Regards d'Experts

L'expertise des techniciens du CDG 11 au service des employeurs territoriaux

N°3
Sept. 2024

COMPRENDRE LES CYBERATTAQUES ET Y FAIRE FACE

CDG 11
CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DE L'AUDE

« Le mot du président »

Serge BRUNEL
Président du CDG 11

J'ai le plaisir de vous présenter le 3ème numéro de notre « Regard d'Experts », le magazine élaboré par les experts du CDG 11 à destination des experts des ressources humaines dans les collectivités ou établissements publics.

Nous avons choisi pour cette édition le sujet de la cybermenace et son corollaire, la cybersécurité. La transformation digitale que nous connaissons depuis plusieurs années accélère les mutations de notre monde. Si les avantages en sont indéniables, cette évolution s'accompagne aussi d'un ensemble de risques nouveaux auxquels nous ne sommes pas encore totalement préparés.

Les communes ou établissements publics victimes de cyber attaques sont de plus en plus nombreux et nous voyons quotidiennement telle ou telle institution paralysée par un blocage de son système informatique. Des attaques moins visibles se développent aussi, c'est le cas par exemple des fraudes aux virements.

Nous pensons souvent « ne pas être concernés », être « trop petits », pourtant, tous les jours, les attaques se multiplient sur nos structures publiques.

Le CDG 11, partenaire privilégié des collectivités et établissements publics, les accompagne dans leurs mutations et s'adapte aux nouveaux besoins auxquels ils sont confrontés. Ce sujet en est l'illustration !

La mission « Protection des données » évolue et devient désormais « Protection des données et Cybersécurité ». Après une matinale dédiée à ce thème en décembre 2023, nous avons souhaité synthétiser dans ce numéro un état des risques auxquels nos structures sont exposées, les motivations et les profils des attaquants, mais aussi les bons gestes à adopter au quotidien, ainsi qu'une procédure en cas de cyber-attaque. Un bon guide pour vous accompagner dans vos pratiques !

Les experts du CDG 11 restent bien sûr à vos côtés pour vous accompagner dans votre démarche de sécurisation, n'hésitez pas à les contacter pour plus d'informations.

Je vous souhaite une bonne lecture !

Sommaire

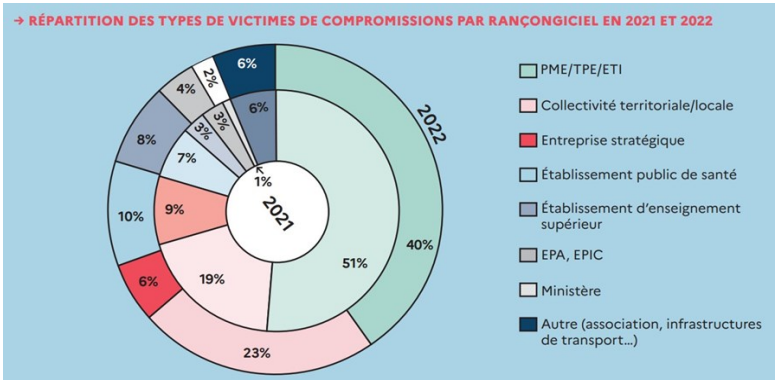
Les cyberattaques, de quoi parle-t-on ?

Malgré une profonde transformation numérique des collectivités et établissements publics, l'angle de la cybersécurité reste encore peu appréhendé.

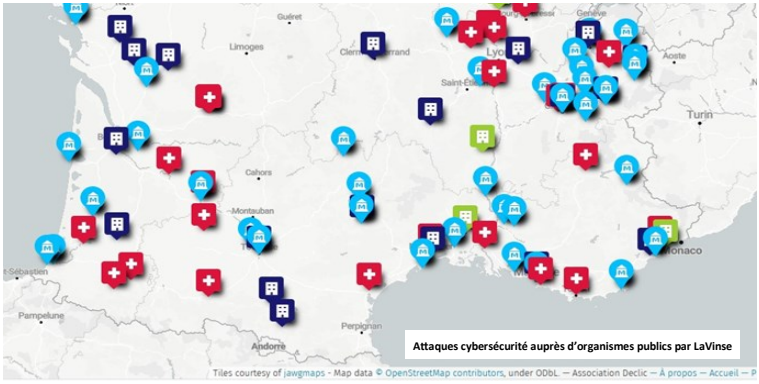
Pourtant, les structures publiques de toutes tailles sont la cible d'actes de cybermalveillance de plus en plus nombreux et les conséquences ne sont pas négligeables : systèmes d'information bloqués, vol de données personnelles, missions interrompues, préjudices financiers, séquelles psychologiques pour les agents, etc.

