PÔLE D'EXCELLENCE CYBER

GUIDE

Intégration du risque cyber au plan communal de sauvegarde des petites communes

Novembre 2024

Région Bretagne

MINISTÈRE DES ARMÉES ET DES ANCIENS COMBATTANTS
Liberté
Égalité
Fraternité

SOMMAIRE

PRÉAMBULE

La cyberattaque est un nouveau risque, de plus en plus prégnant, que les maires doivent prendre en compte en complément des multiples risques déjà existant existants (catastrophes naturelles, industrielles…).

Ce document, dans cette première version, se focalise sur la sécurité des systèmes d'information (SSI), et plus précisément sur la sécurité face aux actes malveillants ou attaques exploitant des vulnérabilités informatiques.

Destiné aux petites communes typiquement de moins de 3500 habitants, il doit les aider à **inclure ce risque dans leur Plan Communal de Sauvegarde (PCS) afin de gérer efficacement une crise cyber au regard des ressources dont elles disposent.**

Vous y trouverez en complément quelques bonnes pratiques, en particulier pour prévenir en amont de tels risques, quelques recommandations pour prendre en compte la cybersécurité dans les projets ou encore pour pouvoir estimer son niveau de résilience ou de protection des données de son système d'information.

Ce document est le fruit d'un travail collectif entre les membres du CSF des industries de sécurité et du Pôle d'Excellence Cyber qui, collectivement, s'attachent à travailler de concert pour la cybersécurité de nos territoires[1] . Il a vocation à se bonifier au fil du temps au regard des retours que pourront nous apporter les petites collectivités.

Il est déjà prévu d'y ajouter prochainement un volet sur la protection des données personnelles et un autre sur la prise en compte d'exigence en cybersécurité pour les achats dans le numérique.

Par ailleurs, ses échanges ont mis en évidence des axes de travail complémentaires que nous approfondirons dans le cadre des travaux du CSF des industries de sécurité et du Pôle d'Excellence Cyber. On identifie en particulier le sujet des RSSI partagés, la mutualisation de moyens de secours à déployer en cas d'attaque (en particulier pour les communications) ou encore des sources communes entre collectivités à se partager pour spécifier les commandes d'équipements de cybersécurité au juste nécessaire.

Comme tous les ans, le fruit de ces travaux fera l'objet d'une présentation lors de la session «villes et territoires numériques de confiance face à la menace cyber» organisée dans le cadre de l'European Cyber Week[2], cette année 2024 le 19 novembre à Rennes.

Jean GODOT,
Ingénieur d'application chez ALL4TEC

Paul-André PINCEMIN,
Délégué à la cybersécurité chez Rennes Ville & Métropole

1 Vous trouverez en annexe F, l'historique de cette dynamique
2 ECW : www.european-cyber-week.eu

REMERCIEMENTS

Nous tenons à remercier les différents contributeurs à l'élaboration de cette première version du document :

- Pierre BARRIAL, RSSI mutualisé pour les communes de la métropole européenne de Lille, qui nous a éclairé de son retour d'expérience ;
- François BELOT, responsable de la gestion des risques urbains de Rennes Ville et Métropole, qui nous a fait profiter de son expérience, en particulier pour ce qui concerne l'élaboration des PCA ;
- Christian CEVAER délégué régional Bretagne de l'ANSSI qui nous a accompagné dans cette initiative ;
- Guillaume CHÉREAU, responsable du CSIRT Breton Breizh Cyber qui a, en particulier, alimenté nos réflexions de retours terrains très concrets ;
- Florian DUMAS, RSSI du département de l'Isère et président du club de la sécurité numérique des collectivités, club regroupant plus de 120 RSSI de collectivités, pour ses contributions et le lien qu'il fait avec les membres de son club ;
- Jean GODOT, ingénieur d'application chez ALL4TEC, qui a copiloté ce groupe de travail avec Rennes Ville & Métropole ;
- Christine LE GOFF-PAGE, DPO de Rennes Ville et Métropole et animatrice du club des DPO des métropoles et des grandes villes, qui nous a apporter son regard quant à la protection des données personnelles ;
- Nathalie MARIN, RSSI de Rennes Ville et Métropole, qui entreprend de compléter le document sur des recommandations à prendre en compte pour les achats dans le numérique ;
- Marin PERZO conseiller numérique de la préfecture d'Ille-et-Vilaine qui nous a fait profiter de tout le travail déjà accompli au profit des maires du département ;
- Paul-André PINCEMIN, délégué à la cybersécurité chez Rennes Ville & Métropole qui a copiloté ce groupe de travail avec ALL4TEC en particulier quant à l'animation des sessions de travail et l'activation de son réseau ;
- Gilles PIRMAN, chargé de mission stratégie des territoires, qui nous a rejoint dès sa prise de poste et sur lequel nous pourrons compter pour la promotion de ces travaux.

Nous remercions également Jérôme ALLAIRE, maire d'Entrammes (53260), qui nous a aidé mieux appréhender le contexte d'une petite commune notamment en nous aidant à identifier les activités gérées et réalisées par une collectivité de cette échelle ainsi que Yann HUAUMÉ, vice-président numérique de Rennes Métropole et maire de Saint Sulpice la Foret, ville de 1500 habitants, qui s'est assurer tout au long de nos travaux de l'adéquation du document au vécu et contraintes des maires de petite communes.

PRÉFET D'ILLE-ET-VILAINE
Liberté
Égalité
Fraternité

conseil national de l'industrie
CSF des industries de sécurité

C.S.N.C

MEL
MÉTROPOLE
EUROPÉENNE DE LILLE

Rennes Métropole

ALL4TEC
CYBER RISK INSIGHT

Breizh Cyber

isère
LE DÉPARTEMENT

Ce guide a été élaboré dans le cadre du groupe de travail "Collectivités", du Pôle d'excellence cyber, animé par Rennes Métropole et All4Tech.

Chapitre I : les missions pouvant être impactées et leurs conséquences

La prolifération des cyberattaques concerne toutes les structures. Les collectivités territoriales ne sont pas épargnées[1][2]. Les plus grandes comme les métropoles, ont en leur sein des services permettant de prendre en compte ce risque, tant en mettant en place les moyens pour se protéger, qu'en s'entrainant à gérer une crise cyber. Celles de taille intermédiaire ont l'opportunité de pouvoir profiter de mesures très efficaces mises en place en particulier par l'ANSSI pour monter en compétence. Par contre, pour les plus petites communes il est encore difficile d'adresser pleinement cette problématique, par manque de moyens internes et de référent, même si des ressources sont mis à leur disposition comme celles de cybermalveillance.gouv.fr. Or, que ce soit en termes d'impact sur le fonctionnement de la commune, de responsabilité pénale ou de confiance entre l'institution et le citoyen, le sujet est de même nature que pour les autres collectivités.

Une commune de moins de 3500 habitants peut s'apparenter à une petite entreprise, de par le nombre d'agents qui compose son effectif et le type des activités internes qu'elle doit mener telles que la gestion des ressources humaines ou encore la gestion administrative et financière.

En revanche comme toute collectivité, leur spécificité est, d'une part, la diversité des activités opérationnelles à mener, pour beaucoup de service public qui, uniques, se doivent d'être résilientes (gestion de l'état civil, d'une cantine et de la distribution des repas, du cimetière, de la voirie et des espaces verts, etc.). D'autre part, le public pour qui elles sont destinées est très large, c'est-à-dire chaque citoyen de la commune, et conduit au recueil de multiples données personnelles dont la protection est un enjeu majeur, y compris pour le lien de confiance entre la collectivité et les citoyens.

1 https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-008.pdf
2 https://umap.openstreetmap.fr/fr/map/attaques-cybersecurite-aupres-dorganismes-publics_821557#6/46.868/-1.791

Basé sur des incidents réellement traités, on peut constater que les préoccupations les plus importantes des services municipaux pour garantir la continuité du service public concernent :

- Logiciel de gestion de cuisine centrale (gestion des stocks, des commandes, du grammage des denrées, etc.) permettant de fournir en repas les EHPAD ou établissements scolaires sous la responsabilité des communes (écoles maternelles et élémentaires), le mode dégradé étant de fournir des repas de substitution
- Logiciel de gestion de la délivrance des titres d'identité (cartes d'identité, passeports) qui génère de fortes attentes des citoyens (déplacements à l'étranger, démarches administratives, etc.)
- Logiciel de paye notamment pour le versement des salaires des agents communaux (possibilité de rejouer la paie du mois précédent en mode dégradé) mais aussi de facturer les services fournis aux citoyens (places en EHPAD, services périscolaires, activités culturelles et sportives, etc.)
- Logiciel de gestion du cadastre des cimetières municipaux (impossibilité de procéder aux cérémonies funéraires)
- Logiciel de gestion des listes électorales (uniquement en période électorale), gestion en mode dégradé avec les services préfectoraux pour éditer les listes électorales des bureaux électoraux de la commune et remontée des résultats
- Logiciel de gestion des familles (inscriptions en temps périscolaire, etc.) souvent des solutions en mode SaaS non impactées par la compromission des SI de la commune
- Les services de fourniture d'eau potable, de transport public, de gestion des déchets, de gestion des eaux usées sont rarement gérés en direct par les services municipaux des petites communes mais par des délégataires donc rarement impactés par la compromission des SI de la commune. Ces opérateurs sont soumis à des réglementations spécifiques en matière de cybersécurité

En annexe C, vous trouverez une liste d'évènements pouvant être redoutés pour les différentes missions que peut porter une collectivité et sur laquelle vous pouvez vous appuyer pour cartographier vos risques.

Lorsqu'une petite commune souhaite travailler sur sa cybersécurité les premiers freins peuvent être tout simplement de ne pas savoir par où commencer et sur quelles sources d'information s'appuyer. Dans ce document, nous proposons, d'une part, quelques éléments pour la prise en compte de ce risque dans leur plan communal de sauvegarde (PCS), incluant l'élaboration du plan de continuité d'activité (PCA) et le mise en place de cellule de gestion de crise. D'autre part, nous répertorions des ressources adaptées à leur contexte.

