Webinaire numérique dans les collectivités

La confiance numérique

AGATE
AGENCE ALPINE
DES TERRITOIRES

SOMMAIRE

AGATE
AGENCE ALPINE DES TERRITOIRES

01

Introduction

AGATE
AGENCE ALPINE
DES TERRITOIRES

Introduction

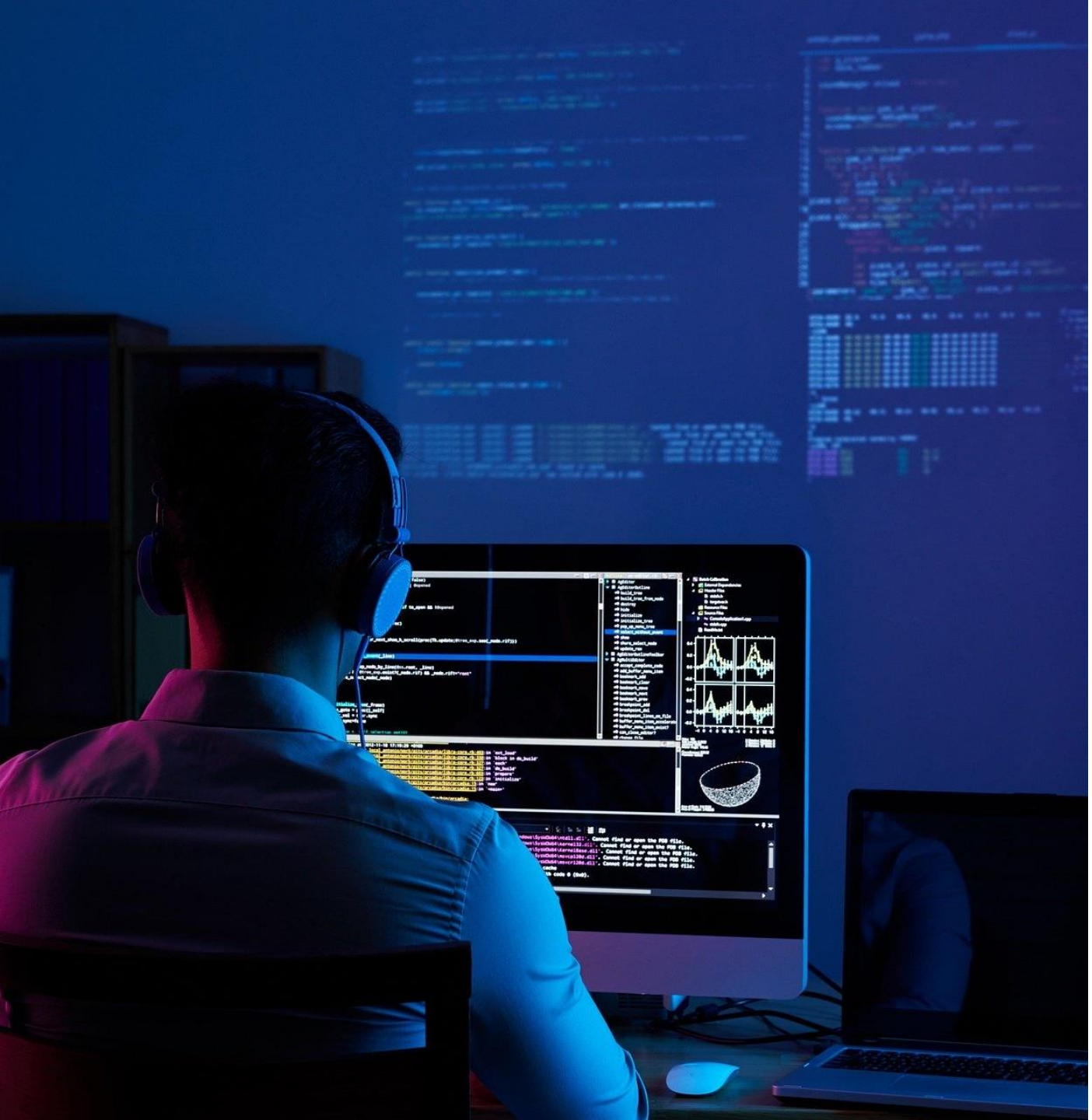
1. Pourquoi Agate et la « confiance numérique » ?

