Association Suisse pour le Label de Cybersécurité

Cybersécurité : êtes-vous suffisamment protégés ?

UCV, 3 septembre 2020, Echallens

Plan de la soirée

I. Présentation de l'Association et du Label

II. Retour d'expériences /projet pilote avec l'UCV

III. Atelier cybersécurité pour les communes

I. Présentation de l'Association et du Label

L’association - origines

- Créé en 2018 par 9 membres fondateurs

- Constats:
  - Importance grandissante de la cybersécurité
  - Petites et moyennes organisations démunies (65% vs. 1%)
  - Barrières: prise de conscience, coûts, compétences, incertitudes.

- La sensibilisation: nécessaire mais pas suffisante; quelles incitations?

L’association - objectifs

➔ Un label pour aider les PMO à atteindre un niveau de cybersécurité acceptable

- Abaisser les coûts:
  - Pragmatisme (loi de Pareto)
  - Solution simples, documentation
- Rendre accessible la cybersécurité
  - Traduire la cybersécurité en CHF; aide à la décision et feuille de route
  - Etablir un pont entre les PMO et le monde de la cybersécurité (participation)
- Modèle incitatif
- Neutralité et indépendance

L’association - qui

- Monde économique, politique, académique et associatif
- 8’500 PME et > 300 communes représentées
- Partenaire en CH-D:

ISSS Information Security Society Switzerland

GIM-CH Groupement suisse de l’industrie mécanique
SWISSMECHANIC Suisse romande

SKO ASC ASQ Association suisse des cadres

heig-vd

.ICØN

EPFL

Hes·so

UNION DES COMMUNES VAUDOISES

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

CVCI Chambre vaudoise du commerce et de l’industrie

CCIG Chambre de commerce, d’industrie et des services de Genève

Chambre Valaisanne de Commerce et d’Industrie
Walliser Industrie- und Handelskammer

FPE-CIGA Fédération Patronale et Économique

frc

Fédération des Entreprises Romandes Neuchâtel

Le Label - approche

- Définition collective des exigences: par et pour les PMO
- Un comité de pilotage
  - Une Commission de normalisation
- Les exigences varient selon le niveau d'impact des cyber incidents de l'organisation candidate.
- **Crédibilité** et **neutralité**: pas de vente de mesures de remédiations (association et auditeurs).
- Exigences publiées en *Creative Commons* (DE + FR)
- Outil en ligne et évaluation basés sur les exigences

Le Label - processus

Evaluation de l'existant

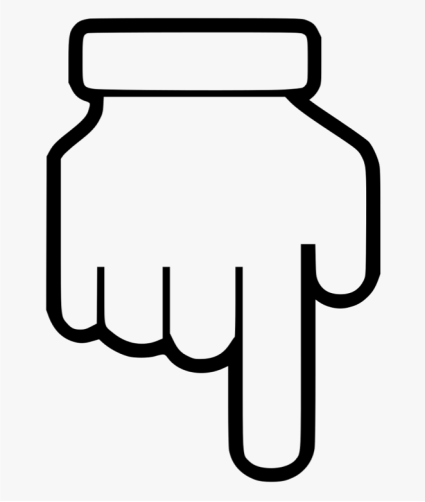
- des compétences : (phishing, 6x)
- de l'organisation (questionnaire dynamique)
- de l'infrastructure IT (scans de vulnérabilités interne et externe)