Chapitre II : les bonnes pratiques pour être en mesure d'agir efficacement dès l'identification d'une attaque

La source de risque majeure est l'attaque par rançongiciel. Reconnaître ce type d'attaque est très simple : toutes les données sur les serveurs sont chiffrées, les applications sont indisponibles et l'attaquant a déposé une note de rançon. Dans ce cas, il est recommandé de faire appel au CSIRT régional dont la commune dépend.

Pour les autres types d'incidents, il convient dans un premier temps de faire qualifier l'incident par le service informatique ou le prestataire informatique habituel. Au moindre doute sérieux, l'appel au CSIRT régional pour confirmer la qualification de l'évènement est recommandé

Les premiers gestes sont primordiaux pour limiter les impacts d'une cyberattaque. Ils sont très simples, faut-il encore les avoir en tête et s'y être préparé car ils ont des conséquences sur le fonctionnement interne mais aussi dans les services rendus aux citoyens. Pour ce faire il faut être au clair en amont pour savoir qui aura autorité pour décider de ces gestes urgents et qui les mettra en œuvre.

Le premier geste donc, le plus important, consiste à couper le réseau informatique en débranchant le câble réseau, se mettre en mode avion ou couper la box internet. L'attaquant alors n'aura plus de prise sur le système d'information, sauf à ce qui est autonome sur le SI.

Ensuite, il faut aussi déconnecter les ordinateurs et, en particulier, celui ou ceux qui semblent impactés.

Par contre, il ne faut surtout pas éteindre les ordinateurs sans quoi on supprime les données techniques relatives à l'attaque, informations dont on a besoin tant pour l'analyse technique que pour l'instruction judiciaire.

Il est impératif aussi de ne pas utiliser dans ce premier temps les sauvegardes, y compris les sauvegardes « hors ligne ». L'attaquant peut être présent dans le système depuis plusieurs jours et des portes dérobées peuvent être présente sur les sauvegardes. Quant à celles « hors ligne », même si le réseau est coupé, des logiciels malveillants implantés par l'attaquant pourrait les corrompre en les connectant aux systèmes à restaurer.

Dans un deuxième temps et sans attendre, il faut faire appel à des ressources spécialisées : vous n'êtes pas seul. Il faudra les mentionner dans le PCS avec leurs numéros de téléphone, adresses de courrier électronique ou éventuellement référence du site internet si c'est par ce biais qu'il est prévu de les solliciter puis indiquer qui sera en charge de prendre contact. Les différents soutiens sont :

- Naturellement votre prestataire s'il cela est prévu au contrat ;
- Cybermalveillance.gouv.fr ;
- Le CSIRT de votre région s'il y en a un (voir annexe A) ;

Pour les deux deniers, il est intéressant de les contacter à l'occasion de l'élaboration du PCS pour connaître leur domaine et modalités d'intervention, en particulier horaire. Il est à noter que les CSIRT régionaux basculent sur les CERT-FR national, en cas de fermeture.

Pour rappel, les compétences en cybersécurité demeurent une spécialité du domaine informatique que tous les professionnels du numérique ne possèdent pas.

Assurez-vous que votre prestataire les maîtrise, qu'il connaisse l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et ses publications ainsi que sa formation en ligne Secnumacademie.gouv.fr. Il pourra idéalement avoir des compétences validées par le label ExperCyber délivré par Cybermalveillance.gouv.fr voire une qualification de l'ANSSI (visa de sécurité).

Il est aussi impératif de prévenir les collaborateurs pour éviter de mauvaises manipulations qui pourraient aggraver la situation.

En parallèle, il faut **activer la cellule de crise et le plan de continuité d'activité** (PCA), et dans un premier temps s'accorder sur le message à porter collectivement, tant en interne qu'à l'extérieur. D'emblée, il faut informer, sans plus de détail, de l'existence de cet incident, laissant ainsi un peu de temps pour plus d'investigations et une communication complémentaire[1].

Les membres de la cellule de crise, sous l'autorité du maire, doivent être bien identifiés en amont, en précisant la mission de chacun. Pour ce faire on peut s'appuyer sur les organisations déjà prévues dans les PCS, en y intégrant le responsable informatique. Ne pas sous-estimer par ailleurs l'impact potentiel d'un crise cyber sur les moyens de communications (mail, téléphone, accès aux fichiers…).

Enfin, il faut contacter les forces de l'ordre en vue de **porter plainte et déclarer l'incident à la CNIL** s'il y a suspicion de compromission de données personnelles.

- Pour ce qui est de la notification à la CNIL par le DPO ou celui faisant office de au sein de la commune : https://notifications.cnil.fr/notifications/index
- Si les plaintes sont encore à déposer auprès d'un commissariat de Police ou une Brigade de Gendarmerie, un dispositif en ligne devrait prochainement être accessible, il serait appelé le « 17Cyber ».

Pour mémoire, si pour quelque raison que ce soit le CSIRT n'est pas impliqué dans le traitement de votre attaque ou incident bien que ce soit l'interlocuteur privilégié, il semble important de l'en informer, tant pour qu'il puisse être en veille sur d'autres attaques du même type que pour son rôle d'observateur au profit des instances nationales. Toutes ses informations ont vocation à figurer dans un volet «risque cyber» du PCS. Il est à noter que ce dernier doit rester, au regard de l'énumération des vulnérabilités, confidentiel. Considérant que le PCS se doit d'être consultable par les citoyens on prévoira une version caviardée, exempte de toute information sensible (numéros de téléphone, nom, mail, risque particulier etc.).

Par ailleurs, il **doit être disponible, à jour, sous format papier (ou numérique mais hors ligne)** car lors d'une attaque il se peut que l'ensemble des ordinateurs soient indisponibles.

Vous trouverez en annexe B quelques modèles de fiches réflexes, à amender et renseigner. La fiche réflexe à vocation à être intégrée dans le PCS. Elle doit pourvoir servir de fil rouge pour la cellule de crise.

Par ailleurs, vous trouverez au chapitre III quelques recommandations concernant la cellule de gestion des crises et au chapitre IV et annexes associées la méthode pour élaborer le PCA.

Simuler sur table une gestion de crise cyber une fois par an semble une bonne initiative, les réflexes s'affine et cela permet de s'assurer que la fiche est à jours. Y convier quelques agents en observateur peut par ailleurs être des meilleurs effets en terme de sensibilisation mais aussi en terme de communication comme quoi le sujet est pris au sérieux.

---

1 voir si souhait d'approfondir ce point le guide de l'ANSSI https://cyber.gouv.fr/publications/anticiper-et-gerer-sa-communication-de-crise-cyber

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

QUE FAIRE EN CAS DE CYBERATTAQUE ?
(élus/dirigeants de collectivités)

ÉLU ALERTEZ IMMÉDIATEMENT VOTRE SUPPORT INFORMATIQUE

TECHNICIEN ISOLEZ LES SYSTÈMES ATTAQUÉS

ÉLU CONSTITUEZ UNE ÉQUIPE DE GESTION DE CRISE

TECHNICIEN TENEZ UN REGISTRE DES ÉVÉNEMENTS

ÉLU PRÉSERVEZ LES PREUVES DE L'ATTAQUE

TECHNICIEN IDENTIFIEZ L'ORIGINE DE L'ATTAQUE ET SON ÉTENDUE

ÉLU DÉPOSEZ PLAINTE

ÉLU NOTIFIEZ L'INCIDENT À LA CNIL

TECHNICIEN METTEZ EN PLACE DES SOLUTIONS DE SECOURS

ÉLU GÉREZ VOTRE COMMUNICATION

VOTRE SUPPORT INFORMATIQUE

Nom du contact :

N° de téléphone :

CONSEILS, SIGNALEMENT 24H/24
www.cert.ssi.gouv.fr/contact

CONSEILS ET ASSISTANCE
www.cybermalveillance.gouv.fr

NOTIFICATION DE VIOLATION DE DONNÉES PERSONNELLES
www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

POLICE, GENDARMERIE 17

TECHNICIEN FAITES UNE REMISE EN SERVICE PROGRESSIVE ET CONTRÔLÉE

ÉLU TIREZ LES ENSEIGNEMENTS DE L'ATTAQUE ET DÉFINISSEZ LES PLANS D'ACTION

DOCUMENT RÉALISÉ AVEC NOS MEMBRES:

avicca · BANQUE des TERRITOIRES · coTer numérique · DÉCLIC

POUR PLUS D'INFORMATIONS
www.cybermalveillance.gouv.fr

Chapitre III : Quelques recommandations concernant la cellule de gestion de crise cyber

La numérisation rapide des services publics, amplifiée par l'adoption du télétravail, a rendu les systèmes d'information incontournables pour le bon fonctionnement des collectivités. Cependant, cette dépendance croissante aux systèmes d'information expose les collectivités à des cyberattaques de plus en plus sophistiquées, dont les conséquences peuvent être graves : perte de données, dysfonctionnements, voire l'arrêt total ou partiel des activités. Ainsi, sécuriser ces systèmes est une priorité pour prévenir et atténuer ces risques. Il convient toutefois de reconnaître que le risque zéro n'existe pas, et les collectivités doivent également faire face à des menaces plus classiques, comme les pannes électriques ou les interruptions de réseaux, souvent provoquées par des événements climatiques.

Pour faire face à ces risques, il est impératif d'adopter une approche globale visant à renforcer la résilience des collectivités. Cela inclut la mise en place de mécanismes garantissant la continuité des activités critiques, même en mode dégradé, en cas d'indisponibilité des systèmes d'information due à une cyberattaque ou à d'autres perturbations. Cette résilience permet à une collectivité de maintenir ses services essentiels en toutes circonstances, limitant ainsi l'impact d'une crise sur les citoyens.

Pour ce faire dans le cadre d'un attaque cyber, tout repose sur la performance de la cellule de gestion de cris.

Fonctionnement de la cellule de crise

Qu'il s'agisse d'une cyberattaque ou d'une perturbation des moyens de communication (panne électrique, coupure réseau), la mise en place d'une **cellule de gestion de crise** est cruciale. Cette cellule doit être capable de fonctionner en **mode dégradé** et prévoir :

- **Lignes de téléphonie RTC** : Identifier les lignes encore fonctionnelles pour maintenir les communications en cas de coupure internet.
- **Annuaire de contacts** : Disposer d'un annuaire papier des numéros des interlocuteurs clés pour faciliter les alertes.
- **Équipements spécifiques** : Prévoir des équipements de secours tels que des talkies-walkies ou des téléphones satellites pour pallier toute panne imprévue.