2. Présentation des intervenants de ce webinaire

02

Risques et menaces en matière de numérique

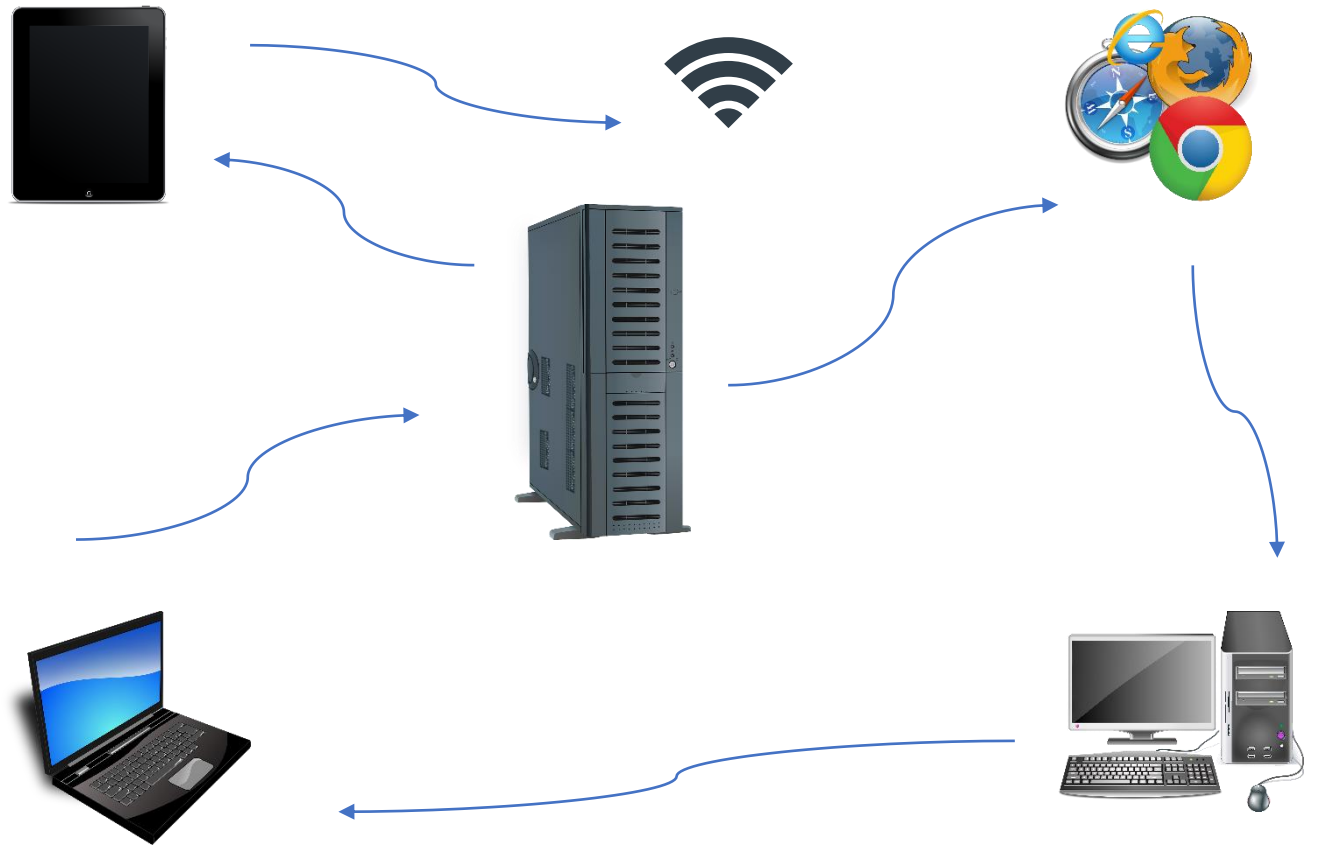
AGATE
AGENCE ALPINE DES TERRITOIRES



LES RISQUES LIÉS AUX OUTILS INFORMATIQUES

La cybersécurité, un mot qui fait peur !
Mais elle concerne avant tout les utilisateurs, car chaque intervenant peut influer sur la sécurité du système d'information.

Savez-vous ce qu’est un Système d’Information ?



L’informatique

1982
Les unités Centrales
IBM développe les unités de traitements de données.

1984
Sauvegarde
Création des disques et bandes pour transférer les données entre unités.

1996
Système d’Information
Les premiers terminaux connectés entre eux (minitel, fax, etc).

1997
Réseau Mondial
Les Télécoms, ont déployé massivement leur réseau.

2010
L’ère de la connexion
Les objets du quotidien deviennent connectés (Téléphone, Voiture, Electroménager, etc).

2021
Le Cloud
Les données sont accessibles en tout temps, tout lieux, sur tous les appareils !

Un monde ultra-connecté !

PLUS DE CONNEXIONS = RISQUES

Chaque connexion permet une intrusion,
et dans un monde ou tout devient connecté, les systèmes d'informations deviennent vulnérables.

DÉCOUVRONS COMMENT
LES PROTÉGER AU MAXIMUM !

L’accès aux données

02
PUBLIQUE

Les réseaux sociaux, forum, blog exposent nos données en ligne. Adresse mail, pseudonyme, et même parfois nom réel.

03
EN ENTREPRISE

Pour faciliter la production et l’échange, les entreprises et administrations disposent de leur propre système d’information pour communiquer.

01
PERSONNEL

Nous avons presque tous un système d’information personnel à la maison. Box ADSL, Imprimante, Ordinateur, etc.

04
CACHÉ

Certains réseaux sont « cachés » comme le bluetooth, qui relie toutefois plusieurs appareils, mais offre un terrain d’attaque particulier (Montre, Lunette, Voiture, etc).

Les données échangées

API

Sont utilisées pour interconnecter plusieurs services et/ou applications entre elles. Elles se chargent de faire transiter les données d'un service à l'autre.

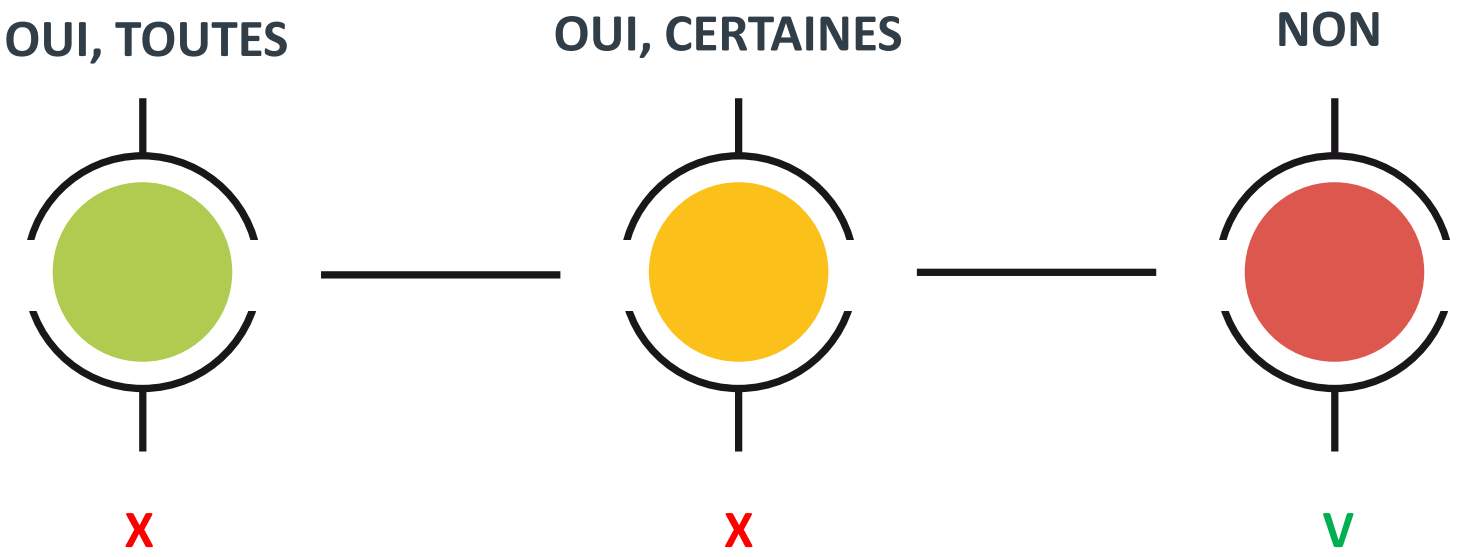
Les sites internet

Les sites internet exposent vos données sur le web, ils garantissent un accès aux données stockées comme les cookies ou les informations des utilisateurs.