Amélioration

- Calcul du cyber-risque => score en CHF
- Plan de route à appliquer

Suivi pendant 2 ans

- Scans de vulnérabilités
- Phishing



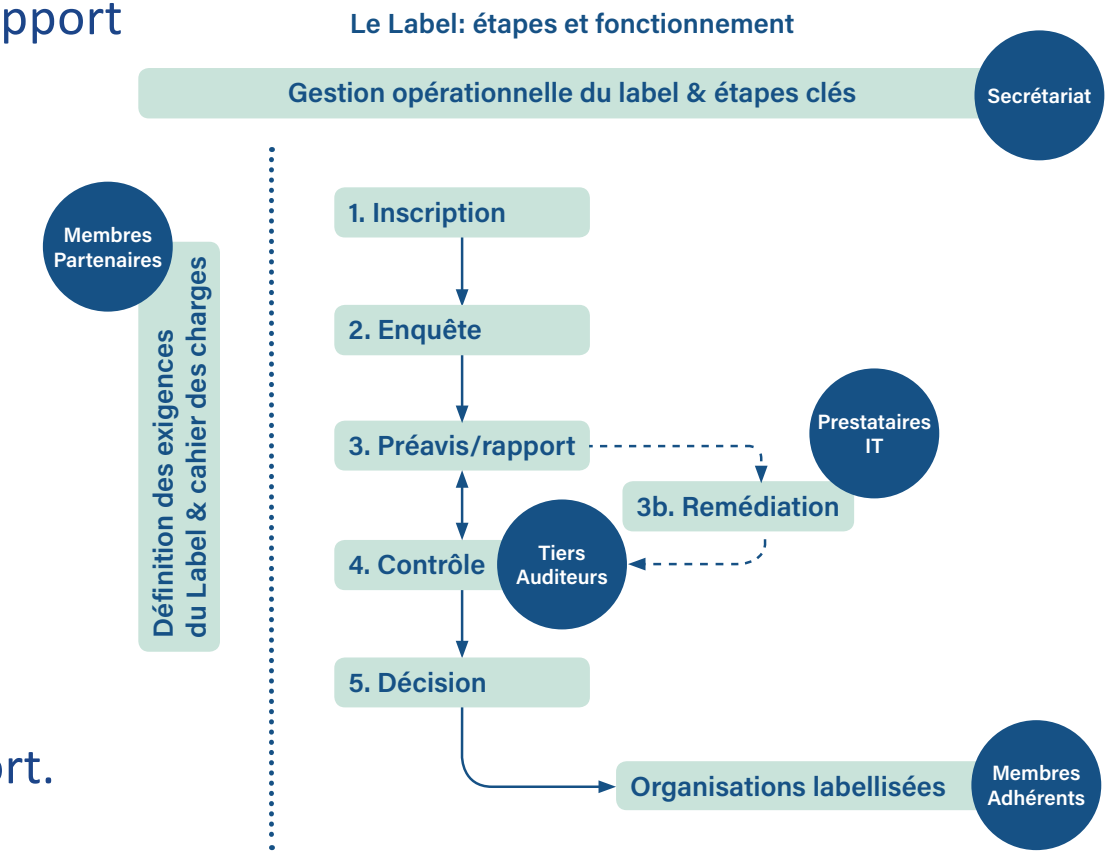
Outil gratuit en ligne :

www.cyber-safe.ch

Le Label – étapes

- Questionnaire gratuit (en ligne) et rapport préliminaire

  Si intérêt à poursuivre:
- Accompagnement (présentiel):
  - scans réseaux
  - collecte e-mails
- Campagne de phishing
- Rapport final
  - Niveau de risque
  - Remédiations exigées et priorités
- Période de mise en œuvre
- Audit (présentiel 0.5 à 1.5 j) et rapport.
- Décision d'octroi du Label
- *Mesures de suivi (2ans)*