Les collectivités locales constituent la deuxième catégorie de victimes la plus affectée par des attaques par rançongiciel derrière les TPE, PME et ETI[1].

Elles représentent ainsi 23 % des incidents en lien avec des rançongiciels traités par ou rapportés à l'ANSSI (Agence nationale de la sécurité des systèmes d'information) en 2022.



Source : réf CERTFR-2023-CTI-001/panorama de la cybermenace 2022



Source : Cartographie interactive proposée par l'association DECLIC concernant les cyberattaques déclarées qui sont subies par les collectivités territoriales, les intercommunalités, les départements, les régions, les établissements de santé et les SDIS depuis 2019.

[1] *TPE (Très Petites Entreprises), PME (Petites et Moyennes Entreprises), ETI (Entreprises de Taille Intermédiaire)*

Le cadre juridique

Selon une étude menée par « cybermalveillance.gouv.fr », 65 % des collectivités pensent que le risque numérique est faible, voire inexistant, ou ne savent pas l'évaluer.

En matière de risques, les collectivités territoriales et leurs établissements publics sont déjà tenus à plusieurs obligations dans le cadre de leurs missions à destination du public, notamment celle relative à la protection des données personnelles.

Il leur appartient, à cet effet, de respecter la **mise en place de mesures de protection** techniques et organisationnelles pour y parvenir.

Alors que la menace cyber augmente et que les systèmes d'information restent pour partie vulnérables, la directive européenne NIS 2 *(Network and Information Security ou sécurité des réseaux et de l'information)*, publiée au Journal Officiel de l'Union européenne en décembre 2022, représente une opportunité unique pour les structures publiques de mieux se protéger.

Définitions

Afin d'appréhender plus facilement le domaine de la cybersécurité, il est nécessaire de définir certains termes[2].

- ***Système d'information*** : ensemble organisé de ressources : matériel, logiciel, personnel, données, procédures permettant d'acquérir, traiter, stocker, communiquer des informations *(sous forme de données, textes, images, sons, etc…)* dans des organisations.
- ***Cybersécurité*** : état d'un système d'information qui résiste aux cyberattaques et aux pannes accidentelles survenant dans le cyberespace.
- ***Cyberespace*** : espace constitué par les infrastructures interconnectées relevant des technologies de l'information, notamment l'Internet.
- ***Cyberattaque*** : ensemble coordonné d'actions menées dans le cyberespace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité.
- **Crise cyber** : une crise « d'origine cyber » se définit par la déstabilisation immédiate et majeure du fonctionnement courant d'une structure (arrêt des activités, impossibilité de délivrer des services, pertes financières lourdes, perte d'intégrité majeure, etc.) en raison d'une ou de plusieurs actions malveillantes sur ses services et ses outils numériques *(cyberattaques de type rançongiciel, déni de service, etc.).*

[2] Définitions issues du site Internet de l'ANSSI *(https://cyber.gouv.fr/glossaire)*

Les motivations et profils des attaquants

Les structures publiques sont confrontées à différents types d'attaques informatiques depuis de nombreuses années et les **motivations des pirates sont multiples :**

L'appât du gain

Les attaques à but lucratif sont le plus souvent réalisées par des groupes de cybercriminels organisés. C'est la principale menace pour l'ensemble des collectivités locales.

L'espionnage

Les cyberattaques ayant une finalité de renseignement étatique ou économique sont le plus souvent réalisées en infiltrant les systèmes d'information d'une organisation ou d'un individu pour s'emparer des données qui y sont conservées, et les exploiter.

L'objectif de telles opérations est de maintenir un accès discret et durable au système infiltré afin de capter toute information stratégique d'intérêt.

De fait, il faut parfois **des années à une organisation pour s'apercevoir qu'elle a été victime d'espionnage.**

La déstabilisation

Les opérations de déstabilisation peuvent prendre plusieurs formes :

- En compromettant des contenus légitimes *(boîtes courriels, sites internet)* afin de pouvoir les utiliser lors de campagne de diffusion de fausses informations ;
- En défigurant un site internet ou en le saturant de connexions automatisées afin de décrédibiliser la structure ciblée ;
- Par des actions de sabotage informatique qui consistent à rendre inopérant tout ou partie du système d'information.

Les auteurs de cyberattaques affichent des **profils d'une grande diversité** : États et leurs agences de renseignements, différentes organisations criminelles, hacktivistes, entreprises spécialisées dans la vente d'offres de services cyber, amateurs ou encore du personnel interne.