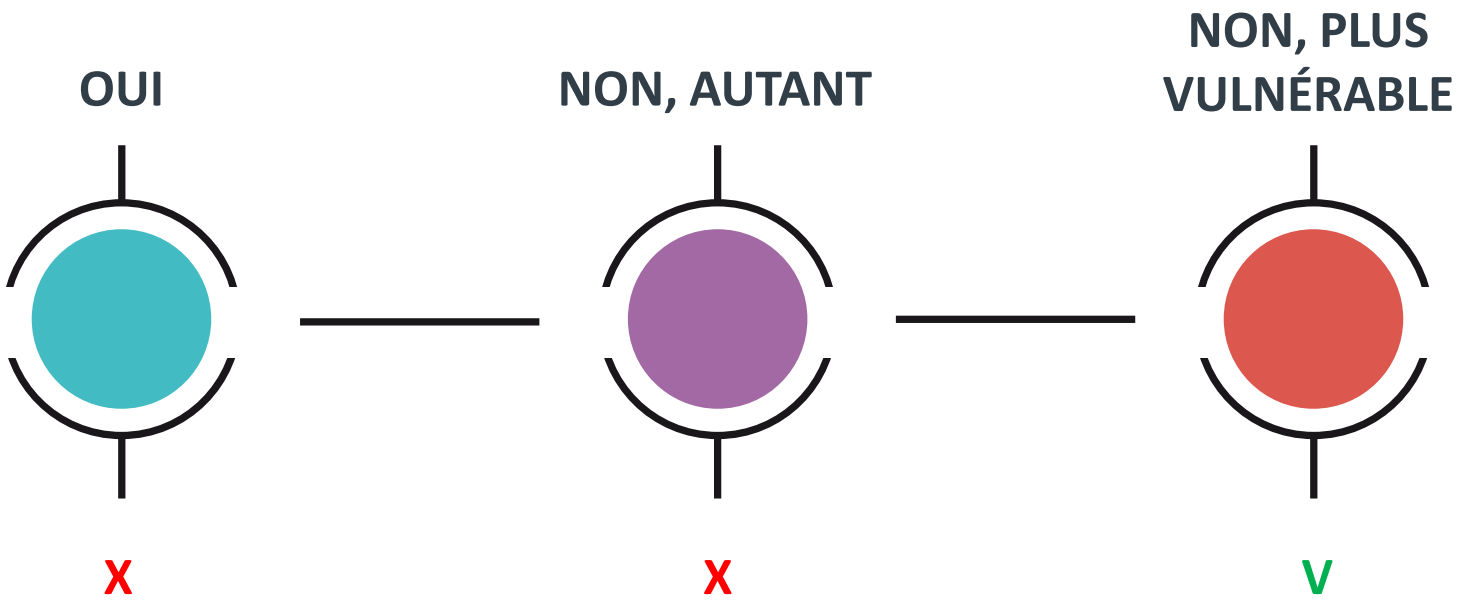
Applications

Qu'elles soient locales ou hébergées, les applications collectent, utilisent et s'échangent vos données entre elles.

Pensez-vous que ces technologies soient sans risque ?



Pensez-vous qu'un réseau à domicile est moins vulnérable qu'un réseau d'entreprise ?



03

Les cyberattaques : principes

AGATE
AGENCE ALPINE
DES TERRITOIRES

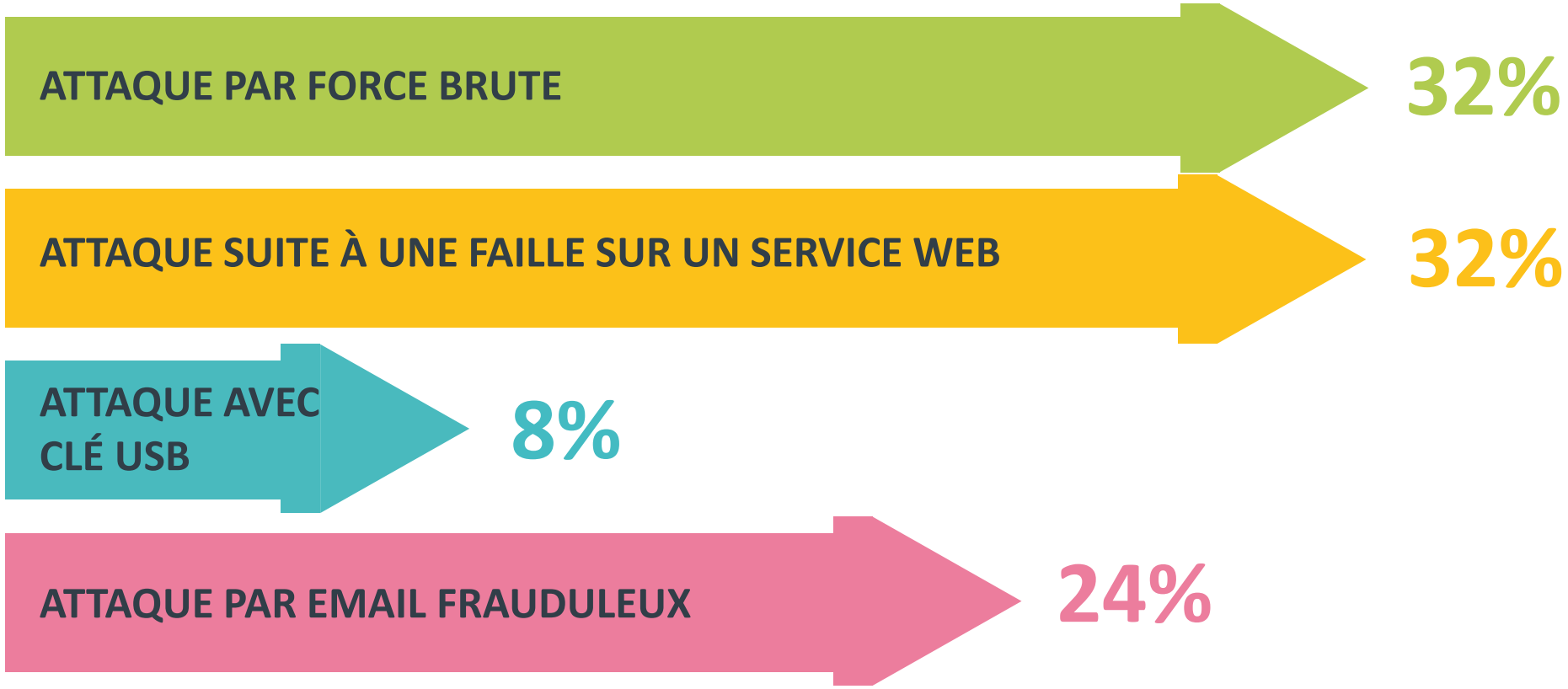
QU'EST CE QU'UNE CYBERATTAQUE ?

On définit comme cyberattaque, une atteinte à l'intégrité des systèmes informatiques dans un but malveillant.

Elle cible différents dispositifs, ordinateur ou serveur, imprimante, téléphone, application, etc.

