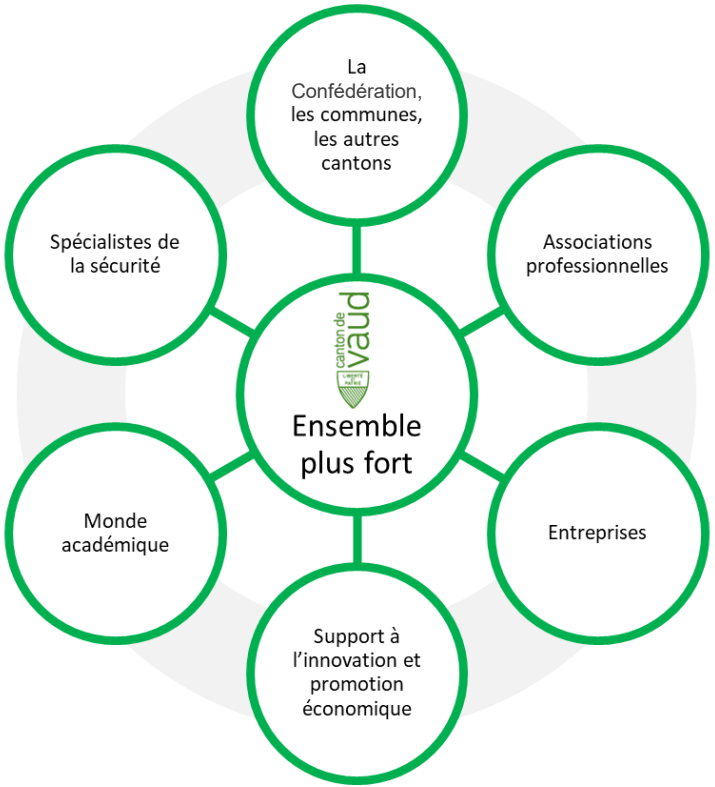
Assemblée générale AdCV, Denens

PLUS FORT CONTRE LES CYBERRISQUES

Direction générale du numérique et des systèmes d'information
Avenue de Longemalle 1, CH-1020 Renens
Tél: +41 21 316 26 00