Les motivations de ces attaquants varient selon leur profil *(vengeance, déstabilisation, appât du gain…).*

Les attaques cyber

Les différents types

Les attaques se limitent rarement à une seule technique et sont perpétrées par une large palette d'acteurs, de l'individu isolé aux organisations offensives étatiques.

Afin de conduire leurs campagnes offensives, les pirates peuvent utiliser plusieurs types d'attaques telles que :

Fraude au président ou aux faux virements

Consiste à usurper l'identité d'un donneur d'ordre, qu'il soit président, maire, directeur pour exiger d'un employé, en urgence et de façon confidentielle, un important virement.

Hameçonnage

Il s'agit de soutirer des informations, souvent bancaires, avec de faux courriels.

Récemment, l'ingénierie sociale est au cœur des préoccupations car les pirates jouent sur la confiance ou sur les habitudes pour tromper la vigilance de leurs cibles *(par exemple en soutirant des informations lors d'un échange téléphonique).*

Compromission de compte de messagerie

L'objectif est de prendre le contrôle d'une messagerie professionnelle dans l'optique de l'utiliser avec des intentions malveillantes.

Intrusion dans le système d'information *(hors rançongiciel)*

Accès non autorisé à un système informatique ou à un réseau, obtenu en contournant ou en désamorçant les dispositifs de sécurité en place.

Logiciels malveillants *(malwares)* tels que les rançongiciels

Les attaques de type « rançongiciel » *(ransomware)* ciblent tous types de structures.

Très répandus, les rançongiciels sont des logiciels malveillants qui chiffrent l'ensemble des données, outils et applications de la victime *(fichiers, messagerie, etc.)*.

Pour les récupérer, cette dernière se voit demander le paiement d'une rançon en échange de la clé de déchiffrement.

Les cybercriminels exfiltrent parfois les données internes de leur cible avant l'attaque, afin d'augmenter leur pression en menaçant de les publier.

Attaques par point d'eau

L'attaque par point d'eau consiste à piéger un site internet légitime afin d'infecter les équipements informatiques des visiteurs.

Défiguration de sites internet

Ce type d'attaque exploite souvent des vulnérabilités connues mais non corrigées, pour ajouter ou modifier des informations dans une page Internet à des fins de revendications.

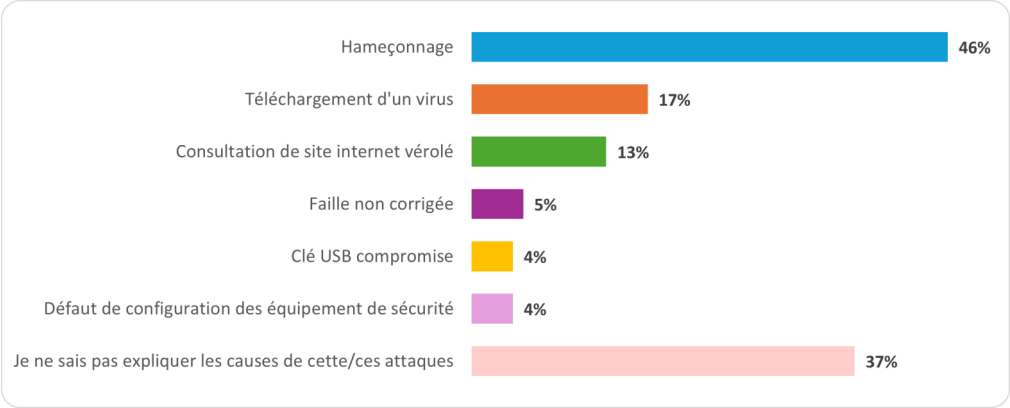
Ces opérations sont généralement revendiquées par des hacktivistes pour des motifs politiques ou idéologiques, ou à des fins de défi technique entre attaquants.

Attaques par déni de service

Attaque par laquelle un acteur malveillant vise à rendre un ordinateur ou un autre appareil indisponible pour ses utilisateurs en le submergeant ou en le saturant de requêtes jusqu'à ce que le trafic normal ne puisse plus être traité.

