller gedrückter Tastatur-Tasten
   - Wegkopieren von Daten der Harddisk
   - Einschalten der Kamera, Mikrofon, …
   - …



Beispiel:

Die Malware Gozi ist seit über 10 Jahren aktiv!

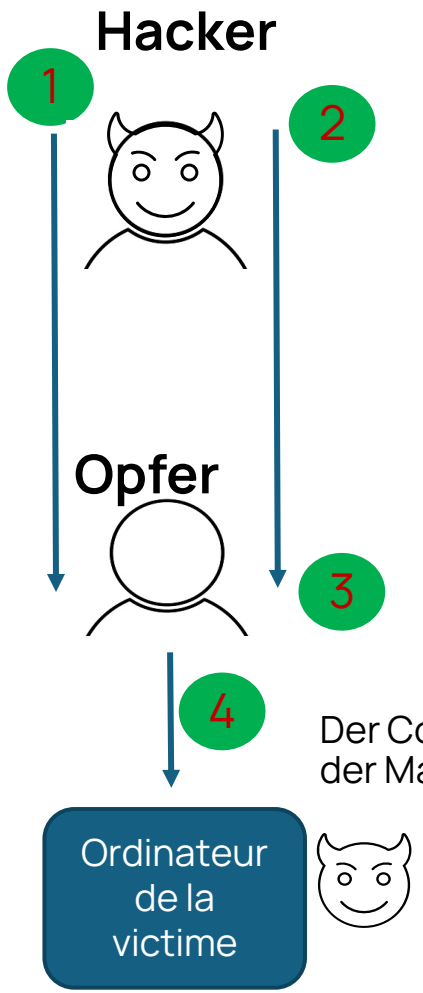
- 2016 wurde die Webseite von 20min.ch durch Gozi infiziert
- 2020 wurde eine abgeänderte Variante von Gozi per E-Mail-Anhang verschickt

Schutz: Antivirus und aktuelle Software (Updates)

Social Engineering und Malware [3]

Mithilfe sozialer Netzwerke erkundigt sich ein Hacker über das Opfer.

Er telefoniert mit dem Opfer. Er erzählt eine Geschichte und gibt an, dass er eine E-Mail mit einem Dateianhang versenden wird.



Direkt nach dem Telefonat, wird das Mail mit dem betrügerischen Inhalt ver-schickt.

Das Opfer öffnet die Datei

Der Computer des Opfers ist mit der Malware infiziert.

Schutz:

- Verhalten
- Antivirus
- Aktuelle Software (Updates)

Passwörter

Ein gutes Passwort muss folgende Kriterien erfüllen:

- Minimum 14 Zeichen lang sein
- Grossbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen
- Keine Zeichenfolgen: *asdf1234*
- Keine «richtigen» Wörter (Dictionary-Attack): *Haus123, Auto$*
- Pro Webseite ein eigenes Passwort
- Akzente nicht nutzen: ç, é, è, ä, ü, … (*problematisch beim Eingegeben*)

Beispiel eines guten Passworts:

`ISiWidCHsdS200T/J`

- Das Problem liegt darin, sich daran zu erinnern
- Ausserdem braucht man verschiedene Passwörter für jede Seite → «Password Manager»

USING CHATGPT HARDWARE TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	1 secs
9	Instantly	Instantly	4 secs	21 secs	1 mins
10	Instantly	Instantly	4 mins	22 mins	1 hours
11	Instantly	6 secs	3 hours	22 hours	4 days
12	Instantly	2 mins	7 days	2 months	8 months
13	Instantly	1 hours	12 months	10 years	47 years
14	Instantly	1 days	52 years	608 years	3k years
15	2 secs	4 weeks	2k years	37k years	232k years
16	15 secs	2 years	140k years	2m years	16m years
17	3 mins	56 years	7m years	144m years	1bn years
18	26 mins	1k years	378m years	8bn years	79bn years

HIVE SYSTEMS

› Learn how we made this table at hivesystems.io/password

Passwörter

In Sierre im Wallis in der Schweiz scheint die Sonne 200 Tage pro Jahr

ISiWidCHsdS200T/J

Ein weiterer Tipp: Verwenden Sie einen langen Satz (ohne Leerzeichen)