Le Label - tarifs

- Fonction du nombre de PC de la commune

  3’000 CHF pour 3 PCs
  9’900 CHF pour 249 PCs

-> inclus questionnaire, scans, phishing, audit et suivi sur 2 ans

- Calcul du prix disponible en ligne
- Rabais partenaires

II. Retour d'expériences: projet pilote avec l'UCV

www.cyber-safe.ch

Le projet pilote avec l'UCV

UNION DES COMMUNES VAUDOISES

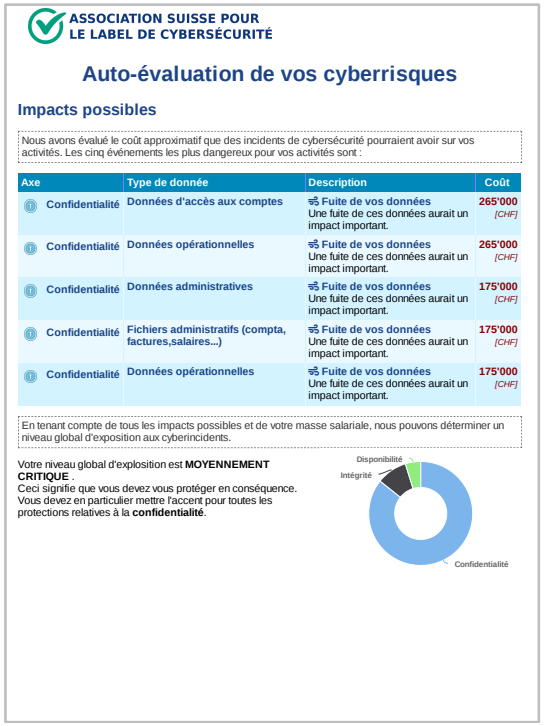
- Participation à l'élaboration des exigences (cahier des charges)
- 3 Labels **offerts**
- 3 communes pilotes membres de l'UCV :
  - Tailles variées (9'000, 1'500, 1'000)
  - Gestion à l'interne ou à l'externe de l'IT, mutualisation
  - Sensibilités variées à la thématique:

    « Nos données sur les citoyens ont-elles de la valeur? »

Le(s) rapport(s)

UNION DES COMMUNES VAUDOISES

- Questionnaire – quid de la valorisation des données
- Connaissance de l'IT et de l'organisation communale



ASSOCIATION SUISSE POUR LE LABEL DE CYBERSÉCURITÉ

Auto-évaluation de vos cyberrisques

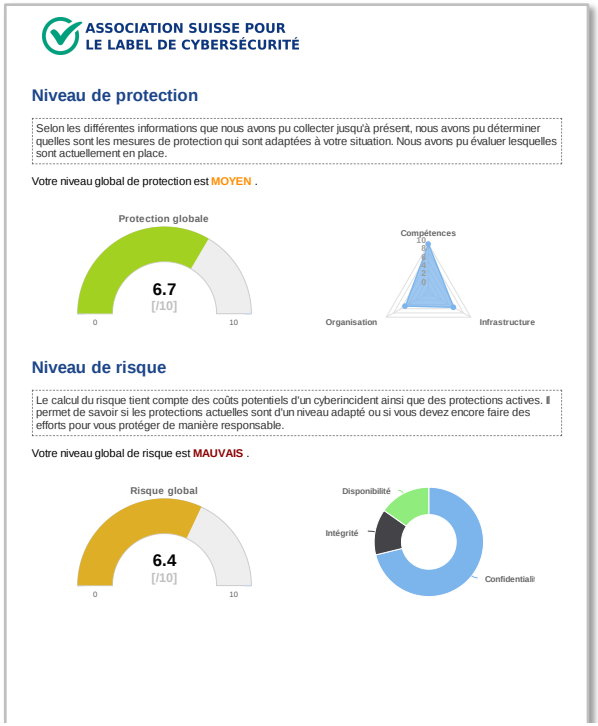
Impacts possibles

Nous avons évalué le coût approximatif que des incidents de cybersécurité pourraient avoir sur vos activités. Les cinq événements les plus dangereux pour vos activités sont :

Axe	Type de donnée	Description	Coût
Confidentialité	Données d'accès aux comptes	Fuite de vos données Une fuite de ces données aurait un impact important.	265'000 *[CHF]*
Confidentialité	Données opérationnelles	Fuite de vos données Une fuite de ces données aurait un impact important.	265'000 *[CHF]*
Confidentialité	Données administratives	Fuite de vos données Une fuite de ces données aurait un impact important.	175'000 *[CHF]*
Confidentialité	Fichiers administratifs (compta, factures,salaires...)	Fuite de vos données Une fuite de ces données aurait un impact important.	175'000 *[CHF]*
Confidentialité	Données opérationnelles	Fuite de vos données Une fuite de ces données aurait un impact important.	175'000 *[CHF]*

En tenant compte de tous les impacts possibles et de votre masse salariale, nous pouvons déterminer un niveau global d'exposition aux cyberincidents.