AGATE
AGENCE ALPINE DES TERRITOIRES

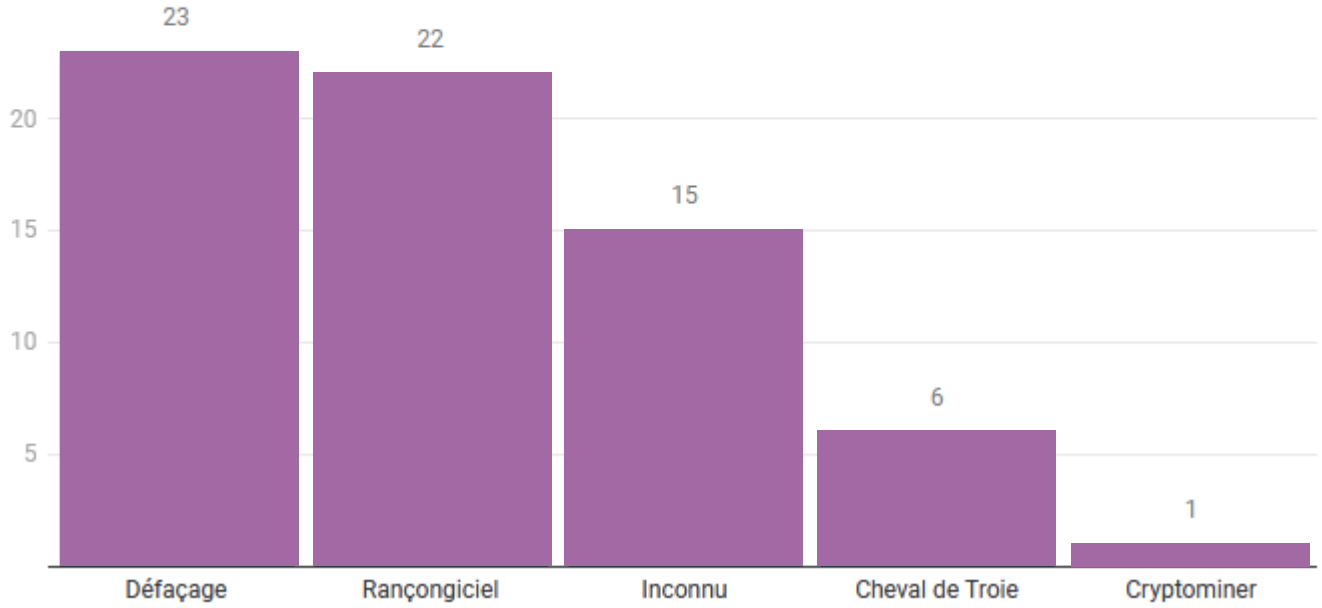
Les 4 « sources » de cyberattaques



Les types de cyberattaques

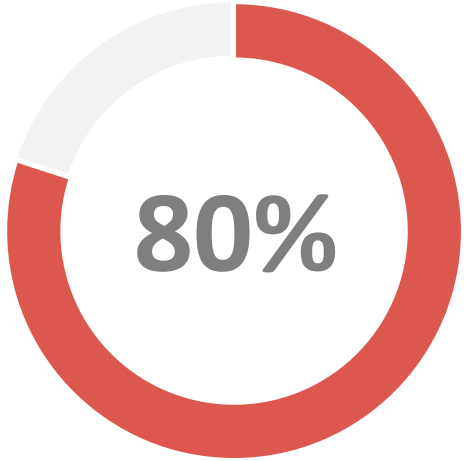
En 2020, au moins 67 collectivités touchées par des cyberattaques de tout genre

Cyberattaques connues contre des collectivités en 2020, en fonction du type d'attaque. Le défaçage est une intrusion sur le site internet pour en modifier le contenu. Le rançongiciel un chiffrement des données assortie d'une demande de rançon. Un cheval de Troie ouvre une porte dans l'infrastructure pour permettre une utilisation frauduleuse. Un *cryptominer* utilise les infrastructures d'une collectivité pour générer des cryptomonnaies.



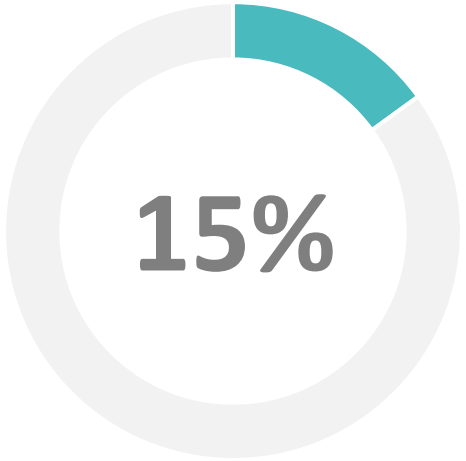
Graphique: La Gazette des communes • Source: La Gazette des communes • Récupérer les données

Zoom sur ces attaques



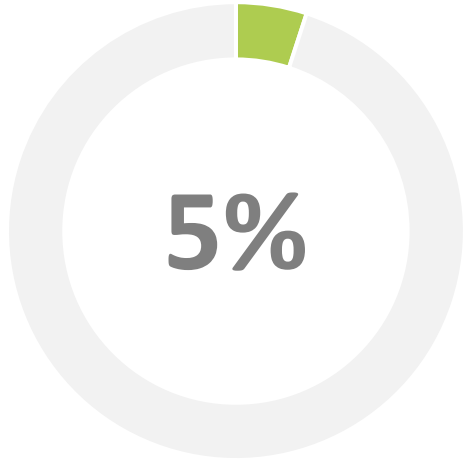
Attaques de Masse

Très courantes, elles visent à toucher le plus de personnes avec le minimum de coûts investis pour extraire le plus d'argent possible.



Attaques Ciblées

Un mode opératoire complexe et parfaitement orchestré ; il vise là où ça fait mal et cherche à détruire et/ou à corrompre complètement sa cible.



Autre type

Espionnage, infection de vers ou ordinateur zombie, ces attaques « transparentes » pour l'utilisateur servent à créer un réseau de « Botnet ».

03

Les cyberattaques : exemples et conséquences

AGATE
AGENCE ALPINE DES TERRITOIRES

Quelques exemples d'attaques… publiquement connues !

26/10 2021

AVEYRON – Saint-Affrique : **Une cyberattaque de grande ampleur bloque le réseau informatique de la mairie.** L'attaque a eu lieu dans la nuit de samedi à dimanche et bloque tout le système.

27/04 2021

SAVOIE – la mairie de Bourg-Saint-Maurice : **Cible d'une cyberattaque.** Un retour à la normale prendra certainement plusieurs semaines. *« Il s'agit d'une grosse cyberattaque et nous n'avons, à ce stade, aucune visibilité à court terme. »* Cette attaque a impacté la Communauté de Communes de Haute-Tarentaise ainsi que la commune de Séez (moins de 3000 habitants).

27/12 2020

HAUTE-SAVOIE – l'agglomération d'Annecy : **Victime d'une cyberattaque avec demande de rançon.** Une partie du système informatique est paralysée et les auteurs réclament une rançon.

13/02 2020

ISÈRE – Crêts-en-Belledonne : **La mairie a été la cible d'une cyberattaque d'une grande ampleur** par cryptovirus qui a la particularité de chiffrer toutes les données contenues sur le serveur informatique. Les agents communaux n'ont plus accès à leurs fichiers ni à leurs messageries. (moins de 4000 habitants)

24/01 2020

LOIRE – Saint-Paul-en-Jarez : Dans le week-end du 18 et 19 janvier 2020**, la mairie a été la cible d'une cyberattaque** par cryptovirus via le logiciel de type SODINOKIBI, qui a la particularité de chiffrer toutes les données contenues sur le disque dur. (moins de 5000 habitants)

Et plus récemment…

25 NOVEMBRE 2021

ANNECY VICTIME D'UNE 2E CYBERATTAQUE EN MOINS D'UN AN !

DÉROULÉ :

Vers 10h, jeudi 25 novembre, la mairie d'Annecy a subi une cyberattaque de nature inconnue. Les services suivants ne sont plus accessibles :

- Le portail service famille (crèche, cantine…)
- La prise de RDV en ligne
- Le service de bibliothèques
- L'ensemble des démarches en ligne accessibles depuis le site internet
- Les services municipaux ne sont pas joignables par téléphone
- Impossibilité de réaliser les tournées du CCAS etc.