Im2020-2021herrschtediePandemie

31 Zeichen, Grossbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen

Ein Passwort pro Website

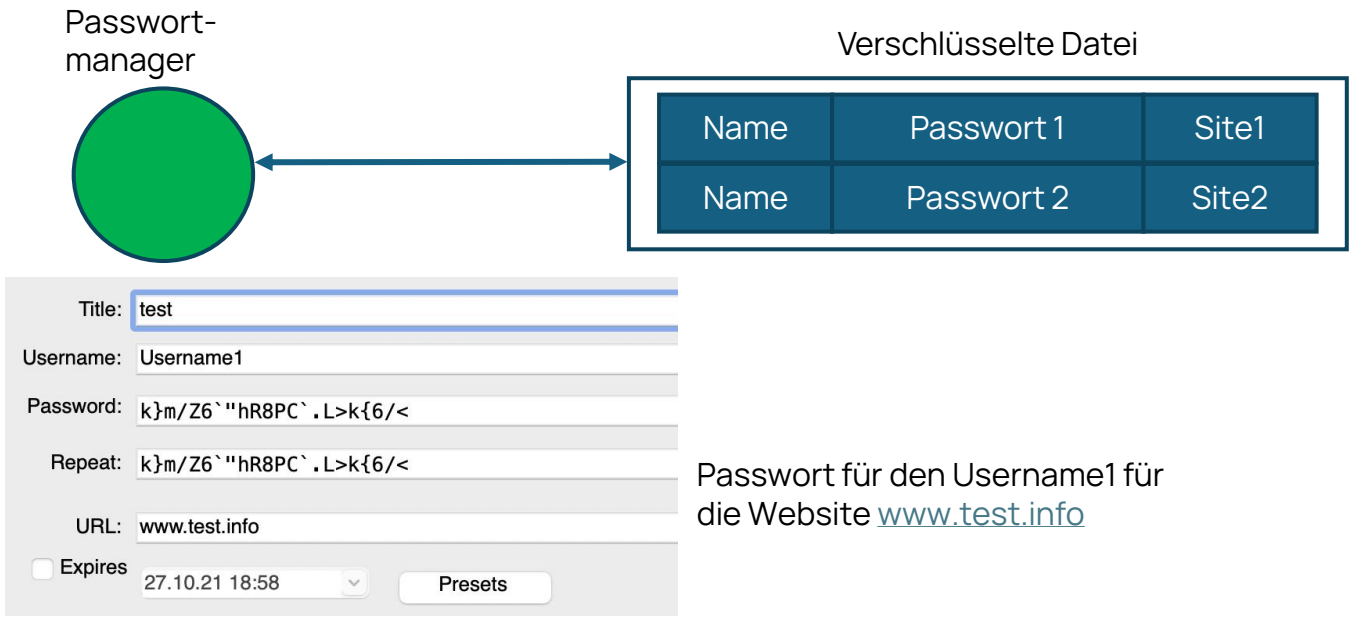
- Oft verwenden Personen überall das gleiche Passwort. Wenn das Passwort gestohlen wird, haben Hacker Zugang zu allen Konten mit diesem Passwort

- Für jede Webseite soll ein anderes Passwort verwendet werden. Ein Passwortmanager kann hier sehr hilfreich sein (nicht abschliessende Liste):
  - NordPass
  - LastPass
  - 1Password
  - KeePass
  - Bitwarden

- Passwörter **nicht** im Browser speichern!
- Passwörter **nie** auf einen Zettel (PostIt) schreiben!

Passwortmanager

- Ein Passwortmanager speichert Passwörter, Namen, Sites in einer verschlüsselten Datei
- Um die Datei zu ver- und entschlüsseln, benötigt der Benutzer nur ein einziges Passwort (welches natürlich sicher sein muss)

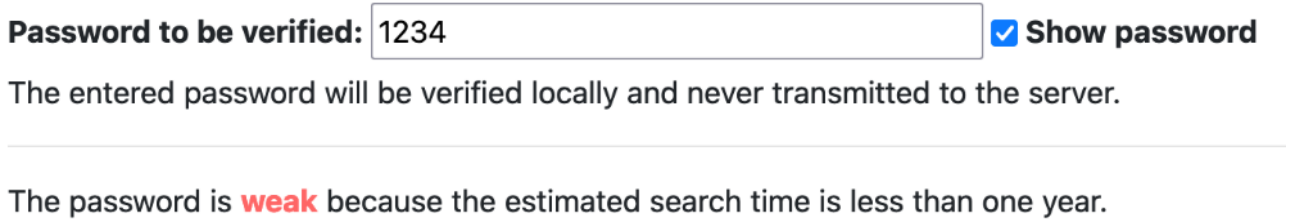


Passwort für den Username1 für die Website www.test.info

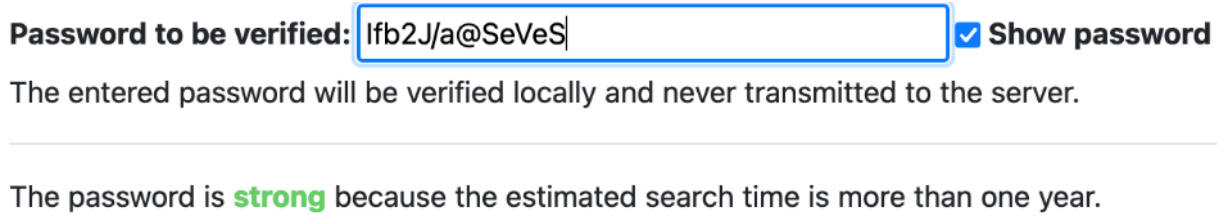
Testen der Passwort-Qualität

Sie können Ihr Passwort (oder ein ähnliches Passwort) auf dieser Webseite testen: www.passwortcheck.ch