Il est à noter que, autant les services en propre de la commune risquent d'être impactés, il se peut que ceux externalisés (comme la messagerie selon qu'elle est hébergée en interne ou pas) soient toujours fonctionnels. Un état des lieux sur ce point doit être fait et mentionné dans le PCS.

Gestion autonome lors d'une crise

Lors de l'activation de la cellule de crise, il est impératif de disposer d'un **éclairage autonome** et de matériel simple, comme du papier et des crayons. Il faut également conserver des copies papier des documents essentiels (ex. : Plan Communal de Sauvegarde - PCS), ainsi que des **formulaires prêts à l'emploi** pour enregistrer les décisions mais aussi communiquer en particulier auprès des usagers. Les **cartes de la commune** doivent être accessibles et affichables pour la gestion sur le terrain.

Chapitre IV : Plan de Continuité d'Activité (PCA)

Face à la menace croissante des cyberattaques, la mise en place d'un **Plan de Continuité d'Activité (PCA)** est cruciale pour limiter l'impact d'une crise. Ce plan, travaillé en amont, vise à :

- **Garantir un accès minimal aux services publics essentiels**, comme l'eau potable, la sécurité et les soins de santé.
- **Éviter l'apparition de crises secondaires** en minimisant les interruptions prolongées.
- **Assurer la résilience des communications**, malgré une dégradation possible des moyens (électricité, télécommunications).

Les éléments clés d'un PCA :

1. **Cartographie des services essentiels** : Identifier les services publics critiques en fonction de leur confidentialité, intégrité et disponibilité.
2. **Priorisation des services :** Déterminer les services à maintenir en priorité en fonction de leur importance pour la collectivité.
3. **Procédures de continuité** : Élaborer des plans détaillés pour assurer la continuité des activités essentielles en mode dégradé.
4. **Sauvegarde des données** : Mettre en place des sauvegardes régulières et sécurisées des données critiques pour en assurer la disponibilité.

Missions prioritaires

Les missions classées comme prioritaires sont celles qui ne peuvent être interrompues, ou qui doivent impérativement reprendre dans les premiers jours suivant une crise cyber. Il est essentiel de **décrire les processus dégradés** pour garantir une continuité minimale, ainsi que de prévoir une montée en charge progressive avec des renforts post-crise, si nécessaire.

Une méthodologie d'Élaboration d'un Plan de Continuité d'Activité dans une Collectivité Territoriale figure en annexe D et une méthodologie détaillée en annexe E

Adaptabilité du PCA

Un PCA efficace doit être **flexible et adaptable**. Chaque crise étant unique, il est important de pouvoir ajuster les plans en fonction des circonstances. Cela peut inclure l'adoption de **stratégies temporaires** ou alternatives, comme le recours à des solutions manuelles lorsque les infrastructures informatiques sont hors service. Dans les situations prolongées, il peut être nécessaire de créer des **structures d'urgence** pour accueillir les citoyens et maintenir les services essentiels.

L'importance de l'amélioration continue et des tests réguliers

Pour garantir l'efficacité du PCA, celui-ci doit être **régulièrement testé et mis à jour**. Les exercices de simulation de crise permettent d'évaluer la réactivité des équipes, de détecter les faiblesses des procédures et d'ajuster les stratégies. En plus de ces tests, il est crucial de tenir compte des évolutions technologiques et des nouvelles menaces, afin que le PCA soit toujours adapté au contexte.

Promouvoir une culture de résilience

La mise en place d'un PCA efficace nécessite la création d'une **culture de résilience** au sein des collectivités. Cela implique de **sensibiliser les agents** aux bonnes pratiques en matière de cybersécurité et de gestion de crise. Les agents doivent comprendre leur rôle dans la continuité des activités et adopter les mesures nécessaires pour protéger les systèmes d'information. Cela passe par des **formations régulières**, des consignes claires et une communication fluide entre les services.

Collaboration avec les partenaires externes

La résilience ne peut être atteinte sans une collaboration avec des **partenaires externes** : fournisseurs technologiques, entreprises privées, et autorités nationales. En cas de crise, ces partenaires jouent un rôle crucial en fournissant un soutien technique ou logistique pour rétablir les systèmes d'information et garantir la continuité des services publics.

Conclusion

En conclusion, un **Plan de Continuité d'Activité** (PCA) bien conçu et régulièrement mis à jour est un outil indispensable pour permettre aux collectivités de résister aux crises, qu'elles soient causées par des cyberattaques ou d'autres événements perturbateurs. En plus d'assurer la résilience technologique, un PCA efficace renforce la capacité d'une collectivité à faire face aux imprévus, à protéger ses citoyens et à maintenir la confiance du public. La **préparation**, la **formation continue** et les **tests réguliers**, associés à une culture de résilience, garantissent que la collectivité est prête à répondre aux crises de manière proactive et organisée.

Chapitre V : quelques bonnes pratiques pour limiter l'impact ou prévenir en amont

1. Les 10 bonnes pratiques pour augmenter à moindre coût votre sécurité numérique

De nombreuses sources présentes des mesures essentielles pour préserver votre sécurité numérique, la grande majorité d'entre-elles sont actionnables à moindre frais.

Parmi ces bonnes pratiques nous recommandons 10 actions :

1. Gérez vos mots de passe avec soin ;
2. Sauvegardez régulièrement vos données, avec une attention toute particulière sur celle hors ligne ;
3. Effectuez des mises à jour régulières ;
4. Protégez-vous des virus et autres logiciels malveillants ;
5. Évitez les réseaux Wi-Fi publics ou inconnus ;
6. Veillez à séparer vos usages professionnels et personnels ;
7. Évitez les sites qui vous semblent douteux et effectuez vos téléchargements depuis des sources sûres ;
8. Accordez le juste niveau de privilèges ;
9. Protégez votre messagerie électronique ;
10. Maîtrisez vos informations diffusées sur Internet.

Vous retrouverez ces éléments en détail sur le site de l'ANSSI : https://cyber.gouv.fr/bonnes-pratiques-protegez-vous

D'autres sources de confiance sont à votre disposition pour compléter votre protection numérique comme cybermalveillance.gouv.fr ou le guide de l'ANSSI « la cybersécurité pour le TPE/PME en 13 questions » également pertinent pour une collectivité.

https://www.cybermalveillance.gouv.fr/bonnes-pratiques

https://cyber.gouv.fr/publications/la-cybersecurite-pour-les-tpepme-en-treize-questions

Par ailleurs, en cas d'indisponibilité du réseau internet, certains opérateurs prévoient la mise à disposition d'offre 4G qui peut s'avérer une bonne solution de secours. Il est recommandé de regarder ce qu'il en est dans votre contrat et de préciser dans le PCS les modalités de basculement.

2. Sensibiliser élus et agents aux risques cyber ainsi qu'aux bonnes pratiques

La sensibilisation des agents aux risques cybers et aux bonnes pratiques est un enjeu majeur tant pour éviter les risques que pour permettre aux agents de se sentir à l'aise avec le numérique et sans doute de réduire d'autant l'exclusion numérique.

Pour ce faire, une opportunité s'offre à tous : le «cyber mois». Cet évènement national piloté par cybermalveillance.gouv.fr se déroule durant tous les mois d'octobre. Il incite l'ensemble des acteurs à se mobiliser pour promouvoir les bonnes pratiques et pour ce faire met à disposition des supports de sensibilisation. L'ensemble des évènements y est par ailleurs recensé. Vous trouverez tous ces éléments sur le site :

https://cybermois24.cybermalveillance.gouv.fr pour l'année 2024 et pour 2025 le site pourra être trouvé sur www.cybermalveillance.gouv.fr

Il est à noter que sur certains territoires, des collectifs se mettent en place à l'instar du club» cyber mois» sur Rennes Métropole. Ne pas hésiter à contacter cybermalveillance.gouv.fr pour savoir s'il en existe un sur votre territoire que vous pourriez rejoindre.

Chapitre VI : Comment prendre en compte la cybersécurité dans nos relations avec un infogéreur

Nombre de petites communes s'appuie sur des infogéreurs auprès desquels sont sous traités une grande partie de leur services numériques. Si la proximité est un atout pour la réactivité, elle ne doit pas pour autant omettre de prendre en compte le niveau de cybersécurité offert.

Pour ce faire, il est judicieux de se poser quelques questions :

- Où sont géographiquement situées les données que vous lui confiez ?
- Est-ce que des sauvegardes existent, sont-elles testées régulièrement, sont-elles conservées hors ligne ?
- Des mises à jour régulières de vos systèmes d'information sont-elles effectuées et des rapports vous sont-ils communiqués ?
- Comment puis-je exercer mon droit de regard et de contrôle sur les données ?
- Tous les composants de mon système d'information sont-ils bien couverts par un contrat ?
- Comment votre prestataire gère-t-il la sécurité et la confidentialité des données que vous lui confiez ?
- Votre prestataire est-il monté en compétences ces dernières années : certifications, diplômes, formations ?

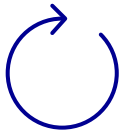
Un travail de sensibilisation auprès des communes du département d'Ille-et-Vilaine a été mené sur ce point par la préfecture. Vous pouvez retrouver le détail sur leur site : https://www.ille-et-vilaine.gouv.fr/contenu/telechargement/69598/563394/file/Plaquette%20maire_SIDPC_2023_web.pdf

LES QUESTIONS À SE POSER

Êtes-vous en mesure de répondre aux questions suivantes concernant votre contrat avec votre prestataire ?

Où sont géographiquement situées les données que vous lui confiez ?

Comment puis-je exercer mon droit de regard et de contrôle sur les données ?



Est-ce que des sauvegardes existent et sont-elles testées régulièrement ?

Tous les composants de mon système d'information sont-ils bien couverts par un contrat ?

Des mises à jour régulières de vos systèmes d'information sont-elles effectuées et des rapports vous sont-ils communiqués ?

Comment votre prestataire gère-t-il la sécurité et la confidentialité des données que vous lui confiez ?

VOUS CONNAISSEZ VOTRE PRESTATAIRE DEPUIS DES ANNÉES ? ATTENTION DANGER !