Un rôle actif pour fédérer et réunir les efforts

#compétenceslocales #ensembleplusfort



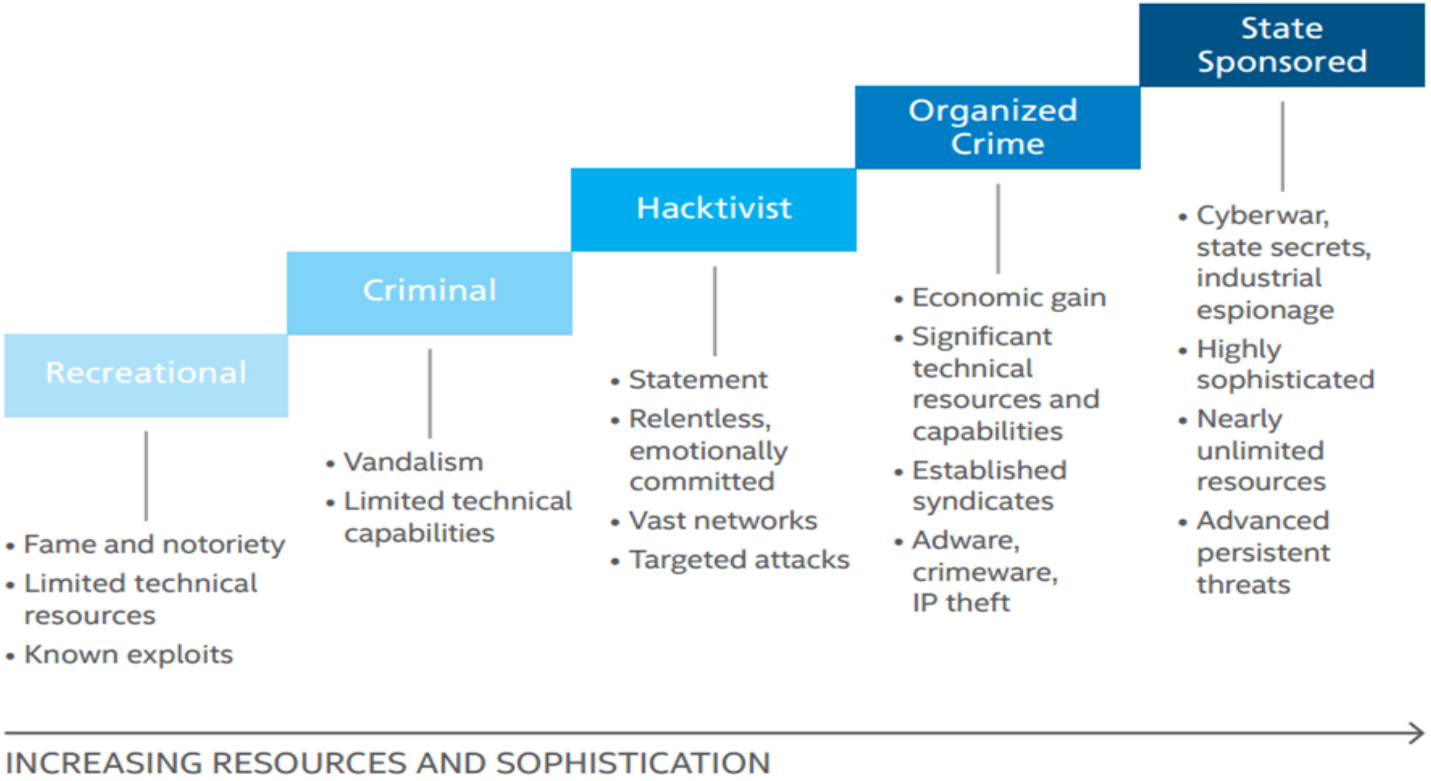
Classification : Publique

Direction générale du numérique et des systèmes d'information
Avenue de Longemalle 1, CH-1020 Renens
Tél: +41 21 316 26 00

Les 3 axes d'action de la stratégie cantonale de cybersécurité

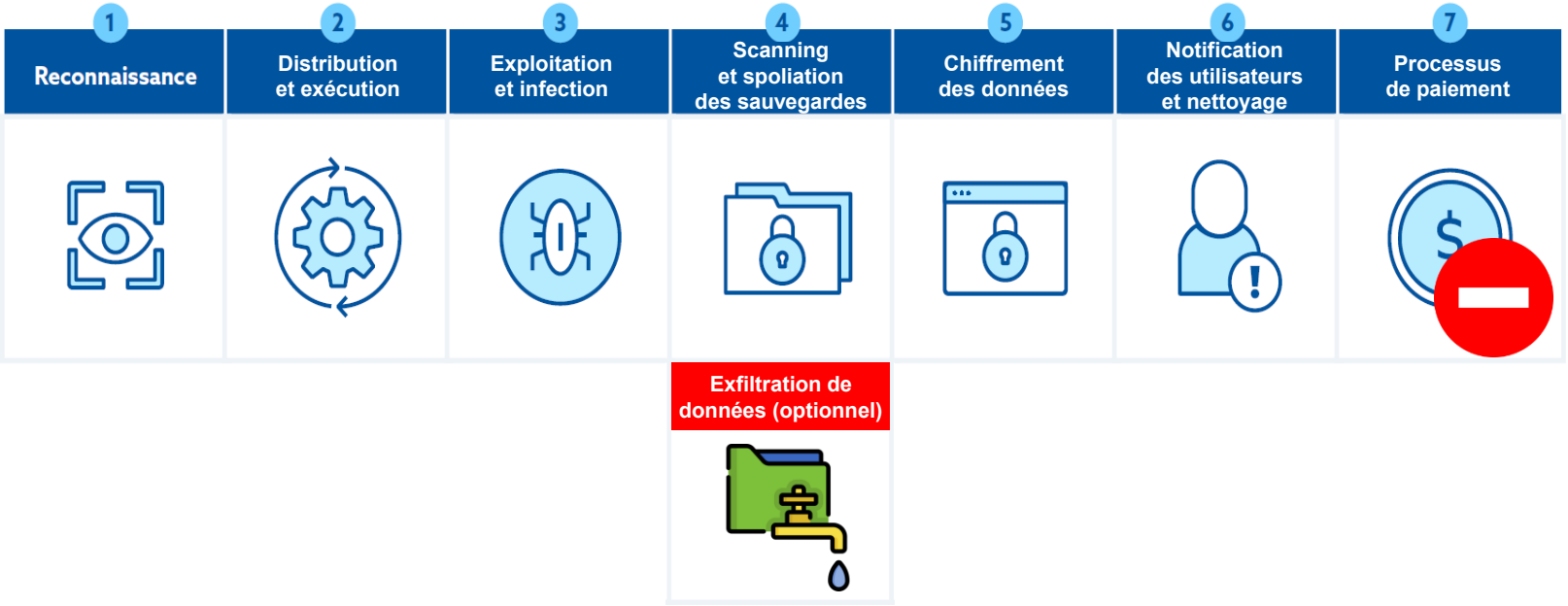
Direction générale du numérique et des systèmes d'information
Avenue de Longemalle 1, CH-1020 Renens
Tél: +41 21 316 26 00