Schwaches Passwort:



Starkes Passwort:



Testen, ob die E-Mail-Adresse kompromittiert ist

Verwenden Sie Tools wie https://haveibeenpwned.com/, um Ihre E-Mail-Adresse zu testen.

Was tun, wenn sich Ihre E-Mail-Adresse in "haveibeenpwned" befindet?

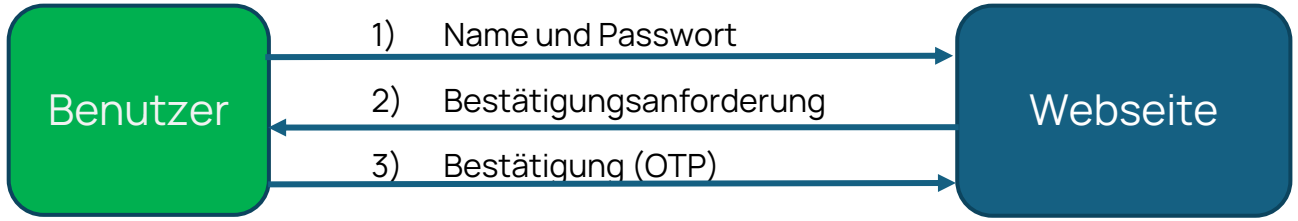
- Ändern Sie Ihr Passwort (Vorsicht, wenn Sie nur 1 Passwort verwenden)

Es ist möglich, sich bei https://haveibeenpwneed.com anzumelden, um informiert zu werden, wenn die E-Mail-Adresse in der Datenbank auftaucht.

2-Faktor Authentifizierung

Wenn möglich, sollten sie eine 2-Faktor Authentifizierung einsetzen:

1. Sie geben ihr Benutzername und Passwort ein (1. Faktor)
2. Die Gegenstelle fordert eine Bestätigung mit einem **OTP** (*One Time Password*) an. Die Bestätigung kommt auf dem Smartphone (SMS, MobileID, Authenticator, ...) oder in einer anderen Anwendung (z. B. RSA Token) an. Das ist der 2. Faktor
3. Sie bestätigen Ihre Anmeldung

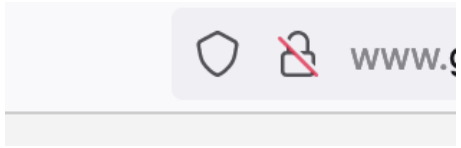


Geschützter Zugriff, https

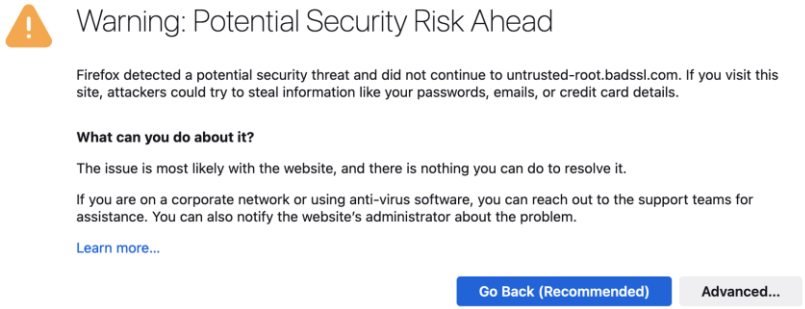
- Wenn man sich zu einer offiziellen Website (Kanton, Gemeinden, ...) verbindet, muss man https und das Schloss kontrollieren
- https sagt aus «abgesichert», man ist mit der richtigen Website verbunden und die Daten werden verschlüsselt übertragen

Geschützter Zugriff: https

- Sie sind auf einer offiziellen Website angemeldet, die kein https hat und das Schloss ist durchgestrichen