Confiance et compétence sont deux notions différentes. **La confiance n'exclut pas le contrôle.** À défaut, vous pourriez être exposé à de sérieuses vulnérabilités. Question à vous poser : votre prestataire est-il monté en compétences ces dernières années : certifications, diplômes, formations ?

Chapitre VII : Comment savoir où en est la résilience des systèmes et le niveau de protection des données : éléments d'analyse de risque…

Pour réaliser un état des lieux de votre système d'information et vous posez les bonnes questions, différents guides et outils sont à votre disposition :

- **MonAideCyber** de l'ANSSI (https://www.monaidecyber.ssi.gouv.fr/) sans doute le plus adapté pour les petites communes – il s'agit d'un service gratuit qui met en relation des aidants avec les bénéficiaires. Il est notamment proposé un diagnostic cyber de premier niveau qui aboutira à la proposition d'un plan d'action de mesures de sécurité abordables à mettre en œuvre dans les 6 prochains mois. La plateforme donne également accès à des ressources documentaires : guides, référentiels…

- **La cybersécurité pour les TPE/PME en 13 questions** de l'ANSSI (https://cyber.gouv.fr/sites/default/files/document/anssi-guide-tpe_pme.pdf) – Ce guide bien que plutôt destiné à des sociétés privées s'adaptent très bien aux petites collectivités qui ont généralement une organisation, un effectif et un système informatique proche de ce que peut avoir une TPE/PME. Ce guide propose des mesures accessibles pour une protection globale. Certaines recommandations relèvent des bonnes pratiques, d'autres requièrent un investissement plus important.

- **Le dispositif Diagonal** (DIAGnostique Opérationnel NationaL cyber) de la Gendarmerie Nationale (https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/avec-diagonal-le-pre-diagnostic) – Ce dispositif destiné aux TPE/PME est également mobilisable par les collectivités locales. Il s'agit d'un pré-diagnostic qui s'organise en 3 phases : auto-évaluation de l'organisation à partir d'un questionnaire ; entretien en présentiel avec un gendarme ; remise d'un rapport d'évaluation assorti de préconisations.

- **Le programme d'accompagnement pour la cyber-résilience des territoires et des entreprises – PACTE** (https://www.pole-excellence-cyber.org/nos-programmes/pacte/) – PME/PMI ETI, collectivités et établissements du secteur public, le Pôle vous accompagne pour accélérer votre montée en maturité Cyber. Ce programme repose sur la réalisation d'un «cyberdiagnostic» qui s'appuie sur les derniers référentiels en vigueur.

- **Questionnaire d'évaluation de la maturité en gestion de crise cyber** de l'ANSSI (https://cyber.gouv.fr/actualites/publication-dun-outil-dautoevaluation-de-gestion-de-crise-cyber) – ce guide n'est pas destiné à l'évaluation de votre système d'information mais pour celle de votre gestion de crise ce qui peut être un bon complément par rapport aux éléments présenté précédemment.

Chapitre VIII : Quelques pistes pour approfondir ses connaissances en cybersécurité

Apprendre et tester ses connaissances :

Forte de son expérience dans le domaine de l'assistance et de la sensibilisation au profit des victimes, l'équipe de Cybermalveillance.gouv.fr a souhaité proposer une **e-sensibilisation accessible à tous**. Ce MOOC de trois heures est décomposé en trois volets : comprendre, agir, transmettre. Il permet de découvrir les mécanismes des principales menaces sur Internet et d'apprendre à mieux vous en protéger. À l'issue de l'e-sensibilisation une attestation de suivi vous sera remise.

https://www.cybermalveillance.gouv.fr/sens-cyber/apprendre

Vous pouvez aussi vous abonner à la newsletter mensuelle de cybermalveillance.gouv.fr. Les publications abordent l'actualités, les nouveaux contenus et ressources thématiques pour vous sensibiliser aux risques numériques et aux bonnes pratiques associées ou bien encore des informations sur l'évolution des cybermenaces.

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/lettres-d-information

Sensibiliser ses collaborateurs

Si le MOOC mentionné supra est un excellent outil à proposer à ses collaborateurs pour se sensibiliser aux risques cyber, sa durée de 3h, peut rebuter certains. Cybermalvaillance.gouv.fr a également développé un kit de sensibilisation constitué d'une dizaine de fiches recto verso abordant de façon très pédagogiques les différents sujets que sont les mots de passe, la sécurité sur les réseaux sociaux, la sécurité des appareils mobiles, les sauvegardes, les mises à jour ou encore la sécurité des usages pro-perso.

https://www.cybermalveillance.gouv.fr/medias/2019/02/kit_complet_de_sensibilisation.pdf

S'initier à la cybersécurité

L'ANSSI a réalisé un MOOC d'initiation à la cybersécurité. Vous y trouverez l'ensemble des informations pour vous initier à la cybersécurité, approfondir vos connaissances, et ainsi agir efficacement sur la protection de vos outils numériques.

Il est décomposé en quatre sessions : Panorama de la SSI, Sécurité de l'authentification, Sécurité sur Internet et Sécurité du poste de travail et nomadisme.

Ce dispositif est accessible gratuitement. Le suivi intégral de ce dispositif vous fera bénéficier d'une attestation de réussite.

https://secnumacademie.gouv.fr/

Pour s'entrainer à la gestion de crise cyber

Les experts en gestion de crise cyber du Comcyber-MI appuyés par les réservistes de la gendarmerie nationale se sont associés à Cybermalveillance.gouv.fr pour accompagner les petites et moyennes entreprises, associations et collectivités à faire face aux cyberattaques.

Ce MOOC comprend des outils et conseils simples à mettre en oeuvre pour mettre en place ou améliorer le dispositif de gestion de crise cyber au sein de votre organisation

https://www.cybermalveillance.gouv.fr/gestion-de-crise/sency-crise

Pour approfondir la sécurisation de son organisation

L'ANSSI développe depuis plusieurs années de nombreuses ressources qui s'adresse aux dirigeants, aux gestionnaires de risques et de crises (FSSI, RSSI, CISO...), aux directeurs du numérique, aux chefs de projets, ainsi qu'aux experts en cybersécurité des organisations publiques et privées :
Les fondamentaux pour se sécuriser ;

- Connaitre la menace ;
- Définir la gouvernance de sécurité numérique adaptée à son organisation ;
- Intégrer la sécurité dans les projets ;
- Structurer ses mesures de sécurité ;
- Anticiper et gérer une crise Cyber ;
- Sensibiliser, développer ses compétences et s'entrainer ;
- Incident – Vulnérabilité ;
- Piloter la remédiation d'un incident cyber ;
- Trouver un produit/service de sécurité évalué.

Vous trouverez l'ensemble de ses ressources sur le site de l'ANSSI à l'adresse suivante :

https://cyber.gouv.fr/securiser-son-organisation

Comment s'appuyer au mieux sur un écosystème cyber pour face aux menaces d'attaques : l'exemple du département de l'Ille et Vilaine en Bretagne

Sous l'impulsion du préfet du département, l'ensemble des acteurs accompagnant la bonne prise en compte de la cybersécurité par les communes mais aussi les accompagnants lors d'attaque cyber s'est constitué en pack afin de travailler de concert en soutien des collectivités territoriales du département : AMR35, AMF 35, CDG35, Mégalis Bretagne, ANSSI, Pôle d'Excellence Cyber, Breizh Cyber (CSIRT breton), OFAC, Groupement de Gendarmerie d'Ille et Vilaine.

Cette organisation a fait l'objet d'une présentation à plus de 200 élus et personnels des services. Les planches qui y ont été présentées sont très largement applicable pour d'autres territoires souhaitant s'inscrire dans une même dynamique. Vous pouvez les retrouver sur le lien suivant :

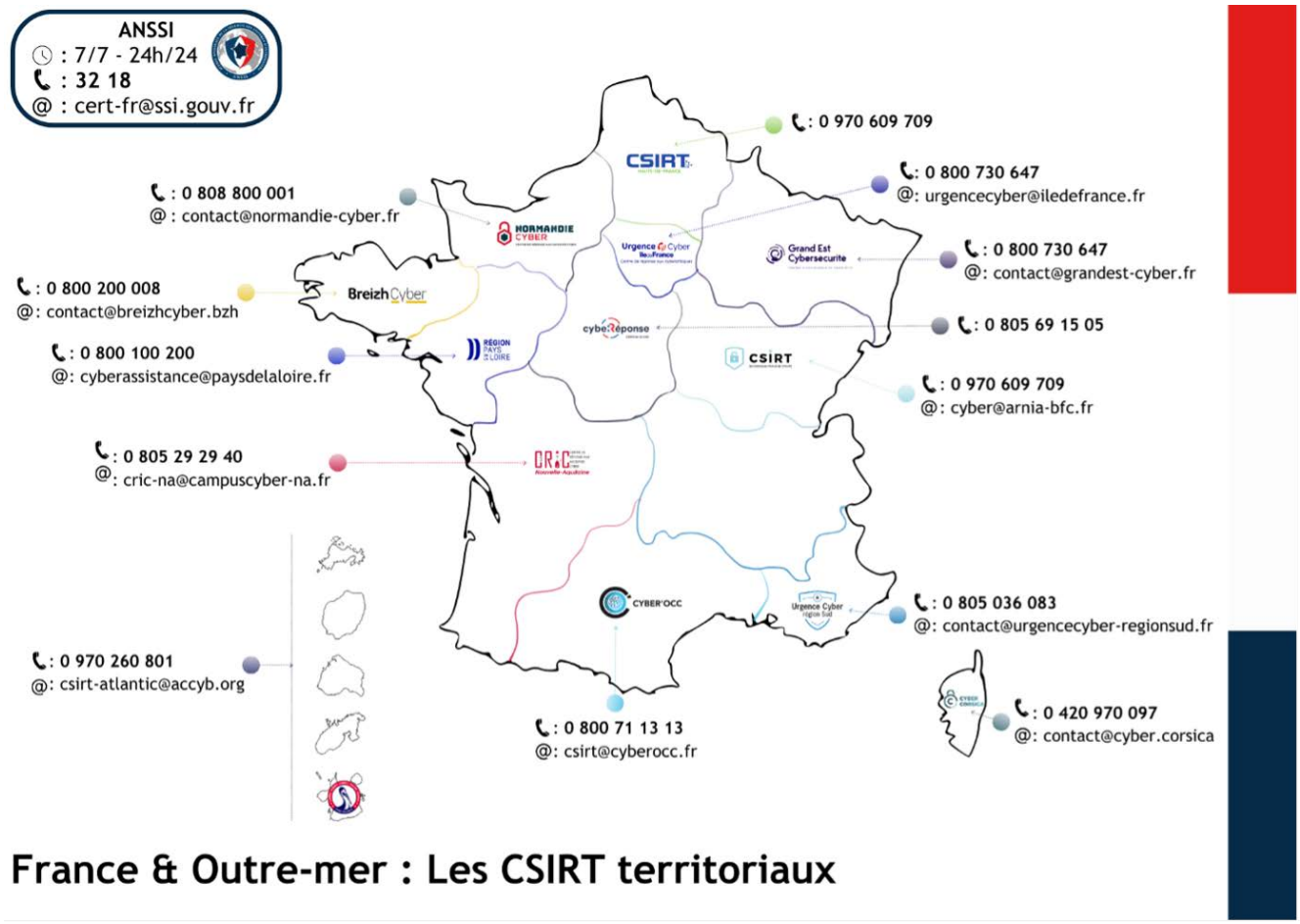
https://www.ille-et-vilaine.gouv.fr/Actions-de-l-Etat/Securite-civile-et-Securite-interieure/Cybersecurite/Collectivite