Les attaquants…



Source : Security Intelligence IBM

Les 7 étapes typiques d'une cyberattaque «rançongiciel»



Source de l'illustration : Cloud Security Alliance (publication Ransomware in the Healthcare Cloud, 2021)

Une réponse, 2 plans de continuité à activer et coordonner

CYBER
RÉACTION

Rupture de services informatiques / cyber-attaque

1 Plan de continuité des activités - PCA

Assurer la continuité des activités critiques de l'entité sans IT

2 Plan de secours informatique - PSI

Réactiver les services IT dans les meilleurs délais avec le minimum de perte de données

La gestion des cyberattaques avec le support du Canton

Légende: Canton | Commune, Paraétatique

Fonctionnement normal – hors crise

Annonce via 117 (unité cybercrime)

Fonctionnement en crise

CYBER **RÉACTION**

Municipalité, direction de l'entité

Cellule de crise

Municipalité, direction de l'entité
Décisions, validations

Structure de conduite de crise
Coordination et support à la gestion de crise

EMCC
VaudCERT (SOC)
Cybercrime (PolCant)

Support pour réponse technique

Experts pour réponse technique
Avec partenaire privé pour prise en charge de la réponse technique

Equipes IT — *Corrections et réparations* — Equipes IT

Prestataires IT — *Selon services contractualisés* — Prestataires IT

Principales parties prenantes externes à intégrer / coordonner en cas de crise

- *GovCERT, NCSC*
- *Etat de Vaud*
- *Confédération*
- *APDI*
- *Médias - Presse*
- *Collaborateurs*
- *Administrés*
- *Cybercriminels*