Votre niveau global d'explosion est **MOYENNEMENT CRITIQUE** .
Ceci signifie que vous devez vous protéger en conséquence. Vous devez en particulier mettre l'accent pour toutes les protections relatives à la **confidentialité**.



ASSOCIATION SUISSE POUR LE LABEL DE CYBERSÉCURITÉ

Niveau de protection

Selon les différentes informations que nous avons pu collecter jusqu'à présent, nous avons pu déterminer quelles sont les mesures de protection qui sont adaptées à votre situation. Nous avons pu évaluer lesquelles sont actuellement en place.

Votre niveau global de protection est MOYEN .

Niveau de risque

Le calcul du risque tient compte des coûts potentiels d'un cyberincident ainsi que des protections actives. Il permet de savoir si les protections actuelles sont d'un niveau adapté ou si vous devez encore faire des efforts pour vous protéger de manière responsable.

Votre niveau global de risque est MAUVAIS .

ASSOCIATION SUISSE POUR LE LABEL DE CYBERSÉCURITÉ

Vos priorités en un coup d'oeil

Voici, par ordre de priorité, les prochaines étapes que nous vous suggérons d'implémenter:

Priorité	Action	Détail	Requis	Coût	Effort
TRÈS HAUTE	Corriger les vulnérabilités critiques du réseau interne	Plusieurs vulnérabilités critiques existent sur votre réseau interne. Les détails se trouvent dans l'annexe. Dans la plupart des cas il s'agit d'effectuer une mise à jour des systèmes concernés.	Oui doc	$	15,0 *[h]*
HAUTE	Contrôler la sauvegarde	En cas de coup dur votre sauvegarde pourrait être salvatrice. Vérifiez qu'elle se passe correctement.	Oui doc	$$	5,0 *[h]*
HAUTE	Installer, mettre à jour et contrôler les antivirus	Les anti-virus sont des vaccins pour votre informatique. Vous devez vous assurer qu'ils sont installés sur chaque poste de travail et qu'ils sont bien mis à jour.	Oui doc	$$	20,0 *[h]*
HAUTE	Appliquer et contrôler les mises à jour des systèmes d'exploitation	Les mises à jour des systèmes d'exploitation des appareils contiennent des correctifs de sécurité. Vous devez veillez à ce que les mises à jour soient correctement appliquées.	Oui doc	$	20,0 *[h]*
HAUTE	Faire un test de récupération	La seule sauvegarde valable est celle qui vous permet de récupérer vos données. Vous devez régulièrement vérifier que ce soit bien possible.	Oui doc	$	18,0 *[h]*
HAUTE	Vérifier le fonctionnement	Il est important que votre pare-feu soit fonctionnel et à jour pour détecter les comportements	Oui doc	$	35,0 *[h]*
HAUTE					
HAUTE	Appliquer une politique de complexité des mots de passe	Il arrive encore trop souvent que des attaquants arrivent à voler les empreintes de vos mots de passe. Lors ceux-ci sont de moins de 10 caractères il leur est facile de les deviner. Pour éviter cela vous devez appliquer une politique de complexité dans votre système.	Oui doc	$	6,0 *[h]*
HAUTE	Limiter	La première action d'un pirate est de trouver et	Oui	$	20,0

[OSVDB:142291] The SSH service running on the remote host is affected by multiple vulnerabilities.
Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
Niveau de criticité : 10,0
Sur les hôtes suivants : *NBG6617.local*