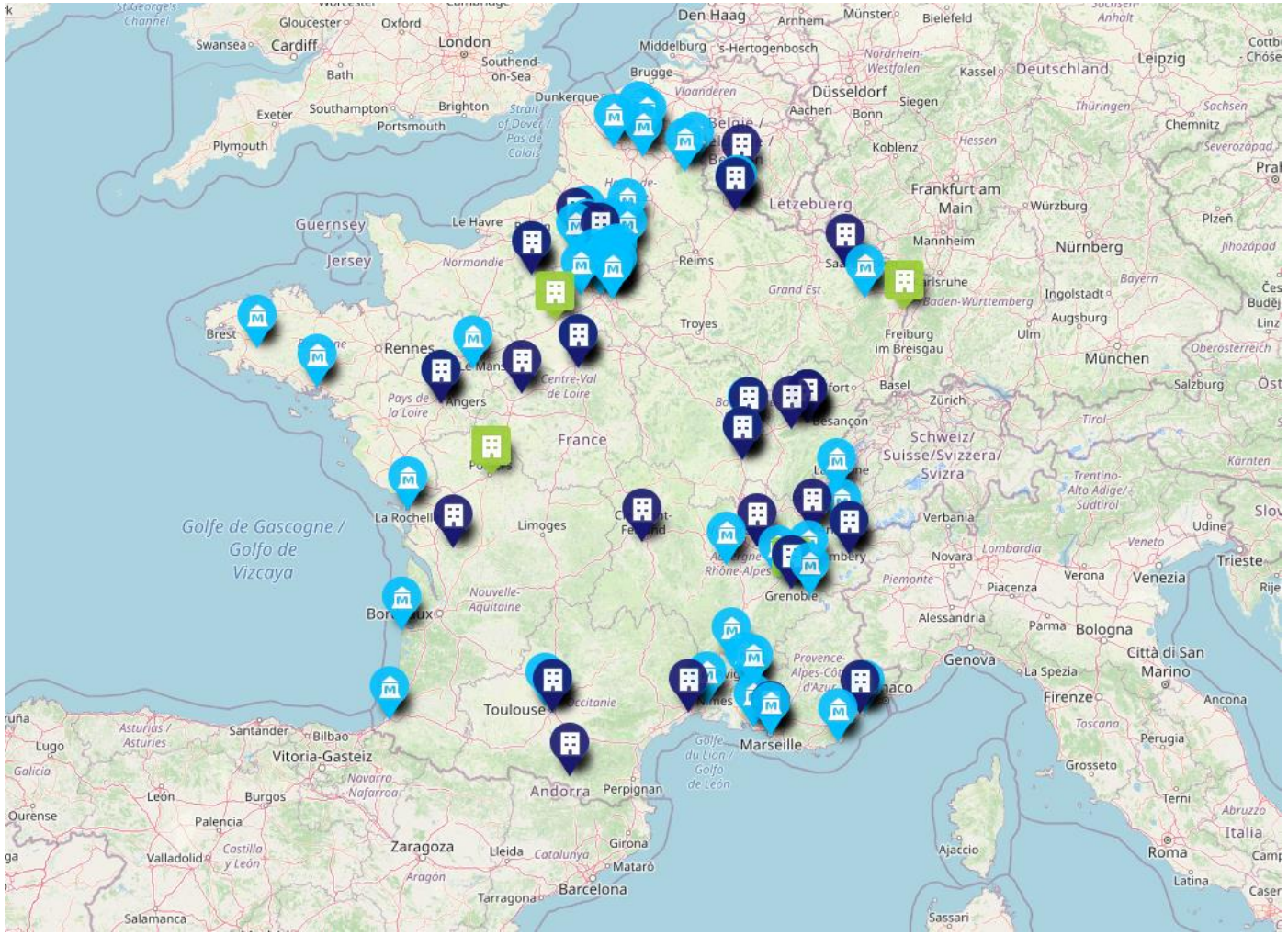
Au mieux, retour à la normale le 6 décembre, soit 12 jours d'interruption de services, dans le meilleur scénario.

Quelques exemples … En France

- **Le nombre de cyberattaques a été multiplié par quatre en France en 2020**. L'ANSSI observe que les hackers ciblent de plus en plus **les collectivités locales**, le secteur de l'éducation et de la santé

- **9%** des plaintes déposées suite à des attaques sont issues des collectivités (2000 attaques en 5 ans – **32% d'augmentation entre 2016 et 2019**)

- Rançon de 130.000 euros en moyenne (ANSSI)



https://umap.openstreetmap.fr/fr/map/cyberattaques-sur-les-organismes-publics-2019-2021_635160#6/45.283/3.516

En chiffres… dans le monde

Date	Entreprise	Secteur d'activité	Siège	Conséquences
Janvier - mars 2021	Flagstar Bank	Finance et banque	Etats-Unis	Vol de numéros de sécurité sociale.
Mars 2021	Microsoft Exchange	Informatique	Etats-Unis	Attaques informatiques sur les serveurs Exchange affectant entre 30 000 et 60 000 organisations dans le monde, dont des banques, agences gouvernementales, écoles, ... L'Autorité Bancaire Européenne figure parmi les victimes.
Mars 2021	ACER	Informatique	Taiwan	Attaque par ransomware (Logiciel mal veillant) avec une demande de rançon de 50 millions USD. L'entreprise ne s'étant pas pliée aux exigences des cybercriminels, les données volées ont été divulguées sur le dark web.
Mai 2021	CNA Financial	Finance, assurance	Etats-Unis	Une cyberattaque par ransomware a entrainé l'arrêt des services pendant quelques jours. CNA Financial a dû payer une rançon de 40 millions USD.
Mai 2021	AXA	Assurance	France	3 téraoctets (1) de données appartenant à AXA ont été volées. 5,5 milliards USD de pertes estimées. 100 giga-octets de données volées.
Mai 2021	Groupe Colonial Pipeline	Energie	Etats-Unis	Arrêt du système informatique, interruption de toutes les opérations de pipelines, ce qui a entraîné une pénurie de carburant. Payement de 4,4 millions USD de rançon.

Le coût actuel des cyberattaques mondiales augmente chaque année et représente **1,3 trillions (1300 milliards) d'USD de perte,**

soit **1,3% du PIB mondial**.

https://usine-digital.com

Quelles conséquences ?

MATÉRIELLES

- Endommagement des matériels
- Destruction des Serveurs
- Plus de téléphonie (si ToIP)

ORGANISATIONNELLES

- Postes de travail bloqués
- Blocages de dossiers informatiques
  Plus d'inscription en ligne
  (ex : cantine et périscolaire)
- Destruction / détournement de données personnelles
- Site internet inaccessible
- Blocages des paiements des factures
- Rupture dans la continuité des missions

FINANCIÈRES

- Rançon
- Amende de la CNIL en cas de plainte déposée
- Coût engendrés par les investigations informatiques, l'endommagement du parc informatique ainsi que la restauration du Service Informatique. *Par exemple, Une cyberattaque coûte 550 000 euros à la ville de Chalon-sur-Saône*

CONSÉQUENCES

Comment une cyberattaque se déroule ?