- Während der Verbindung werden Fehlermeldungen angezeigt

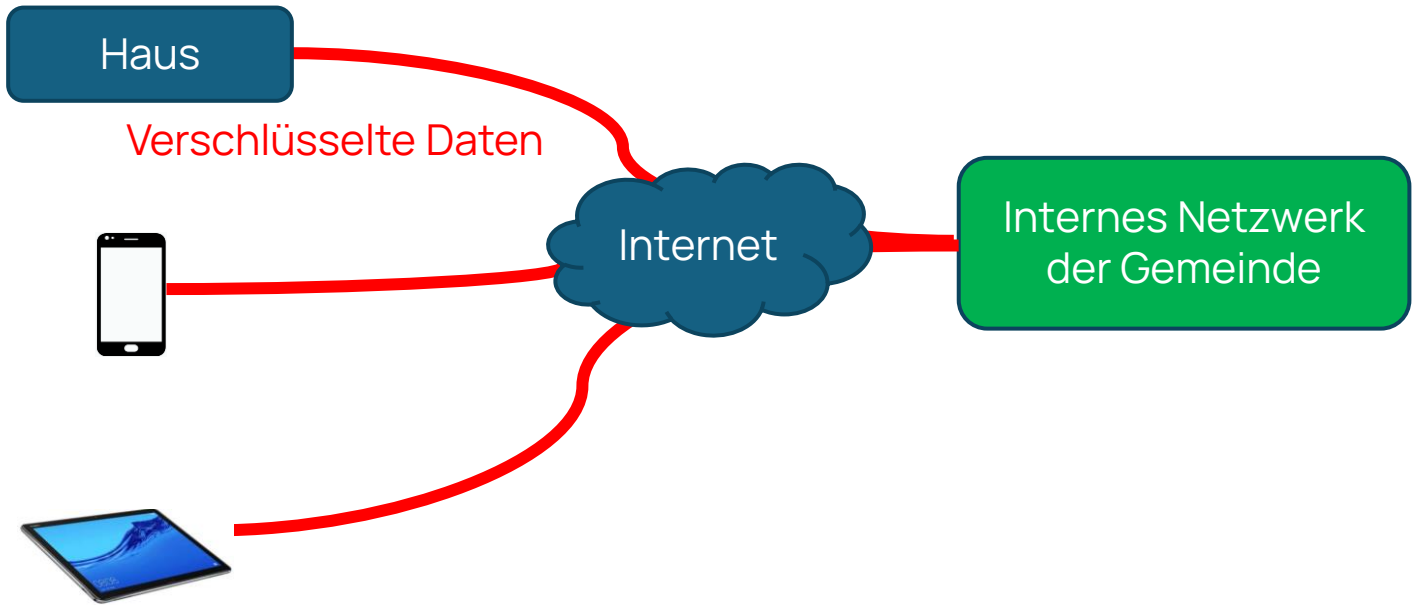


Regel: Nicht weitergehen, erkundigen Sie sich bei der IT-Abteilung der Gemeinde

Geschützter Zugriff: VPN

- Wenn Sie von einem Computer, einem Smartphone oder einem Tablet auf das interne Netzwerk der Gemeinde zugreifen müssen, dann müssen Sie ein VPN-Programm verwenden, welches die Kommunikation absichert und verschlüsselt

- Dieses VPN-Programm wird (normalerweise) durch den IT-Service installiert und betrieben



Werkzeugkiste

Hier ist eine Liste der wichtigsten Fragen zur Überprüfung der Sicherheit:

- Ist des Betriebssystems aktuell? (Update: Windows, MacOS, Android, iOS)
- Sind die gängigen Programme aktuell? (Word, Excel, **Browser** (!) …)
- Sind die spezifischen Gemeinde-Anwendungen aktuell? (Einwohnerkontrolle, Steuern, Buchhaltung, …)
- Ist ein Antiviren-Programm installiert, ist es aktuell und aktiv?
- Wie ist die Qualität der Passwörter? Wie werden sie verwaltet?
- Wer muss im Fall eines Vorfalls/Fehlers (Öffnen einer bösartigen Datei, Alarm des Antivirus, …) kontaktiert werden?
- Gibt es Backups, wo sind die Backups aufbewahrt, kann man die Backups lesen, ist der Wiederherstellungsprozess bekannt?
- Hat die Gemeinde ein IT-Sicherheitsaudit durchgeführt?