Annexe A : liste des CSIRT régionaux

Issu d'un projet du plan France Relance en 2021, les CSIRT territoriaux (Computer Security Incident Response Team) sont des centres de réponse aux incidents cyber au plus près des entités implantées sur leurs territoires. Ils traitent les demandes d'assistance des acteurs de taille intermédiaire (ex : PME, ETI, collectivités territoriales et associations) et les mettent en relation avec des partenaires de proximité : prestataires de réponse à incident et partenaires étatiques. Ils peuvent aussi traiter à leur niveau des incidents de gravité faible ou modérée.

L'émergence de ces CSIRT doit permettre de fournir localement un service de réponse à incident de premier niveau gratuit, complémentaire de celui proposé par les prestataires, la plateforme Cybermalveillance.gouv.fr et les services du CERT-FR.

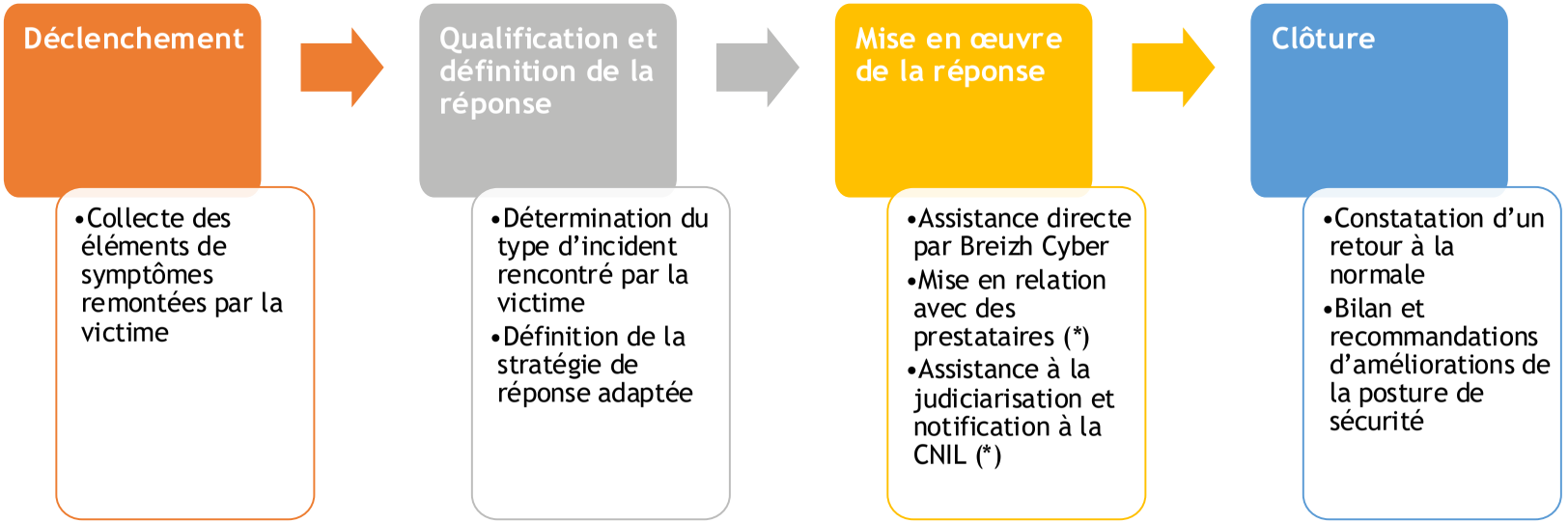
Ces équipes portent également des missions de prévention, sensibilisation et d'accompagnement dans la montée en maturité des acteurs de leurs territoires. Le dispositif est à ce jour constitué de 12 CSIRT territoriaux en métropole et un ultra marin.



France & Outre-mer : Les CSIRT territoriaux

TLP:CLEAR

Déroulé type d'une assistance



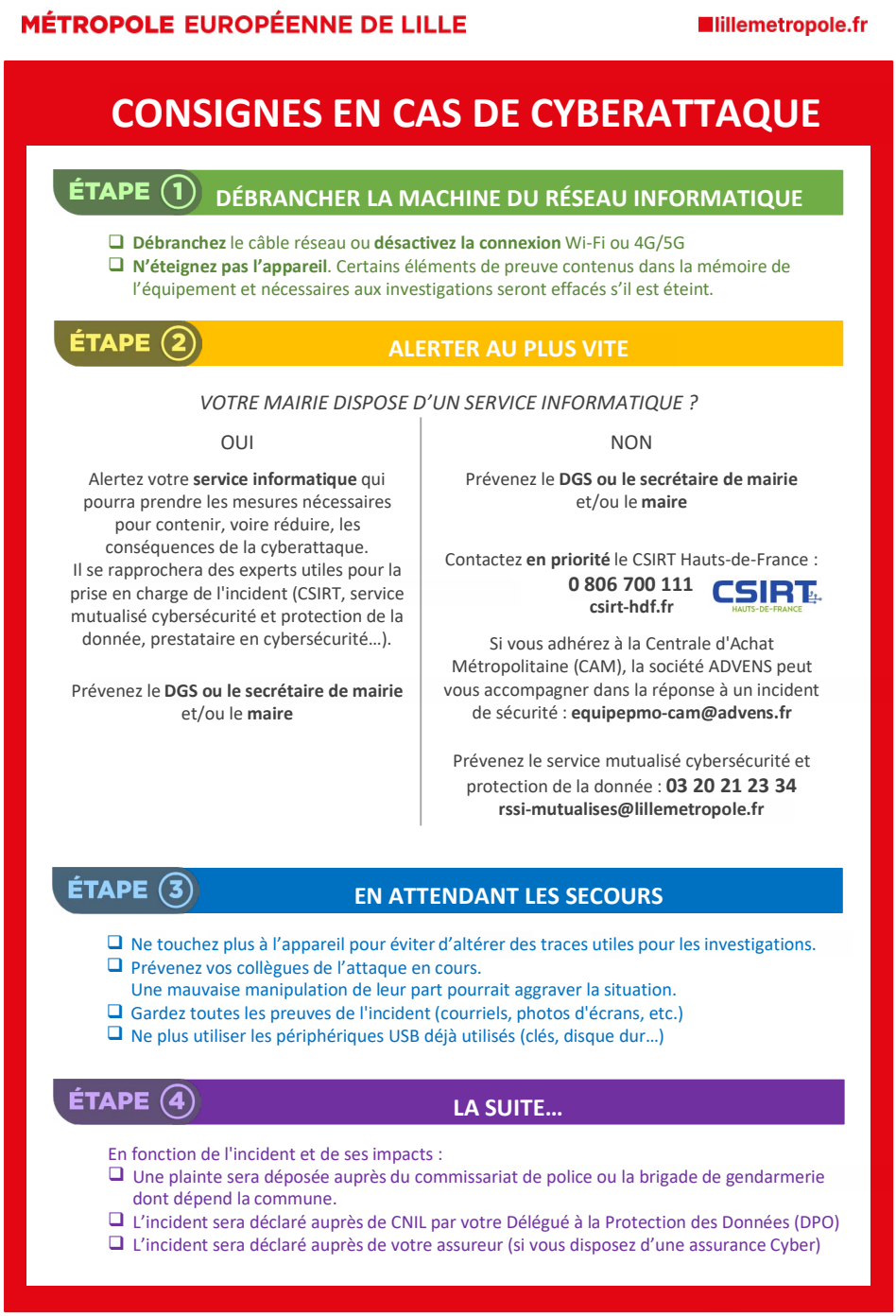
(*) la mise en relation avec des prestataires n'est pas systématique. L'assistance à la judiciarisation et à la notification CNIL est coordonnée avec les autres acteurs publics.

Breizh Cyber

Annexe B : trame de fiche "réflexe"

Vous trouverez dans cette annexe quelques exemples de fiche réflexe dont vous pourrez, pour toute ou partie, vous inspirer :

- Fiche réflexe «consigne en cas de cyberattaque» de la MEL
- Fiche réflexe «que faire en cas de cyberattaque « pour les élus et dirigeants de collectivités réalisé par Cybermalveillance.gou.fr
- Fiche réflexe à l'attention des collectivités locales «Que faire en cas de cyberattaque ?» élaborée par la préfecture d'Ille-Et-Vilaine ;



MÉTROPOLE EUROPÉENNE DE LILLE

lillemetropole.fr

CONSIGNES EN CAS DE CYBERATTAQUE

ÉTAPE 1 DÉBRANCHER LA MACHINE DU RÉSEAU INFORMATIQUE

- ❑ **Débranchez** le câble réseau ou **désactivez la connexion** Wi-Fi ou 4G/5G
- ❑ **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.

ÉTAPE 2 ALERTER AU PLUS VITE

VOTRE MAIRIE DISPOSE D'UN SERVICE INFORMATIQUE ?