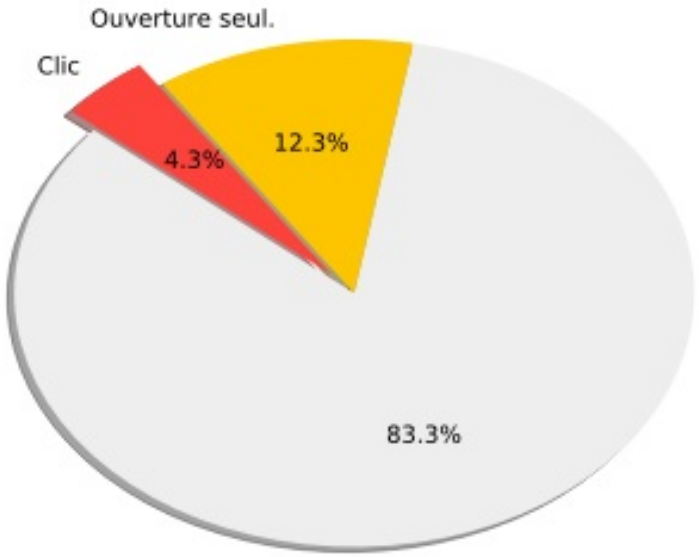
Le Label – pilote UCV

UNION DES COMMUNES VAUDOISES

- Principaux résultats:
  - Infrastructure IT: détection de vulnérabilités hautement critiques (2/3)
  - Phishing: 20% de clics sur certaines tentatives.
  - Organisation: charte utilisateurs, tests de récupération, localisation et inventaire des données, politique de sécurité des SI, plan de reprise (DRP).
- 1 commune en phase d'obtenir le Label
- 1 commune: changement de stratégie (collaboration intercommunale)
- 1 commune: audit auprès du prestataire (spécialisé commune)

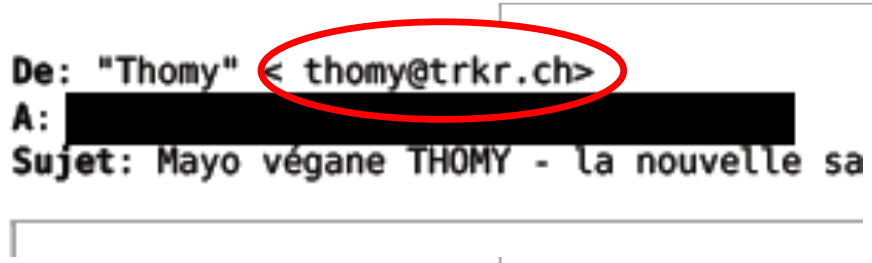
Détail des résultats - phishing

Plus de 20% de clics sur les tentatives plus « ciblées »!



Date	Email	Ouvert.	Clics
07/02/2020	A ne pas manquer: des articles de marque à tout petits prix!	12	9
09/02/2020	Les ventes privées de tous les sports !	13	3
12/02/2020	Grand concours digitec.ch - Gagnez un Panasonic !	21	3
14/02/2020	Une nouvelle machine à café pour le bureau ?	17	8
18/02/2020	Comment scorer sur Tinder	20	2
19/02/2020	Demande de remboursement	22	12

Détail des résultats - phishing



Ne mordez pas à l'hameçon:

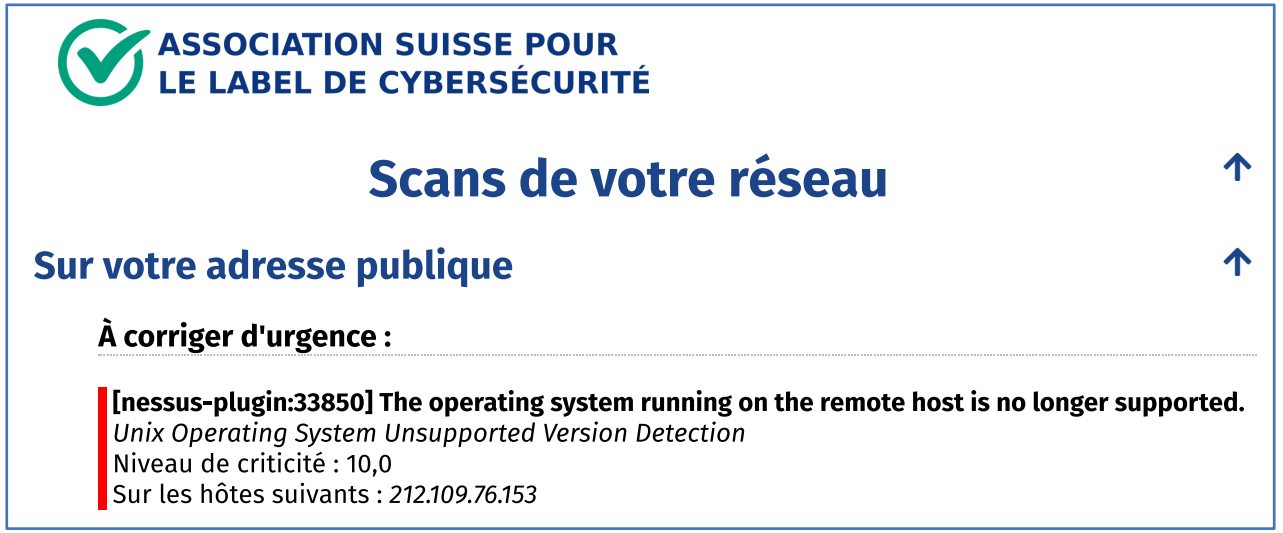
- *Vérifiez l'adresse email*
- *Incohérences?*