Audits und Labels, *wie funktioniert das?*

Jean-Roland Schuler, jean-roland.schuler@hefr.ch

François Buntschu, francois.buntschu@hefr.ch

Michael Mäder, michael.maeder@hefr.ch

Referenzen

[1]: https://www.srf.ch/news/schweiz/it-sicherheit-von-name-bis-ahv-nummer-sind-die-daten-auf-der-gemeinde-sicher (Von Name bis AHV-Nummer: Sind die Daten auf der Gemeinde sicher?, DE)

[2]: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024 (Global Security Index 2024 – ITU Publications, International Telecommunication Union (ITU), EN)

[3]: https://www.iso27001security.com/html/iso27000.html (About the ISO27k standards, EN)

[4] https://www.cyber-safe.ch/ (Das Schweizer Cybersecurity Label, DE FR)

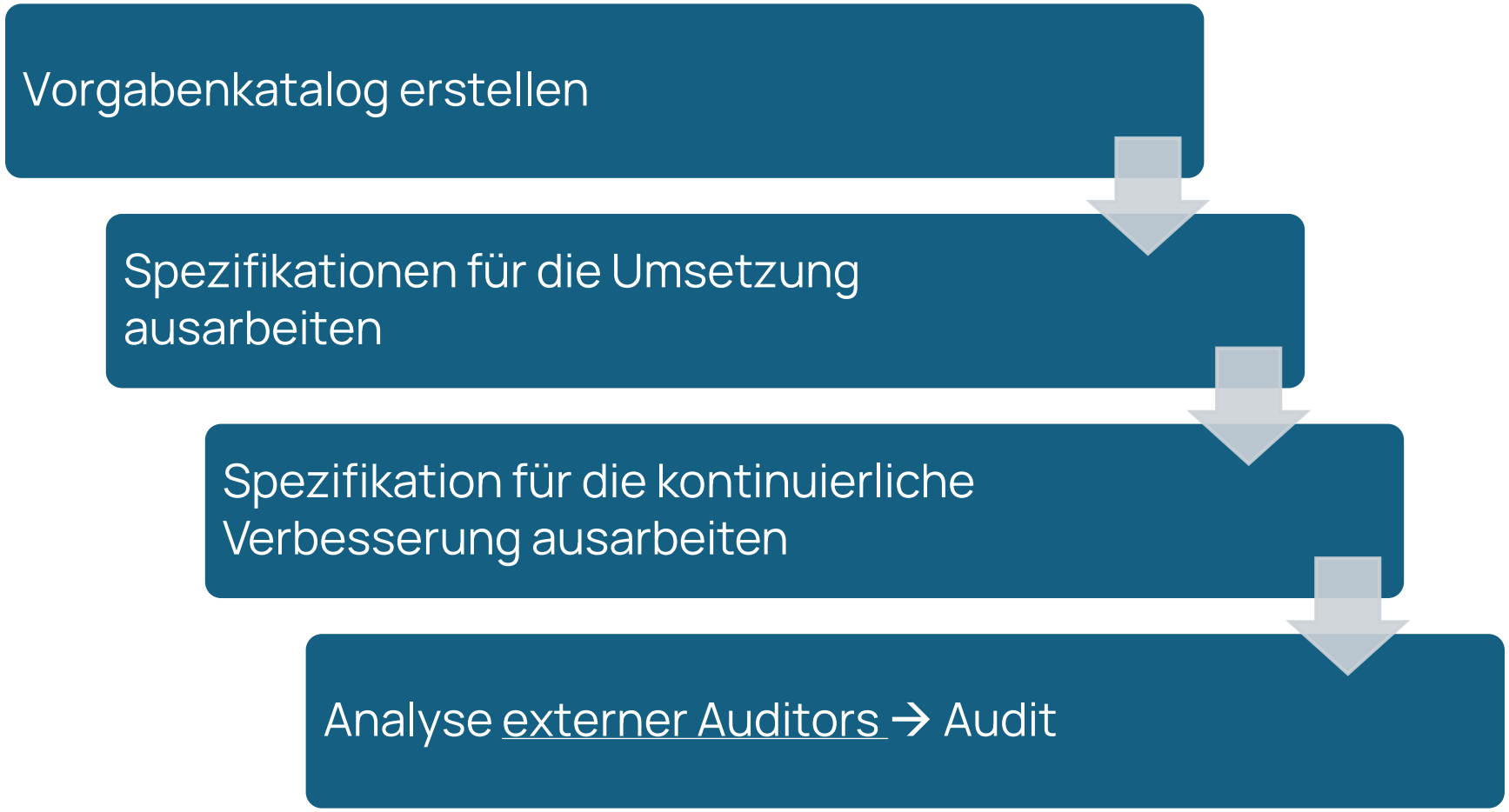
Inhalt

- Audits, Standards, Labels: was bringt das?
- ISO 27k
- CyberSafe, das Schweizer Cybersecurity Label
    - CyberSafe, wie funktioniert das?

Wozu dient ein Audit / Label?