La typologie des cyber attaques touchant les collectivités

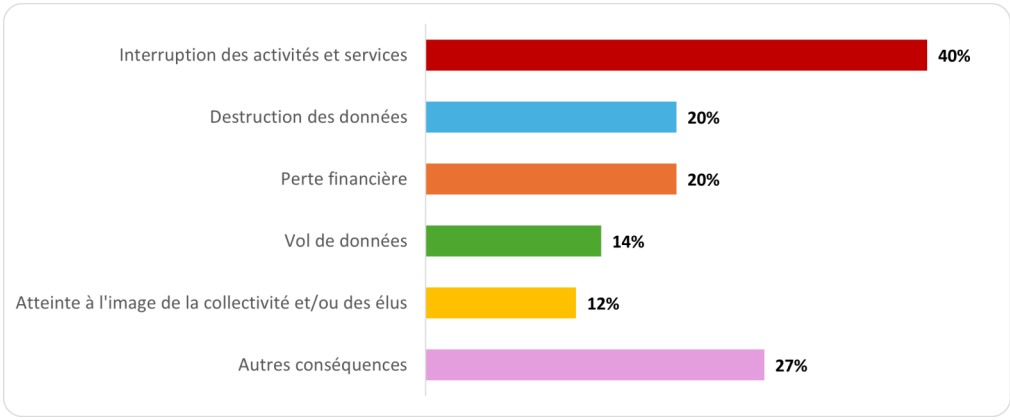
La majorité de celles touchant les structures territoriales sont de **type hameçonnage** par la réception d'un **courriel frauduleux** mais il est compliqué d'identifier exactement la source et l'attaque qui les touche.



Graphique : Vie-publique.fr / DILA . Source : Etude - Maturité des collectivités en matière de sécurité - Créé avec Datawrapper

Les principales conséquences pour les collectivités

Lorsque les structures territoriales sont victimes d'attaques, cela a pour principale conséquence d'**impacter leur capacité à accomplir leurs missions de service public** *(service à la population, état civil, permis d'inhumer…)*.



Graphique : Vie-publique.fr / DILA . Source : Etude - Maturité des collectivités en matière de sécurité - Créé avec Datawrapper

Les bonnes pratiques à adopter pour améliorer sa sécurité informatique

Face aux risques cyber, des règles élémentaires sont à adopter telles qu'effectuer des sauvegardes, utiliser des mots de passe robustes, se méfier de courriels inattendus ou vérifier que tous ses systèmes sont à jour…

Ainsi, chaque structure publique doit mettre en place les mesures suivantes :

Protégez vos accès avec des mots de passe solides

Mal aimé, notamment dans le secteur public, le mot de passe est jugé à tort trop compliqué à retenir ou comme une entrave au travail quotidien.

Résultat, cela engendre de mauvaises pratiques, telles que des ordinateurs sans mot de passe, des mots de passe partagés entre collègues ou bien trop simples et pas renouvelés.

Il est donc impératif pour les structures d'adopter des **mots de passe robustes**, par exemple de douze caractères, avec des minuscules, majuscules et caractères spéciaux.

Ils doivent être uniques et renouvelés régulièrement, l'idéal étant d'utiliser un coffre-fort numérique permettant de retenir les mots de passe de manière sécurisée.

COMBIEN DE TEMPS FAUT-IL A UN PIRATE INFORMATIQUE POUR TROUVER VOTRE MOT DE PASSE ?					
Nombre de caractères / longueur du mot de passe	Seulement des nombres	Seulement des minuscules	Des lettres majuscules et minuscules	Des nombres, des lettres majuscules et minuscules	Des nombres, des lettres majuscules et minuscules et des caractères spéciaux
Exemples	*12345*	*motdepass*	*MotDePass*	*MotDePass12345*	*@MotDePass12345!*
4 caractères	Immédiatement	Immédiatement	Immédiatement	Immédiatement	Immédiatement
5 caractères	Immédiatement	Immédiatement	Immédiatement	Immédiatement	Immédiatement
6 caractères	Immédiatement	Immédiatement	Immédiatement	Immédiatement	Immédiatement
7 caractères	Immédiatement	Immédiatement	1 seconde	2 secondes	4 secondes
8 caractères	Immédiatement	Immédiatement	28 secondes	2 minutes	5 minutes
9 caractères	Immédiatement	3 secondes	24 minutes	2 heures	6 heures
10 caractères	Immédiatement	1 minute	21 heures	5 jours	2 semaines
11 caractères	Immédiatement	32 minutes	1 mois	10 mois	3 ans
12 caractères	1 seconde	14 heures	6 ans	53 ans	226 ans
13 caractères	5 secondes	2 semaines	332 ans	3 000 ans	15 000 ans

Sauvegardez régulièrement vos données

Il est impératif de procéder à une **sauvegarde régulière des données** de la structure pour, notamment, éviter un éventuel fastidieux et compliqué travail de ressaisie.

Sur ce sujet, la méthode « 3-2-1 » est préconisée, soit trois copies d'un même fichier, sur deux supports différents et une sauvegarde stockée ailleurs, si possible hors ligne ; les attaquants ciblant aussi les serveurs de sauvegarde.

Enfin, il ne faut pas oublier de tester régulièrement ses sauvegardes pour éviter de découvrir un bug en plein milieu d'une crise.