LES CAUSES :

Une erreur humaine due à un **personnel peu/pas formé ni sensibilisé aux risques**, ou des **procédures inadaptées**
Et/ou des **moyens techniques de sécurisation peu/pas adaptés**

04

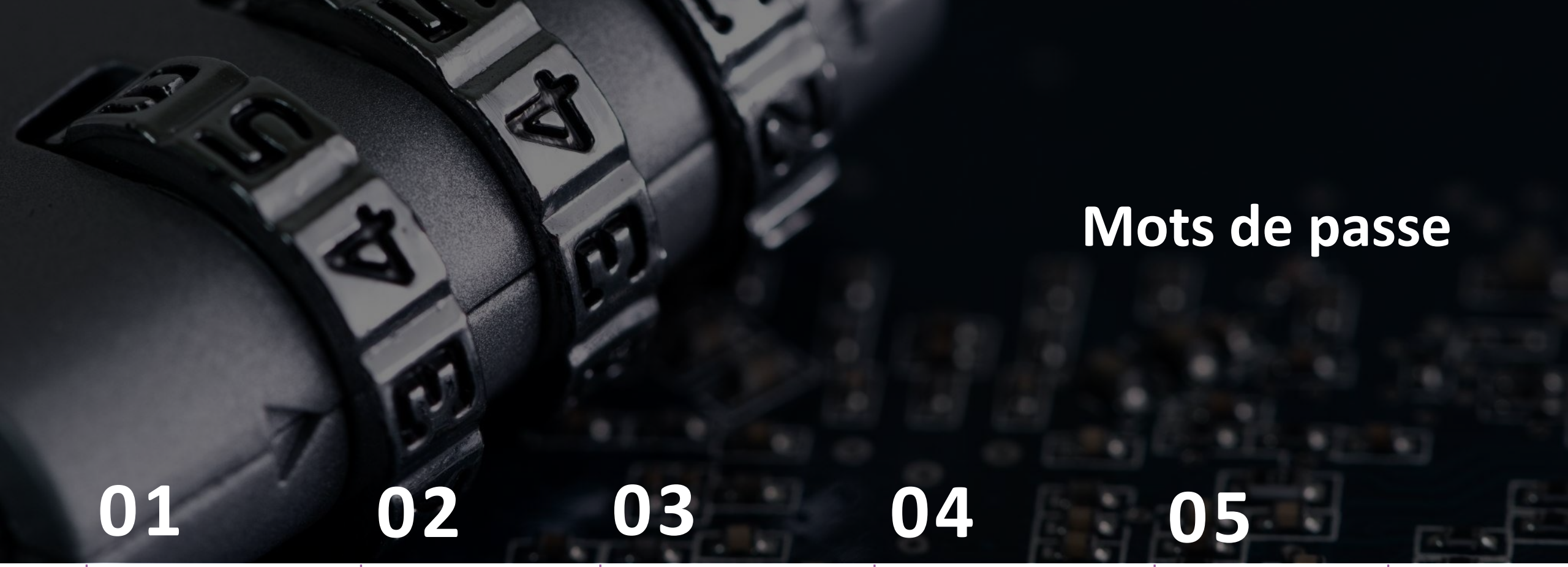
Comment éviter les pièges ?

- Quelles questions se poser ?
- Quels sont les bons réflexes ?

AGATE
AGENCE ALPINE
DES TERRITOIRES

Quelles questions se poser ?

AGATE
AGENCE ALPINE DES TERRITOIRES



Mots de passe

01	02	03	04	05
Choisir des mots de passe longs (12 caractères)	Ne pas y intégrer d'informations personnelles	Utiliser un mot de passe unique pour chaque usage	Changer ses mots de passe par défaut	Ne pas communiquer ses mots de passe

AGATE
AGENCE ALPINE DES TERRITOIRES

Hameçonnage

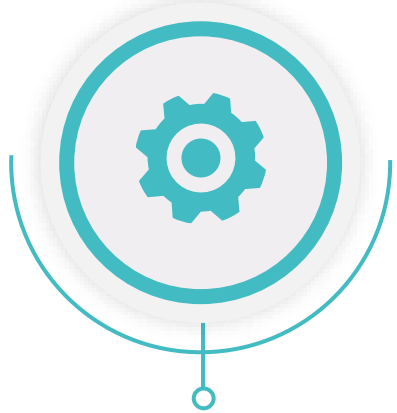
?

L'HAMEÇONNAGE OU PHISHING
est un sms ou un mail frauduleux destiné à tromper la victime pour l'inciter à communiquer des données personnelles et/ou bancaires en se faisant passer pour un tiers de confiance.

BUT

Voler des informations personnelles ou professionnelles
(identité, adresses, comptes, mots de passe, données bancaires…)
pour en faire un usage frauduleux

TECHNIQUE



Leurre envoyé via un faux message, SMS ou appel téléphonique
d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce

Hameçonnage : exemples

De : Cloud Facturation <admin@contact-support.com> <- 1. L'expéditeur
Envoyé : samedi 2 octobre 2021 03:55
À : [redacted]
Objet : Action requise - Veuillez completer votre paiement

OVHcloud

Cher client,,

Nous avons détecté un problème avec le renouvellement automatique du nom de domaine [redacted]

La cause de l'échec peut être due à 2 facteurs :

- Votre carte CB a expiré.
- Votre institution financière a refusé le prélèvement.

Votre nom de domaine sera alors suspendu.

Régulariser votre renouvellement automatique débloquera vos services en quelques heures.

Pour éviter ce problème, nous vous invitons à remplir manuellement le formulaire de renouvellem étapes du lien ci-dessous :

https://u14584890.ct.sendgrid.net/ls/click?upn=duv0udsvr4fu8isdqqunt3xy3fn9echbowcheq-2bkdghqimqxtug7hpgtdapk5x5pivnw_gjun5q0oy-2fa9pvsh-2f3tteyctxhu8g4aaurfgbnveik6ay9iktd4ofzn34o4izbyzi0rrd1ms-2bes8cgegkbaoeoojawcet0bjja1-2flqamqv6vsekxl-2fx47ngba-2f91vke9vxh4wvczac7fkde5uppzrynxx6wjoepwgvqhhhvt3b4wcw14kfryphcvjxuzftcdngwg0tccsyhhjxxlp7hc1a-3d-3d
Cliquez ou appuyez pour suivre le lien.

https://www.ovh.com/fr/order/express/#/instant/displayOrder?orderId=c3RlZmFuZUBpZGVhdmlucy5jb20 <- 2. Les liens cliquables

si nous ne recevons pas votre paiement dans les 3 jours, vos services seront définitivement supprimés.

N'hésitez pas à contacter notre service client en cas de problème ou toute autre question :

Cordialement,
OVHcloud Support

Réponse rapide

PP Philippe POURCHET <abdullahisale3387@gmail.com>
À Edmond WACH
mer. 8:58

Nous avons supprimé les sauts de ligne en surnombre dans ce message.

Bonjour Edmond,

J'entre dans une réunion à huis clos en ce moment, et j'ai besoin que vous fassiez une tâche courte mais urgente. Répondez avec votre numéro de portable et attendez mon sms. Merci

Cordialement.

Obtenez Outlook pour iO

Hameçonnage

COMMENT DÉTECTER UN MESSAGE D'HAMEÇONNAGE ?