- Bestimmung der aktuellen Cybersicherheit Maturität
- Umsetzung von Verbesserungen
  - Kurzfristig
  - Langfristig (Prozesses)
- Sensibilisierung der Benutzer für Cybersicherheit

Beispiel: Standard ISO27k



About the ISO27k standards

Search

Search this site

Home | ISO27k standards | FREE ISO27k Forum | FREE ISO27k Toolkit | FREE ISO27k FAQ | About us

ISO/IEC 27000
ISO/IEC 27001
ISO/IEC 27002
ISO/IEC 27003
ISO/IEC 27004
ISO/IEC 27005
ISO/IEC 27006
ISO/IEC 27007
ISO/IEC TS 27008
ISO/IEC 27009
ISO/IEC 27010
ISO/IEC 27011
ISO/IEC 27013
ISO/IEC 27014
ISO/IEC TR 27016

The "ISO27k" suite comprises more than seventy standards in the ISO/IEC 27000 series, about fifty of which have been published so far:

1. ISO/IEC 27000:2018 - an overview and introduction to the ISO27k standards plus a glossary for the specialist vocabulary. **FREE!**
2. ISO/IEC 27001:2013 is the **I**nformation **S**ecurity **M**anagement **S**ystem requirements standard, formally specifying a certifiable ISMS. A new version is expected early in 2022.
3. ISO/IEC 27002:2013 is the code of practice for information security describing good practice information security controls. A new version is expected early in 2022.
4. ISO/IEC 27003:2017 provides pragmatic guidance on how to implement ISO/IEC 27001.
5. ISO/IEC 27004:2016 covers information security management measurement.
6. ISO/IEC 27005:2018 covers information [security] risk management.
7. ISO/IEC 27006:2015 is a guide to the process used by accredited ISMS certification bodies to verify and certify ISMS against ISO/IEC 27001. The current standard is being revised and will become part 1, with a new part 2 covering certification of PIMS.
8. ISO/IEC TS 27006:2021 is an accreditation standard for organizations certifying compliance of PIMS against ISO/IEC 27701.
9. ISO/IEC 27007:2020 is a guide to auditing the *management system* elements of an ISMS.
10. ISO/IEC TS 27008:2019 concerns the assessment of 'technical' security controls.
11. ISO/IEC 27009:2020 advises those producing sector- or industry-specific ISO27k standards, in effect an SC 27 internal guideline.

About the ISO27k standards

Search
Search this site

Home | ISO27k standards | FREE ISO27k Forum | FREE ISO27k Toolkit | FREE ISO27k FAQ | About us

ISO/IEC 27000
ISO/IEC 27001
ISO/IEC 27002
ISO/IEC 27003
ISO/IEC 27004
ISO/IEC 27005
ISO/IEC 27006
ISO/IEC 27007
ISO/IEC TS 27008
ISO/IEC 27009
ISO/IEC 27010
ISO/IEC 27011
ISO/IEC 27013
ISO/IEC 27014
ISO/IEC TR 27016

The "ISO27k" suite comprises more than seventy standards in the ISO/IEC 27000 series, about fifty of which have been published so far:

1. ISO/IEC 27000:2018 - an overview and introduction to the ISO27k standards plus a glossary for the specialist vocabulary. **FREE!**
2. ISO/IEC 27001:2013 is the **I**nformation **S**ecurity **M**anagement **S**ystem requirements standard, formally specifying a certifiable ISMS. A new version is expected early in 2022.
3. ISO/IEC 27002:2013 is the code of practice for information security describing good practice information security controls. A new version is expected early in 2022.
4. ISO/IEC 27003:2017 provides pragmatic guidance on how to implement ISO/IEC 27001.
5. ISO/IEC 27004:20[illegible] information security management measurement.
6. ISO/IEC 27005:2018 covers information [security] risk management.
7. ISO/IEC 27[illegible] a guide to the processes conducted by certification bodies to verify and certify ISMS against ISO/IEC 27001. The current standard is being revised and will become part 1, with a new part 2 covering certification of PIMS.
8. ISO/IEC TS 27006:2021 is an accreditation standard for organizations certifying compliance of PIMS against ISO/IEC 27701.
9. ISO/IEC 27007:2020 is a guide to auditing the *management system* elements of an ISMS.
10. ISO/IEC TS 27008:2019 concerns the assessment of 'technical' security controls.
11. ISO/IEC 27009:2020 advises those producing sector- or industry-specific ISO27k standards, in effect an SC 27 internal guideline.

Sehr komplex...
... und daher aufwendig und teuer

Qualitätslabel

CYBER SAFE

Cybersecurity-Diagnose

Wir testen Ihre IT-Systeme, Ihre Mitarbeiter und Ihre Governance, um Lücken und SCHWACHSTELLEN zu identifizieren und eine Bestandsaufnahme Ihrer Cyber-Sicherheit zu erstellen.