Appliquez les mises à jour de sécurité sur tous vos appareils

Les pirates informatiques s'introduisent dans des réseaux en exploitant des vulnérabilités déjà bien connues et souvent relativement anciennes. Ainsi, il convient de **maintenir à jour ses logiciels et appareils**, notamment en configurant des mises à jour automatiques.

Utilisez un antivirus et dotez-vous d'un antispam

Installer un logiciel antivirus aide à **protéger l'ordinateur** contre les logiciels malveillants et les attaques de cybercriminels : il analyse les données, pages web, fichiers, logiciels et applications qui transitent par le réseau vers les appareils.

Se doter d'une solution antispam permet de **filtrer les courriels non sollicités** et dangereux avant qu'ils n'atteignent la boîte de réception, et limite « les clics » malencontreux sur des liens frauduleux, réduisant ainsi le risque d'attaques réussies et de pertes de données.

Téléchargez vos applications sur les sites officiels

Les applications peuvent elles aussi être vectrices de programmes malveillants. Par conséquent, il est vivement conseillé de se rendre sur des **sites de téléchargement officiels**.

De plus, il est recommandé de **restreindre** la possibilité de **téléchargement par les utilisateurs** en laissant cette faculté à l'administrateur ; cela permet le contrôle des applications téléchargées, et la réduction des risques pour la sécurité informatique.

Soyez vigilants avec les courriels reçus

Il n'est pas aisé de traquer les courriels d'hameçonnage, ces messages qui vous invitent à cliquer sur un lien ou à ouvrir une pièce jointe malveillante.

Ils constituent l'une des portes d'entrée préférée des pirates informatiques.

Il faut rester vigilant et **analyser divers éléments du courriel** : l'adresse de l'expéditeur, l'objet mentionné, l'état général du courriel, sa vraisemblance et le fait d'avoir une incitation à une action *(comme cliquer sur un lien)*.

En cas de doute, il convient **d'appeler directement son interlocuteur**.

Malgré les protections qui peuvent exister sur votre poste, l'ouverture d'un fichier malveillant risque de démarrer un programme qui ne sera pas détecté comme le déploiement d'un rançongiciel qui va discrètement se lancer dans l'ombre.

Vérifiez les sites internet sur lesquels vous naviguez

De manière générale, il convient de ne pas se rendre sur des sites douteux ou illicites qui sont susceptibles d'héberger des contrefaçons et peuvent contenir des virus.

Il y a lieu de **vérifier méticuleusement l'adresse du site** *(l'URL)* et certains indices qui peuvent vous orienter sur la fiabilité du site : un cadenas représente une connexion sécurisée et privée, un signe de danger indique que le site peut cacher des logiciels malveillants, le symbole info dans un cercle signifie que le site n'est pas entièrement sécurisé et qu'il utilise encore le protocole http...

De fait, **privilégiez une navigation sur des sites en HTTPS.**

Gardez la maitrise de vos réseaux sociaux

Les réseaux sociaux sont des outils de communication et d'information puissants et facilement accessibles qui n'échappent pas aux activités malveillantes *(usurpation d'identité, désinformation…)*.

Les utilisateurs doivent rester vigilants et **adopter de bonnes pratiques en matière de sécurité :**

- Protégez l'accès aux comptes par des mots de passe uniques et complexes ;
- Contrôlez les paramètres de confidentialité *(visibilité des informations)* ;
- Maitrisez les publications *(ne diffusez pas d'informations à caractère personnel sans l'accord des personnes concernées)* ;
- Respectez les législations *(certains propos sont punis par la loi tels que ceux incitant à la haine ou à la violence, au cyberharcèlement, à la pédophilie...)* ;
- Soyez vigilant dans vos échanges en ligne, contrôlez les applications tierces *(examiner les demandes d'autorisation d'accès à certaines données)* ;

- Évitez les connexions aux appareils publics *(ordinateurs, Wifi)* ;
- Vérifiez fréquemment les connexions aux comptes *(privilégier la double authentification)* ;
- Supprimez les comptes inactifs.

Séparez vos usages personnels et professionnels

Avec le développement du numérique, nous pouvons avoir accès à l'ensemble de nos données partout et à n'importe quel moment, ce qui a pour conséquence d'amenuiser la frontière qui sépare la vie professionnelle et la vie personnelle.

C'est pourquoi il est important de bien **distinguer les usages** et d'apprendre à se protéger pour éviter toute perte de données personnelles ou professionnelles qui pourraient potentiellement nuire à l'entité ou à votre vie privée.