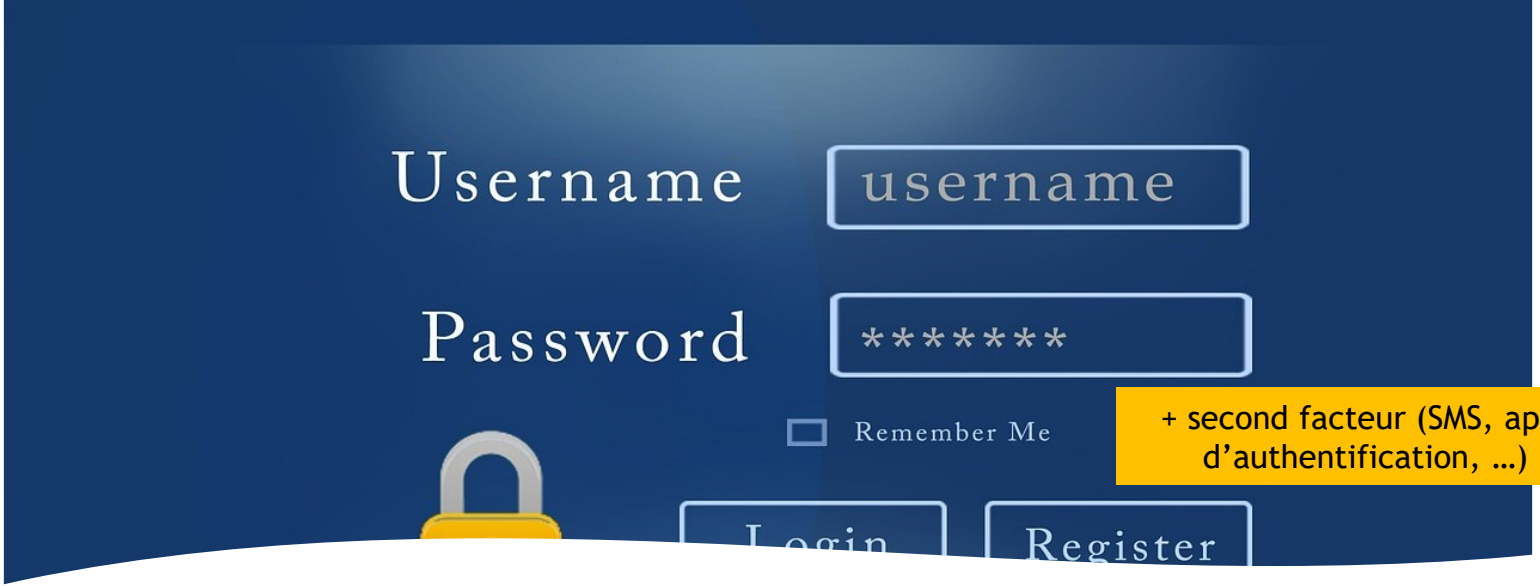
Direction générale du numérique et des systèmes d'information
Avenue de Longemalle 1, CH-1020 Renens
Tél: +41 21 316 26 00

Classification : Publique

UNE APPLICATION MOBILE POUR FAIRE FACE AUX CYBERRISQUES

→ www.vd.ch/cybersecurite

5 bonnes pratiques contre les ransomwares



+ second facteur (SMS, app. d'authentification, …)