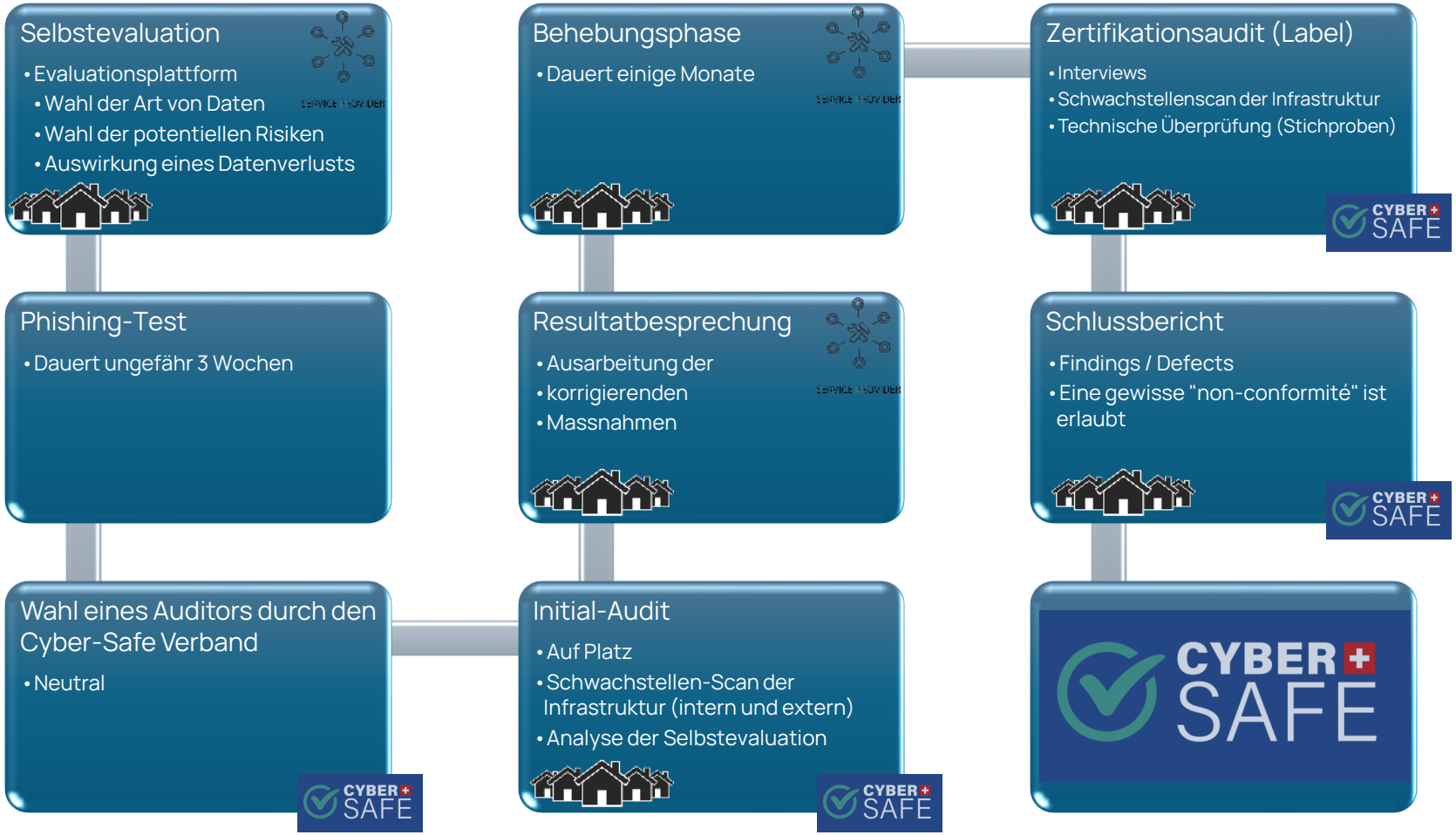
Entscheidungshilfe

Eine Anleitung für das operative Management (Verwaltung der Prioritäten nach Risiken, finanziellen Auswirkungen und Geschäftsbereichen). Basierend auf Ihrer Diagnose, eine PRIORISIERTE LISTE von Maßnahmen zur Verbesserung Ihrer Cybersicherheit.

Cybersecurity-Audit

Wir auditieren Kandidaten und überprüfen, ob die vorgeschlagenen VERBESSERUNGsmassnahmen umgesetzt wurden und prüfen die Umsetzung von Cyber Security-Praktiken und -Prozessen, die den Anforderungen des Labels entsprechen.