OUI

Alertez votre **service informatique** qui pourra prendre les mesures nécessaires pour contenir, voire réduire, les conséquences de la cyberattaque.
Il se rapprochera des experts utiles pour la prise en charge de l'incident (CSIRT, service mutualisé cybersécurité et protection de la donnée, prestataire en cybersécurité…).

Prévenez le **DGS ou le secrétaire de mairie** et/ou le **maire**

NON

Prévenez le **DGS ou le secrétaire de mairie** et/ou le **maire**

Contactez **en priorité** le CSIRT Hauts-de-France :
0 806 700 111
csirt-hdf.fr
CSIRT HAUTS-DE-FRANCE

Si vous adhérez à la Centrale d'Achat Métropolitaine (CAM), la société ADVENS peut vous accompagner dans la réponse à un incident de sécurité : **equipepmo-cam@advens.fr**

Prévenez le service mutualisé cybersécurité et protection de la donnée : **03 20 21 23 34**
rssi-mutualises@lillemetropole.fr

ÉTAPE 3 EN ATTENDANT LES SECOURS

- ❑ Ne touchez plus à l'appareil pour éviter d'altérer des traces utiles pour les investigations.
- ❑ Prévenez vos collègues de l'attaque en cours.
  Une mauvaise manipulation de leur part pourrait aggraver la situation.
- ❑ Gardez toutes les preuves de l'incident (courriels, photos d'écrans, etc.)
- ❑ Ne plus utiliser les périphériques USB déjà utilisés (clés, disque dur…)

ÉTAPE 4 LA SUITE…

En fonction de l'incident et de ses impacts :

- ❑ Une plainte sera déposée auprès du commissariat de police ou la brigade de gendarmerie dont dépend la commune.
- ❑ L'incident sera déclaré auprès de CNIL par votre Délégué à la Protection des Données (DPO)
- ❑ L'incident sera déclaré auprès de votre assureur (si vous disposez d'une assurance Cyber)

Juin 2023 - Sources et conseils complémentaires : cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

QUE FAIRE EN CAS DE CYBERATTAQUE ?
(élus/dirigeants de collectivités)

1 PREMIERS RÉFLEXES

ÉLU — **Alertez immédiatement votre support informatique si vous en disposez** afin qu'il prenne en compte l'incident (DSI, prestataire, personne en charge).

TECHNICIEN — **Isolez les systèmes attaqués** afin d'éviter que l'attaque ne puisse se propager à d'autres équipements en coupant toutes les connexions à Internet et au réseau local.

ÉLU — **Constituez une équipe de gestion de crise** afin de piloter les actions des différentes composantes concernées (technique, RH, financière, communication, juridique…).

ÉLU — **Tenez un registre des évènements et actions réalisées** pour pouvoir en conserver la trace à disposition des enquêteurs et tirer les enseignements de l'incident a posteriori.

TECHNICIEN — **Préservez les preuves de l'attaque :** messages reçus, machines touchées, journaux de connexions…

2 PILOTER LA CRISE

TECHNICIEN — **Identifiez l'origine de l'attaque et son étendue** afin de pouvoir corriger ce qui doit l'être et éviter un nouvel incident.

ÉLU — **Déposez plainte** avant toute action de remédiation en fournissant toutes les preuves en votre possession.

ÉLU — **Notifiez l'incident à la CNIL (*)** dans les 72h si des données personnelles ont pu être consultées, modifiées ou détruites par les cybercriminels.

TECHNICIEN — **Mettez en place des solutions de secours** pour pouvoir continuer d'assurer les services indispensables. Activez vos plans de continuité et de reprise d'activité (PCA-PRA) si vous en disposez.

ÉLU — **Gérez votre communication** afin d'informer avec le juste niveau de transparence vos administrés, agents, partenaires, fournisseurs, médias…

NE PAYEZ PAS LA RANÇON !

Car vous encourageriez les cybercriminels à chercher à vous attaquer à nouveau et financeriez leur activité criminelle tout en n'ayant aucune garantie qu'ils tiendront leur parole.

FAITES-VOUS ACCOMPAGNER

Par des prestataires spécialisés en cybersécurité que vous pourrez trouver sur www.cybermalveillance.gouv.fr

PRENEZ EN COMPTE LES RISQUES PSYCHOLOGIQUES

Une cyberattaque peut engendrer une surcharge exceptionnelle d'activité et un sentiment de sidération, d'humiliation, d'incompétence voire de culpabilité susceptible d'entacher l'efficacité de vos équipes durant la crise et même au-delà.

(*) Le règlement général sur la protection des données européen (RGPD) oblige depuis mai 2018 à désigner un délégué à la protection des données (DPO en anglais) en charge notamment de ces notifications.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

3 SORTIR DE LA CRISE

TECHNICIEN

Faites une remise en service progressive et contrôlée après vous être assuré que le système attaqué a été corrigé de ses vulnérabilités et en en surveillant son fonctionnement pour pouvoir détecter toute nouvelle attaque.

ÉLU

Tirez les enseignements de l'attaque et définissez les plans d'action et d'investissements techniques, organisationnels, contractuels, financiers, humains à réaliser pour pouvoir éviter ou a minima pouvoir mieux gérer la prochaine crise.

CONTACTS UTILES

Support informatique	Conseils, signalement 24h/24
Nom du contact : _____ N° de téléphone : _____	Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (ANSSI/CERT-FR) www.cert.ssi.gouv.fr/contact
Conseils et assistance	**Notification de violation de données personnelles**
Dispositif national de prévention et d'assistance aux victimes de cybermalveillance www.cybermalveillance.gouv.fr	Commission nationale informatique et liberté (CNIL) www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Police – gendarmerie : 17

DOCUMENT RÉALISÉ AVEC NOS MEMBRES :

POUR PLUS D'INFORMATIONS :
www.cybermalveillance.gouv.fr

PRÉFET
D'ILLE-
ET-VILAINE
Liberté
Égalité
Fraternité

Fiche réflexe
à l'attention des collectivités locales
Que faire en cas de cyberattaque ?

En cas de cyberattaque ou de soupçon de cyberattaque face à un comportement anormal d'un ordinateur, le maire ou tout personnel de la mairie, doit :

➔ **Actions réflexes :**

1. Déconnecter les ordinateurs d'internet et du réseau informatique, en débranchant le câble réseau et/ou en désactivant la connexion Wifi ou 4/5G. L'objectif est d'éviter que l'attaque ne puisse se propager à d'autres équipements ou que des données soient exportées
2. Ne pas éteindre les équipements compromis pour éviter de supprimer des traces de l'attaque utiles pour les investigations à venir, certains éléments de preuve disparaissant lorsque l'on éteint l'appareil
3. Ne pas connecter les sauvegardes hors ligne

➔ **Alerte précoce :**

4. Alerter au plus vite le référent informatique de la collectivité qui prendra les mesures nécessaires pour contenir les conséquences de la cyberattaque (ex : déconnexion des sauvegardes automatisées)
5. Alerter Breizh cyber → 3218 depuis la France métropole, 09 70 83 32 18 et/ou → https://breizhcyber.bzh
   C'est le centre de réponse à incident du conseil régional de Bretagne. Il fournit une première aide d'urgence gratuite aux entreprises (PME et ETI), collectivités et associations du territoire, en cas de cyberattaque. Breizh cyber vous mettra en relation avec les prestataires cyber spécialisés
6. Prévenir les agents et élus de la collectivité. Une mauvaise manipulation de la part d'un collaborateur pourrait aggraver la situation
7. Prévenir l'astreinte sécurité de la préfecture

➔ **Mesures de gestion de crise :**

8. Déclencher le plan communal de sauvegarde et constitution d'une équipe de gestion de crise afin de piloter les actions nécessaires (technique, RH, financière, communication, juridique…)
9. Informer avec le juste niveau de transparence vos administrés, agents, partenaires, fournisseurs, média, etc. Un plan de communication peut rassurer vos usagers
10. Ne pas payer la rançon - Ne jamais prendre contact avec l'attaquant
11. Tenir à disposition un maximum de preuves (fichiers, photos des écrans, vidéos, clés USB, disques durs, etc.)

➔ **Dépôt de plainte et judiciarisation :**

12. Déposer plainte auprès de la Police nationale ou de la Gendarmerie nationale sous 72 heures maximum, à compter du moment où vous avez eu connaissance de l'incident. Cette étape est obligatoire pour permettre une indemnisation au titre d'un contrat d'assurance cyber[6]
13. Déclaration en ligne obligatoire auprès de la CNIL dans les 72 heures en cas de violation présentant un risque pour les droits et libertés des personnes tel que la fuite de données personnelles (art.33 RGPD). Le signalement peut être complété par la suite. N'oubliez pas d'aviser également votre délégué à la protection des données (DPO).
    Lien : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Contacts :

- Breizh Cyber : 0 800 200 008 ,
- CERT-FR (ANSSI) : 32 18 (permanence 7j/7, 24h/24). Cette structure nationale a vocation à traiter les attaques subies par les administrations de l'État et les structures privées les plus sensibles mais peut apporter des conseils aux collectivités en dehors des horaires d'ouverture de Breizh Cyber

POUR ALLER PLUS LOIN
Sites de référence : • https://breizhcyber.bzh • www.cybermalveillance.gouv.fr • https://cyber.gouv.fr/ Autres fiches réflexes : • https://www.cybermalveillance.gouv.fr/medias/2020/10/AfficheA3_premiers-gestes-en-cas-cyberattaque.pdf • https://www.senat.fr/rap/r21-283/r21-2832.png

Annexe C : évaluation de la gravité des événements redoutés

#	✓/❐	Valeurs métier	Évènement redouté	Gravité si concerné[7]	Description
1		Élections	Le registre des listes électorales est indisponible à l'approche d'une élection		
2		Élections	L'application pour déclarer les résultats est indisponible le jour des élections		
3		Élections	Le registre des listes électorales a été modifié		
4		Élections	Les données transmises comme résultat sont modifiées		
5		État civil	Perte de confidentialité des données d'état civil des citoyens		
6		État civil	Perte de disponibilité des activités permettant de travailler sur l'état civil		
7		État civil	Perte d'intégrité de l'état civil ou lors du processus d'enregistrement d'une personne		
8		Gestion de la location de bâtiments et de matériel (ex : salle des fêtes)	Impossibilité de gérer la location de bâtiments et de matériel (salle des fêtes)		
9		Gestion de la santé des élèves	Divulgation des données de santé des élèves		