7 points de contrôle qui doivent vous alerter :

1. Une notification de la messagerie ou de l'antivirus
2. Un nom d'émetteur inhabituel
3. Une adresse d'expédition fantaisiste
4. Un objet de message succinct ou alarmiste
5. Un message aguicheur ou inquiétant
6. Des fautes de français surprenantes
7. Une incitation à ouvrir un lien ou une pièce jointe

AGATE
AGENCE ALPINE DES TERRITOIRES

Séparer les usages personnels des usages professionnels

Que faire en cas d'attaque ?

05

Ressources

AGATE
AGENCE ALPINE
DES TERRITOIRES

Les ressources existantes

Cybermalveillance.gouv.fr a lancé un **programme de sensibilisation aux risques numériques dans les collectivités territoriales**.

UN PROGRAMME DE SENSIBILISATION EN 3 ÉTAPES

1. Menaces et réflexes essentiels pour la sécurité numérique des collectivités
2. Vigilance face aux cyberattaques : les collectivités sont toutes concernées !
3. Sensibilisation aux risques numériques : les collectivités se mobilisent

RESSOURCES DESTINÉES AUX COLLECTIVITÉS :

- **Vidéos de sensibilisation** sur les risques numériques
- **3 fiches :** gestion mots passe, usages élus/pro/perso, hameçonnage
- **Des supports** pour résumer les premiers gestes en cas de cyberattaque
- **I.M.M.U.N.I.T.É Cyber :** un auto-diagnostic rapide pour aider les élus
- Guides pratiques en cybersécurité

Les ressources existantes

Vidéos de sensibilisation sur les risques :
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/campagne-videos-sensibilisation-risques-numeriques-elus

Kit de sensibilisation :
https://medias.amf.asso.fr/upload/files/Kit_RisquesNum.pdf

Guide pratique pour une collectivité et un territoire numérique de confiance :
https://www.cybermalveillance.gouv.fr/medias/2020/10/Guide-collectivite-confiance-numerique.pdf

Sur le site Cybermalveillance.gouv.fr :

- 3 fiches sur la gestion des mots de passe, les usages élus / professionnels / personnels et le risque d'hameçonnage
- 3 mémos sur la gestion des mots de passe, les usages élus / professionnels / personnels et le risque d'hameçonnage
- Les premiers gestes en cas de cyberattaque

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

AGATE
AGENCE ALPINE DES TERRITOIRES

mémo

L'HAMEÇONNAGE

CYBERCRIMINEL

VOL DE DONNÉES

Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires ? Vous êtes peut-être victime d'une attaque par hameçonnage (*phishing* en anglais) !

BUT
Voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux.

TECHNIQUE
Leurre envoyé via un faux message, SMS ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce…

VICTIME

COMMENT RÉAGIR ?

- Ne communiquez jamais d'information sensible suite à un message ou un appel téléphonique
- Au moindre doute, contactez directement l'organisme concerné pour confirmer
- Faites opposition immédiatement (en cas d'arnaque bancaire)
- Changez vos mots de passe divulgués/compromis
- Déposez plainte
- Signalez-le sur les sites spécialisés (voir ci-dessous)

LIENS UTILES

Signal-spam.fr

Phishing-initiative.fr

Info Escroqueries
0 805 805 817 (gratuit)

Pour en savoir plus ou vous faire assister, rendez-vous sur Cybermalveillance.gouv.fr

mémo

10 CONSEILS POUR GÉRER VOS MOTS DE PASSE

1. Utilisez un mot de passe différent pour chaque service
2. Utilisez un mot de passe suffisamment long et complexe
3. Utilisez un mot de passe impossible à deviner
4. Utilisez un gestionnaire de mots de passe
5. Changez votre mot de passe au moindre soupçon
6. Ne communiquez jamais votre mot de passe à un tiers
7. N'utilisez pas vos mots de passe sur un ordinateur partagé
8. Activez la double authentification lorsque c'est possible
9. Changez les mots de passe par défaut des différents services auxquels vous accédez
10. Choisissez un mot de passe particulièrement robuste pour votre messagerie

Pour en savoir plus ou vous faire assister, rendez-vous sur Cybermalveillance.gouv.fr

06

Offres d'Agate

- Audit
- Accompagnement / sensibilisation
- Outils

AGATE
AGENCE ALPINE
DES TERRITOIRES

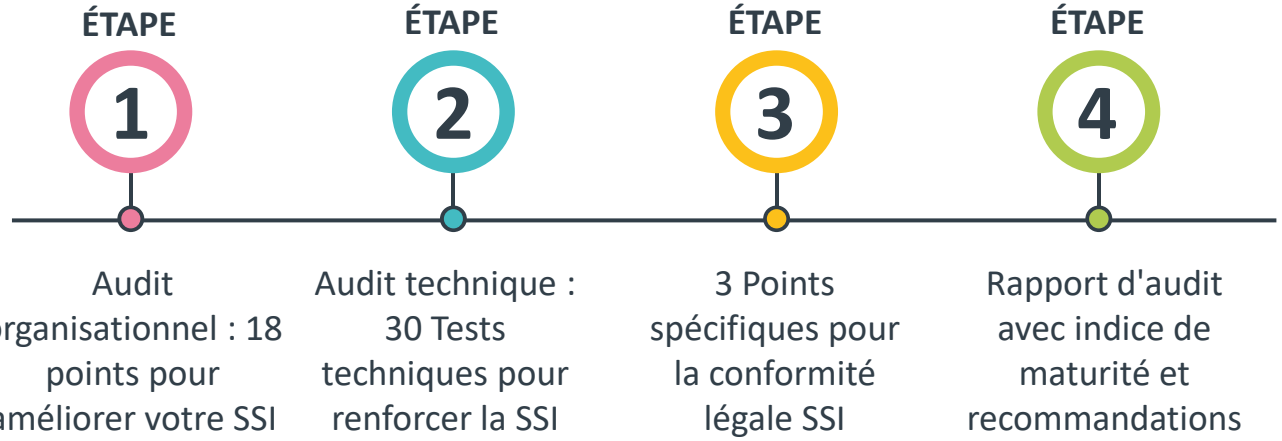
Les Audits de diagnostics et de conseils

Nous proposons 3 types d'audits de diagnostics, qui **fournissent tous une liste de recommandations** à l'issue de ces derniers afin de vous aiguiller au mieux dans vos démarches.

Un Audit « flash » de sécurité informatique initial (1,5 jours)

Le but de cet Audit est d'avoir rapidement une cartographie de vos applications, métiers et services numériques.
De plus il permet de reprendre la main sur son système d'informations, en faisant un inventaire du matériel et des outils informatiques utilisés.
Enfin, cet audit permet de présenter et anticiper une feuille de route des besoins, matériels et organisationnels, afin de vous aider au mieux dans la prise de décision concernant l'avenir de votre système d'informations, au travers de recommandations organisationnelles.

