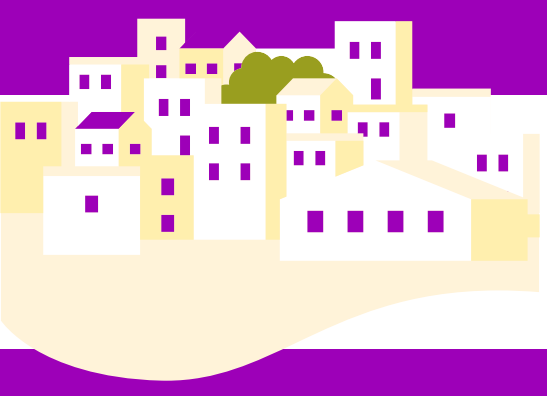
Les cyberattaques visent les collectivités

88 millions €

88 millions € : Dans le cadre du plan de relance transformation numérique de l'État et des territoires, le Gouvernement consacre une enveloppe de 88 millions d'euros pour accompagner les projets numériques de 3 200 collectivités pour une durée de trois ans, à compter de 2021.[1]



Les Collectivités Territoriales (CT) sont une cible privilégiée des cyberattaques.

329

Collectivités demandent de l'aide pour les attaques de ransomware en 2022.[2]

60 millions €

C'est le montant que le gouvernement débloque pour lutter contre les cyberattaques dans les collectivités locales. [4]

54 %

Au T1 2023, 18 cyberattaques ont dores et déjà été signalées par les collectivités, soit 54 % du total des attaques signalées en 2022. (Mais la plupart des attaques ne sont pas rendues publiques, ces chiffres sont sous-estimés.) [3]

Stratégies d'attaques populaires

Phishing

Les emails de phishing semblent provenir de marques que vous connaissez, et auxquelles vous faites confiance.

28 %

Ransomware

Les malwares et ransomwares sont souvent remis via la pièce jointe d'un email.

Collectivités locales demandant une assistance en ligne pour des attaques de phishing en 2022, la première menace signalée. [5]

Quelques exemples de ransomwares :

Avaddon	Petya
Conti	Ragnar Locker
DoppelPaymer	Ranzy Locker
Maze	REvil
Nefilim	Sodinokibi
Netwalker	CryptoLocker

Conséquences sur les collectivités :

- **Perte de temps et de productivité** – les collectivités peuvent être mises à l'arrêt, pendant plusieurs jours voire des mois…
- **Le vol de données** – les malfaiteurs demandent souvent une rançon contre la restitution des données volées aux collectivités.
- **Dégâts économiques** – en plus de la rançon à payer, reconstruction du système informatique, manque de recettes…

Conseils pour se prémunir des cyberattaques véhiculées par les emails

- Déployer une sécurité de l'email basée sur l'IA dans votre environnement.
- Passer le curseur sur les liens des emails pour visualiser leur véritable destination.
- Ne jamais ouvrir les pièces jointes provenant d'expéditeurs inconnus.
- Sensibiliser les équipes à la sécurité de l'email.
- Signaler les emails suspects au service informatique.

[1] Intercommunalités de France. « Poursuivre la transformation numérique des territoires sans France Relance. » 27 Janvier 2023.
[2] Cybermalveillance.gouv.fr. « Le rapport d'activité 2022. » 23 Mars 2023.
[3] Kon Briefing. « Cyber attacks on local governments & public sector. » 01 Mai 2023.
[4] ANSSI. Cybersécurite : Proteger les services publics et les collectivités territoriales avec France relance.
[5] Cybermalveillance.gouv.fr. « Le rapport d'activité 2022. » 23 Mars 2023.

Pour en savoir plus sur les solutions permettant de protéger vos collectivités contre les cyberattaques véhiculées par les emails, contactez Vade.

À propos de Vade :

- 1,4 milliard de boites mails protégées
- 100 milliards d'emails analysés par jour
- + 1 400 partenaires dans le monde
- Renouvellement annuel de 95 %
- 17 brevets internationnaux actifs

En savoir plus :

www.vadesecure.com

Contact :

Service commercial

sales@vadesecure.com