Détail des résultats – scans réseaux

- Infrastructure IT: détection de vulnérabilités hautement critiques
  - Score CVSS (Common Vulnerability Scoring System)
  - Exigence cyber-safe.ch: pas de faille avec un score ≥ 9
  - = faille connue et facilement exploitable!

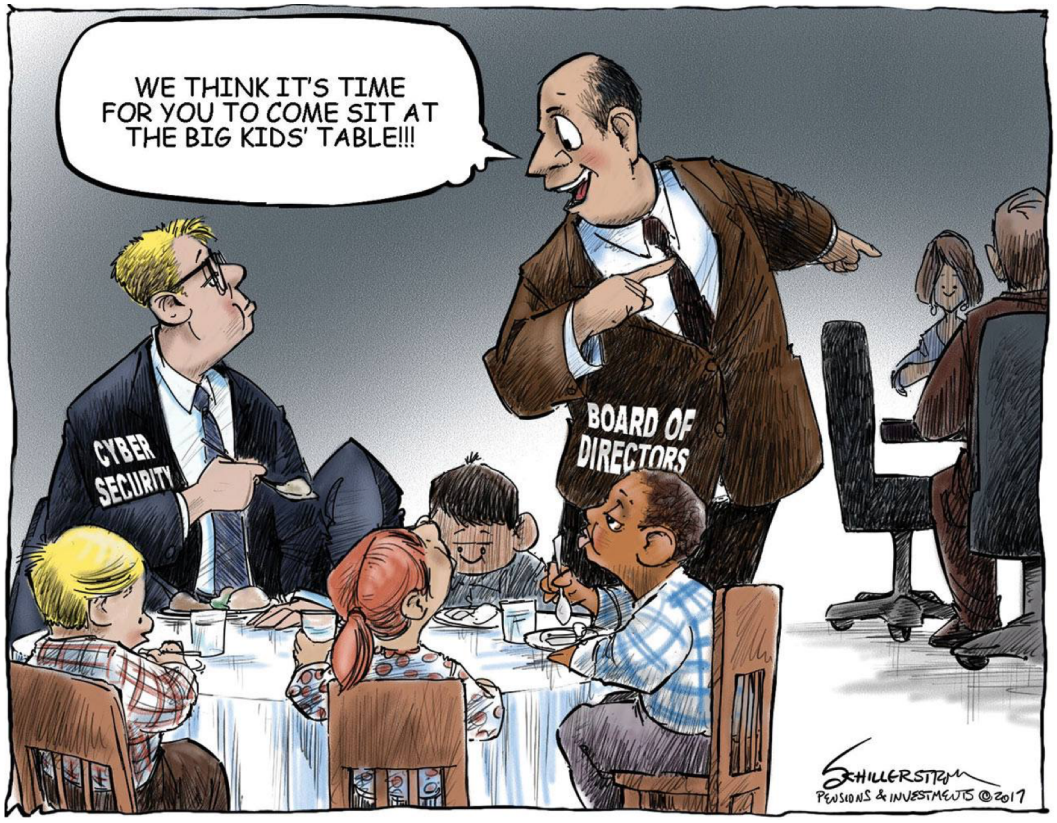
- 2/3 des organisations avec des vulnérabilités hautement critiques

- Mesures de correction (en cours)