[7] Mineure, Significative, Grave, Critique

10		Gestion de la santé des élèves	Modification des données de santé des élèves		
11		Gestion de la santé des élèves	Indisponibilité des données de santé des élèves		
12		Gestion de la voirie	Impossibilité de gérer les activités sur la voirie (ex : travaux)		
13		Gestion des accès, de la vidéosurveillance des bâtiments et autre gestion technique des bâtiments	Interruption de fonctionnement des systèmes d'accès physiques, de la vidéosurveillance des bâtiments et autre gestion technique des bâtiments		
14		Gestion des accès, de la vidéosurveillance des bâtiments et autre gestion technique des bâtiments	Modification des identifiants d'accès, ou de la vidéosurveillance des bâtiments ou encore des données techniques de gestion des bâtiments		
15		Gestion des accès, de la vidéosurveillance des bâtiments et autre gestion technique des bâtiments	Divulgation des données de gestion des accès, de la vidéosurveillance des bâtiments et autre gestion technique des bâtiments		
16		Gestion des demandes d'autorisation d'urbanisme	Impossibilité d'assurer l'activité de gestion des demandes d'autorisation d'urbanisme		
17		Gestion des demandes d'autorisation d'urbanisme	Modification des demandes d'autorisation d'urbanisme		
18		Gestion des écoles	Impossibilité de mener les activités en lien avec la gestion des écoles		

19		Gestion des équipements sportifs	Impossibilité d'assurer la gestion des équipements sportifs		
20		Gestion des espaces verts	Impossibilité d'assurer les processus de gestion des espaces verts		
21		Gestion des établissements culturels (médiathèque, école de musique...)	Impossibilité d'assurer les activités de gestion des établissements culturels (médiathèque, école de musique...)		
22		Gestion des marchés publics	Indisponibilité du système de gestion des marchés publics		
23		Gestion des marchés publics	Modification des données en lien avec la gestion des marchés publics		
24		Gestion des marchés publics	Divulgation de données en lien avec les marchés publics		
25		Gestion des signalements concernant l'espace public	Impossibilité de suivre et de traiter les signalements concernant l'espace public		
26		Gestion des subventions	Impossibilité de mener l'activité de gestion des subventions (pas de demande ni de réception)		
27		Gestion des subventions	Modification de données de gestion des subventions (montant, RIB...)		
28		Gestion des subventions	Divulgation d'informations en lien avec les subventions et leur gestion		
29		Gestion du parc automobile et autre matériel	Impossibilité d'assurer la gestion du parc automobile et autre matériel		

30		Gestion du périscolaire	Impossibilité d'assurer le périscolaire		
31		Gestion financière (budget, finance, comptabilité)	Impossibilité de mener l'activité de gestion financière (budget, finance, comptabilité)		
32		Gestion financière (budget, finance, comptabilité)	Modification de données de gestion financière (montant, RIB...)		
33		Gestion financière (budget, finance, comptabilité)	Divulgation de données financières et sur la gestion (budget, finance, comptabilité)		
34		Gestion funéraire	Impossibilité d'assurer les activités de gestion funéraire		
35		Gestion funéraire	Modification des données de gestion funéraire		
36		Gestion informatique incluant des actifs comme la messagerie ou d'autres selon l'infrastructure	Indisponibilité de l'ensemble du système informatique (messagerie, NAS, serveurs...)		
37		Gestion RH	Divulgation des données RH des agents de la mairie		
38		Gestion RH	Modification des données RH		
39		Gestion RH	Indisponibilités des données RH et de la réalisation de la gestion		
40		Plan communal de sauvegarde	Divulgation du plan communal de sauvegarde (ses chapitres et annexes confidentiels)		
41		Plan communal de sauvegarde	Indisponibilité du Plan Communal de Sauvegarde		
42		Plan communal de sauvegarde	Modification du Plan Communal de Sauvegarde		

43		Processus de demande d'aides sociales, de logement...	Modification des demandes d'aides sociales, de logement…		
44		Processus de demande d'aides sociales, de logement...	Divulgation de données en lien avec des demande d'aides sociales, de logement...		
45		Processus de demande d'aides sociales, de logement...	Impossibilité d'assurer le processus de demande d'aides sociales, de logement...		
46		Recensement citoyen	Impossibilité de réaliser le recensement citoyen		
47		Recensement citoyen	Modification des données du recensement citoyen		
48		Recensement de la population	Impossibilité de réaliser le recensement de la population		
49		Recensement de la population	Modification des données du recensement de la population		

Annexe D : Méthodologie d'Élaboration d'un Plan de Continuité d'Activité (PCA) pour une Collectivité Territoriale

Le Plan de Continuité d'Activité (PCA) vise à garantir la continuité des activités essentielles lors d'une crise, notamment en cas d'indisponibilité des systèmes d'information (SI). Il se construit en plusieurs étapes :

1. Identification des Activités Critiques :
- Définir les tâches essentielles à maintenir.
- Mettre en place des procédures alternatives pour ces activités.
- Prioriser les ressources indispensables pour assurer leur continuité.

2. Mise en place du PCA :
- Assurer un accès minimal aux services vitaux.
- Éviter l'aggravation de la crise.
- Gérer la dégradation des moyens de communication.

Méthodologie pour une Collectivité :
1. Obtenir l'engagement des dirigeants et définir les objectifs du PCA.
2. Identifier les risques et évaluer leur impact sur les services.
3. Cartographier les processus clés et définir les activités critiques*.
4. Élaborer des stratégies de continuité adaptées aux perturbations.
5. Rédiger, valider le PCA.
6. Former le personnel et tester régulièrement le plan.

* Les activités critiques sont celles qui ne peuvent être interrompues et doivent reprendre dans les premiers jours de la crise. Il est crucial de décrire les processus dégradés et de prévoir leur évolution post-crise.

Annexe E : Méthodologie détaillé d'élaboration d'un Plan de Continuité d'Activité dans une Collectivité Territoriale

Objectif du Plan de Continuité d'Activité - PCA

Ce document vise à préparer la continuité de vos activités essentielles en cas de crise Cyber. Il sert de guide pour anticiper les modalités de fonctionnement en situation dégradée, en cas d'indisponibilité totale du Système d'Information (SI), qui pourrait durer de plusieurs jours à plusieurs mois. Voici les points essentiels développés dans les questionnaires ci-dessous :

- Identification des Activités Critiques : Déterminer les activités et tâches prioritaires à maintenir (voir Onglet Missions).
- Identification des Moyens Indispensables : Lister et prioriser les moyens nécessaires pour fonctionner en mode dégradé (voir Onglet Moyens).
- Définition des Procédures Dégradées : Établir les procédures de fonctionnement alternatif (voir Onglet Procédures).

Méthodologie pour l'Élaboration d'un Plan de Continuité d'Activité dans une Collectivité Territoriale

1. Préparation de la Démarche :
- Obtenir le soutien et l'engagement des dirigeants de la collectivité.
- Définir les objectifs et attentes du PCA.
- Constituer une équipe projet dédiée.

2. Analyse et Évaluation des Risques :
- Identifier les risques potentiels pour les SI.
- Évaluer l'impact de ces risques sur les services essentiels.

3. Identification des Activités Critiques :
- Cartographier les processus clés.
- Déterminer les activités critiques à maintenir en cas de perturbation.

4. Définition des Stratégies de Continuité :
- Élaborer des scénarios de continuité pour chaque type de perturbation.
- Développer des mesures spécifiques pour chaque scénario afin d'assurer la continuité des services critiques.

5. Rédaction et Validation du PCA :
- Rédiger un document formel du PCA.
- Valider le PCA avec toutes les parties prenantes.

6. Formation et Tests :
- Former le personnel sur les procédures du PCA.
- Tester régulièrement le PCA pour assurer son efficacité et sa mise à jour.

La construction d'un Plan de Continuité d'Activité (PCA) pour faire face à l'indisponibilité des SI repose sur plusieurs étapes clés :

1. Identification des Activités Critiques :
- **Déterminer les activités et tâches essentielles** : Identifier les fonctions prioritaires à maintenir en cas de défaillance des SI.
- **Définir des procédures de fonctionnement dégradé** : Élaborer des processus alternatifs pour assurer la continuité de ces activités.
- **Prioriser les moyens nécessaires** : Identifier et classer les ressources indispensables pour réaliser ces activités en mode dégradé.

Ces éléments permettront de définir des priorités et de prendre des décisions éclairées en cas de crise cyber, améliorant ainsi la réactivité et la résilience de la collectivité.

2. La mise en place d'un Plan de Continuité d'Activité (PCA) est essentielle pour :
- Assurer un accès minimal aux services publics, notamment les services vitaux.
- Éviter la survenue de crises supplémentaires.
- Prendre en compte la dégradation des moyens de communication.

Désigner un Référent et un Suppléant : Identifiez une personne responsable de la sauvegarde, de l'impression, et de l'actualisation du document. Son suppléant doit également être désigné pour assurer une couverture continue.

Centraliser des Documents Clés : Les documents essentiels doivent être clairement identifiés, centralisés dans un lieu sécurisé (ex. : dossier PCA Cyber dans un coffre), et régulièrement actualisés. La rédaction de ce document doit permettre une vue d'ensemble et définir les fréquences de mise à jour ainsi que les acteurs responsables.

Définition du Mode Dégradé : Ce mode fait référence à un fonctionnement alternatif minimal pour assurer la continuité des activités. Par exemple, cela pourrait inclure le travail sur papier ou le traitement des demandes urgentes uniquement.

Guide d'Entretien pour Recueillir les Éléments de l'Étude

Ce guide d'entretien vise à recueillir les informations nécessaires pour élaborer un PCA. Il ne doit pas nécessairement être complété dans son intégralité, mais il fournit un support pour éviter les lacunes et adapter les questions aux interlocuteurs et contextes spécifiques.

1. Identification des Tâches Critiques :
- Q1 : En cas d'interruption des outils informatiques, quelles tâches doivent absolument être maintenues sans impact majeur pour l'activité ou la collectivité ? Quelles tâches peuvent supporter un report de 2 jours à 2 semaines ?