Dans l'idéal, il est conseillé **d'utiliser un ordinateur pour chaque usage**, de ne pas mélanger la messagerie personnelle et professionnelle, d'utiliser des mots de passe différents pour chaque service et de ne pas conserver d'informations professionnelles sur vos stockages personnels.

Les règles d'utilisation des outils numériques *(droits et obligations)* doivent être précisées dans une charte informatique.

Évitez les réseaux wifi publics ou inconnus

Les réseaux wifi publics ou inconnus, facilement accessibles, sont une formidable porte d'entrée pour les **pirates informatiques qui peuvent les contrôler et intercepter les informations personnelles** des internautes.

Ainsi, il convient d'adopter certaines bonnes pratiques :

- Désactivez les connexions sans-fil *(Wifi, Bluetooth…)* lorsque vous ne vous en servez pas ;
- Privilégiez une connexion privée associée à un abonnement mobile et sécurisez le partage de connexion des appareils par un mot de passe robuste ;
- Si vous utilisez un réseau wifi public, veillez à ne jamais y réaliser d'opérations à caractère sensible *(paiement par carte bancaire, déclaration d'impôts, renseignement d'informations confidentielles, etc.)* et si possible utilisez un réseau privé virtuel *(VPN)*.

Pour résumer, chaque utilisateur doit adopter ces bonnes pratiques quant à l'usage d'outils numériques.

Le risque zéro n'existe pas !

Restons vigilants en tout temps face à la cybermenace.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

PRÉJUGÉ N°4

«LA CYBERSÉCURITÉ, JE N'AI PAS LE TEMPS !»

Se libérer de ses préjugés, c'est assurer sa cybersécurité.
Rendez-vous sur cybermalveillance.gouv.fr

Le Dossier des experts : Mettre en place une procédure de gestion de crise cyber

Malheureusement, toute structure publique sera potentiellement touchée par une cyberattaque.

Ainsi, on retrouve deux types d'organisations : celles qui en ont déjà été victimes et celles qui le deviendront.

Une telle situation peut avoir de graves conséquences : techniques, financières, réputationnelles, juridiques ou encore humaines.

Une cyberattaque peut se produire à tout moment et, parfois, ce sont les personnels de la structure visée qui en sont les premiers témoins : fichiers chiffrés *(illisibles)*, difficultés ou impossibilité d'accès aux logiciels ou systèmes informatiques, etc.

De ce fait, il est impératif pour les collectivités locales et les établissements publics de se préparer à une crise cyber pour pouvoir réagir efficacement, notamment en mettant en place des procédures internes de gestion de crise.

1. Se préparer à affronter une crise cyber

La gestion de crise suppose la mise en œuvre d'un schéma managérial collaboratif de l'ensemble des acteurs concernés.

Afin de mobiliser les ressources nécessaires à la sortie de crise, il convient de formaliser certaines procédures.

<table>
<tr><th></th><th>OBJECTIF STRATÉGIQUE</th><th>OBJECTIF OPÉRATIONNEL</th></tr>
<tr><td>Connaître et maîtriser ses systèmes d'information</td><td>Cartographier ses applications et ressources métiers critiques</td><td>Cartographier son système d'information</td></tr>
<tr><td>Mettre en place un Plan de Continuité d'Activité (PCA) et un Plan de Reprise d'Activité (PRA)</td><td colspan="2">Adapter le plan de continuité d'activité au scénario de crise cyber
Réaliser un plan de reprise d'activité pour le scénario cyber
Mettre en place des outils de conduite de crise résilients</td></tr>
<tr><td>Formaliser une stratégie de communication de crise cyber</td><td colspan="2">Établir une liste des parties prenantes à contacter
Anticiper la stratégie de communication de crise</td></tr>
<tr><td>Adapter son organisation de crise au scénario cyber</td><td colspan="2">Mettre en place des critères et des procédures d'activation des cellules de crise
Organiser ses cellules de crise cyber</td></tr>
<tr><td rowspan="2">Préparer ses capacités de réponse aux incidents</td><td colspan="2">Identifier les experts à solliciter en temps de crise</td></tr>
<tr><td>Mettre en place les capacités de réactions stratégiques face aux différentes menaces</td><td>Mettre en place des capacités de réactions techniques face aux différentes menaces</td></tr>
<tr><td>Mettre en place des polices d'assurance adaptées</td><td colspan="2">Adapter l'assurance aux besoins de l'organisation</td></tr>
<tr><td>S'entraîner pour pratiquer et s'améliorer</td><td colspan="2">Définir un plan d'entraînement de crise cyber</td></tr>
</table>

2. Réagir efficacement en adoptant de bonnes pratiques

Durant la période de crise, les acteurs *(élus, direction, agents, prestataires…)* agissent avec pour objectifs de limiter les impacts de la cyberattaque et de rétablir les services critiques dans un délai acceptable.