Un Audit de Sécurité Informatique en 50 points de contrôle (2,5 jours)



Les Audits de diagnostics et de conseils

Un Audit de sécurité informatique renforcé (6 jours)

Audit organisationnel, comprendre vos enjeux et adapter la SSI à vos métiers (1 jour)

- Vérifications des process en place
- Entretiens pour définir le périmètre des métiers
- Formations en réponse à incident

Audit technique, test d'intrusion et vérifications de la SSI (2 jours)

- Une journée de test d'intrusion
- Une journée de contrôle technique de la sécurité en place

Rédaction d'une charte informatique ou politique de sécurité des SI adaptée (2 jours)

- Une charte informatique permet de responsabiliser et sensibiliser les collaborateurs
- Une PSSI permet de définir un plan d'action à suivre pour garantir la sécurité du SI

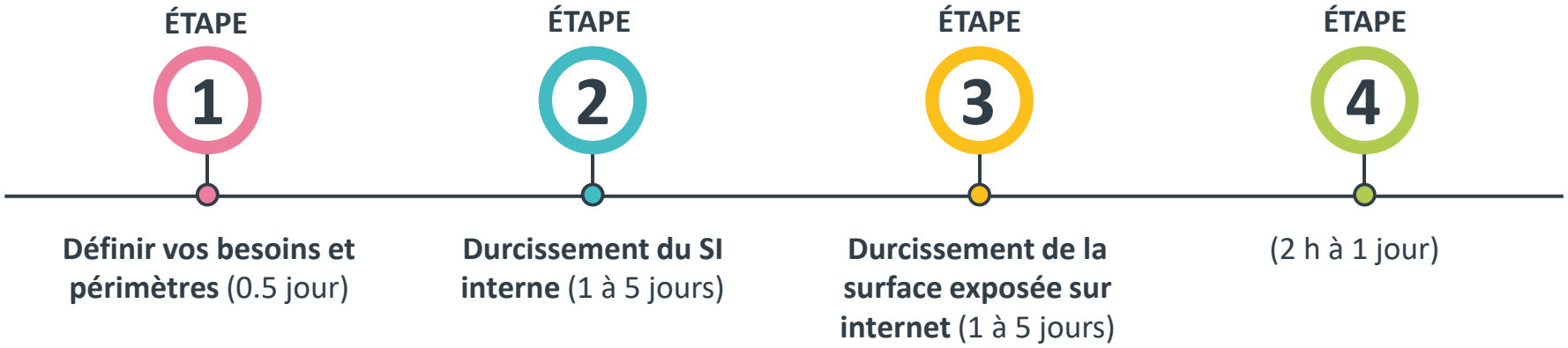
Rapport d'audit avec indice de maturité et recommandations (1 jour)

AGATE
AGENCE ALPINE DES TERRITOIRES

Accompagnement à la sécurisation informatique

Agate propose également un accompagnement à la sécurisation de votre système informatique, après Audit pour **vous accompagner à mettre en place les recommandations,** ou un accompagnement purement technique pour sécuriser vos systèmes, en fonction de vos besoins.

Accompagnement à la sécurisation (sur devis)



Cet accompagnement se déroule en collaboration avec vos prestataires / fournisseurs actuels.

Sensibilisation et formation du personnel ou des élus

Agate propose également des sensibilisations à la carte de vos équipes et ou de vos élus

- Réunion de sensibilisation
- Formation (2h à 1 jour)
- Campagnes de faux phishing et simulations de cyberattaques
- Outils de mesure des compétences numériques (Pix)

Mise à disposition d’outils

Agate réfléchit également à vous proposer des solutions vous permettant d’améliorer votre cybersécurité :

- Antivirus « avancé »
- Gestionnaire de mot de passe
- Anti-spam

- Et … sauvegarde (diapo suivante)

Nouvelle offre sauvegarde (postes de travail et serveur)

Préambule :
Lancement de l'offre en 2020 avec l'outil BL-Pilot IT : **20 collectivités ont adhéré**

Retour d'expérience :
- Offre trop chère par rapport au marché d'aujourd'hui
- Assistance BL peu réactive
- Problème de sauvegarde lors de débit trop faible

Nous avons lancé un cahier des charges à plusieurs prestataires, pour réduire les coûts et avoir une meilleure assistance.

Nous sommes en phase de test avec un éditeur. Les tarifs sont en cours de réalisation.

Nouvelle offre sauvegarde

Cette nouvelle offre se composera :

1

Accompagnement et démarrage du logiciel

- Prise de rendez-vous téléphonique pour définir vos besoins
- Installation du logiciel et configuration de vos données à sauvegarder

2

Suivi de l'accompagnement

- Suivi quotidien du bon fonctionnement de votre sauvegarde par notre équipe
- En cas de problème, nous vous contactons pour l'analyser et le corriger
- Rapport périodique envoyé (mensuel, trimestriel, semestriel,…)

3

Détails techniques

- Chiffrement automatique de vos données lors de l'envoi
- Déduplication des espaces de stockage
- Datacenter implanté en France

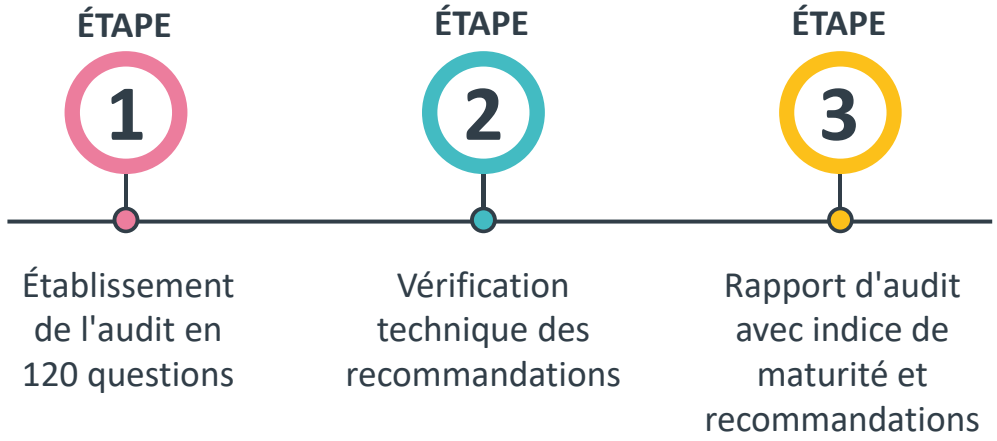
Rappel offre RGPD

Accompagnement des collectivités au démarrage du processus de mise en conformité au RGPD comprenant :

- Une formation pratique de la personne référente au sein de la collectivité (élu ou technicien, ou les deux)
- Mise à disposition de documentations et de fiches pratiques sur les principales notions et procédures à mettre en œuvre avec des exemples de clauses et/ou de rédaction de mentions à utiliser
- Une assistance à l'élaboration du registre de traitements
- La fourniture d'un plan d'actions
- Un service DPO mutualisé avec une "hotline" pour répondre aux questions des agents et élus.

En option, en lien avec le pôle numérique :

Audit de sécurité informatique axé RGPD (sécurité des données personnelles) (1,5 jours)



PROCHAIN WEBINAIRE SUR

LES COMPETENCES NUMERIQUES & PRATIQUES COLLABORATIVES

LA SEMAINE PROCHAINE !

Agate, Agence Alpine des Territoires

Bâtiment Évolution • 25 Rue Jean Pellerin • 73000 Chambéry

04 79 68 53 00 • numerique@agate-territoires.fr

www.agate-territoires.fr

AGATE
AGENCE ALPINE
DES TERRITOIRES