2. Fonctionnement Dégradé :
- Q2 : Comment pouvez-vous fonctionner de manière dégradée pour ces tâches en cas d'indisponibilité des SI ?

3. Existence et Opérationnalité des Solutions Dégradées :
- Q3 : Les solutions/procédures dégradées existent-elles ? Sont-elles opérationnelles ?
- Q4 : Si oui, sont-elles formalisées, partagées, et régulièrement mises en pratique ? Peuvent-elles être mises en œuvre rapidement ?

4. Activation des Procédures Dégradées :
- Q5 : Qui peut activer ces procédures et pour quel motif ?

5. Manques Identifiés :
- Q6 : Si ces solutions n'existent pas, quels éléments manquent pour les rendre opérationnelles (procédures, outils, moyens humains) ?

6. Durabilité des Solutions :
- Q7 : Ces solutions peuvent-elles être maintenues au-delà de 2 jours, 2 semaines, ou 1 mois ?
- Q8 : Comment pourriez-vous les rendre plus durables ? Quels moyens, applications ou données sont nécessaires lors de la reprise progressive des SI?

En suivant cette méthodologie, les collectivités peuvent se préparer efficacement à faire face aux crises et garantir la continuité des services essentiels pour les citoyens.

Identification des Matériels Essentiels pour la Continuité des Missions Prioritaires en Mode Dégradé

Pour assurer la continuité des missions critiques en mode dégradé, il est impératif de déterminer les matériels essentiels dont vous aurez besoin, ainsi que les délais associés à leur mise en place en situation de crise. Voici une liste des équipements et ressources nécessaires, à spécifier par échelon temporel et nombre requis :

1. PC Hors Réseau
- Nombre nécessaire : [Préciser le nombre]
- Délais de mise à disposition : [Préciser les délais]

2. Besoin d'Impression
- Nombre d'imprimantes nécessaires : [Préciser le nombre]
- Délais pour obtenir et installer les imprimantes : [Préciser les délais]

3. Besoin de Photocopier
- Nombre de photocopieurs nécessaires : [Préciser le nombre]
- Délais pour obtenir et installer les photocopieurs : [Préciser les délais]

4. Moyens de Communication Vocale (Interne)
- Type de moyens (ex. : téléphones fixes, radios, etc.) : [Préciser]
- Nombre nécessaire : [Préciser le nombre]
- Délais pour mise en place : [Préciser les délais]

5. Moyens de Communication Vocale (Partenaires Externes)
- Type de moyens (ex. : téléphones mobiles dédiés, systèmes de conférence) : [Préciser]
- Nombre nécessaire : [Préciser le nombre]
- Délais pour mise en place : [Préciser les délais]

6. Moyens de Communication Vocale (Population)
- Type de moyens (ex. : systèmes de notification d'urgence, annonces publiques) : [Préciser]
- Nombre nécessaire : [Préciser le nombre]
- Délais pour mise en place : [Préciser les délais]

7. Moyens de Stockage de Documents Informatisés
- Type de moyens (ex. : clés USB, disques durs externes) : [Préciser]
- Nombre nécessaire : [Préciser le nombre]
- Délais pour mise en place : [Préciser les délais]
- Note : Prioriser les sauvegardes papier pour la sécurité.

8. Mail
- Nombre de boîtes de service nécessaires : [Préciser le nombre]
- Délais pour configuration : [Préciser les délais]

9. Boîte Mail Spécifique pour Échanges Confidentiels
- Nombre nécessaire : [Préciser le nombre]
- Délais pour configuration : [Préciser les délais]

10. Coffre-Fort
- Nombre nécessaire : [Préciser le nombre]
- Délais pour mise en place : [Préciser les délais]

11. Logiciels / Applications
- Liste des logiciels/applications nécessaires : [Préciser le nom et créer une ligne pour chaque logiciel]
- Délais pour configuration : [Préciser les délais]

12. Moyens de Connexion Internet
- Type de moyens (ex. : modems, routeurs de secours) : [Préciser]
- Nombre nécessaire : [Préciser le nombre]
- Délais pour mise en place : [Préciser les délais]

13. Accès aux Archives
- Type d'accès requis (ex. : accès physique, accès via réseau de secours) : [Préciser]
- Délais pour mise en place : [Préciser les délais]

14. Plan de Communication en Absence de Téléphonie IP et Carnet d'Adresse Outlook
- Méthodes alternatives (ex. : listes de contacts papier, téléphones portables) : [Préciser]
- Délais pour mise en place : [Préciser les délais]
- Note : Tout document contenant des données personnelles doit être sécurisé (ex. : coffre-fort, mot de passe).

Organisation pour Poursuivre les Missions Essentielles en Mode Dégradé

1. Documents Indispensables pour Fonctionner en Mode Dégradé
- Liste des documents nécessaires : [Préciser]
- Organisation de leur stockage et accessibilité : [Préciser]

2. Interdépendances avec Autres Services ou Partenaires
- Liste des services ou partenaires inter-dépendants : [Préciser]
- Éléments échangés : [Préciser]
- Moyens de transmission : [Préciser]
- Contraintes de délai : [Préciser]

3. Préparation à la Reprise Post-Crise
- Organisation nécessaire pour la reprise : [Préciser]
- Documents à ressaisir après crise : [Préciser]
- Plan pour gérer la surcharge de travail (ex. : recrutement de renfort, maintien de la priorisation des activités) : [Préciser]

Annexe F : Origine de la démarche

La prolifération des attaques cyber concerne toutes les structures. Les collectivités territoriales ne sont pas épargnées. Les plus grandes comme les métropoles, ont en leur sein des services permettant de prendre en compte ce risque, tant en mettant en place les moyens pour se protéger, en sensibilisant leurs agents qu'en s'entrainant à gérer une crise cyber. Celles de taille intermédiaire ont l'opportunité de pouvoir profiter de mesures très efficaces mises en place en particulier par l'ANSSI pour monter en compétence. Par contre les plus petites communes restent l'angle mort. Or, que ce soit en termes d'impact sur le fonctionnement de la commune, de responsabilité pénale ou de confiance entre l'institution et le citoyen, le sujet est de même nature que pour les autres collectivités.

Dans le cadre du Comité Stratégique de Filière des industries de sécurité, et plus particulièrement dans le grand projet collectivités territoriales, les travaux menés depuis 2018 eu sein du groupe de travail "villes et territoires numériques de confiance face à la menace cyber" piloté par Rennes Ville & Métropole ont bien mis en lumière cette difficulté, typiquement pour les communes de moins de 3500 habitants, et la nécessité de les accompagner à mieux appréhender les risques cyber.

Les aider à faire figurer ce risque dans leur plan communal de sauvegarde (PCS) a été identifié comme l'approche la plus pragmatique, tant par sa dimension politique (c'est un document de responsabilité des élus) que par sa finalité très pragmatique (c'est une déclinaison opérationnelle locale des plans ORSEC). Par ailleurs, c'est un document dont la construction, par nature, embarque l'ensemble des protagonistes concernés, élus, services techniques, organismes externes impliqués par les différents sujets abordés.

Il est à noter que le risque cyber n'étant pas du périmètre ORSEC, nativement rien n'est prévu dans les plans types des PCS.

C'est sur cet axe qu'a souhaité, en priorité, travailler le "GT collectivités territoriales" du PEC en partenariat avec le CSF, en y apportant également quelques éléments permettant d'appréhender leur analyse de risque ainsi que quelques recommandations, voire d'identifier les supports permettant à un agent ou un élu volontaire de monter en compétence sur ce sujet.

Le présent document est le premier livrable de ce GT. Cette première version a vocation à être éprouver auprès de collectivités puis amendé au regard de leurs remarques afin qu'il soit encore plus une aide pour la prise en compte du risque cyber au sein de petites collectivités.

Annexe G : Lexique

ANSSI - Agence Nationale de la Sécurité et des Systèmes d'Information.

Évènement redouté - Un événement redouté est associé à une valeur métier et porte atteinte à un critère ou besoin de sécurité de la valeur métier.
Exemple : indisponibilité d'un service, modification illégitime de données, divulgations de données classifiées.
Les événements redoutés à exploiter sont ceux des scénarios stratégiques et se rapportent à l'impact d'une attaque sur une valeur métier. Chaque événement redouté est évalué selon le niveau de gravité des conséquences, à partir d'une métrique.

Gravité - Estimation du niveau et de l'intensité des effets d'un risque. La gravité fournit une mesure des impacts préjudiciables perçus, qu'ils soient directs ou indirects.

Menace - Terme générique utilisée pour désigner toute intention hostile de nuire dans le cyber espace. Une menace peut être ciblée ou non sur l'objet de l'étude.

Mesures de sécurité - Moyen de traiter un risque prenant les formes de solutions ou d'exigences pouvant être inscrite dans un contrat.
Nota : une mesure peut être d'ordre fonctionnel, technique ou organisationnel ; elle peut agir sur une valeur métier, un bien support, une partie prenante de l'écosystème, certaines mesures peuvent se renforcer mutuellement en agissant selon les axes complémentaires (gouvernance, protection, défense, résilience).

Plan de continuité d'activité (PCA) - Le PCA représente l'ensemble des mesures visant à assurer, selon divers scénarios de crises, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services ou d'autres tâches opérationnelles essentielles ou importantes de l'entreprise, puis la reprise planifiée des activités.

Plan de reprise d'activité (PRA) - Un PRA représente un ensemble de procédures, sous forme de plan d'actions structuré et documenté, qui vise à aider une entreprise à faire face à une catastrophe ou un incident tout en relançant rapidement son activité professionnelle.

Valeur métier - Dans le cadre de l'étude, composante importante pour l'organisation dans l'accomplissement de sa mission. Cela peut être un service, une fonction support, une étape dans un projet ou toute information ou savoir-faire associé.
Nota : les valeurs métier représentent le patrimoine informationnel qu'une source de risque aurait intérêt à attaquer pour porter atteinte à l'objet de l'étude.

Vulnérabilité - Faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser. Une vulnérabilité peut être utilisée par un code d'exploitation et conduire à une intrusion dans le système.

PÔLE D'EXCELLENCE
CYBER

www.pole-excellence-cyber.org