Leurs actions, s'articulent autour de quatre grandes phases de crise :

PHASE 1 - ALERTER, MOBILISER ET ENDIGUER

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT[3]
Activer son dispositif de crise cyber	Décider de l'activation d'une cellule de crise	Alerter les équipes de gestion de crise de la situation
	Mobiliser les équipes	
Piloter son dispositif de crise	Se focaliser sur la compréhension de l'attaque et l'étendue des impacts	Endiguer l'attaque
Soutenir ses équipes de gestion de crise	Assurer un support aux volets communication et juridique	Créer des « équipes » cyber
	Mettre en place un support RH adapté	
	Organiser les aspects logistiques de la gestion de crise	
Activer ses réseaux de soutien	Activer son assurance cyber Mobiliser et centraliser les demandes de renfort Déclarer son incident auprès des autorités compétentes	

PHASE 2 - MAINTENIR LA CONFIANCE ET COMPRENDRE L'ATTAQUE

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
Communiquer efficacement	Adapter son plan de communication à la situation	Informer la cellule stratégique de la situation
	Rassurer ses parties prenantes et les médias	Rassurer les équipes techniques des parties prenantes
Conduire l'investigation numérique	Appuyer la stratégie d'investigation Focaliser son attention sur l'attaque plutôt que sur un/des responsable(s)	Établir la stratégie d'investigation Organiser les investigations
Mettre en place un mode de fonctionnement dégradé pour les métiers impactés	Définir les modes d'utilisation des solutions de contournement	Soutenir le déploiement de solutions de contournement

[3] Les technologies de l'information

PHASE 3 - RELANCER LES ACTIVITÉS MÉTIERS ET DURCIR LES SYSTÈMES D'INFORMATION

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
Durcir et remédier	Objectiver les orientations sur le durcissement et la remédiation	Reprendre le contrôle des systèmes et durcir pour empêcher de nouvelles compromissions
	Reconstruire un cœur de confiance	
Préparer et développer la reconstruction	Organiser et adapter le comportement des utilisateurs	Sécuriser le développement de la reconstruction

PHASE 4 - TIRER LES LEÇONS DE LA CRISE ET CAPITALISER

	VOLET STRATÉGIQUE	VOLET OPÉRATIONNEL CYBER ET IT
Organiser sa sortie de crise	Adapter des seuils de sortie de crise	Permettre la reprise progressive des outils numériques
Tirer les leçons de la crise	Organiser le RETEX *(retour d'expérience)* Valoriser le RETEX	

3. Exemples d'outils pratiques d'aide à la gestion de crise

Il apparait pertinent d'élaborer une documentation à destination de la direction et des personnels afin de rappeler les consignes à adopter lors d'une cyberattaque.

Voici deux modèles qui peuvent faire l'objet d'un affichage dans les locaux et à proximité de chaque poste de travail.

Pour la direction

1 PREMIERS RÉFLEXES

- **Alerter immédiatement votre prestataire ou service informatique**
- **Isoler les systèmes attaqués** en coupant les connexions à Internet et au réseau local *(pour éviter la propagation)*
- **Constituer une équipe de gestion de crise** avec les services concernés *(technique, RH, finances, communication, informatique…)*
- **Tenir un registre des évènements et actions réalisées** *(notamment pour les enquêteurs)*
- **Préserver les preuves de l'attaque** *(messages reçus, matériel touché, journaux de connexion…)*

NE PAS PAYER LA RANÇON !

En payant la rançon, nous ne savons pas qui et ce que l'on finance ! Et nous ne sommes pas sûrs de récupérer les données. De plus, les cybercriminels peuvent chercher à attaquer à nouveau.

2 PILOTER LA CRISE

- **Mettre en place des solutions de secours** en activant les PCA-PRA *(Plans de Continuité et de Reprise d'Activité)* pour continuer d'assurer les services indispensables
- **Déclarer le sinistre à l'assureur** *(dédommagement ou assistance au regard du contrat)*
- **Alerter la trésorerie**
- **Déposer plainte** auprès de la gendarmerie ou de la police *(en fournissant les preuves à disposition).*
- **Identifier l'origine et l'étendue de l'attaque** *(pour corriger ou éviter un nouvel incident)*
- **Notifier l'incident à la CNIL** *(dans les 72h si atteinte à des données personnelles)*
- **Gérer la communication avec justesse en ne distillant que l'information nécessaire** *(pour les collectivités et EP, prestataires, institutions…)*