Principaux résultats – mesures organisationnelles

- « Charte utilisateur » signées, politique de sécurité des SI
- Tests de récupération
- Localisation et inventaire des données
- Plan de reprise des activités (Disaster Recovery Plan)



Valeur ajoutée et impacts

- Prise de conscience (les bonnes questions)
- Connaissance fine de la situation
- Définition des priorités
- Initiation d'une réflexion stratégique
- Evaluation indirecte du prestataire
- Justification (budgets alloués et/ou demandes)
- Adaptations de l'outil en ligne (côté ASLaC) pour une meilleure prise en compte des spécificités des communes (cat. de risque)

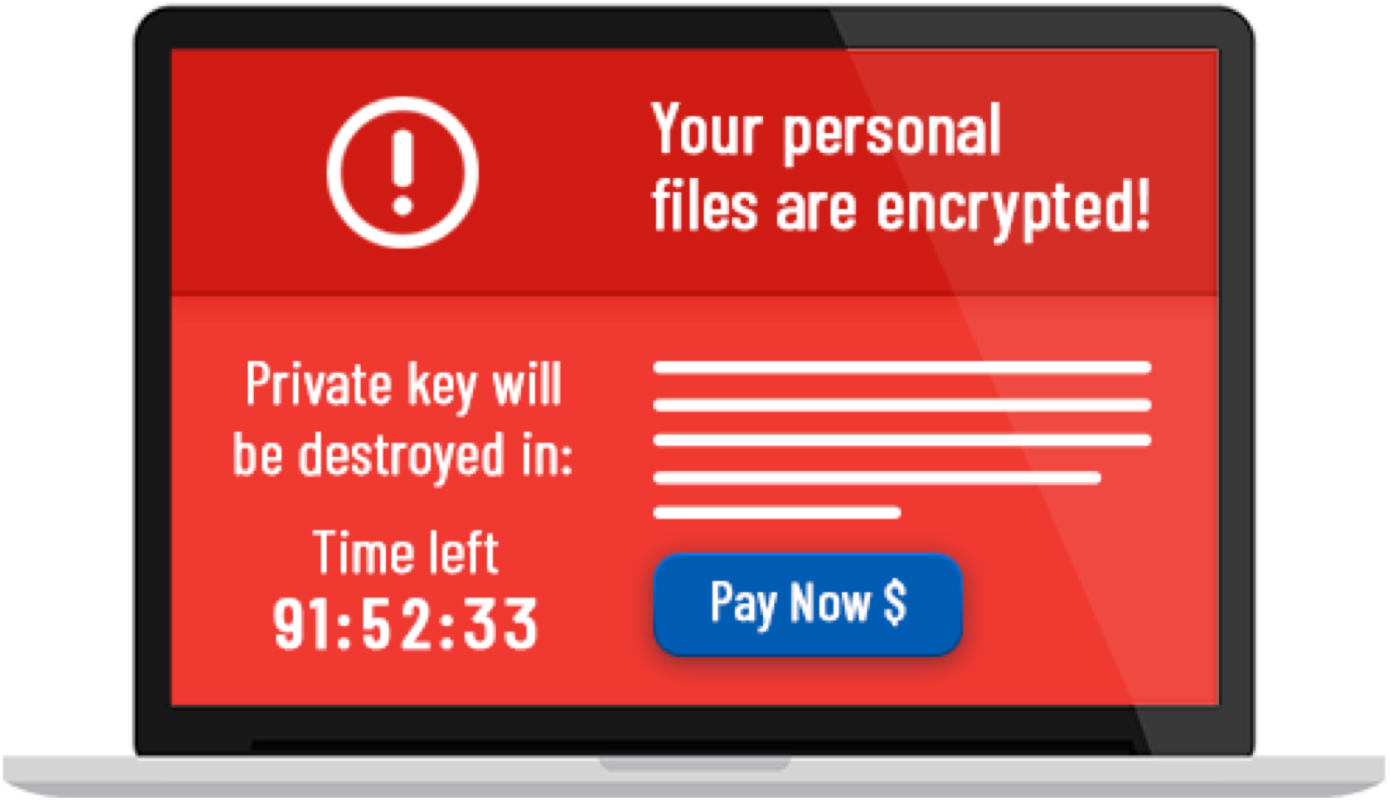
Développements en cours pour les communes

- Projet au niveau Suisse (09.2020 – 09.2021)
  - Avec le soutien de la Confédération, du Réseau National de Sécurité (RNS) et Association des Communes Suisses (ACS)
  - Choix de 15 communes (CH-D) et conduite du processus de labellisation
  - Rapports individuels (confidentiels) et rapport d'ensemble (public)
  - Opportunité d'étendre l'expérience dans le cadre de la stratégie de la Confédération (SNPC 2018-2022).