L'AUTHENTIFICATION FORTE EST AUJOURD'HUI UNE OBLIGATION POUR LES ACCÈS À DISTANCE

Les 5 principales protections contre les cyberattaques

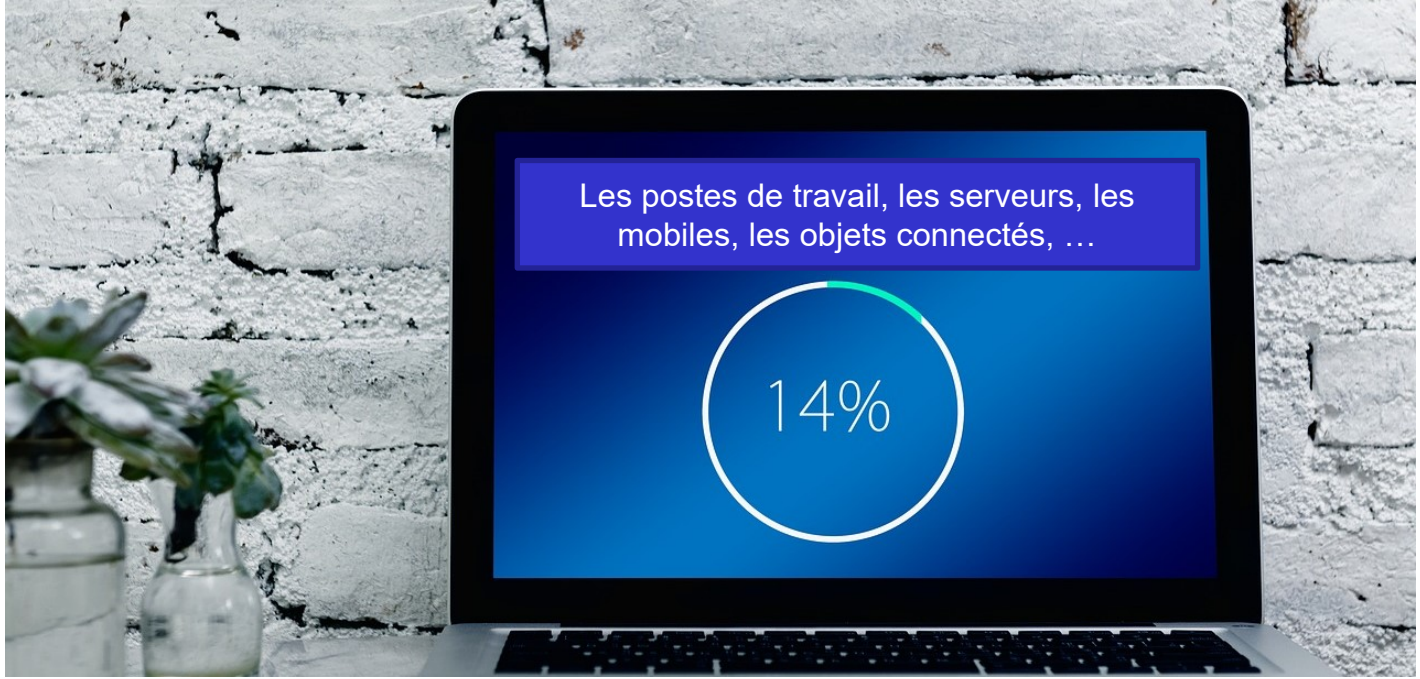
Sécurisation des accès à distance:
Les accès à distance, comme le VPN ainsi que tous les autres accès aux ressources internes doivent **obligatoirement** être sécurisés avec un second facteur (authentification forte).

L’IMPORTANCE VITALE D’AVOIR DES SAUVEGARDES “DÉCONNECTÉES”

Les 5 principales protections contre les cyberattaques

Sauvegardes hors ligne:
Créez régulièrement des copies de secours de vos données.

Assurez-vous à chaque fois que le canal sur lequel vous effectuez les copies de secours soit physiquement séparé de l'ordinateur et du réseau, et protégé après l'opération de sauvegarde.



LES MISES À JOUR CORRIGENT DES FAILLES DE VULNÉRABILITÉS RECHERCHÉES PAR LES CYBERCRIMINELS

Les 5 principales protections contre les cyberattaques

Gestion des correctifs et des cycles de vie: En matière de sécurité, tous les systèmes doivent être systématiquement et régulièrement mis à jour. Les logiciels ou les systèmes qui ne sont plus actualisés par le fabricant (fin de vie) doivent être désactivés ou transférés dans une zone du réseau séparée et isolée.

LA MESSAGERIE EST UN VECTEUR D'ATTAQUE TRÈS UTILISÉ PAR LES CYBERCRIMINELS

Les 5 principales protections contre les cyberattaques

Blocage des pièces jointes et des liens à risque dans les courriels:
Bloquez la réception de pièces jointes dangereuses sur votre messagerie, y compris les **documents Office avec macros**. Sensibilisez et formez vos collaboratrices.teur.s à reconnaître les courriels suspicieux, par exemple avec des exercices de prévention du phishing

Direction générale du numérique et des systèmes d'information
Avenue de Longemalle 1, CH-1020 Renens
Tél: +41 21 316 26 00

UNE SURVEILLANCE CONTINUE EST NÉCESSAIRE POUR RÉAGIR RAPIDEMENT ET RÉDUIRE LES IMPACTS D'UNE CYBERATTAQUE

Les 5 principales protections contre les cyberattaques

Surveillance des fichiers journaux (logs), en particulier de l'accès à distance:
Une surveillance continue de l'environnement IT est nécessaire pour réagir rapidement et réduire les impacts d'une cyberattaque.

Les cyberrisques sont l'affaire de tous : privés, entreprises et administrations

Ensemble
Soyons plus forts !

Ensemble
Soyons cyberrésilients !