SE FAIRE ACCOMPAGNER

Votre Délégué à la Protection des Données, la Gendarmerie *(17)*,
le dispositif Cyber'Occ *(0 800 71 13 13)*, Cybermalveillance.gouv.fr, l'ANSSI, la CNIL

3 SORTIR DE LA CRISE

- **Faire une remise en service progressive et contrôlée** *(après correction des vulnérabilités et les précautions essentielles)*
- **Tirer les enseignements de l'attaque en définissant un plan d'action** *(divers investissements techniques, humains…)*

PRENDRE EN COMPTE LES RISQUES PSYCHOLOGIQUES

Une cyberattaque peut engendrer une surcharge exceptionnelle d'activité et différents sentiments *(humiliation, incompétence, culpabilité)* **susceptibles de nuire à l'efficacité des personnels pendant la crise et au-delà**

Pour les personnels

1	**DÉBRANCHEZ L'APPAREIL D'INTERNET OU DU RÉSEAU INFORMATIQUE**
	Débranchez le câble réseau (Internet) et désactivez la connexion Wifi ou les connexions de données pour les appareils mobiles
2	**N'ÉTEIGNEZ PAS L'APPAREIL**
	Certains éléments de preuve contenus dans la mémoire de l'équipement et nécessaires aux investigations seront effacés s'il est éteint
3	**ALERTEZ AU PLUS VITE VOTRE PRESTATAIRE OU SERVICE INFORMATIQUE ET VOTRE DÉLÉGUÉ À LA PROTECTION DES DONNÉES *(DPD)***
	Votre prestataire ou service informatique pourra prendre les mesures nécessaires pour contenir, voire réduire, les conséquences de la cyberattaque. ***Le DPD vous accompagnera en cas d'atteinte aux données personnelles***
4	**N'UTILISEZ PLUS L'ÉQUIPEMENT POTENTIELLEMENT COMPROMIS**
	Ne touchez plus à l'appareil pour éviter de supprimer des traces de l'attaque utiles pour les investigations à venir
5	**PRÉVENEZ VOTRE DIRECTION & VOS COLLÈGUES DE L'ATTAQUE EN COURS**
	La direction prévenue pourra donner les consignes à l'ensemble du personnel afin d'éviter de mauvaises manipulations pouvant aggraver la situation

Comment le service « Protection des données & Cybersécurité » du CDG 11 peut-il vous accompagner ?

Le service Protection des données & Cybersécurité du CDG 11

Le service accompagne depuis 2016 ses 163 adhérents dans leurs obligations relatives à la protection des données.

Afin d'étoffer son offre de service et de répondre aux besoins des structures publiques, le service évolue sur la sphère cybersécurité.

En complément de l'accompagnement en matière de protection des données, le service propose également en matière de cybersécurité :

- Un audit fonctionnel et de la sensibilisation *(questionnaire cybersécurité)* ;
- L'organisation de diverses matinées d'information ;
- Une veille juridique accrue ;
- Le développement du réseau des partenaires institutionnels ;
- Une mise à disposition de documentation.

Comment contacter le service ?

Pour adhérer au service ou avoir plus de renseignements sur le contenu de la prestation et les modalités tarifaires, n'hésitez pas à solliciter le service Protection des données & Cybersécurité du CDG 11 par courriel ou par téléphone :

Service Protection des données & Cybersécurité

04.68.77.79.71 / 04.68.77.79.60

dpd@cdg11.fr

CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DE L'AUDE

www.cdg11.fr

cdg11@cdg11.fr

04.68.77.79.79

Siège à Carcassonne

85, avenue Claude Bernard
CS 60050
11 890 Carcassonne Cedex

Du lundi au jeudi 8h30-12h30 / 13h30-17h
Le vendredi 8h30-12h30 / 13h30-16h

Antenne de Narbonne

IN'ESS - Entrée côté parking intérieur
21, rue du Verdouble
11 100 Narbonne

Du lundi au jeudi 9h-12h30 / 13h30-17h
Le vendredi 9h-12h30 / 13h30-16h

Revue périodique du Centre de gestion de la Fonction Publique Territoriale de l'Aude
Maison des Collectivités ▪ 85 avenue Claude Bernard - CS60050 - 11890 Carcassonne Cedex ▪ 04.68.77.79.79 ▪ cdg11@cdg11.fr ▪ www.cdg11.fr
Directeur de publication : Serge BRUNEL ▪ **Rédaction** : l'ensemble des services du CDG 11
Conception/Réalisation : Claude DARD
Photos : Communication CDG 11 / Crédits photos : Stocklib - IA Microsoft Designer et Copilot - Vincent photographie ▪ **N° ISSN : 2970-474X**