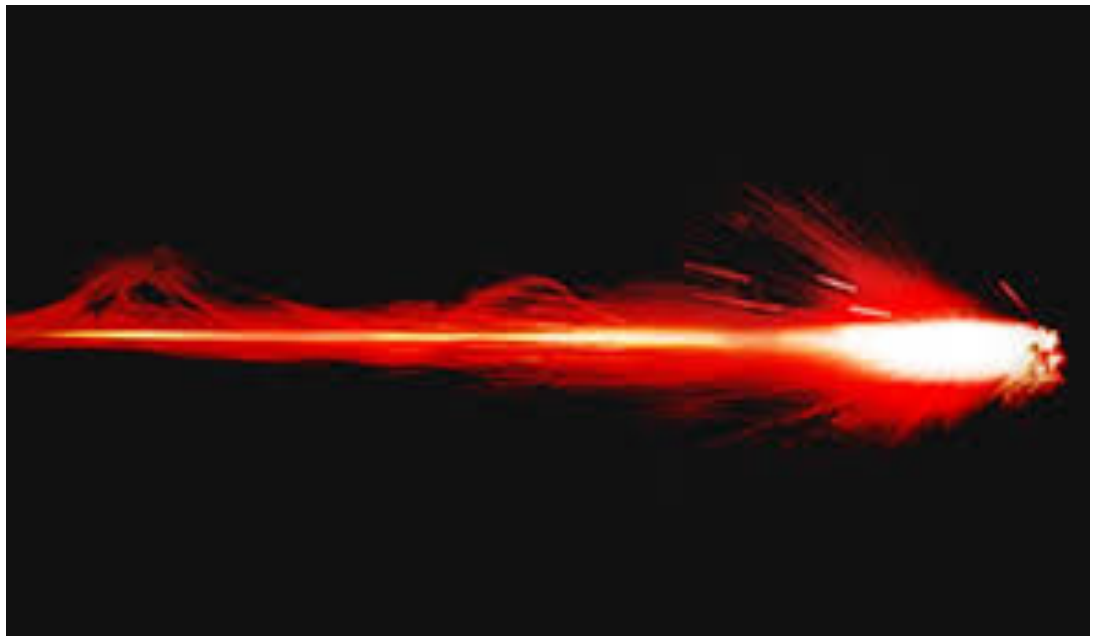
III. Atelier: la cybersécurité, par où commencer?

Démonstration...

Imaginez que le hacking soit a portée de tous...



À vous de jouer !



1. Que faites-vous? Définissez vos 5 premières actions

Et pour encore mieux s'y préparer:

2. Quels sont les deux types de données

   (de fichiers) que vous récupérez en premier ?

3. Sur la base de votre réponse à la Q2, remplissez le tableau suivant:

Fiche de réflexion sur les dangers

Trouvez dans votre organisation quels sont les biens qui doivent être protégés et effectuez selon chaque axe une évaluation des dangers.
Notez chaque danger avec une note de 0 à 5, 0 étant un impact nul et 5 catastrophique.

Bien concerné	Confidentialité	note	Intégrité	note	Disponibilité	note
Exemple : le carnet d'adresse	Un concurrent obtient une copie des adresses de tous nos clients.	4	Erreur de saisie d'un collaborateur, le numéro du client principal est faux.	1	Activation d'un crypto virus, toutes les données sont inaccessibles jusqu'au moment de récupération de la sauvegarde.	2

Merci pour votre participation!

Questions et renseignements complémentaires:

chauert@cyber-safe.ch
www.cyber-safe.ch