CyberSafe, wie funktionniert das?



https://www.cyber-safe.ch

Zusammenfassung

- Bewertung der aktuellen Maturität im Bereich der Cyber-Security
- Einleiten von Verbesserungen
  - Kurzfristig
  - Langfristig (Prozesse, Verhalten, …)
- Sensibilisierung der Mitarbeitenden für die Cyber-Security (Schulungen)
- Überprüfung der Einhaltung der Cyber-Safe Anforderungen

Wie reagiere ich bei einem Verdacht auf einen Angriff oder eine Bedrohung?

Matthieu Landert, Kommissar, Kantonspolizei Freiburg

Sébastien Ruffieux, Brigadenchef, Kantonspolizei Freiburg

Inhalt

- Cyberkriminalität im Kanton Freiburg
- Wie soll man bei einem Verdacht auf einen Angriff oder eine Bedrohung reagieren?
- Die Rolle der Polizei
- Fragen?

Cyberkriminalität im Kanton Freiburg

- Zunahme der Cyber-Fälle (ca. 1700 Fälle mit 14 Mio. Schaden).
- Jeder Fall ist anders, die Szenarien ändern sich, aber sie können zu Phänomenen zusammengefasst werden.
- Nationale und internationale Koordination Zahlreiche Internetlinks, Vorgehensweisen existieren

Wie reagiere ich bei einem Verdacht auf einen Angriff oder eine Bedrohung?

- Gerät isolieren, vom Netzwerk trennen (WLAN, WIFI).
- Wenden Sie sich an
  - Interner IT-Verantwortlicher, Hierarchie
  - Polizei (Strafanzeige, Spurensicherung, Beratung, Verhandlung)

- Melden
  - NCSC (www.ncsc.ch)
  - Gemeindeverband (können ebenfalls demselben Angriff ausgesetzt sein).
  - Meldepflicht - Gesetz über die Informationssicherheit (ISG Art. 74b lit.b)

Wie reagiere ich bei einem Verdacht auf einen Angriff oder eine Bedrohung?

Eigene Organisation in der Gemeinde

- Wer ist verantwortlich / Kontaktperson? Stab für den Krisenfall?
- Den IT-Dienstleister einschalten!
- Vorgesetzte, Mitarbeiter, Partner, usw informieren
- Zusammenarbeit mit der Polizei
- Medienmitteilung vorbereiten

Die Rolle der Polizei

- Analyse der Malware und der beschlagnahmten Daten, Definition der Vorgehensweise, Versuch, die kriminellen Urheber zu identifizieren.
- Technische Beratung durch IT-Spezialisten (keine Reparatur unsererseits!)
- „Coaching“ zur Kontaktaufnahme - Austausch mit den Kriminellen (Verhandlungsgruppe)

Die Rolle der Polizei

- Zusammenarbeit mit anderen Kantonspolizeien, Fedpol, Europol, Interpol (oft gibt es Fallserien).
- Anzeige bei der Staatsanwaltschaft

Fragen ?

Police cantonale POL

Police de sûreté - *Kriminalpolizei*
Commissariat cybercriminalité
Place Notre-Dame 2, 1701 Fribourg
T +41 26 304 17 19, www.policefr.ch I cybercrime@fr.ch

Beispiele in den Gemeinden: *Verfahren und Schulung*

Bruno Marmier, Ammann, Villars-sur-Glâne

Sergio Serras, Informatiker, Villars-sur-Glâne

Inhalt

- Bestandsaufnahme: Infrastruktur und IT-Struktur
- Schulungsmassnahmen für Nutzer (Personal und Politik)
- Wiederherstellungsverfahren
- Label CyberSafe
- Risikomanagement

Bestandsaufnahme: Infrastruktur und IT-Struktur

- *Unterschied nach Gemeindegrössen*
- *Sicherheitsrelevante Fragen sind identisch*

Schulungsmassnahmen für Nutzer (Personal und Politik)

- *Erinnerung an gesetzliche und vertragliche Bestimmungen*
- *Sensibilisierungskampagnen zu bewährten Praktiken (Passwörter, Spam erkennen, …)*
- *Praktische Übungen - Quiz*

Wiederherstellungsverfahren

Wir möchten Hackerangriffe vermeiden.
Aber wir müssen uns auf den Fall vorbereiten:

- *Verfahren vorsehen (Krisenteam, wen informieren? …)*
- *Auflistung der betroffenen Aufgaben und Vorschläge für Lösungen*
- *Was ist mit dem Personal im Falle eines Hacks?*

Label Cybersafe

- *Mehrwert des Labels Cybersafe?*

Risikomanagement

- *Der Beauftragte muss alle nötigen Massnahmen im Bereich der IT-Sicherheit ergreifen (Referenzpunkte, Risikomanagement, internes Kontrollsystem)*

- *Aber 95% der Fehler sind von Menschen gemacht*

Fragen – Bemerkungen?

Toolbox Cybersicherheit

Wegleitung Cybersicherheit